IEC TR 61850-90-13

Edition 1.0 2021-02

TECHNICAL REPORT

colour inside

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

Communication networks and systems for power utility automation – Part 90-13: Deterministic networking technologies

IEC TR 61850-90-13:2021-02(en)

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2021 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 Central Office
3, rue de Varembé
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 It also gives information on projects, replaced and withdrawn publications.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 online collection - oc.iec.ch
Discover our powerful search engine and read freely all the publications previews. 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 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

IEC TR 61850-90-13

Edition 1.0 2021-02

TECHNICAL REPORT

colour inside

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

Communication networks and systems for power utility automation – Part 90-13: Deterministic networking technologies

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-8322-9283-9

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

® Registered trademark of the International Electrotechnical Commission

CONTENTS

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

Part 90-13: Deterministic networking technologies

FOREWORD

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

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

IEC TR 61850-90-13, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

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

Draft TR	Report on voting
57/2236/DTR	57/2301/RVDTR

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

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

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

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 "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

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

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

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

INTRODUCTION

Deterministic networking technologies enable applications that require bounded communication delays regardless of network load or reconfiguration. They allow traffic of different time-criticality to share the same physical medium. Deterministic network technologies are based on the pre-allocation of resources using for example scheduling, traffic shaping and the pre-emption of low priority messages to guarantee the timely delivery of high-priority traffic.

Power automation and control is an industry domain where deterministic networking is needed to support existing use cases and applications (requiring real-time communication), and to enable new developments. This networking is currently being provided by SDH networks or dedicated (for protection communications) Ethernet networks; however significant drives (economic and political) are now emerging to use "converged" Ethernet networks.

In this document the term WAN is used for the inter-substation communication networks, with the driving force usually being the desire of a utility to use the same network infrastructure for IT as well as for operational tasks such as inter-substation protection communications.

The term LAN is used for the intra-substation communication networks. Converged networks are those supporting mixed traffic (e.g. process data, configuration management, voice and video surveillance data) in the same network being used for critical power automation applications. In the same way that using public transportation to get from A to B in a timely (deterministic) manner requires the ability to be guaranteed a seat at a particular time, using a communication network for the deterministic delivery of data also requires the guarantee of access at a particular time. This document identifies, describes, and discusses the known technologies to address this determinism issue.

Summary:

Clause 5 describes the problem (with non-deterministic networks);

Clause 6 provides use cases;

Clause 7 lists deterministic networking technologies;

Clause 8 discusses interoperability issues;

Clause 9 suggests changes to the IEC 61850 standards needed to support determinism;

Annex A lists some related works and liaisons.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

Part 90-13: Deterministic Networking Technologies

1 Scope

This part of IEC 61850, which is a Technical Report, provides information, use cases, and guidance on whether and how to use deterministic networking technologies. Furthermore, this document comprises technology descriptions, provides guidance how to achieve compatibility and interoperability with existing technologies, and lays out migration paths. It will separate the problem statement from the possible solutions.

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

IEC 60870-5-104:2006, *Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles*

IEC/IEEE 61588:2009*, Precision clock synchronization protocol for networked measurement and control systems*

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

IEC 61850-5:2013, *Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and device models*

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

IEC 61850-8-1:2011, *Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*

IEC 61850-9-2, *Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3*

IEC/IEEE 60802, *Time-sensitive networking profile for industrial automation*

IEC/IEEE 61850-9-3-2016, *IEC/IEEE International Standard – Communication networks and systems for power utility automation – Part 9-3: Precision time protocol profile for power utility automation*

IEC TR 61850-90-1:2010, *Communication networks and systems for power utility automation – Part 90-1: Use of IEC 61850 for the communication between substations*

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

IEC TR 61850-90-2:2016, *Communication networks and systems for power utility automation – Part 90-2: Using IEC 61850 for communication between substations and control centres*

IEC TR 61850-90-4:2020, *Communication networks and systems for power utility automation – Part 90-4: Network engineering guidelines*

IEC TR 61850-90-5:2012, *Communication networks and systems for power utility automation – Part 90-5: Use of* IEC *61850 to transmit synchrophasor information according to* IEEE *C37.118*

IEC TR 61850-90-12:2020, *Communication networks and systems for power utility automation – Part 90-12: Wide area network engineering guidelines*

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 62439-3:2016, *Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*

IEEE 802.1AS, *IEEE Standard for Local and Metropolitan Area Networks – Timing and Synchronization for Time-Sensitive Applications*, available at http://www.ieee.org

IEEE 802.1Q, *IEEE Standard for Local and metropolitan area networks – Bridges and Bridged Networks;* available at <http://www.ieee.org>

IEEE 802.1Qcc-2018, *IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks – Amendment 31: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements*

IEEE 802.3-2018, *IEEE Standard for Ethernet*

IEEE C37.94-2017, *IEEE Standard for N times 64 kbps Optical Fiber Interfaces between Teleprotection and Multiplexer Equipment*

IEEE C37.118.1-2011, *IEEE Standard for Synchrophasor Measurements for Power Systems*

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

3 Terms and definitions, abbreviated terms and acronyms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

3.1.1
Centralized Network Configuration
CNC
logical component that configures network resources on behalf of TSN applications (users)

3.1.2
Centralized User Configuration
CUC
logical component that discovers and configures application (user) resources in end stations; the CUC exchanges information with the CNC in order to configure TSN features on behalf of its end stations

3.1.3
convergence
heterogeneous applications running on devices connected to the same physical network (LAN, WAN, or combination of both) which are able to exchange data, within the defined QoS parameters derived from application requirements

3.1.4
deterministic jitter
property of a system to change its output in response to a change of its input after a guaranteed minimum delay and before a guaranteed maximum delay, under error-free conditions

3.1.5
deterministic latency
property of a system to change its output in response to a change of its input within a guaranteed maximum delay, under error-free conditions

3.1.6
deterministic networking
predictable network behaviour which can be characterized by bounded latency, nearly zero jitter and extremely low data loss rates

3.1.7
DetNet
IETF Deterministic Networking (DetNet) Working Group

3.1.8
end station
device attached to a local area network (LAN) or wide area network (WAN), which acts as a source of, and/or destination for, traffic carried on the LAN or WAN

Note 1 to entry: The term end-station is used in relation to time-sensitive networking.

3.1.9
EtherCAT
Ethernet fieldbus system according to the type 12 specifications of IEC 61158 (all parts)

3.1.10
hard real time
property of a system with a deterministic latency

3.1.11
jitter
time variation of an expected occurrence with respect to a defined period

3.1.12
Listener
end station that is the destination, the receiver of a Stream

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

3.1.13
Pdelay
measure of the time from when a message is transmitted from one device to when the same part of the same message is received by the other device and vice versa as defined in IEC/IEEE 61588 and IEEE 802.1AS-2020

3.1.14
pre-emption
suspension of the transmission of a pre-emptible frame to allow one or more express frames to be transmitted before transmission of the pre-emptible frame is resumed

3.1.15
process data
data object containing application objects designated to be transferred cyclically or acyclically for the purpose of processing

3.1.16
project
system part with ownership of a set of IEDs, typically those located in one substation, and handled by one system configuration tool

3.1.17
soft real-time
property of a system whose latency is a probabilistic function with a low probability to exceed defined upper and lower bounds under error-free conditions

3.1.18
Stream
unidirectional flow of time-sensitive application data between from one source (Talker) to one or more destinations (Listeners)

3.1.19
Talker
end station that is the source or producer of a Stream

3.1.20
traffic shaping
queue management technique in packet-based networks to administrate data rates and bandwidth

3.1.21
TSN
series of Ethernet standards which is developed by the Time-Sensitive Networking task group in the scope of IEEE 802.1

3.2 Abbreviated terms and acronyms

The following abbreviated terms and acronyms apply to this document.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

ARP	Address Resolution Protocol
CIP	Critical Infrastructure Protection
CNC	Centralized Network Configuration
CUC	Centralized User Configuration
DC	Distributed Clocks
DDoS	Distributed Denial of Service
DoS	Denial of Service
DER	Distributed Energy Resources
DL-	Data-link layer (as a prefix)
DLL	DL-layer
DLPDU	DL-protocol-data-unit
ENI	EtherCAT Network Information
ESI	EtherCAT Slave Information
ESP	Electronic Security Perimeter
FQTSS	Forwarding and Queueing for Time-Sensitive Streams
GNSS	Global Navigation Satellite System
GOOSE	Generic Object Oriented Substation Event
HMI	Human Machine Interface
HSR	High-availability Seamless Redundancy
ID	Identification
IED	Intelligent Electronic Device – any programmable or configurable device in the system
IERS	International Earth Rotation and Reference Systems Service
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
IT	Information Technology
LAN	Local area network
LD	Logical Device (IEC 61850)
MAC	Media Access Control
MPLS	Multiprotocol Label Switching
MSRP	Multiple Stream Registration Protocol (MSRP)
NERC	North American Electric Reliability Corporation
NFV	Network Function Virtualization
OSI	Open System Interconnect
PDF	Portable Document Format
PMU	Phasor Measurement Unit
PRP	Parallel Redundancy Protocol
PTP	Precision Time Protocol
QoS	Quality of Service
RAS	Remedial Action Scheme

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

RSTP	Rapid Spanning Tree Protocol
SA	Substation Automation
SCD	System Configuration Description in the sense of 61850-6. Output of a system tool of a project to configure the IEDs belonging to the project (imported by IED tools).
SCL	Substation Configuration description Language according to IEC 61850
SDH	Synchronous Digital Hierarchy
SDN	Software Defined Networking
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical NETwork
SRP	Stream Reservation Protocol
SP	Synchrophasor
SPS	Special Protection Schemes
SS	Substation System
SV	Sampled Values
SW	Software
TAI	International Atomic Time
TDM	Time-division Multiplexing
TCP	Transmission Control Protocol
TP	Tele-Protection
TSN	Time Sensitive Networking
UDP	User Datagram Protocol
UNI	User Network Interface
VLAN	Virtual LAN
WAN	Wide area network
XML	eXtensible Markup Language
YANG	Yet Another Next Generation, a modeling language for network management

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

4 Characteristics of determinism

4.1 Deterministic latency

A system with a deterministic latency is characterized by a guaranteed maximum delay between a change at its input and the reaction at its output, under error-free conditions.

Mathematically, the input to output delay of a system with a deterministic latency presents a probability distribution function (pdf) that has an upper bound smaller than a given deadline, in contrast to a non-deterministic system whose delay has a low, but non-zero probability, to exceed the deadline under error-free conditions, see Figure 1.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

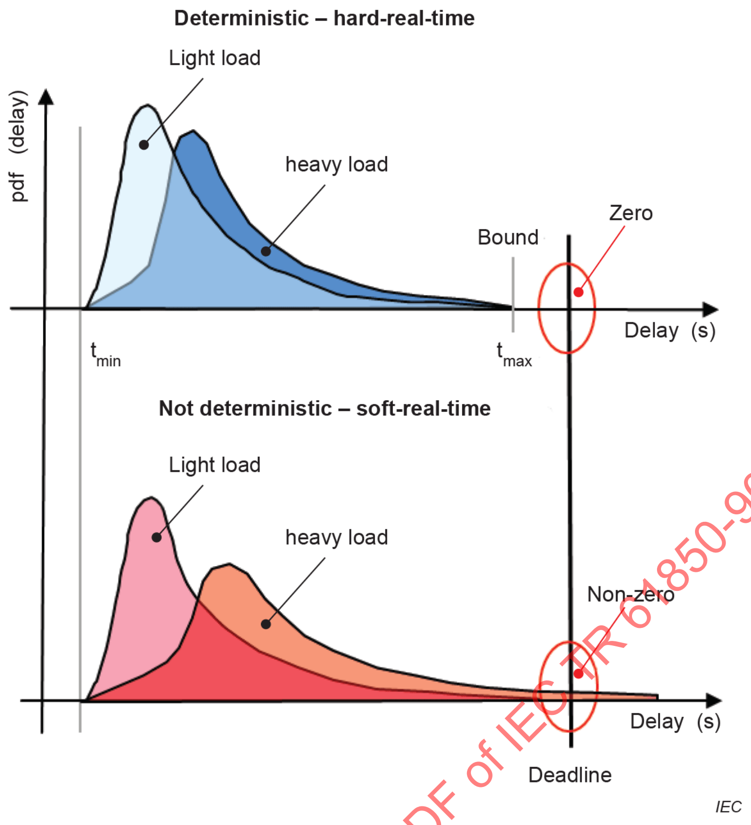


Figure 1 – Delay probability for hard- and soft-real-time system

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

Determinism is provided under all normal operating conditions, in particular, irrespective of the network traffic, but not in case of any hardware failure. Redundancy can provide deterministic behaviour in spite of a limited number of hardware failures.

A deterministic delay allows in particular to detect a hardware failure in case the deadline is not met.

The basis of determinism is the exclusive, pre-allocation of resources (bandwidth, processing power, buffers) for a given transmitted data item. Different networking methods exist for it, in particular cyclic polling or time-triggered protocols.

In a network, each critical data item to be transmitted is assigned a given bandwidth, a delivery bound and a maximum production rate. The receiver of the data is informed of the age of the received data, and can take action if the deadline is expired. The network elements also need this information to assign the resources.

Determinism therefore requires that the resources can be allocated. For instance, if the transmission of a critical data takes 1 microsecond (100 bits at 100 Mbit/s) on the medium and its deadline is 1 ms, at most 1 000 such messages can be transmitted, in reality less since the propagation time is not included and other traffic (management, etc.) may share the medium.

Data can be grouped in critical sets with the same delivery bound and production rate.

4.2 Deterministic jitter

A jitter is defined as the deviation σ with respect to a fixed, mean value. A low-jitter system exhibits a pdf that is a small, tall pulse around a defined mean delay, with a minimum delay greater than zero and a maximum delay, see Figure 2.

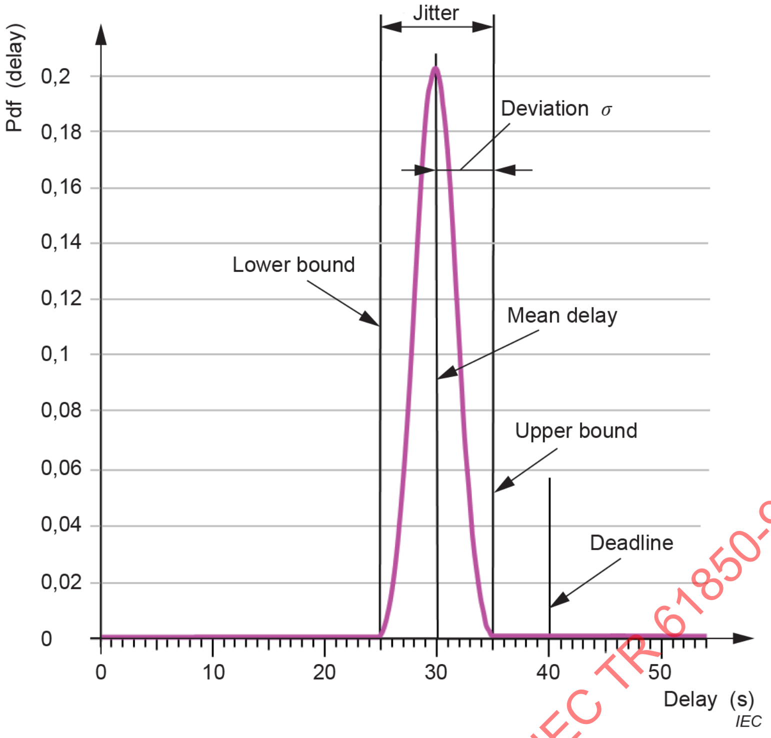


Figure 2 – Low jitter – jitter deterministic delay

To achieve such a behaviour, the mean value must be respected. This may imply delaying purposely the output (e.g. in air traffic control or manufacturing).

Low-jitter operation requires determinism, but it does not request a jitter-free transmission, if a global time is available.

Low-jitter is the essence of streaming video or telephone over a packet-switched network.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

5 Problem Statement

5.1 Overview

Deterministic networking technologies evolve and provide means to support and improve existing use cases as well as opportunities to foster new applications. These use cases are typically clustered into two application domains: Substation-LAN and WAN-based.

IEC 61850-5 and IEC TR 61850-90-12 identify communication requirements between intelligent electronic devices within plants and substations in the power system, between such stations (e.g. between substations for line protection) and between the plant or substation and higher-level remote operating places (e.g. network control centre) and maintenance places. Clause 11 of IEC 61850-5:2013 defines the performance requirements related to the different messages used in IEC 61850-based substation networks. Additional requirements for communication between substation and substation and control centres are specified in IEC TR 61850-90-12:2020, Clause 5. These messages are classified using their type and performance requirements. They also define requirements for data and communication quality (Data Integrity, Reliability, Availability). Finally, they cover the communication system requirements for performance, communication redundancy, failure recovery and recovery delay.

The performance requirements of IEC 61850-5 and the recommendations in IEC TR 61850-90-12 assume transfer delay under normal conditions without disturbed communication (IEC 61850-5:2013, 11.1.2.1). These documents do not require bounded latency and bounded jitter explicitly. Although, some applications could benefit from bounded latency and bounded jitter under condition such as network congestion.

Installed substation networks meet the requirements of IEC 61850-5 and operate well with current technology. This TR addresses technology change and future needs such as migration to packet switching technology, digitization of substation and RAS, combined with Distributed Generation, DER, upcoming new trends in the energy markets and society, significant emergence of software for the integrated/centralized protection and substation automation functions and OT/IT/Telecom/Security convergence. See Clause 6 for more detailed discussion of the typical use cases.

5.2 Problems with existing technologies

For inter-substation WANs, the protection functions used by power utilities to protect their critical assets are mostly using TDM communication networks with deterministic channel latencies of a few milliseconds. In order to avoid maintaining these TDM networks that are being phased out or for other reasons, many utilities are moving to packet-based networks. When this migration is combined with the integration of inter-substation protection and RAS functions with the corporate needs on a common communication platform, new problems arise. For such migrations, since the protection fault-clearing times affect a transmission power line's power-handling rating, the replacement Ethernet channel latency shall not be higher than that of the original TDM channel.

Actual packet switching technologies face higher challenges than TDM technologies to meet the latency requirements of the applications (e.g. the <5 ms specified in IEC TR 61850-90-12 for current differential protection). The difficulty to predict the latencies encountered as traffic traverses a network is the major problem (queuing latencies) especially for networks carrying other (IT) traffic.

A more challenging problem for some utilities is a requirement that the bidirectional latencies of channels used for current-differential be symmetric, typically with an asymmetry below 0,4ms (or even lower according to CIGRE recommendations [1][1]). This requirement is needed only for relays without an external timing source (e.g. GNSS, PTP) [2].

For Substation-LANs,

- Integration and convergence of networks in the substation over a single infrastructure, for all types of traffic, is a trend for some utilities. It may lead to increased network loading, impacting the need to prioritize protection function traffic.
- Protection function traffic, especially sampled values and some mission-critical GOOSE messages, shall be continuously prioritized over the substation telecom network, even with traffic fluctuations.

Present grid automation communication based on packet-switched networks exhibit a traffic-dependent, variable latency. Every increase in non-critical traffic can increase the latency of time-critical data. This makes it difficult to add new traffic to an existing network. Present networks have insufficient control over the traffic, therefore the network engineers overprovision the network. A proper network design and priority planning, as well as enhanced quality of service mechanism can limit the effects to a level which is not critical anymore for usual applications. Simulation tools offer only a limited support. Overprovisioning of network bandwidth is one of the techniques currently used to increase the probability of delivery of critical traffic by preventing network congestion. The overprovisioning of network bandwidth is not an efficient resource usage. Utilities are looking for new ways to optimize the bandwidth usage and minimize the overdesigning of their networks.

[1] Numbers in square brackets refer to the Bibliography.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

IEC TR 61850-90-4 and IEC TR 61850-90-12 recommend the use of VLANs and QoS mechanisms for increasing the probability of meeting the communication requirements specified in IEC 61850-5. These mechanisms do not guarantee that these requirements will be met in case of network congestions that may impact the transmission of critical flows.

In large substations, the number of IEDs and the necessity of doing multicast filtering make the configuration of the network and specifically the VLANs very complex. Today system-engineering tools can support the design and configuration of substation networks.

5.3 Improvements in networking communication from using the capabilities of deterministic communication technologies

The upcoming trends and future evolutions are bringing new use cases and operational modes that will change the way the substation and its functions are seeing currently. On the other hand, the current activities on the IEC 61850 extensions that are going on in the Working Group 10 of IEC Technical Committee 57 will also generate some new impacts for the Utilities. Is the current network architecture and technology sufficient for them?

Communication networks based on Ethernet and IP are the deployed technologies to meet the performance requirements of IEC 61850-5 over substation LANs. MPLS or IP (IPv4, IPv6) is becoming a commonly deployed technology to meet requirements and implement architectures over the WAN. These technologies evolve over time and new network capabilities to improve performance are getting developed and standardized. Additionally, deterministic network technologies are available as standards for the LAN and WAN environments. These standards explicitly address real-time and deterministic behaviour for domains such as industrial and power automation, automotive, transportation, and audio/video. Along these lines, deterministic networking technologies may provide capabilities to meet the following requirements in power utility automation:

- Functional requirements like performance and quality of data exchange;
- Non-functional requirements such as manageability;
- Flexibility in network topology meeting redundancy requirements (e.g. meshed network with seamless redundancy);
- 1+n redundancy schemes are achievable;
- Enhancements of network security (e.g. network access control, filtering, visibility);
- System and architectural aspects such as converged networking to enable a multi-service architecture in a substation (Security Monitoring, IoT, SPS/TP/SCADA, Phone [Safety requirements imposed by the NERC], Tele-commissioning, Market info, Management of Telecom components, HMI, etc.) and over the WAN.

5.4 Drawbacks of deterministic networking

5.4.1 General

It is one key objective of this document to address the challenges of introducing new network technologies, even within a layered architecture such as IEC 61850. Use and application of deterministic networking technologies should consider integration and compatibility with existing network technologies and applications. This encompasses the engineering process as well as other configuration efforts. This Technical Report provides guidance regarding co-existence and interoperability with existing technologies and how to address technology changes. In addition, it assesses the impact on application operation and considers migration strategies. It is key to choose the appropriate deterministic networking technology in order to meet the requirements, to accomplish the improvements, and to achieve co-existing with current-use cases and deployments. The deployment of deterministic network technologies may impose the following issues and raise potential questions:

- Compatibility with existing solutions;
- Deterministic networking requires specific configuration across the network. How does this fit with existing configurations?

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

- Publishers / subscribers of data may need to be deterministic networking-aware devices
- New challenges in case of fully converged networks in terms of security,
- New challenges regarding operation and maintenance, responsibility boundaries, operational processes.

5.4.2 Change in network design

Since thousands of grid automation networks today operate reliably, one of the major motivations for determinism is to allow "convergence", i.e. merging the time-critical and non-critical traffic on the same network. This convergence is not broadly accepted, especially in the substation, because of security and responsibility concerns. This document will bring clarity to which network convergence applies: process bus, station bus, inter-substation or wide area network to Control Centres or Phasor Data Concentrators. The deterministic technology employed may depend on the particular network. Determinism is an end-to-end property, from application to applications. Making only the network deterministic does not ensure overall determinism. The time-critical traffic can only be protected from random, non-critical traffic if all elements in the chain (IEDs, bridges, routers, etc.) behave deterministically and all delays and generation rates are predictable, which is not the case today. The network engineer will have to estimate the maximum production rate of the publishing applications and the performance of the network nodes (per hop behaviour). This requires a better understanding of the network traffic patterns than today.

5.4.3 Changes to the network infrastructure

All network elements must support deterministic operation and provide the resources. For instance, in the case of TSN, bridges would implement at least a subset of the TSN standard suite [3] and provide the corresponding SNMP, YANG or IEC 61850 management. Even if classical RSTP is displaced, traffic characterisation, traffic limitation and topology restrictions will have to be observed in the same way as today.

5.4.4 Change to the network tools

Manufacturer-independent tools will be needed to configure and troubleshoot the deterministic network since the network operation cannot anymore be handled manually. Such tools rely on characterization of the bridge performance and on characterization of the data production patterns of the IEDs. They must be integrated with the substation configuration tools (CID, SCD) and generate the corresponding resource reservation, either in a static or in a dynamic way.

5.4.5 Hardware changes to the IEDs

IEDs need to support deterministic operation, at least to support basic scheduling. The current technology in the IEC 61850 IEDs may need to be extended by new clock synchronisation, redundancy and hardware components.

5.4.6 Change to the IED applications

The introduction of deterministic network may require changes in the applications.

5.4.7 Change to the standard

The communication object models (IEC 61850-7-x) and SCD (IEC 61850-6) need extension to support the configuration of the network elements. A new SCSM IEC 61850-8-x specification is needed to support determinism. In the case of TSN, a profile of the TSN standard suite for grid automation is needed. A TSN profile for industry automation started in 2018 as IEC/IEEE 60802 and it would be advisable to align the IEC Technical Committee 57 profile with the outcome of that joint development.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

5.4.8 Backward compatibility and transition phase

A migration from the current best-effort network to the deterministic system is needed. Therefore, groups of devices will emerge: those that support determinism and those who do not and their interoperability may have limitations.

5.5 Survey about problem statement

As part of the work of this task force a survey about the problem statement was performed and a questionnaire was distributed to utilities through CIGRE SC B5 and Working Group 10 of IEC Technical Committee 57. The main goal was to receive feedback and input to the problem statement. Answers from 8 utilities were received. As could be expected, the responses were mixed, but following some key points from the feedback:

- utilities main concern is less about application problems or performance of the existing networks. The main concerns are rather related to Network Synchronization, Cyber Security and System Configuration & Monitoring;
- transmission delay and bandwidth usage is a concern, however the utilities mainly seem to be satisfied with the performance of current substation installations / current technologies;
- brownfield installations, migration scenarios and interoperability are a general concern;
- differential protection over packet network (WAN) is still a challenge. Improvements are expected in the future;
- multiservice/converged networks are generally accepted in the WAN. In the substation, utilities follow different concepts/strategies;
- factors to prompt the introduction of deterministic networking: Utilities expect improvements on configuration, Operations and Management and Cyber Security;
- factors to prevent the introduction of deterministic networking: interoperability and cost.

6 Deterministic networking – support and improvements for existing use cases

6.1 Use cases for the LAN

6.1.1 Requirements

As shown in Table 1, for trips and blockings, a channel of <3 ms is required.

Table 1 – Transfer time requirements of IEC 61850-5

Transfer time class	Transfer time [ms]	Application example, transfer of
TT0	> 1 000	Files, events, log contents
TT1	1 000	Events, alarms
TT2	500	Operator commands
TT3	100	Slow automatic interactions
TT4	20	Fast automatic interactions
TT5	10	Releases, Status changes
TT6	3	Trips, Blockings

Source: IEC 61850-5:2013, Table 1

Fortunately, there is no need for the substation LAN used for the above Ethernet traffic to also handle the non-protection substation traffic (they can be on separate LANs), so good engineering of the protection LAN is likely to be able to ensure that the protection latency requirements are met.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

6.1.2 Substation automation

The topology of today's substation communication networks is usually subdivided into station bus on station level and process bus on bay and process level. See Figure 3 and 4.3 of IEC TR 61850-90-4:2020.

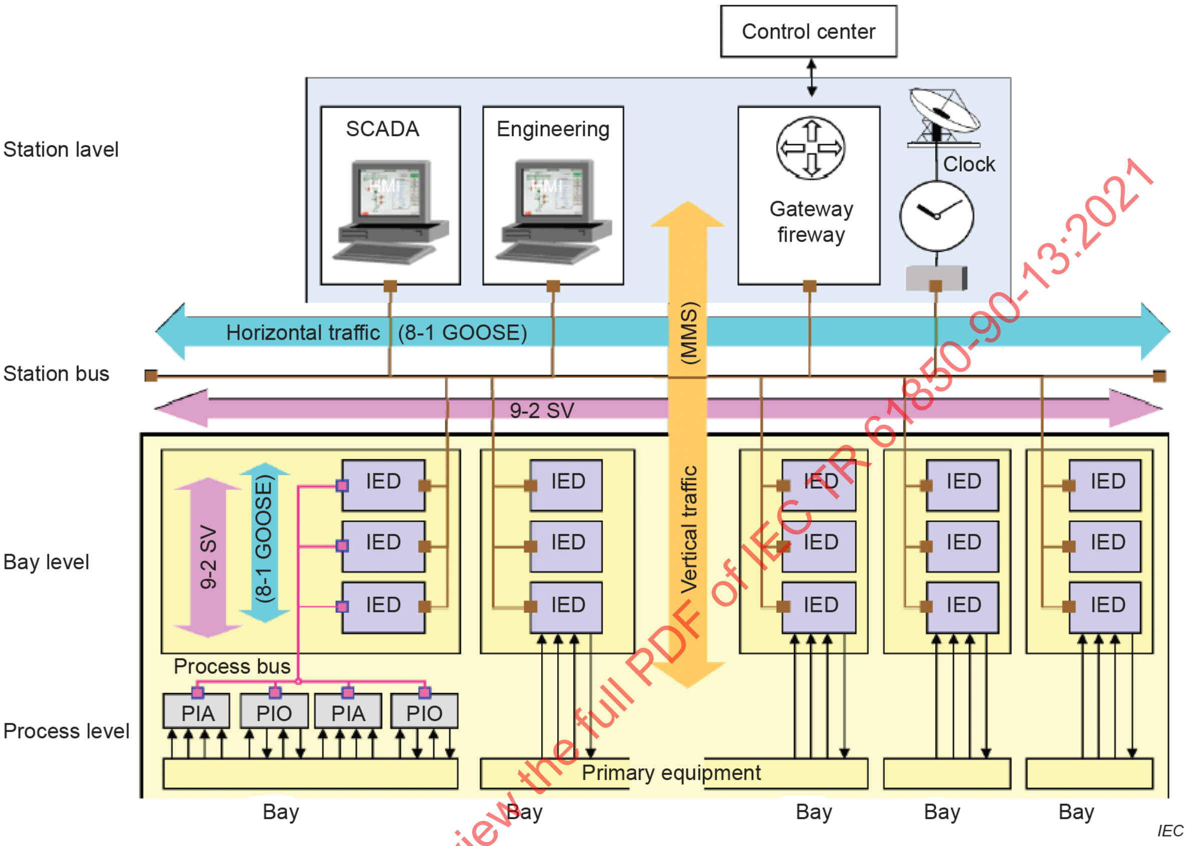


Figure 3 – Substation station bus, process bus and traffic example (IEC TR 61850-90-4, Figure 11)

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

The process bus connects primary measurement and control equipment to IEDs, e.g. protection relays. The process bus typically carries sampled values (SV), trip commands (GOOSE), control traffic (MMS), IEC 61850-9-3 (PTP) synchronization and protocol control messages (e.g. ARP, RSTP, HSR, PRP, LLDP). Ring and star topologies are common on process bus. There are high performance and quality requirements on this real-time communication regarding transfer time (latency), time synchronization, data integrity, reliability and availability. See IEC 61850-5:2013, Clause 10. The usual Ethernet provides Class of Service based traffic prioritization but it does not provide resource, especially link bandwidth reservation capabilities. The result is that high and low priority traffic shares the link bandwidth on a first-come-first-served basis. High and low priority traffic interferes with each other on common links and the degree of interference usually increases with the link bandwidth occupation level. This well-known behaviour is mitigated by experienced network engineers in many cases by limiting the average traffic bandwidth usage or, in other words, by leaving enough spare bandwidth up to the nominal link bandwidth. This is achieved, for example, by limiting the number of devices on Ethernet rings and by physical traffic separation. The latter means e.g. that process data traffic on the one hand and engineering and management traffic on the other hand is sometimes carried over separate Ethernet LANs where the IEDs are connected via separate interfaces. This results in an increased number of network components (e.g. Ethernet bridges) and higher wiring and network management efforts.

The station bus interconnects the whole substation and provides connectivity to SCADA and between substation central engineering and management on the one hand and the individual bays and their IEDs on the other hand. Ring, star and meshed topologies are used. In big substations the station bus is hierarchically organized and segmented. It interconnects up to hundreds of IEDs, work stations and other devices (e.g. VoIP phones, surveillance cameras). The bandwidth utilization on central links can be accordingly high. The station bus carries typically TCP/IP and UDP/IP based traffic (IEC 60870-5-104, MMS, HTTPS, NTP, SNMP, FTP, VoIP telephony, video streams etc.), IEC 61850-9-3 (PTP), protocol control messages and also GOOSE and SV for some applications with relaxed (compared to the process bus) performance requirements. This shows that the station bus is a multi-tenant, multi-service network which is shared by multiple applications with quite different communication requirements. Mutual impact between applications cannot be avoided due to the limited Layer 2 QoS capabilities. It can only be reduced by physical and virtual network segmentation (VLAN), traffic pruning (multicast filtering), Class of Service based traffic prioritization, limiting the number of devices per segment and link bandwidth over-provisioning. Careful network design based on rules and experiences is very important. There are IEDs with real-time applications like PMUs in substations, which communicate over the WAN with counterparts in other substations or control centres based on IEEE C37.118.1 or IEC TR 61850-90-5. These IEDs are usually not connected to the substation edge routers over the station bus because latter cannot satisfy the high-performance requirements of these applications. Instead, the IEDs are connected via separate networks or direct Ethernet cables to the substation routers, occupying this way additional expensive router ports. The high requirements on communication reliability and availability are fulfilled in today's substations by using the PRP and HSR seamless redundancy protocols. PRP is based on a doubled LAN infrastructure which requires a doubled number of Ethernet bridges in the LAN and special PRP redundancy boxes for connecting PRP-unaware nodes. Consequently, the wiring and management effort is significantly higher compared to a single LAN infrastructure (running e.g. RSTP which is not seamless redundant). HSR is more economical here but it is usually implemented in a ring topology.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

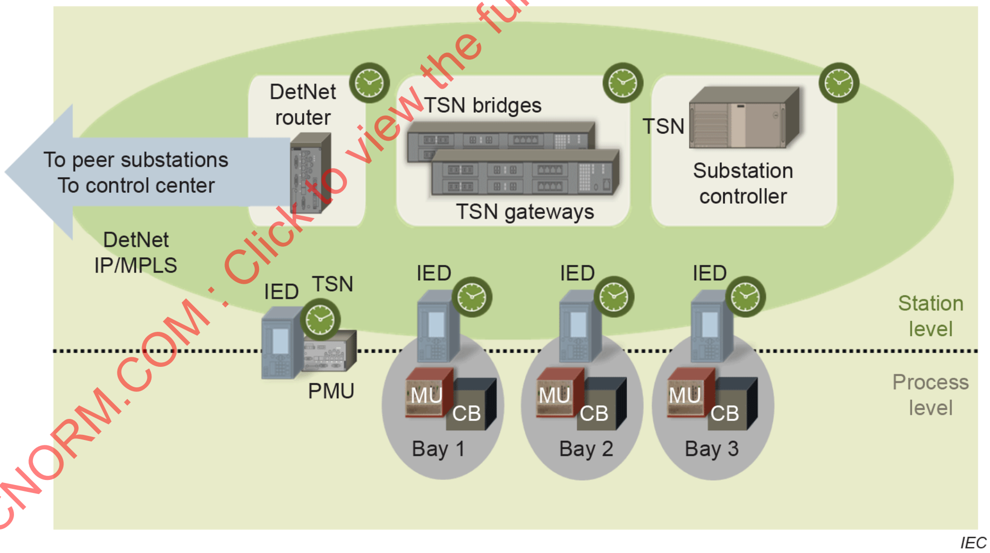


Figure 4 – Substation with Deterministic Ethernet

Figure 4 depicts a high-level architecture where TSN and DetNet-based technologies are used in a substation automation network connected to other substation(s) and/or a control centre.

Deterministic Ethernet with its hard real-time capabilities like traffic class based shaping and scheduling and the resulting traffic separation and Quality of Service guarantees (bounded latency, low jitter, close to zero packet loss) can enable converged, multi-service networks which are shared by critical real-time, high-bandwidth-consuming video-streaming and best-effort applications. In case of process bus, the periodic SV could be carried in separate time slices with QoS guarantees, which mostly eliminate any impact from other interfering traffic. GOOSE frames could be classified into two classes, according to their criticality (based on IEC 61850-8-1):

- critical traffic (1A) could use deterministic services (e.g. TSN time-aware shaper with deterministic latency and zero jitter);
- less critical traffic (1B) could use QoS-bounded services (e.g. TSN credit-based shaper).

The remaining time and bandwidth on the process bus could be used by engineering and management traffic to the IEDs. Where currently used, the separate network and the dedicated IED interfaces for engineering and management purposes could be avoided, reducing engineering and equipment costs. Today's practice of limiting the average link bandwidth usage is not needed anymore which would allow a higher number of IEDs to be connected on an Ethernet network.

In the case of a station bus the transport of the various communications could be done according to their mapping to deterministic traffic classes. Similar to the process bus, periodical real-time communication like SV is handled in separate time slices. Other event driven and time-constraint communication like GOOSE or MMS can be carried with high priority, bounded latency and reserved bandwidth. Streaming-style communication like VoIP and video can be transmitted with less priority but reserved bandwidth. Best-effort traffic, e.g. HTTPS, is separated in time and traffic-shaped. Overall, the impact on real-time communication from other interfering traffic could mostly be avoided or significantly reduced and QoS guarantees on latency, jitter and packet loss rate be applied. But also other traffic would not be displaced, e.g. in high-load situations, if bandwidth reservation is used. PMUs could be connected over the process bus (if appropriate) and the station bus to the substation edge routers. The Deterministic Ethernet hard real-time and QoS capabilities could be used for fulfilling the performance requirements of synchro-phasor communication. The Stream-level traffic separation would provide isolation from the substation-internal traffic. The Deterministic Ethernet supports seamless redundancy by Stream replication at the source side and duplicate packet elimination at the destination side. This procedure is somehow similar to the method used by PRP and HSR but it does not require a doubled LAN infrastructure like PRP and it is not limited to ring or multiple-ring topologies like HSR. This means it can be more economical and flexible regarding the network topology if latter provides disjoint communication paths.

In summary, the introduction of Deterministic Ethernet could help to overcome many of today's constraints on network topology design. The substation network topology would become more flexible and could be better tailored to the power utility needs. The hierarchical organization of the network on station, bay and process level will probably not become obsolete. But today's usual network segregation of the station bus and process bus LANs (with selective interconnection by IEDs or e.g. Ethernet bridges) could be replaced by Stream-level separation of time-constrained, other prioritized and best effort traffic on a common network. This can help to foster the adoption of applications like centralized protection where the central protection function can be placed e.g. on station instead of bay level. Table 2 and Table 3 describe the communication specifics in today's substations and possible benefits/improvements with TSN for station bus and process bus, respectively.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

Table 2 – Station bus communication specifics in today's substations and possible benefits / improvements with TSN

Substation Network	Communication specifics in today's substations	Benefits / Improvements with TSN
Station Bus	Multiple services (with different properties, priorities) share station bus	Traffic separation on shared network – minimum impact on high-priority traffic from other traffic -> bounded latency, minimum jitter
	High traffic load on station bus in big substations	Resource reservation (esp. bandwidth) for high-priority traffic -> reduced latency, jitter; congestion avoidance, i.e. close to zero packet drops
	Different network topologies (star, mesh, ring, combinations of them)	Different topologies possible, as appropriate; more flexibility since topology dependency is mostly removed
	Different redundancy protocols (HSR, PRP, RSTP)	Seamless redundancy by stream replication – similar to HSR but topology independent (disjoint paths needed)
	Increasing importance of security	Build-in security by traffic separation, resource reservation and stream filtering
	Network overprovisioning due to missing guarantees on latency, jitter, packet loss of high priority traffic	QoS guarantees -> higher link bandwidth and network equipment usage – reduced link bandwidth and equipment overprovisioning

Table 3 – Process bus communication specifics in today's substations and possible benefits / improvements with TSN

Substation network	Communication specifics in today's substations	Benefits / Improvements with TSN
Process Bus	Real-time services (sampled values, tripping, time synchronization …) on process bus. Non-real-time traffic (engineering, fault recording, management, …) handled via separate network.	Real-time and non-real-time traffic can share the process bus. Traffic separation, resource reservation -> bounded latency, minimum jitter, congestion avoidance of high-priority real-time traffic
	Usually star or ring topology (with PRP resp. HSR redundancy)	Star, ring, mesh topology possible, as appropriate; seamless redundancy by stream replication
	High requirements on latency, time synchronization accuracy, availability, dependability of protection communication; therefore, limited number of IEDs and/or network overprovisioning due to missing guarantees on latency, jitter, packet loss	QoS fulfilment guarantees; number of IEDs increased, network overprovisioning reduced or avoided
	Increasing importance of security	Build-in security by traffic separation, resource reservation and stream filtering

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

6.1.3 WAN-based use cases

6.1.3.1 Protection schemes

There are two schemes used to detect faults on transmission power lines. These comprise:

- current-differential;
- impedance based protection.

The first requires a communication channel between the ends' relays for comparing the ends' line currents' magnitudes and phases.

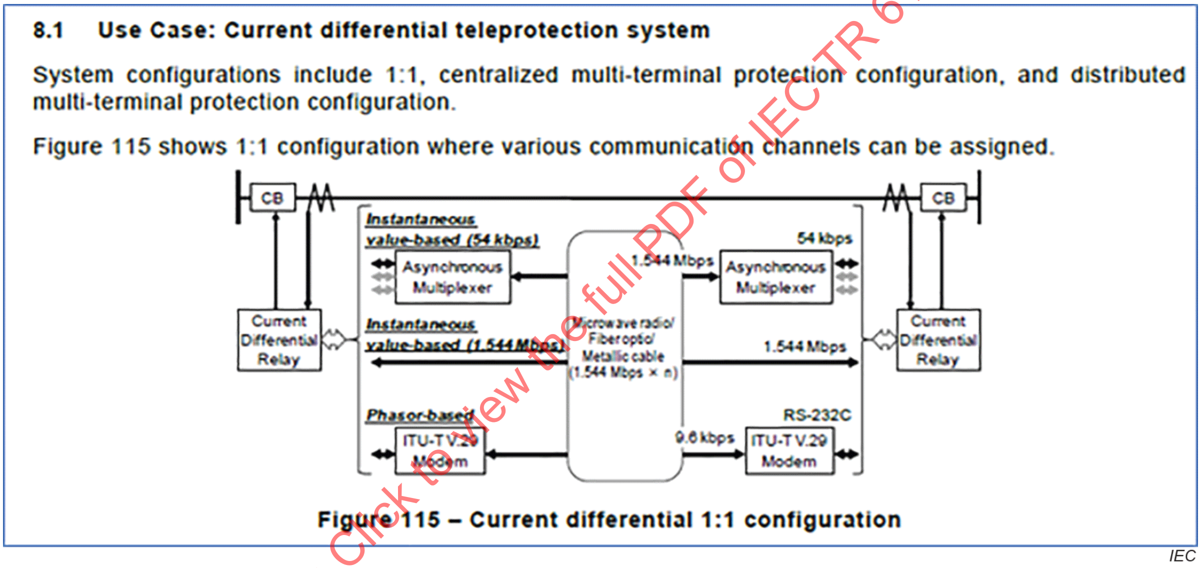
Using the second scheme, a substation can reliably detect faults only up to about 90 % of the line's length, so it needs to send a status signal to the far end substation (e.g. for tripping its breaker).

Note that with the current best-practice of using SDH/SONET links for its WAN communications, utilities have engineered their transmission power lines to make use of the performance of these links; thus for alternative communication technologies to be used, they must provide the same deterministic latencies.

Since these two protection schemes are the most critical uses for WAN communications, these schemes are the ones described in more detail in 6.1.3.2.

6.1.3.2 Tele-protection for current-differential protection schemes

Figure 5 shows a line current-differential scheme where the current entering a line is compared with current leaving the line to determine if there is a fault. With no faults the currents are equal. A difference in the measured current values suggests a fault on the line, which may result, after further analysis, in the relay initiating a breaker trip sequence.



8.1 Use Case: Current differential teleprotection system

System configurations include 1:1, centralized multi-terminal protection configuration, and distributed multi-terminal protection configuration.

Figure 115 shows 1:1 configuration where various communication channels can be assigned.

CB
CB
Instantaneous value-based (54 kbps)
54 kbps
1.544 Mbps
Asynchronous Multiplexer
Asynchronous Multiplexer
Current Differential Relay
Current Differential Relay
Instantaneous value-based (1.544 Mbps)
Microwave radio/ Fiber optic/ Metallic cable (1.544 Mbps × n)
1.544 Mbps
Phasor-based
RS-232C
9.6 kbps
ITU-T V.29 Modem
ITU-T V.29 Modem

Figure 115 – Current differential 1:1 configuration

IEC

Figure 5 – Current differential tele-protection system (IEC TR 61850-90-12:2015)

Note that the accuracy of these schemes depends on the accuracy of the currents' phase-comparisons.

The specific requirements for Tele-protection applications are mainly driven by the large installed base of legacy protection relays with its strict performance requirements in terms of mutual synchronisation over a WAN (in case of differential protection). A deterministic network, with bounded jitter, can ensure that the ping-pong synchronisation protocol is executed correctly, by limiting the maximum error within the protection algorithm due to communications asymmetry (and thereby mitigating the risk of protection mal-operation due to this factor). It is challenging to guarantee bounded latency and bounded jitter in existing packet-based networks, but technologies exist to alleviate the impact of jitter. This use case is described in further detail in the following paragraphs.

Tele-protection systems have conventionally been implemented using TDM-based communications technologies such as SDH/SONET and using protection relay interfaces such as IEEE C37.94 which provides 1 to 12 times 64 kbit/s for tele-protection data. Such legacy protection systems must be maintained by utilities for many years. Current differential protection requires time synchronisation between the two (or more) terminals, so that the relays can make time adjustments to the received remote current phasor measurements. In many cases, relays

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

use the simple "ping-pong" protocol to estimate the communications path latency [1], using the same communications channel as for exchanging the current phasor data. This approach calculates the average of the round-trip latency, and it therefore assumes symmetrical latency; the presence of asymmetrical latency will introduce an error in the estimated path latency. Therefore, in some circumstances, the presence of communications jitter can interfere with this timing mechanism, which can affect the current differential protection algorithm, potentially leading to a protection maloperation because time adjustments made to current phasors will be incorrect.

The use of GNSS to provide a better quality of time synchronization – eliminating the issue of asymmetrical latency – is often not reliable or is susceptible to jamming or other interference. The IEC/IEEE 61588 Precision Time Protocol (PTP) (such as the IEC/IEEE 61850-9-3 profile in substation LANs and the ITU G.8265.1 [4] and ITU G.8275.1 [5] profiles in inter-substation WANs) can be used as an alternative.

TDM-based transport technologies naturally avoid jitter and the associated issues. Depending on the utility requirements, signalling can be used to block protection operation during communications network reconfiguration (assuming that a suitable, independent backup protection scheme is in operation). Packet-based networks instead emulate TDM-like behaviour using a Circuit Emulation Service. De-jitter buffers (along with traffic engineering and QoS provisions) are used to absorb instantaneous jitter, but there are still situations (particularly during initialisation of the service) where this is inadequate and can lead to protection maloperation. Commercial solutions exist to retrospectively correct misaligned de-jitter buffers, by injecting or dropping bytes of data. An alternative solution which does not require the connection of an external timing source to each tele-protection relay, is to provision a deterministic network which has clearly defined bounded jitter for tele-protection services. In case of TSN however, the complete network shall be properly synchronized instead.

6.1.3.3 Tele-protection for transfer-trip protection schemes

Faults on a power transmission line change the impedance (Voltage/Current) seen at the terminating substations; the closer-to-the-fault substation has a more reliable decision to trip its breaker and so (in case needed) will send a "Transfer Trip" command to the far end substation. The time taken to clear the fault thus depends on the latency of the communication channel for this command.

Power transmission system shall be able to survive line faults (e.g. lightning initiated flashover or an insulator failure). As a result, transmission line nominal power rating depends on the fault-clearing time of its protection scheme; thus the decision to replace an existing TDM communication channel with an Ethernet communication channel will likely depend on the ability of the latter to meet required Tele-protection standard requirements as defined in IEC 61850-5 and/or in IEC 60834-1 as the TDM solution did.

6.1.3.4 IEC 61850 latency requirements for protection schemes

IEC TR 61850-90-12 requires the maximum allowed latency for tele-protection schemes to be as low as 2,5 ms, as shown in Table 4 (extract from IEC TR 61850-90-12, showing tele-protection latency characteristics).

Table 4 – Latency requirements for protection schemes

Tele-protection scheme	Maximum Latency
Differential Protection	2,5 ms to 10 ms
Trip blocking	10 ms
Trip permissive	20 ms
Trip transfer	40 ms

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

Tele-protection using current-differential schemes can tolerate similar latencies, but (unless time-synchronized by external means) require that the latencies of the two communication directions be closely matched. IEC TR 61850-90-12 requires a latency matching better than 200 µs (for a differential current error under 4 %).

6.1.3.5 Synchrophasor networks

Synchrophasor data generated by Phasor Measurement Units (PMU) are typically used for utility monitoring applications, and also have the potential to be used to enable real-time control systems e.g. for fast-acting frequency regulation. Although synchrophasor traffic in such applications could benefit from bounded latency, this is generally less critical compared to tele-protection applications. Furthermore, synchrophasor packets are time-stamped at the measurement location, which can mitigate the impact of network latency and jitter. Therefore, typical applications using synchrophasor data will not require the very stringent bounded latency and bounded jitter performance provided by deterministic networking technologies, and existing WAN technologies are likely to be capable of providing the required performance.

6.1.4 Protection and control for Distributed Energy Resources (DER)

6.1.4.1 Microgrids

One of the trends in the direction of mostly decentralized power generation based on renewables is the implementation of microgrids. Microgrids are usually situated in certain geographical areas, campuses or critical infrastructures and combine renewable, sometimes fossil electric power and heat generation, storage and the distribution to energy consumers, see Figure 6. Microgrids can be operated either isolated from or coupled with the power grid.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

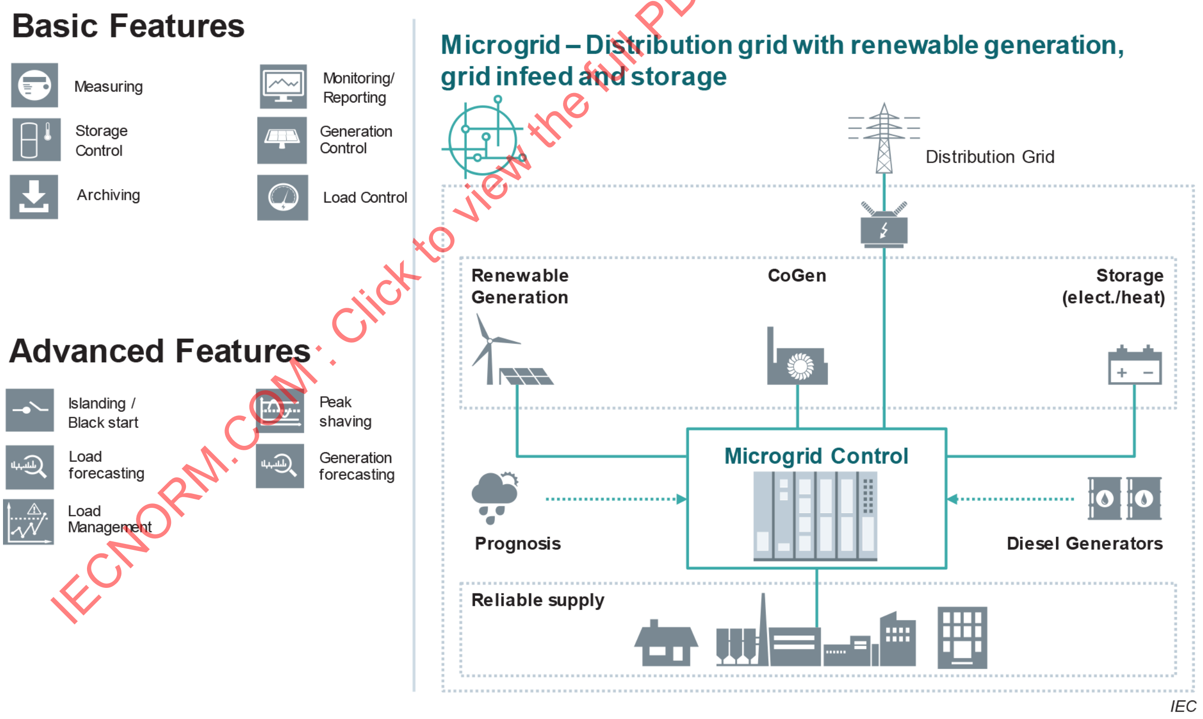


Figure 6 – Microgrid with renewable generation, storage and grid infeed

The classical power generation relies on the high inertia of rotating machines for AC (alternate current) frequency and phase control. This is usually not available in microgrids, which tend to be dominated by renewables. Moreover, renewable energy sources such as solar panels and battery storages provide DC (direct current) and therefore require conversion into AC at the frequency and phase of the power grid. Additionally, renewables (e.g. wind turbines and solar panels) are characterized by fluctuating production behaviour. Microgrid control, in more detail the active and reactive power control loop, requires fast and reliable communication with the connected energy producers, with reaction time within seconds and in some cases within milliseconds. Here are some communication-related requirements from the microgrid control loop:

- latency and turn-around time for use cases like primary control reserve (in case of market participation) or load shedding (in case of island operation) must be reliably within 25 ms and 100 ms (local control, geographical dimension of several km);
- as microgrid assets become smaller and their number increases, an aggregation concept is needed which is requiring fast communication between the aggregator and local microgrid control (currently 1 s to 5 s; required is < 1 s) (the wide area dimension is typically < 250 km);
- spontaneous, event-based communication is required (e.g. for fast load shedding) to secure the grid stability;
- the communication transport layer is subject to change, but for the industrial protocols used (mainly Modbus TCP) no fast replacement is expected.

Deterministic networking technologies like TSN and DetNet are expected to support high-reliable communication with bounded maximum latency and therefore could help in fulfilling these communication requirements for local and wide area control communication.

Deterministic networks could help in separating the time-critical control traffic from other, bandwidth consuming communication like large data sets e.g. for power analytics and this way minimize the impact on the prioritized traffic.

The traffic segmentation and Quality-of-Service guarantees of deterministic networks could be considered as build-in IT security provisions which need to be combined with other security measures for multi-level defence against cyber security threats.

Deterministic networks can automate the process of communication network management, significantly reducing or eliminating the manual configuration effort of network components. This could especially be advantageous for microgrids where the communication network topology may change more often than in the substation automation area.

6.1.4.2 IIC Testbed – Integration of DER Microgrids

In April 2018, the IIC (Industrial Internet Consortium) announced the results of the Distributed Energy Resources (DER) Integration Testbed and published a whitepaper titled "Synchronized and Business-Ready Microgrid" [6]. The testbed demonstrates an architecture and implementation of DER power-generation-based microgrids. Microgrids are installations that cover a small region and typically comprise decentralized energy sources such as wind and solar including primary and secondary equipment to operate protection and control, sometimes in combination with storage capacities. One of the key objectives of the testbed is the implementation of real-time analytics and control in order to guarantee accurate and reliable power generation, making the grid more resilient and stable under various conditions. In the scope of the testbed, time- sensitive networking (TSN) is deployed to operate a network for distributed control between the inverter nodes to provide sub-millisecond synchronized measurement of phase, frequency and voltage. The goal of these applications is to shift the phase angle of a microgrid to match the main power grid in a short time. TSN provides the network capabilities to meet the applications requirements such as the transmission of sub-millisecond synchronized measurement of phase, frequency and voltage and real-time control based on it. Furthermore, it allows advanced analytics and control in order to optimize microgrid operation and enables predictive maintenance based on the availability of real-time data. The architecture of the IIC microgrid comprises two tiers: edge (microgrid) control and cloud-based management including visualization and analytics connected via a real-time data-bus over a TSN-enabled network.

According to the white paper and the documented results, the testbed provides a system and installation, which allows controlling adaptive loads in order to connect, island and reconnect with the main power grid [2].

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

6.1.5 Use cases in which determinism supports non-functional requirements

6.1.5.1 Multi-service architecture and network convergence

Multi-service capabilities help to increase efficiency in deployment, management and maintenance. In IEC TR 61850-90-4, station and process bus are explained including the traffic types and protocols used on both networks. Especially on the station bus, deterministic network technologies can ensure that different traffic types do not impact each other by scheduling a designated Stream for each of them. As an example, with the focus on substation automation, when deploying new or re-modelling substations, utilities are required to deploy several networks in parallel in order to support three types of use cases:

- substation automation and protection (process and station bus) to fulfil the requirements for power grid automation and protection including SCADA;
- video Surveillance and security including back-end services to protect the substation installation also physically;
- maintenance functions to support critical use cases such as firmware updates, debugging capabilities or remote services.

While a number of utilities chose to keep these networks separate, others prefer to merge these three networks into one physical network for cost efficiency and maintenance reasons. With today's communication network devices and QoS techniques, one can meet the individual requirements of the three core use cases only with separate physical networks or with a careful and complex management of the transport and queuing mechanism. For both options, an overprovisioned network is required to address bandwidth availability. Deterministic technologies such as TSN facilitate the mixing of flows as it separates traffic by scheduling and in addition, this way eliminates interference by nature. Without TSN and related deterministic technologies, it is not feasible to guarantee the requirements on a converged network. A striking example to illustrate this is the need to monitor devices (IED's, RTU's) in order to detect incidents and security breaches. IEC 62351-7 (network and system management data object models) does exactly specify this. It would be not efficient to operate this security service on a parallel network. Deterministic networking technologies allow this monitoring on the same network with no impact on the protection and control traffic.

6.1.5.2 Network security

Network security is essential for power automation system networks. A security in depth approach is recommended to protect installation such as electrical substation adequately. This typically comprises network security such as segmentation, network access control and end-to-end security based on standards such as IEC 62351 (all parts) (depending on end device support). Deterministic networking based on TSN provides inherent network security enhancements for TSN flows based on the functions listed by the subsequent bullets:

- temporal firewall – all messages must comply with the schedule(s) for the pre-configured flows and the related ingress policing. Conversely, all inserted and modified messages are dropped. Intercepted and removed messages might trigger an incident and alarm management for further handling;
- topological firewall – all messages shall follow the pre-configured explicit paths for the flow(s). Re-routed messages are dropped and cannot impact the installation;
- the above firewall features are implemented in hardware. They are fast and require no extra management overhead regarding their enforcement;
- TSN flows are immune to best effort Denial of Service (DoS) attacks. They are scheduled and have higher priority than best-effort packets. DoS attacks are critical to the availability of the underlying protection and control system. The inherent architecture of TSN-Flows including ingress policing supports network resiliency.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

Security requirements defined in NERC-CIP (currently version 5) [7] have impact on process bus implementations. The deployment of TSN technologies can support a network architecture with strict and pre-defined network flows to separate traffic by definition. Furthermore, the capability to allow monitoring traffic according to IEC 62351-7 on the same network, strengthen the security countermeasures in total because it makes the deployment of this security control much more efficient and doable. Security in depth is an essential paradigm to protect power automation systems adequately. Adding another control and layer to the existing security architecture will increase the level of protection. The overall security will benefit from these inherent measures and security enhancements. As a result, a multiservice architecture is achievable because the security measures in total will allow network convergence also from the security perspective. Traffic monitoring as defined in IEC 62351-7 could exist on the same network and would not require a separate installation. This fosters adoption and integration into existing network security management.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

6.1.5.3 Usability and ease of use in engineering and network configuration

The concept based on Centralized Network Configuration (CNC), a core part of the fully centralized model as defined in TSN (IEEE 802.1Qcc), supports an integrated approach to enhance usability and to integrate the network configuration with the engineering process of the control and automation solution, e.g. substation engineering. The CNC, a centralized component that configures network resources on behalf of TSN applications and users, provides an open interface which enables the integration with existing engineering tools. An integrated engineering process, comprising network and power automation equipment (in this example IEC 61850-based devices in a substation environment), would typically encompass the following steps:

- a protection engineer uses an engineering tool to engineer the substation solution based on the required functions for protection and control. The engineering tool encapsulates an instance of the CUC;
- the TSN-controller receives the network configuration from the engineering tool via the CUC and a well-defined interface. Based on the information, typically the communication relations between IEDs (in the Substation Automation Solution), the CNC computes the paths and schedules the TSN flows;
- via the southbound interface, the CNC distributes the configuration based on schedules to all TSN-enabled components (bridges) in the substation network, using a network management protocol. As a result, the bridges are configured and no additional network configuration is necessary;
- the engineering process of the IEDs and substation solution as it is/was is not impacted and follows the established workflow.

In summary, based on the integration with the CNC, the engineering tool programs the substation network with "intent" using the logical component CUC. Ease of use and great flexibility make the engineering process easier and limited complexity fosters the security of the entire installation because the engineering process is less error prone and misconfiguration can be avoided. Furthermore, network trouble-shooting capabilities are manifold using the integrated controller concept. All these additional features are advantageous improvements for the complex task of substation network configuration and engineering and addressing OT/IT convergence.

6.2 New use cases (in substation automation and over the WAN)

6.2.1 Large control loops

Deterministic networking technologies will enable new use cases because of their inherent capabilities to guarantee essential QoS requirements. A combination of LAN-based (e.g. TSN) and WAN-based (e.g. DetNet) technologies allows the implementation and operation of critical processes in a cloud environment. The current work in the IEEE 802.1TSN-working group and in the DetNet working group does address use cases and deployment where both technologies are used to combine deterministic LAN and WAN segments. There is already a trend to virtualize automation and control functions. With deterministic networking provided for/over various network architectures and segments, a deployment in the cloud is achievable along with the integration of other hosted applications.

6.2.2 Multi-service networks

Multi-service capabilities based on technologies that enable converged networking can help to increase efficiency in deployment, management and maintenance. One use case, which was already pointed out during the development of IEC 62351-7 (Network and System Management (NSM) data object models) by ENEL is depicted in Figure 7: network and security monitoring traffic can exist on the same tele-control network for hydro generation plants and would provide another layer of security without adding and operating a separate physical network.

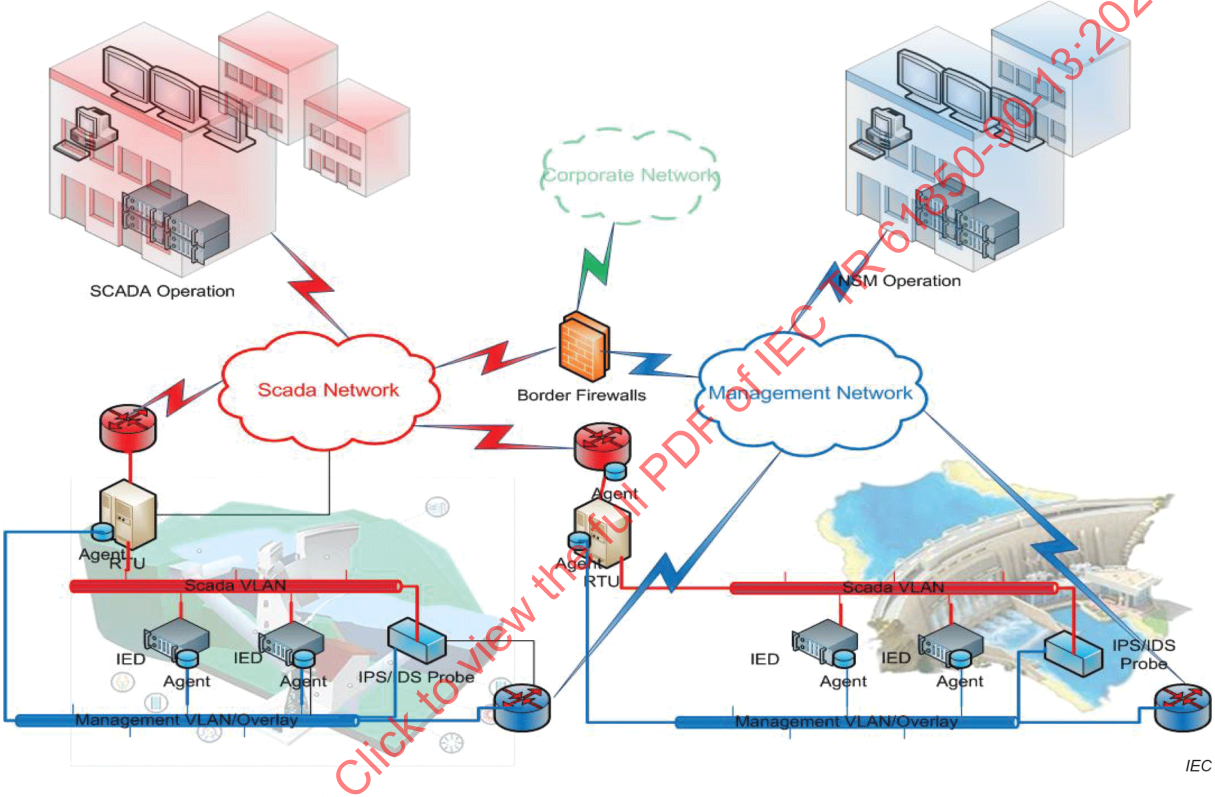


Figure 7 – Multi-Service Networks

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

The information that flows over the WAN between Control Centres and plants and on the plant automation LANs basically belongs to few different services categories:

- tele-control data flow based on IEC 60870-5-104 protocol. This data flow is the most important for the generation plant and therefore deserve the highest priority and granted bandwidth. The bandwidth requirement is basically around 64 kbit/s. Latency optimal value is below 0,5 s but is tolerated up to 1 second (the solution can be operated also through backup satellite connections). Jitter is tolerated in the same degree of latency;
- authentication services (directory service domain). The generation plant work stations require user authentication which is performed through the directory service infrastructure. The domain controllers are located in the management centre even if a local controller is usually located in the plant. The data flow that this service requires is normally very limited with some significant peak values when group policy or controller synchronization is taking place. Difficult to estimate but handled as best effort traffic;
- end devices malware protection (antivirus update or software whitelisting control) and device patch management. This class of data flow has a very peak behaviour oriented. The typical update cycle is daily for Antivirus signatures and weekly for patch management. It is handled as best effort traffic;

- overall system monitoring: collection of system performance and events is performed through IT protocols (e.g. web services). A typical traffic up to 2 Mbit/s is expected. This traffic is left in best effort range of the overall available bandwidth.

Based on traffic type classification and mapping to shaping and configuration mechanisms, these service categories can be transported over the same physical network(s) adhering to required Quality of Service, security and other requirements.

7 Deterministic networking

7.1 Capabilities and improvements

7.1.1 General

Deterministic networking may require time synchronization across the network as well as a change in the way the network is managed. It also enhances the QoS. The subsequent paragraphs explain, analyse and define the capabilities based on the core principles of deterministic networking including any identified improvements.

Capabilities and improvements are strongly related to the characteristics outlined in 7.2.2.2. There are the following core principles to enable deterministic networking in order to design distributed automation and control systems:

- time synchronization;
- quality of service (QoS);
- network configuration and management.

These principles will evolve and merge with other system aspects such as network security and redundancy mechanisms. The subsequent paragraphs analyse and define the capabilities based on the core principles including the identified improvements. The principle architecture comprises a deterministic network, end stations (devices) connected to the network (typically devices such as controller in an automation and control network) as well as a configuration entity.

7.1.2 Time synchronization

From the system perspective, precise time synchronization enables event coordination, data correlation, and time stamping as well as supporting time-scheduled deterministic networking. In protection and control systems, distributed clock synchronization is typically implemented based on the IEC/IEEE 61588 Precision Time Protocol (PTP) and its various profiles including IEEE 802.1AS-2020. In the IEC 61850 environment, it is IEC/IEEE 61850-9-3.

7.1.3 Quality of service (QoS)

Deterministic networking enhances Quality of service (QoS) by capabilities such as:

- guaranteed bounded latency;
- low bounded jitter;
- zero congestion for very low packet loss.

The primary reason for packet loss in a network as well as for latency and jitter is the same: egress and buffer congestion. The key to preventing congestion is to regulate the traffic in each Stream, hop-by-hop based on deterministic forwarding. It is reached by reserving physical resources along the path. In order to meet the requirements regarding bandwidth latency and resource reservation, traffic-shaping mechanisms such as credit-based traffic shaper and time-aware, scheduled traffic technologies are defined.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

The benefits and improvements for automation and control applications are in bounding and minimizing the latency and path delay variation for critical traffic based on the time-synchronized gate control list capabilities. This allocation ensures the transmission of the critical control traffic at pre-defined time intervals. It enables the execution of automation and control functions within a guaranteed time frame and based on predicted and guaranteed latency. High-priority traffic and traffic with lower priority can be transmitted in separated time slots. This scheduled transmission based on the time-synchronized gate mechanism enables the convergence of critical and non-critical traffic on the same network infrastructure. The scheduled transmission is comparable with using time slots in a TDM (e.g. SDH) network.

7.1.4 Network configuration and management

Deterministic networking requires typically distinct configuration and management of network components (e.g. bridges) and end devices. This comprises aspects like transmission scheduling, network access, and redundancy mechanisms. Standards like Time Sensitive Networking (IEEE 802.1TSN) in the scope of IEEE 802.1 [8] specify this in detail based on configuration models as described in 7.2.2.4.

7.2 Deterministic networking technologies

7.2.1 Deterministic HSR

A communication system based on HSR will deliver its highest-priority data within a guaranteed maximum delay, under the condition that all applications limit the production rate of their highest priority data and leave sufficient time for the transmission delay of at least one message in each node, assuming bandwidth availability. This condition can be asserted by a cyclic transmission, for instance as the IEC 61850-9-2 Sampled Values foresees, where all sensor nodes produce periodic data at the same rate and each node introduces a predictable delay. The jitter will however not be deterministic. The low-priority traffic can be significantly delayed if unevenly-spaced, high-priority frames occupy the buffers. Grouping the time-critical traffic allows to keep a phase open for the transmission of low-priority frames and therefore to reduce their delay. This method assumes that all transmitting nodes are precisely synchronized e.g. with PTP and that the time slots are pre-allocated to define a periodic phase for time-critical data and a sporadic phase for non-time critical data. At a given point in time, the same for all nodes in the ring, each node triggers the transmission of exactly one high-priority frame prepared in a buffer, as illustrated in Figure 8. This preserves a sporadic phase of sufficient length to transmit at least one long, sporadic frame without influencing the high-priority frames.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

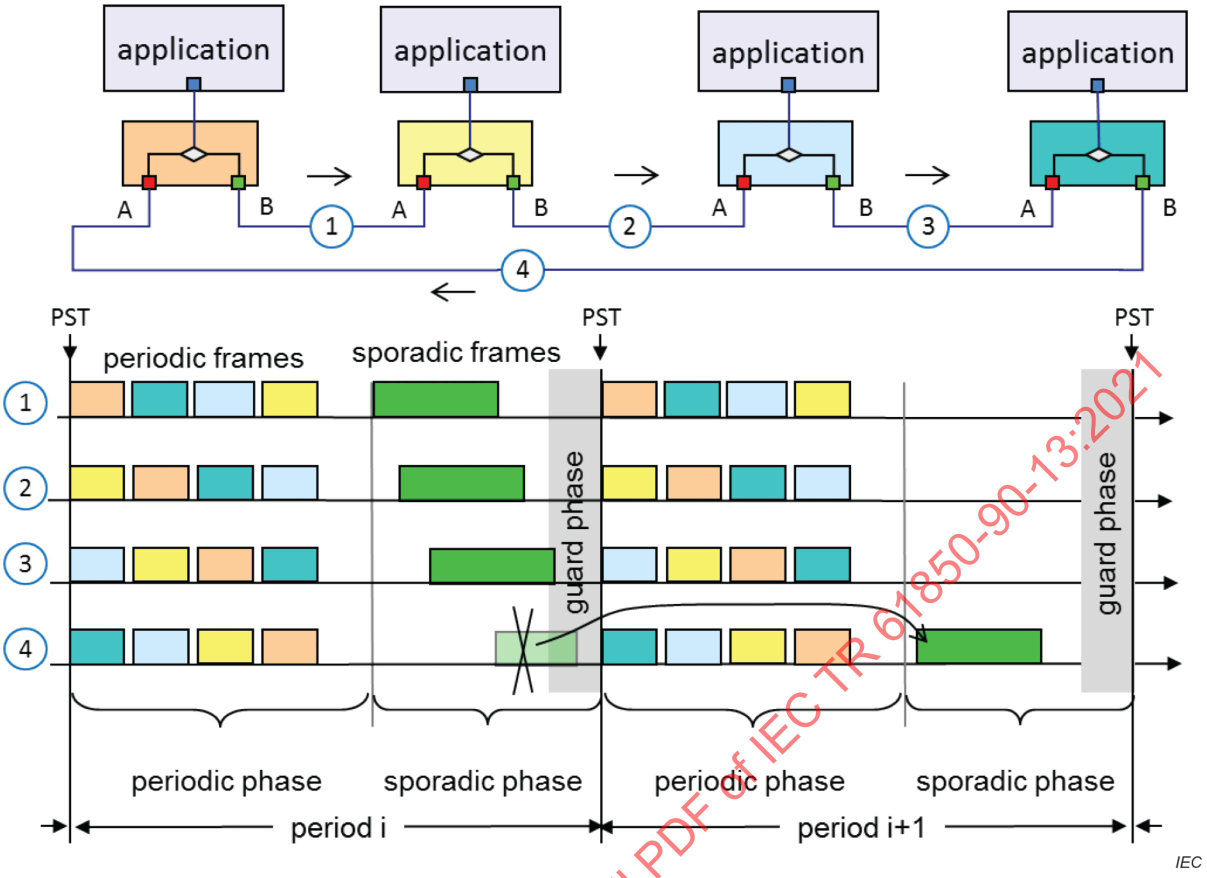


Figure 8 – Precise sending in HSR

EXAMPLE For instance, one of the transmission rates foreseen by IEC 61869-9 [9] for sampling of voltage and current values is 4,8 kHz, which corresponds to a base period of 208,3 µs. If each frame has a length of 12,8 µs at 100 Mbit/s, and if the longest low-priority frame has a size of 123 µs at 100 Mbit/s, the guard time is set to 123 µs. A deterministic delivery delay and space for one low-priority frame will be guaranteed as long as there are no more than (208 – 123)/12,8 = 6 nodes transmitting high-priority frames, leaving a reserve of 35 µs for the propagation in the nodes. An upgrade to 1 Gbit/s would allow more nodes. The clock inaccuracy between the nodes must be less than the minimum Ethernet frame duration, which is about 6 µs at 100 Mbit/s, or 600 ns at 1 Gbit/s. The example shows a period of 208,3 µs and 123 µs guard time. This is more than 50 % of the bandwidth for guard time, which can only be used if a (best-effort) frame is ready for transmission just before the guard phase begins. Only one frame (no matter of its size) can be transmitted during guard time.

The relatively high guard time for sporadic, partly best-effort frames results in the remaining low time budget for periodic, critical traffic and consequently in this low maximum number of merging units on the HSR ring. TSN faces the same problem but it can mostly be resolved by using pre-emption of best-effort frames. Not supporting frame pre-emption is expected to be a showstopper, at least on 100 Mbit/s line speed.

In a simplified arrangement, each node sends exactly one periodic frame at a fixed interval, but the frame could have a different structure in consecutive periods. The network interface stores the frame and sends it at the exact clock tick as synchronized by the PTP clock. The network interface prevents sporadic frames from being sent if the time to send them before the clock tick is insufficient (i.e. is smaller than the guard time). If the size of the transmitted frame would be unknown at ingress, at 100 Mbit/s, about half of the bandwidth should be reserved for the guard phase. HSR takes advantage of the length of the frame given in the HSR tag. This allows the logic to decide if there is sufficient time for transmission of the total frame before the start of the next period. It therefore reduces the guard phase to the size of the minimum frame size. To further save bandwidth, nodes can have different periods depending on criticality, provided the periods are a power of 2 multiple (2, 4, 8 …) of the basic period.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

7.2.2 IEEE 802.1 Time-sensitive networking (TSN)

7.2.2.1 General

The series of IEEE 802.1 TSN standards specifies deterministic services and related mechanisms, such as management and configuration, for IEEE 802-based networks.

These services are being defined to guarantee packet transport and comprise the following characteristics:

- guaranteed bounded latency;
- low bounded jitter;
- very low packet loss.

With that, the IEEE 802.1 TSN standard series enhances the best-effort capabilities of existing IEEE 802-based networks with deterministic services. To achieve this, three core mechanisms are used:

- time transport and synchronization;
- delay and latency management;
- resource and path reservation.

Every mechanism (TSN component) comprises several technologies that are defined in the underlying standards. Figure 9 depicts the relationships.

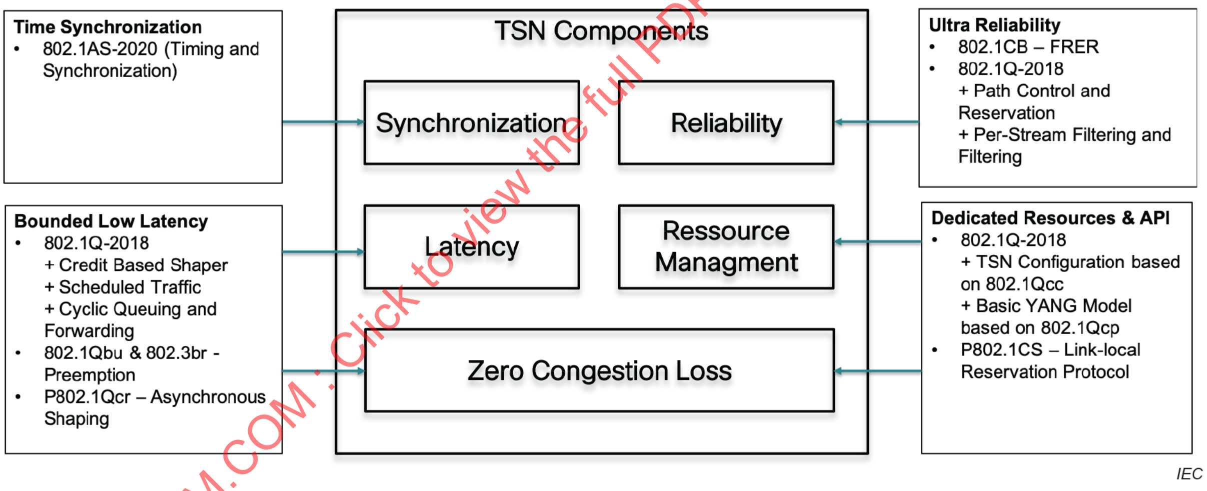

Time Synchronization
• 802.1AS-2020 (Timing and Synchronization)
TSN Components
Synchronization
Reliability
Latency
Ressource Managment
Zero Congestion Loss
Ultra Reliability
• 802.1CB – FRER
• 802.1Q-2018
+ Path Control and Reservation
+ Per-Stream Filtering and Filtering
Bounded Low Latency
• 802.1Q-2018
+ Credit Based Shaper
+ Scheduled Traffic
+ Cyclic Queuing and Forwarding
• 802.1Qbu & 802.3br - Preemption
• P802.1Qcr – Asynchronous Shaping
Dedicated Resources & API
• 802.1Q-2018
+ TSN Configuration based on 802.1Qcc
+ Basic YANG Model based on 802.1Qcp
• P802.1CS – Link-local Reservation Protocol
IEC

Figure 9 – TSN Components

The implementation of such deterministic services to establish Time-Sensitive Networking does not imply that all standards of the series must be implemented. Use cases, application requirements, and network infrastructure capabilities typically determine the selection. One approach to achieve this in a reusable and standardized way is the creation of profiles. Two TSN-profiles already exist, for Audio Video Bridging (AVB) Systems and for Fronthaul Networks. More profiles are currently underway. Especially the joint-effort between IEC and IEEE on a TSN-Profile for Industrial Automation (IEC/IEEE 60802) is important to mention here because there is a liaison between Working Group 10 of IEC Technical Committee 57 and IEEE 802.1 and requirements as well as product groups (e.g. bridges) are quite similar.

Technologies based on IEEE 802.1TSN provide the deterministic network capabilities for Ethernet networks based on IEEE 802.1 and IEEE 802.3. As a result, deployments are predominantly expected to happen in a LAN environment such as for substation networks. In addition, IEEE 802.1 TSN works as a building block for IETF DetNet-based architecture. In this context, deployments in a WAN environment present another area of use case scenarios.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

7.2.2.2 Determinism and converged networking

A key capability and benefit of deterministic networking is the convergence of critical data Streams and other traffic, typically ordinary best-effort or QoS managed traffic, on a single physical network. Networks exist in which there is no other traffic than deterministic traffic (e.g. SDH, Interbus-S). Deterministic forwarding prevents congestion by regulating the traffic in each Stream, hop-by-hop. Buffer congestion is the primary reason for packet loss in a network, and the primary reason for delivering packets late. The underlying concept of deterministic shapers and/or scheduled outputs as defined in IEEE 802.1TSN prevent the loss of critical data by allocating bandwidth and buffer resources at each hop, running at exactly the critical Stream's bandwidth, and preventing the queues from draining at line speed.

7.2.2.3 Overview of IEEE 802.1 TSN standards

7.2.2.3.1 General

The IEEE Time-Sensitive Networking task group has been working since 2012 on standardizing real-time and deterministic functionality in Ethernet [8]. TSN (Time-Sensitive Networking) is a series of IEEE 802 Ethernet sub-standards that are developed in the task group. The website of the IEEE 802.1 TSN task group provides a comprehensive overview on the status https://1.ieee802.org/tsn/. Standards with capital letters, e.g. IEEE 802.1CB, are independent standards. Lower cases represent amendments to existing standards.

Credit-based shaper mechanisms allow bandwidth reservation for high-priority traffic and ensure at the same time that best effort traffic is not displaced. The maximum interference from high-priority traffic is limited and known based on credit-based mechanism. IEEE 802.1Qav-2009 specifies *Forwarding and Queueing for Time-Sensitive Streams (FQTSS)*.

Time-aware traffic scheduling is a mechanism to achieve predictable latency. For bridged networks, this is specified in IEEE 802.1Qbv-2015 [10] (see 7.2.2.3.3). The underlying architecture is based on time-aware transmission gates associated with traffic classes and queues. The gate open and gate closed mechanisms are application triggered, time-aware and configurable via a gate control list. The precise time synchronization allows a coordinated control over all gates within the entire network including the end points, given that the endpoints implement IEEE 802.1Qbv and act in this notion as Listener and Talker.

7.2.2.3.2 IEEE 802.1AS/AS-Rev

IEEE 802.1AS-2020 (Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks) defines a Layer-2 time synchronizing service. It specifies a protocol and procedures for the transport of synchronized timing information over bridged and virtual bridged local area networks. With that, it enables end-stations to meet the requirements of time-sensitive applications including scenarios that comprise multiple Streams delivered to multiple end-stations.

7.2.2.3.3 IEEE 802.1Qbv

IEEE 802.1Qbv-2015 (Enhancements for Scheduled Traffic) is at the core of TSN and defines time-aware shaper in order to prevent interfering traffic by ensuring only one traffic class has access to the network. The standard defines up to 8 queues per port for forwarding traffic as well as transmission gates between these queues and a transmission selector that are controlled by a repeated time-based schedule. Each port has an assigned gate control list which contains a list of gate operations. These gate operations change the transmission gate state for the gate associated with each of the port's traffic class queues. Time-aware shapers block non-scheduled traffic, so that the port is idle when the scheduled traffic is scheduled for transmission. The principle of time-aware shaper deterministically schedules traffic based on queues, so-called TSN-Streams, through a bridged network. The priority field of the VLAN tag is used to assign and identify Ethernet frames to queues based on traffic classes. Using the time-aware shaping mechanism, bounded latency can be guaranteed. This standard has been integrated into IEEE Std 802.1Q-2018.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

7.2.2.3.4 IEEE 802.1Qcc

IEEE 802.1Qcc-2018 (Stream Reservation Protocol (SRP) Enhancements and Performance Improvements) specifies mechanisms to improve existing reservation protocols (e.g. SRP = Stream Reservation Protocol) to meet the requirements of automation systems.
Furthermore, it covers TSN configuration of Streams between Talker and Listener/s located within end stations. The standard defines a software interface between the user (e.g. time-sensitive application) and the network components (e.g. bridges). This user/network interface (UNI) is specified as a data model that can be applied to any protocol capable of carrying YANG or TLVs. Using the UNI, the user provides Stream requirements (e.g. latency), and the network configures resources from Talker to Listener/s to meet those requirements. It specifies three configuration models: (1) Fully Distributed Model, (2) Centralized Network / Distributed User Model, and (3) Fully Centralized Model. Table 5 maps the TSN features and capabilities to the configuration models as specified in the standard and depicts the capabilities of each model.

Table 5 – IEEE 802.1 Qcc Configuration Models

Model	Capabilities and TSN features
Fully Distributed Model	Credit-based shaper algorithm As UNI, the Stream Reservation Protocol (SRP) can be used, also to propagate configuration info to the bridges in the network
Centralized Network / Distributed User Model	Credit-based shaper algorithm Frame Pre-emption Scheduled Traffic Frame Replication and Elimination for Reliability (IEEE Std 802.1CB) AS UNI, the Stream Reservation Protocol (SRP) can be used MRP External Control can be used to exchange configuration info with the CNC
Fully Centralized Model	Credit-based shaper algorithm Frame Pre-emption Scheduled Traffic Frame Replication and Elimination for Reliability (IEEE Std 802.1CB)

Network configuration and management are crucial to put the application requirements into action. The configuration models as defined in IEEE 802.1Qcc address the dynamic configuration requirements for deterministic networks based on management entities for forwarding and queuing for time-sensitive Streams. The configuration principle is based on the concept of a Stream of data, which is sent by an end station (Talker) to one or more receiving end station (Listeners). The standard amends IEEE Std 802.1Q-2018.

7.2.2.3.5 IEEE 802.1Qbu

IEEE Std 802.1Qbu-2016 amends IEEE Std 802.1Q-2014 and defines the forwarding process that support frame pre-emption. Frame pre-emption allows one or more higher priority frames (express frames) to interrupt the transmission of a lower priority (pre-emptable) frame, the pre-emptable frame transmission being resumed and completed once the express frame(s) have been transmitted. Using frame pre-emption, bigger non-fitting frames can be split into smaller frames. Minimum fragment size is 64 bytes including CRC. Frame pre-emption reduces the size of the delay. It allows getting some amount of useful bandwidth, even if the scheduled traffic takes up most of the bandwidth, leaving relatively small windows for the best-effort traffic. In essence, pre-emption can help to reduce guard bands, and increase bandwidth utilization for best-effort traffic. The standard has been integrated into IEEE Std 802.1Q-2018.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

7.2.2.3.6 IEEE 802.1Qca

The standard IEEE 802.1Qca (Path Control and Reservation) specifies protocol extensions, procedures, and managed objects to IS-IS for providing capabilities beyond shortest path bridging for Bridged Networks in order to create multiple paths through a network. It comprises explicit path control, bandwidth reservation, and redundancy (protection, restoration) for data flows. The standard defines extensions to the Intermediate System to Intermediate System (IS-IS) protocol to establish explicit trees. It has been integrated into IEEE Std 802.1Q-2018.

7.2.2.3.7 IEEE 802.1Qci

Per-stream filtering and policing (PSFP) allows decisions and execution of frame handling and queuing per Stream by bridges and end stations implementing IEEE P802.1Qci. It requires support of Stream identification. Policy-based gate control mechanisms (gate open, gate closed) are defined to avoid traffic overload, either caused by misconfiguration or triggered by malicious attacks (DoS, DDoS). Ingress policing are typically applied per traffic class (represented by a Stream) on a respective input gate. The standard amends IEEE Std 802.1Q-2014 and it has been integrated into IEEE Std 802.1Q-2018.

7.2.2.3.8 IEEE 802.1CB

The standard IEEE 802.1CB-2017 [11] specifies a redundancy mechanism in order to increase availability. Redundant copies of the same message are sent in parallel over disjoint paths through the network. These paths are computed and set up based on the mechanism defined in IEEE 802.1Qca (Path Control and Reservation). In contrast to PRP and HSR as defined in Clause 4 of IEC 62439-3:2016, IEEE 802.1CB supports seamless redundancy on a single mesh network as well as for individual Streams. Furthermore, IEEE 802.1CB specifies Stream transformation mechanism that are useful means to enable the integration in brownfield scenarios.

7.2.2.4 TSN-models for network configuration

7.2.2.4.1 Architecture and scope

Three models of network configuration have been defined by the IEEE in the IEEE 802.1Qcc specification:

- a fully distributed model;
- a centralized network/distributed user model;
- a fully centralized model.

All these three models use the concept of a Stream that is transmitted by a Talker to one or more Listeners. Talkers and Listeners are located into end stations. The configuration information exchange between the Talker / Listener and the network is defined in a User/Network interface (UNI). The user side of the interface represents Talkers and Listeners. The network side of the interface comprises the bridges that transfer frames of the Stream from each Talker to its Listeners. Each user specifies requirements for its data, but without detailed knowledge of the network. The network obtains requirements from users, analyses the topology and TSN capabilities of bridges, and configures the bridges to meet user requirements. The network returns information about the success or failure of each Stream's configuration to the user.

7.2.2.4.2 Fully distributed model

In the fully distributed model, as depicted in Figure 10, the end stations that contain users of Streams (i.e. Talkers and Listeners) communicate the user requirements directly over the TSN user/network protocol. The network is configured in a fully distributed manner, without a centralized network configuration entity. The distributed network configuration is performed using a protocol that propagates TSN user/network configuration information along the active topology for the Stream (i.e. bridges in the tree from Talker to Listeners).

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

As user requirements propagate through each bridge, management of the bridge's resources is effectively performed locally. This local management is limited to the information that the bridge has knowledge of, and does not necessarily include knowledge of the entire network.

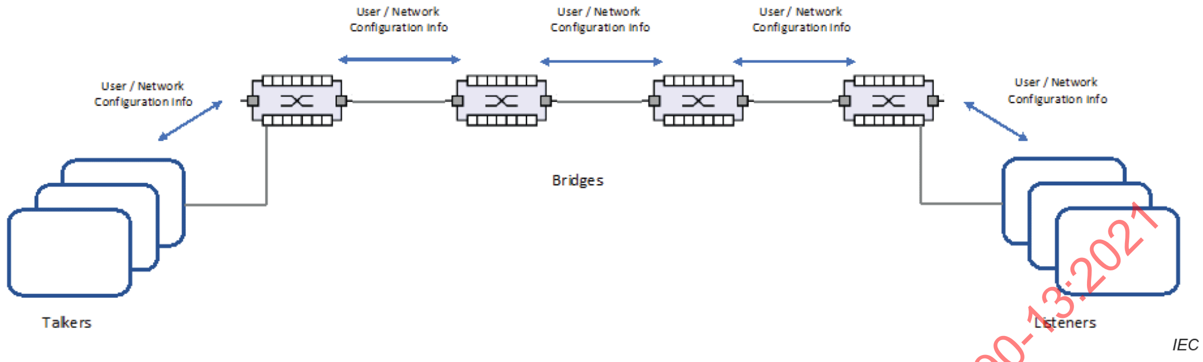

User / Network Configuration Info
User / Network Configuration Info
User / Network Configuration Info
User / Network Configuration Info
User / Network Configuration Info
Bridges
Talkers
Listeners
IEC

Figure 10 – Fully Distributed Model

The Stream Reservation Protocol (SRP) is one example of a protocol that may be used to perform the reservation task.

7.2.2.4.3 Centralized Network / Distributed User model

There are some TSN use cases that can benefit from a complete knowledge of all Streams in the network. For example, if the bandwidth for multiple Streams is greater than the available bandwidth along the shortest path between Talkers and Listeners, it is helpful to forward a subset of those Streams along a path other than the shortest. For these use cases, a centralized entity can gather information for the entire network in order to find the best configuration. The centralized network / distributed user model is similar to the fully distributed model, in that end stations communicate their Talker/Listener requirements directly over the TSN UNI. In contrast, in the centralized network / distributed user model the configuration information is directed to/from a Centralized Network Configuration (CNC) entity. All configuration of bridges for TSN Streams is performed by this CNC using a network management protocol. The CNC has a complete view of the physical topology of the network, as well as the capabilities of each bridge. This enables the CNC to centralize complex computations. The CNC can exist in either an end station or a bridge. The CNC knows the address of all bridges at the edge of the network (those with an end station connected). The CNC configures those edge bridges to act as a proxy, transferring Talker/Listener information directly between the edge-bridge and the CNC, rather than propagate the information to the interior of the network. Figure 11 shows the hybrid model.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

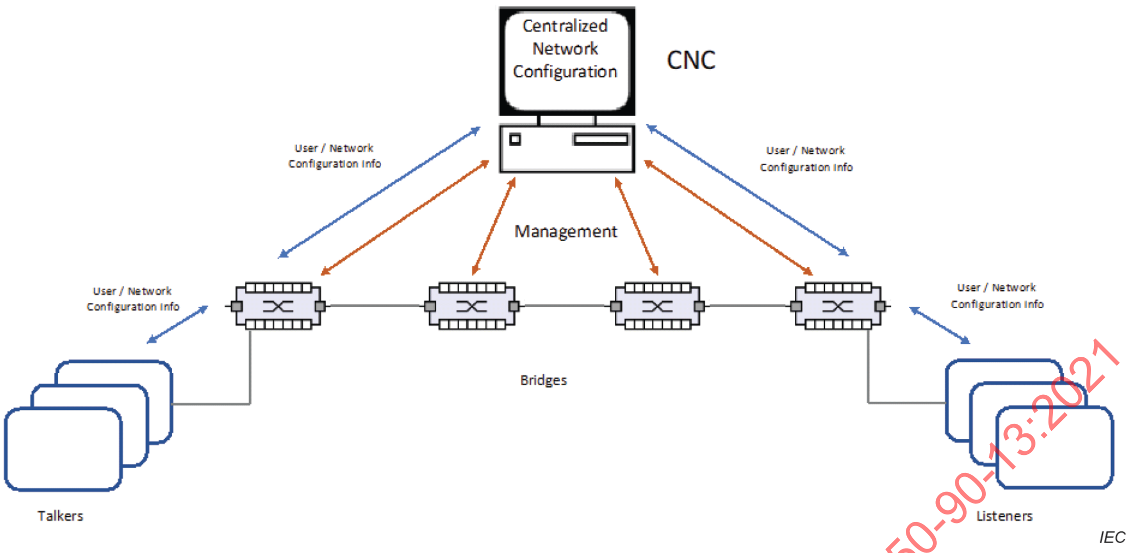

Centralized Network Configuration
CNC
User / Network Configuration Info
User / Network Configuration Info
Management
User / Network Configuration Info
User / Network Configuration Info
Bridges
Talkers
Listeners
IEC

Figure 11 – Hybrid Model

7.2.2.4.4 Fully centralized model

Many TSN use cases require significant user configuration in the end stations that act as Talkers and Listeners. For example, in many automotive and industrial control applications, the timing of physical inputs and outputs is determined by the physical environment under control, and the timing requirements for TSN Streams are derived from that I/O timing. In some use cases, these I/O timing requirements can be computationally complex, requiring detailed knowledge of the application software/hardware within each end station. In order to accommodate this sort of TSN use case, the fully centralized model enables a Centralized User Configuration (CUC) entity to discover end stations, retrieve end station capabilities and user requirements, and configure TSN features in end stations. The centralized model is shown in Figure 12. The protocols that the CUC uses for this purpose are specific to the user application, outside the scope of this document. From a network perspective, the primary difference between the fully centralized model and the centralized network / distributed user model is that all user requirements are exchanged between the CNC and CUC. Therefore, the TSN UNI exists between the CNC and CUC.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

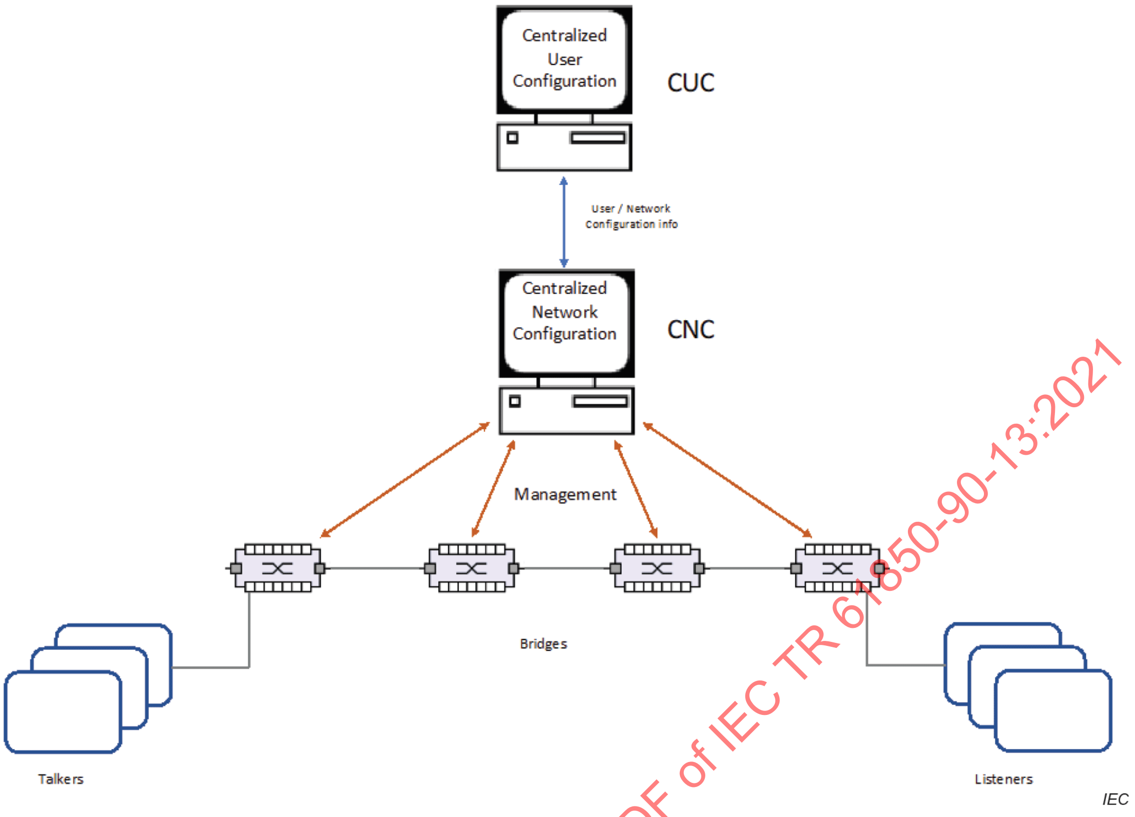

Centralized User Configuration
CUC
User / Network Configuration info
Centralized Network Configuration
CNC
Management
Bridges
Talkers
Listeners
IEC

Figure 12 – Central Model

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

A configuration workflow would typically comprise the following steps:

a) the end stations transmit the Stream quality of service requirements to the corresponding CUC component;

b) these requirements are sent to the CNC component via a well-defined interface;

c) the CNC component processes the calculations to define data paths, schedules and other deterministic network configurations in order to meet the quality of services requirements for the Streams;

d) in case of successful calculation (the deterministic network can meet the requirements of the application/user/end stations), the following steps are executed by the CNC:

- configuration of the bridges in the TSN network based on the requirements regarding quality of service of the end stations (user); technically, this is handled using managed objects (bridges) and network management protocols
- return of relevant status and Stream definition information to the CUC via the north-bound interface

e) CUC starts to configure end stations based on the CNC and CUC calculations and definitions pertaining to the Streams.

The fully centralized model enables an automated approach of network management based on application requirements. The information exchange between CUC and CNC allows network configuration based on configuration data already available in domain specific engineering and configuration tools.

7.2.2.5 TSN scheduling challenges

The core technology introduced by TSN (in IEEE 802.1Qbv) to enable deterministic latency eliminates the interference to each critical-flow Stream from all other traffic (critical and best-effort) by sending critical Streams within separate time-slots ("protected window" in TSN parlance), with "gates" to allow the critical Streams, while blocking all other Streams, during the time-slot.

If the inter-bridge latencies were all zero, the same time-slot could be used at all bridges; however, this is not reality, and the cable latencies (typically 5 microseconds per km) and the processing time in bridges could be many milliseconds for large utility networks. This link propagation delay and residence time is addressed in the scope IEEE 802.1Qcc. This link propagation delay is addressed in the scope of the IEEE 802.1 TSN configuration process as a necessary input parameter for scheduling flows.

Scheduling the time-slots allocations for all the critical-flow Streams, for all the network bridges, is not in the scope of the IEEE 802.1 TSN standards. The IEEE 802.1 TSN standards provide the interfaces and managed objects to enable scheduling but leave this task intentionally to the equipment vendors in order to foster innovation in this critical problem space. This topic, being a significant mathematical challenge, would be expected to be attractive to the academic community and this has materialized with their reports supporting the (expected) difficulty of the scheduling problem ("run times of days"). Scheduling algorithms and tools are available from equipment vendors allowing network simulation and planning as critical success criteria for deployments. Until scheduling algorithms have been developed, implemented, and tested with documented performance to show the ability of TSN as an underlying technology for DetNet to handle the inter-substation critical-flow Streams of different size utility networks, this technology should be considered experimental for WAN-based use cases.

7.2.3 IETF DetNet

7.2.3.1 Scope of DetNet

In 2015, a new Internet Engineering Task Force Working Group, DetNet, was approved [12]. The core objective of DetNet is to translate the advantages of TSN in the bridged world into the routed world, and thus expand the physical and logical reach of a "critical flow" to an enterprise-sized network, which would enable new use cases such as large control loops.

The scope of the IETF DetNet Working Group comprises the following key areas:

- overall architecture;
- specification of the Data Plane (IP and/or MPLS support);
- data flow information model;
- YANG models (link capabilities and link resources);
- security definitions;
- use cases.

It is part of the scope definitions that a DetNet-based network is always under a single administrative control or within a closed group of administrative control entities. This concept is different from the Internet, which is based on a vast group of domains. The objective of DetNet-based services is to provide the capabilities for data flows with extremely low packet loss rated and bounded end-to-end delivery latency. Essential DetNet building blocks are congestion protection, service protection, and explicit routes.

DetNet is relying on underlying technologies such as TSN to provide deterministic layer-2 capabilities. This includes challenges such as those mentioned in 7.2.2.5.

7.2.3.2 Overview on IETF DetNet documents

Table 6 contains the current documents.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

Table 6 – DetNet documents

Document [12]	Scope
RFC 8578	Deterministic Networking Use Cases
RFC 8557	Deterministic Networking Problem Statement
RFC 8655	Deterministic Networking Architecture
RFC 8938	DetNet Data Plane Framework
draft-ietf-detnet-flow-information-model-13	DetNet Flow Information Model
RFC 8939	DetNet Data Plane: IP
draft-ietf-detnet-tsn-vpn-over-mpls-05	DetNet Data Plane: IP over MPLS
draft-ietf-detnet-mpls-over-udp-ip-08	DetNet Data Plane: IP over IEEE 802.1 Time Sensitive Networking (TSN)
draft-ietf-detnet-tsn-vpn-over-mpls-05	DetNet Data Plane: MPLS
draft-ietf-detnet-security-13	DetNet Data Plane: MPLS over UDP/IP
draft-ietf-detnet-yang-09	DetNet Data Plane: IEEE 802.1 Time Sensitive Networking over MPLS
draft-ietf-detnet-security-04	Deterministic Networking (DetNet) Security Considerations
draft-ietf-detnet-topology-yang-00	Deterministic Networking (DetNet) Topology YANG Model

Status information is available from: http://datatracker.ietf.org/wg/detnet/

Technologies based on DetNet are specified for use cases and deployments in WAN-based scenarios. RFC 8578 (Deterministic Networking Use Cases) [12] contains use cases from a number of industries including power utilities which have common requirements such as bounded latency and guaranteed bandwidth in order to provide deterministic networking capabilities.

7.2.4 Other technologies

7.2.4.1 General

The following paragraphs are based on individual contributions. VSN is a technology used for WAN-based use cases, while EtherCat (IEC 61158 [all parts]) is a fieldbus technology using a master/slave approach applied in industrial automation networks, a typical LAN environment. The applicability of these technologies depends on the use cases (e.g. protection) and the related requirements (e.g. L2 multicast) and is not in the scope of this paragraph. In this sense, this paragraph on Other technologies does not list all technologies available and does not claim completeness. Prominent examples for other deterministic protocols are real-time fieldbus technologies for LANs such as Profinet RT (IEC 61784-2 [13]) and Ethernet Powerlink. The fieldbus types are clustered into Communication Profile Families (CPFs) within the IEC 61158 standard series. They are designed and specified for an industrial automation and process control environment.

7.2.4.2 VSN (Virtual SDH Network)

7.2.4.2.1 General

This technology addresses the challenges encountered when trying to use corporate Ethernet networks for inter-substation tele-protection traffic.

This solution works by using a Pseudowire packetizing technology (IETF RFC 3985 [14]) to have all the substation's traffic mapped into a single Ethernet stream, since this can be transported deterministically, using low-latency tunnels, to provide almost the same performance as conventional SDH networks.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

Since the streams can come from packetized SDH signals, a network using this technology could be considered a "Virtual SDH Network"; i.e. it would have the same functionality, and could have the same (except for a negligible increase in latency) performance.

7.2.4.2.2 Reserved time slots

Each tele-protection circuit (whether TDM or Ethernet access) can have its own dedicated timeslots within the Ethernet stream (using the normal SDH container pointers).

7.2.4.2.3 Network latencies

There is only a single Ethernet stream between each connected substation, with each stream comprising a well-behaved train of regularly-spaced constant-length packets.

As an example, a 155 Mbit/s STM-1 VSN stream at 10 GbE would likely comprise an approximate 0,1µs-length packet each 5 µs approximately.

Since such a stream will arguably have no significant impact on other network traffic (for the example above delaying other traffic by at most 0,1 µs), it can be given unique access to the network's top-priority egress queues.

Assuming the use of "strict-priority" queue schedulers, this guarantees the worst-case PDV for each network egress port (being the time for a lower-priority packet to complete an already-started egress (e.g. 1,2 µs for a 1 518 Byte packet at 10 GbE)).

(For the likely concern that a defective VSN source could block other services, particularly NMS, the network's VSN ports should have their CIR/PIR rates configured appropriately.)

7.2.4.2.4 Network example

Figure 13 shows an IT/OT network being used to provide deterministic substation-to-substation communications. The heavy blue paths denote the main and backup -inter-substation packetized SONET streams. With each network bridge only required to handle a single well-behaved stream, the stream can be assigned the bridge's top-priority queue to assure only low-microsecond latency degradations from the queuing of the other converged traffic. Note that the normal SONET/SDH path-protection(failover) is used.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

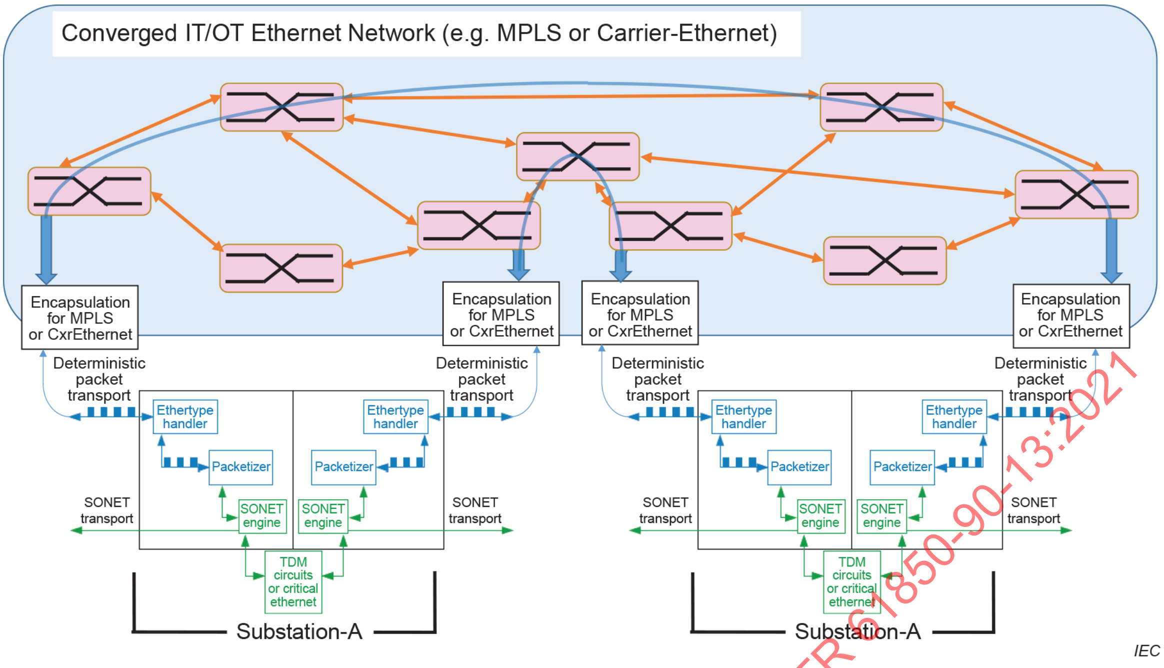

Converged IT/OT Ethernet Network (e.g. MPLS or Carrier-Ethernet)
Encapsulation for MPLS or CxrEthernet
Deterministic packet transport
Ethertype handler
Packetizer
SONET engine
SONET transport
TDM circuits or critical ethernet
Substation-A
IEC

Figure 13 – Topology of a WAN network using VSN

7.2.4.3 EtherCAT

7.2.4.3.1 Operating principle

EtherCAT is a real-time Ethernet technology that aims to maximize the utilization of the full duplex Ethernet bandwidth. Medium access control employs the master/slave principle, where the master node (typically the control system) sends the Ethernet frames to the slave nodes, which uses data elements in the frames on the path between the master to the slave node. The forwarding principle is fixed and does not depend upon addresses but transfers the incoming data to the next open port. EtherCAT is IEC 61158 standard and consists of application and data link layer specifications. The DLL definitions can be used in combination with different application layer protocols.

From an Ethernet point of view, an EtherCAT segment is a single Ethernet device which receives and sends standard ISO/IEC 8802-3 Ethernet frames. However, this Ethernet device is not limited to a single Ethernet controller with downstream microprocessor, but may consist of a number of EtherCAT slave devices. Incoming Ethernet frames reading data from the Ethernet frame and/or inserting their own data into the frame before transferring the frame to the next slave device. This procedure utilizes the full duplex capability of Ethernet: both communication directions are operated independently with reading and writing by the slaves on the outbound path and just pass the frame on the inbound path. Communication between a master device and an EtherCAT segment do not require IEEE 802.1 elements. EtherCAT allows efficient forwarding in a line topology as well as in combination with spurs.

EtherCAT allows ring topologies and master redundancy for very reliable applications. The protocol allows a simple extension to compensate the loss of measurement data with a very small overhead.

EtherCAT DLL is defined in IEC 61158-3-12 [15] and IEC 61158-4-12 [16].

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

7.2.4.3.2 EtherCAT device interaction

In order to achieve maximum performance, the Ethernet frames should be processed directly "on the fly". A slave node identifies relevant commands and executes them accordingly while the frames are passed on. The service interface is not the classical send and receive messages but a read and write command structure at DL. Thus, devices have an addressable memory that can be accessed with read or write services, either with direct device access or with a group access method. Several EtherCAT DLPDUs can be embedded within an Ethernet frame, each DLPDU addressing a cohesive data section as shown in Figure 14.

NOTE 1 EtherCAT can be implemented using standard Ethernet components at the master side.

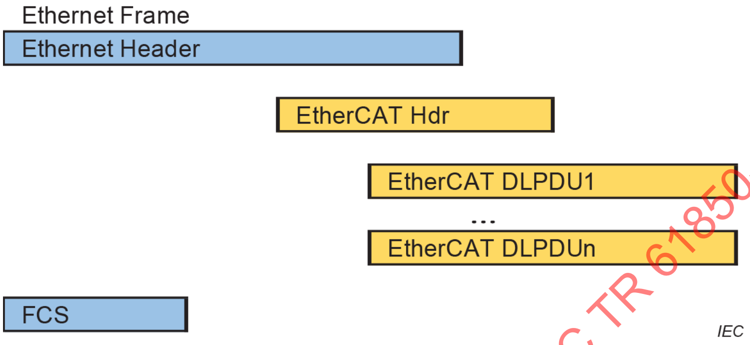


Figure 14 – Frame Structure

Multiple EtherCAT segments can be connected to one or several bridges according to IEEE 802.1Q. The Ethernet MAC address of the first node within the segment is used for addressing the EtherCAT segment. The stream concept of IEEE 802.1Q shall be used to map EtherCAT data transmission which uses two streams per EtherCAT segment. One of them is used to transfer the data from the master to the segment and the other to send data back to the master. Thus, EtherCAT can be embedded in IEEE 802.1Q networks with the advantage of handling a group of devices with a single pair of streams and reduces the load of frame processing in the control system significantly.

NOTE 2 Further addressing details are given in the data-link layer service definition (see IEC 61158-3-12 [15]).

Several EtherCAT DLPDUs can share a single Ethernet frame. The nodes can be addressed individually by these DLPDUs. This method leads to better utilization of the Ethernet bandwidth compared to individual Ethernet frames to and from each slave node.

For further increase of efficiency, a slave node may also support logical address mapping. The process data can be inserted anywhere within a logical address space. If an EtherCAT DLPDU is sent that contains read or write services for a certain process image area located at the corresponding logical address the nodes insert the data at or extract the data from their appropriate place(s) within the process data, as noted in Figure 15. The master can assemble a completely sorted logical process image via a single EtherCAT DLPDU, independent of the physical wiring order of the slave devices.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

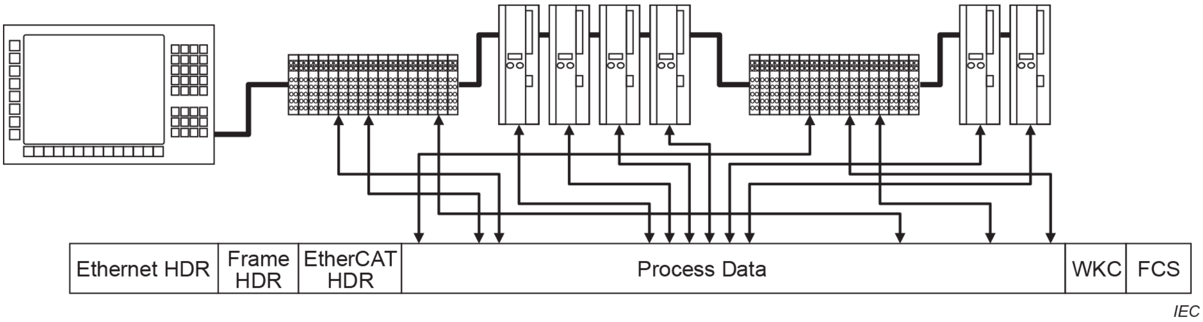


Figure 15 – Mapping data in a single EtherCAT DLPDU

7.2.4.3.3 Error detection principles

EtherCAT master and slave nodes (DLEs) check the Ethernet frame check sequence (FCS) to determine whether a frame is received correctly. Since one or several slaves may modify the frame during the transfer, the FCS is checked by each node on reception and recalculated during retransmission. If a slave detects a checksum error, the slave does not repair the FCS but flags the master by incrementing an error counter, so that the source of a single fault can be located precisely within the topology.

When reading data from or writing data to an EtherCAT DLPDU, the addressed slave increments a working counter (WKC) positioned at the end of the DLPDU. By comparing the working counter with the expected number of accessing slave nodes, a master can check whether the expected number of nodes have processed the corresponding DLPDU.

7.2.4.3.4 Synchronization

EtherCAT enables synchronization using distributed clock (DC) which enables all slave devices to have the same time. The first slave device within the segment that contains a clock is the clock reference. Its clock is used to synchronize the slave clocks of the other slave devices and of the master device. The master device sends synchronisation at certain intervals in which the slave device containing the reference clock enters its current time. The slave devices with slave clocks then read the time from the same DLPDU with a read-multiple-write service.

Since each slave introduces a small delay in the outgoing and return direction (within the device and also on the physical link), the propagation delay time between reference clock and the respective slave clock shall be considered during the synchronisation of the slave clocks. For measuring the propagation delay, the master device sends a broadcast to the receive time register of port 0, which causes each slave to save the time when the Ethernet Frame was received in the outgoing direction and on the way back. The master can read these saved times and set up a delay register accordingly. This method is similar to the Pdelay measurement as described in IEEE 802.1AS but the residence time of the device is included in the delay value of the following link. This can be done as there is no delay variation in the forwarding of Ethernet frames beyond the clock jitter between the two paths.

The DC control loop to adjust the local clock to the reference clock is implemented in hardware. Thus, a high frequency synchronization can be achieved which may cause only small errors even if there is a statistical error in the forwarding of frames. The synchronization DLPDU can share the Ethernet frame with the process data which allows synchronisation rates of 1 ms or smaller which results in an accuracy in a range of 100 ns between two clocks.

External synchronisation is accomplished by mechanisms specified in IEEE 802.1AS. Any device with external communication interfaces may contain a boundary clock. The slave with the master clock is synchronized to the boundary clock. EtherCAT segments shall have only one active grandmaster clock at any time.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

7.2.4.3.5 Discovery and Configuration

EtherCAT supports a simple procedure to detect the nodes connected. This is done by the so-called auto increment addressing (position address) of nodes. Each slave device increments the 16-bit address field as the DLPDU transits the slave device; that device which receives a DLPDU with an address field of value 0 is the one being addressed. Thus, the number of increments is the number of slaves connected.

This topology-based addressing mechanism has the advantage that no slave node addresses need to be set manually at the slaves and a replacement of a node does not require any settings. The topology can be discovered very easily by this mode combined with the port link status of the slave.

The configuration can be done offline with an xml-based device description language ESI. The ESI files can be used to determine the expected structure of a system. Only a few number of DL parameters is needed as EtherCAT does not allow a number of options. The configuration with the ESI files and the user settings will be stored in an ENI file (EtherCAT Network Information). This is the blueprint for the physical topology and will be checked at start-up. The ESI information is stored in the device. Thus, a plug and play setup is possible as well.

7.2.4.3.6 Mapping onto OSI Basic Reference Model

EtherCAT services are described using the principles, methodology and model of ISO/IEC 7498-1 (OSI) [17]. The OSI model provides a layered approach to communications standards, whereby the layers can be developed and modified independently. The EtherCAT specification defines functionality from top to bottom of a full OSI communications stack. Functions of the intermediate OSI layers, layers 3 to 6, are consolidated into either the EtherCAT data-link layer or the DL user of the EtherCAT data-link layer.

The data-link layer provides basic time-critical support for data communications among devices connected. The term "time-critical" is used to describe applications having a time window, within which one or more specified actions are required to be completed with a defined level of certainty. Failure to complete specified actions within the time window risks failure of the applications requesting the actions, with attendant risk to equipment, plant and possibly human life. The EtherCAT architecture allows to reduce this risk significantly.

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

8 Co-existence and interoperability with existing and emerging technologies (and how to address technology changes)

8.1 Relation of TSN to technologies such as SDN (Software Defined Networking) and NFV (Network Function Virtualization)

Software Defined Networking (SDN) and Network Function Virtualization (NFV) are technologies related to computer networking. With SDN, the network and functionality that depends on them is centrally managed rather than being managed in a distributed fashion. The component, which encapsulates the management functions, is called controller. This could be a sort of similarity with TSN, specifically with the centralized model as specified in IEEE 802.1Qcc. On the other hand, TSN does not mandate the entire architecture and the implementation of network elements such as bridges. Conventional technology might co-exist with TSN and scheduling mechanisms in single device. Furthermore, the distributed configuration model for TSN networks, as defined in IEEE 802.1 Qcc, would not meet the criterias of Software Defined Networking at all.

TSN is no replacement for SDN, and SDN is not replacement for TSN. TSN and SDN are different technologies with different objectives. SDN does not provide Deterministic Networking capabilities intrinsically.

Network Function Virtualization (NFV) is a concept based on virtualization technologies as used in modern Enterprise-IT systems to virtualize network nodes to provide communication services.

Network functions are executed in a virtual machine environment, which makes hardware-based appliances obsolete. Currently, there is no real relation to TSN where the network nodes are hardware-based devices such as bridges.

8.2 Relation and interoperability to existing architectures for high-availability and redundancy based on PRP/HSR

Within the IEEE 801.TSN toolbox, the standard IEEE 802.1CB-2017 [11] (Frame Replication and Elimination for Reliability) specifies procedures, managed objects, and protocols for bridges and end systems that enable identification and replication of packets for redundant transmission, identification of duplicate packets, and elimination of duplicate packets. The standard contains two paragraphs (HSR sequence tag, PRP sequence trailer) with the intent to enable interworking functions between end systems using the Redundancy tag (according to IEEE 802.1CB) and the HSR sequence tag and/or the PRP sequence trailer.

From the perspective of HSR and PRP, specified in IEC 62439-3, the efforts to enable interworking functions are pending. A liaison between both working groups is in place. It is based on the fact that that the mechanisms in IEEE 802.1CB are similar to the seamless redundancy mechanisms of High-Availability Seamless Redundancy (HSR) and the Parallel Redundancy Protocol (PRP). In IEEE 802.1CB, the HSR tag and the PRP trailer are called out as alternate mechanisms to be used to mark Ethernet frames with sequence numbers.

8.3 Relation and interoperability to existing WAN-architectures based on MPLS (IP/MPLS, MPLS-TP)

IETF DetNet, which is currently a Work In Progress, is defining several mapping methods to interoperate with network technologies like MPLS, TSN and IP. One RFC has been published and six IETF drafts are being developed [12]:

- DetNet Data Plane: IP;
- DetNet Data Plane: IP over MPLS;
- DetNet Data Plane: IP over IEEE 802.1 Time Sensitive Networking (TSN);
- DetNet Data Plane: MPLS;
- DetNet Data Plane: MPLS over IEEE 802.1 Time Sensitive Networking (TSN);
- DetNet Data Plane: MPLS over IP;
- DetNet Data Plane: IEEE 802.1 Time Sensitive Networking over MPLS.

These drafts will cover the support of deterministic and non-deterministic traffics over a Detnet network.

8.4 Brownfield deployment options

Brownfield deployment refers to use case scenarios in which devices that are not conformant to deterministic standards and/or profiles are attached to a network with deterministic characteristics and devices, typically bridges. As an example, an IED, which is not conformant to a profile based on IEEE 801.TSN shaping and configuration mechanisms, is connected to a substation network, which is TSN-enabled. Because of equipment life cycle, product roadmaps and other deployment specifics, these scenarios are foreseeable and will exist in many deployments. It is paramount to understand and address these scenarios when defining profiles, for instance a TSN-Profile for Utility Automation, similar to the work in the JWG IEC/IEEE 60802 (Time-sensitive networking profile for Industrial Automation). It should be allowed and supported to extend brownfield installations and to integrate brownfield devices. Brownfield traffic QoS requirements shall be met without any limitation. A key requirement should be that the network characteristics and underlying functions such as shaping mechanisms do not impact the IED functions and the application behaviour. In other words, the characteristics of the network are transparent and should not affect the functions of an IED and the Substation Automation Solution in general. Conversely, this means that the network traffic which is already based on deterministic technologies, say TSN-shaping mechanism, is protected from the

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

brownfield traffic to minimize interferences. There are two options to achieve this required behaviour:

– based on network (bridge) configuration, addressing the composition, capabilities and configuration of the devices attached to the network – a pre-configured gateway mechanism;

– based on automated traffic (and Stream) identification and mapping to pre-defined traffic types and underlying classes.

More details would require technology decisions and selections. As an example, IEEE P802.1CBdb as part of the development in the IEEE 802.1TSN group, allows enhanced Stream identification and would enable standard based Stream translation to support traffic management mechanisms like ingress policing, traffic scheduling, congestion management, mapping to traffic classes which includes the handling of brownfield traffic.

Figure 16 depicts a logical architecture how to integrate Non-TSN capable devices (e.g. IEDs) into a TSN-enabled substation automation network. The gateway in this depiction is a logical component which could be hosted on a dedicated device or as a bridge function.

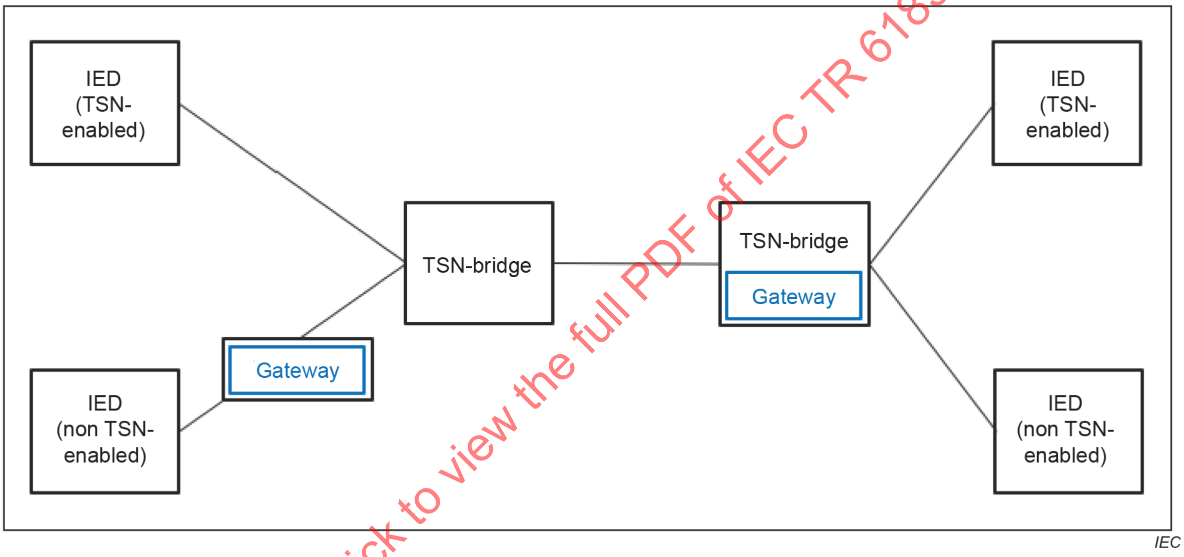


Figure 16 – Brownfield configuration options

IECNORM.COM : Click to view the full PDF of IEC TR 61850-90-13:2021

The convergence of networks within a substation could also be achieved using VLANs and TSN in conjunction. TSN, in this case, is used to implement network slicing which allows for isolation of different networks on the same infrastructure. Each VLAN will be allocated the required bandwidth and no VLAN traffic will interfere with the traffic of the other VLANs, thanks to IEEE 802.1Qbv. This offers a bandwidth guaranty per VLAN. The only limitation is that no VLAN could benefit from the unused bandwidth of the other VLANs. This mechanism allows the convergence of networks without changes of the VLANs substation configuration and IEDs.

8.5 Migration path

Ideally, deterministic networking advantages could be utilized to the maximum if both end devices and networking devices are deterministic networking capable. However, in the substation automation world, simultaneous migration of the whole install base of both end devices and networking devices is likely impractical. Therefore, the migration process will be gradual, and the most typical expected scenario will be as follows:

a) First, networking devices get replaced with deterministic-networking-capable ones with no change in the IED's domain;

b) Brownfield support (i.e. deterministic networking gateway functionality) described in the previous clause is utilized to maintain the existing install base of end devices;