

CONSOLIDATED VERSION

VERSION CONSOLIDÉE



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

**Réseaux de communication industriels – Réseaux de haute disponibilité pour
l'automatisation –
Partie 1: Concepts généraux et méthodes de calcul**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 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.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

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 also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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: csc@iec.ch.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

CONSOLIDATED VERSION

VERSION CONSOLIDÉE



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

**Réseaux de communication industriels – Réseaux de haute disponibilité pour
l'automatisation –
Partie 1: Concepts généraux et méthodes de calcul**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040; 35.040; 35.100.01

ISBN 978-2-8322-3220-0

Warning! Make sure that you obtained this publication from an authorized distributor. Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.
--

REDLINE VERSION

VERSION REDLINE



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

**Réseaux de communication industriels – Réseaux de haute disponibilité pour
l'automatisation –
Partie 1: Concepts généraux et méthodes de calcul**

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope	8
2 Normative references	8
3 Terms, definitions, abbreviations, acronyms, and conventions	9
3.1 Terms and definitions	9
3.2 Abbreviations and acronyms	16
3.3 Conventions	17
3.3.1 General conventions	17
3.3.2 Conventions for state machine definitions.....	18
3.3.3 Conventions for PDU specification.....	18
3.4 Reserved network addresses	18
4 Conformance requirements (normative).....	19
4.1 Conformance to redundancy protocols	19
4.2 Conformance tests.....	19
4.2.1 Concept.....	19
4.2.2 Methodology	20
4.2.3 Test conditions and test cases	20
4.2.4 Test procedure and measuring	21
4.2.5 Test report.....	21
5 Concepts for high availability automation networks (informative).....	22
5.1 Characteristics of application of automation networks.....	22
5.1.1 Resilience in case of failure.....	22
5.1.2 Classes of network redundancy	22
5.1.3 Redundancy maintenance	23
5.1.4 Comparison and indicators	23
5.2 Generic network system.....	25
5.2.1 Network elements	25
5.2.2 Topologies.....	27
5.2.3 Redundancy handling.....	32
5.2.4 Network recovery time.....	33
5.2.5 Diagnosis coverage.....	33
5.2.6 Failures	33
5.3 Safety	34
5.4 Security.....	34
6 Classification of networks (informative)	34
6.1 Notation	34
6.2 Classification of robustness	35
7 Availability calculations for selected networks (informative)	36
7.1 Definitions	36
7.2 Reliability models	37
7.2.1 Generic symmetrical reliability model.....	37
7.2.2 Simplified symmetrical reliability model.....	38
7.2.3 Asymmetric reliability model.....	39
7.3 Availability of selected structures	40

7.3.1	Single LAN without redundant leaves	40
7.3.2	Network without redundant leaves	40
7.3.3	Single LAN with redundant leaves	41
7.3.4	Network with redundant leaves	41
7.3.5	Considering second failures	42
7.4	Caveat	44
8	RSTP for High Availability Networks: configuration rules, calculation and measurement method for ~~deterministic~~ predictable recovery time ~~in a ring topology~~	44
8.1	General	44
8.2	Deployment and configuration rules for the ring topology	45
8.3	Calculations for fault recovery time in a ring	45
8.3.1	Dependencies and failure modes	45
8.3.2	Calculations for non-considered failure modes	45
8.3.3	Calculations for the considered failure modes	45
8.4	Timing measurement method	46
8.4.1	Measurement of T_{PA}	46
8.4.2	Measurement of T_L	47
8.4.3	Measurement of $(T_{TC} + T_F)$	48
8.4.4	System test example	50
8.5	RSTP topology limits and maximum recovery time	51
8.5.1	RSTP protocol parameters	51
8.5.2	RSTP-specific terms and definitions	51
8.5.3	Example of a small RSTP tree	53
8.5.4	Assumption on TxHoldCount	54
8.5.5	Worst case topology and radius determination	54
8.5.6	Method to determine the worst case radius in case of a ring-ring architecture	55
8.5.7	Worst case radius of an optimized multilayer architecture	56
8.5.8	Approximated upper bond reconfiguration time for RSTP networks	57
	Bibliography	60
	Figure 1 – Conformance test overview	20
	Figure 2 – General network elements (tree topology)	25
	Figure 3 – Link Redundancy Entity in a Doubly Attached Node (DAN)	26
	Figure 4 – Example of tree topology	28
	Figure 5 – Example of linear topology	28
	Figure 6 – Example of ring topology	29
	Figure 7 – Example of a partially meshed topology	30
	Figure 8 – Example of fully meshed topology	30
	Figure 9 – Single LAN structure without redundant leaf links	31
	Figure 10 – Single LAN structure with redundant leaf links	31
	Figure 11 – Redundant LAN structure without redundant leaf links	32
	Figure 12 – Redundant LAN structure with redundant leaf links	32
	Figure 13 – General symmetrical fault model	37
	Figure 14 – Simplified fault model	38
	Figure 15 – Asymmetric fault model	39
	Figure 16 – Network with no redundancy	

Figure 17 – Network with no single point of failure	42
Figure 18 – Network with resiliency to second failure	43
Figure 19 –Test rig for T_{PA} measurement	47
Figure 20 –Test rig for T_L measurement.....	48
Figure 21 –Test rig for $(T_{TC} + T_F)$ measurement.....	49
Figure 22 –Test rig for system test	50
Figure 23 – Diameter and Bridge Max Age	53
Figure 24 – Worst path determination.....	55
Figure 25 – Example ring-ring topology	55
Figure 26 – Example multilayer topology	57
Table 1 – Examples of application grace time	22
Table 2 – Examples of redundancy protocols.....	24
Table 3 – Code assignment for the <TYPE> field.....	35
Table 4 – Code assignment for the <PLCYleaf> field	35
Table 5 – Code assignment for the <TPLGY> field.....	35
Table 6 – Code assignment for the <ITYPE> field.....	36

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – HIGH AVAILABILITY AUTOMATION NETWORKS –

Part 1: General concepts and calculation methods

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.

DISCLAIMER

This Consolidated version is not an official IEC Standard and has been prepared for user convenience. Only the current versions of the standard and its amendment(s) are to be considered the official documents.

This Consolidated version of IEC 62439-1 bears the edition number 1.2. It consists of the first edition (2010-02) [documents 65C/583/FDIS and 65C/589/RVD], its amendment 1 (2012-06) [documents 65C/684/FDIS and 65C/691/RVD] and its amendment 2 (2016-02) [documents 65C/834/FDIS and 65C/841/RVD]. The technical content is identical to the base edition and its amendments.

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendments 1 and 2. Additions are in green text, deletions are in strikethrough red text. A separate Final version with all changes accepted is available in this publication.

International Standard 62439-1 has been prepared by subcommittee 65C: Industrial Networks, of IEC technical committee 65: Industrial-process measurement, control and automation.

This edition includes the following significant technical changes with respect to IEC 62439 (2008):

- adding a calculation method for RSTP (rapid spanning tree protocol, IEEE 802.1Q),
- adding two new redundancy protocols: HSR (High-availability Seamless Redundancy) and DRP (Distributed Redundancy Protocol),
- moving former Clauses 1 to 4 (introduction, definitions, general aspects) and the Annexes (taxonomy, availability calculation) to IEC 62439-1, which serves now as a base for the other documents,
- moving Clause 5 (MRP) to IEC 62439-2 with minor editorial changes,
- moving Clause 6 (PRP) was to IEC 62439-3 with minor editorial changes,
- moving Clause 7 (CRP) was to IEC 62439-4 with minor editorial changes, and
- moving Clause 8 (BRP) was to IEC 62439-5 with minor editorial changes,
- adding a method to calculate the maximum recovery time of RSTP in a restricted configuration (ring) to IEC 62439-1 as Clause 8,
- adding specifications of the HSR (High-availability Seamless Redundancy) protocol, which shares the principles of PRP to IEC 62439-3 as Clause 5, and
- introducing the DRP protocol as IEC 62439-6.

The French version of this standard has not been voted upon.

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

A list of the IEC 62439 series can be found, under the general title *Industrial communication networks – High availability automation networks*, on the IEC website.

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

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

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

INTRODUCTION

The IEC 62439 series specifies relevant principles for high availability networks that meet the requirements for industrial automation networks.

In the fault-free state of the network, the protocols of the IEC 62439 series provide ISO/IEC 8802-3 (IEEE 802.3) compatible, reliable data communication, and preserve determinism of real-time data communication. In cases of fault, removal, and insertion of a component, they provide deterministic recovery times.

These protocols retain fully the typical Ethernet communication capabilities as used in the office world, so that the software involved remains applicable.

The market is in need of several network solutions, each with different performance characteristics and functional capabilities, matching diverse application requirements. These solutions support different redundancy topologies and mechanisms which are introduced in IEC 62439-1 and specified in the other Parts of the IEC 62439 series. IEC 62439-1 also distinguishes between the different solutions, giving guidance to the user.

The IEC 62439 series follows the general structure and terms of IEC 61158 series.

INDUSTRIAL COMMUNICATION NETWORKS – HIGH AVAILABILITY AUTOMATION NETWORKS –

Part 1: General concepts and calculation methods

1 Scope

The IEC 62439 series is applicable to high-availability automation networks based on the ISO/IEC 8802-3 (IEEE 802.3) (Ethernet) technology.

This part of the IEC 62439 series specifies

- the common elements and definitions for other parts of the IEC 62439 series;
- the conformance test specification (normative);
- a classification scheme for network characteristics (informative);
- a methodology for estimating network availability (informative);
- the configuration rules, calculation and measurement method for a deterministic recovery time in RSTP.

2 Normative references

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

IEC 60050-191:1990, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

IEC 61158-6-10, *Industrial communication networks – Fieldbus specifications – Part 6-10: Application layer protocol specification – Type 10 elements*

ISO/IEC 8802-3:2000, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

IEEE 802.1Q, *IEEE standards for local and metropolitan area network. Virtual bridged local area networks*

IEEE 802.1D:2004, *IEEE standard for local Local and metropolitan area networks Media Access Control (MAC) Bridges*

IETF RFC 791, *Internet Protocol*; available at <<http://www.ietf.org>>

3 Terms, definitions, abbreviations, acronyms, and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-191, as well as the following, apply

3.1.1

availability (performance)

ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided

NOTE 1 This ability depends on the combined aspects of the reliability performance, the maintainability performance, and the maintenance support performance.

NOTE 2 Required external resources, other than maintenance resources, do not affect the availability performance of the item.

[IEV 191-02-05]

3.1.2

channel

layer 2 connection between two end nodes which consists of one or more paths (for redundancy) between end nodes

3.1.3

common mode failure

failure that affects all redundant elements for a given function at the same time

3.1.4

complete failure

failure which results in the complete inability of an item to perform all required functions

[IEV 191-04-20]

3.1.5

connection

logical relationship between two nodes

3.1.6

coverage

probability that a failure is discovered within a time short enough for redundancy to handle it, also expressing the percentage of failures caught up by redundancy vs. total number of failures

3.1.7

cut-through switching

a technology in which a switching node starts transmitting a received frame before this frame has been fully received

3.1.8

degradation failure

failure which is both a gradual failure and a partial failure

[IEV 191-04-22]

3.1.9 dependability

collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance

NOTE Dependability is used only for general descriptions in non-quantitative terms.

[IEV 191-02-03]

3.1.10 device

physical entity connected to the network composed of communication element and possibly other functional elements

NOTE Devices are for instance nodes, routers and switches.

3.1.11 doubly attached node

node that has two ports for the purpose of redundant operation

3.1.12 edge port

port of a switch connected to a leaf link

3.1.13 end node

node which is producer or consumer of application data

NOTE For the purpose of the IEC 62439 series, further specification is given in 0.

3.1.14 error

discrepancy between a computed, observed or measured value or condition and the specified or theoretically correct value or condition

NOTE 1 An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.

NOTE 2 The French term "erreur" may also designate a mistake (see IEC 191-05-25).

[IEV 191-05-24, modified]

3.1.15 failure

termination of the ability of an item to perform a required function

NOTE 1 After a failure, the item has a fault.

NOTE 2 "Failure" is an event, as distinguished from "fault", which is a state.

NOTE 3 This concept as defined does not apply to items consisting of software only.

[IEV 191-04-01]

3.1.16 fault

state of an item characterized by its inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

NOTE A fault is often the result of a failure of the item itself, but may exist without prior failure.

[IEV 191-05-01]

3.1.17

fault recovery time

time from the fault event, to the time when the network regains its required communication function in the presence of the fault

NOTE After fault recovery, the network is operating in a degraded mode using some of the redundancy elements, so it has reduced fault resilience, and may not be able to recover from a second fault.

3.1.18

frame

unit of data transmission on an ISO/IEC 8802-3 MAC (Media Access Control) that conveys a protocol data unit (PDU) between MAC service users

[IEEE 802.1Q, modified]

3.1.19

(instantaneous) failure rate

limit, if it exists, of the quotient of the conditional probability that the instant of a failure of a non-repaired item falls within a given time interval $(t, t + \Delta t)$ and the duration of this time interval, Δt , when Δt tends to zero, given that the item has not failed up to the beginning of the time interval

[IEV 191-12-02]

NOTE The failure rate is the reciprocal number of the MTTF when the failure rate is constant over the lifetime of one item.

3.1.20

inter-switch link

link between two switches

3.1.21

inter-switch port

port of a switch connected to another switch via an inter-switch link

3.1.22

LAN

A layer 2 broadcast domain in which MAC addresses are unique and can be addressed from any other device belonging to that broadcast domain

NOTE 1 A VLAN allows multiplexing several LANs on the same network infrastructure.

NOTE 2 In the context of redundancy, a network may consist of several LANs operated in redundancy, in which case it is called a redundant LAN.

3.1.23

leaf link

link between an end node and the LAN

NOTE For the purpose of the IEC 62439 series, further specification is given in 5.2.1.3.

3.1.24

linear topology

topology where the switches are connected in series, with two switches each connected to only one other switch and all other switch each connected to two other switches (that is, connected in the shape of a line)

NOTE 1 This topology corresponds to that of an open ring.

NOTE 2 This configuration is sometimes named “daisy chain”. The IEC 62439 series does not use the term “daisy chain” because of possible confusion with the term “daisy chain” used elsewhere for busses. From the wiring point of view they require two different implementations.

[IEC 61918, 3.1.39, modified]

3.1.25

link

physical, point-to-point, generally duplex connection between two adjacent nodes

[ISO/IEC 11801, 3.1.51, modified]

NOTE “Link” is different from “bus”, which is a broadcast physical medium.

3.1.26

Link Redundancy Entity

entity at layer 2 that hides port redundancy from the upper layers, by forwarding to the upper layers the frames received from the active redundant ports as if they came from a single port, and by forwarding to the active redundant ports a frame coming from the upper layers

3.1.27

link service data unit

data transported within a protocol layer on behalf of the upper layer

NOTE The link service data unit in an Ethernet frame is the content of the frame located between the Length/Type field and the Frame Check Sequence.

3.1.28

mean failure rate

mean of the instantaneous failure rate over a given time interval $\lambda(t_1, t_2)$.

[IEV 191-12-03]

NOTE The IEC 62439 series uses “failure rate” for the meaning of “mean failure rate” defined by IEV 191-12-03.

3.1.29

mean operating time between failures

MTBF

expectation of the operating time between failures

[IEV 191-12-09]

3.1.30

mean time to failure

MTTF

expectation of the time to failure

[IEV 191-12-07]

3.1.31

mean time to recovery

MTTR

expectation of the time to recovery

[IEV 191-13-08, modified]

3.1.32

mesh topology

topology where each node is connected with three or more inter-switch links

3.1.33

message

ordered series of octets intended to convey information

NOTE Normally used to convey information between peers at the application layer.

3.1.34

network

communication system consisting of end nodes, leaf links and LAN(s)

NOTE A network may have more than one LAN for the purpose of redundancy.

3.1.35

node

network entity connected to one or more links

NOTE Nodes may be either a switch or an end node or both.

[IEC 61784-2, 3.1.16, modified]

3.1.36

partial failure

failure which results in the inability of an item to perform some, but not all, required functions

3.1.37

path

set of links and switches joined in series

NOTE There may be two or more paths between two switches to provide redundancy.

3.1.38

plant

system that depends on the availability of the automation network to operate

EXAMPLE Plants can be power plants, printing machines, manufacturing systems, substations, vehicles.

3.1.39

port

connection point of a node to the network

[ISO/IEC 8802-3, modified]

NOTE 1 This definition is different from a TCP port or a UDP port, which the IEC 62439 series qualifies explicitly if necessary.

NOTE 2 A port includes the layer 1 and 2 implementation.

3.1.40

recovery

event when the network regains the ability to perform its required communication function after a disruption

NOTE Examples of disruptions could be a fault or removal and reinsertion of a component.

3.1.41

recovery time

time period between disruption and recovery

3.1.42

redundancy

existence in an item of two or more means for performing a required function

[IEV 191-15-01]

NOTE In the IEC 62439 series, the existence of more than one path (consisting of links and switches) between end nodes.

3.1.43
reinstatement recovery time

time to reinstate the original, or pre-fault, network configuration, including original operating and management states in each device

3.1.44
reliability

ability of an item to perform a required function under given conditions for a given time interval

[IEV 191-02-06]

NOTE 1 It is generally assumed that the item is in a state to perform this required function at the beginning of the time interval.

NOTE 2 The term “reliability” is also used as a measure of reliability performance (see IEC 191-12-01).

3.1.45
repair

action taken for the re-establishment of the specified condition

3.1.46
repair recovery time

delay between the start of the repair action and the completion of repair of the faulty element such that the network has regained both its required communication function and its required fault resilience

NOTE 1 This time includes any network down time caused by the repair process, for example a network outage to replace a switch with several good ports and one faulty port.

NOTE 2 This time does not include re-instatement time to return the network from its backup mode of operation to the original mode of operation.

3.1.47
ring link

link that connects two switches of a ring

3.1.48
ring port

port of a switch to which a ring link is attached

3.1.49
ring topology

topology in which each node is connected in series to two other nodes

NOTE 1 Nodes are connected to one another in the logical shape of a circle.

NOTE 2 Frames are passed sequentially between active nodes, each node being able to examine or modify the frame before forwarding it.

3.1.50
robustness

behaviour of the network in face of failures

3.1.51
root bridge

switch with the lowest value of an RSTP Bridge Identifier parameter in the network

[IEEE 802.1D]

3.1.52

route

layer 3 communication path between two nodes

3.1.53

single failure criterion

capacity of a system that includes redundant components to maintain its full functionality upon one failure of any of its components, prior to maintenance or automatic recovery

3.1.54

single point of failure

single failure point

component whose failure would result in failure of the system and is not compensated for by redundancy or alternative operational procedure

NOTE A single point of failure or single failure point causes a common mode failure. It may be caused by a design error in the redundant elements or by an external cause that affects all redundant elements in the same way, e.g. extreme temperature.

3.1.55

singly attached node

node that has only one port to a LAN

3.1.56

stand-by redundancy

redundancy wherein a part of the means for performing a required function is intended to operate, while the remaining part(s) of the means are inoperative until needed

[IEV 191-15-03]

NOTE This is also known as dynamic redundancy.

3.1.57

star topology

topology in which all devices are connected to a central node

3.1.58

store-and-forward switching

a technology in which a switching node starts transmitting a received frame only after this frame has been fully received

3.1.59

switch

switch node

MAC bridge as defined in IEEE 802.1D

NOTE The term “switch” is used as a synonym for the term “switch node”.

3.1.60

switching end node

an end node and a switch combined in one device

3.1.61

systematic failure

failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

NOTE 1 Corrective maintenance without modification will usually not eliminate the failure cause.

NOTE 2 A systematic failure can be induced by simulating the failure cause.

[IEV 191-04-19]

3.1.62
topology

pattern of the relative positions and interconnections of the individual nodes of the network

[derived from IEC 61918, 3.1.67]

NOTE Additional aspects such as the delay, attenuation and physical media classes of the paths connecting network nodes are sometimes also considered to be properties of the topology.

3.1.63
tree topology

topology in which any two nodes have only one path between them and at least one switch is attached to more than two inter-switch links

3.1.64
trunk portion

part of a switched LAN that carry traffic for several end nodes

3.1.65
upper layer entity

parts of the protocol stack immediately above the redundancy handling layer

3.1.66
worst case recovery time

maximum expected recovery time amongst all faults and for all allowed configurations

NOTE This delay is important for a network designer to indicate which aspects of the network need special treatment to minimize communication disruption.

3.1.67
bridge
device connecting LAN segments at layer 2 according to IEEE 802.1D

NOTE The words “switch” and “bridge” are considered synonyms, the word “bridge” is used in the context of standards such as RSTP (IEEE 802.1D), PTP (IEC 61588) or IEC 62439-3 (PRP & HSR).

3.1.68
network recovery time

time span from the moment of the first failure of a component or media inside the network to the moment the network reconfiguration is finished and from which all devices that are still able to participate in network communication are able to reach all other such devices in the network again

NOTE When a network redundancy control protocol (like RSTP) reconfigures the network due to a fault, parts of the network may still be available and communication outages may vary in time and location over the whole network. In the calculations, only the worst case scenario is considered.

3.2 Abbreviations and acronyms

BRP	Beacon Redundancy Protocol, IEC 62439-5
BPDU	Bridge management Protocol Data Unit, according to IEEE 802.1D
CRP	Cross-network Redundancy Protocol, see IEC 62439-4
DAN	Doubly Attached Node
DRP	Distributed Redundancy Protocol, see IEC 62439-6
DUT	Device Under Test

HSR	High-availability Seamless Redundancy, see IEC 62439-3
IP	Internet Protocol, layer 3 of the Internet Protocol suite
IT	Information Technology
LAN	Local Area Network
LRE	Link Redundancy Entity
MAC	Media Access Control
MRP	Medium Redundancy Protocol, see IEC 62439-2
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTFN	Mean Time To Failure of Network
MTTFS	Mean Time To Failure of System
MTTR	Mean Time To Repair
MTTRP	Mean Time To Repair Plant
OUI	Organizational Unique Identifier
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PRP	Parallel Redundancy Protocol, see IEC 62439-3
QAN	Quadruply Attached Node
RFC	Request For Comments of the Internet Society
RRP	Ring-based Redundancy Protocol, see IEC 62439-7
RSTP	Rapid Spanning Tree Protocol, see IEEE 802.1D
SAN	Singly Attached Node
SRP	Serial Redundancy Protocol, see IEC 62439-3
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol, layer 4 of the Internet Protocol suite
UDP	User Datagram Protocol, layer 4 of the Internet Protocol suite

3.3 Conventions

3.3.1 General conventions

The protocols specified in the IEC 62439 series follow the structure defined in IEC/TR 61158-1.

General guidelines are specified in IEC 61158-6-10, 3.7.

3.3.2 Conventions for state machine definitions

The IEC 62439 series follows the conventions used in IEC 61158-6-10, 3.8. The following is a summary.

- Each state is described by one table, with a separate row for each transition that may cause a state change.
- Transitions are defined as events that may carry arguments and be subject to conditions.
- The action field expresses the action that takes place in case the event is fired.
- For space reasons, the event and the actions are in the same cell.
- The right column indicates the next state that is entered after the action is finished.

3.3.3 Conventions for PDU specification

PDUs are described according to specification RFC 791, Appendix B.

In particular:

- bits, octets and arrays are numbered starting with 0;
- the “Network Byte Ordering” (big-endian, most significant octet first) convention is observed.

IEC 61158-6-10 distinguishes bit identification from the bit offset.

EXAMPLE In a bit string of 8 bits, the rightmost bit (Least Significant Bit) is labelled bit 0, but it has bit offset 7 within the bit string octet.

When specifying data objects rather than PDUs, the bit identification according to IEC 61158-6 series is used. Consequently, bits of a bit string are specified in ascending bit identification, although they are transmitted in the opposite order.

3.4 Reserved network addresses

The following is a summary of the network addresses reserved for the purpose of the IEC 62439 series, whilst the prescribed values are specified in the respective parts of the IEC 62439 series.

For the purpose of the IEC 62439 series, the OUI 00-15-4E has been reserved by IEEE. All bands within this OUI are reserved for the IEC 62439 series. The following bands are assigned:

- MRP (see IEC 62439-2) uses 00-15-4E, band 00-00-xx.
- PRP (see IEC 62439-3) uses 00-15-4E, band 00-01-xx.
- **HSR (see IEC 62439-3) uses 0x892F.**
- CRP (see IEC 62439-4) uses an IP multicast MAC address.
- BRP (see IEC 62439-5) uses 00-15-4E, band 00-02-xx.
- DRP (see IEC 62439-6) uses 00-15-4E, band 00-03-xx.
- **RRP (see IEC 62439-7) uses 00-E0-91-02-05-99.**

For the purpose of the IEC 62439 series, the following Ethertypes (see IEEE 802a) have been reserved by IEEE:

- MRP (see IEC 62439-2) uses 0x88E3.
- PRP (see IEC 62439-3) uses 0x88FB.
- CRP (see IEC 62439-4) uses 0x0800 (IP) with UDP port 3622.
- BRP (see IEC 62439-5) uses 0x80E1.
- DRP (see IEC 62439-6) uses 0x8907.
- **RRP (see IEC 62439-7) uses 0x88FE.**

4 Conformance requirements (normative)

4.1 Conformance to redundancy protocols

A statement of compliance with a part of the IEC 62439 series shall be stated as:

- compliance to IEC 62439-2 (MRP), or
- compliance to IEC 62439-3 (PRP), or
- compliance to IEC 62439-4 (CRP), or
- compliance to IEC 62439-5 (BRP),
- compliance to IEC 62439-6 (DRP),
- **compliance to IEC 62439-7 (RRP).**

A conformance statement shall be supported with appropriate documentation as defined in 4.2. The supported protocols and options shall be specified as PICS, in the format: PICS_62439-X_supported options.

EXAMPLE PICS_62439-5_BlockingSupported.

4.2 Conformance tests

4.2.1 Concept

The concept of this conformance test is to verify the capabilities of a device under test (DUT) against a consistent set of indicators under simulated worst case conditions. The conformance test shall assert the interoperability of devices which claim compliance with the same protocol.

The IEC 62439 series contains specifications that are to be observed by different actors:

- the device builder, who designs and tests a compliant interface;
- the network manager, who defines the topology;
- the user of the network, who respects the operational limitations.

A device sold as being fully compliant with a protocol of the IEC 62439 series could underperform if the network configuration rules are not observed when it is used.

Figure 1 gives an overview of the conformance test related to the protocols of the IEC 62439 series.

NOTE Conformance test implementation and conformance test execution are not defined in the IEC 62439 series.

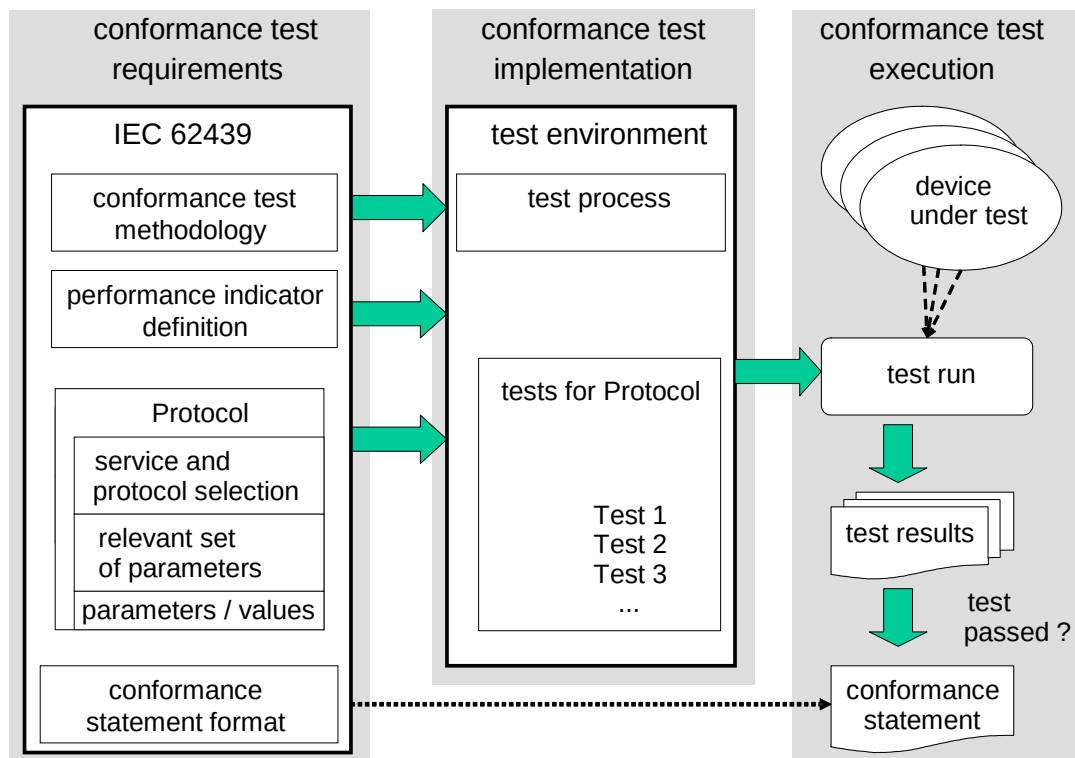


Figure 1 – Conformance test overview

IEC 328/10

4.2.2 Methodology

Test cases shall be developed in a way that tests are repeatable. Test results shall be documented and shall be used as the basis for the conformance statement.

Conformance tests of a device shall include, as appropriate, the verification of

- correctness of the specified functionality,
- network related indicator values,
- device related indicator values.

The performance indicator values of the protocol and of the device under test shall be used.

NOTE 1 A description of a conformance testing process is given in ISO/IEC 9646 series.

NOTE 2 It is assumed that the quality of the test cases guarantees the interoperability of a tested device. If any irregularities are reported the test cases will be adapted accordingly.

4.2.3 Test conditions and test cases

Test conditions and test cases shall be defined and documented based on a specific redundancy protocol. This shall include the following indicators, when applicable:

- number of nodes;
- network topology;
- number of switches between nodes;
- type of traffic.

For each measured indicator, test condition and test case documents shall be prepared and shall describe:

- test purpose;

- test setup;
- test procedure;
- criteria for compliance.

Test set-up describes the equipment set-up necessary to perform the test including measurement equipment, device under test, auxiliary equipment, interconnection diagram, and test environmental conditions.

Parts of the test environment may be emulated or simulated. The effects of the emulation or simulation shall be documented.

The test procedure describes how the test should be performed, which also includes a description of a specific set of indicators required to perform this test. The criteria for compliance define test results accepted as compliance with this test.

4.2.4 Test procedure and measuring

The measured indicators shall include, when applicable:

- redundancy recovery time,
- impact of redundancy overhead on normal operation.

The test procedure shall be based on the principles of 4.2.3.

The sequence of measuring actions to complete a test run shall be provided.

The number of independent runs of the test shall be provided.

The method to compute the result of the test from the independent runs shall be provided if applicable.

4.2.5 Test report

The test report shall contain sufficient information so that the test can be repeated.

The test report shall contain at least

- a) the reference to the conformance test methodology according to 4.2.2,
- b) the reference to the performance indicator definitions,
- c) the reference to the redundancy protocol of the IEC 62439 series,
- d) a description of the conformance test environment including network emulators, measurement equipment and the person or organization responsible for the test execution, and the date of testing,
- e) a description of the device under test, its manufacturer, and hardware and software revision,
- f) the number and type of devices connected to the network together with the topology,
- g) a reference to the test case specifications,
- h) the measured values,
- i) a statement regarding compliance with the redundancy protocol.

5 Concepts for high availability automation networks (informative)

5.1 Characteristics of application of automation networks

5.1.1 Resilience in case of failure

Plants rely on the correct function of the automation system. Plants tolerate a degradation of the automation system for only a short time, called the grace time. The network recovery time should be shorter than the grace time since the application typically needs to perform additional tasks (related to protocol and data handling, waiting for the next scheduled communication cycle etc.) before the plant is back to the fully operational state. Applications can be distinguished by their grace time, as the Table 1 shows.

Table 1 – Examples of application grace time

Applications	Typical grace time s
Uncritical automation, e.g. enterprise systems	20
Automation management, e.g. manufacturing, discrete automation	2
General automation , e.g. process automation, power plants	0,2
Time-critical automation, e.g. synchronized drives	0,020

Some plants have stricter requirements when they are required to operate continuously, having no idle period during which the plant may be maintained or reconfigured. In this case, the grace time holds for the stricter requirement, for instance dictated by the hot-swapping of parts of the equipment.

Automation systems may contain redundancy to cope with failures. Methods differ on how to handle redundancy, but their key performance factor is the recovery time, i.e. the time needed to restore operation after occurrence of a disruption. If the recovery time exceeds the grace time of the plant, protection mechanisms initiate a (safe) shutdown, which may cause significant loss of production and plant operational availability.

A key characteristic of recovery is its determinism, i.e. the guarantee that the recovery time remains below a certain value as long as the basic assumptions (single failure at a time, no common mode of failure, less than maximum system extension) are met. **A network provides a deterministic recovery if it is possible to calculate a finite worst case recovery time of a given topology when a single failure occurs.**

Whenever operation depends on the correct function of the automation network, it may become necessary to increase the availability of the network.

Raising availability by increasing reliability of the elements or improving maintenance is outside the scope of the IEC 62439 series. The IEC 62439 series considers only protocols that introduce redundancy and automatically reconfigure redundant network elements in case of failure.

5.1.2 Classes of network redundancy

5.1.2.1 General

The IEC 62439 series considers two classes of network redundancy:

- a) redundancy managed within the network;
- b) redundancy managed in the end nodes.

NOTE The IEC 62439 series does not consider redundancy of the end nodes themselves, i.e. the use of redundant end nodes, since this is highly application specific.

5.1.2.2 Redundancy managed within the network

Redundancy within a network has been applied to wide area networks and to legacy field busses.

Layer 3 routers (not considered in the IEC 62439 series) calculate alternate routes upon link failures. The corresponding protocols are well proven as part of the IP suite, but the recovery time is in the order of dozen of seconds, if not minutes, depending on the topology. Such recovery times are only tolerated by the most benign applications.

Automation networks usually operate within one single Local Area Network (LAN), i.e. messages for operation are threaded through layer 1 repeaters or layer 2 switches, but do not cross routers. Messages to and from the outside world over routers or firewalls do exist, but are considered to be uncritical.

Classically, redundancy within a LAN is handled by protocols that react to loss of links and switches by reconfiguring the LAN, using redundant links and switches, such as the Rapid Spanning Tree Protocol (RSTP) according to IEEE 802.1D.

Improved Layer 2 redundancy protocols build on similar principles as RSTP, but provide a faster recovery by exploiting the assumption that the automation network has a ring topology. End nodes are unmodified automation nodes.

5.1.2.3 Redundancy managed in the end nodes

Further improvements in recovery time require managing of redundancy in the end nodes, by equipping the end nodes with several, redundant communication links. In general, doubly attached end nodes provide sufficient redundancy. In this type of redundancy, no assumption about the switches within the LAN is made.

For time-critical applications such as synchronized drives, the parallel operation of disjoint networks provides a seamless recovery, but requires complete duplication of the network. Some critical plants also require doubly attached nodes in order to cope with a failure of a leaf link, even if they do not require a very short recovery time.

5.1.3 Redundancy maintenance

Redundancy can be affected by latent faults, which can be detected by testing. The testing interval allows availability to be estimated. All protocols provide the means to test the redundant or spare components and report detected failures to the network management.

5.1.4 Comparison and indicators

The protocols specified in the IEC 62439 series offer:

- a maximum, deterministic and guaranteed recovery time (that may depend on the topology),
- transparency of the actual communication towards the application under all circumstances, and
- for doubly attached nodes, interoperability with singly attached devices (off-the-shelf, IT equipment).

Table 2 compares some characteristics of some redundancy protocols, ordered by recovery time.

Table 2 – Examples of redundancy protocols

Protocol	Solution	Frame Loss	Redundancy protocol	End node attachment	Network Topology	Recovery time for the considered failures
IP	IP routing	Yes	Within the network	Single	Single meshed	> 30 s typical not deterministic
STP	IEEE 802.1D	Yes	Within the network	Single	Single meshed	> 20 s typical not deterministic
RSTP	IEEE 802.1D	Yes	Within the network	Single	Single meshed, ring	Can be deterministic following the rules of Clause 8
CRP	IEC 62439-4	Yes	In the end nodes	Single and double	Doubly meshed, cross-connected	1 s worst case for 512 end nodes
DRP	IEC 62439-6	Yes	Within the network	Single and double	Ring, double ring	100 ms worst case for 50 switches
MRP	IEC 62439-2	Yes	Within the network	Single	Ring, meshed	500 ms, 200 ms, 30 ms or 10 ms worst case for 50 switches depending on the parameter set and network topology
BRP	IEC 62439-5	Yes	In the end nodes	Double	Doubly meshed, connected	4,8 8,88 ms worst case for ~~500~~ 100 end nodes
RRP	IEC 62439-7	Yes	In the end nodes	Double (switching end nodes)	Single ring	8 ms in 100BASEX, 4 ms in 1000BASEX
PRP	IEC 62439-3	No	In the end nodes	Double	Doubly meshed, independent	0 s
HSR	IEC 62439-3	No	In the end nodes	Double	Ring, meshed	0 s

NOTE For the redundancy protocols specified in the IEC 62439 series, the recovery times in Table 2 are guaranteed when using the settings and parameters specified in the associated part of IEC 62439 series. Faster recovery times may be achieved using different settings and parameters under the user's responsibility.

The indicators for the different solutions include, when applicable:

- fault recovery time,
- repair recovery time,
- reinstatement recovery time,
- worst case recovery time,
- impact on normal operation.

The fault cases include:

- failure of the current active network manager (if it exists) followed by repair and reinstatement;
- failure of the current source of network time (if it exists), followed by repair and reinstatement.

Subclause 5.2 generalizes the above considerations and introduces a classification scheme.

5.2 Generic network system

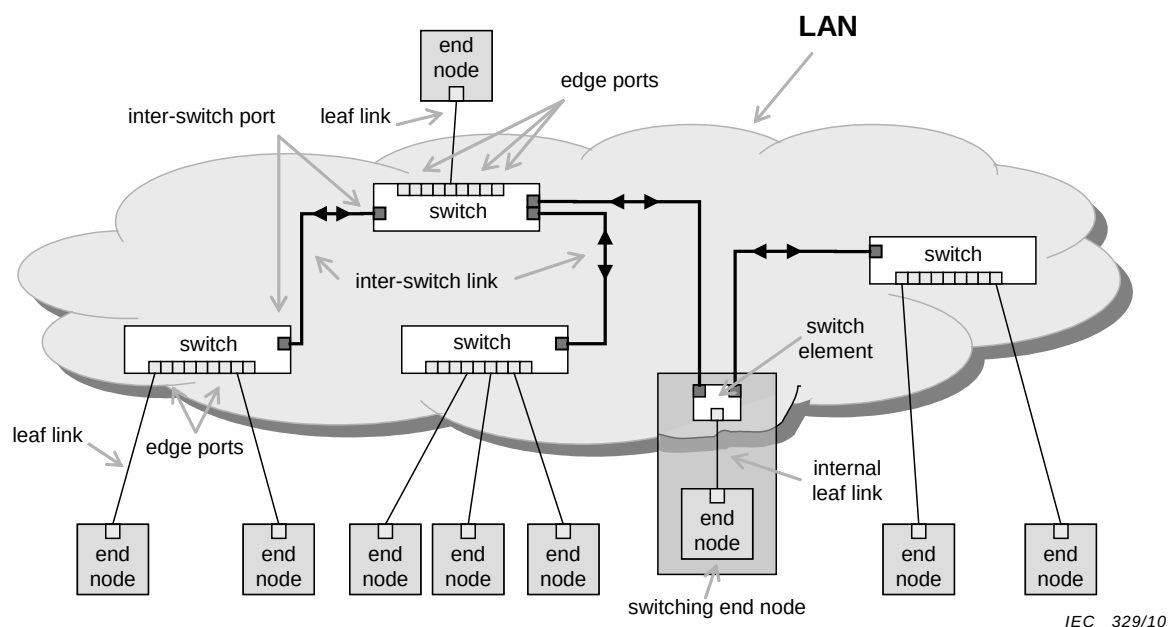
5.2.1 Network elements

5.2.1.1 General

The generic network is modelled with the functional elements listed below and represented in Figure 2.

- End nodes
- Leaf links
- Switches (with edge ports and inter-switch ports)
- Inter-switch links
- Switching end nodes

The LAN consists of all network components, except the end nodes and leaf links.



NOTE Edge ports are shaded in light grey, inter-switch ports are shaded in dark grey, inter-switch links are drawn with a thick line, leaf links drawn with a thin line.

Figure 2 – General network elements (tree topology)

5.2.1.2 End node

An end node requires one connection port to the LAN for its normal operation.

The connection port of an end node is connected to an edge port of a switch in a LAN by a leaf link.

5.2.1.3 Leaf link

A leaf link connects an end node with a LAN.

This connection may be internal to a device, in the case where the device combines the end node and switch or LRE functionality (switching end node in Figure 2).

5.2.1.4 Inter-switch link

An inter-switch link connects the switches within a LAN.

There may be several inter-switch links between two switches to increase availability.

5.2.1.5 Switches

Switches are layer 2 connecting elements as defined in IEEE 802.1D.

NOTE Bridges according to IEEE 802.1D are called switches in the IEC 62439 series.

Switches are connected to each other by inter-switch links.

A switch is connected to a leaf link through an edge port.

5.2.1.6 Switching end node

A switch element may be implemented within the same piece of physical equipment as the end node. Although this makes the end node appear to be a doubly attached node, internally the operating principle is different, since there is no need for a Link Redundancy Entity because the switch element plays this role.

5.2.1.7 End nodes with multiple attachments

End nodes may have more than one connection port for redundancy. Connection ports of an end node may be connected to the same LAN or may be connected to different LANs.

End nodes with more than one attachment require a Link Redundancy Entity (LRE) in their communication stack to hide redundancy from the application, as shown in Figure 3.

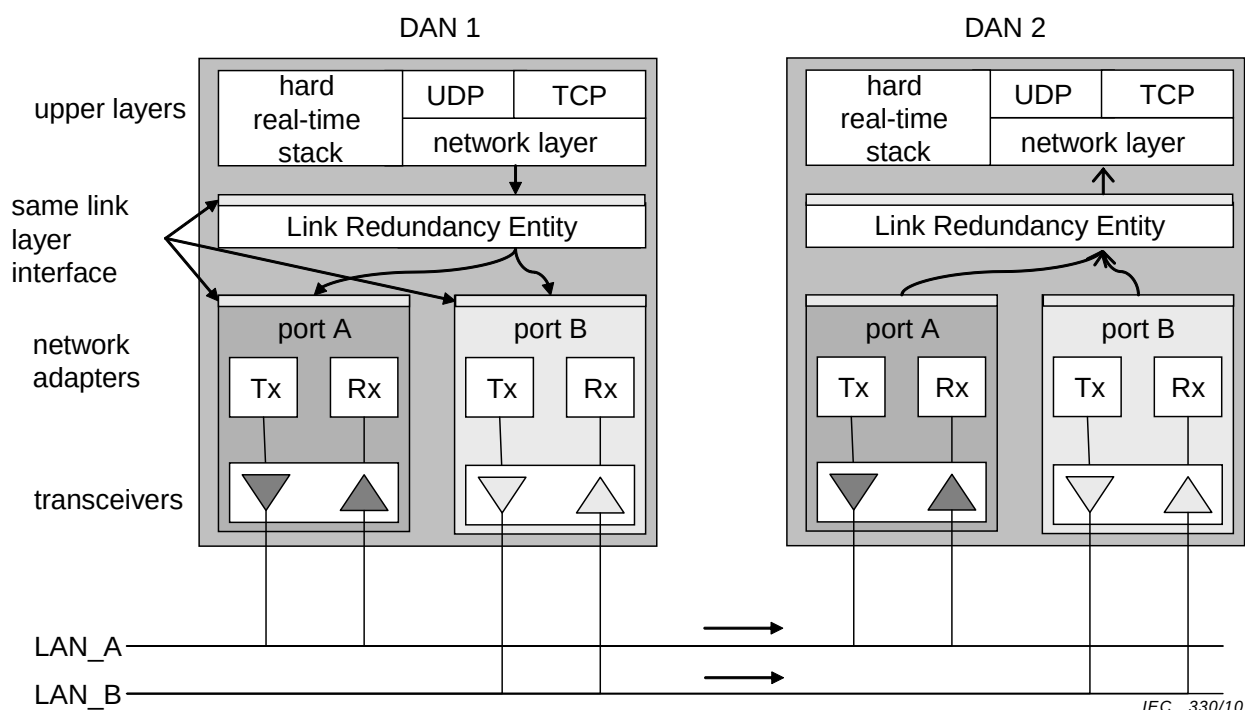


Figure 3 – Link Redundancy Entity in a Doubly Attached Node (DAN)

An end node connected to one or two LANs of the same network through two leaf links is a Doubly Attached Node (DAN).

An end node connected to one or more LANs of the same network through four leaf links is a Quadruply Attached Node (QAN).

NOTE End nodes using different communication ports for independent networks are not considered here, the considerations apply to each network separately.

5.2.2 Topologies

5.2.2.1 General

Redundancy within the network considers the presence of more network elements (switches, links) than necessary for operation, in order to prevent loss of communication caused by a failure. To this effect, there is more than one physical path between any two end nodes.

IEC 61918 specifies various kinds of basic physical topologies, some of which are used by the IEC 62439 series to define different topologies.

a) Topologies without redundancy

- Tree topology (Figure 4);
- Linear topology (Figure 5).

b) Topologies with redundant links

- Ring topology (Figure 6);
- Partial meshed topology (Figure 7);
- Fully meshed topology (Figure 8).

There are four top level structures:

- Single LAN without redundant leaf links (see 5.2.2.4.1);
- Single LAN with redundant leaf links (see 5.2.2.4.2);
- Redundant LANs without redundant leaf links (see 5.2.2.4.3);
- Redundant LANs with redundant leaf links (see 5.2.2.4.4).

When redundancy is handled in the LAN, end nodes can be singly attached. In the case of switch or leaf link failure, such end nodes may lose communication.

5.2.2.2 Topologies without redundancy

5.2.2.2.1 Tree topology

In a tree topology, at least one switch has more than two inter-switch links and there is only one path between any two devices. Figure 4 shows an example of tree topology.

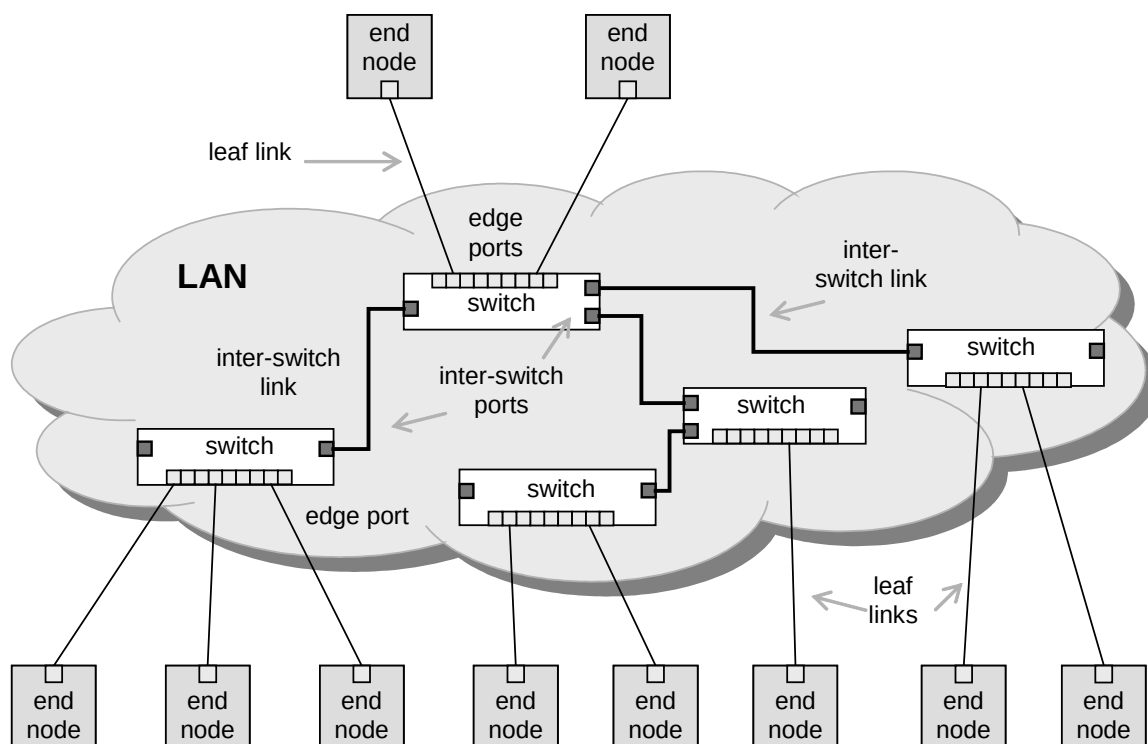


Figure 4 – Example of tree topology

IEC 331/10

5.2.2.2.2 Linear topology

In a linear topology, all switches are connected to each other in line and no node has more than two inter-switch links but the two nodes located at the end of the line have only one inter-switch link. Figure 5 shows an example of linear topology.

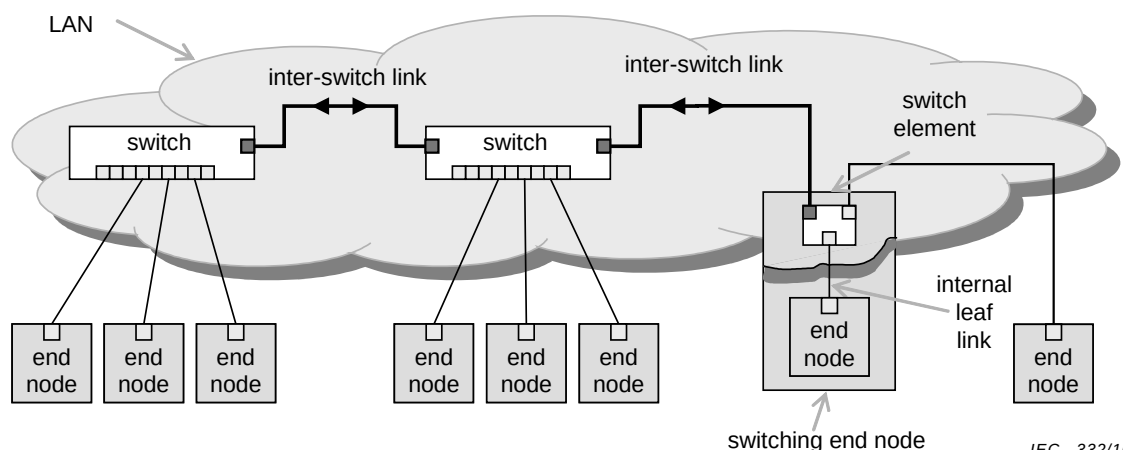


Figure 5 – Example of linear topology

IEC 332/10

NOTE A node may be a switching end node, as shown in the second rightmost end node of Figure 5.

5.2.2.3 Topologies with redundant links

5.2.2.3.1 Ring topology

NOTE This topology applies to RSTP (see Clause 7), MRP (IEC 62439-2) and DRP (IEC 62439-6) redundancy.

In a ring topology, every switch has two inter-switch links and any two end nodes have two paths between them when all components are operational. Figure 6 shows an example for the ring topology.

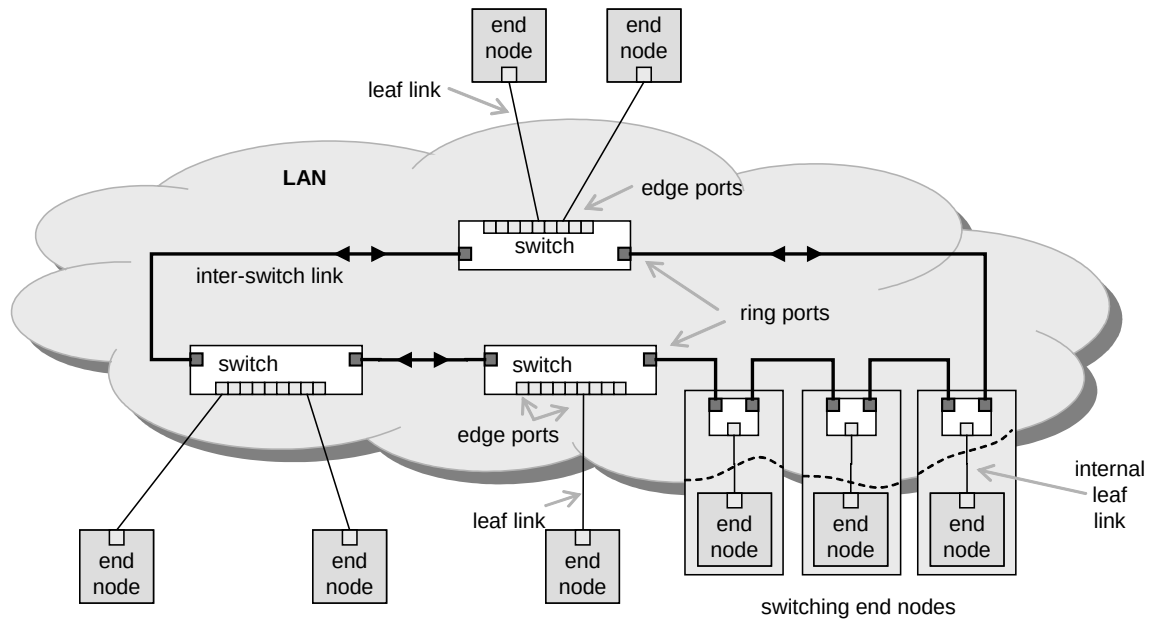


Figure 6 – Example of ring topology

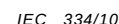
IEC 333/10

A ring topology introduces a loop in the LAN that could lead to flooding by permanently circulating frames. Protocols such as the Rapid Spanning Tree Protocol (RSTP) and the Media Redundancy Protocol (MRP) ensure that the switches maintain a logical linear topology during initialization, operation and reconfiguration.

If a switch or an inter-switch link fails, the switch is excluded from the ring, and a new logical linear topology is established. However, end nodes connected to a failed switch lose connectivity.

5.2.2.3.2 Partially meshed topology

In a partially meshed topology, at least one switch has more than two inter-switch links and there exists more than one path between some devices. Figure 7 shows an example of a partially meshed topology.



5.2.2.3.3 Fully meshed topology

In a fully meshed topology, the failure of any inter-switch link and of any switch can be tolerated. However, end nodes connected to a failed switch loose connectivity. Figure 8 shows an example of a fully meshed topology.

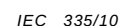


Figure 8 – Example of fully meshed topology

5.2.2.4 Top level structures of networks

5.2.2.4.1 Single LAN without redundant leaf links

This topology has only one path between any two nodes (see Figure 9).

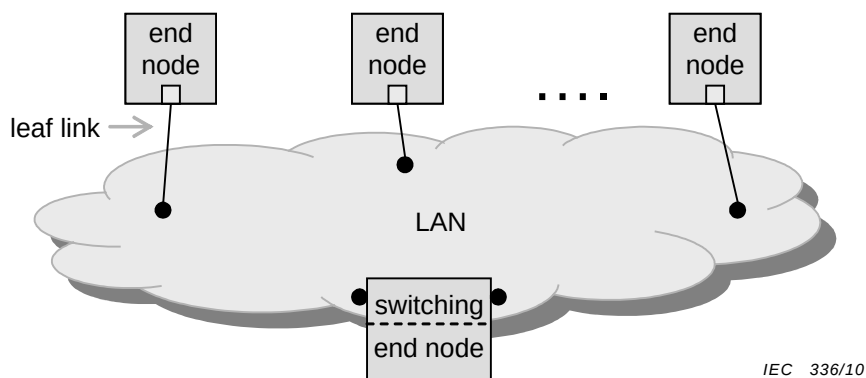


Figure 9 – Single LAN structure without redundant leaf links

Examples of this topology are the tree and linear topologies (see Figure 4 and Figure 5).

5.2.2.4.2 Single LAN with redundant leaves

NOTE This topology applies e.g. to nodes incorporating a RSTP switch or a subset thereof.

Doubly attached nodes (DANs) are connected to the same LAN through leaf links. Each edge port may belong to the same switch or to different switches. Figure 10 shows an example.

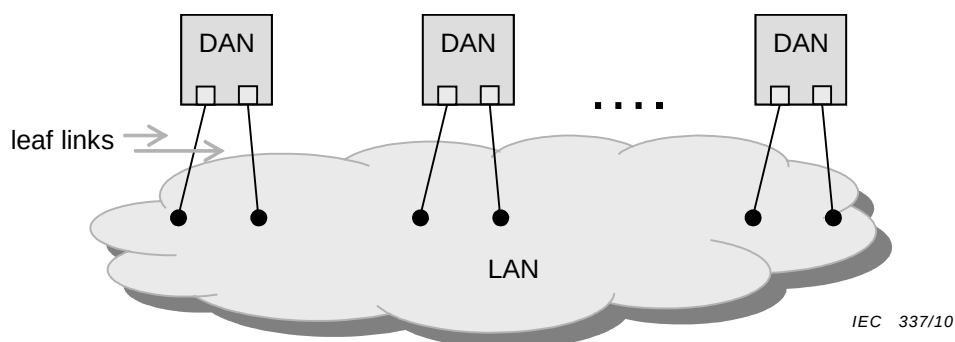
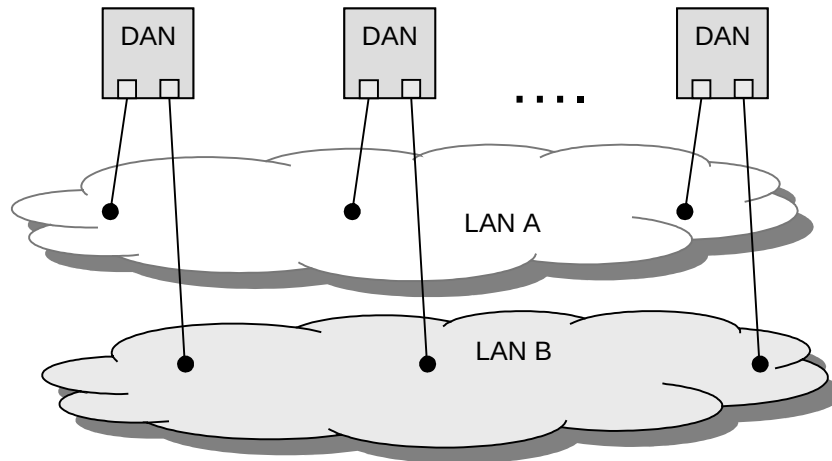


Figure 10 – Single LAN structure with redundant leaf links

5.2.2.4.3 Network without redundant leaves

NOTE This topology applies to PRP (see IEC 62439-3), CRP (see IEC 62439-4) and BRP (see IEC 62439-5).

In this type of topology, paths do not overlap. Redundant leaf links are connected to different LANs. An example is shown in Figure 11.

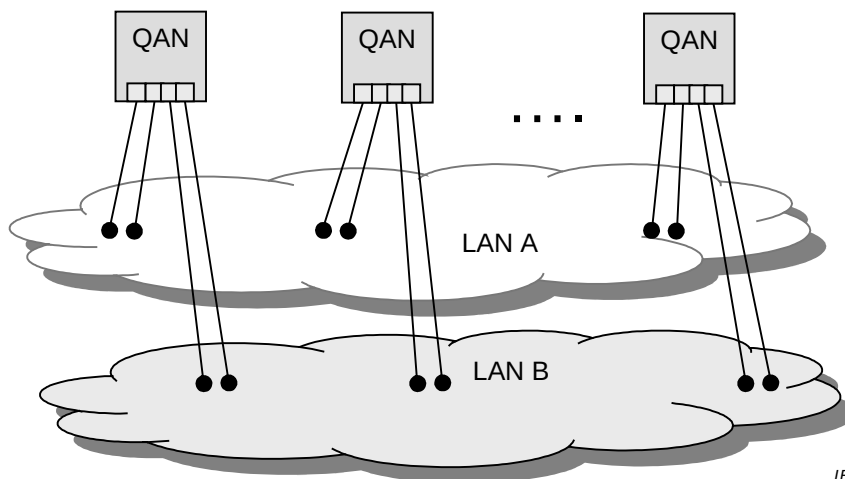


IEC 338/10

Figure 11 – Redundant LAN structure without redundant leaf links

5.2.2.4.4 Redundant LAN with redundant leaf links

Redundant leaf links are connected both to the same LAN and different LANs. Nodes are quadruply attached nodes (QANs). An example is shown in Figure 12.



IEC 339/10

Figure 12 – Redundant LAN structure with redundant leaf links

5.2.3 Redundancy handling

5.2.3.1 Backup mode

In the backup mode, only one of the redundant paths is selected as on-service while the other paths are in stand-by.

If the on-service path becomes unavailable, another path backs it up.

During the elapsed time from the loss of the on-service path to the beginning of operation of the backup path, messages can be lost, therefore the channel is considered in disconnected state.

NOTE IECV calls this kind of redundancy “stand-by” or “passive” redundancy. The term “dynamic redundancy” is also used.

5.2.3.2 Alternate (active) mode

In the alternate mode, redundant paths are used alternately, at random or according to regular patterns, and messages are transmitted via one of the redundant paths.

If it is detected that one of the redundant paths is in disconnected state, that path stops being used while other paths continue being used alternatively.

This mode allows checking the availability of the components continuously and therefore increases coverage.

5.2.3.3 Parallel (active) operation

In the parallel operation, messages are transmitted via all available redundant paths.

The receiving end node selects one of the received messages.

NOTE The term “static redundancy” or “work-by” is also used.

5.2.4 Network recovery time

Network recovery time is called recovery time in the IEC 62439 series because the IEC 62439 series deals only with networks. The definition in 3.1.41 applies.

5.2.5 Diagnosis coverage

Faults are detected through error detection mechanisms that detect only a percentage of the faults. The coverage is the probability that diagnosis mechanisms detect an error within a time that allows recovery before other mechanisms take action to protect the plant or before the plant suffers damage.

5.2.6 Failures

5.2.6.1 Kinds of failure

There are three kinds of failure:

- transient failure,
- component failure and
- systematic failure.

They affect the following elements:

- end nodes,
- leaf links,
- switches,
- inter-switch links.

5.2.6.2 Transient failures

A transient failure such as EM interferences causes transient errors, which leave the hardware essentially intact but disrupt the function. In this case, the failed part can be automatically reintegrated after automatic testing. Such mechanisms are partially implemented in the redundancy protocols specified in the IEC 62439 series.

NOTE EM interferences can become systematic failures.

5.2.6.3 Component failure

A component failure may be partial or complete. Only complete failures of components (not intermittent, not spurious) are considered in the IEC 62439 series.

5.2.6.4 Systematic failure

A systematic failure affects several redundant components at the same time; it is therefore a single point of failure. Configuration errors also belong to this category. The redundancy protocols specified in the IEC 62439 series do not consider systematic failures but allow detecting some.

NOTE Diversity of the design is possibly able to reduce impact of systematic failure.

5.2.6.5 End node failure

End node failure is out of scope of the IEC 62439 series.

5.2.6.6 Leaf link failure

Leaf link failure is caused by:

- failure of the connection port of end node,
- failure of the leaf link cable, or
- failure of the edge port.

5.2.6.7 Switch failure

A switch consists of a core switch functionality (for instance processor, power supply) and a number of ports.

For calculation purposes, a switch failure considers only the failure of the core switch function.

Failure of an edge port of the switch is considered as a leaf link failure.

Failure of an inter-switch port of the switch is considered as an inter-switch link failure.

5.2.6.8 Inter-switch link failure

Inter-switch link failure is caused by:

- failure of either inter-switch port or
- failure of the inter-switch link cable.

5.3 Safety

The IEC 62439 series does not consider safety aspects e.g. integrity.

NOTE Even though safety is not directly addressed, high reliability is a desirable feature in a safety system.

5.4 Security

The IEC 62439 series does not consider security (for example privacy, authentication) issues.

6 Classification of networks (informative)

6.1 Notation

The network structure of a high availability network is expressed by the following notation:

< TYPE >< NUMsn >< PLCYleaf >< NUMleaf >< TPLGY >< PLCYsn >
where

TYPE	indicates the type of top level redundant structure;
NUMsn	indicates the number of redundant LANs;
PLCYleaf	indicates the policy of leaf link redundancy;
NUMleaf	indicates the number of redundant leaves;
TPLGY	indicates the LAN topology.

EXAMPLE "A1N1RB" represents a single ring network without leaf link redundancy.

The <TYPE> field is defined in Table 3.

Table 3 – Code assignment for the <TYPE> field

Code	Top level redundant structure
A	Single LAN structure without redundant leaves
B	Single LAN structure with redundant leaves
C	Redundant LANs structure without redundant leaves
D	Redundant LANs structure with redundant leaves

The <PLCYleaf> field is defined in Table 4.

Table 4 – Code assignment for the <PLCYleaf> field

Code	Policy of leaf link redundancy
P	Parallel operation
A	Alternate operation
B	Backup operation
O	Other redundant policy
N	Not applicable or no leaf link redundancy

The <TPLGY> field is defined in Table 5.

Table 5 – Code assignment for the <TPLGY> field

Code	LAN topology
S	Simplex topology
R	Ring topology
P	Partial mesh topology
M	Full mesh topology
O	Other topology

6.2 Classification of robustness

Robustness of a high available network is expressed by the following notation:

<ITYPE>-L< NUMleaf >T< NUMtrunk >S< NUMsw >

where

ITYPE indicates the impact to be considered;

NUMleaf indicates the number of leaf link failures acceptable for the network operation;
NUMtrunk indicates the number of inter-switch link failures acceptable for the network operation;
NUMsw indicates the number of switch failure acceptable for the network operation.

The <ITYPE> field is defined in Table 6.

Table 6 – Code assignment for the <ITYPE> field

code	Impact for robustness classification
N	No impact is observed
R	Every end node is able to communicate with any other end nodes, but there is some period of interruption
L	Limited number of end nodes is not able to communicate, but other end nodes are able to communicate with some interruption

EXAMPLE “R-L0T1S0” means that one inter-switch link failure does not affect the network operation except for some period of interruption but failure of a leaf link or of a switch is not overcome by redundancy.

7 Availability calculations for selected networks (informative)

7.1 Definitions

The network is considered functional if every end node is able to communicate with any other end node in the network. It is assumed that a plant becomes unavailable if the automation network is not functional.

NOTE 1 This definition may be relaxed if graceful degradation is considered, but this is application-dependent and not considered here.

Availability of the network is defined as the fraction of time in which the network is functional, over its lifetime. The MTTF of the network is the mean time from an initial good state to failure of a component. Assuming that availability is high, the MTTF is roughly equal to the Mean Time Between Failures (MTBF), which is the mean time between maintenance calls.

Since the lifespan of the network is much longer than the MTTF, the figure that describes best the behaviour of the network under fault conditions is the Mean Time To Failure of the Network, or MTTFN.

The availability of the network is then deduced as Equation (1):

$$A_N = \frac{MTTFN}{MTTFN + MTTRN} \quad (1)$$

where

MTTFN is the Mean Time To Failure of Network, and

MTTRN is the Mean Time To Repair Network.

NOTE 2 The plant availability is lower because there are other causes of failure than the network and because the time to restore the plant after a network failure is larger than the time to repair the network.

The failure rates of the following elements are considered when used:

λ_L = failure rate of leaf links including both ports;

λ_S = failure rate of switches core, not considering the ports;

λ_T = failure rate of inter-switch links including both ports.

NOTE 3 The failure rate applies to the network only, reliability of the application in a device is not considered.

NOTE 4 For the purpose of the calculations in the following examples, an example network is considered which consists, in the non-redundant case, of 5 switches with 8 ports each, connected in a ring. Typical failure rates of the elements that are used in the following examples are:

$$\lambda_S = 1 / \text{MTTF}_{\text{switch}} = 1/100 \text{ years}$$

$$\lambda_L = \lambda_T = 1 / \text{MTTF}_{\text{link}} = 1/50 \text{ years (copper or optical link)}$$

7.2 Reliability models

7.2.1 Generic symmetrical reliability model

The general fault model of a network consisting of redundant and non-redundant parts is shown in Figure 13. This symmetrical model assumes that the roles of main and back-up (stand-by or work-by unit) are interchangeable, i.e. once the network operates with the back-up there is no need to revert to the former main after repair.

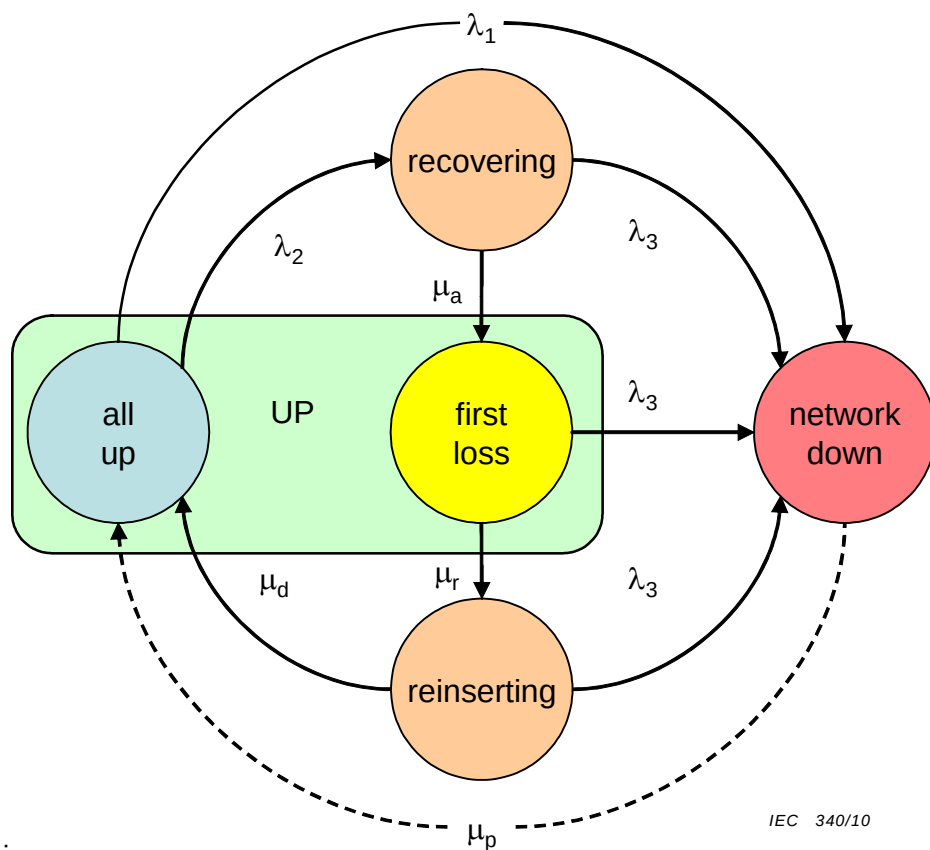


Figure 13 – General symmetrical fault model

The transitions are:

λ_1 = failure rate of the non-redundant components
(including single point of failure and probability of unsuccessful recovery)

λ_2 = failure rate of the redundant components
(for which a redundancy exists and recovery is successful)

λ_3 = failure rate of the remaining components

μ_a = rate of auto-recovery
(time from occurrence of a fault until its recovery)

μ_d = disruption rate
(mean network disruption time caused by reinsertion)

μ_r = recovery rate
(time from occurrence of a fault until redundancy restoration, includes on-line repair)

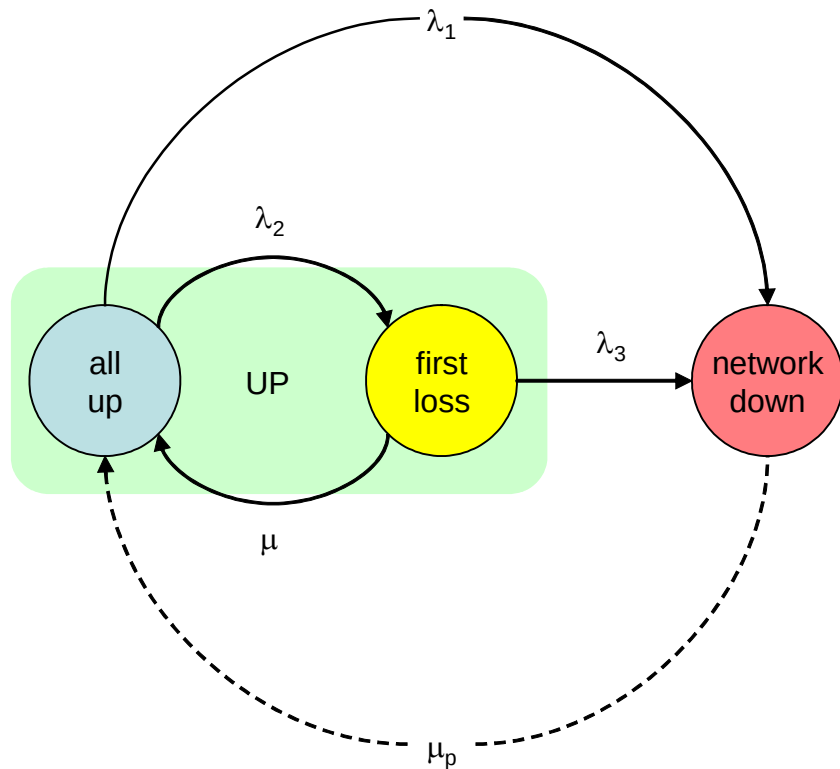
μ_p = plant repair rate
(time from occurrence of a non-recoverable fault until plant is up again)

NOTE Lurking faults are considered in μ_r and λ_1 rather than by introducing an additional state

This model contemplates two short disruptions: on a first failure, there is a short fault recovery time to activate the redundancy; after repair, there is a short redundancy reinserting recovery time to restore redundant operation. As long as these disruptions remain below the acceptable disruption time, they do not affect availability calculations.

7.2.2 Simplified symmetrical reliability model

Assuming that the network spends very little time in the “recovering” and “reinserting” states, these states can be collapsed into the “first loss” state, as Figure 14 shows.



IEC 341/10

Figure 14 – Simplified fault model

The general solution of the simplified model is expressed in Equation (2):

$$MTTFN = \frac{\mu + \lambda_2 + \lambda_3}{(\lambda_1 + \lambda_2)(\lambda_3 + \mu) - \mu \times \lambda_2} \quad (2)$$

where

λ_2 is the failure rate of the redundant components;
 λ_3 is the failure rate of the remaining components;
 μ is the repair rate.

It would be in principle necessary to introduce separate transitions and states for the failure of switches and the failure of links. However, since the network consists of a large number of elements and the failure rates of switches and links are not too different, one can use only one “1st failure” state.

7.2.3 Asymmetric reliability model

In many cases, the main and back-up roles are not interchangeable. Full redundancy is only restored when the original main is again in place. Therefore, the asymmetric model considers more disruptions, as Figure 15 shows. The transitions of this model are not detailed since this model is only included to remind to consider possible additional disruptions. As in the preceding case, the disruption states P1, P2, P4 and P6 have no influence on the dependability calculations as long as their duration remains below the maximum acceptable disruption time.

NOTE As an analogy, consider a car where the spare tyre is for emergency only and is intended only for reaching safely the next garage. When a tyre is punctured, two changes of tyre are needed to restore normal operation. By contrast, where the spare tyre is identical to the one it replaces, only one disruption is necessary.

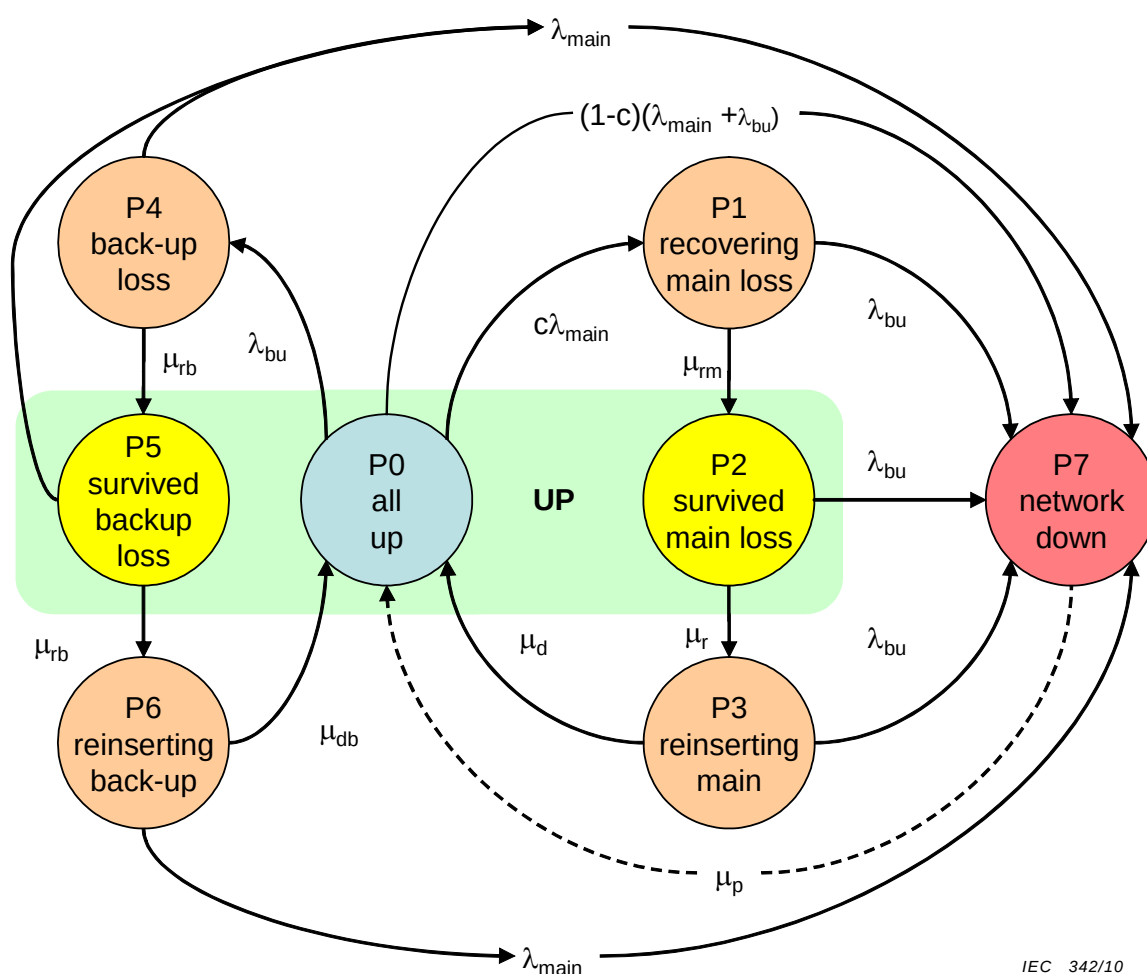


Figure 15 – Asymmetric fault model

IEC 342/10

7.3 Availability of selected structures

7.3.1 Single LAN without redundant leaves

In a non-redundant network, the failure of any element leads to network failure, as Figure 16 shows.

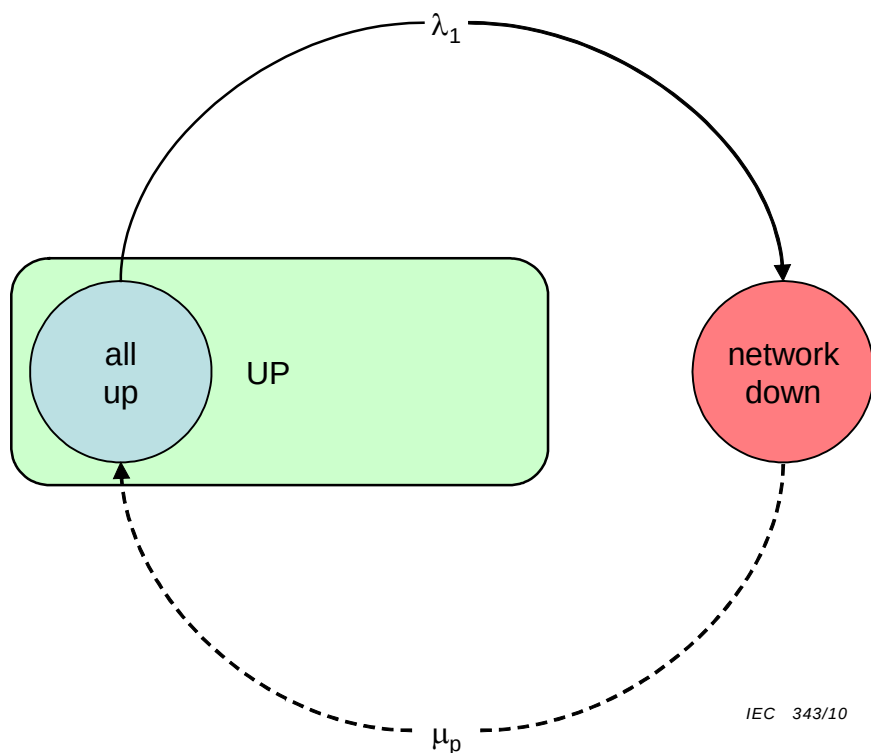


Figure 16 – Network with no redundancy

Therefore, the MTTFN simplifies into Equation (3).

$$\text{MTTFN} = \frac{1}{\lambda_1} \quad (3)$$

$$\text{where } \lambda_1 = \Sigma (\lambda_L + \lambda_S + \lambda_T)$$

EXAMPLE For the example network (5 switches, 40 leaf links, 5 inter-switch links)

MTTFN = 1,05 year and

MTTF = 1,05 year.

7.3.2 Network without redundant leaves

Under the assumption that the repair rate is much higher than the failure rate, only the reliability of the leaf links matters and Equation (3) simplifies to Equation (4):

$$\text{MTTFN} = \frac{1}{\lambda_1} \quad (4)$$

where $\lambda_1 = \Sigma (\lambda_L)$, assuming that all switches and inter-switch links are redundant.

This means that, if repair rate is reasonably high (MTTR some days vs. some years of MTTF), reliability is entirely dictated by the non-redundant parts of the network and that redundancy just allows to ignore the redundant elements in the MTTFN calculation.

EXAMPLE For the example network (5 switches, 40 non-redundant leaf links, 6 inter-switch links)

MTTFN = 1,17 year

MTTF = 1,03 year.

NOTE In the case of switching end nodes, the MTTFN is much higher since the leaf links are internal to the nodes and are considered in the node's failure rate.

7.3.3 Single LAN with redundant leaves

In this case, the failure rate of the leaf links can be ignored. Since the number of ports per switch is assumed to be constant, the number of switches is doubled.

EXAMPLE For the example network (10 switches, 80 redundant leaf links, 11 redundant inter-switch-links):

MTTFN = 9,78 year

MTTF = 0,52 year.

NOTE 1 This shows that the reliability increase obtained by double-attachment of nodes is reduced by the increased number of switches that are necessary. The MTTF doubles with respect to the non-redundant case since the number of links and ports doubled. Therefore, this structure makes only sense in the context of graceful degradation, where important devices are redundantly attached, but do not need connectivity to all end nodes.

NOTE 2 In the case of switching end nodes, the MTTFN is much higher since the leaf links are internal to the nodes and their unreliability is considered in the node's failure rate.

7.3.4 Network with redundant leaves

Assuming that all elements of the network are redundant, the failure rate λ_1 is reduced to single point of failure and recovery/reinsertion failures. If these can be ignored by proper design, the reliability model is given in Figure 17.

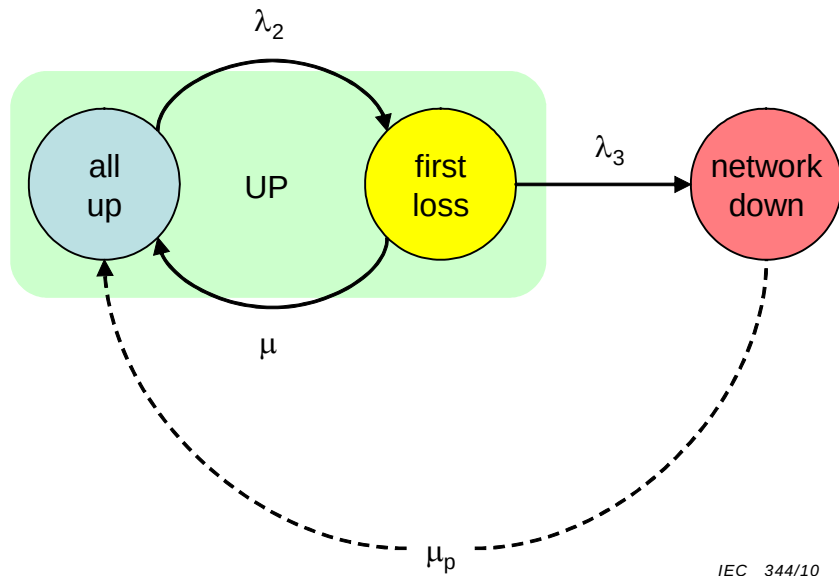


Figure 17 – Network with no single point of failure

The MTTFN simplifies to Equation (5):

$$\text{MTTFN} = \frac{\mu + \lambda_2 + \lambda_3}{(\lambda_1 + \lambda_2)(\lambda_3 + \mu) - \mu \times \lambda_2} \quad \lambda_1 = 0 \quad \sim \quad \text{MTTFN} = \frac{1}{\lambda_2} \times \frac{(\mu + \lambda_2 + \lambda_3)}{\lambda_3} \quad \mu \gg (\lambda_2 + \lambda_3) \quad \sim \quad \frac{\mu}{\lambda_2 \lambda_3} = \frac{1}{\lambda_2} \frac{2\mu}{\lambda_2} \quad (5)$$

where $\lambda_2 = \Sigma (\lambda_L + \lambda_S + \lambda_T)$ and $\lambda_3 = \lambda_2/2$

The failure rate λ_3 of the remaining elements is assumed to be half that of the full network, since second failures of the already impaired LAN do not affect function.

Roughly, the MTTFN is increased with respect to the non-redundant case by twice the ratio of repair rate to failure rate, which is usually high, e.g. MTTR = 24 hours vs. MTTF = 1 year.

EXAMPLE For the example network (2 × 5 switches, 2 × 40 leaf links, 2 × 6 inter-switch links):

MTTFN = 196 year.

MTTF = 0,58 year.

NOTE 1 This shows that even if the network is fully redundant, the availability is still limited and that network duplication causes double as high maintenance rate, since there are twice as many elements that can fail.

NOTE 2 This seemingly high MTTFN was calculated ignoring common mode errors. When considering the reliability of the whole automation system, the end node failure rate dominates the MTTFN and end node redundancy should be envisioned. Even a single non-redundant element or common cause of failure such as a software error brings the MTTFN severely down.

7.3.5 Considering second failures

The above calculation is pessimistic since it assumes that a second failure impairs the remaining network with a probability of 100 %. This is correct for switches when the LAN has internally no redundancy, but it is not the case for leaf links since the probability of a second failure impairing the same end node is not given by $\Sigma (\lambda_L)$, but simply by λ_L .

For a more precise estimation, the transition diagram of Figure 18 can be used.

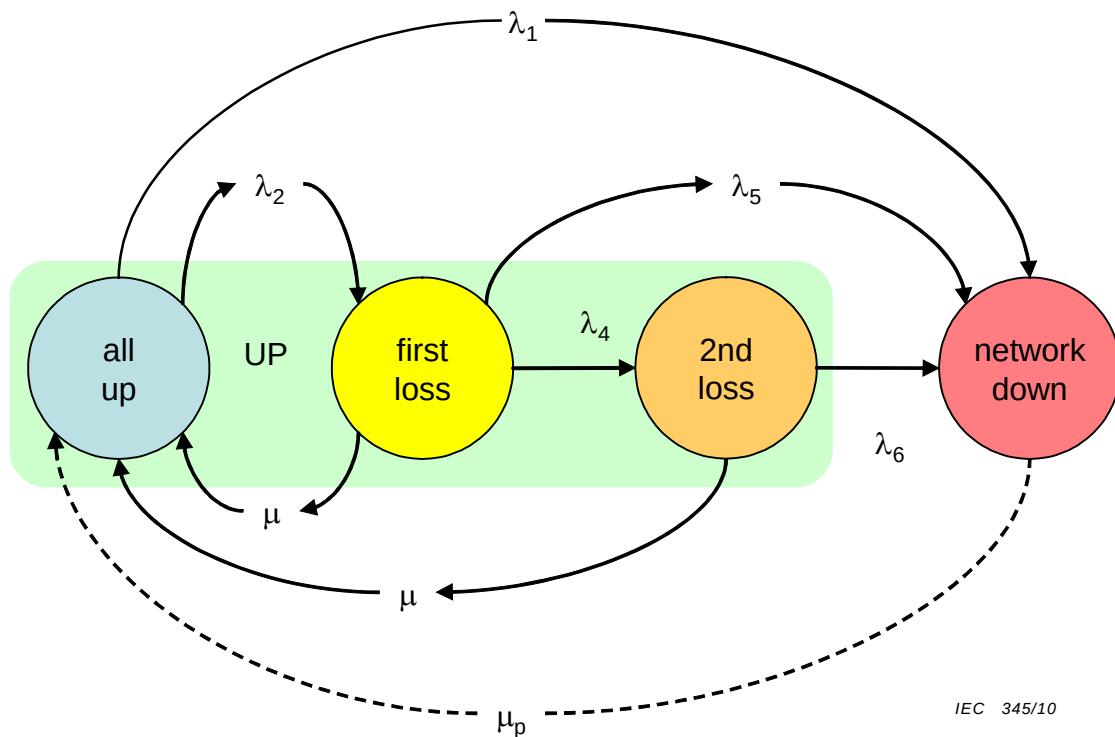


Figure 18 – Network with resiliency to second failure

The transitions are:

λ_1 = failure rate of the non-redundant components
(including single point of failure and probability of unsuccessful recovery).

λ_2 = failure rate of the redundant components
(for which a redundancy exists and recovery is successful).

λ_4 = failure rate of the remaining components which do not cause loss of the network.

λ_5 = failure rate of the remaining components which cause loss of the network
(the sum of λ_4 and λ_5 is approximately equal to λ_2 , so $\lambda_5 = f\lambda_2$,
where f is the probability that the second error results in a network failure).

λ_6 = failure rate of the remaining components after a second failure.

μ = recovery rate
(time from occurrence of a fault until redundancy restoration, includes on-line repair)

μ_p = plant repair rate
(time from occurrence of a non-recoverable fault until plant is up again).

The MTTFN of the network is given by Equation (6).

$$\text{MTTFN} = \frac{(\mu + \lambda_2 + \lambda_4 + \lambda_5) + \frac{\lambda_2 \lambda_4}{\mu + \lambda_6}}{\lambda_1(\mu + \lambda_4 + \lambda_5) + \lambda_2 \left(\lambda_5 + \lambda_4 \left(\frac{1}{1 + \frac{\mu}{\lambda_6}} \right) \right)} \approx \frac{1}{\lambda_1 + \lambda_2 \frac{f}{\mu}} \quad \mu \gg \sum (\lambda_i) \quad (6)$$

Assuming that common mode failures (λ_1) can be ignored, the MTTFN is improved with respect to the structure of Figure 14 roughly as the ratio of recoverable second failures to non-recoverable second failures, λ_4 to λ_5 , this ratio depending on the topology.

The failure rate from the 2nd loss to the network failure does not significantly influence the result, since the system spends very little of its lifetime in the 2nd loss state if the repair rate is high.

EXAMPLE With $\lambda_1 = 0$ (no common mode of failure), $\lambda_2 = \Sigma (\lambda_L + \lambda_S + \lambda_T)$, $\lambda_4 = 0,9 \lambda_2$, $\lambda_5 = 0,1 \lambda_2$ (1 fault in ten is not recoverable), $\lambda_6 = \lambda_2$.

MTTFN = 1 868 year.

7.4 Caveat

These calculations should be used as a caveat that redundancy is not able to solve all reliability problems and that the basic assumption, that the network is operational when all nodes can communicate with all other nodes, can be slackened in particular cases.

8 RSTP for High Availability Networks: configuration rules, calculation and measurement method for ~~deterministic~~ predictable recovery time in a ring topology

NOTE In the context of this Clause, the word “bridge” is used in place of “switch”, respectively “bridging” instead of “switching”.

8.1 General

The Rapid Spanning Tree Protocol (RSTP) as specified in IEEE 802.1D provides loop prevention and redundancy management for an arbitrary topology of switched Ethernet networks.

RSTP provides recovery from two types of network faults

- a) an inter-switch link failure and
- b) a switch failure, which can be of two types, depending on the role of the switch at the time it fails:
 - 1) a non-root, which RSTP handles like an inter-switch link failure or
 - 2) a root switch failure, which RSTP handles by reconfiguration of the network.

Although RSTP includes an efficient algorithm for network recovery, the actual fault recovery time depends on the topology and the RSTP implementation.

Generally RSTP provides deterministic recovery time even in an arbitrary meshed topology in case of a link failure or non-root switch failure. However, in case of a root switch failure it is difficult to predict the recovery time in an arbitrary meshed topology.

By contrast, when the topology is restricted to a ring, RSTP fault recovery time is deterministic in all scenarios and can be calculated, provided that RSTP timing performance characteristics of the switches are known.

This subclause specifies the reference ring topology, the calculation method to calculate the recovery time for this reference topology, the method for measuring the relevant timing performance characteristics of an RSTP implementation and the form in which they should be disclosed.

8.2 Deployment and configuration rules for the ring topology

To achieve a deterministic recovery time, and for the purpose of the following calculations, the following configuration rules are to be observed:

- the network topology shall be restricted to a single ring of N devices.
- as RSTP specifications prescribe, N shall be less or equal 40.
- ring ports shall be enabled for RSTP operation.
- non-ring ports shall not be enabled for RSTP operation.
- all links shall be configured to operate in a full-duplex mode.
- media-converters, if used in inter-switch connections, shall be operated in transparent link mode.
- switches shall be configured so they do not use the highest available class of service except for BPDUs, or, if this is not achievable, then at least 10 % of the highest available class of service bandwidth shall be reserved for BPDUs.

NOTE Disabling the non-ring ports for RSTP has the consequence that loops connected to non-ring ports will not be prevented by RSTP

8.3 Calculations for fault recovery time in a ring

8.3.1 Dependencies and failure modes

The RSTP fault recovery time depends on the following factors:

- location of the point of failure related to the discarding port(s) that terminate(s) the affected spanning tree branch(es),
- combination of RSTP configuration parameters in different switches in the affected network segment(s).

The following failure modes are considered:

- loss of an inter-switch link,
- loss of a node in the non-root role,
- loss of a node in the root role.

RSTP depends on link state detection.

8.3.2 Calculations for non-considered failure modes

If a failure occurs such that no link error is detected and no BPDUs are forwarded, the recovery time will rise to a value that is three times the HelloTime, which is currently specified as minimum 1 s in IEEE 802.1D:2004.

NOTE Mechanisms to prevent this situation are possible, but are not prescribed in IEEE 802.1D.

8.3.3 Calculations for the considered failure modes

The formulas below present the upper bound of the fault recovery time in a ring network:

- $T_L + N \cdot \max(T_{PA}, (T_{TC} + T_F))$ – for inter-switch link failure and non-root switch failure
- $T_L + 2 \cdot N \cdot T_{PA}$ – for root switch failure

where:

N is the number of switches in the ring;

T_L is the time required by a switch to detect a link failure;

T_{PA} is the time required by a pair of switches to perform RSTP Proposal Agreement

handshaking; equal to the sum of the BPDU processing times in both switches of the pair.

T_{TC} is the time required by a pair of switches to propagate a Topology Change BPDU; equal to the sum of the BPDU processing times in both switches of the pair;

NOTE 1 T_{TC} is about half T_{PA} because no acknowledgement is involved.

T_F is the time required by a switch to flush its MAC address table.

Other parameter not used in the formulas above is defined for timing measurements:

T_{Proc} is the RSTP processing time, i.e. the time required to process a full RSTP state machine cycle.

NOTE 2 T_{PA} is actually the sum of one switch's "downlink" processing time plus the adjacent switch's "uplink" processing time (generating a Proposal BPDU, processing the Proposal BPDU and generating an Agreement BPDU, and processing the Agreement BPDU). Full RSTP state machine cycle includes one switch's both "uplink" and "downlink" processing times, i.e. roughly $T_{Proc} = T_{PA}$.

EXAMPLE To achieve 130 ms recovery time in a ring of 40 devices, for all switches, the time T_L should be lower than 10 ms for 100Base-TX and 100Base-FX links and the time T_{PA} and the sum ($T_{TC} + T_F$) should be lower than 3 ms.

NOTE 3 This requires that switch port hardware supports fast link failure detection, as specified by ISO/IEC 8802-3 (IEEE 802.3).

NOTE 4 1000Base-T links cannot be used for inter-switch connections in this application due to their long link failure detection time.

NOTE 5 This can be ensured by prioritizing the link monitoring and RSTP processing firmware tasks and by appropriate processor speed and RSTP firmware implementation.

8.4 Timing measurement method

8.4.1 Measurement of T_{PA}

8.4.1.1 Measurement

It is impossible to separately measure some time values defined above. Therefore, some tests measure a combination of several time values, so that the time in question can be calculated from the measured value.

This test is actually measuring T_{Proc} time but T_{Proc} is equal to T_{PA} , as explained in 8.3.3.

8.4.1.2 Setup

Configure the system as follows:

- a) Build the test network as shown in Figure 19.