

TECHNICAL REPORT



**Communication networks and systems for power utility automation –
Part 90-22: SCD based substation network automated management with with
visualization and supervision support**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2024 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Secretariat
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IECNORM.COM : Click to view the full PDF of IEC 1250-30-22:2024

TECHNICAL REPORT



**Communication networks and systems for power utility automation –
Part 90-22: SCD based substation network automated management with with
visualization and supervision support**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-8327-0064-8

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	7
INTRODUCTION.....	9
1 Scope.....	10
2 Normative references	10
3 Terms, definitions and abbreviated terms	11
3.1 Terms and definitions.....	11
3.2 Abbreviated terms.....	13
4 Problem statement	15
4.1 Available technologies	15
4.2 Technical issues with current solution	15
4.2.1 Substation network configuration issues	15
4.2.2 Substation network testing and troubleshooting issues	16
4.2.3 Substation network operation and maintenance issues	17
4.2.4 Substation network cyber security issues.....	17
4.3 Proposed technical solutions for present issues.....	17
4.3.1 Substation network configuration based on SCD file	17
4.3.2 Substation network supervision and visualization.....	19
5 Use cases	20
5.1 Common actors.....	20
5.2 Use case 1: Substation network static-routing.....	21
5.2.1 Overview	21
5.2.2 Use case description	21
5.2.3 Example: An illustration of substation network static-routing	23
5.2.4 Static-routing scenario: Move of IED to a different port or bridge	27
5.2.5 Static-routing scenario: Add IEDs and bridges	29
5.2.6 Static-routing: Alternative technologies using SDN	30
5.3 Use case 2: Substation network auto-routing	31
5.3.1 Overview	31
5.3.2 Use case description	32
5.3.3 Example: An illustration of substation network auto-routing	33
5.3.4 Auto-routing scenario: Move of IED to a different port or bridge	35
5.3.5 Auto-routing scenario: Add IEDs and bridges.....	36
5.3.6 Auto-routing scenario: substation network topology recovery	38
5.3.7 Auto-routing scenario: forwarding path calculation	43
5.4 Use case 3: GOOSE/SV path visualization.....	45
5.4.1 Overview	45
5.4.2 Use case description	45
5.4.3 GOOSE/SV path visualization scenario: Normal state	46
5.4.4 GOOSE/SV path visualization scenario: Communication fail	47
5.4.5 GOOSE/SV path visualization scenario: IED duplication	48
5.5 Use case 4: Bridge configuration management	49
5.5.1 Overview	49
5.5.2 Use case description	50
5.6 Use case 5: Network information provided to HMI	50
5.6.1 Overview	50
5.6.2 Use case description	51

5.7	Use case 6: Impact analysis in case of adding simulation device	51
5.7.1	Overview	51
5.7.2	Use case description	51
6	Details of the auto-routing network configuration method	52
6.1	Requirement	52
6.1.1	Communication network topology discovery	52
6.1.2	IED-learning	53
6.1.3	Information presentation and monitoring	53
6.1.4	LN for bridge model	53
6.2	Principle for auto-routing	53
6.2.1	Auto-routing overview	53
6.2.2	IED-learning	54
6.2.3	Network topology discovery	55
6.2.4	Plot GOOSE/SV path	56
6.2.5	Install VLAN/MAC table configuration to bridges	56
6.2.6	Verify the correctness of built GOOSE/SV paths	57
6.2.7	TRILL example	57
6.3	Comparison of existing technologies	63
6.3.1	General	63
6.3.2	Comparison of network redundancy technology	63
6.3.3	Comparison of traffic control technology	64
6.3.4	Other available technology	64
6.4	Network device configuration	65
6.4.1	General	65
6.4.2	Network re-configuration scenarios	65
6.4.3	Silent IED support by IID	65
6.4.4	GOOSE/SV path configuration using BCD	66
6.4.5	Configuration version control	66
6.4.6	Example for network device configuration management	66
7	GOOSE/SV path presentation and monitoring	69
7.1	General	69
7.2	"Substation network static-routing" based approach	69
7.3	"Substation network auto-routing" based approach	69
7.3.1	GOOSE/SV path presentation	69
7.3.2	GOOSE/SV path monitoring	70
7.3.3	GOOSE/SV path data modelling	70
7.3.4	Example for information presentation and monitoring	72
8	GOOSE/SV path traffic control and engineering strategy	73
8.1	Overview	73
8.2	"Substation network static-routing" based approach	73
8.3	"Substation network auto-routing" based approach	74
8.3.1	GOOSE/SV path traffic control	74
8.3.2	Example for GOOSE/SV path traffic control	74
8.3.3	GOOSE/SV path traffic engineering strategy	75
8.3.4	Example for GOOSE/SV path traffic engineering strategy	75
9	Handling of simulated GOOSE/SV messages	77
9.1	General	77
9.2	"Substation network static-routing" based approach	77

9.3	"Substation network auto-routing" based approach	77
9.3.1	Dividing different operation plane with "s" bit	77
9.3.2	Example for handling the simulated GOOSE/SV message	78
10	Guidance on auto-routing network usage.....	81
10.1	General.....	81
10.2	Implementation of substation network auto-routing.....	81
10.3	Auto-routing usage case	85
10.3.1	IED position change or adding a new IED	85
10.3.2	Adding a new bay	89
10.3.3	SCD GOOSE/SV list application	90
10.4	Substation network visualization support.....	92
10.4.1	Substation network health state	92
10.4.2	Performance assessment of substation network	93
Annex A	(informative) Illustration for bridge configurator and BCD file	95
A.1	Generate BCD file with bridge configurator	95
A.2	Description of the demo use case	96
A.3	Demo BCD file	101
A.4	Usage of BCD file	103
A.4.1	General	103
A.4.2	Usage to perform IED learning.....	103
A.4.3	Usage to generate bridge configuration.....	104
Annex B	(informative) Recommendation of logical nodes	106
B.1	LN: AR-Bridge Name LARB.....	106
B.2	LN: AR-bridge Port Name: LARP.....	106
B.3	LN: AR-bridge Neighbour Name: LARN	107
B.4	LN: IED-Learning Outcome Name: LILO.....	107
B.5	LN: GOOSE/SV Egress Path Name: LGEP	108
Bibliography		109
Figure 1	– Static-routing engineering procedure, first stage	22
Figure 2	– Static-routing engineering procedure, second stage	23
Figure 3	– Physical substation network connectivity and planned GOOSE/SV path	24
Figure 4	– Static-routing within an RSTP ring.....	25
Figure 5	– Static-routing with a HSR ring	27
Figure 6	– Static-routing scenario diagram: Move of IED to a different port or bridge	28
Figure 7	– Static-routing scenario diagram: Add IEDs and bridges	29
Figure 8	– Use case diagram for substation network auto-routing	32
Figure 9	– Demonstration of a physical substation network topology	33
Figure 10	– Demonstration of substation network auto-routing	34
Figure 11	– Auto-routing scenario diagram: Move of IED to a different port or bridge	35
Figure 12	– Auto-routing scenario diagram: Add IEDs and bridges	37
Figure 13	– Use case diagram for substation network topology recovery.....	38
Figure 14	– Redundancy with Auto-routing and STP/RSTP	40
Figure 15	– Simplified Auto-routing network topology with STP/RSTP ring	40
Figure 16	– Redundancy with auto-routing and HSR	41
Figure 17	– Redundancy with auto-routing and PRP	42

Figure 18 – Redundancy in pure auto-routing network	43
Figure 19 – Use case diagram for forwarding path calculation.....	44
Figure 20 – Use case diagram for GOOSE/SV path visualization	45
Figure 21 – GOOSE/SV path visualization scenario diagram: Path normal state	46
Figure 22 – GOOSE/SV path visualization scenario diagram: Communication fail	47
Figure 23 – GOOSE/SV path visualization scenario diagram: IED duplication	49
Figure 24 – Use case diagram for bridge configuration management	50
Figure 25 – Use case diagram for Network information provided to HMI.....	51
Figure 26 – Use case diagram of impact in case of adding a simulated device	52
Figure 27 – TRILL encapsulating and decapsulating	58
Figure 28 – Ethernet and TRILL headers	59
Figure 29 – Illustration of LSP flooding	61
Figure 30 – Forwarding process of GOOSE/SV packet with TRILL	62
Figure 31 – LSP update procedure of an IED disconnection/addition	62
Figure 32 – LSP update procedure of a bridge addition/disconnection	63
Figure 33 – Origin network topology for BCD file (Version 1.00).....	67
Figure 34 – Minor version change due to bay extension.....	67
Figure 35 – Major version change of owe to the finish of substation phases.....	68
Figure 36 – Multiport AR-bridge model.....	71
Figure 37 – Logical relationship between the LNs	71
Figure 38 – Example of a GOOSE path presentation and monitoring (normal state).....	72
Figure 39 – Example of a GOOSE path presentation and monitoring (abnormal state)	73
Figure 40 – Illustration of GOOSE/SV path traffic control	74
Figure 41 – Illustration of GOOSE/SV path engineering	76
Figure 42 – Example of GOOSE/SV path traffic engineering	76
Figure 43 – Topology and subscription relationship for three bays	78
Figure 44 – Coexistence of simulation and actual signals	80
Figure 45 – Bridges and IEDs to be connected	82
Figure 46 – Final physical substation network.....	82
Figure 47 – Flow chart of auto-routing implementation	83
Figure 48 – Demonstration of IED move and addition.....	85
Figure 49 – IED move action.....	86
Figure 50 – Add new IED action.....	88
Figure 51 – Demonstration of adding a new bay.....	89
Figure 52 – Adding a new bay action	90
Figure 53 – Example of SCD GOOSE/SV list application.....	91
Figure 54 – Example of visual physical and logical topology	93
Figure 55 – Example of substation network assessment	94
Figure A.1 – Generation of BCD file.....	95
Figure A.2 – Logical view of exempld IEDs	97
Figure A.3 – Demo SCD file information (relevant and irrelevant to BCD)	98
Figure A.4 – Demo IID file information (relevant and irrelevant to BCD)	99
Figure A.5 – Demo BCD file structure generated from the demo SCD file and IID file.....	100

Figure A.6 – Using the demo BCD file to perform IED-learning	104
Figure A.7 – Using the demo BCD file to generate bridge configuration	105
Table 1 – Current steps followed on building GOOSE/SV paths in SCD	15
Table 2 – Pros and cons of static-routing and auto-routing.....	19
Table 3 – Common actor	20
Table 4 – Extracted subscription information of IED1, IED2 and IED3	24
Table 5 – Generated bridge configuration information	25
Table 6 – Generated bridge configuration information with redundancy path	26
Table 7 – Generated bridge configuration information (including all interconnect ports of the RSTP ring)	26
Table 8 – Extracted subscription information of IED1, IED2 and IED3	33
Table 9 – Outcome of IED learning	34
Table 10 – Example of GOOSE/SV ingress flow table	54
Table 11 – Advantages and drawbacks of auto-routing versus RSTP, HSR or PRP	64
Table 12 – Advantages and drawbacks of different traffic control strategies	64
Table 13 – Scenarios requiring network re-configuration	65
Table 14 – Traffic estimation	75
Table 15 – Data flow inside a bay	78
Table 16 – Data flow cross bays	78
Table 17 – Extracted subscription information of the example	79
Table 18 – Example forwarding table of maintenance plane (SW1)	79
Table 19 – Example forwarding table of working plane (SW1)	81
Table 20 – Example forwarding table of working plane (SW2)	81
Table 21 – GOOSE/SV associations abstracted from SCD file	83
Table 22 – Topology discovered and IED-learning result of Figure 44	84
Table 23 – Generated GOOSE/SV flow table	84
Table 24 – Example forwarding table of AR-bridge SW1	85
Table 25 – GOOSE/SV associations related with IED e7	86
Table 26 – SCD GOOSE/SV list example of SW2	91
Table A.1 – Elements different between SCD file and BCD file.....	95
Table A.2 – IED subscription information in demo SCD file	96
Table B.1 – Data objects of LARB	106
Table B.2 – Data objects of LARP	107
Table B.3 – Data objects of LARN	107
Table B.4 – Data objects of LILO	108
Table B.5 – Data objects of LGEP	108

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**COMMUNICATION NETWORKS AND SYSTEMS –
FOR POWER UTILITY AUTOMATION –****Part 90-22: SCD based substation network automated management with
visualization and supervision support**

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC TR 61850-90-22 has been prepared by IEC technical committee 57, Power systems management and associated information exchange. It is a Technical Report.

The text of this Technical Report is based on the following documents:

Draft	Report on voting
57/2692/DTR	57/2737/RVDTR

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

The language used for the development of this Technical Report is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all parts in the IEC 61850 series, published 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 document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The "colour inside" logo on the cover page of this document 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

As an international standard, IEC 61850 currently serves thousands of substations around the world. Meanwhile, SCD configuration is subject to changes that could be brought up by retrofit, addition or removal of IED(s), etc., and the configuration of bridges needs to be updated accordingly. The procedures of these works have always relied on manual approaches.

Some questions raised naturally are the following.

- How does a bridge in the substation network update its configuration (e.g. VLAN setting) dynamically in case of SCD changes?
- How does a GOOSE/SV path rebuild automatically following the SCD update instead of being done manually?
- How does the bridge learn that a newly added IED is connected to it?
- How does a bridge discover the change in case of substation network connectivity changes?

These questions are the drivers to set up a Task Force to investigate the above questions and develop IEC TR 61850-90-22. These issues were demonstrated, gaps were identified, requirements were analysed and use cases are described in this document, which is a Technical Report.

To address these, the concept of auto-routing is introduced in this document.

At present, auto-routing is a system-level functionality of substation network performing through a combination of a variety of advantages of AR-Bridges as specified in this document. AR-Bridges could provide sophisticated function compared with IEC 61850 bridges that are employed in existing network systems. Auto-routing is an independent functionality and can co-exist with HSR/PRP and RSTP within a network.

The recovery time of auto-routing network is not addressed in this document. The key reason for this is that the system or AR-bridge should take out of service for the testing of the functionality after distribution or updating of the new SCD.

COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

Part 90-22: SCD based substation network automated management with visualization and supervision support

1 Scope

This part of IEC 61850, which is a Technical Report, aims to provide analysis, principles, use cases and guidance on how to use GOOSE/SV static-routing or auto-routing based on System Configuration Description (SCD) file to automated manage the substation network while without changing the requirements of IEDs. Furthermore, this document also intends to give novel practices on network and GOOSE/SV path condition monitoring which support visualization and supervision from higher level application side.

Using the concepts developed in the IETF's Transparent Interconnection of Lots of Links (TRILL) using IS-IS protocol that is defined in RFC 6326 and ISO/IEC 10589 standards, this document defines network and system management data object models that are specific to power system operations. These data objects will be used to monitor the health of networks and systems, to detect abnormal behaviours of IEDs which contradict SCD file, such as unexpected IEDs or unexpected GOOSE/SV flows, and to support the management of the performance and reliability of the information infrastructure.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 61850 (all parts), *Communication networks and systems for power utility automation*

IEC 62351 (all parts), *Power systems management and associated information exchange – Data and communications security*

IEC 62351-7:2017, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and System Management (NSM) data object models*

IEC TR 62351-90-3:2021, *Power systems management and associated information exchange – Data and communications security – Part 90-3: Guidelines for network and system management*

IEC 62439-1, *Industrial communication networks – High availability automation networks – Part 1: General concepts and calculation methods*

IEC 62439-3:2021, *Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*

IEC 62443 (all parts), *Security for industrial automation and control systems*

IEEE Std 802.1AB™, *IEEE Standard for local and metropolitan area networks – Station and Media Access Control Connectivity Discovery*

IEEE Std 802.1D™, *IEEE Standard for local and metropolitan area networks –Media Access Control (MAC) Bridges*

IEEE Std 802.1Q™, *IEEE Standard for local and metropolitan area networks – Bridges and bridged networks*

IETF RFC 6325, *Routing Bridges (RBriges): Base Protocol Specification*

IETF RFC 6326, *Transparent Interconnection of Lots of Links (TRILL) Use of IS-IS*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in IEC TR 61850-90-4 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

3.1 Terms and definitions

3.1.1

GOOSE/SV auto-routing

method of dynamic building of GOOSE/SV paths using VLAN/MAC tables in bridges, according to GOOSE/SV association together with the outcome from network topology discovery and IED learning, abbreviated as auto-routing in this document

3.1.2

GOOSE/SV static-routing

method of static building of GOOSE/SV paths using VLAN/MAC table in bridges according to the information defined in SCD file, abbreviated as static-routing in this document

3.1.3

AR-bridge

AutoRouting-bridge

bridge with sophisticated function extended from IEC 61850 bridge, that is the fundamental device or component to approach the performance of substation network auto-routing

3.1.4

AR-bridge neighbour

node that physically connects to the AR-bridge, and responds to the information it is advertising

3.1.5

bridge

network device that connects network segments at the data link layer (layer 2) of the OSI model, according to the principles of IEEE 802-2014

Note 1 to entry: A bridge is often referred to as a "layer 2 switch". In this document, the word "bridge" means the logic used to forward a frame from one port to another at layer 2, while "switch" designates a device with additional functionalities.

Note 2 to entry: In case of confusing with primary switch, bridge is used to represent switch in this document.

[SOURCE: IEC TR 61850-90-4:2020, 3.1.1, modified (addition of Note 2 to entry)]

3.1.6

diagnostic device

device/software that can capture arbitrary IEC 61850 packets, analyse the contents of packets, and reveal the transmission behaviour of packets

3.1.7

IEC 61850 bridge

subset of the IEEE 802.1 options with extensions defined in IEC 61850-8-1 and IEC TR 61850-90-4

Note 1 to entry: With the following functionality:

- A bridge port operates in full-duplex mode.
- A bridge supports loop prevention only through RSTP/MSTP; Compatible variants offered by vendors to speed up recovery are allowed, although the claimed performance is usually only achieved within a one-vendor environment.
- A bridge keeps MAC address filtering always enabled. The lifetime of a filtering database entry is limited to 10 seconds (IEEE 802.1Q recommends 300,0 s).
- A bridge supports VLAN traffic filtering, but contrarily to IEEE 802.1Q, an egress port may send a frame with VLAN ID = 0, although this practice is deprecated.
- A bridge (edge) port may forward frames with different VLAN ID to an end device (thus behaving as a trunk port). A bridge port is not obliged to remove the VLAN tags. Contrarily to the intention of VLANs, end devices may be attached simultaneously to several VLANs, but ignore the VLAN header.
- A bridge port accepts VLAN-tagged frames from an end device even when they do not match its default VLAN-ID.
- A bridge supports frames of at least 1 522 octets to allow redundancy control in HSR or PRP, support of up to 1 535 octets is recommended. Jumbo frames are not used.
- A bridge may start transmission of a frame over the egress port while the frame over the ingress port has not been completely received ("cut-through"), although IEEE 802.1 only allows sending after the frame has been completely received ("store-and-forward").
- A bridge acting as a Transparent Clock for the Precision Time Protocol modifies the time stamp in the frame body, but it is not allowed to modify the source address, contrarily to the debated IEEE 802.1 rule.
- A bridge supports network management by IEC 61850-90-4 especially for the purpose of ports and RSTP settings, VLAN and priorities settings and multicast filtering.

3.1.8

IED-learning

mechanism that learns by bridges of the port that IEDs are connected to by detecting the unique identity (for instance MAC, APPID, or a combination of elements) of GOOSE/SV packets, and mapping between them and the IED name, which are extracted from SCD file, similar to the MAC address learning

3.1.9

GOOSE/SV association

relation expressed in an SCD file between an IED (serving a data by publishing a GOOSE/SV control block containing this data in its dataset) and one or more IEDs (consuming this specific data by subscribing the GOOSE/SV)

Note 1 to entry: The consumption of this data by the IED subscribing to the GOOSE/SV is described by an ExtRef in the consuming IED referencing the data and the GOOSE/SV carrying the data.

3.1.10

GOOSE/SV path

GOOSE/SV multicast distribution tree created in substation network to implement GOOSE/SV association, rooted at source port of a GOOSE/SV packet from one publisher, ended at destination ports of all subscribers, including intermediate bridges

3.1.11

GOOSE/SV simulator

device/software that generates simulated GOOSE/SV packets for a given existing frame

3.1.12 maintenance plane working plane

logical independent virtual working area created by an AR-bridge for IEDs in testing mode or related testing instruments generating simulated GOOSE/SV messages

3.1.13 plug-and-play

feature of substation network that allows an IED to be connected to any port of any bridge without the need of configuration of the bridge

3.1.14 RedBox

device attaching single attached nodes to a redundant network

3.1.15 Routing Bridge RBridge

bridge using IS-IS protocol routing and encapsulation of traffic with a header that includes a hop count to provide optimal pair-wise forwarding without configuration, safe forwarding even during periods of temporary loops, and support for multipathing of both unicast and multicast traffic, and compatible with previous IEEE 802.1 customer bridges

Note 1 to entry: The definition is taken from "RFC 6325:2011 Routing Bridges (RBridges): Base Protocol Specification".

3.1.16 SCD GOOSE/SV list

list of GOOSE/SV defined in SCD file by which the accessing legality of IEDs in substation network is identified

3.1.17 switch

interconnection device between network parts, e.g. a simple repeater (hub), a layer 2 connecting device (bridge) or a layer 3 connecting device (router) or a combination thereof

Note 1 to entry: This document uses "switch" for a complex device, while bridge refers to the IEEE 802-2014 functionality. Electrical switches are designated as "switchgear", "circuit breaker" or "disconnecter".

[SOURCE: IEC TR 61850-90-4:2020, 3.1.30]

3.1.18 silent IED

IED that does not publish any packets but may be a subscriber

3.1.19 topology discovery

automated process that keeps detecting and tracking switches and their interconnection in substation network

Note 1 to entry: Topology in the document refers to communication network, not electrical power system.

3.2 Abbreviated terms

ACL	Access Control List
APPID	Application ID in GOOSE and SV messages
AR	Auto Routing
BCD	Bridge Configuration Description
BFD	Bidirectional Forwarding Detection

BPDU	Bridge Protocol Data Unit (RSTP)
DMAC	Destination MAC address
ECMP	Equal Cost Multipath
FIB	Forwarding Information Database
GMRP	Generic Multicast Registration Protocol
GOOSE	Generic Object Oriented Substation Event (IEC 61850-7-2, IEC 61850-8-1)
HMI	Human-Machine Interface
HSR	High-availability Seamless Redundancy (IEC 62439-3)
IED	Intelligent Electronic Device (IEC 61850-1)
IID	Instantiated IED Description (IEC 61850-6)
IP	Internet Protocol (IETF RFC 791)
IS-IS	Intermediate System to Intermediate System
L2	Layer 2
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol (IEEE 802.1AB)
LN	Logical Node
LSP	Link State Protocol
MAC	Media Access Control (IEEE 802.3)
MIB	Management Information Base (IETF RFC 3416)
MMRP	Multiple Multicast Registration Protocol
MU	Merging Unit (Logical Device), merging unit (physical device)
OAM	Operations, Administration, and Maintenance
O&M	Operation and Maintenance
PRP	Parallel Redundancy Protocol (IEC 62439-3)
PTP	Precise Time Protocol
RSTP	Rapid Spanning Tree Protocol (IEEE 802.1Q-2018, 13.4)
SDN	Software Define Network
SMAC	Source MAC address
SNMP	Simple Network Management Protocol (IETF RFC 3416)
SPB	Shortest Path Bridging
SV	Sampled (measurement) values (IEC 61850-9-2)
VID	VLAN identifier (IEEE 802.1Q)
VLAN	Virtual Local Area Network (IEEE 802.1Q)

4 Problem statement

4.1 Available technologies

In a substation based on IEC 61850, a communication network is utilized to exchange GOOSE/SV messages between IEDs, which replace the point-to-point cable wiring mode in a traditional substation. GOOSE/SV messages use for propagation the L2 multicast domain; consequently, without applying traffic engineering strategies and techniques, the GOOSE/SV traffic will be forwarded to every available egress port in the whole substation network. Therefore, if all IEDs in a network are on a single multicast domain, the traffic on each bridge port may go far beyond the port forwarding capability under some abnormal circumstances. Currently, the main solutions for traffic engineering are the usage of VLAN, GMRP, and L2 multicast filtering; the deployment needs to be done partially or entirely manually, and it results in inefficiency, especially with larger-scale substation network.

In addition, other communication principles exist, such as point-to-point communication and webservices, which are not addressed in this document.

4.2 Technical issues with current solution

4.2.1 Substation network configuration issues

In an IEC 61850 substation, time-critical control/protection tasks are performed by coordination among multiple IEDs. While legacy copper wiring is mostly a peer-to-peer direct connection without any communication network configuration, GOOSE/SV paths, however, are multi-node chains built on top of bridges and thus configuration work is inevitable. The steps listed in Table 1 are followed to build GOOSE/SV paths in SCD.

Table 1 – Current steps followed on building GOOSE/SV paths in SCD

Steps	Description
Step 1	Retrieve the latest version of SCD file of the substation and extract all GOOSE/SV associations in the SCD file. This implicates an existing SCD is a pre-requisite to substation network setup.
Step 2	Collect network topology, including the trunk ports between bridges and IEDs connected to bridge port(s). Meanwhile, network with redundancy should be considered.
Step 3	Plot distribution tree for each GOOSE/SV packet based on the information collected in steps 1 and 2. Output all GOOSE/SV VLAN filtering table and/or MAC multicast filtering table for each bridge.
Step 4	Load VLAN filtering table and/or MAC multicast filtering table to each bridge.
Step 5	Verify the setup of each GOOSE/SV path by collecting information from all subscribe IEDs.

In field practices, the GOOSE/SV path setup has never been a one-time job. Some factors, such as SCD update, could trigger a network re-configuration process. An efficient network configuration method is so fundamental that it stays along with the life cycle of a substation. The amount of network configuration work load depends on the size of the substation network; it arises with the scale. Although there might be some tools that could help, this does not alleviate the fundamental problem, such as the work of verification of bunches of inputs.

Post-configuration verification presents another challenge. Verification means that on each bridge port connected to IED, the GOOSE/SV packets this IED is subscribed to are actually being forwarded to that port. To verify the correctness of the GOOSE/SV setup, one pre-requisite is that all GOOSE/SV packets are generated either from the publishing IED or a GOOSE/SV simulator device. After all GOOSE/SV packets are ready, there are two possible methods to verify that packets are properly forwarded.

- 1) Passive inspection: a kind of thorough inspection mode by connecting a packet sniffer to each port of the bridge that the subscriber IED would be connected to, capturing the packets and verifying if the packets are the ones the IED has subscribed to.
- 2) Active report: a method that let subscriber IEDs report extra or missing GOOSE/SV packets, then collect all these reports to make decision.

The configuration for large-scale substation network might be a challenge for engineers without automatic approaches. This is the issue addressed in this document.

4.2.2 Substation network testing and troubleshooting issues

Any system level functionality test that involves multiple IEDs has to be conducted in a networked environment, no matter in the factory or in the field. In such case, there are at least three parties participating in testing in which an IED can be a subscriber and a publisher at the same time:

- 1) Publisher IED(s) that generate GOOSE/SV packets.
- 2) Network that forwards GOOSE/SV packets.
- 3) Subscriber IED(s) that receive GOOSE/SV packets.

When testing goes wrong, a debugging process is brought into place. Then the network, with redundancy or not, naturally becomes a first place to look at. A diagnostic device is expected to be connected to the network under the situation to monitor those suspicious ports, analysing the head of GOOSE/SV packets to get a question glimpse. Normally, a mirror port would be set to connect the diagnostic device, and a typical troubleshooting procedure is as follows:

- 1) Does the network actually receive GOOSE/SV packets from publisher IEDs as expected? If not, fix the publisher IEDs, otherwise, go to the next step.
- 2) Does the network actually forward those GOOSE/SV packets to subscriber IEDs without lost? If not, fix the network, otherwise check the subscriber IED(s).

In a networked environment many things can go wrong, e.g., GOOSE duplication, unexpected connection of redundant network, loop, excessive packet loss due to poor bandwidth allocation, etc. ([1]¹, [2]). It is obvious that a certain level of support provided by the network infrastructure will help efficient system level testing.

On the other hand, there are new challenges when an IEC 61850 substation extension project is taking place, and it will run into more complicated situations. To thoroughly conduct system testing for newly added IEDs because of substation extension, a temporary working environment/plane may help ease the engineering process, which includes:

- 1) A properly configured network that connects newly added IEDs for GOOSE/SV/MMS communication.
- 2) A path by which certain GOOSE/SV packets from operational system are able to be forwarded to working plane, but not otherwise.
- 3) PTP service might be necessary in working plane.

After the system test is completed, two more steps are needed to put newly added IEDs into the operational system:

- 1) Procedures that merge the working plane into the operational system.
- 2) Procedures that update the SCD to newer version on existing system, update cross bay functionalities (bus protection relay, etc.), if any.

¹ Numbers in square brackets refer to the bibliography.

The network plays an important role in such a scenario that the test mode architecture defined in IEC 61850 system has not yet matured enough in IEDs. Essentially, it supports two working spaces at the same time, one for the operational system, and one for testing purposes. It also needs to have provisions that two working spaces can interact in a controlled manner, as well as flexibility to make merging process relatively easy.

4.2.3 Substation network operation and maintenance issues

The substation network implements logical connections among IED devices, but these connections are not materialized in a concrete way directly; they are normally shown in the form of a table. The only visible thing is the physical network topology. With reference to the network topology, the maintenance operator can only acquire the devices that are connected to the bridges.

In respect of O&M, there are several challenges. The network is basically a black box for the O&M operator in terms of the GOOSE/SV path. The only useful information for the operator or maintenance personnel is a collection of disconnected pieces of information, such as the SCD file, network configuration, etc. but the operator lacks:

- 1) the experience to judge whether the configuration of bridges can fulfil the implementation of GOOSE/SV association in SCD file;
- 2) runtime information about GOOSE/SV path, for example, mapping between a bridge port and a connected IED.

4.2.4 Substation network cyber security issues

Cyber security issues are not covered by this document.

IEC 62351 (all parts) and IEC 62443 (all parts) can be referred to if there is a cyber security problem in substation.

NOTE The functionality of GOOSE/SV auto-routing is not impacted when MACsec (Media Access Control Security) is used, for other layer 2 encryption mechanism, it depends.

4.3 Proposed technical solutions for present issues

4.3.1 Substation network configuration based on SCD file

This document describes two approaches that have the goal to automate the configuration of substation networks, which is achieved by using information about substation network topology and data from the SCD file to automatically determine the configuration of network devices, such as bridges and routers, so that the end devices like IEDs and MUs can communicate with each other as defined in the SCD. A summary of these two approaches is introduced here, and more detailed information can be found in corresponding clauses in this document.

The first approach is substation network static-routing, which is described in 5.2 and which accommodates that the functionality of substations often is static and remains unchanged during quite a long life cycle – apart from functional improvements and extensions, technology changes in the hardware or corrections of recognized problems. The static-routing approach targets the use of well-established equipment and technologies such as VLAN-aware bridges and redundancy protocols like PRP/HSR or time synchronization protocols like PTP, which in turn enables the continued use of the installed base.

The basic principle of the static-routing approach is that the entire network configuration is computed offline based on the data exchange between devices, network topology and optionally bridge object model representing the network switches, all of them documented in SCD.

This can be achieved using one or several System Configurator Tools (SCT). When several SCTs are involved, they may for instance interact in an iterative process as illustrated in Figure 1 and Figure 2 to engineer the overall substation configuration of end devices and network devices. The engineering of end devices – like IEDs, MUs and how they communicate with each other – is done by one SCT A (IEDs) while the engineering of network devices is done by another SCT B (Bridges) which is called "Bridge Configurator" in 5.2 of this document. Since both SCTs need to mutually exchange information, the static-routing approach follows IEC 61850-6:2018, Clause 5 (Intended engineering process with SCL) which defines SED files for this purpose.

Since the paths of the GOOSE/SV streams depend on the network topology of the substation, the SCT with the bridge configurator role needs to know what the network topology looks like. This can be achieved in different ways, for example by designing and configuring the network topology offline or detecting an existing network topology with well-established protocols such as LLDP. The SCT with the bridge configurator role parses the content of the SED file that was exported by SCT A (IEDs) and renders the paths of the GOOSE/SV streams between publishers and subscribers. The SCT with the bridge configurator role can then determine the paths through the topology and derive the required bridge configuration. Based on this information, the SCT with the bridge configurator role generates an SED file that contains the corresponding configuration data for all bridges through the individual bridge object model, which is specified in IEC 61850-90-4:2020. The SCT A (IEDs) uses the data from the imported SED file to extend the content in the overall SCD with the data of the bridges, so that the substation SCD reflects a model of the whole substation application including the required communication of the corresponding bridges. The deployment of the bridge configuration can be done by means of well-established protocols like SNMP/MIB, Netconf/YANG, etc.

The second approach is substation network auto-routing. A related use case is described in 5.3, which considers a more dynamic approach in which the communication paths between end devices are built by means of the GOOSE/SV associations in the SCD file, together with the substation physical network topology that is auto-obtained from the outcome of network topology discovery and IED-learning. In this approach, the physical connectivity information is detected by network devices themselves, and the VLAN/MAC table will be generated and installed to the bridges automatically. The auto-routing way can keep the current SCD file unchanged; if the physical connectivity is described by communication in the SCD file, then it is irrelevant to the building of GOOSE/SV communication paths, but useful for the path verification. In the same way as substation network static-routing, a bridge configurator is required to parse SCD files to abstract the necessary information to build GOOSE/SV paths. The differences are that the bridges need to know their neighbours' information via control protocols (like TRILL) to build the network topology and then participate calculating the communication paths for GOOSE/SV streams, so more sophisticated functions would be expected to be provided by the bridges which support auto-routing, which is called AR-bridge in this document.

Both static-routing and auto-routing offer a solution for auto-configuration of substation network and have individual pros and cons that are summarized in Table 2.

Table 2 – Pros and cons of static-routing and auto-routing

Use Case	Idea	Pros	Cons
Static-Routing	1) Info about network topology (i.e. bridge-bridge and bridge-IED connections) is configured by means of the Bridge Configurator and is added to the SCD file. 2) The Bridge Configurator parses the SCD file, renders the paths of the GOOSE/SV streams through the topology, derives the required bridge configurations and loads them into bridges.	• Network device base is not affected. • Usage of well-introduced protocols possible. • Bridge Configurator provides central view of network configuration.	• Development/deployment of Bridge Configurator required.
Auto-Routing	1) SCD file does not contain network topology info. 2) BCD file (which is a reduced SCD file) is loaded into bridges; bridges parse the BCD file and learn logical GOOSE/SV paths. 3) Bridges auto-detect connected IEDs (by parsing GOOSE/SV messages). 4) Bridges auto-detect bridge inter-connection topology via intelligent network control protocol (e.g. TRILL). 5) Each bridge calculates overall network topology, renders required configuration for itself and applies it.	• Intelligent Bridge Configurator is not required, bridges both parse the BCD file and take care of their own configuration. • Plug-and-play engineering environment provided for IEDs and bridges.	• Network device base must be replaced with more sophisticated bridges (AR-bridges). • AR-bridges use more advanced network control protocols. This might require extra configuration effort of those network control protocols.

In general, the idea of static-routing and auto-routing is that based on SCD file, the bridges in the network can be configured automatically to precisely implement the GOOSE/SV forwarding by the appropriate information extracted from the SCD file with a related technical mechanism. Utilizing one single configuration file to fit all the bridges in a substation is achievable, and a BCD file is proposed in this document to implement this goal, as exemplified in Annex A. Although the idea of configuring the substation network with the SCD file has been mentioned in IEC TR 61850-90-4:2020, it does not provide practical guidelines, which are addressed by this document. Network topology and GOOSE/SV association are the necessary elements of the static-routing and auto-routing application. This information can be used to automatically derive the configuration of all network devices such as bridges and/or routers so that the required communication can be carried out as needed for the streams defined in the SCD. Static-routing or auto-routing only impact the network forwarding of GOOSE/SV messages, other types of messages are irrelevant.

NOTE A bridge supporting auto-routing requires more sophisticated functions than typical IEEE802-2014 bridges currently used in substations.

4.3.2 Substation network supervision and visualization

On top of the implementation of substation network automatic configuration, more supervision and visualization on substation networks could be gained from the standpoint of the function model, such as visualization of network topology and accessed IEDs, GOOSE/SV path information statistics, GOOSE/SV forwarding tree graphic display, precise fault location and SCD GOOSE/SV list, etc.

A list of GOOSE/SV multicast addresses that are related to the IEDs defined in the SCD file, by which to identify the accessing legality of IEDs in substation networks, could be used to help ease the management of substation networks. Related bridges' data information, including bridge ID, port ID, port link status, port counter statistical data and connected IED information etc. could also be gathered as the information source to support the substation network supervision and visualization, then sent to HMI by appropriate means. Protocols such as SNMP can be utilized to supervise the relevant information of the network to some extent.

5 Use cases

5.1 Common actors

Table 3 contains the list of the actors commonly used in this document. If additional (and specific) actors are needed in the description of the use case, they will be described in the corresponding subclause dedicated to the given use case.

Table 3 – Common actor

Actor name	Actor type	Actor description
Intelligent Electronic Device (IED)	System	Any device incorporating one or more processors, with the capability to receive or send, data/control from, or to, an external source, for example electronic multi-function meters, digital relays, controllers. Device capable of executing the behaviour of one or more specified logical nodes in a particular context and delimited by its interfaces. [SOURCE: IEC TS 61850-2:2019, 3.38]
Bridge	System	Refer to definition of bridge, 3.1.5 Bridge is defined as interconnection device between network parts, e.g. a simple repeater (hub), a layer 2 connecting device (bridge) or a layer 3 connecting device (router) or a combination thereof). [SOURCE: IEC 61850-90-4:2020, 3.1.1]
System configurator	System	An IED independent system level tool that can import or export configuration files defined by IEC 61850, it allows system information to be added to perform system level engineering and generate SCD file. The system configurator should be able to read a system specification file for example as a base for starting system engineering, or to compare it with an engineered system for the same substation. [SOURCE: IEC 61850-6:2009, 5.3, modified]
IED configurator	System	A manufacturer-specific tool that can import or export the files defined by IEC 61850, it provides IED specific settings and generates IED-specific configuration files, or it loads the IED configuration to the IED. [SOURCE: IEC 61850-6:2009, 5.3, modified]
Bridge configurator	System	A tool that can extract GOOSE/SV associations from SCD and IID file and generate an SED file that contains the corresponding network device configuration data which can be used to update the SCD with the bridge related configuration data, If the IED configuration tool for bridges is integrated, it can generate bridge configuration, and load it to bridges.
Substation design specification	Document	Documentation that can specify and guide the construction of substation, including physical network topology.
O&M staff	People	A local user which is a technician having to intervene on the process of substation engineering, operation and maintenance.
Archive	Process	The process to store documentation.
Publisher IED	System	An IED which has the source of dataset for publishing.
Subscriber IED	System	An IED which subscribes the dataset of publishers.
Pure Subscriber Device	System	Any device that only subscribes to the publisher's message and without publishing any messages.
Simulation device	system	A device or software that generates simulated GOOSE/SV packets for a given existing frames.
HMI	system	Human machine interface used to configure, maintain and manage substation with graphic display.

5.2 Use case 1: Substation network static-routing

5.2.1 Overview

Substation network static-routing provides a way to statically build a path for GOOSE/SV messages according to the substation physical network connectivity and relative information extracted from the SCD file and IID file (optional, normally for use of add-ons or adapted values). Configuration information (e.g. VLAN/Multicast MAC table) is generated to configure the bridges in substation network to make the GOOSE/SV messages forward along the pre-designed transmission path.

NOTE IID for the fixed IED that existed in SCD file or about for permanent use could be incorporated into the SCD file, while suggesting that the IID file for temporary IED not merge into the SCD file.

In the substation network static-routing use case, the necessary information required to generate the static GOOSE/SV paths includes GOOSE/SV associations, physical connectivity between IED and bridge, and interconnection between bridges. As described in 4.3.1 this information is documented in the SCD and any element changes (i.e. IED move, IED add/remove etc.) will trigger the rebuild process of GOOSE/SV paths.

The substation network engineering process includes that the substation O&M staff completes the configuration of the substation network and the IEDs, connects the bridges and the IEDs according to the substation design specification, and puts the substation network into working state. When the GOOSE/SV packet sent by an IED publisher arrives at a bridge, the bridge looks up its static configured VLAN/MAC entries and then forwards the packet to the specified egress port. The workflow is illustrated in the following subclauses.

5.2.2 Use case description

Figure 1 and Figure 2 show the workflow and interaction of the different components that are involved in the engineering procedure. The procedure is based on the approach described in 5.3.6.3 of IEC 61850-4:2020. The "System configurator tool A (IEDs)" takes care of the configuration of all end devices like IEDs and MUs while the "System configurator tool B (Bridges)" – or Bridge Configurator Tool – takes care of the configuration of all bridges in the substation network. If applicable, network topology could be handled by the System Configurator Tool A (IEDs).

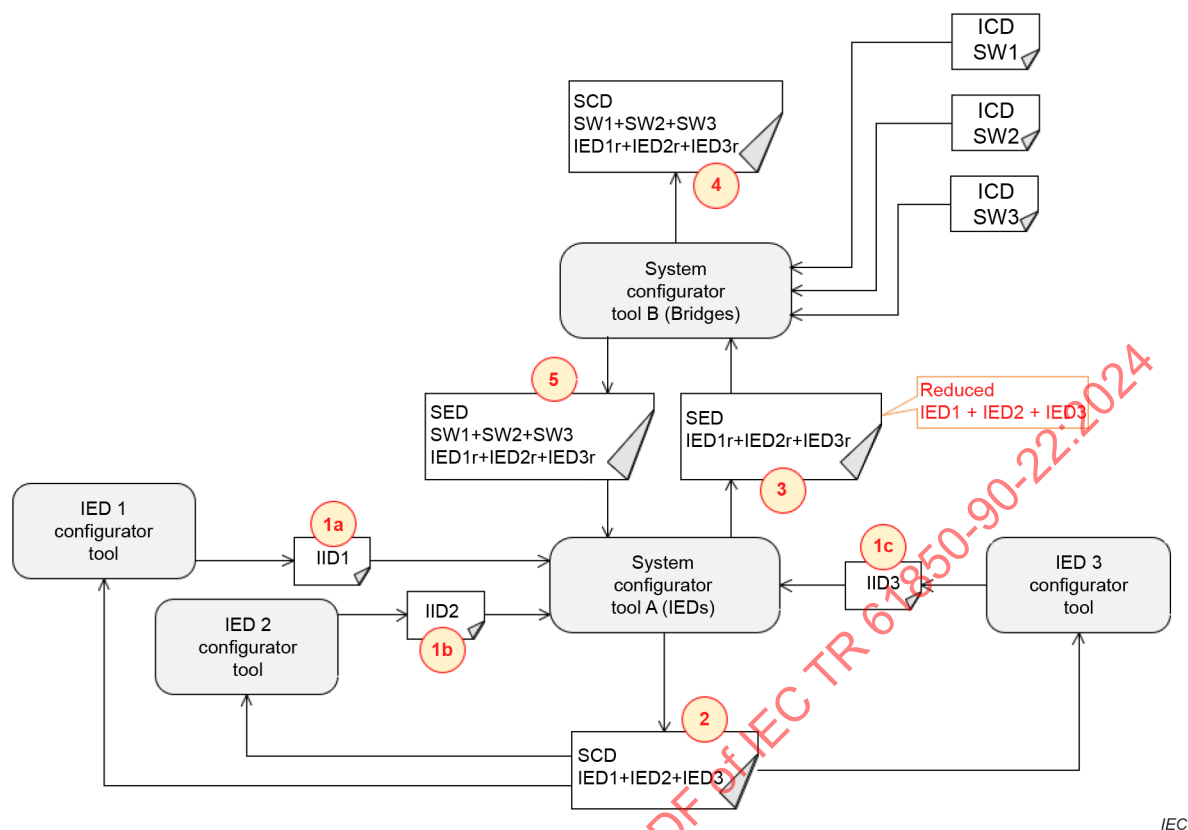
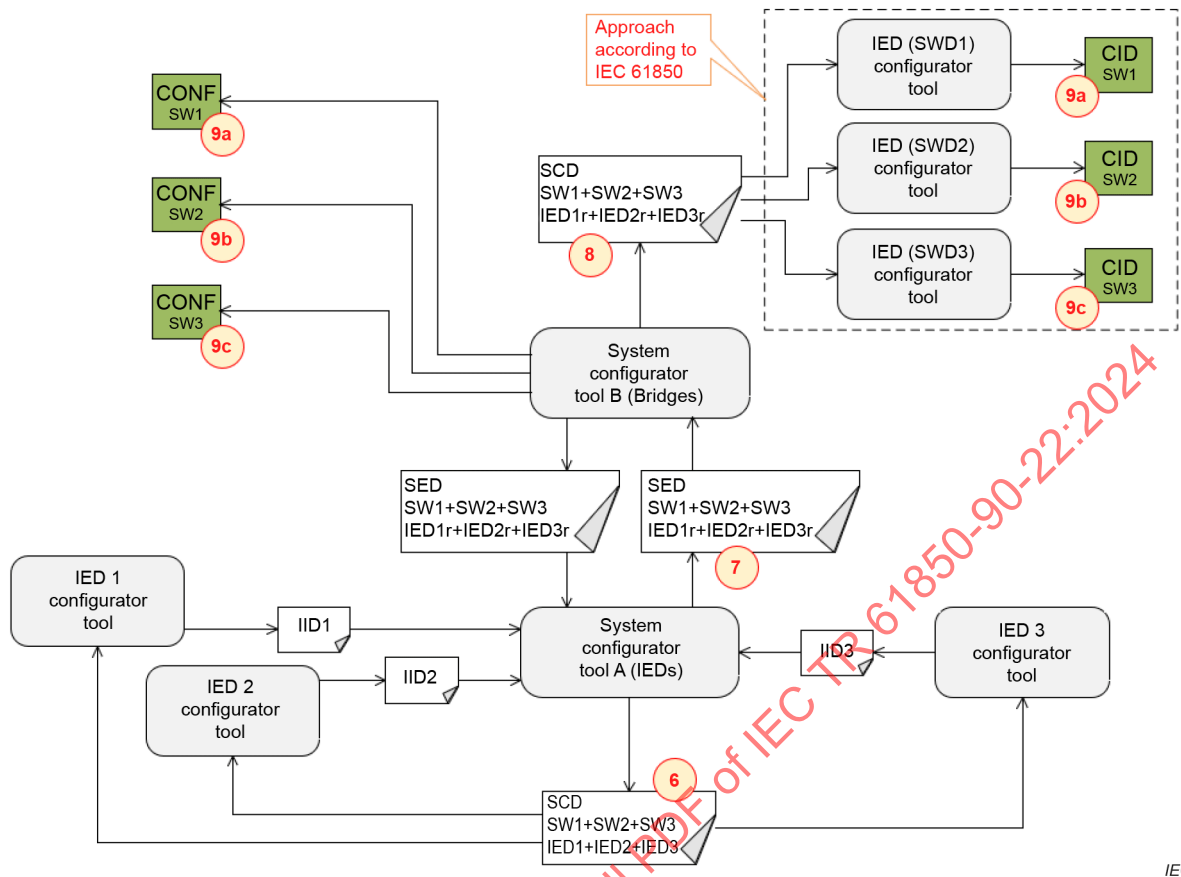


Figure 1 – Static-routing engineering procedure, first stage

- Step 1: IED Configurator Tools create .iid files for IED1, IED2 and IED3.
- Step 2: System configurator tool A (IEDs) creates a .scd file describing IED1, IED2 and IED3 and using the previous .iid files.
- Step 3: SCT A (IEDs) creates a new .sed file IED1r, IED2r and IED3r, which gives only required information of all IEDs needed for the engineering of the bridges (hence "Reduced IED1r+IED2r+IED3r").
- Step 4: System configurator tool B (Bridges) imports the .sed file from the previous step and .icd files representing the bridge data (SW1, SW2 and SW3). The network topology is added unless already present. SCT B (Bridges) evaluates the corresponding GOOSE/SV streams and computes the corresponding VLAN, Multicast Filtering etc. configuration of the bridges. According to the IEC 61850 engineering process, SCT B (Bridges) stores an .scd SW1+SW2+SW3 and IED1r+IED2r+IED3r file. This .scd file can be considered a "reduced" SCD because it contains the network topology and data of all bridges but only reduced information of the end devices (IEDs, MUs).
- Step 5: SCT B (Bridges) exports an .sed SW1+SW2+SW3 and IED1r+IED2r+IED3r file.



IEC

Figure 2 – Static-routing engineering procedure, second stage

- Step 6: SCT A (IEDs) updates the .scd file describing IED1+IED2+IED3 and SW1+SW2+SW3, using the .sed file from the previous step created by SCT B (Bridges) and taking into account its own context. This .scd file can be considered a "main" SCD of the whole substation deployment of end devices (IEDs, MUs) and bridges.
- Step 7: SCT A (IEDs) creates a new .sed file IED1r+IED2r+IED3r and SW1+SW2+SW3 that reflects the changes of the previous step.
- Step 8: SCT B (Bridges) performs the identical actions as described in Step 4 (apart from the .icd file import since the bridge data SW1+SW2+SW3 already exists) and stores an .scd SW1+SW2+SW3 and IED1r+IED2r+IED3r file reflecting the changes of the previous step.
- Step 9: SCT B (Bridges) provides all bridges SW1, SW2 and SW3 with their corresponding configuration (CONF). This could be conducted by means of CLI commands, SNMP/MIB, Netconf/YANG, IEC 61850 MMS or any other means. According to IEC 61850-4:2020 and IEC 61850-6:2018, the bridge configuration for SW1, SW2 and SW3 can be created by means of IED configurator tools that create .cid files.

All bridge related configuration data in the .scd is stored using the Bridge Object Model defined in IEC 61850-90-4:2020.

5.2.3 Example: An illustration of substation network static-routing

5.2.3.1 Static-routing in non-redundant network

A simple example is used to illustrate the substation network static-routing in non-redundant network. The subscription relationships between the devices of IED1, IED2 and IED3 are specified by an assumed SCD file as follows:

- IED1 subscribes the SV messages of IED2 and IED3.

- IED2 subscribes the GOOSE messages of IED1.
- IED3 subscribes the GOOSE messages of IED1.

The information that is extracted from the SCD file can be represented by Table 4. The physical connectivity of substation network topology specified in the substation design specification is shown in Figure 3, and the dotted lines in Figure 3 indicate the planned GOOSE/SV path.

Table 4 – Extracted subscription information of IED1, IED2 and IED3

Publisher					Subscriber
iedName	Multicast Address	APPID	VLAN	SVID/GOID	iedName
IED1	01-0C-CD-01-00-01	0X1001	100	IED1/LLN0\$GO\$GoCB1	IED2, IED3
IED1	01-0C-CD-01-00-02	0X1002	123	IED1/LLN0\$GO\$GoCB2	IED2, IED3
IED2	01-0C-CD-04-00-02	0X4002	100	IED2/LLN0.smbcb0	IED1
IED3	01-0C-CD-04-00-03	0X4003	100	IED3/LLN0.smbcb0	IED1

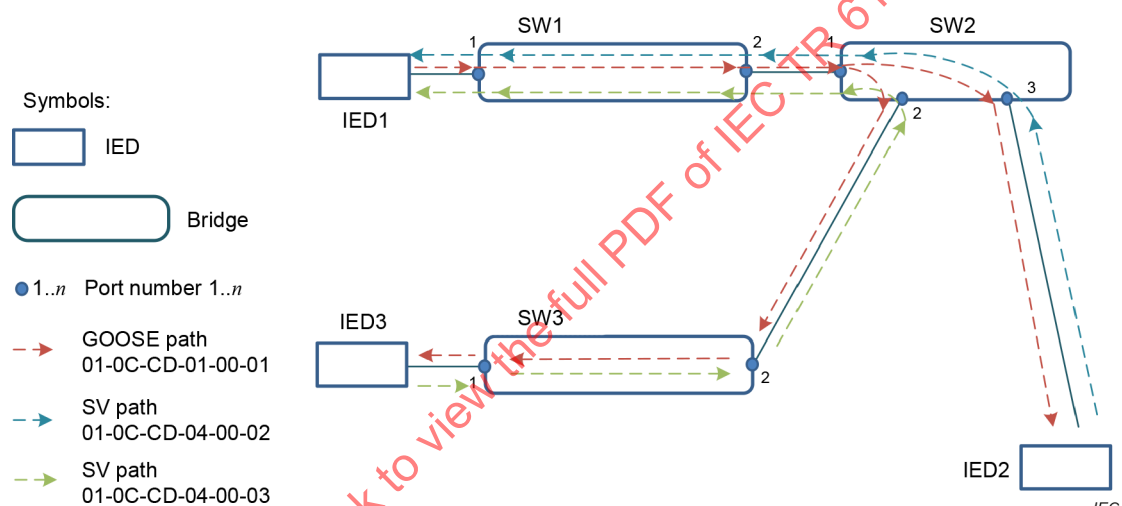


Figure 3 – Physical substation network connectivity and planned GOOSE/SV path

The bridge configuration information that is generated from the above information could be demonstrated in Table 5.

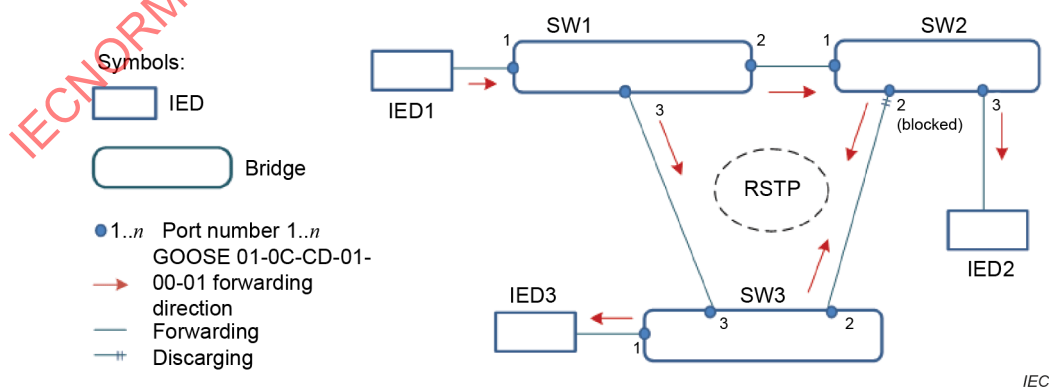
Table 5 – Generated bridge configuration information

SW1 VLAN/MAC table		
DMAC	Egress port	VLAN
01-0C-CD-01-00-01	2	100
01-0C-CD-01-00-02	2	123
01-0C-CD-04-00-02	1	100
01-0C-CD-04-00-03	1	100
SW2 VLAN/MAC table		
DMAC	Egress port	VLAN
01-0C-CD-01-00-01	2,3	100
01-0C-CD-01-00-02	2,3	123
01-0C-CD-04-00-02	1	100
01-0C-CD-04-00-03	1	100
SW3 VLAN/MAC table		
DMAC	Egress port	VLAN
01-0C-CD-01-00-01	1	100
01-0C-CD-01-00-02	1	123
01-0C-CD-04-00-03	2	100

Verify the validity of the GOOSE/SV path on IED1~IED3: IED1 would only receive the SV messages from IED2 (with MAC address of 01-0C-CD-04-00-02) and IED3 (with MAC address of 01-0C-CD-04-00-03), IED2 and IED3 would only receive the GOOSE message sent by IED1 (with MAC address of 01-0C-CD-01-00-01 and 01-0C-CD-01-00-02).

5.2.3.2 Static-routing in redundant network

During the process of static-routing, if the redundant network is included, the related topology information will be considered when generating bridge configuration. Most importantly, whether the redundancy mechanism is RSTP, HSR or PRP, the MAC addresses of the GOOSE/SV messages to be delivered need to be considered on the egress ports of all possible transmission paths (including backup paths) along the forwarding direction. An example is given to demonstrate how the static-routing deal with the Multicast filtering table when an RSTP ring existed in the network, as shown in Figure 4.

**Figure 4 – Static-routing within an RSTP ring**

GOOSE message (01-0C-CD-01-00-01) published by IED1 is subscribed by IED2 and IED3. It will be forwarded in the RSTP ring to the destination. Assuming the port 2 of bridge SW2 is blocked at first by the RSTP operation, the regular GOOSE path from IED1 to IED2 starts from port 1 of SW1, goes through port 2 of SW1 and port 1 of SW2, and lastly passes through port 3 of SW2, and its redundancy path begins from port 1 of SW1, then crosses port 3 of SW1 and port 3 of SW3, emits from port 2 of SW3 then terminates on port 2 of SW2. For reserving the redundant GOOSE/SV path, it needs to be embodied in the bridge configuration information to ensure its availability under static-routing case. The red line arrows in Figure 4 illustrate the delivery direction of GOOSE (01-0C-CD-01-00-01) messages from IED1 to IED2 and IED3, and the multicast filtering items in Table 6 need to be presented in bridge configuration information.

Table 6 – Generated bridge configuration information with redundancy path

SW1 VLAN/MAC table		
DMAC	Egress port	VLAN
01-0C-CD-01-00-01	2,3	100
SW2 VLAN/MAC table		
DMAC	Egress port	VLAN
01-0C-CD-01-00-01	2,3	100
SW3 VLAN/MAC table		
DMAC	Egress port	VLAN
01-0C-CD-01-00-01	1,2	100

Under normal circumstances, GOOSE message (01-0C-CD-01-00-01) launches from IED1. It will be forwarded to port 2 of bridge SW2 but blocked at the port. When the link between SW1 and SW2 fails, the blocked port 2 of SW2 will be activated by RSTP to make the backup path between SW2 and SW3 valid to forward the message according to the VLAN/MAC table.

It is easier to put the multicast items that need be forwarded on the interconnected ports of the RSTP ring when designing the MAC/VLAN tables. According to this, the VLAN/MAC table in Table 6 can be replaced with Table 7.

**Table 7 – Generated bridge configuration information
(including all interconnect ports of the RSTP ring)**

SW1 VLAN/MAC table		
DMAC	Egress port	VLAN
01-0C-CD-01-00-01	2,3	100
SW2 VLAN/MAC table		
DMAC	Egress port	VLAN
01-0C-CD-01-00-01	1,2,3	100
SW3 VLAN/MAC table		
DMAC	Egress port	VLAN
01-0C-CD-01-00-01	1,2,3	100

In this case, traffic of the GOOSE messages (01-0C-CD-01-00-01) will go up, so the item quantity that is configured on the interconnected ports needs to be considered to avoid the bandwidth burdened.

If an HSR ring composed by RedBox is connected to the network as shown in Figure 5, make sure that the multicast item is configured on port 2 of SW1.

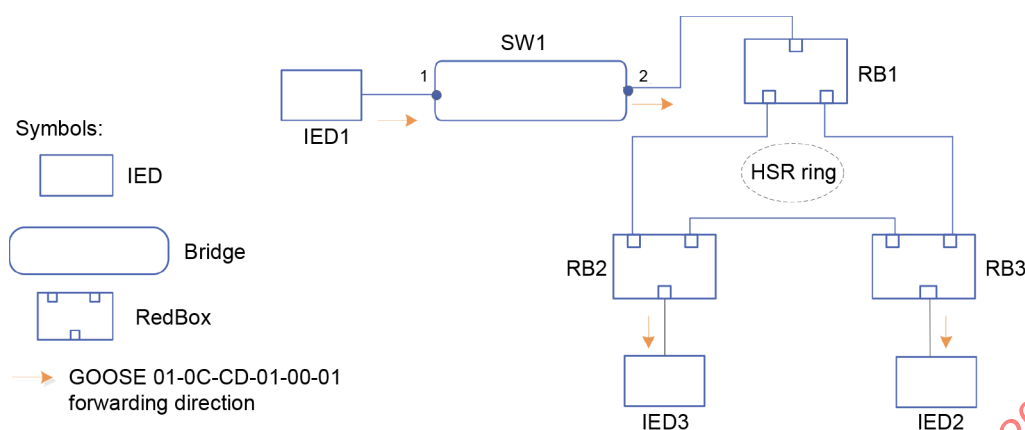


Figure 5 – Static-routing with a HSR ring

For the topology type of PRP, it means the substation network is doubled with the same connection relationships between IEDs and bridges in two separated sub-networks. The consideration for bridge configuration is the same with the single network.

However, although redundancy design provides backup paths for message transmission in the substation network, it is necessary to replace the bridge port or bridge itself after link failures or bridge outages being discovered, whatever the redundancy mechanism is.

5.2.4 Static-routing scenario: Move of IED to a different port or bridge

5.2.4.1 Overview

When the requirement of moving an IED to another different port of the bridge or a different bridge was demanded before or after the substation was about to operate, the physical topology of the substation network would change and the relevant GOOSE/SV path would be triggered to reconstruct the configuration. In this scenario, the network topology information would change according to the specific conditions of the connected port change. The bridge configuration needs to be regenerated based on the changed network topology and then uploaded to the bridge, and if possible, the update process would have no impact on the irrelevant existing network traffic. This scenario is also suitable for the replacement of the IED while moving it at the same time, when the IED is replaced without position change, then the GOOSE/SV path would not need to be updated. The engineering workflow of this scenario is identical to what is depicted in Figure 1 and Figure 2.

5.2.4.2 Scenario description

The static-routing use case diagram under the scenario 'Move of IED to a different port or bridge' is shown in Figure 6.

Diagram(s) of the scenario

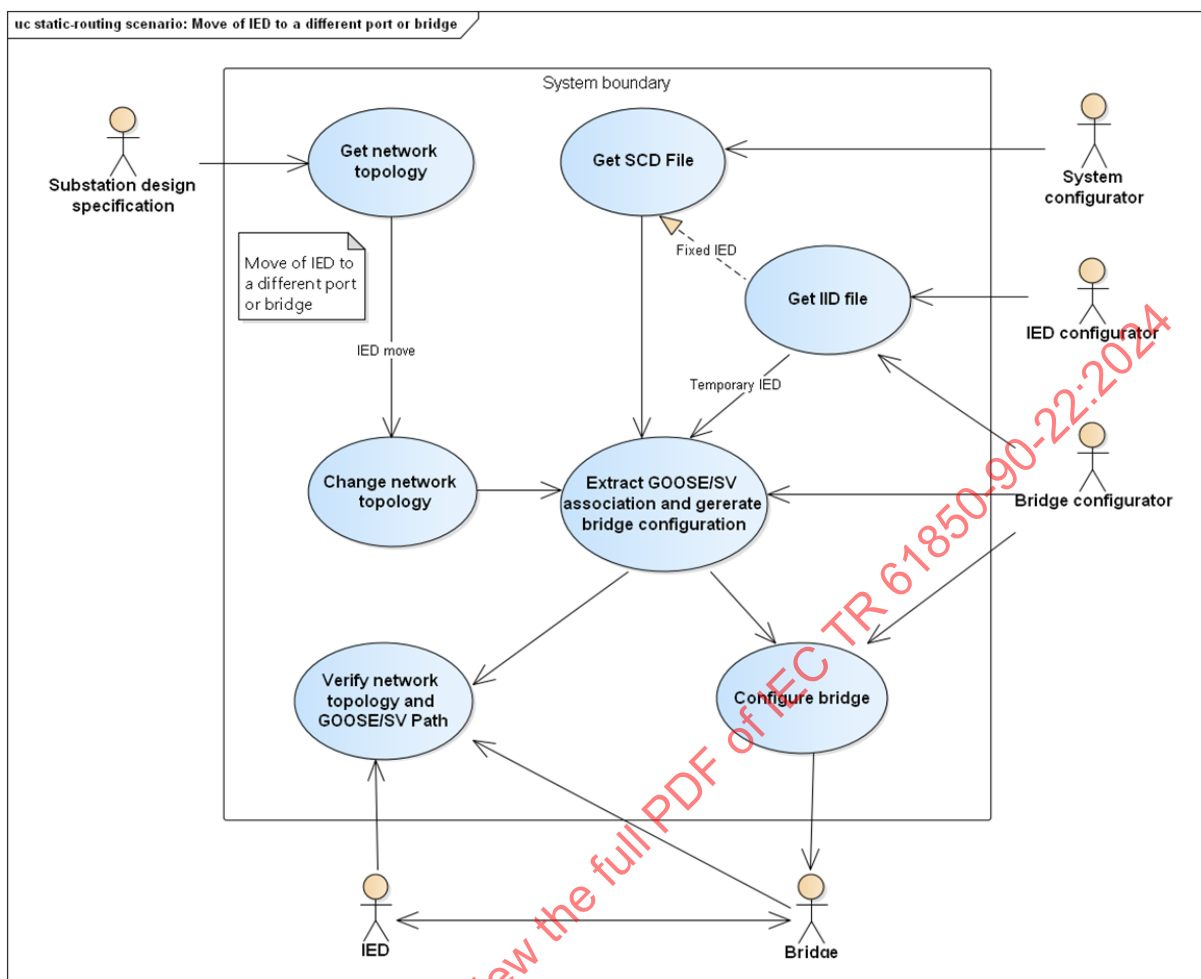


Figure 6 – Static-routing scenario diagram: Move of IED to a different port or bridge

The use case under this scenario includes the following steps:

Use case step	Primary actor	Description
Step 1	System configurator, IED configurator, Bridge configurator	Get SCD file and IID file currently used in the substation.
Step 2a	Substation design, specification	Get the information of current physical substation network topology.
Step 2b	Substation design, specification	Modify the topology information according to the specific altering requirement of the IED's port move. If "PhysConn" elements are used to describe the connection between IEDs and bridges by SCD/IID, then this step is optional.
Step 3	Bridge configurator	Evaluate whether the bandwidth of the altering port is enough for the following data transmission during the bridge configuration generating process. If it is not, the port modification requirement will be rejected, otherwise, move to the next step.
Step 4	Bridge configurator	Generate new bridge configuration combined the information of physical substation network topology and IED associations that extract from SCD file, identify and mark the bridges that configuration need to be changed, and then configure the bridges.
Step 5	IED, Bridge	IED send GOOSE/SV messages, bridge forward the packets to the ports subscriber IEDs connected and verify with the end nodes of the GOOSE/SV path.

5.2.5 Static-routing scenario: Add IEDs and bridges

5.2.5.1 Overview

In the case that the substation needs to add IEDs and bridges for bay extension or needs to insert a diagnostic device to do the trouble-shooting, it will cause adjustment and variation of the network topology. In this scenario, the SCD file needs to be modified, adding the new IED models and their related GOOSE/SV association. In addition, the new physical connectivity between the added IEDs and bridges need to be incorporated in the network topology information. The engineering workflow of this scenario is identical to what is depicted in Figure 1 and Figure 2.

NOTE In the case of predefined with prespecified entry points for a diagnostic device, there is no impact to the network topology, so no changes with the action of static-routing.

5.2.5.2 Scenario description

The static-routing use case diagram under scenario Add IEDs and bridges is shown in Figure 7.

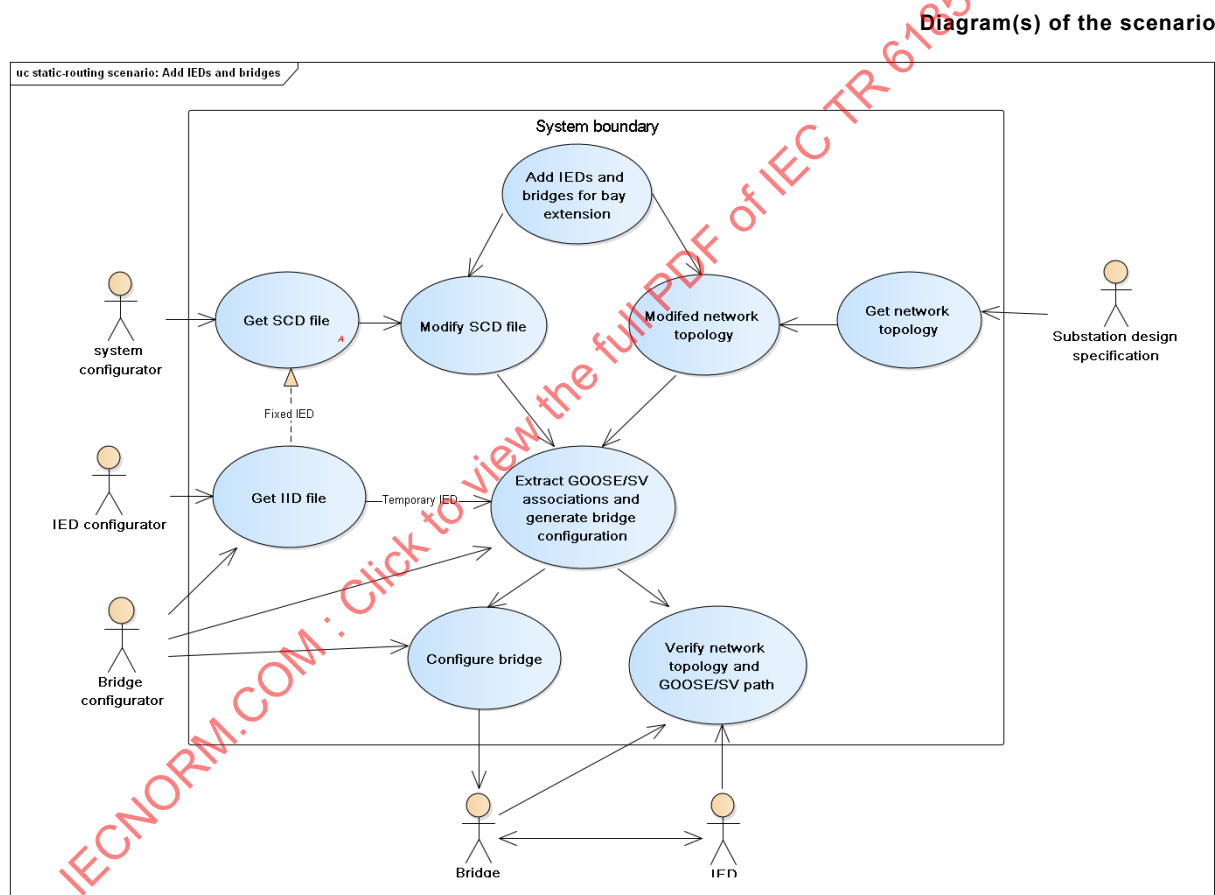


Figure 7 – Static-routing scenario diagram: Add IEDs and bridges

The use case under this scenario includes the following steps:

Use case step	Primary actor	Description
Step 1a	System configurator, IED configurator, Bridge configurator	Get SCD file and IID file currently used in the substation.
Step 1b	System configurator, IED configurator, Bridge configurator	Add the new IED models in SCD file or IID file.
Step 2a	Substation design specification	Get the information of current physical substation network topology.
Step 2b	Substation design specification	Modify the network topology information according to the designed IEDs and bridges expansion planning.
Step 2c	System configurator	Add related subscription information according to the designed IEDs and bridges expansion planning.
Step 3	Bridge configurator	Evaluate whether the bandwidth of the related port is enough for the following data transmission during the bridge configuration generating process. If it is not, the bridge addition requirement will be rejected, otherwise, move to the next step.
Step 4	Bridge configurator	Generate new bridge configuration, combined the information of physical substation network topology and IED associations that extract from SCD file, identify and mark the bridges that configuration changed, and then configure the bridges.
Step 5	IED, Bridge	IED send GOOSE/SV messages, bridge forward the packets to the ports subscriber IEDs connected and verify with the end nodes of the GOOSE/SV path.

5.2.6 Static-routing: Alternative technologies using SDN

Comparable to static-routing, Software Defined Networking (SDN) is an alternative approach which also provides a way to statically build a path for GOOSE/SV messages according to the substation physical network connectivity by extracting information from the SCD file and IID file.

SDN is a technology which can be applied for statically managing the forwarding of Ethernet packets through a network. Bridging hardware typically encompasses three planes, namely, the control plane, data plane and the management plane. The control plane is the system that decides where the traffic is sent. The data plane is the system that performs the forwarding of the traffic. In bridges which support SDN, however, the control plane is centralised in software called an SDN flow controller. In bridges without SDN functions, the control plane is in the appliance hardware.

Several interfaces and protocols have been defined to provide an interface between the control plane and the data plane. OpenFlow is one such example, and is an interface specification developed by the Open Networking Foundation (ONF) to enable interoperability between different flow controller implementations and different manufacturer's bridge hardware. Using a standardized interface between the SDN flow controller and the bridges allows the centrally managed network controller (control plane) to interoperate with the data plane of each bridge. For redundancy, two or more SDN flow controllers may be used to communicate with the bridges. Several methods can be used to achieve this redundancy, including synchronization methods between the controllers or having a local backup of the controller.

SDN uses the following terminology:

- In a flow rule, the matching criteria specifies header information of a packet against which each ingress packet is compared.
- An instruction defines a specific action or set of actions that is applied to all packets that meet specified matching criteria. Instructions define out of which port to forward a packet.
- A flow is defined by a set of matching criteria and corresponding instructions that are applied to each packet that ingresses a bridge.
- The SDN flow controller is the centralized controller that programs the rules and flows in each bridge.
- Counters are maintained for each flow table entry and used to maintain statistics on traffic by flow, port, queue, and so on.

The SDN flow controller gives each bridge a set of rules (or flows) containing matching criteria and instructions to determine the operations that should be performed on each packet the bridge receives. The bridge matches the packet header information against each rule contained in the flow table. If a matching flow table entry is found for a packet, the actions associated with that flow table entry are executed, such as sending the packet a specific port number, modifying a field (e.g. adding VLAN information), or dropping the packet.

Using SDN as an alternative to the static-routing method provides the following benefits:

- Automated network management can be achieved by consuming the SCD/SED or IID files in the SDN flow controller, or using a bridge configurator which consumes these files and communicates to the SDN flow controller to set up the correct flows appropriately on the bridges.
- Configuration can be applied centrally instead of managing the configuration of each individual network appliance.
- When changes need to be made, these can be made by reimporting the SCD file with the changes or using an IID file which will result in the smallest impact to the larger system.
- Scaling to larger systems is greatly simplified as individual configuration of the network appliances is not required and the same effort is required to configure the network through the SDN flow controller, irrespective of the size of the network.
- SDN follows a deny-by-default security profile. If a packet enters a bridge which does not have a matching rule, it is dropped. This eliminates unwanted traffic on the network.
- SDN flow controllers also provide the ability to monitor traffic at an application / flow level.
- Using the SCD file, the bridge understands where to send packets.
- Reduces the multi-cast and broadcast traffic burden when using GOOSE and SV on the network by sending traffic from source to destination only.
- Reduces the processing burden on protection IEDs as they are no longer required to process and discard unintended traffic of multicast GOOSE/SV messages.

5.3 Use case 2: Substation network auto-routing

5.3.1 Overview

Substation network auto-routing provides a way to dynamically build GOOSE/SV path according to GOOSE/SV associations in the SCD file, together with the substation physical network topology that is auto-obtained from the outcome of network topology discovery and IED learning. In that case, physical connectivity described by communication in SCD is irrelevant and would not be used to generate the GOOSE/SV path, only for GOOSE/SV verification. The VLAN/MAC table generated by auto-routing will be installed to the bridge automatically without manual intervention.

5.3.2 Use case description

The use case diagram for substation network auto-routing is shown in Figure 8.

Diagram(s) of use case

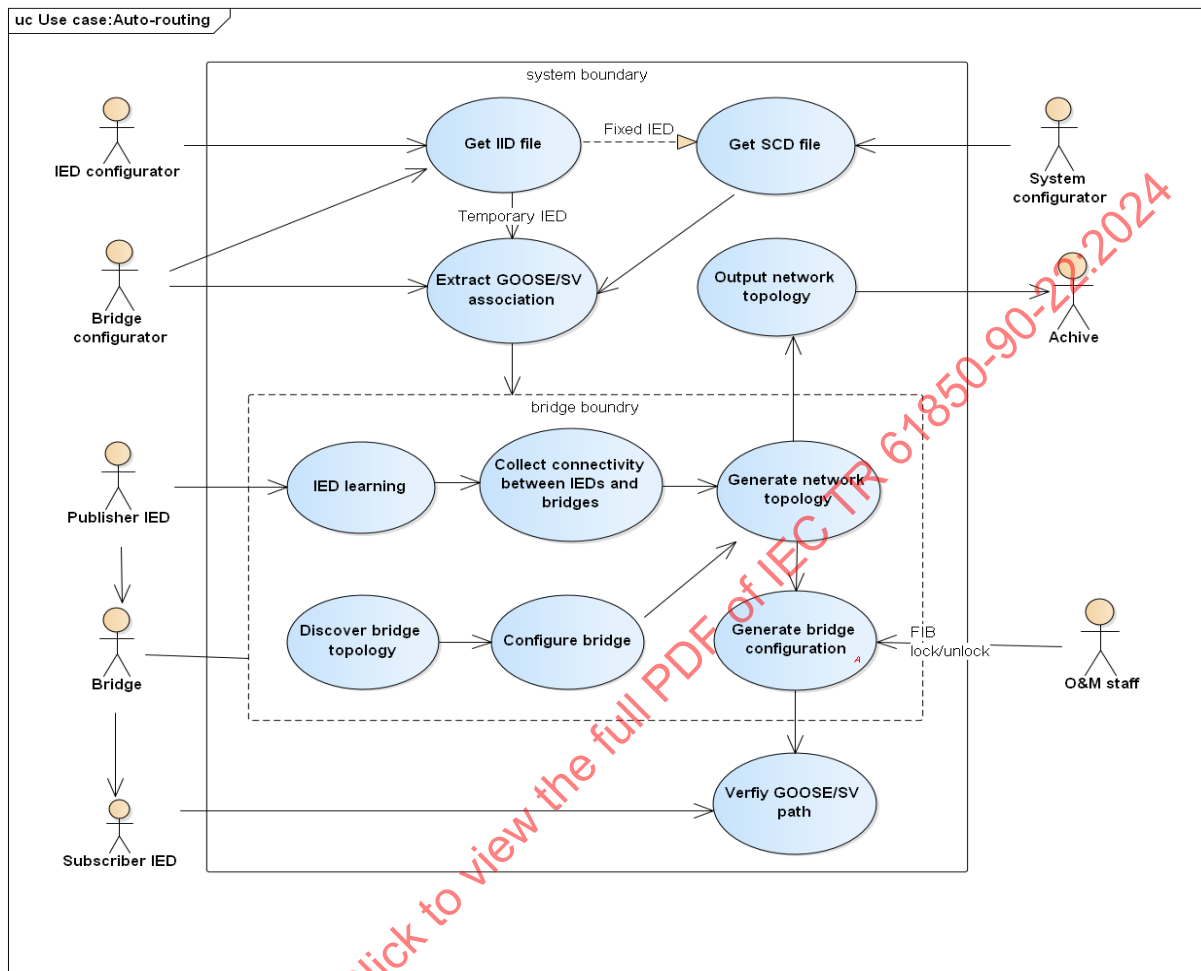


Figure 8 – Use case diagram for substation network auto-routing

The use case includes the following steps:

Use case step	Primary actor	Description
Step 1	System configurator, IED configurator, Bridge configurator	Generate substation SCD file with system configurator, get the SCD file, if necessary, generate IID file with IED configurator/bridge configurator, and get the IID file.
Step 2	Bridge configurator	Extract necessary information (e.g. GOOSE/SV association) from SCD file and IID file if any, then load it to the bridge.
Step 3	Publisher IED, Bridge	Perform auto-discovery of bridges interconnection; obtain the connectivity between IEDs and ports of bridges by means of IED learning; combined with the IED associations extracted from SCD file to generate bridges configuration automatically and make the configuration to be valid.
Step 4	Publisher IED, Bridge, Subscriber IED	Publisher IED send GOOSE/SV messages, bridge forward the packets to the ports subscriber IEDs connected and verify with the end nodes of the GOOSE/SV path.
Step 5	O&M staff, Bridge	Lock the bridge configuration if needed (optional step).
Step 6	Archive	Output and store the network topology if needed (optional step).

5.3.3 Example: An illustration of substation network auto-routing

A simple example is used to illustrate the substation network auto-routing. To better represent the attributes independency of IEDs, the APPID shall be uniquely distributed in the SCD file. The subscription relationship between the IED1, IED2 and IED3 devices is specified in the assumed SCD file as follows (same as the static-routing example in 5.2.3.1):

- IED1 subscribes the SV messages of IED2 and IED3.
- IED2 subscribes the GOOSE messages of IED1.
- IED3 subscribes the GOOSE messages of IED1.

The subscription relationship between IED1, IED2 and IED3 extracted from the SCD file can be represented by Table 8.

Table 8 – Extracted subscription information of IED1, IED2 and IED3

iedName	Publisher				Subscriber
	Multicast Address	APPID	VLAN	SVID/GOID	/
IED1	01-0C-CD-01-00-01	0X1001	123	IED1/LLN0\$GO\$GoCB	IED2、IED3
IED2	01-0C-CD-04-00-02	0X4002	123	IED2/LLN0.smbcb0	IED1
IED3	01-0C-CD-04-00-03	0X4003	123	IED3/LLN0.smbcb0	IED1

The demonstration of a physical connection of IED1, IED2, IED3 and the bridges is shown in Figure 9.

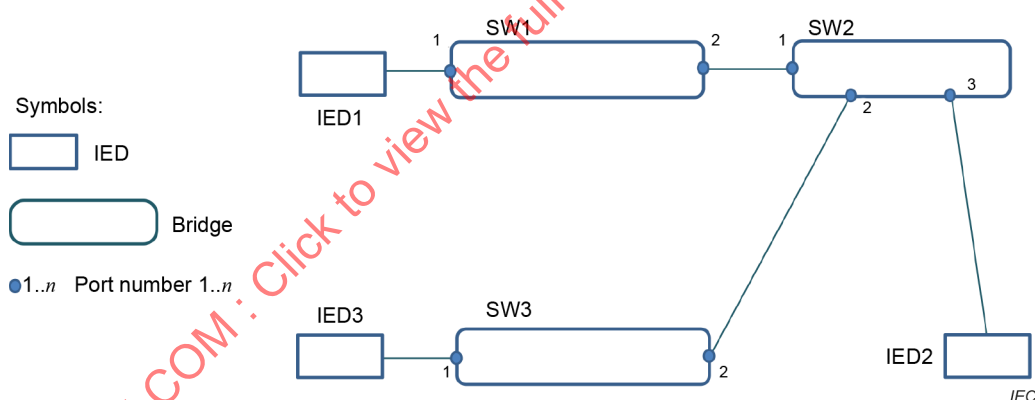
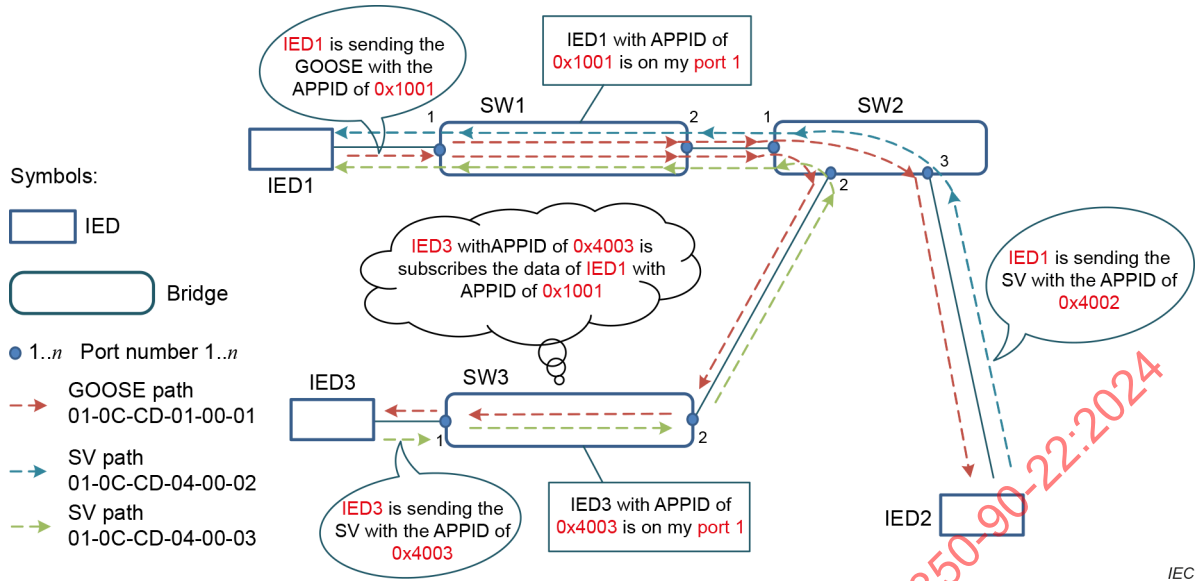


Figure 9 – Demonstration of a physical substation network topology

The implementation process of auto-routing is graphically demonstrated in Figure 10.



Description of the auto-routing with the example of GOOSE (01-0C-CD-01-00-01) message is detailed as follows:

- After the first GOOSE (01-0C-CD-01-00-01) packet issued by IED1 arrives at the port 1 of bridge SW1, SW1 identifies it was the IED1 which sent the packet according to the subscription information in Table 8 and associates it to port 1 (process of IED-learning). Similarly, bridge SW2 and SW3 identify IED2 and IED3 and associate them with the corresponding ports. Then the bridge can obtain the connection between the IED and the bridge port as shown in Table 9.

Table 9 – Outcome of IED learning

Bridge ID	Port	IED connected (iedName/DMAC/APPID)
SW1	1	IED1/01-0C-CD-01-00-01/0X1001
SW2	3	IED2/01-0C-CD-04-00-02/0X4002
SW3	1	IED3/01-0C-CD-04-00-03/0X4003

- Bridge SW1, SW2 and SW3 automatically obtain the physical port connections between them by means of exchanging the link-state information and subscription information that IED2 and IED3 need to receive the GOOSE (01-0C-CD-01-00-01) message sent by IED1. With these two aspects of the information, the two GOOSE/SV paths that are rooted from IED1 and are destined to IED2 and IED3 respectively are built, as shown by the dotted line in Figure 10. Each bridge generates a forwarding entry for the GOOSE packet along the GOOSE/SV path.
- The GOOSE packet is forwarded to its respective egress port along the GOOSE path by bridge SW1, SW2 and SW3 according to the generated forwarding entry. Check the receiving status of the packet on the destination node IED3.

5.3.4 Auto-routing scenario: Move of IED to a different port or bridge

5.3.4.1 Overview

When there is the requirement to move an IED to a different port of the bridge or a different bridge during substation commissioning phase, the physical topology of the substation network changes, and it will trigger the connected bridges to do the IED learning, update the network topology, and re-compute to generate a new GOOSE/SV path. This scenario is also suitable for the replacement of the IED while moving it at the same time, when the IED is replaced without position change, then the GOOSE/SV path would not need to be updated.

5.3.4.2 Scenario description

The auto-routing use case diagram under scenario Move of IED to a different port or bridge is shown in Figure 11.

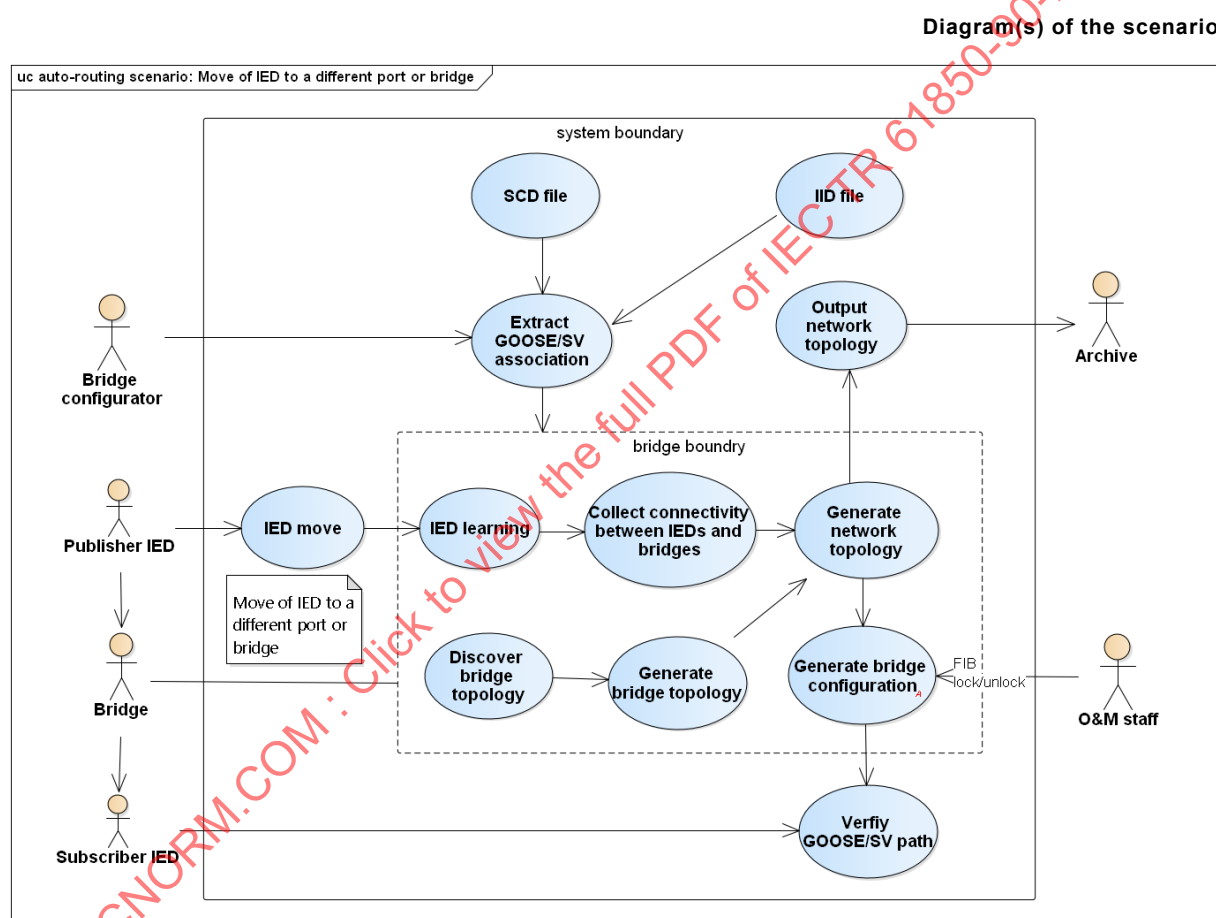


Figure 11 – Auto-routing scenario diagram: Move of IED to a different port or bridge

The use case under this scenario includes the following steps:

Use case step	Primary actor	Description
Step 1	System configurator IED configurator, Bridge configurator	Get SCD file and IID file that currently used in the substation.
Step 2	Bridge configurator, Publisher IED, Bridge	Extract VLAN/MAC information of GOOSE/SV packets, and their associations from SCD file and IID file, then load it to the bridge, move IED to the bridge port that to be changed.
Step 3	Publisher IED, bridge	The related bridges carry out IED learning, update network topology, re-compute and generate new GOOSE/SV path.
Step 4	Publisher IED, bridge, Subscriber IED	Publisher IED send GOOSE/SV messages, bridge forward the packets to the ports subscriber IEDs connected and verify with the end nodes of the GOOSE/SV path.
Step 5	O&M staff, bridge	Lock the bridge configuration if needed (optional step).
Step 6	Archive	Output and store the network topology if needed (optional step).

5.3.5 Auto-routing scenario: Add IEDs and bridges

5.3.5.1 Overview

In the case that the substation needs to add IEDs and bridges for bay extension or needs to insert a diagnostic device to do the trouble-shooting, it will cause adjustment and variation of the network topology. The auto-routing use case in this scenario is that the SCD file needs to be modified, adding the new IED models and their related GOOSE/SV association. The bridges will re-compute and generate a new GOOSE/SV path according to the updated GOOSE/SV associations and the network topology.

NOTE In the case of predefined with prespecified entry points for a diagnostic device, there is no impact to the network topology, so no changes with the actions of auto-routing.

5.3.5.2 Scenario description

Figure 12 shows the diagram of auto-routing use case under scenario Add/Remove IEDs and bridges.

Diagram(s) of the scenario

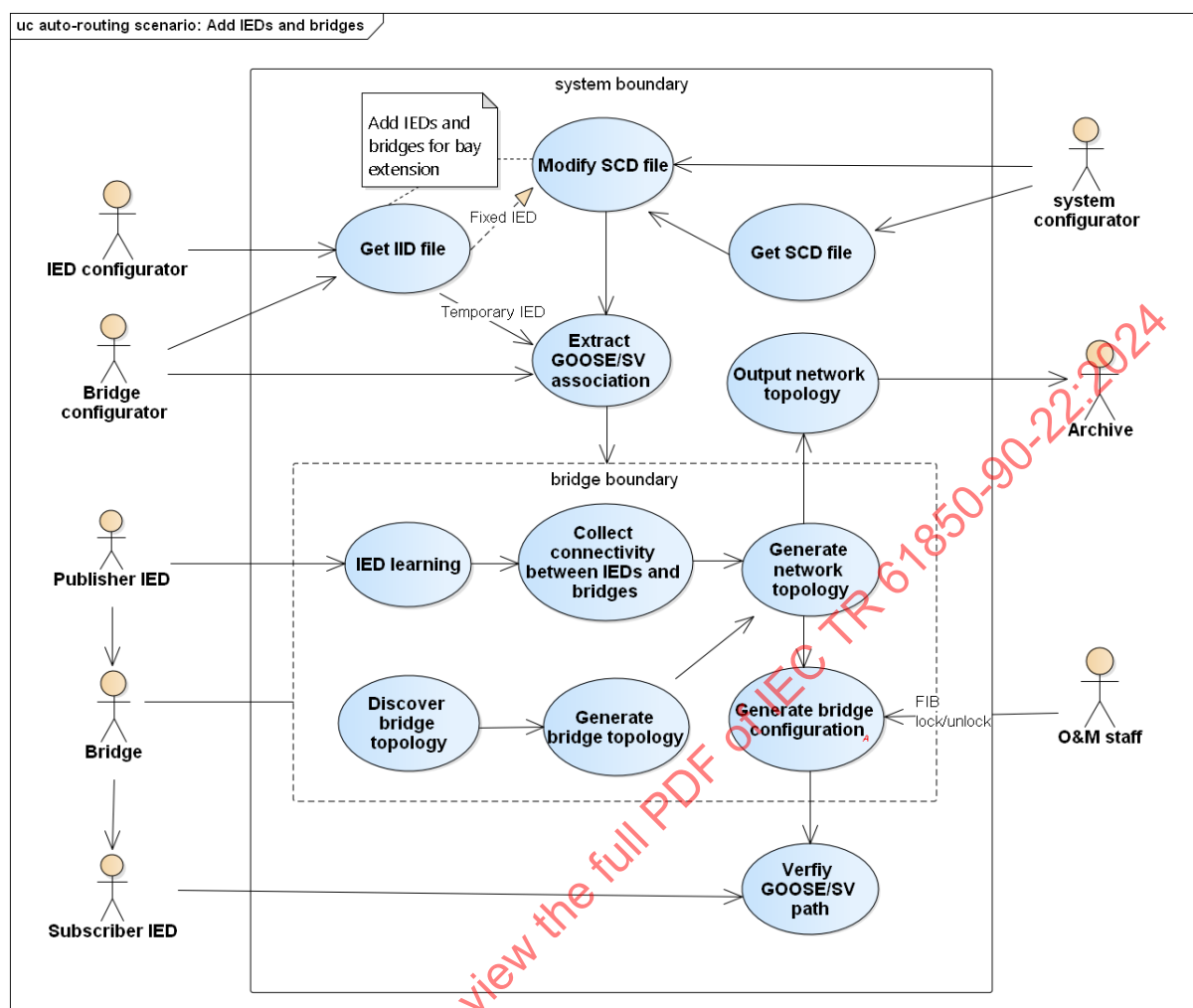


Figure 12 – Auto-routing scenario diagram: Add IEDs and bridges

The use case under this scenario includes the following steps:

Use case step	Primary actor	Description
Step 1a	System configurator, IED configurator, Bridge configurator	Get SCD file and IID file that currently used in the substation.
Step 1b	System configurator, IED configurator, Bridge configurator	Add the new IEDs' models into the SCD file, and modify the GOOSE/SV subscriptions according to the engineering plan, or implement these modifications using IID files.
Step 2	Bridge configurator	Extract VLAN/MAC information of GOOSE/SV packets, and their associations from SCD file and IID file, then load it to the bridge.
Step 3	Bridge, Publisher IED	Bridge auto-discovers their interconnections, obtains connectivity between the IED and its connected bridge port, combined with the extracted IED associations, generates bridge configuration automatically and puts it to be valid.
Step 4	Publisher IED, bridge, Subscriber IED	Publisher IED send GOOSE/SV messages, bridge forward the packets to the ports subscriber IEDs connected and verify with the end nodes of the GOOSE/SV path.
Step 5	O&M staff, bridge	Lock the bridge configuration if needed (optional step).
Step 6	Archive	Output and store the network topology if needed (optional step).

5.3.6 Auto-routing scenario: substation network topology recovery

5.3.6.1 Overview

When there is a single-link or a single-node failure which occurs in the substation network, the physical topology of the substation network changes and the affected GOOSE/SV traffic is redirected by passing through the dynamic recovery mechanism, following a new bridge path. This path can be built through the following steps within the related bridges: fault detection, fault notification, discover bridge topology, and generate bridge topology. Recovery of the affected GOOSE/SV traffic is carried out as follows: the network topology is generated based on the new bridge topology and the connection between IED and bridge, and a new GOOSE/SV path is re-computed and generated.

5.3.6.2 Scenario description

The use case diagram for network topology recovery is shown in Figure 13.

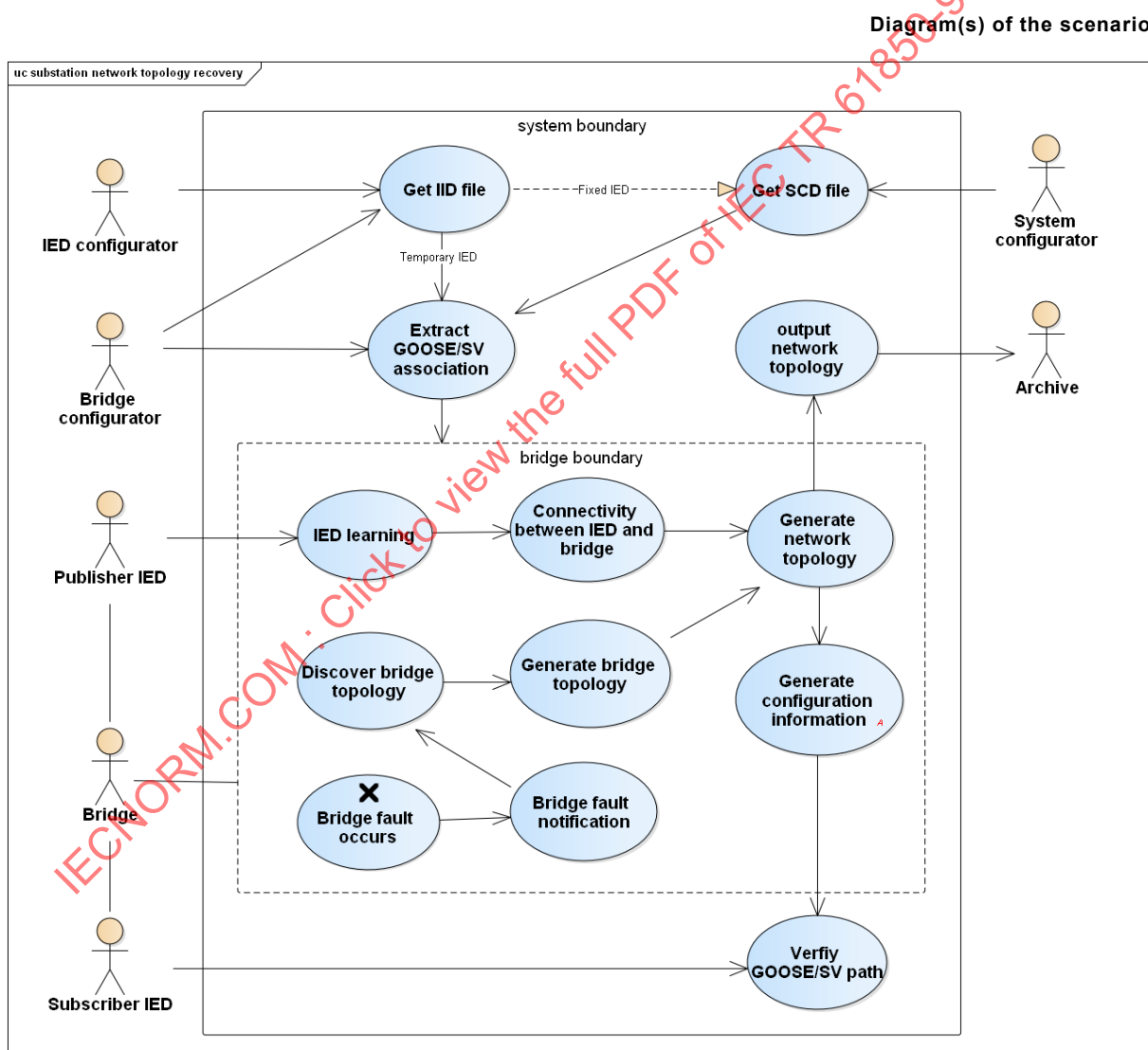


Figure 13 – Use case diagram for substation network topology recovery

The use case includes the following steps:

Use case step	Primary actor	Description
Step 1	System configurator, IED configurator, Bridge configurator	Get SCD file and IID file that currently used in the substation.
Step2	Bridge configurator	Extract VLAN/MAC information of GOOSE/SV packets, and their associations from SCD file and IID file, then load it to the bridge.
Step3	Bridge, Publisher IED, Subscriber IED	A single-link or a single-node failure occurs.
Step 4	Bridge, Publisher IED, Subscriber IED	The related bridges carry out fault detection, fault notification, update network topology, re-compute and generate new GOOSE/SV path, generates new bridge configuration automatically and puts it to be valid.
Step5	Bridge, Publisher IED, Subscriber IED	Publisher IED send GOOSE/SV messages, bridge forward the packets to the ports subscriber IEDs connected and verify with the end nodes of the GOOSE/SV path.
Step 6	Archive	Output and store the network topology if needed (optional step).

5.3.6.3 Example: The integration of auto-routing and STP/RSTP, HSR or PRP

5.3.6.3.1 Overview

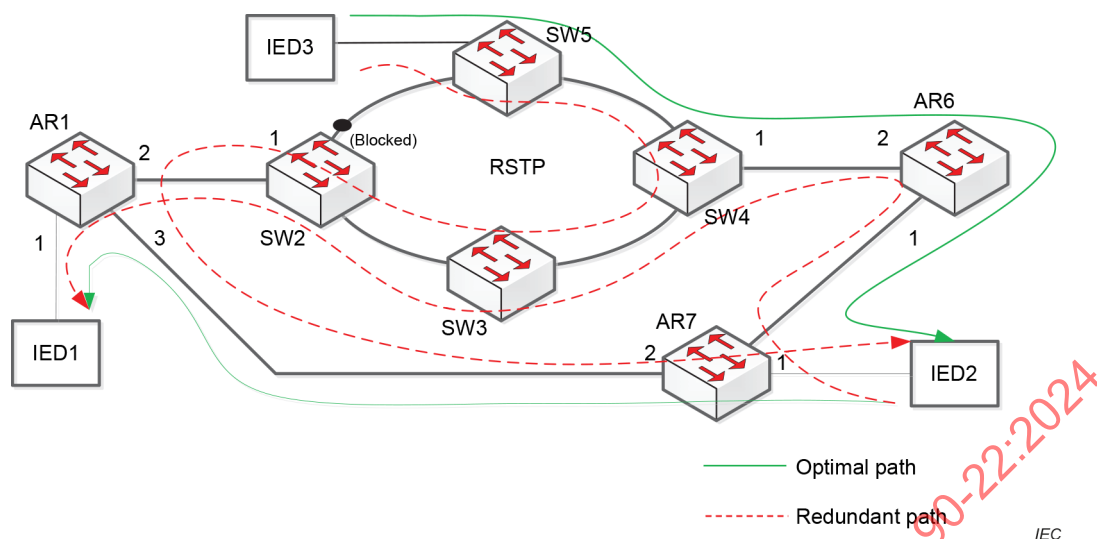
When talking about network recovery, first of all, it means there are multiple paths existing in the network between the source node and destination nodes; this will inevitably be involved in the problem of how to deal with the redundancy paths. Several techniques could be used to construct the network redundancy, like STP/RSTP/MSTP, HSR, PRP and auto-routing proposed in this document. STP/RSTP/MSTP, HSR and PRP work in the MAC layer, while auto-routing operates between the MAC layer and the network layer, so they can cooperate without conflict. Examples are given to demonstrate how auto-routing interoperates with the techniques mentioned above when the corresponding redundancy path exists in the network, and how eventually the forwarding path would be if anything goes wrong in the network.

5.3.6.3.2 Auto-routing and STP/RSTP

In Figure 14, AR1, AR6 and AR7 are AR-bridges; SW2 to SW5 are devices according to the principle of IEEE 802.1D/1W. The topology is simply used to demonstrate the interoperation and coexistence of auto-routing and STP/RSTP.

Assumptions are made here:

- IED1 subscribes messages of IED2.
- IED2 subscribes messages of IED3.
- STP/RSTP protocol is enabled in SW2 to SW5, the link between SW2 and SW5 is blocked.



NOTE The link between SW2 and SW5 being blocked is just one possible result.

Figure 14 – Redundancy with Auto-routing and STP/RSTP

The ring in Figure 14 is controlled by STP/RSTP protocol, and the ring will be pruned into a single tree by blocking the redundancy path, as simplified in Figure 15 (the RSTP ring is simplified as a pseudo bridge). Two available GOOSE/SV paths are left for the message transmission from IED2 to IED1, and IED3 to IED2; the optimal one will be chosen to carry the message (green line), and another is acted as the redundancy path (red and dash line). The process of auto-routing how to select the optimal GOOSE/SV path is described as follows:

- a) Bridge AR1, AR6 and AR7 send interactive messages periodically ("Hello" message is assumed) to discover their neighbours. For the bridge SW2 and SW4, the Hello message from AR1 and AR6 will be forwarded directly through SW3 transparently. Because STP/RSTP does not respond to the Hello messages of auto-routing, the logical next hop for the message from port 2 of AR1 would be the port 2 of AR6, that is to say the bridges with STP/RSTP are transparent nodes to the bridges that support auto-routing. So, the final neighbour relationship in this case would be that each AR-bridge of AR1, AR6 and AR7 has the other two as neighbours, and the STP/RSTP ring is deemed as a pseudo bridge to connect multiple nodes. The final network topology can be simplified as shown in Figure 14. Different from IED1 and IED2, the messages issued by IED3 can be received at both port 2 of AR1 and AR6, and the AR-bridge will select one of them as the optimal access point by a certain process, here assuming AR6 is initially selected.

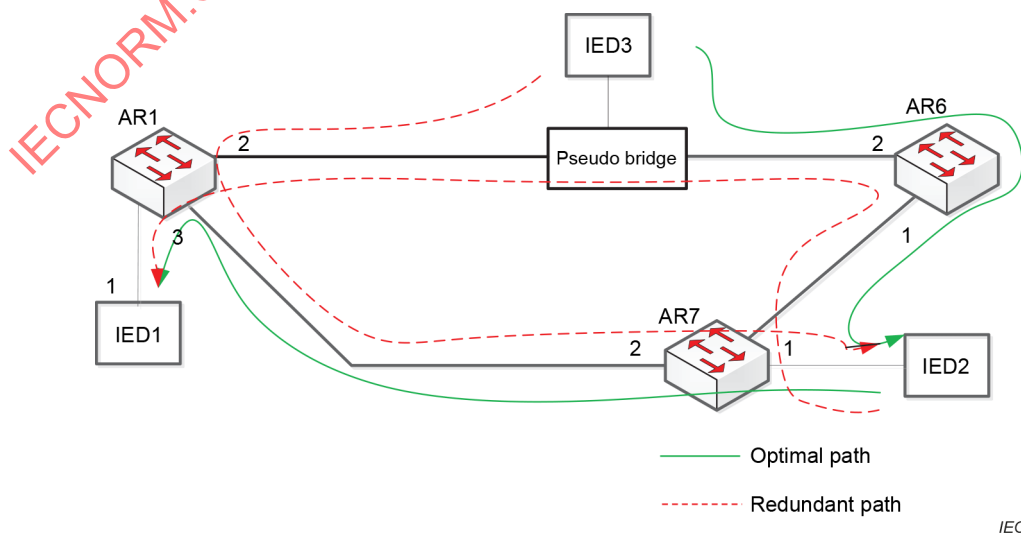


Figure 15 – Simplified Auto-routing network topology with STP/RSTP ring

- b) AR-bridges will flood and synchronize their link-state information among neighbours to eventually get a consistent link-state database, and each AR-bridge will calculate the shortest path rooted from itself to produce forwarding table (generate bridge configuration information). It is supposed that the path from AR1 to AR7 is chosen to be the optimal GOOSE/SV path to the message transmission from IED2 to IED1, and the path from AR6 to AR7 is selected for the message transmission from IED3 to IED2.
- c) If the bridge AR1 does not receive the periodic Hello message on port 3 in a specific time span, the link between AR1 and AR7 would be considered as failure, and it will trigger the bridges to update of synchronization on the link-state information, and new configuration will be updated automatically by itself according to the changed network topology. So, if something is wrong with the link between bridge AR1 and AR7, GOOSE/SV path from IED2 to IED1 will be converged to the redundant path AR1-SW2-SW3-SW4-AR6-AR7.
- d) If the live path on the STP/RSTP ring fails (link between SW4 and SW5), the backup path will be activated according to STP/RSTP protocol, and it only affects the AR-bridges interconnection between AR1 and AR6, so the GOOSE/SV path from IED3 to IED2 looks like having no changes. But if the link between AR6 and AR7 fails, that will trigger the auto-routing link-state update as described in step c), so the GOOSE/SV path from IED3 to IED2 will be transferred to another redundant path SW5-SW4-SW3-SW2-AR1-AR7.

If a normal bridge not only supports auto-routing function but also STP/RSTP, in such case, compared to the RSTP blocking the redundant links, auto-routing can make full use of them, and also can recover more faster than RSTP. Theoretically, the converge time of auto-routing is equivalent to one tenth of the RTSP's under the same network scale, so as for performance wise, the auto-routing is preferred, and the utilization of the ports can be increased by using of the multiple links. However for compatibility reasons, RSTP could be selected.

5.3.6.3.3 Auto-routing and HSR

With the similarity to auto-routing and STP/RSTP, as shown in Figure 16, the HSR ring made with RedBox (RB2 to RB4) is connected between AR-bridges AR1 and AR6.

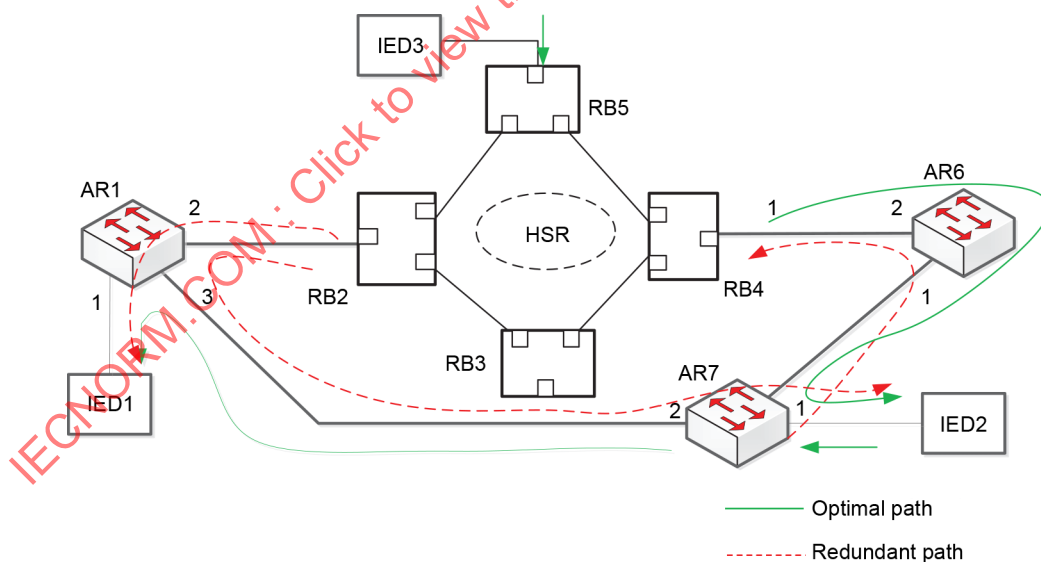


Figure 16 – Redundancy with auto-routing and HSR

HSR, as specified in Clause 5 of IEC 62439-3:2021, provides a way to make the messages in the ring be transmitted bidirectionally on the ring, and the messages receiving direction decided by the data arrival time, so no packet loss occurs due to the mechanism of dual transmission when a single failure occurs to the ring; that is significantly different from the loop control result by STP/RSTP.

From the point of view of auto-routing, the HSR ring constructed by RedBox RB2 to RB5 without responding auto-routing interactive messages is also considered as a hub to connect multiple nodes, so the simplified network topology is the same as Figure 15 from an auto-routing perspective, and the process of optimal GOOSE/SV path chosen is similar to the condition of auto-ring and STP/RSTP, except that the message forwarding direction on the HSR ring is unknown whenever under normal or failure cases, and if failure occurs between AR-bridges, the process of path convergence is the same as the case of auto-routing and STP/RSTP.

5.3.6.3.4 Auto-routing and PRP

As specified in Clause 4 of IEC 62439-3:2021, PRP is a layer 2 redundancy protocol which relies on complete duplication of the sub-network to provide seamless operation in case of loss of any link or bridge. Both sub-networks operate in parallel and each individually can use STP/RSTP or HSR together with auto-routing, as shown in Figure 17.

To facilitate the description, Figure 17 adopts the above network construction to demonstrate the coexistence of auto-routing and PRP. IED1, IED2 and IED3 are connected into two identical sub-networks operating in parallel by PRP-supported nodes or other devices. Each sub-network operates independently, and optimal GOOSE/SV path selection is running isolated with the same process as has been described above.

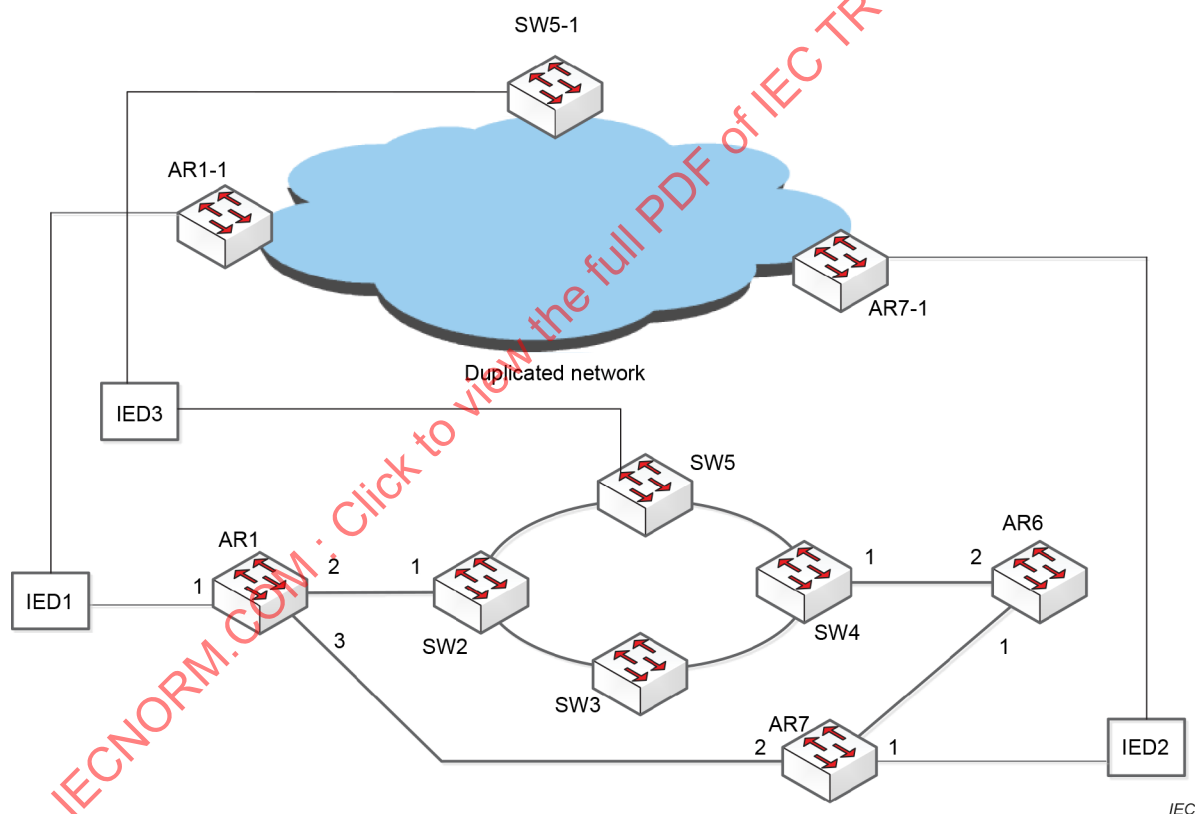


Figure 17 – Redundancy with auto-routing and PRP

5.3.6.3.5 Redundancy in pure auto-routing network

If the bridges were all auto-routing supported, then there would be more than two GOOSE/SV paths existed for the GOOSE/SV message that transmitted from IED2 to IED1 as shown in Figure 18.

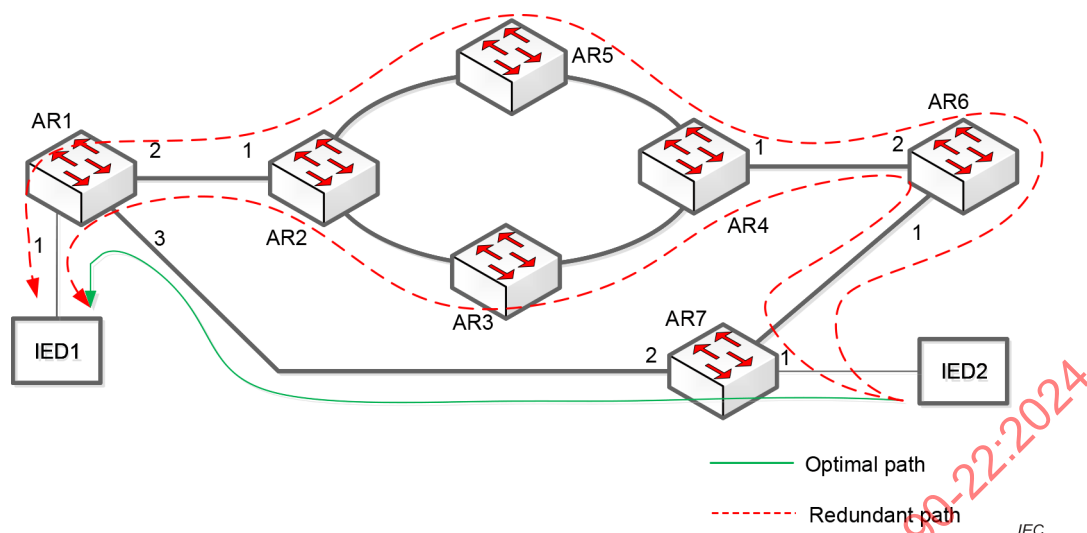


Figure 18 – Redundancy in pure auto-routing network

Unlike being treated as transparent nodes above, AR-Bridges AR2 to AR5 would be discovered by their neighbours and get the synchronized link-state database, optimal GOOSE/SV path would be calculated and selected, and then the bridges configuration would be generated. If the link fails or the bridge wrecks in the network, the corresponding bridges which are involved would rediscover the bridge topology, update and flood the changed link-state database, and then regenerate the bridges' configuration.

Auto-routing is designed to fully use the network path resource other than the way that involves STP/RTSP blocking the redundant path or the bidirectional transmission of HSR. The coexistence with STP/RSTP or HSR is not recommended on the same individual bridge ports. The AR-bridge is backwards compatible.

5.3.7 Auto-routing scenario: forwarding path calculation

5.3.7.1 Overview

Necessary information required to calculate the GOOSE/SV path includes the GOOSE/SV messages sent from the publisher IED, the GOOSE/SV associations extracted from SCD/IID file, physical connectivity between the IED and bridge, and the interconnection between bridges. GOOSE/SV message is sent from the publisher for IED learning. The location of the pure subscriber device (without publishing any messages, also called silent IED) should be identified using the BCD file. With all the information obtained, the bridge could calculate the forwarding path for the connected locally and set the path of non-local learned GOOSE/SV packet to the connected bridges according to the bridge topology that discovered.

5.3.7.2 Scenario description

The use case diagram for forwarding path calculation is shown in Figure 19.

Diagram(s) of the scenario

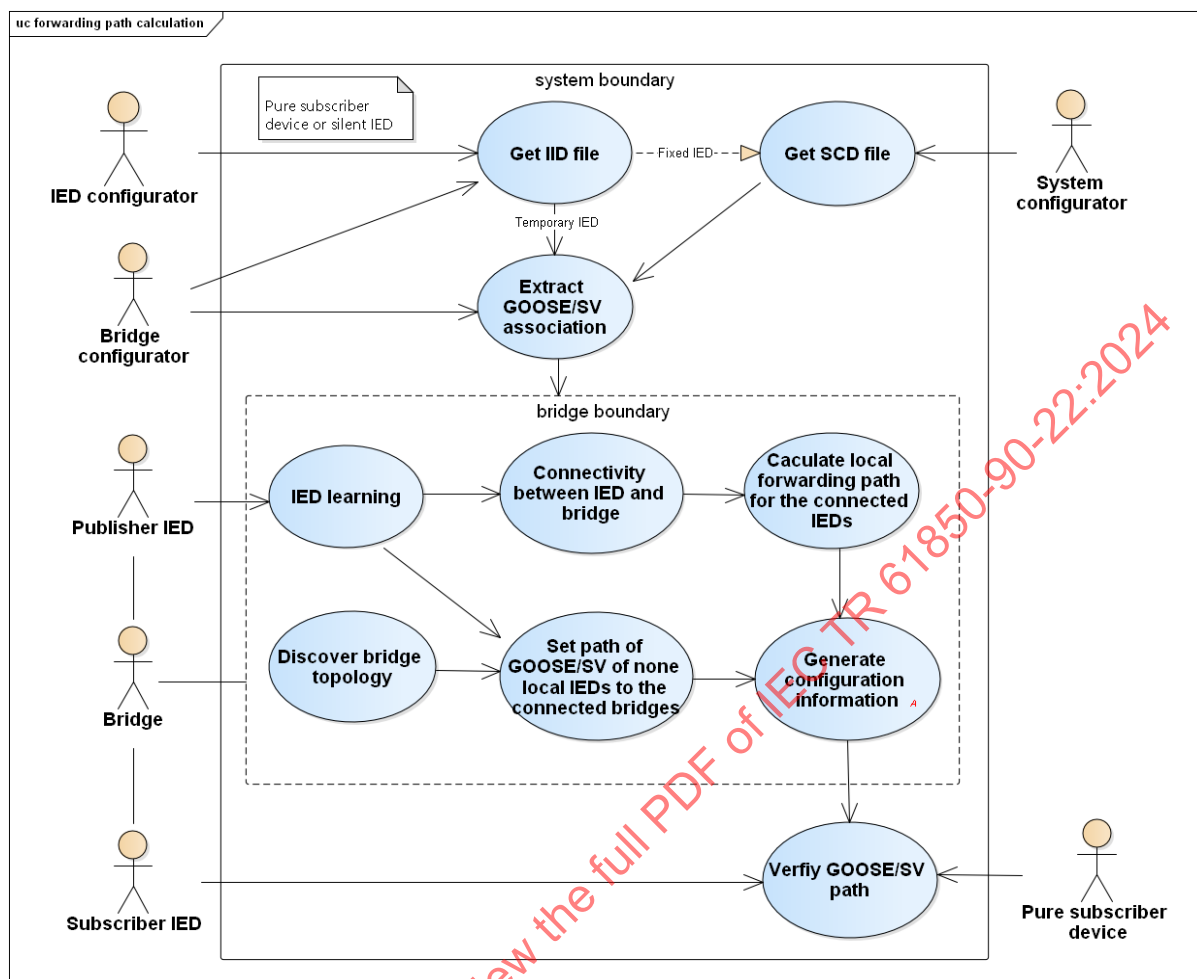


Figure 19 – Use case diagram for forwarding path calculation

The use case includes the following steps:

Use case step	Primary actor	Description
Step 1a	System configurator, IED configurator, Bridge configurator	Get SCD file and IID file currently used in the substation.
Step 1b	System configurator	Add the model of the pure subscriber device (if there are) into SCD file, modify the subscription information according to the pure subscriber device requirement.
Step 2	Bridge configurator	Extract VLAN/MAC information of GOOSE/SV packets, and their associations from SCD file and IID file, then load it to the bridge.
Step 3	Bridge, Pure subscriber device	Connect the pure subscriber device to the specified bridge port.
Step 4	Bridge, Publisher IED, Subscriber IED, Pure subscriber device	Bridge auto-discovers their interconnections, obtains connectivity between the IED and its connected bridge port, combined with the extracted IED associations, generates bridge configuration automatically and puts it to be valid.
Step 5	Bridge, Publisher IED, Subscriber IED, Pure subscriber device	Performing the verification of network topology and GOOSE/SV path, put the IED publisher sending GOOSE/SV messages, then check the packets receiving status of IEDs connected to the bridge ports that are the end nodes of the GOOSE/SV path.

5.4 Use case 3: GOOSE/SV path visualization

5.4.1 Overview

A GOOSE/SV path is defined as a GOOSE/SV multicast distribution tree that created in substation network to implement GOOSE/SV association. It involves several parts in the substation network, the publisher, the subscribers, and intermediate bridges, all the information related is embedded in SCD file and messages, and when there is something wrong with the GOOSE/SV path, it is difficult to locate the fault position.

Visualizing the GOOSE/SV path could provide an easy way to acknowledge the operation status of the protection relay IED, Bay Control Unit, Merging Unit, BIED and other devices related to the GOOSE/SV path. Especially in the case of abnormal situations of equipment, systems, links, etc., the O&M staff can quickly locate the fault point and shorten the system break time.

GOOSE/SV path-related operating status in substation network could be collected, and then compared and verified with the SCD file in real-time. When an abnormality or fault occurs within the substation network or between device communication, the real-time verification work will help to facilitate the fault identification and location. GOOSE/SV path visualization can also be provided to help discover the potential anomalies in the process of substation network operation and maintenance, and finally can improve the transparency and manageability of the substation network.

5.4.2 Use case description

The use case diagram for GOOSE/SV path visualization is shown in Figure 20.

Diagram(s) of use case

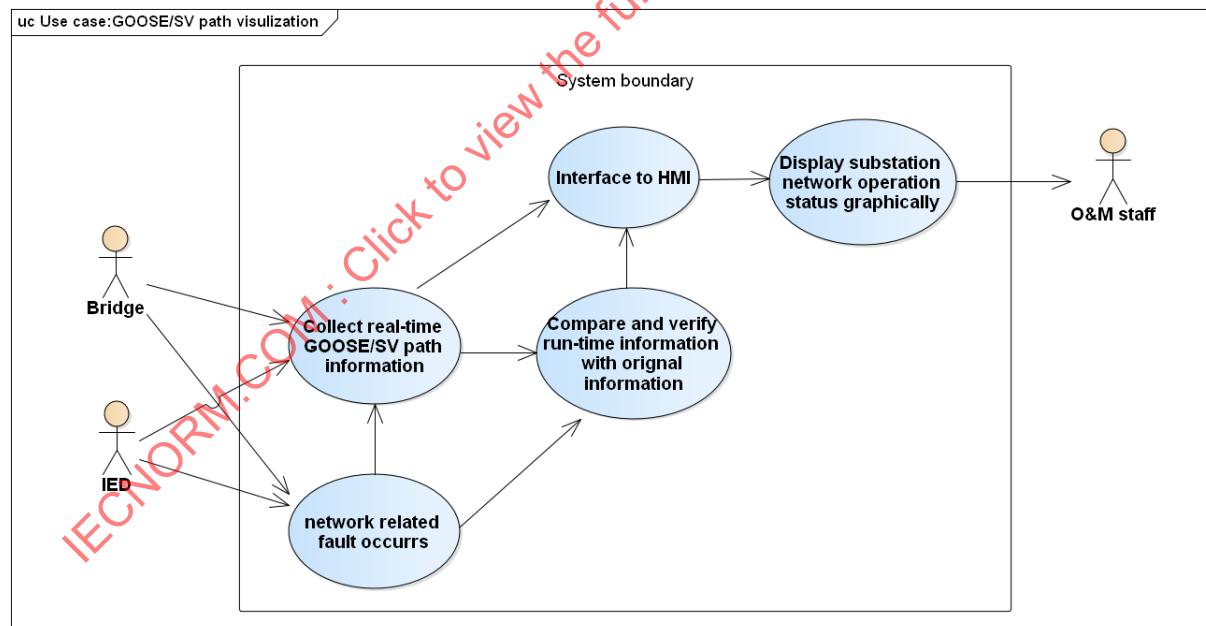


Figure 20 – Use case diagram for GOOSE/SV path visualization

The use case includes the following steps:

Use case step	Primary actor	Description
Step 1	Bridge, IED	After GOOSE/SV path generated, the real-time information of the GOOSE/SV path could be collected and formatted to be communicated to the HMI.
Step 2	Bridge	Perform data adaption to send the GOOSE/SV path information to HMI periodically.
Step 3	Bridge, IED, O&M staff	GOOSE/SV path information graphically displayed on HMI to provide direct real-time information for O&M staff.
Step 4	Bridge, IED	When network related fault occurs, the collected information will help to identify the fault type and locate the fault position quickly, then send to HMI immediately.
Step 5	O&M staff	HMI display the fault identification and location in a graphic way to inform the O&M staff.

5.4.3 GOOSE/SV path visualization scenario: Normal state

5.4.3.1 Overview

Information related to GOOSE/SV path includes information of source node, middle links and destination nodes, like a data set, and collection of this information could be accomplished by AR-bridge's data modelling work that is detailed in Clause 10. When the substation network operates in a normal state, the bridges collect GOOSE/SV path related information automatically and, periodically, encapsulate these data into some specific format that can be decoded by the HMI interface. GOOSE/SV path information includes but is not limited to: bridge IDs, port IDs, ports link status, IED name/APPID, GOOSE/SV transmission statistics etc.

5.4.3.2 Scenario description

The GOOSE/SV path visualization use case diagram under the scenario of normal state is shown in Figure 21.

Diagram(s) of the scenario

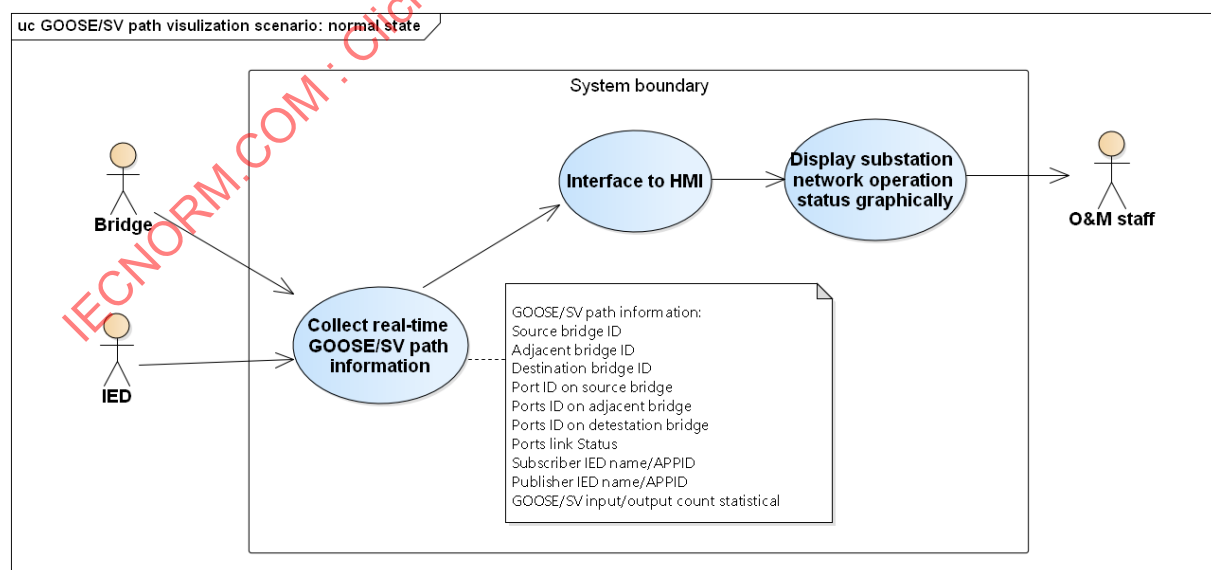


Figure 21 – GOOSE/SV path visualization scenario diagram: Path normal state

The use case under this scenario includes the following steps:

Use case step	Primary actor	Description
Step 1	Bridge, IED	After GOOSE/SV path generated, the real-time information of the GOOSE/SV path could be collected and formatted to be communicated to the HMI.
Step 2	Bridge	Perform data adaption to send the GOOSE/SV path information to HMI periodically.
Step 3	Bridge, IED, O&M staff	GOOSE/SV path information graphically displayed on HMI to provide direct real-time information for O&M staff.

5.4.4 GOOSE/SV path visualization scenario: Communication fail

5.4.4.1 Overview

The GOOSE/SV path is composed by sorts of elements; any element degraded or invalid will cause the communication to fail. Some obvious faults are easy to identify, however, the fault may be easily told but difficult to be located. For example, if one IED did not receive the subscribed GOOSE packets but got the subscribed SV messages correctly from the same publisher IED, every abnormal element between the source and destination could possibly cause the phenomenon to happen, like some ports linked down, optical fibres or cables failed, messages dropped by bridges, or even not sent by the publisher.

With the help of GOOSE/SV visualization, all information about the GOOSE/SV path could be observed on the HMI. Any abnormal element would be indicated in relative real-time with a warning or alarming information or mark to remind the O&M staff to find out and locate the fault position.

5.4.4.2 Scenario description

The GOOSE/SV path visualization use case diagram under the scenario of communication break is shown in Figure 22.

Diagram(s) of the scenario

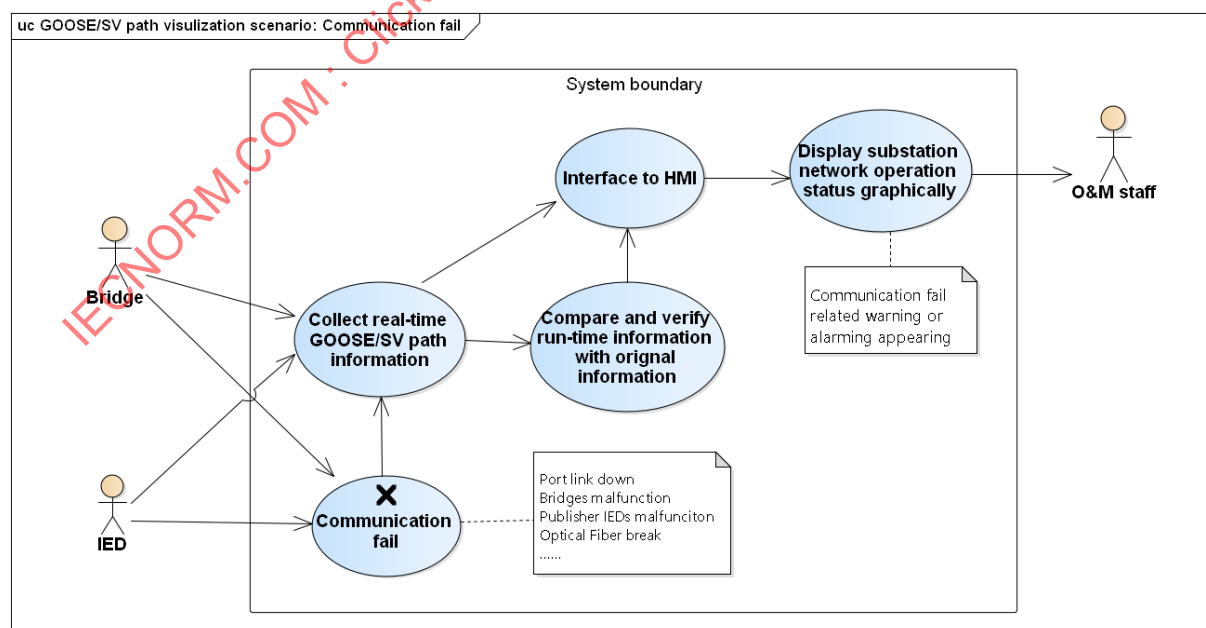


Figure 22 – GOOSE/SV path visualization scenario diagram: Communication fail

The use case under the scenario includes the following steps:

Use case step	Primary actor	Description
Step 1	Bridge, IED	After GOOSE/SV path generated, the real-time information of the GOOSE/SV path could be collected and formatted to be communicated to the HMI.
Step 2	Bridge	Perform data adaption to send the GOOSE/SV path information to HMI periodically.
Step 3	Bridge, IED, O&M staff	GOOSE/SV path information graphically displayed on HMI to provide direct real-time information for O&M staff.
Step 4a	Bridge, IED	Communication fail occurred, abnormal information was sampled and analysed by bridges.
Step 4b	Bridge	Send warning or alarming to HMI immediately with the fault position information.
Step 5	O&M staff	HMI display the warning or alarming on GOOSE/SV path where the fault positioned in a graphic way to inform the O&M staff.

5.4.5 GOOSE/SV path visualization scenario: IED duplication

5.4.5.1 Overview

IED duplication in a substation network will cause unanticipated situations and is difficult to be identified. In the case that an instrument simulates an existing IED's GOOSE/SV packets to carry out a system test but forgets to remove the settings, when the real IED is connected, the system will not work in the same way, and it is difficult to locate the problem.

When a bridge learns an IED is connected to its port, it will sample and compare the IED's information with other existing IEDs that have been learned, so it can identify the state of IED duplication and lock the port the IED connected if necessary.

5.4.5.2 Scenario description

The GOOSE/SV path visualization use case diagram under the scenario of IED duplication is shown in Figure 23.

Diagram(s) of the scenario

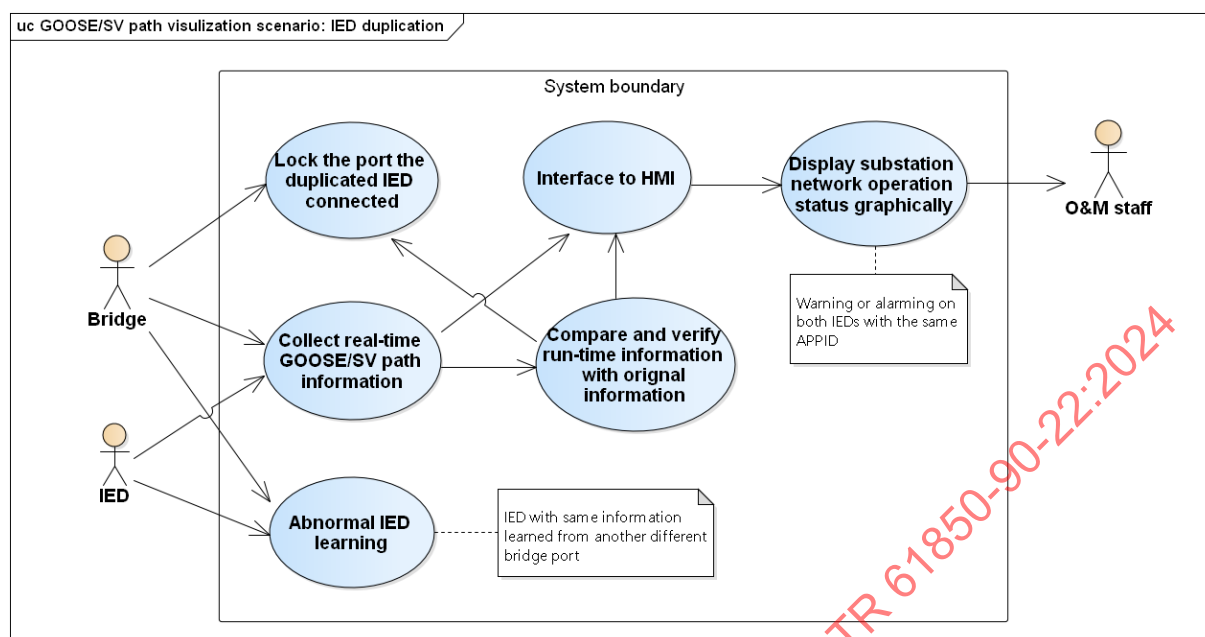


Figure 23 – GOOSE/SV path visualization scenario diagram: IED duplication

The use case under this scenario includes the following steps:

Use case step	Primary actor	Description
Step 1	Bridge, IED	After GOOSE/SV path generated, the real-time information of the GOOSE/SV path could be collected and formatted to be communicated to the HMI.
Step 2	Bridge	Perform data adaption to send the GOOSE/SV path information to HMI periodically.
Step 3	Bridge, IED, O&M staff	GOOSE/SV path information graphically displayed on HMI to provide direct real-time information for O&M staff.
Step 4a	Bridge, IED	IED with same information appeared on bridge's port, abnormal IED learning outcome was sampled and analysed by bridge.
Step 4b	Bridge	Send warning or alarming to HMI immediately with the IED duplication information.
Step 4c	Bridge	Lock the port the duplicated IED connected.
Step 5	O&M staff	HMI display the warning or alarming on GOOSE/SV path where the duplicated IED positioned in a graphic way to inform the O&M staff.

5.5 Use case 4: Bridge configuration management

5.5.1 Overview

Specific configurations of bridges are generated from the information of substation network topology and IED association that are defined in the SCD file, as described in the use cases of substation network static-routing and auto-routing. Bridge configurations need to be updated under the circumstance of adding new devices, replacing faulty bridges, changing the SCD file or physical network topology, etc., and each modification of the configuration needs to be recorded as a new version and archived for traceability.

A change of network topology or update of SCD file could result in a re-configuration of bridges involved. Before any action, the configuration used by the AR-bridge is recommended to be compared with the updated one on the relevant section. Then the necessity of replacement will be provided to engineer or HMI as information, such as through a standardized application interface. This can improve knowledge about the situation and awareness of the IEC 61850 substation automation system.

5.5.2 Use case description

The use case diagram for bridge configuration management is shown in Figure 24.

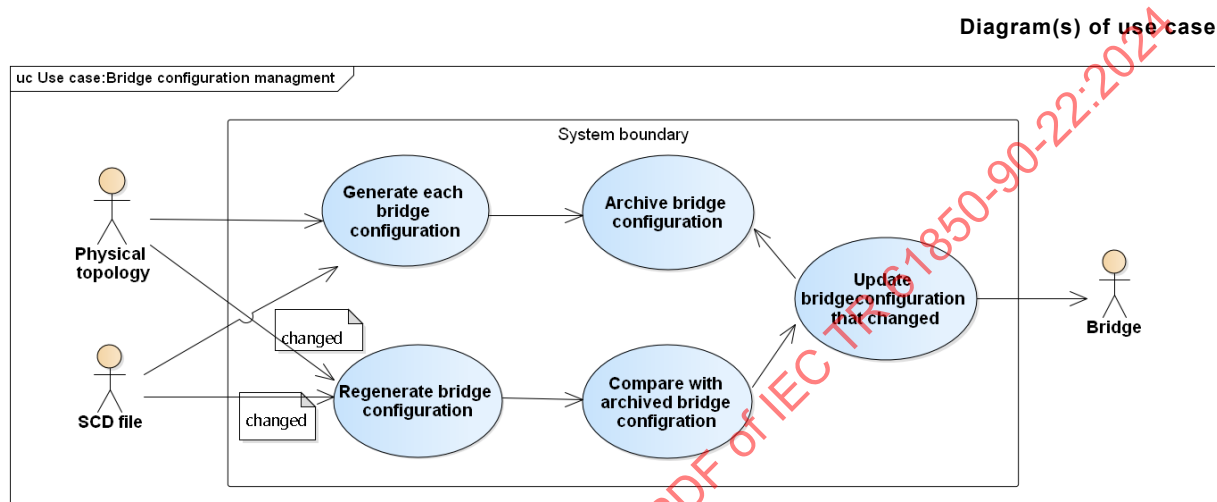


Figure 24 – Use case diagram for bridge configuration management

The use case includes the following steps:

Use case step	Description
Step 1	Generate bridge configuration combined the information of physical substation network topology and IED associations that extract from SCD file.
Step 2	Archive bridge configuration as an origin version.
Step 3	Regenerate bridge configuration when physical network topology and SCD file changed.
Step 4	Compare the regenerated and archived bridge configuration to identify the changed bridge configuration.
Step 5	Updated the bridge configuration that changed.
Step 6	Configure the bridge with updated configuration.
Step 7	Archive the changed configuration as a new version.

5.6 Use case 5: Network information provided to HMI

5.6.1 Overview

The use case is to provide standardized information to HMI (maybe other upper applications) based on the outcome of IEC 62351-7:2017 and IEC TR 62351-90-3:2021. To achieve these specified requirements, any extensions would be needed regarding GOOSE/SV path link status, GOOSE/SV traffic, etc.

In addition, a specified logical node related to the bridge would be addressed in existing projects or documents. Details can be referred to in 6.1.4.

5.6.2 Use case description

The use case diagram for Network information provided to HMI is shown in Figure 25.

Diagram(s) of use case

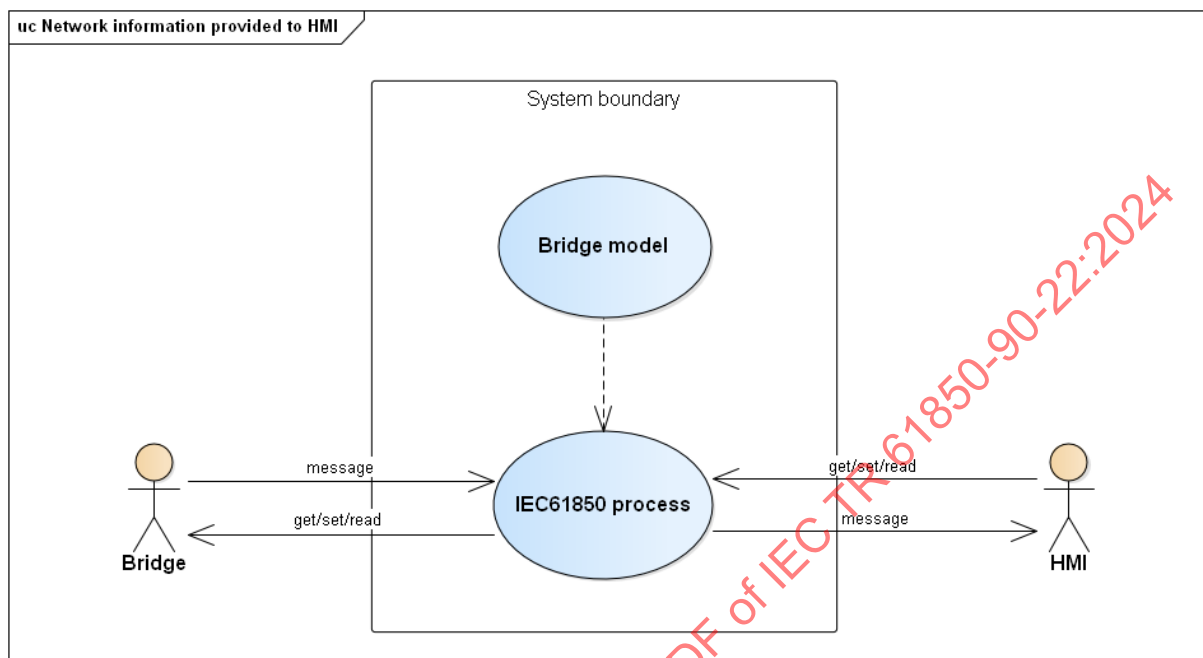


Figure 25 – Use case diagram for Network information provided to HMI

The use case includes the following steps:

Use case step	Primary actor	Description
Step 1	bridge	Necessary network information collected and formatted.
Step 2	Bridge, HMI	Bridge sends formatted data to the HMI periodically, or HMI acquires the interested data from the bridge by instructions.

5.7 Use case 6: Impact analysis in case of adding simulation device

5.7.1 Overview

A simulation device can be defined in this document as a device or software that generates simulated GOOSE/SV packets for given existing frames by one or more publishers. It could simulate devices defined in the SCD file, with a different impact on the operation process.

If the plugged simulation device is aimed to alternate a device which has been defined in SCD file (i.e. no extra device added and no network topology change), then there is no impact on the existing configuration file of the substation network.

5.7.2 Use case description

The use case diagram for impact on configuration file, auto-routing and static-routing in case of adding a simulated device is shown in Figure 26.

Diagram(s) of the use case

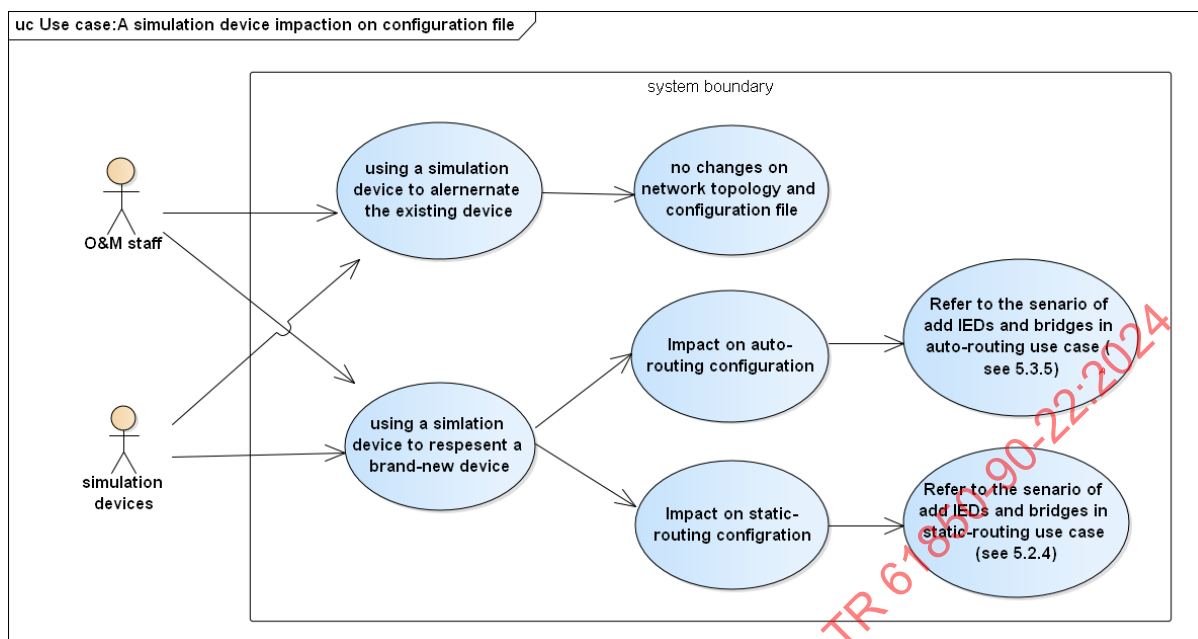


Figure 26 – Use case diagram of impact in case of adding a simulated device

The use case includes the following steps:

Use case step	Primary Actor	Description
Step 1a	O&M staff, simulation device	Using a simulation device to alternate the existing device without changes of subscription associations.
Step 1b	O&M staff, simulation device	The simulation device works as the normal device and no changes needs to be done to the configuration file and network topology.
Step 2a	O&M staff, simulation device	Using a simulation device as a brand-new device plugged in the substation network, new GOOSE/SV subscription association will be introduced.
Step 2b	O&M staff, simulation device	Impact on auto-routing configuration refers to 5.3.5. The scenario of add IEDs and bridges in auto-routing use case.
Step 2c	O&M staff, simulation device	Impact on static-routing configuration refers to 5.2.5. The scenario of add IEDs and bridges in static-routing use case.

6 Details of the auto-routing network configuration method

6.1 Requirement

6.1.1 Communication network topology discovery

To implement communication network topology discovery, the requirement for bridges which support auto-routing include the following capabilities:

- Capability to detect connected neighbour bridges.
- Capability to dynamically identify link state between connected neighbours.
- Capability to dynamically synchronize link state among the bridges.
- Capability to exchange IED subscription information between bridges.

6.1.2 IED-learning

Concerning the requirement for a bridge which has the capability to perform the functionality of IED-learning, the following items should be included:

- Capability to identify and parse the GOOSE/SV message.
- Capability to associate the identified GOOSE/SV messages with the corresponding IED sourced from SCD file.
- Capability to build mapping between bridge port and connected IED.

6.1.3 Information presentation and monitoring

In principle, the collection and presentation of AR-bridge and network information could follow the relevant contents in IEC 62351-7:2017 and IEC TR 62351-90-3:2021. As mentioned in the use case in 5.6, network information needs to be sent to the monitoring system in order to facilitate the awareness of running state and trouble shooting. The goal of this clause is to define services that can provide necessary information and send to monitoring system by AR-bridges.

The following is a list of examples of services that need to be considered during the next stage:

- Provide a counter for auto-routing indicator.
- Provide a counter for error indicator (Error of configuration updated).
- Provide the running state, i.e. resource exhaustive.
- Provide CRC and version of configuration file.
- Provide result of comparison previously configuration file versus the updated one, including the version differences of SCD file.

6.1.4 LNs for bridge model

Considering LNs related to the bridge have been provided in existing documents, i.e. IEC 61850-7-4:2020 and IEC TR 61850-90-4:2020, the performance of auto-routing of substation network may require the development of several dedicated logical nodes, and the same applies to functionality of supervision and visualization.

The following is a list of recommended logical nodes that need to be developed during the next stage:

- LN LARB, to provide the functionality of AR-bridge.
- LN LARP, to give the properties of a bridge port that supports auto-routing.
- LN LARN, to collect the neighbour information of a AR-bridge.
- LN LILO, to instantiate the outcome of IED-learning.
- LN LGEP, to obtain the GOOSE/SV egress path.

6.2 Principle for auto-routing

6.2.1 Auto-routing overview

In an IEC 61850 substation, bridges are building blocks of GOOSE/SV paths. Based on GOOSE/SV association in the SCD file, it is the bridges that turn those logical connections into physical implementation. The goal of auto-routing technology is two-fold: to automate GOOSE/SV path building process that is repeatable, and to have better visibility of built GOOSE/SV paths for maintenance and debugging purposes.

In general, five steps are necessary in the GOOSE/SV path building process:

- a) Collect IED-bridge connectivity information in a network.

- b) Collect bridge topology information in a network.
- c) Plot SV/Goose paths based on information collected in step a), b) and GOOSE/SV association from SCD file.
- d) Configure VLAN or MAC table on each bridge one by one to build all GOOSE/SV paths.
- e) Verify the correctness of built GOOSE/SV paths

If the SCD file is modified, the steps are repeated starting from step a). If the network topology changes, the steps are repeated starting from step b). The auto-routing technology is to try to automate these five steps with less effort.

6.2.2 IED-learning

IED-learning is a new run-time functionality added to AR-bridges that can detect/track/update IED-bridge connectivity information automatically. The principle of IED-learning is to have the bridge deduce which IED(s) is(are) connected on its port by consistently analysing GOOSE/SV packets on ingress. Besides the destination MAC address of a GOOSE/SV packet, there are other application-specific fields carried in the packet, like APPID, GoID/SVID, GoDatRef etc. By combining the information all together, a quite unique pattern is generated, which can be used to pin point the IED that is supposed to source a specific GOOSE/SV packet by going through SCD file.

Inside AR-bridges, two keys need to be extracted, one key for packet forwarding, and the other key to distinguish GOOSE/SV packets from each other, the latter can then be called a GOOSE/SV flow key. To simplify, if each APPID is configured to be unique in SCD, then a minimum 113 bits key (composed of 48 bits source MAC address, 48 bits destination MAC address, 16 bits APPID and 1 bit packet type (GOOSE or SV)) is good enough to identify a unique type of GOOSE/SV packet, called GOOSE/SV flow. With this key and other information, a hash table can then be built to detect/track/update IED(s) connected on its ports; this table can be called GOOSE/SV ingress flow table. An example is illustrated in Table 10.

NOTE If unique APPID cannot be guaranteed, it could impact performance of the subscriber.

Table 10 – Example of GOOSE/SV ingress flow table

Entry	Keys				Values			
	SMAC (48bit)	DMAC (48bit)	APPID (16bit)	TYPE (1 bit)	VALID (1 bit)	SPORT (6bit)	TIMESTAMP (64bit)	LENGTH (12bit)
0	00-01-02-03-04-05	01-0C-CD-01-00-01	1001	1	1	3	158763241	384
1	00-01-02-03-04-06	01-0C-CD-04-40-01	4001	0	1	7	158769247	1168
...								
n	00-01-02-03-04-82	01-0C-CD-04-40-07	4007	0	0	4	158769315	1168

Apart from the above items, several data fields are also necessary for a GOOSE/SV ingress flow table. A source port (SPORT) is used to track IED port movement; this could occur on the same bridge, but also likely between different bridges. A timestamp is also required for two purposes; it can be used to report the very first time the GOOSE/SV packet is received on the bridge port, and it also gets updated each time the following GOOSE/SV packets come in. Packet length is optional, but it is better to have it, which can be used to report the rate of a particular GOOSE/SV flow. In order to detect when the IED is removed from the bridge, a timer is also needed for each flow. On every packet arrival, the timer is reset to a setting value, otherwise timeout is triggered on that flow. This then invalidates the entry in the flow table, and reports flow timeout event to CPU. Depending on the packet type, the GOOSE/SV might need different timeout settings to accommodate different traffic patterns.

IED-learning is essentially a learning process by packet, which means for those silent IED(s) that never send out any GOOSE/SV packets, IED-learning will fail. This limitation on the silent IED could be compensated when the bridges are configured, and it will be addressed in 9.3.

There are still a few more issues that need to be resolved for more practical and reliable IED learning.

- a) How to correlate GOOSE/SV flow table from each bridge to have a global view of the GOOSE/SV path?
- b) How to distinguish those flow entry learned from every edge of the network to the entry learned on trunk ports?

These issues will be addressed in 6.2.3 to 6.2.6.

6.2.3 Network topology discovery

To have the updated network topology is one of the most important factors to GOOSE/SV path building process. Many bridge-related events may happen during every stage of the power substation lifecycle; this could be adding or removing a bridge, replacing malfunction units, upgrading a bridge with a more advanced model, adding or tearing down inter-bridge connection, inter-bridge link up/down etc. All these events could have some level impacts to the usability of GOOSE/SV paths. Network topology discovery is an automatic process that tries to track network topology change and update network topology to trigger GOOSE/SV path rebuilding and verifying process.

Depending on how actively the bridge is taking part in the network topology discovery process, there are two different methods that can do the job, the passive way or the active way. What the passive way does is very limited - only two things, advertising its identity and collecting information from its direct neighbours, for example, Link Layer Discovery Protocol (LLDP). Under this way, the bridge has no capability to use topology information or propagate what it has learned to the rest of the system; someone else needs to collect information from the bridge and do any useful things. The active way is that the bridge will be more involved in the network topology discovery process, like the usage of protocol IS-IS (a kind of Link State Protocol (LSP)). Under this way, bridges can not only actively probe their direct neighbours, learning what other bridges' knowledge of the system is, but also broadcast their knowledge of network topology to others. Protocol LLDP and IS-IS all have been designed/used to track/update network topology, but design philosophy and typical usage scenario are quite different. The details of these two protocols are described in IEEE 802.1AB and RFC 6325.

LLDP has two design decisions to bear in mind: the first one is that each LLDP capable bridge can only exchange LLDP advertisements with directly connected neighbours, it does not know or even care about any bridge that is one hop away. Secondly, neighbourhood information discovered by LLDP is stored in the Management Information Base (MIB). There are two standard MIBs defined for LLDP, LLDP local system MIB and LLDP remote system MIB. LLDP local system MIB stores the information about the local bridge, the device's own information. LLDP remote system MIB stores the information gathered from the LLDP neighbour bridges. It is up to a separate Network Management Software (NMS) stack or device to collect the information of these two MIBs from each bridge over SNMP protocol, and then construct the complete network topology. To build the very first network topology, NMS needs to go through a Bellman-Ford-like process, to collect local MIB of those bridges directly connected to NMS station to retrieve IP address of these bridges first, then retrieve remote MIB of these direct neighbours to retrieve IP address of those bridges one hop away, then continue the same steps until all bridges in a network are finished.

Link-state protocols like IS-IS are based on the idea of a distributed map of the network. When protocol converges, all of the bridges in a network that run the same set of link-state protocol have the same knowledge of the network, which is built up by the routing protocol itself, no external coordinator or server needed. The network topology and all of the information about the bridges and links are kept in a link-state database on each bridge. The database is actually in the form of records representing the topology of the network as a series of links from one bridge to another. The database must be identical on all of the bridges in an area for LSP to work. Initially, each bridge only knows about a piece of the entire network, the local bridge knows only about itself and the local interfaces to its neighbour. Then the LSP routing protocol distributes this information to all of the other bridges so that a complete picture of the network is generated and stored in the link-state database. LSP uses reliable delivery mechanism so that LSP bridges have ways to find out if the information passed to another bridge was received or not. The more bridges and links that LSP has to deal with, the larger the link-state database that has to be maintained in each bridge. The LSP propagation process is exemplified in 6.2.7.3.

6.2.4 Plot GOOSE/SV path

Once the network topology is built up, the algorithm running on each bridge starts to calculate the GOOSE/SV subscription information based on the list of directed IED learning. It uses the information extracted from the SCD file as a dictionary and iterates the IED list as the key to generate two sets of information. One is the local routing information for GOOSE/SV packets to those ports which have IED connected, the second one is the aggregated GOOSE/SV packets which only pass through this bridge without IED connection, then distribute to the network. In centralization implementation, for example SDN, the SDN controller will use this information to plot the GOOSE/SV path for each bridge. In LSP implementation, this information will be put in LSP mode and distribute to the network, whichever bridge has that GOOSE/SV packet will start to forward the packet based on a pruned distributed tree in a related protocol encapsulated form. This distribution is built on the shortest path forwarding algorithm, it could be one tree for all or usage of several trees, depending on the configuration. When the intermediate bridge receives this GOOSE/SV packet, it does a look up in the local forwarding table, if there are requests by IEDs on this bridge, the bridge decapsulates the packet and does local multicast forwarding to those ports. The bridges then execute a second look up to see if any downstream bridge needs this packet, and if so, do a second multicast to downstream bridges in LSP encapsulated form. The building process of GOOSE/SV path is also exemplified in 6.2.7.3.

6.2.5 Install VLAN/MAC table configuration to bridges

Because the auto-routing is still using VLAN/MAC to forward multicast packets, the final GOOSE/SV path presentation would be embodied by a VLAN/MAC table in each bridge in the substation network. After finishing a GOOSE/SV path calculation, auto-routing will generate related configuration information for each bridge involved, and then the bridges involved will create related VLAN/MAC table entries according to the information. So, the installation of GOOSE/SV paths process is to set the generated configuration VLAN or MAC table on each bridge one by one, and this process is also carried out automatically. When topology changes under failure occurring circumstances, the GOOSE/SV configuration information may change as well, and it will trigger the bridges to reconfigure the VLAN/MAC to allocate the new GOOSE/SV path to avoid communication break.

If the SCD file or network topology need to be updated with the demand of bay extension or other cases, the update process needs to be checked and reviewed by the substation operator involved with manual intervention to make sure the correctness and availability of the update documents. Then the AR-bridges can let the auto-routing reconfigure the network automatically with these documents.

6.2.6 Verify the correctness of built GOOSE/SV paths

On-line verification that auto-routing is implemented is a novel method different from the present substation network verification process. Normally GOOSE/SV path verification has two parts, correctness and accurateness, which means that the GOOSE/SV packet shall only go to the port it supposed to and no other ports. The correctness of GOOSE/SV paths verification needs at least three parties participating in testing in which an IED can be a subscriber and a publisher at the same time:

- publisher IED(s) that generate GOOSE/SV packets;
- network that forwards GOOSE/SV packets;
- subscriber IED(s) that receive GOOSE/SV packets.

After auto-routing is deployed in the substation network, and GOOSE/SV path installation is completed, the bridges keep doing IED-learning. The outcome of the IED-learning can be used to verify if the publisher IED(s) has generated only SCD-specified GOOSE/SV packets. If a GOOSE/SV packet does not belong to any GOOSE/SV path defined in SCD file, then a warning message could be generated and reported. On the egress side, a subscriber on a particular GOOSE/SV path will track the reception of GOOSE/SV packets; if packets are not received in two time of TTL periods, it will report path failure to the up-layer system.

6.2.7 TRILL example

6.2.7.1 Overview

Protocols like TRILL and SPB are all applicable to develop substation network auto-routing, they have similarities in some way. Both techniques are taking the goal of overcoming the bandwidth waste problem of traditional STP related protocols and adding a control plane to provide the capability of network topology discovery and utilization of redundancy paths, but their implementation is different, and they are also published by different organizations; TRILL is developed by IETF, while SPB is published by IEEE.

TRILL is an L2 forwarding protocol that operates within one IEEE 802.1-compliant Ethernet broadcast domain. It is kind of a protocol that uses L3 link state routing technology in layer2 traffic transmission. TRILL uses IS-IS route protocol as its control plane on L2, and addressing occurs in the network layer by Nickname. SPB was developed on the top of PBB (Provider Backbone Bridging, IEEE 802.1AH) MAC-in-MAC mechanism, also introduced IS-IS protocol as its control plane to complete network topology learning and path computation work, the addressing is performed by means of MAC address, and it was standardized as IEEE 802.1AQ. Although TRILL and SPB all take use of IS-IS protocol as its control plane, the implementation of each is different, such as encapsulation, ECMP algorithm, header duplication, and OAM etc. A TRILL exampled auto-routing is given in this document.

6.2.7.2 Brief introduction of TRILL protocol

TRILL replaces the spanning tree protocol by using IS-IS routing to distribute link state information and calculate the shortest paths through the network. IS-IS is used because of its pure L2 routing feature that does not require IP to transport the frames. TRILL data packets and IS-IS routing packets are exchanged between Routing Bridges (RBridges). RBridges automatically discover each other via IS-IS "Hello" frames and require no explicit configuration. MAC addresses of end stations (i.e. IEDs) are learned at the edges of a TRILL domain only. RBridges in the core network do not need to keep track of end station MAC addresses. TRILL protocol can easily support highly meshed topologies so the hop count should be minimized to improve real time performance if applicable.

TRILL is chosen as the example implementation of auto-routing for two reasons: firstly, TRILL has been standardized, and some TRILL capable devices have been used widely in data centres; secondly, TRILL is relatively light compared to other similar protocols. TRILL provides a solution for shortest-path frame routing in multi-hop IEEE 802.1-compliant Ethernet networks with arbitrary topologies, using an existing link-state routing protocol technology and encapsulation with a hop count. The current work of the working group is around operational and deployment support for the protocol. This includes an MIB module and other pieces needed for operations, but also additional ways to extend and optimize TRILL for the properties of the networks on which it is deployed.

In a TRILL domain, RBridges encapsulate Ethernet frames at the ingress, route the frames using IS-IS link state routing information, and then decapsulate the Ethernet frames at the egress again. This process is shown in Figure 27.

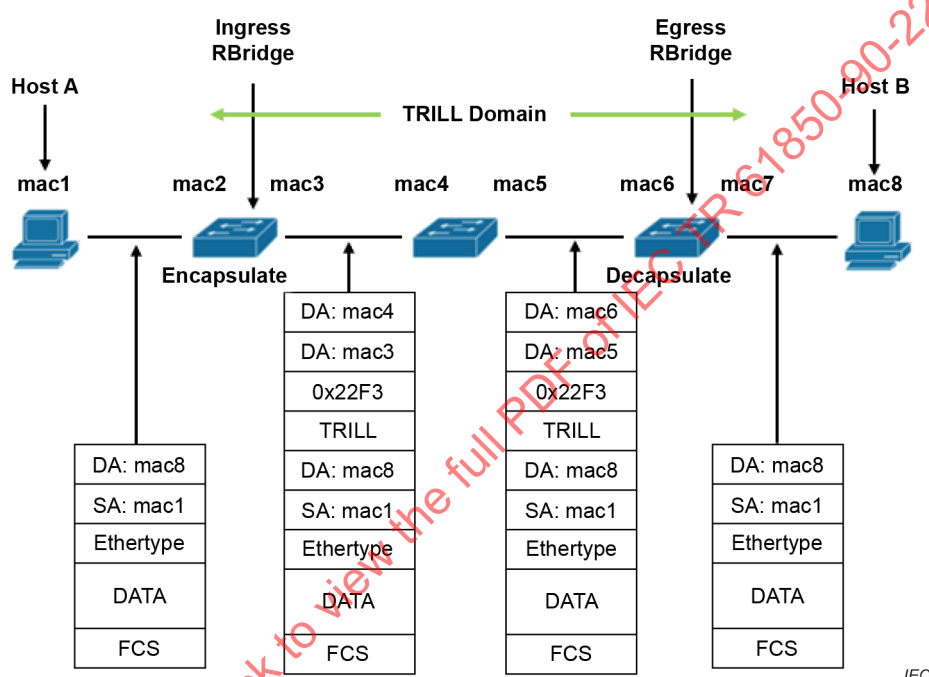


Figure 27 – TRILL encapsulating and decapsulating

When host A on the left (MAC address mac1) in Figure 27 has the requirement to send an Ethernet frame to host B on the right (MAC address mac8), the frame process procedure is as follows:

- The frame is encapsulated by the ingress RBridge with a TRILL header and an Ethernet header. The TRILL header contains a 2-byte identifier of the ingress RBridge and a 2-byte identifier of the egress RBridge. The egress RBridge is determined by the shortest path to the final destination (host B). The TRILL header also contains a hop count.
- The ingress RBridge sets the source address in the outer Ethernet header to the MAC address of its outgoing interface and sets the destination address to the MAC address of the next hop RBridge (determined by IS-IS shortest path routing).
- Each RBridge in the path rewrites the outer Ethernet header with its own MAC address as source and the MAC address of the next hop RBridge as destination. At each RBridge the hop count in the TRILL header is decremented.
- At egress, the encapsulation headers are removed and the original Ethernet frame is sent to the destination (host B).

There can be any number of traditional Ethernet bridges between two R Bridges because bridges that do not support TRILL just forward the traffic based on the destination MAC address and VLAN ID, if present. R Bridges do not propagate spanning tree protocol BPDUs, so R Bridges can limit the span of spanning trees regions.

Figure 28 shows the frame structure of the Ethernet and TRILL headers used by the TRILL protocol.

Destination MAC Address								
Destination MAC Address				Source MAC Address				
Source MAC Address								
Ethertype:0x22F3				V	R	M	OPLen	Hop
Egress RBridge Nickname				Ingress RBridge Nickname				
V		Version			2 bit			
R		Reserved			2 bit			
M		Multi-destination			1 bit			
OPLen		Option leength			5 bit			
Hop		Hop count			6 bit			
Nickname		Nickname			16 bit			

IEC

Figure 28 – Ethernet and TRILL headers

TRILL protocol uses 0x22F3 as EtherType. It can encapsulate untagged or tagged customer frames. The tags in customer frames are preserved while forwarding through a TRILL domain. Unicast frames are sent via the shortest path between ingress and egress R Bridge. R Bridges use distribution trees to forward multi-destination frames (i.e. unicast frames with unknown MAC address, multicast and broadcast frames).

There can be one or more distribution trees in a TRILL domain. R Bridges will pre-compute all the distribution trees that might be used. Each R Bridge advertises the maximum number of distribution trees it can support in its TRILL LSP, but there is only one R Bridge which is chosen by all R Bridges (based on several R Bridge qualifiers) in a TRILL domain to take the following decisions for all R Bridges:

- How many trees will be used?
- Which trees will be used?
- The tree number of each tree.

The number of distribution trees that is decided cannot be higher than the number of trees supported by the R Bridge with the fewest number capacity. Each ingress R Bridge (the appointed forwarder for a certain VLAN) chooses which of the distribution trees it will use for multi-destination frames. Usually, this is the tree whose root has the lowest cost path from the ingress R Bridge. The ingress R Bridge itself could be the root of the chosen tree. It includes the chosen tree information in its LSP distributions, and all other R Bridges keep track of it so that they can use this information in Reverse Path Forwarding (RPF) checks.

The distribution trees are shared across all VLANs, but pruning should take place per VLAN when a branch has no potential receivers. When receiving a native multi-destination frame, the ingress R Bridge converts it to a TRILL data packet. It uses the All-R Bridges multicast address (01-80-c2-02-00-01) as outer destination MAC address.

Multipathing over multiple distribution trees is supported. The ingress and egress R Bridges are the only bridges that learn end station MAC addresses and VLAN information. At ingress, the R Bridge learns local end station information by collecting port and MAC address and VLAN information of received frames. At egress, the R Bridge learns remote end station information by collecting ingress R Bridge and MAC address and VLAN information of the original frame in the TRILL encapsulated packet. Transit R Bridges do not need to collect end station information. They only need to collect MAC addresses of other R Bridges. Thus, the MAC forwarding table of transit R Bridges scales with the number of R Bridges instead of with the number of end stations.

The R Bridges can choose a backbone VLAN in the TRILL domain to communicate with each other. This VLAN is independent from the VLAN used in the original Ethernet frame in the encapsulated TRILL packet. The ESADI (End Station Address Distribution Information) protocol can be used to announce end stations that have been explicitly enrolled. Advertising end station MAC addresses using ESADI is optional, as is learning from these announcements. R Bridges that are the appointed forwarder for a certain VLAN may participate in the TRILL ESADI protocol for that VLAN. All transit R Bridges must properly forward TRILL ESADI frames as if they were multicast TRILL Data frames. There are a couple of advantages of using ESADI. The enrolment might be authenticated (for example, by cryptographically based EAP methods via IEEE Std 802.1X-2010). The ESADI protocol also supports cryptographic authentication of its messages for more secure transmission. Finally, if an end station is unplugged, an immediate update can be sent via the ESADI protocol.

R Bridges can optionally support multipathing. This is done by ECMP routing. If multiple equal cost paths present towards the same destination, an R Bridge can distribute traffic over those multiple paths. This is usually done per flow in order to avoid reordering and path MTU discovery problems.

6.2.7.3 TRILL based auto-routing

6.2.7.3.1 Propagate GOOSE/SV information with TRILL LSP flooding

TRILL can be used to implement GOOSE/SV auto-routing without much difficulty. With the help of IED-learning, each R Bridge can collect GOOSE/SV packets subscribed by those IEDs directly connect to itself, put the list of DMAC or VLAN ID of required GOOSE/SV packets in IS-IS LSP and flooding LSP out to other R Bridges in whole network, as shown in Figure 29. Each R Bridge will calculate same amount of distribution trees which are rooted at each R Bridge, then prune the tree based on list of desired DMAC or VLAN ID embedded in LSP packets.

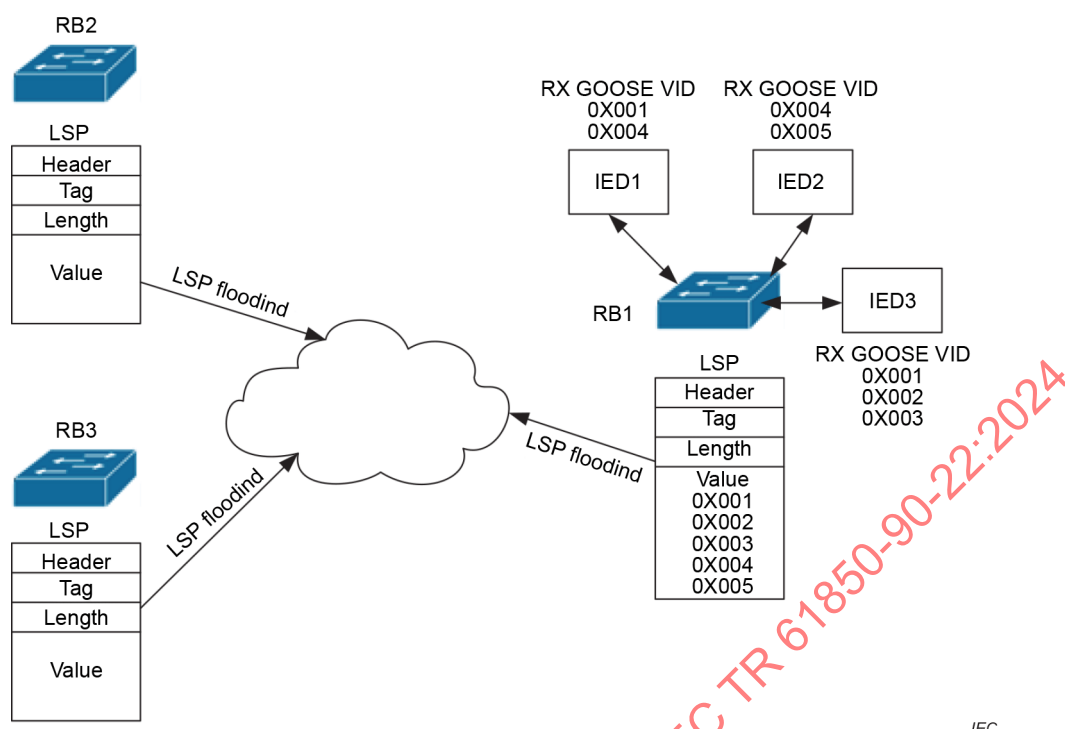
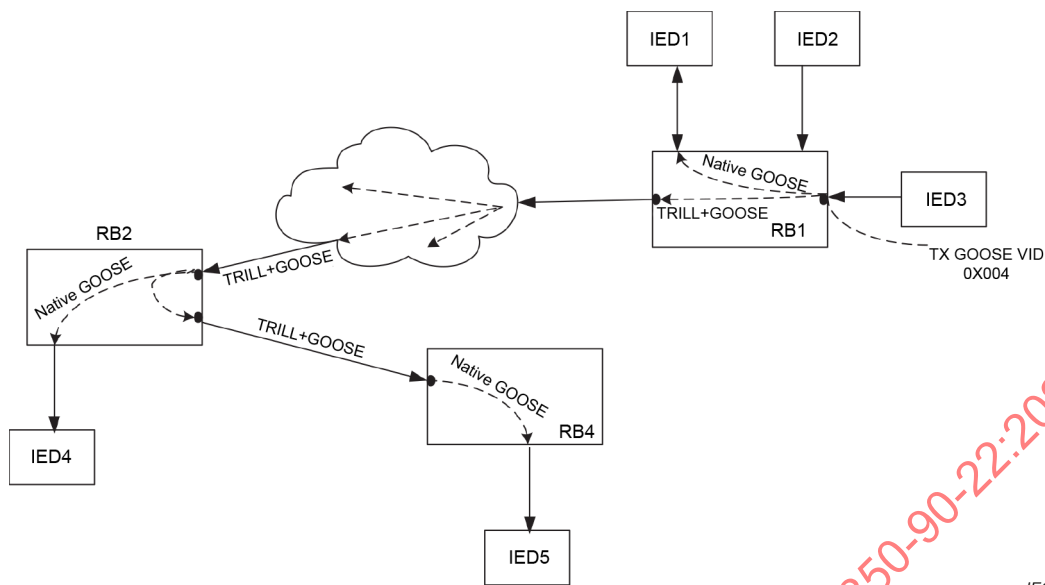


Figure 29 – Illustration of LSP flooding

6.2.7.3.2 GOOSE/SV path built with TRILL

When a native GOOSE/SV packet is received by RBridge, it will do two lookups based on DMAC or VLAN ID; the first lookup decides if this packet is required by any directly connected IEDs, and do normal layer two forwarding procedure if so. The second lookup is to find next hops of the distribution tree, and if so, it will encapsulate native GOOSE/SV packet with a TRILL multicast header and forward to next RBridge.

When a TRILL encapsulated GOOSE/SV packet is received by RBridge, it will do two lookups as well. If these are subscribers on this RBridge, it will de-encapsulate the TRILL header and forward native GOOSE/SV packets to those ports. If this RBridge is a transition node in the distribution tree, it will modify the TRILL header, reduce the hop counter by 1, drop the packet if hop counter reaches zero, and forward the modified GOOSE/SV packets to the next hops. With the end of this look up process, a GOOSE/SV path is built. The forwarding process of a GOOSE/SV packet with TRILL protocol is shown in Figure 30.

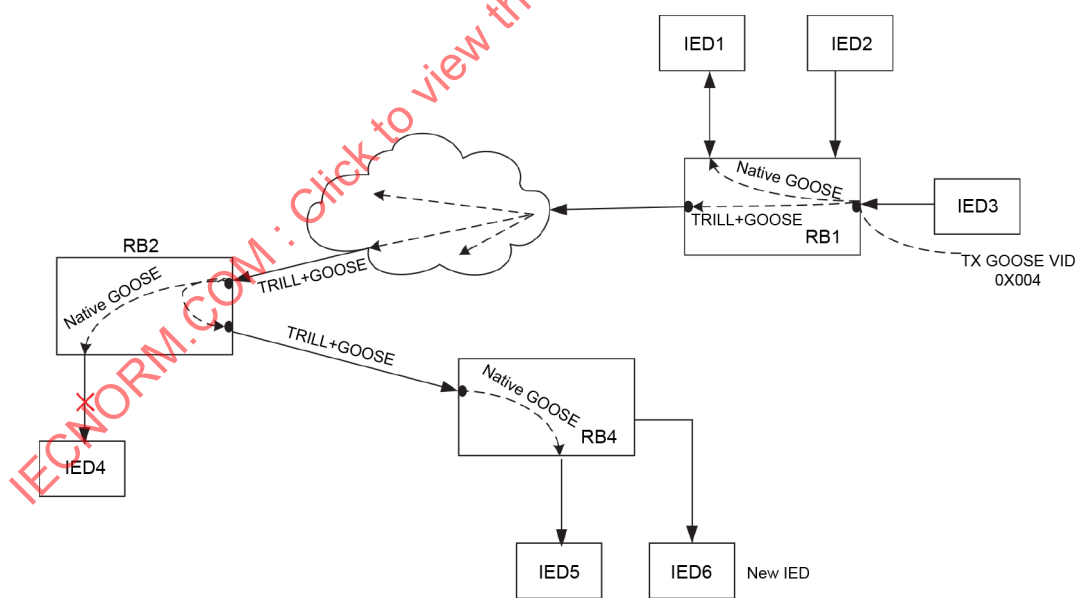


IEC

Figure 30 – Forwarding process of GOOSE/SV packet with TRILL

6.2.7.3.3 Deal with IEDs disconnection/addition with TRILL

When an IED is disconnected from the RBridge, IED-learning will update the list of required DMAC or VLAN ID, it will trigger the IS-IS LSP update, the new version of LSP will be flooded to other Rbridges, and every RBridge will calculate a newer version of distribution tree and pruning. When protocol converges, the GOOSE/SV path to that disconnected IED is removed. The RBridge repeats this procedure every time a new IED is added or existing IED is moved. TRILL LSP update procedure of an IED disconnection/addition is shown in Figure 31.



IEC

Figure 31 – LSP update procedure of an IED disconnection/addition

6.2.7.3.4 Deal with bridges disconnection/addition with TRILL

When a new RBridge is added to the network, the IS-IS hello mechanism will detect a neighbour RBridge, and the IS-IS protocol will update its neighbours and flooding LSP to other RBridges. Meanwhile, it will send the latest LSP to the newly added network device. Every RBridge will re-calculate the distribution tree and pruning that includes this RBridge. When protocol converges, the GOOSE/SV path will be updated to reflect the latest topology. The same procedure is used when an RBridge is disconnected from network. The TRILL LSP update procedure of a bridge disconnection/addition is shown in Figure 32.

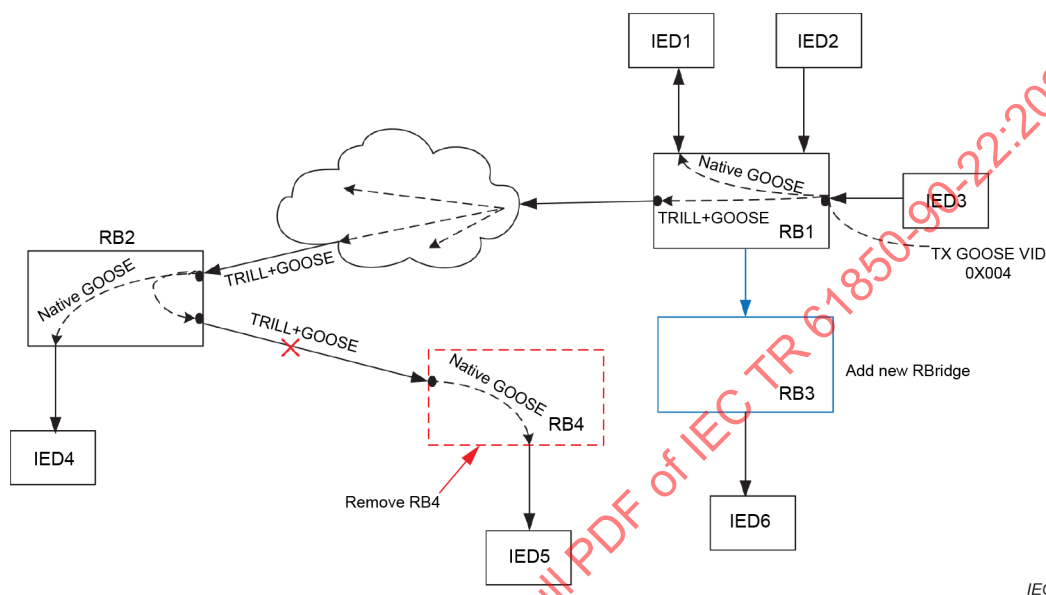


Figure 32 – LSP update procedure of a bridge addition/disconnection

6.3 Comparison of existing technologies

6.3.1 General

Planning and verifying network topology and traffic control strategies are the most important procedures during substation network engineering and commissioning phase. Protocols of RSTP, HSR, and PRP are currently adopted in substations to establish redundancy network topology, and detailed implementation is specified in IEEE 802.1D, IEC 62439-1, IEC 62439-3 and IEC TR 61850-90-4. Of these documents, multicast MAC address filtering, VLAN traffic control and comparison between them is briefly introduced, and they are currently popular related to traffic control strategies.

6.3.2 Comparison of network redundancy technology

HSR and PRP use a special extra tag to mark the data transmission, which is not understood by off-the-shelf devices, so they must use RedBoxes to couple with other HSR/PRP unaware network or devices. Compared with RSTP, the redundancy provided by HSR or PRP is a kind of double alive path; seamless transfer is the most successful characteristic.

The principle of substation network auto-routing technology based on AR-bridges has been described in 6.2. Unlike RSTP/HSR/PRP carried out on Layer 2, auto-routing operates between Layer 2 and Layer 3, so it can work with RSTP, HSR or PRP together without conflict, and obtain seamless recovery combined with using HSR or PRP. A comparison of advantages and drawbacks comparison among auto-routing, RSTP, HSR and PRP is summarized in Table 11.

Table 11 – Advantages and drawbacks of auto-routing versus RSTP, HSR or PRP

Technology	Advantages	Drawbacks
Auto-routing	Multiple paths available from source to destinations (Equal-Cost MultiPathRouting) to full use network source and provide load balance. Awareness to network topology change including AR-bridges and IEDs connected with, auto regenerate and verify optimal GOOSE/SV path without human intervention. Easy to use and verify the relationships between IED publishers and subscribers.	The auto-routing by itself cannot provide seamless recovery performance. The auto-routing has limitation on IED-learning when there are silent IEDs in substation network.
RSTP, HSR or PRP	RSTP applies fast recovery of ring network. HSR applies seamless recovery of ring network. PRP provides seamless recovery via duplicated network in parallel.	Not IEDs awareness. HSR/PRP only suitable for specific network topology. RSTP does not provide seamless recovery.

6.3.3 Comparison of traffic control technology

GOOSE/SV multicast traffic is the main load of substation network; due to the default multicast all direction forwarding mechanism, performing multicast filtering to control traffic can significantly reduce the pressure of bridge forwarding. VLAN together with QoS is used mostly to classify the service and prevent traffic congestion, while rigid network partition needs to be planned and accompanied by large engineering effort. Multicast MAC filtering is normally used together with VLAN, supported by static or dynamic configuration according to specific rules, however, the dynamic resulting network traffic can hardly be predicted, so use of dynamic multicast control protocols (such as GMRP, MMRP) is not recommended. A novel GOOSE/SV traffic control and engineering strategy on top of auto-routing is provided and detailed in Clause 8; Table 12 summarizes the pros and cons of these different traffic control strategies.

Table 12 – Advantages and drawbacks of different traffic control strategies

Technology	Advantages	Drawbacks
Per GOOSE/SV flow traffic control	No need for an 802.1Q support in IEDs. Precisely forwarding bandwidth control for every GOOSE/SV message. Only learned GOOSE/SV messages can be forwarded, and rejected unwanted messages.	Static multicast filtering table needs to be pre-designed according to network topology.
VLAN + Multicast Filtering	Applies to all traffic, including unicast, multicast and broadcast. Separation by VLANs ensures a first level of security, or at least some protection against bad configuration.	Rigid network partition. Top level devices such as SCADA must send VLAN-tagged frames to communicate with devices in different VLANs. Large engineering effort.

6.3.4 Other available technology

Other traffic control technologies can also be effective in a substation network, for example, the use of SDN technology as discussed in 5.2.6. SDN can be used to carry out accurate traffic control by using flows and flow tables to match on different services and applications (e.g. GOOSE and SV) and only permit authorized traffic across a network from the source IED to the destination IED.

6.4 Network device configuration

6.4.1 General

GOOSE/SV association is the essential piece of information to configure substation network by either auto-routing or static-routing, this part normally does not change frequently in the SCD file. Although directly using SCD could satisfy the configuration requirement, this method has a few drawbacks. First, a bulky SCD file might exceed the process capability of the CPU system in bridges. Secondly, there is much information such as dataset definition, data template etc., which is irrelevant to bridge configuration. Third, there are circumstances like adding/removing of diagnostic devices temporarily which are challenging to be part of the SCD file. Introducing a stripped-down version of SCD that is dedicated for bridge configuration would address these drawbacks. This file is called BCD in this document and detailed in Annex A.

6.4.2 Network re-configuration scenarios

GOOSE/SV path modification is the utter driving force of network re-configuration. There are many scenarios that leads to GOOSE/SV path update. Table 13 list some typical scenarios.

Table 13 – Scenarios requiring network re-configuration

Scenarios	Description
bay extension	Substation project could span multiple years and be divided into several phases. If bays are constructed step by step, the SCD evolves along the way, new IEDs and bridges are constantly added to SCD. Existing GOOSE/SV path are extended, new GOOSE/SV path are created and these all require network re-configuration accordingly.
bay update	There are chances that IEDs in the bay might need to be modernized or updated. A new generation of IEDs with more functionality will be added to the SCD and older IEDs will be removed from SCD. In such case, SCD might go through some significant changes in multiple sections, which means network re-configuration is inevitable.
IEDs addition	When IEDs with desired functionality needs to be added, SCD will be modified to reflect newly added IEDs and GOOSE/SV path to support new functionalities.
IEDs consolidation	When IEDs are being consolidated, normally IED organization in SCD and physical connection will be changed which cause network re-configuration.
IED functionality tweaking	Sometimes optional functionality in IED might be enabled or disabled, consequently GOOSE/SV path will be modified as well, demanding network re-configuration.

6.4.3 Silent IED support by IID

Silent IED is a kind of pure subscriber IED, it has two folds. On one side, it could refer to an IED which existed in SCD but never published any GOOSE/SV messages, for example, a busbar protection device with multiple ports, using one port to publish GOOSE/SV message, while using another different port to subscribe GOOSE/SV messages. On the other side, silent IED could be a temporary diagnostic device that cannot be part of SCD, but necessarily for debugging or packets logging. Whatever the kind of silent IED, it fails IED-learning.

The reason that silent IED cripples auto-routing is because of the inability to auto learn which bridge and which port of the bridge it is connected to, while this is the outcome of IED-learning, and this missing information could be incorporated into an IID file which supplied by bridge configurator, then together with SCD file, it can be used to generate the bridge configuration.

In case a silent IED exists, the bridge ID and port index it is connected to are added into a specified IID, and its GOOSE/SV subscriptions are added as well. By doing so, auto-routing treats silent IED no different to normal IED. Steps of how a silent IED is handled are as follows:

- Collect information of the silent IED, at least including the silent IED name, the bridge ID and the specific port it would be connected to, and the GOOSE/SV association it involves;
- Generate an IID file to accommodate this information been collected by using IED configurator;

- c) For the silent IED which existed in the SCD file, this IID file could be incorporated into SCD file by using system configurator for permanent use, for the other kind of silent IED used for temporary, the IID file could be the independent input for auto-routing together with SCD simultaneously;
- d) A bridge configurator then could be used to extract necessary information from SCD/IID file and generate BCD file, and this BCD file then will help to configure the bridges and perform GOOSE/SV auto-routing finally.

More detailed description and examples are placed in Annex A.

6.4.4 GOOSE/SV path configuration using BCD

The essential of the GOOSE/SV path is the combination of VLAN/MAC table or multicast table of the bridges, which could be installed manually or by tools. In this document, the BCD file is introduced as a stripped SCD that only carries GOOSE/SV path information; it could be generated by a bridge configuration tool, such an example is illustrated in Annex A.

6.4.5 Configuration version control

The SCD file has the version control mechanism that is defined in IEC 61850-6 to facilitate file management; when information changes in the SCD file, the version normally updates as well. Because the BCD file is treated as the subset of an SCD file, it would have the same version-controlled way. Fine and coarse version number increment are proposed to represent minor configuration change and major configuration change respectively, and an example is given below.

6.4.6 Example for network device configuration management

6.4.6.1 Minor configuration version change

Normally minor configuration version change happens during the substation debugging process, including bay addition, functionality alteration etc. Another situation where a minor version change may be needed is the functionality configuration change after the substation was put into operation, for example, functionality addition or alteration of a protection unit. When a running substation undergoes renovation and/or expansion, substation network configuration version change could be deemed as minor change during this process. After the commissioning is completed and the substation is put into normal operation, the substation network configuration version number can be updated to a stable running version for archive and backup.

An example is given to demonstrate the BCD file version management under a bay expansion situation accompanied with SCD file version change. The original network topology is shown in Figure 33. The original SCD file version number is set to be V1.00, and the corresponding BCD file version is set as V1.00 also.

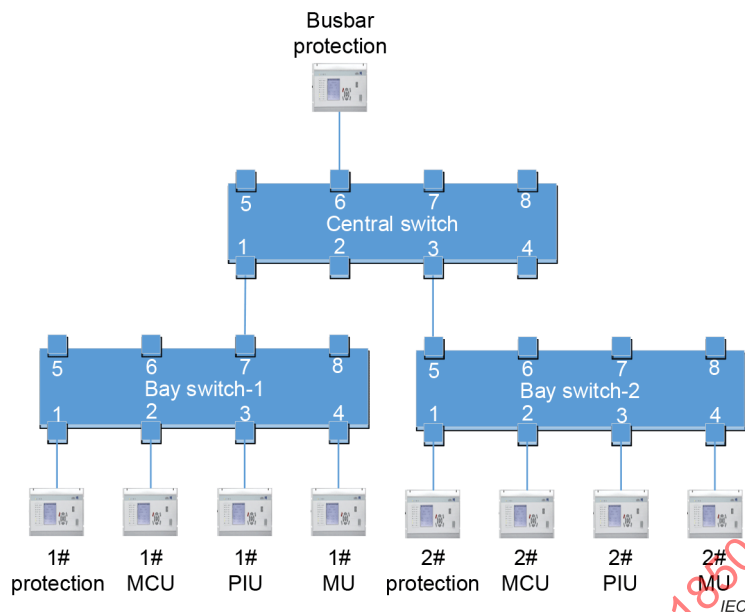


Figure 33 – Origin network topology for BCD file (Version 1.00)

GOOSE/SV subscription relationship is described as follows:

- Busbar protection subscribes the GOOSE/SV control blocks of MU1#, PIU1#, protection1#, MU2#, PIU2# and protection 2#.
- Protection1# subscribes the GOOSE/SV control blocks of MU1# and PIU1#.
- Protection2# subscribes the GOOSE/SV control blocks of MU2# and PIU2#.
- MCU1# subscribes the GOOSE/SV control blocks of MU1# and PIU1#.
- MCU2# subscribes the GOOSE/SV control blocks of MU2# and PIU2#.

When a new bay is demanded according to the plan, as shown in Figure 34, busbar protection needs to subscribe the added GOOSE/SV blocks information from the related IEDs (protection3#, PIU3#, MU3#) that newly connected into the substation network. This association information is added into the SCD file, and then the SCD file version number modified to V1.01.

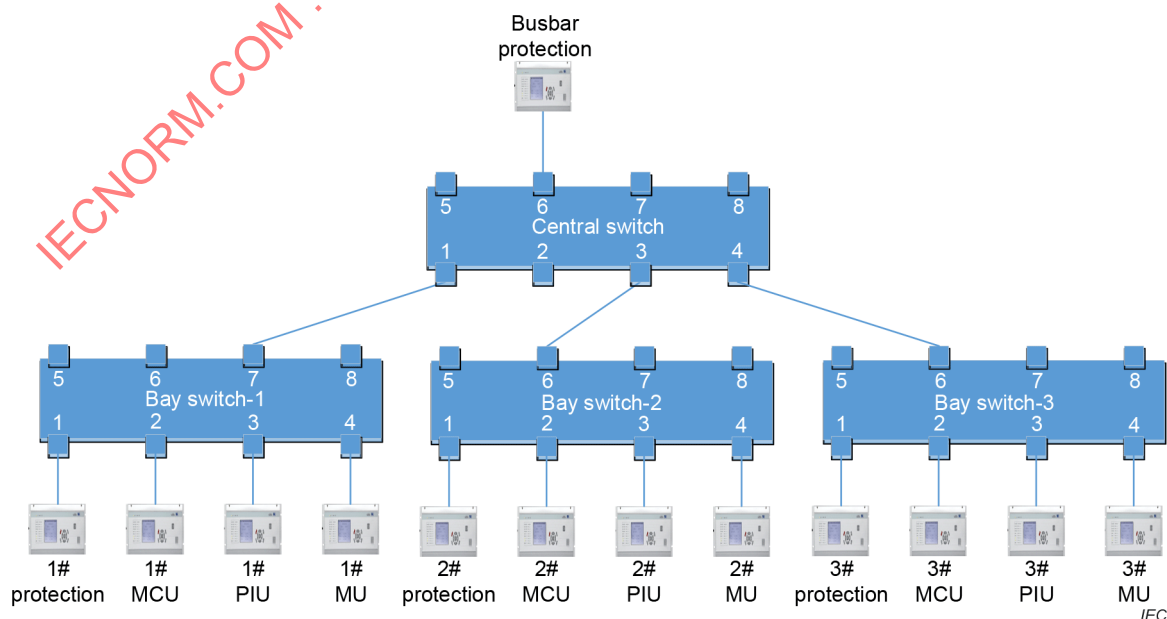


Figure 34 – Minor version change due to bay extension

Comparing and analysing the modification of SCD file, the communication requirement between IEDs (in bay 3#) and the busbar protection will demand the configuration update of central switch, and the new bay switch-3 needs a configuration file. Then the BCD file could be updated to a new version of V1.01 to accommodate the increased GOOSE/SV path information according to the SCD file of version V1.01.

The BCD file of version V1.01 is used to update the configuration of the central switch and bay switch-3. Because bay switch-1 and bay switch-2 have no GOOSE/SV association change, they do not need to be updated. If the bay switch-1 or bay switch-2 needs to be replaced due to malfunction or other cases, both version of V1.00 and V1.01 BCD file can be used to configure the replacement.

6.4.6.2 Major configuration version change

In general, major configuration version change occurs when:

- Substation transfers into regular operation from engineering stage.
- In the case of a substation that is constructed in phases, the first stage substation project goes into operation; the subsequent project starts to run after the substation construction finished.
- Main wiring topology changes in the substation.

Major configuration version change means that a significant event has occurred in a substation. The following example proposes that two substation construction phases be included, as illustrated in Figure 35, the primary project of the substation has been put into operation, and the version number of current SCD and BCD file is V2.00.

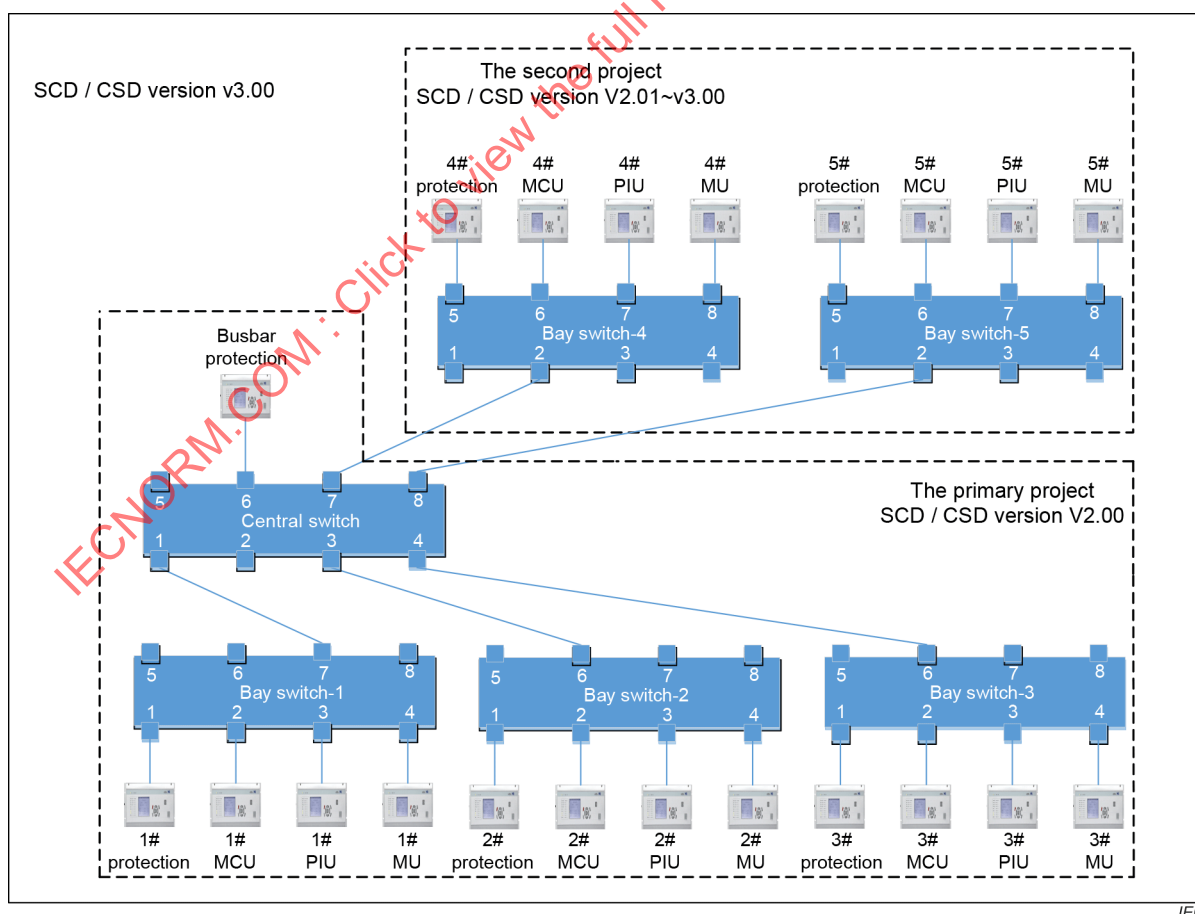


Figure 35 – Major version change of owe to the finish of substation phases

When entering the second substation construction phase, two new bays (bay 4# and bay 5#) are added, and the busbar protection has to subscribe those added GOOSE/SV blocks information from the addition IEDs (for example, protection 4# and 5#, PIU4# and 5#, MU4# and 5#). During the engineering process of this second project, the SCD file and BCD file start to upgrade from version 2.01 to accommodate addition IEDs and their subscription associations, then version change increases according to the minor change rule until the end of the stage. Before the second project is put into operation, the SCD and BCD file version is updated to version 3.00 as the running and archiving stable version for substation network.

7 GOOSE/SV path presentation and monitoring

7.1 General

Like OAM for carrier Ethernet network and BFD (Bidirectional Forwarding Detection) for IP based network, there is certainly a possible similar failure detecting and performance monitoring function for substation GOOSE/SV path that could be specified and built to assist efficient substation network management. As many factors are related to the GOOSE/SV path, including the interfaces, data links, IEDs, and forwarding plane in bridges, a systematic design is required to support various OAM requirements, including but not limited to quick trouble shooting, fault detection, fault device replacement, performance monitoring, reliability analysis and optimization, visual presentation to HMI, etc.

For carrying GOOSE/SV path supervision, information including network topology, IED connection status, GOOSE/SV packets transmit/receive quantity etc. are suggested to be collected. The IED already has data models specified in IEC 61850-7-4 for GOOSE/SV of IED publisher or subscriber, for a bridge, data models for special protocol like RSTP, LLDP are already provided in IEC TR 61850-90-4:2020, but are not sufficient to present a GOOSE/SV path. On top of the existing data models, some new LNs related to AR-bridge are proposed to implement the GOOSE/SV path presentation and monitoring.

7.2 "Substation network static-routing" based approach

The static-routing approach supports GOOSE/SV path presentation and monitoring without the need to extend the already existing data model capabilities of IEC 61850 or to define additional LNs. As described in 5.2 the Bridge Configurator needs to know what the network topology looks like to render the paths of the GOOSE/SV streams between publishers and subscribers as defined in the SCD file. Thus, the Bridge Configurator can visualize and monitor the paths of the corresponding GOOSE/SV streams through the network topology. For the stream monitoring during operation well-established protocols like SNMP/MIB and additionally IEC 61850 MMS data provided by end devices (IEDs and MUs) can be used.

7.3 "Substation network auto-routing" based approach

7.3.1 GOOSE/SV path presentation

The presentation of the GOOSE/SV path is suggested to include the following two types of connection information provided by the AR-bridge.

- a) Connection information between IED and bridge:
 - Physical sourced bridge port related to the GOOSE/SV path.
 - DMAC, SMAC, APPID, and EtherType of the GOOSE/SV message.
 - Packet length of the GOOSE/SV message.
 - Physical destination bridge port of the GOOSE/SV path.
- b) Bridge topology information:
 - Connection relationship of bridges.
 - Link status between adjacent bridges interconnected ports.
 - Link status of GOOSE/SV path.

- Distributed IED subscription information among bridges ports.

7.3.2 GOOSE/SV path monitoring

A GOOSE/SV path originates from the root port to which the publisher IED is connected, and ends at the leaf ports to which subscribers are connected. To monitor the integrity of a GOOSE/SV path, a centralized management tool is needed to collect both ingress and egress flow records on each bridge the GOOSE/SV packets passes by, and assemble these pieces of information to the GOOSE/SV path at run time. This then becomes an object to be monitored or analysed. The monitoring approach can take place via SNMP, IEC 61850 or other possible protocol that bridges supported. On each GOOSE/SV path, the following run time information is recommended to be monitored:

- a) Message and route information such as: APPID, multicast address, ingress port, egress port, link status, used to identify the GOOSE/SV path state.
- b) Traffic information such as: ingress statistical data, egress statistical data, used to supervise and analyse the GOOSE/SV path active state.
- c) Quality information such as: bandwidth utilization, packet loss, latency and jitter, used to report the GOOSE/SV path quality state.
- d) Path update event such as: IED connection port change, bridge cascade port alternation, used to indicate physical network topology change.
- e) Physical link information used to present the actual physical link state such as link speed, link state, duplex mode etc.

The information could also be utilized to do the performance analysis to identify "hot" bridges/links that might have a significant impact when going down.

When a substation network encounters unexpected events, warn/trap should be set up to capture such cases and send an alert to substation operator. Some failures are very obvious, such as link going down, part of GOOSE/SV path being damaged, GOOSE/SV path flap to redundant path, traffic rate surged to abnormal high, and occurrence of a large number of CRC errors. There are other inconspicuous but also valuable information which should be paid attention to, such as the cases where multiple IEDs sent GOOSE/SV packet with the same APPID, test bit of some GOOSE/SV packets was set but whole substation running at operation mode, etc.

7.3.3 GOOSE/SV path data modelling

Basic bridge functions have been modelled in Clause 19 of IEC TR 61850-90-4:2020; a bridge model consists of a collection of LNs including LN LPHD, LLN0, LBRI, LCCH, LCMF, LCVF, LBSP, LPLD and LPCP etc.; to support the management of substation networks, RSTP, HSR and PRP devices are also considered. On top of this bridge model, several models are recommended to support presentation and monitoring of substation networks, as shown in Figure 36, and the logical relationship between the LNs is shown in Figure 37.

The AR-bridge model consists of the following LNs besides those which have been defined in IEC TR 61850-90-4:

- a) LN LARB (for "AR-bridge") suggested in Clause B.1, represents the AR-bridge functionality, is instantiated for each AR-bridge.
- b) LN LARP (for "AR-bridge Port") suggested in Clause B.2 represents the properties of a AR-bridge port, is instantiated for each port.
- c) LN LARN (for "AR-bridge Neighbor") suggested in Clause B.3, represents list of AR-bridge(s) connected to this port, is instantiated for each port.
- d) LN LILO (for "IED-Learning Outcome") suggested in Clause B.4, represents the list of IED(s) connected to this port, is instantiated for each port.
- e) LN LGEP (for "GOOSE/SV Egress Path") suggested in Clause B.5 represents each GOOSE/SV egress path, is instantiated for each APPID.

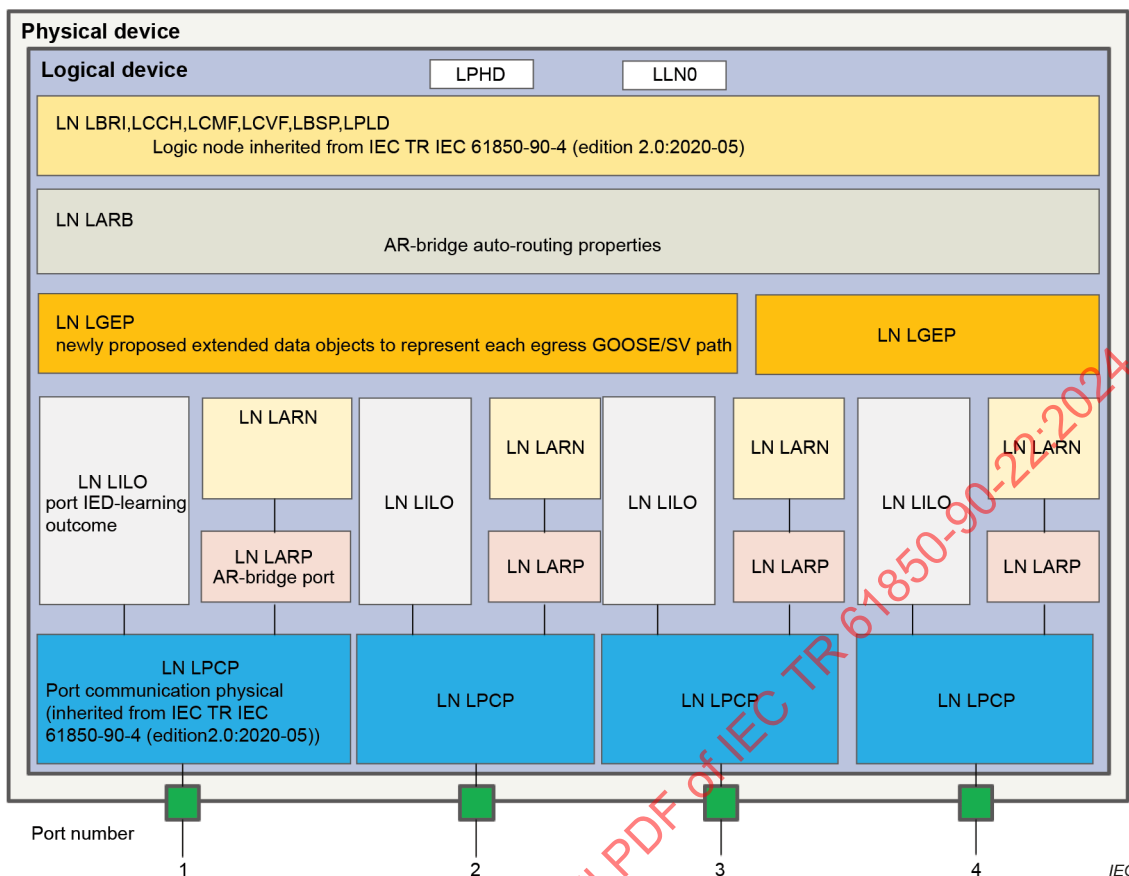


Figure 36 – Multiport AR-bridge model

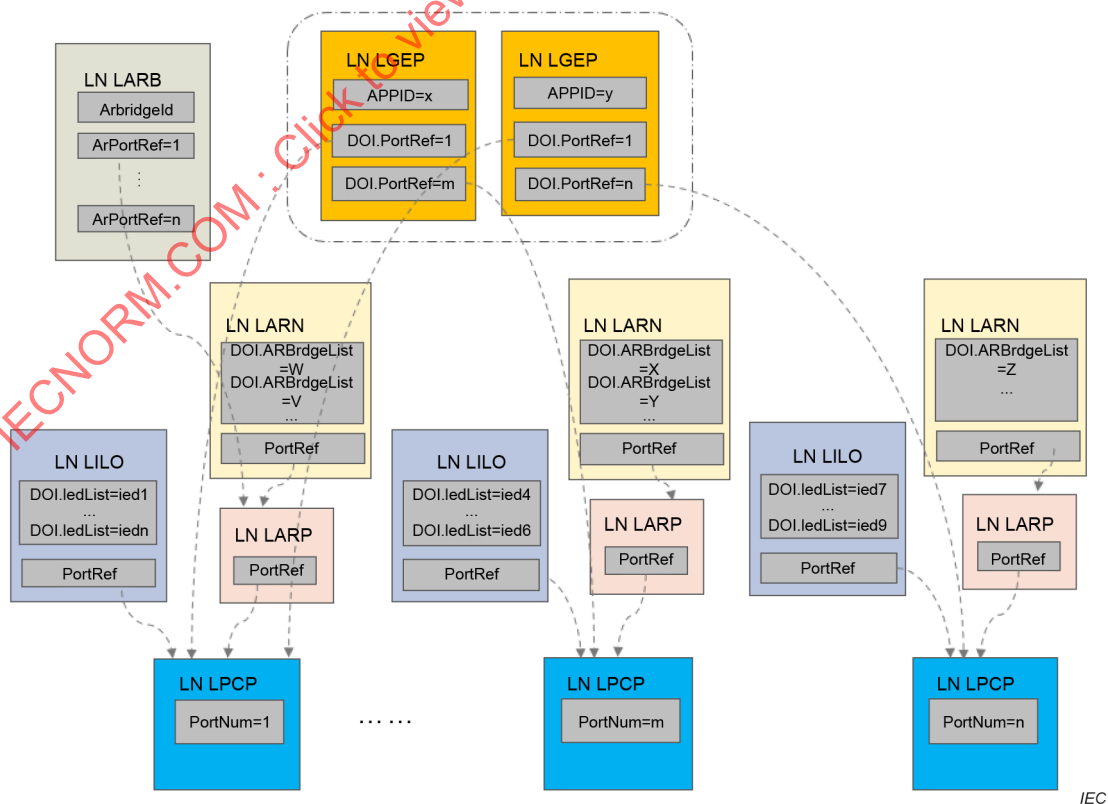


Figure 37 – Logical relationship between the LNs

7.3.4 Example for information presentation and monitoring

The following example is based on unique APPID to identify the GOOSE/SV which may not be the case as APPID could have same value depending on the user specification.

The example of the key information presentation of a GOOSE path and its alarming indication is given based on the following network topology in Figure 38, where the symbol e_n is used to indicate an IED device, and SW_n is used to indicate an AR-bridge. Here Figure 38 is not a complete topology, but only part of IED-bridge connection and the network topology information is given for demonstration only.

Presentation of network connection information can be visualized as the example shows: three AR-bridges are connected in trees. SW_1 is connected to SW_2 and SW_3 respectively, and each AR-bridge has 5 ports connection. SW_1 is connected with IED e_1, e_2, e_3 ; SW_2 is connected with IED e_4, e_5, e_6, e_7 ; and SW_3 is connected with IED e_8, e_9, e_{10}, e_{11} . Each AR-bridge learns GOOSE/SV information (APPID, DMAC, SMAC, EtherType, timestamp, packet length) from IEDs connected to the local port. The key information such as APPID can be displayed in a designed "Port List Window" for each AR-bridge, as the blocks in Figure 38. The leftward arrow in front of the APPID represents the GOOSE/SV message published/sent by the IED, while the rightward arrow represents the message subscribed or supposed to be received by the IED. As shown in Figure 38, the GOOSE path (with APPID 0x0101) indicated by the green arrow, sourced from e_6 to port 3 of SW_2 , aggregated to port 1 of SW_2 , and should end to e_2 (connected to port 3 of SW_1) and e_9 (connected to port 4 of SW_3) respectively.

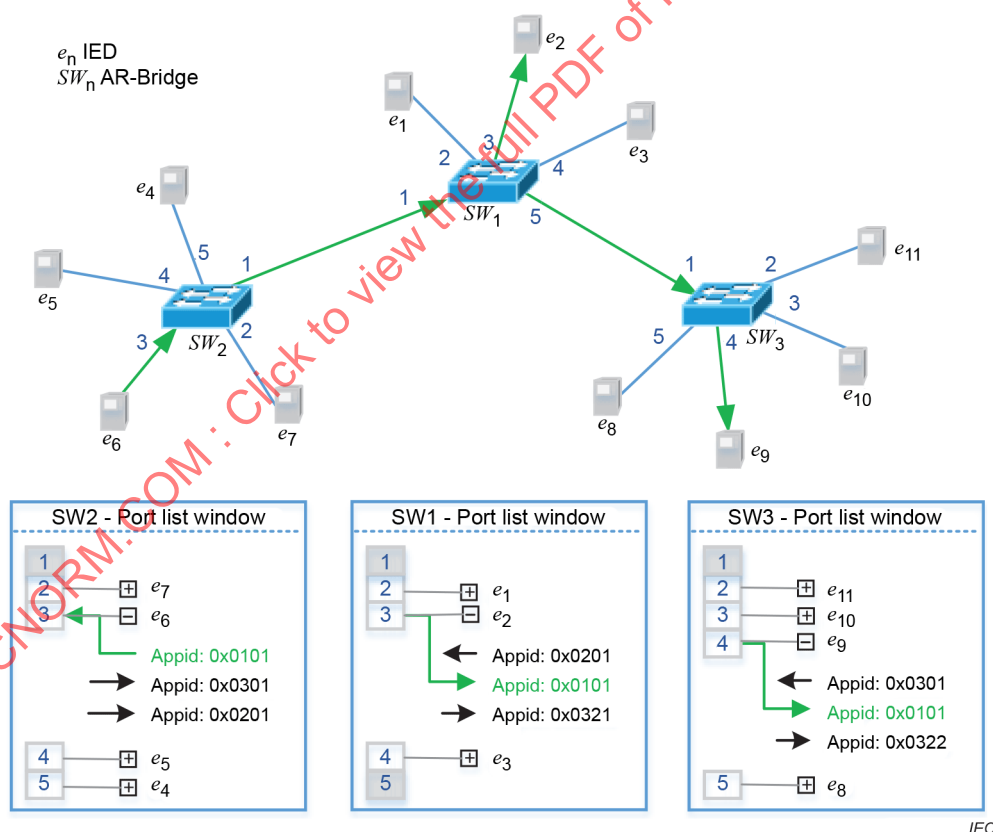


Figure 38 – Example of a GOOSE path presentation and monitoring (normal state)

The physical link status of GOOSE/SV paths that build through network topology discovery can be updated in real time, and abnormalities can be alerted in time, such as physical link disconnection, IED not sending or receiving GOOSE/SV messages. Suppose the physical link fault occurs between port 3 of SW1 and the IED e_2 , then e_2 is disconnected from the network, red dash line and arrow can be used to represent the abnormal state related to e_2 as shown in Figure 39, the GOOSE message e_2 published (with APPID 0x0201) and subscribed to (with APPID 0x0101 and 0x0321) are in alarm status.

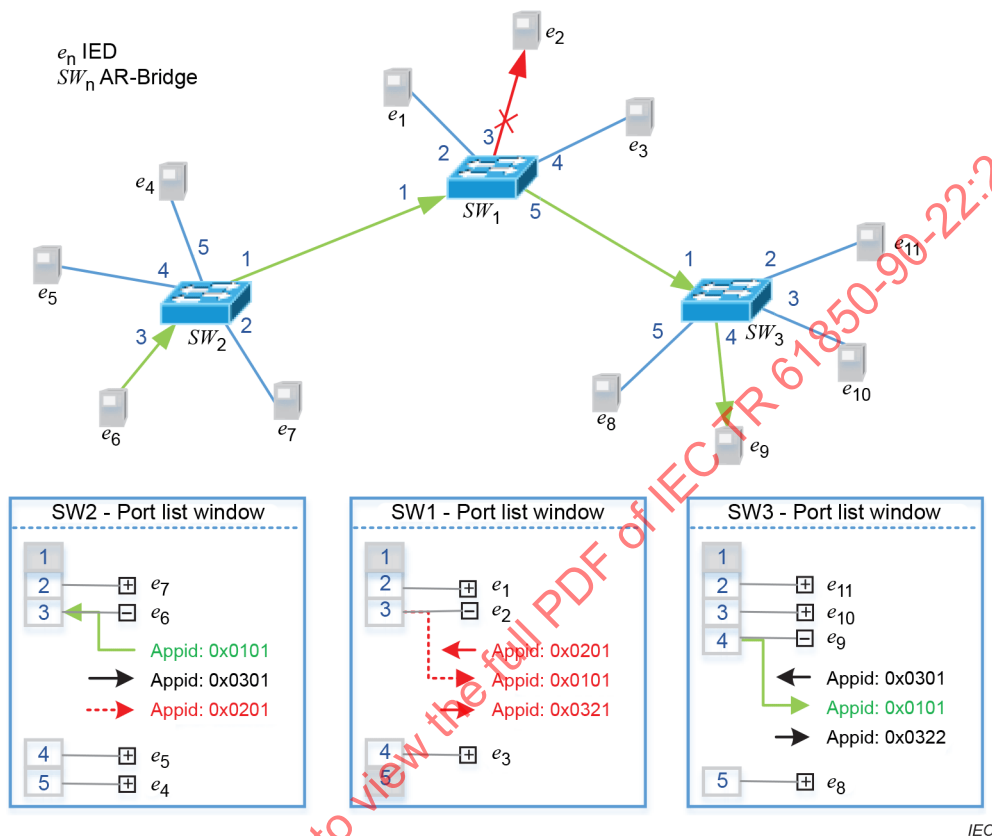


Figure 39 – Example of a GOOSE path presentation and monitoring (abnormal state)

8 GOOSE/SV path traffic control and engineering strategy

8.1 Overview

The purpose of traffic control is to reduce unnecessary traffic in the substation network and limit the traffic that an end device needs to be handled, so as to ensure the overall network real-time performance. Auto-routing mechanism endows AR-bridges with the capability of perceiving the SCD file to build the GOOSE/SV path, so traffic control and engineering strategy based on the GOOSE/SV path can be applied to get better performance, e.g. comparing the GOOSE/SV messages with that defined in the SCD file to filter the substation network traffic, calculating the bandwidth requirement to set an appropriate threshold for each GOOSE/SV path.

8.2 "Substation network static-routing" based approach

As described in 5.2 the Bridge Configurator needs to know what the network topology looks like in order to render the paths of the GOOSE/SV streams between publishers and subscribers as defined in the SCD file. The traffic control is achieved by means of the automated VLAN and multicast MAC address filtering configuration as described in 5.2. In addition, ACLs (Access Control List) can be used in the bridges/switches to filter and control GOOSE/SV traffic. ACLs rules are defined by ACEs (Access Control Entries) that can be configured by the Bridge Configurator.

8.3 "Substation network auto-routing" based approach

8.3.1 GOOSE/SV path traffic control

When the substation network is in the process of commissioning or problems analysing, controlling traffics to be captured, or terminating traffics to reduce unnecessary effecting factors, can efficiently pinpoint the fault location and promote the debugging progress. Several traffic control behaviours are introduced here:

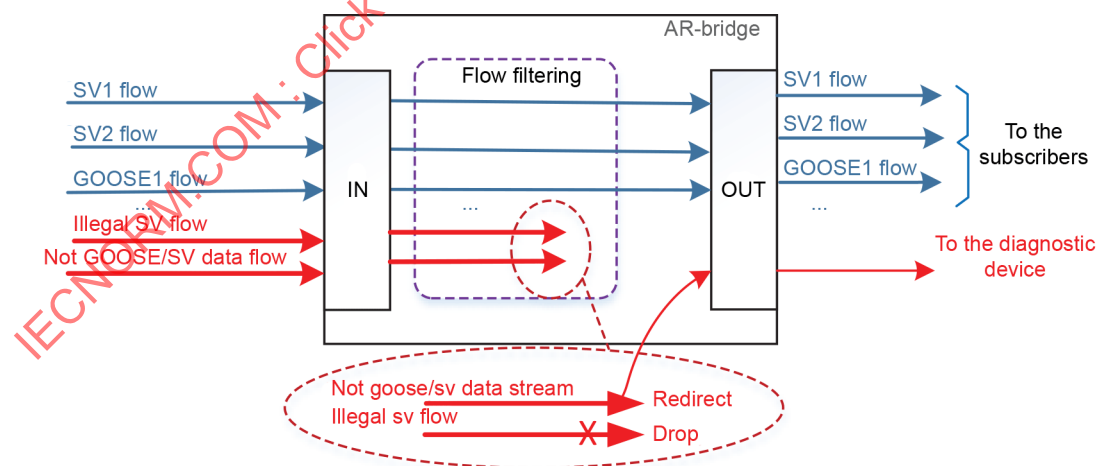
- Detect illegal traffic (the traffic not related with the SCD file), then decline to forward, but can capture, mirror or redirect it to a diagnostic device.
- Identify duplicated traffic (the traffic that issued by a different IED but with the same multicast address and APPID, which may occur if something is wrong with the SCD file or the IED's CID file), report the traffic injection port and the connected IED. Also the traffic can be set to capture, mirror or redirect to a supervision device.
- Forward the specified service traffic to a designated port for analysing purpose if necessary.

8.3.2 Example for GOOSE/SV path traffic control

Based on the SCD file, IED-learning makes AR-bridges have the ability to acquire characteristics of incoming service flows, including the SMAC, DMAC, APPID and other message features. The combination of these features can be used as the basis for data filtering to identify whether the flow entered the port of the AR-bridge has been defined in the SCD file. An example of traffic control on detection of illegal traffic is given, as shown in Figure 40.

One of the red lines means that the SV packet AR-bridge has received is not compliant with the features of the SV message defined in the SCD file, so the AR-bridge would consider them as illegal SV flow and discard directly without forwarding.

For a domain area that focuses on dealing with GOOSE/SV message, the traffic control behaviour for only forwarding a GOOSE/SV message can be set to eliminate other packets. So while IP packets or other non GOOSE/SV data go into the AR-bridge, it can be controlled to discard as well, or redirect to a designated port, which may connect with the diagnostic device according to the trouble shooting requirement, as another red line in the diagram shows.



IEC

Figure 40 – Illustration of GOOSE/SV path traffic control

8.3.3 GOOSE/SV path traffic engineering strategy

Reachable and reliable GOOSE/SV path is the basic requirement for substation network, the following traffic engineering strategy can be utilized to ensure the traffic transmission quality.

- Shortest path first plan to select the most efficiency link for specific GOOSE/SV message when there are multiple paths existed.
- Load balanced to an equivalent path to alleviate traffic stress and avoid data loss if there is a redundant path that can be used.
- Set bandwidth limitation for GOOSE/SV paths across shared physical link to reassure the transmission of high priority traffic.

Port rate limitation is a normal way to suppress the broadcast, multicast or unknown unicast packet, but it is not an efficient way for the substation network when the majority information is carried by multicast of GOOSE and SV messages. Stream-based supervising and managing is available under the support of auto-routing, it is especially helpful when abnormal traffic bursts in the substation network are identified according to the information of SCD file. Statistical information of GOOSE/SV message can be used to set the bandwidth parameter or warning/alarming threshold for each GOOSE/SV path. Due to the parameter set on the logical link layer, it will not be affected by physical topology switching when a GOOSE/SV path changes owing to physical port fault or rearrangement.

8.3.4 Example for GOOSE/SV path traffic engineering strategy

Combined with the substation network topology, the parameters defined in the SCD file (e.g. the number of devices that the IED been subscribed, the sampling rate of the SV message) could be used statistically to calculate the GOOSE/SV path bandwidth through a certain algorithm. For example, according to the network topology and the GOOSE/SV traffic forwarding direction in Figure 41, the AR-bridges will calculate the traffic load and give out estimations of bandwidth range for the GOOSE/SV paths, as shown in Table 14.

Table 14 – Traffic estimation

GOOSE/SV path	Minimum load estimation	Maximum load estimation
SV1 flow	0,5 Mbit/s	2 Mbit/s
SV2 flow	0,5 Mbit/s	2,5 Mbit/s
SV3 flow	1 Mbit/s	5 Mbit/s
GOOSE4 flow	0,1 Mbit/s	1 Mbit/s

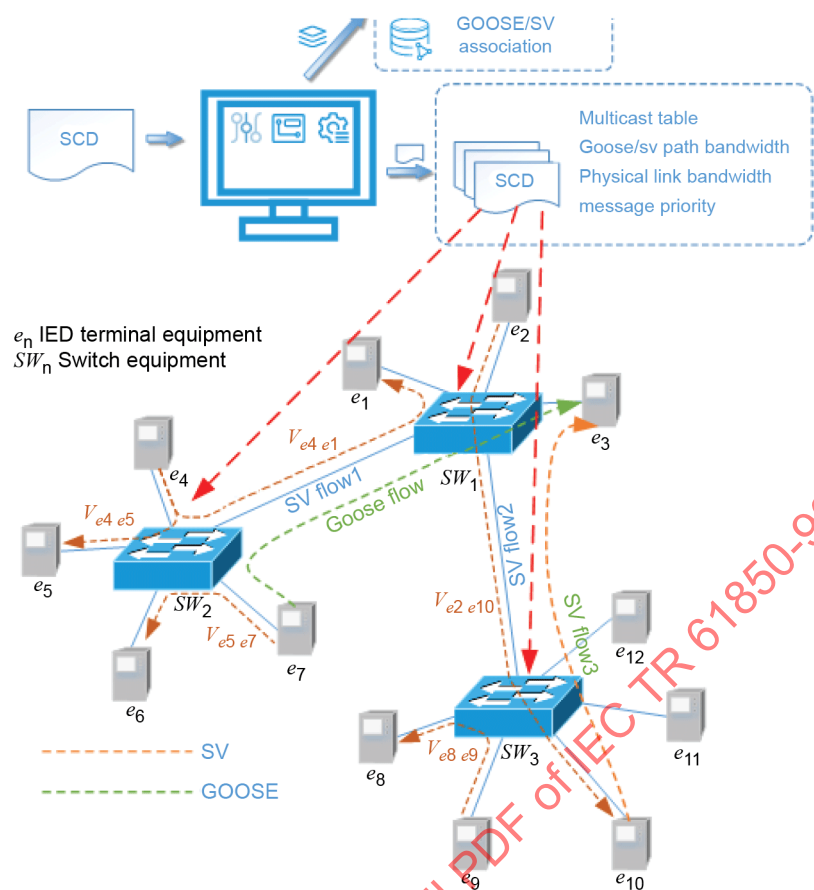


Figure 41 – Illustration of GOOSE/SV path engineering

AR-bridges then can use the maximum bandwidth requirement as a threshold (e.g. 2 Mbit/s) for planning the outbound traffic to avoid abnormal GOOSE/SV traffic squeezing other normal traffic, as shown in Figure 42. When abnormal SV1 flow (red line in the diagram, 20 Mbit/s) is forwarded by the AR-bridge, packets over the threshold will be discarded to make sure the outbound traffic load of this flow is limited to 2 Mbit/s.

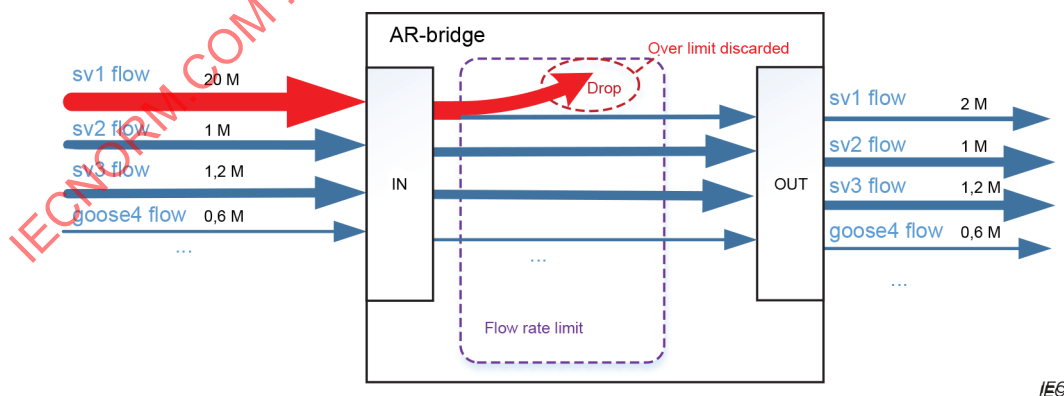


Figure 42 – Example of GOOSE/SV path traffic engineering

9 Handling of simulated GOOSE/SV messages

9.1 General

The identity of simulated GOOSE/SV messages is controlled by the simulation parameter (Boolean type) defined in IEC 61850-7-2 for tests. During the substation network engineering phase, simulated GOOSE/SV messages can be utilized to verify the validity of physical links and logical links, including connected IEDs operation. Especially under fault occurring conditions, simulated GOOSE/SV can facilitate the troubleshooting process and help to quickly locate the fault position. Based on the IED-learning ability, the AR-bridge can be set to tackle the simulated packets or not if normal packets and simulated packets coexist in the network.

Normally simulated GOOSE/SV messages are generated by IEDs or test instruments. If the subscriber IEDs have the ability to handle the "s" bit, when simulated GOOSE/SV packets and normal packets were forwarded in the substation network simultaneously, the simulated GOOSE/SV message will not interfere with the operation of the IED subscribers. But if the IEDs cannot identify the simulated bit, the coexistence of simulated and running GOOSE/SV packets may cause unpredictable problems.

9.2 "Substation network static-routing" based approach

The Bridge Configurator needs to know where test devices are connected to bridges/switches in the topology and what GOOSE/SV traffic will be injected. Since this information is not contained in the SCD file the corresponding data must be provided to the Bridge Configurator in a different way. Once this information is available the automated determination of the stream paths through the network and configuration of VLANs and Multicast MAC filtering works as described in 5.2.

9.3 "Substation network auto-routing" based approach

9.3.1 Dividing different operation plane with "s" bit

Detection of the "s" bit allows the AR-bridge to discriminate the simulated GOOSE/SV packets and support an IED and its duplication copy both to work together without conflict. By creating two different operating planes within a physical AR-bridge to fulfil both maintaining and running requirement, the AR-bridge logically splits itself into two independent parts, the maintaining section which is called the "Maintenance Plane", handles the GOOSE/SV message with the "s" bit being set to "TRUE", and the other section, the "Working Plane", keeps in normal operating state.

The Maintenance Plane and Working Plane share the physical resources of the same AR-bridge, such as CPU, memory, ports, etc., but each has its own independent forwarding resources, including VLAN table, MAC table, and forwarding table. In short, packet forwarding within the Maintenance Plane and packet forwarding within the Working Plane can be understood as the identical packets being forwarded by two independent bridges with different configurations without interfering with each other at the forwarding level.

With the IEDs that support the GOOSE/SV messages with "s" bit, an AR-bridge creates the Maintenance Plane and generates the related forwarding table by auto-routing or static-routing based on SCD file. As for the IEDs that do not support the "s" bit, the creation of the Maintenance Plane needs to be manually operated according to the actual maintenance requirement.

Under the situation that simulated GOOSE/SV messages are cleared out of the substation network after maintaining or testing process is finished, problems may happen when the actual GOOSE/SV packet gets on-line if there is no special maintenance plane created. The AR-bridge can also be set to report the situation and present alarming information to facilitate the troubleshooting.

9.3.2 Example for handling the simulated GOOSE/SV message

A simple example is given to demonstrate the coexistence of simulated and actual GOOSE/SV messages during the substation network maintenance. A typical topology and subscription relationship for three bays with merging unit is shown in Figure 43, also with the protection devices and control devices respectively. The devices in the two bays are connected to AR-bridge1 named SW1. The devices in the busbar bay are connected to AR-bridge2 named SW2, and SW1 is connected with SW2.

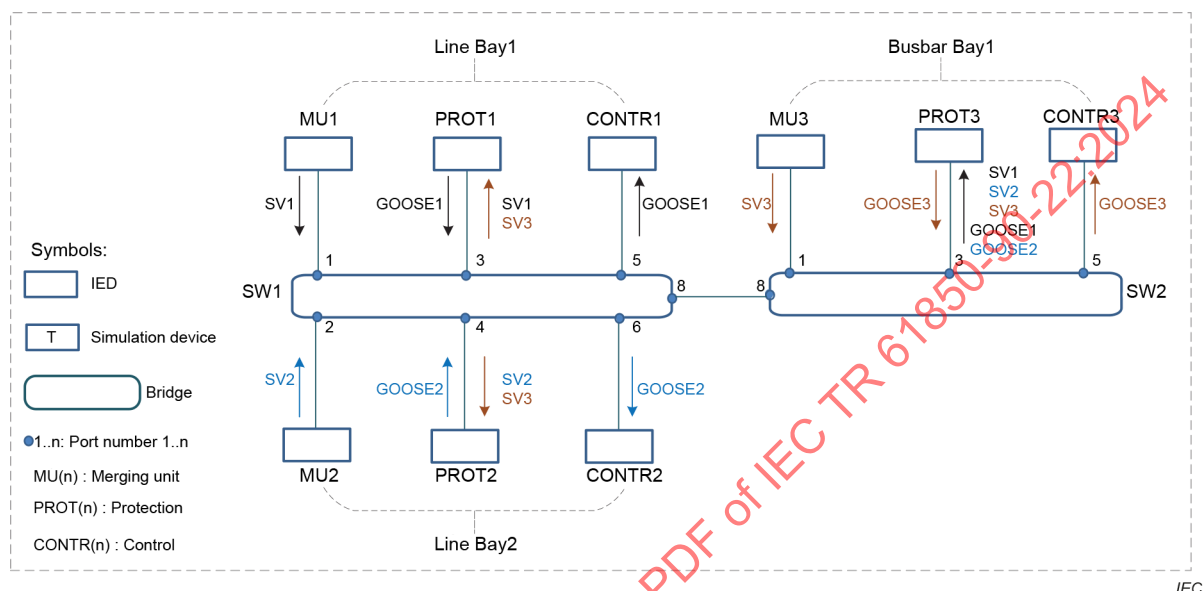


Figure 43 – Topology and subscription relationship for three bays

Normally data flow of process bus inside bay is similar to the following mode in Table 15, and the cross bays data flow is shown in Table 16.

Table 15 – Data flow inside a bay

Inside Bay		
[Merging Unit]	-----SV-----→	[Protection Device]
[Protection Device]	-----GOOSE-----→	[Control Device]

Table 16 – Data flow cross bays

Line Bay		Busbar Bay
[Merging Unit]	-----SV-----→	[Protection Device]
[Protection Device]	-----GOOSE-----→	
[Protection Device]	←-----SV-----	[Merging Unit]

To better represent the attributes of independency of IEDs, the APPID is recommended to be uniquely distributed in the SCD file. The example GOOSE/SV association in the SCD file is given below:

- PROT1 subscribes SV1 and SV3 message of MU1 and MU3 respectively.
- CONTR1 subscribes GOOSE1 messages of PROT1.
- PROT2 subscribes SV2 and SV3 message of MU2 and MU3 respectively.

- CONTR2 subscribes GOOSE2 messages of PROT2.
- PROT3 subscribes SV1, SV2, and SV3 message of MU1, MU2, and MU3 respectively.
- CONTR3 subscribes GOOSE3 messages of PROT3.

The subscription relationship above extracted from the SCD file is illustrated in Table 17.

Table 17 – Extracted subscription information of the example

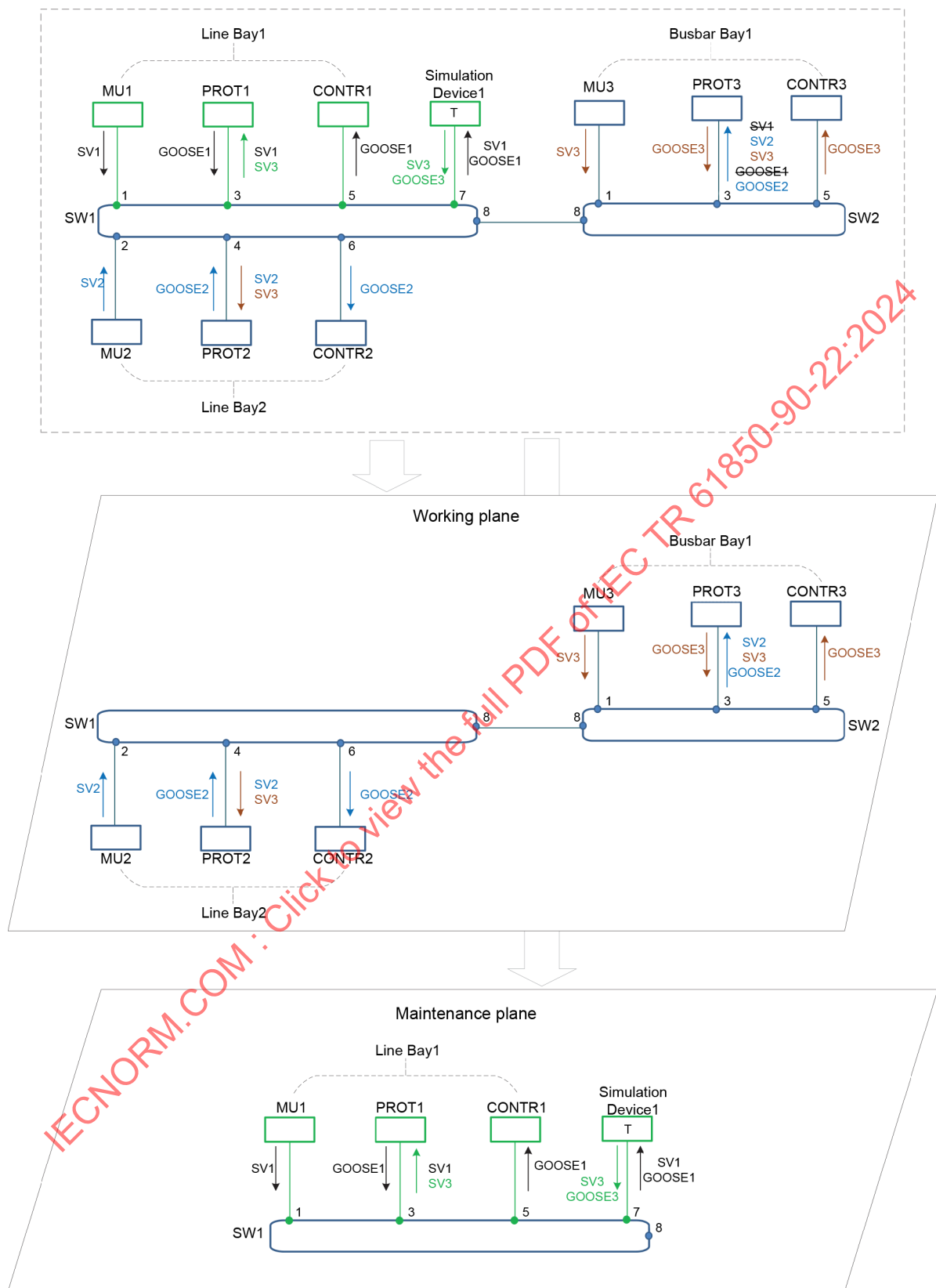
Publisher					Subscriber
iedName	Multicast Address	APPID	VLAN	SVID/GOID	/
MU1	01-0C-CD-04-00-01	0x4001	123	MU1/LLN0.smbcb0	PROT1, PROT3
PROT1	01-0C-CD-01-00-01	0x1001	123	PROT1/LLN0\$GO\$GoCB	CONTR1, PROT3
MU2	01-0C-CD-04-00-02	0x4002	123	MU2/LLN0.smbcb0	PROT2, PROT3
PROT2	01-0C-CD-01-00-02	0x1002	123	PROT2/LLN0\$GO\$GoCB	CONTR2, PROT3
MU3	01-0C-CD-04-00-03	0x4003	123	MU3/LLN0.smbcb0	PROT1, PROT2, PROT3
PROT3	01-0C-CD-01-00-03	0x1003	123	PROT3/LLN0\$GO\$GoCB	CONTR3

As mentioned above, the AR-bridge has the ability to be divided into two independent planes according to the simulation "s" bit to support on-line maintaining requirements. Under the circumstance that line bay1 has the requirement to be maintained, the involved devices in line bay1 are isolated from the operating environment of the substation. As shown in Figure 44, AR-bridge SW1 is separated logically into two independent sections, one part is to carry IEDs of MU1, PROT1 and CONTR1 of line bay1 that requires maintenance, which is in the maintenance plane using maintenance forwarding table, and the other part of the SW1 that carries the line bay2 remains in normal operating status, which is in the working plane using the original forwarding table without change.

By default, all ports of the AR-bridges in the substation network operate in the Working Plane as indicated in Figure 44. In order to carry out maintenance test in line bay1, port 1, 3, 5 of SW1 that connected the IEDs of MU1, PROT1 and CONTR1 with test mode would be allocated to the maintenance plane, and port 7 which connected to the simulation device1 that emulating MU3 and PROT3, would also be allocated to the Maintenance Plane. For the port 8 that interconnects AR-bridge SW1 and SW2 can stay at both Maintenance Plane and Working Plane according to the requirement of maintenance. The remaining ports of SW1 and SW2 are still running in the working plane. After the Maintenance Plane is created and activated, GOOSE/SV messages sent by devices of the line bay1 can only be forwarded within the port group that belongs to the Maintenance Plane according to its own forwarding table, as shown in Table 18.

Table 18 – Example forwarding table of maintenance plane (SW1)

Multicast Address	VLAN	"s" bit	Ingress port	Egress port
01-0C-CD-04-00-01	123	TRUE	1	3,7
01-0C-CD-04-00-03	123	TRUE	7	3
01-0C-CD-01-00-01	123	TRUE	3	5,7
01-0C-CD-01-00-03	123	TRUE	7	/



IEC

Figure 44 – Coexistence of simulation and actual signals

GOOSE/SV messages sent by devices of the line bay2 and the busbar bay1 can only be forwarded in the port group that belongs to the working plane. As a result, the protection device PROT3 of the busbar bay1 connected to the port of the Working Plane will not get the SV1 and GOOSE1 that have been divided into the Maintenance Plane; the following forwarding table of the Working Plane is shown in Table 19 and Table 20.

Table 19 – Example forwarding table of working plane (SW1)

Multicast Address	VLAN	"s" bit	Ingress port	Egress port
01-0C-CD-04-00-02	123	FALSE	2	4,8
01-0C-CD-04-00-03	123	FALSE	8	4
01-0C-CD-01-00-02	123	FALSE	4	6,8

Table 20 – Example forwarding table of working plane (SW2)

Multicast Address	VLAN	"s" bit	Ingress port	egress port
01-0C-CD-04-00-02	123	FALSE	8	3
01-0C-CD-04-00-03	123	FALSE	1	3,8
01-0C-CD-01-00-02	123	FALSE	8	3
01-0C-CD-01-00-03	123	FALSE	3	5

In order to simulate the merging unit MU3 and the protection device PROT3 of the busbar bay1 in the Maintenance Plane, the Simulation Device1 publishes simulated SV3 and GOOSE3 to the port 7 of the SW1. According to the subscription relationship in Table 18, the protection device PROT3 receives the multicast simulation signal SV3 sent by Simulation Device1 instead of the actual signal SV3 sent by MU3. GOOSE3 is discarded since the control device CONTR3 is out of the maintenance plane. Meanwhile, the SW1 recognizes the Simulation Device1 connected to port 7 as MU3 and PROT3 through the IED learning as described in 6.2.2. Therefore, SV1 and GOOSE1 can be forwarded to Simulation Device1.

10 Guidance on auto-routing network usage

10.1 General

Auto-routing can provide plug-and-play and online-verification to facilitate the construction and operation of a substation network, getting rid of the predesigning VLAN and IED-related port cable/fibre connecting checking step. In addition, with aid of auto-routing, the substation network running state supervision, fault diagnostic and IEDs access controlling could be provided to facilitate the substation daily maintenance. The way that auto-routing works in a substation network to facilitate the engineering, operating and maintaining process is demonstrated in the following examples.

10.2 Implementation of substation network auto-routing

After substation modelling is finished and the related SCD file is generated, the bridges and IEDs which have been prepared shall be assembled to construct the substation secondary system. Normally three things are considered and performed:

- What kind of network topology should be adopted to connect the IEDs?
- How many VLANs should be set to control the network traffic and the port VLAN ID setting design according to SCD file?
- Connect the IED to its related pre-distributed bridge port to implement physical networking.

Under the support of auto-routing, the last two sophisticated steps above can be simplified profoundly, and the IEDs can be connected to the substation network without position limitation.

A simple example is given here to demonstrate the implementation of auto-routing applied in the substation network. Before connecting the substation network and IEDs, the subscription information should be abstracted from the SCD file to compose of the BCD file and then uploaded to the bridges. In the following example, three sets of AR-bridges connected in tree compose the substation network, 11 different types of IEDs need to be connected to the substation network to complete the substation function ($e_1 \sim e_{11}$, e_{12} is used for the next step as a new IED to be added). The original substation network state is shown in Figure 45.

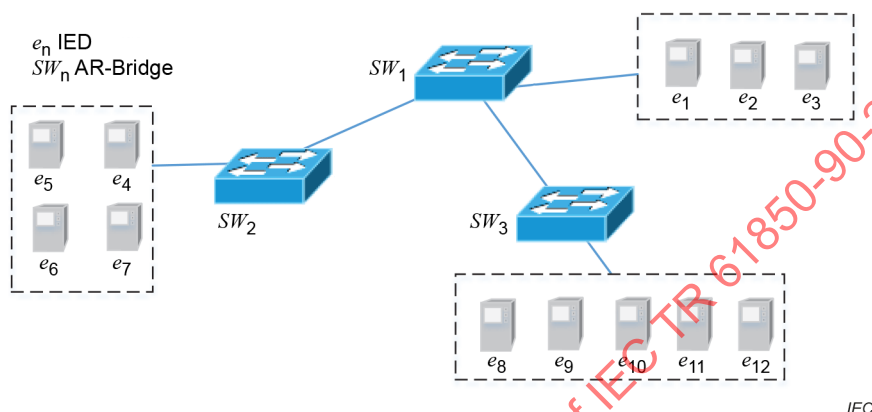


Figure 45 – Bridges and IEDs to be connected

During the engineering phase, when the bridge network has been positioned as shown in Figure 45, with the support of auto-routing mechanism provided by the AR-Bridges, the IEDs can be connected to the bridges nearby without considering which IED is connected to which bridge. IED e_1 can be connected to port 1 of SW1, and can also be connected to another nearby AR-bridge's port, for example, port 1 of SW2; there is no essential discrimination for the forwarding path calculation of auto-routing.

Suppose the final physical substation network is shown in Figure 46 after all IEDs were connected. When the AR-Bridges and IEDs are all put into work, network topology would be discovered and plotted, the IED-learning procedure would be triggered when GOOSE/SV messages injected into the network. A flow chart of auto-routing implementation is shown in Figure 47.

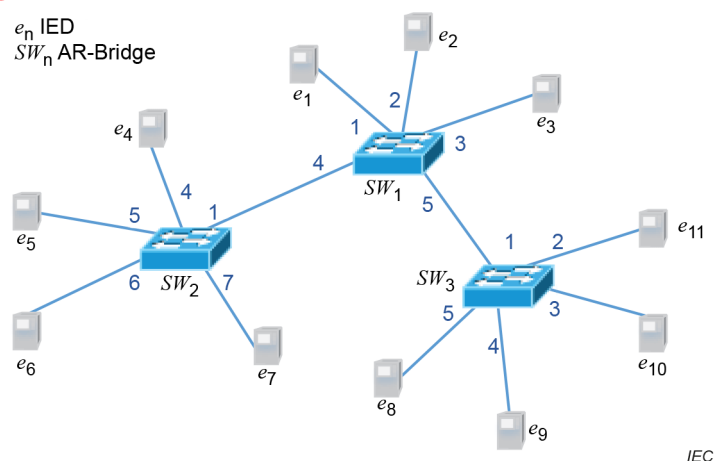


Figure 46 – Final physical substation network

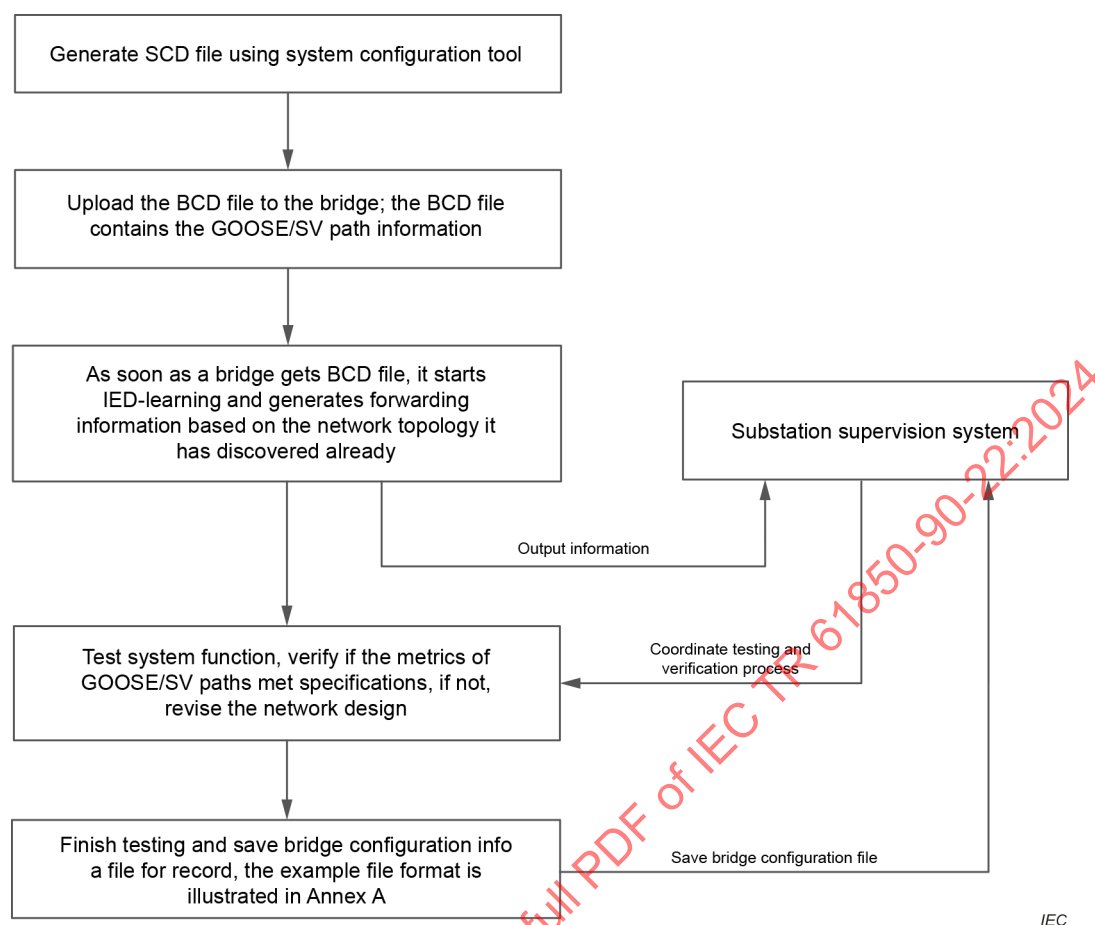


Figure 47 – Flow chart of auto-routing implementation

GOOSE/SV associations abstracted from the SCD file are listed in Table 21, combining with the outcome of discovered network topology and IED-learning, see Table 22, and the GOOSE/SV flow that each AR-bridge detected, see Table 23, end to end GOOSE/SV paths would be calculated, and the forwarding table of each AR-bridge is generated to carry the GOOSE/SV paths.

Table 21 – GOOSE/SV associations abstracted from SCD file

iedName	Publisher				Subscriber
	Multicast Address	APPID	VLAN ID	SVID/GOID	iedName
e1	01-0C-CD-01-00-01	0X1001	123	e1/LLN0\$GO\$GoCB	e4, e8
e2	01-0C-CD-01-00-02	0X1002	123	e2/LLN0\$GO\$GoCB	e5, e9
e3	01-0C-CD-01-00-03	0X1003	123	e3/LLN0\$GO\$GoCB	e6, e10
e4	01-0C-CD-04-00-04	0X4004	123	e4/LLN0.smbcb0	e2, e8
e5	01-0C-CD-04-00-05	0X4005	123	e5/LLN0.smbcb0	e1
e6	01-0C-CD-04-00-06	0X4006	123	e6/LLN0.smbcb0	e1
e7	01-0C-CD-04-00-07	0X4007	123	e7/LLN0.smbcb0	e2
e8	01-0C-CD-04-00-08	0X4008	123	e8/LLN0.smbcb0	e2,e7,e11
e9	01-0C-CD-04-00-09	0X4009	123	e9/LLN0.smbcb0	e10
e10	01-0C-CD-04-00-10	0X4010	123	e10/LLN0.smbcb0	e3
e11	01-0C-CD-04-00-11	0X4011	123	e11/LLN0.smbcb0	/

Table 22 – Topology discovered and IED-learning result of Figure 44

AR-Bridge	Port ID	Connected device	Port type
SW1	1	e1	edge
	2	e2	edge
	3	e3	edge
	4	SW2	inter-bridge
	5	SW3	inter-bridge
SW2	1	SW1	inter-bridge
	4	e4	Edge
	5	e5	Edge
	6	e6	Edge
	7	e7	Edge
SW3	1	SW1	inter-bridge
	2	e11	Edge
	3	e10	Edge
	4	e9	edge
	5	e8	edge

In Table 22, an edge port means that an IED is connected, that an inter-bridge port means the port is used to connect with another bridge. The result information of IED-learning (i.e. correspondence between bridge physical ports and connected IEDs) will be propagated over inter-bridge ports by taking the way of exchanging link state database.

Table 23 – Generated GOOSE/SV flow table

Entry		Keys				Values			
		SMAC (48bit)	DMAC (48bit)	APPID (16bit)	TYPE (1 bit)	VALID (1 bit)	SPORT (6bit)	TIMESTAMP (64bit)	LENGTH (12bit)
SW1	0	00-01-00-00-00-01	01-0C-CD-01-00-01	1001	1	1	1	158763241	384
	1	00-02-00-00-00-02	01-0C-CD-01-00-02	1002	1	1	2	158769385	384
	2	00-03-00-00-00-03	01-0C-CD-01-00-03	1003	1	1	3	158772479	384
SW2	0	00-04-00-00-00-04	01-0C-CD-04-00-04	4004	0	1	4	158753277	1168
	1	00-05-00-00-00-05	01-0C-CD-04-00-05	4005	0	1	5	158759253	1168
	2	00-06-00-00-00-06	01-0C-CD-04-00-06	4006	0	1	6	158771376	176
	3	00-07-00-00-00-07	01-0C-CD-04-00-07	4007	0	1	7	158764940	176
SW3	0	00-08-00-00-00-08	01-0C-CD-04-00-08	4008	0	1	5	158763713	1168
	1	00-09-00-00-00-09	01-0C-CD-04-00-09	4009	0	1	4	158768484	1168
	2	00-10-00-00-00-10	01-0C-CD-04-00-10	4010	0	1	3	158774793	176
	3	00-11-00-00-00-11	01-0C-CD-04-00-11	4011	0	1	2	158763503	176

When an AR-bridge receives GOOSE/SV packets, it parses the packets and builds the ingress flow table as shown in Table 23.

When the subscriber IED and the publisher IED are connected to the same bridge, the bridge can build the forwarding table by itself. However, when the subscriber IED and the publisher IED are not connected to the same bridge, a forwarding table will be built based on the information of Table 22 and Table 23 using the shortest path algorithm to let the packet across the bridges arrive its destination. The example forwarding table is shown in Table 24.

Table 24 – Example forwarding table of AR-bridge SW1

Entry	Destination Multicast Address	APPID	VLAN	Priority	Ingress port	Egress port
SW1	0	01-0C-CD-01-00-01	0X1001	123	4	1
	1	01-0C-CD-01-00-02	0X1002	123	4	2
	2	01-0C-CD-01-00-03	0X1003	123	4	3
	3	01-0C-CD-04-00-04	0X4004	123	7	4
	4	01-0C-CD-04-00-05	0X4005	123	7	4
	5	01-0C-CD-04-00-06	0X4006	123	7	6
	6	01-0C-CD-04-00-07	0X4007	123	7	5
	7	01-0C-CD-04-00-08	0X4008	123	7	5
	8	01-0C-CD-04-00-10	0X4010	123	7	5

In a similar manner, the forwarding table will be built by bridge SW2 and SW3.

10.3 Auto-routing usage case

10.3.1 IED position change or adding a new IED

Based on the above substation network topology, an IED position move and addition is demonstrated as shown in Figure 48.

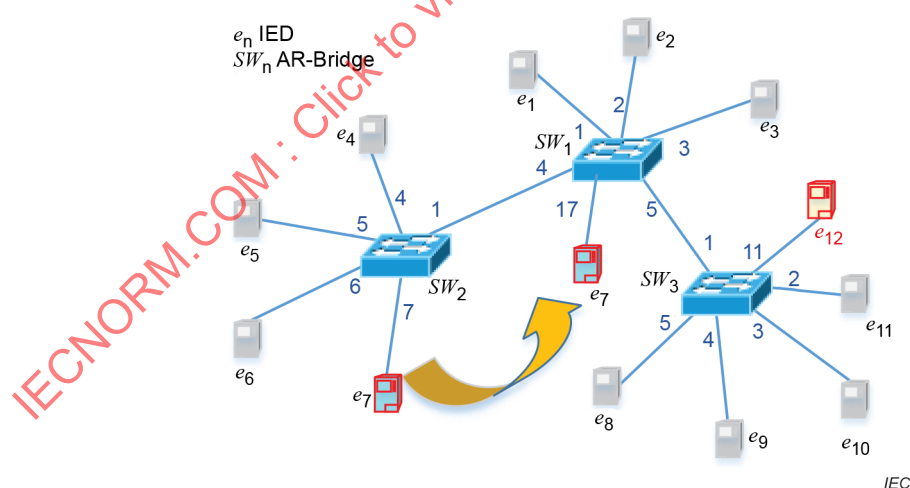


Figure 48 – Demonstration of IED move and addition

a) Move IED e7

IED movement is very simple under auto-routing. Suppose only IED e7 is about to be moved from bridge SW2 to SW1 while no other changes, considering that the e7 here is not a silent IED, so just unplug cable of IED e7 from the SW2, then plug it in any available port on SW1, for example port 17, the bridge SW1 will know that e7 is connected, via IED-learning, and then update its configuration of GOOSE/SV path. The steps are illustrated in Figure 49.

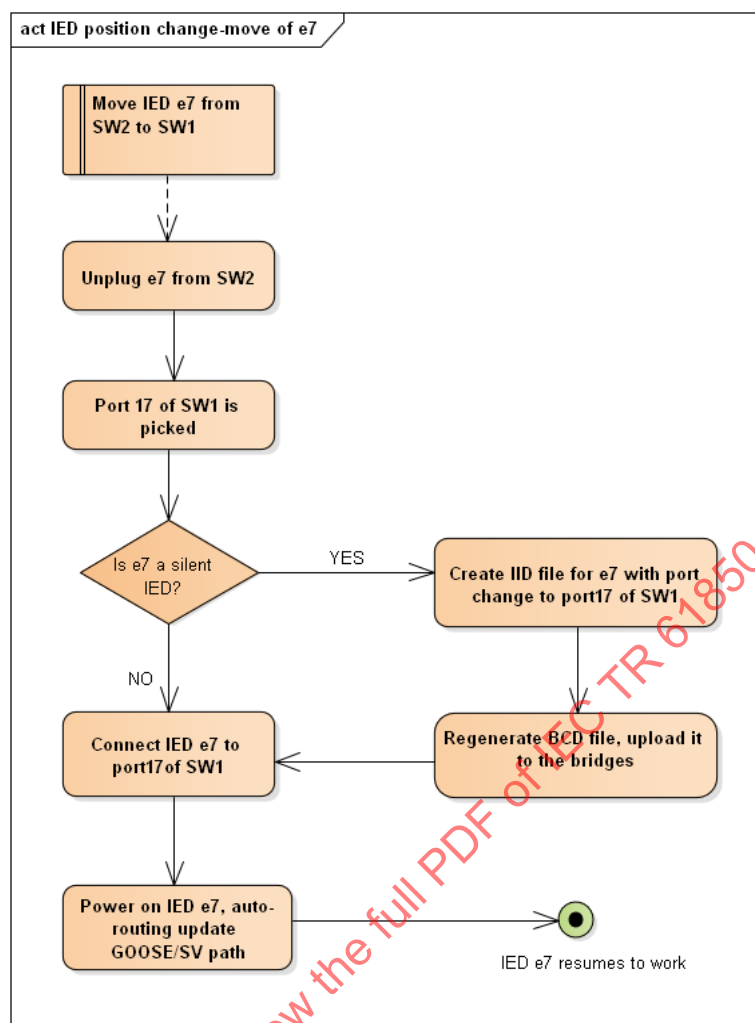


Figure 49 – IED move action

When IED e7 is disconnected from port 7 of SW2, the link down event triggers the IED-learning aging mechanism, it informs auto-routing software on SW2 that e7 is no longer connected to this bridge, according to Table 25, it then stops forwarding SV packet with APPID 0x4008 to its port 7. Since IED e7 is the only subscriber to this SV packet on SW2, auto-routing software on SW2 will further notify other bridges in network that this SV packet is not needed any more on SW2, therefore, SW2 updates its forwarding table for this SV packet to exclude port 7, and SW1 updates its forwarding table to exclude port 4 for this SV packet. Because e2 on SW1 still needs this SV packet, the forwarding table of SW3 will remain unchanged.

Table 25 – GOOSE/SV associations related with IED e7

Publisher					Subscriber
iedName(Source Address)	Multicast Address	APPID	VLAN ID	SVID/GOID	iedName
e7(00-07-00-00-00-07)	01-0C-CD-04-00-07	0X4007	123	e7/LLN0.smbcb0	e2
e8(00-08-00-00-00-08)	01-0C-CD-04-00-08	0X4008	123	e8/LLN0.smbcb0	e2, e7, e11

Meanwhile, for the SV path that sourced on IED e7 starts to timeout on SW2 and SW1, its subscriber e2 will no longer receive this SV packet anymore, then SW1, SW2, e2 will all report this SV path down event to management system.

When IED e7 is connected to port 17 of bridge SW1, IED-learning process on SW1 will detect that IED e7 is on-line, it then informs auto-routing software on SW1 that e7 is now connected on port 17, then later will add port 2 on SV 0x4007's forwarding entry, so SV path 0x4007 will reach e2 on SW1 again. At meanwhile, auto-routing software on SW1 will also update forwarding table for SV 0x4008 to include port 17 to restore SV path to reach e7.

In general, due to no change of SCD file, nothing extra except the safely move action needs to be considered under the circumstance that an IED (excluding silent IED) position changes operation.

b) Adding new IED e12

For adding a new IED case, suppose IED e12 is about to connect to bridge SW3 for some reason, due to the role of this new IED, three conditions are considered respectively, as shown in Figure 50.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-22:2024

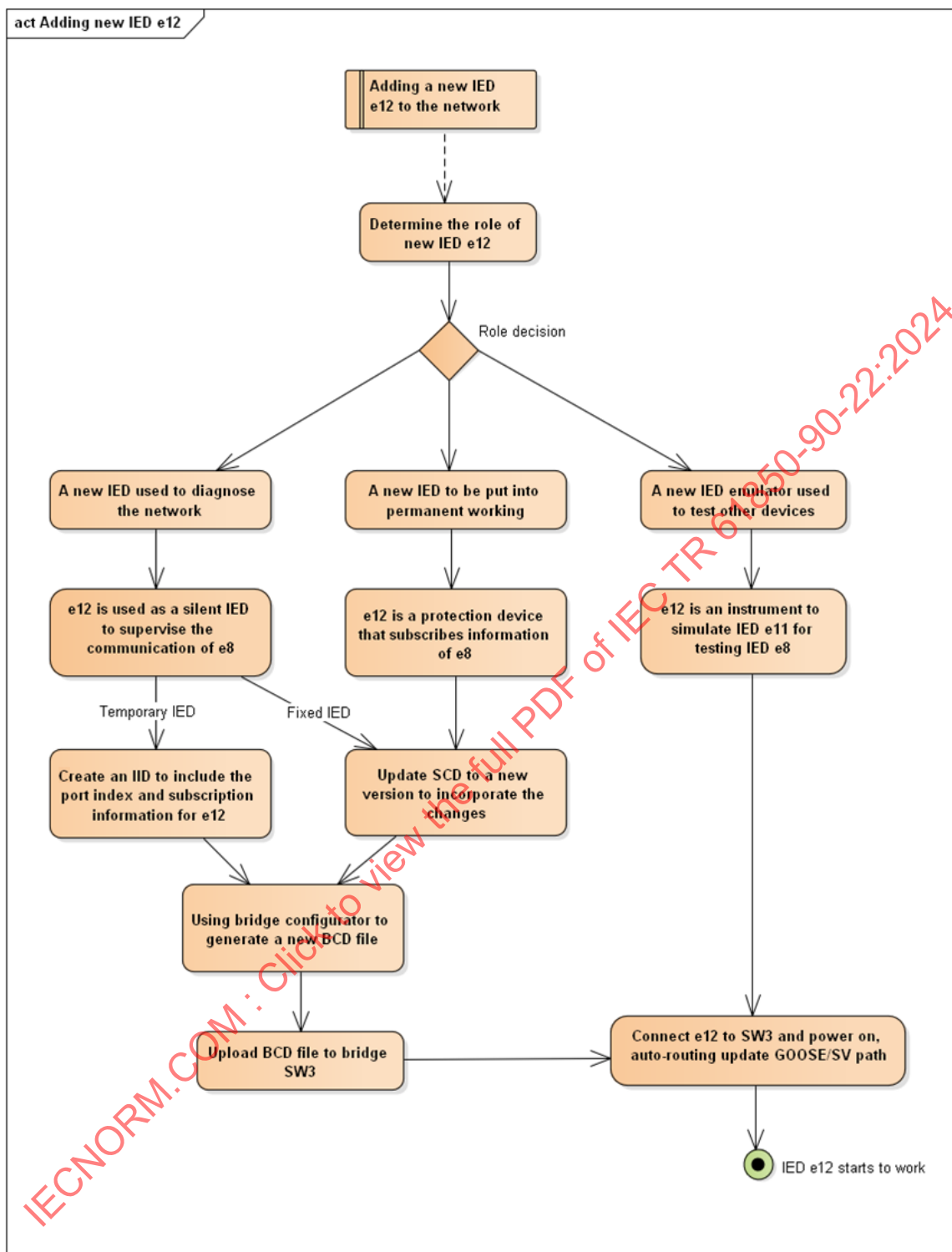


Figure 50 – Add new IED action

- 1) If e12 is a silent IED to be used as a diagnostic device to supervise other IED's data exchanging conditions, for example, the actions of IED e8, then e12 should be added to GOOSE/SV path that e8 publishes and subscribes in SCD file if it will be kept in the network afterwards, or using the IID file to do this work instead if the e12 will only be used temporarily.

- 2) If e12 is a protection device for permanent working purpose, and it subscribes the messages of e8, also delivers GOOSE message with multicast address of 01-CD-0C-01-00-12 to e8. The IED model of e12 and its subscription information should be added into the SCD file and archived to an updated version. Because the new IED e12 only related to e8 within SW3, only SW3 needs the new BCD file to regenerate bridge configuration to update the GOOSE/SV path for carrying the related message that e12 requires.
- 3) If e12 is an IED emulator, for example, emulating e11 to test if other IEDs can receive the right GOOSE/SV messages that e11 published. Meanwhile, it can also verify GOOSE/SV messages that e11 subscribed to. In this case, the SCD file will not involve in change, so as the bridges configuration.

One thing which needs to be remembered is that if IED e12 is temporarily connected for diagnosing, the SCD file and bridge configuration file of SW3 during the debugging phase is just a temporary version and shall be rolled back to the original version after the job is done.

10.3.2 Adding a new bay

Auto-routing is especially useful when a substation network needs to be expanded, for example, add a new bay, the relative new bridges and IEDs needs to be added respectively. Based on the above example, suppose a new bridge SW4 and IED e13, e14 and e15 are about to be added into the substation network, as shown in Figure 51, the auto-routing action flow is illustrated in Figure 52.

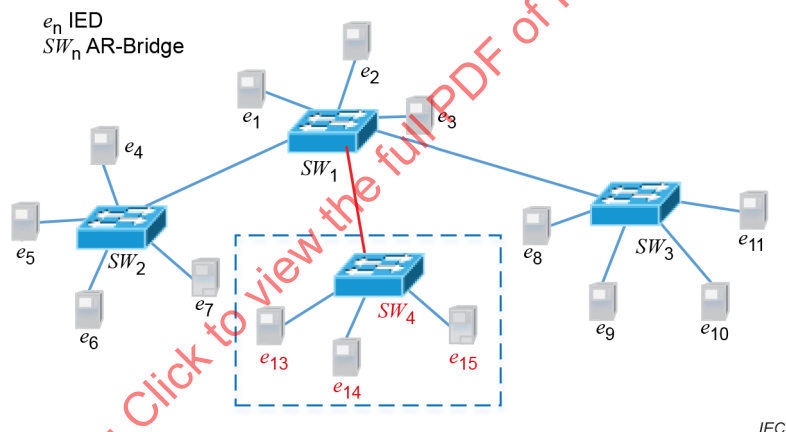


Figure 51 – Demonstration of adding a new bay

Under the substation network topology update circumstance, the SCD file version needs to be updated to accommodate the increased devices and their GOOSE/SV associations.

In general, the process of adding new bridges and IEDs is quite simply handled with the support of auto-routing, the key thing is to make sure of the integrity and correctness of the SCD file update.