IEC 62439-1

Edition 1.2 2016-02

CONSOLIDATED VERSION

VERSION CONSOLIDÉE

colour inside

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

IEC 62439-1:2010-02+AMD1:2012-06+AMD2:2016-02 CSV(en-fr)
Copyright International Electrotechnical Commission

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 Varembé
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.

Copyright International Electrotechnical Commission

IEC 62439-1

Edition 1.2 2016-02

CONSOLIDATED VERSION

VERSION CONSOLIDÉE

colour inside

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.

® Registered trademark of the International Electrotechnical Commission
Copyright International Electrotechnical Commission, de la Commission Electrotechnique Internationale

Copyright International Electrotechnical Commission

IEC 62439-1

Edition 1.2 2016-02

REDLINE VERSION

VERSION REDLINE

colour inside

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

IEC 62439-1:2010-02+AMD1:2012-06+AMD2:2016-02 CSV(en-fr)
Copyright International Electrotechnical Commission

CONTENTS

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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>

Copyright International Electrotechnical Commission

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]

Copyright International Electrotechnical Commission

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 IEV 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]

Copyright International Electrotechnical Commission

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 + Δt) 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.

Copyright International Electrotechnical Commission

[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.

Copyright International Electrotechnical Commission

[IEC 61784-2, 3.1.14]

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.

Copyright International Electrotechnical Commission

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 IEV 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]

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

[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

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

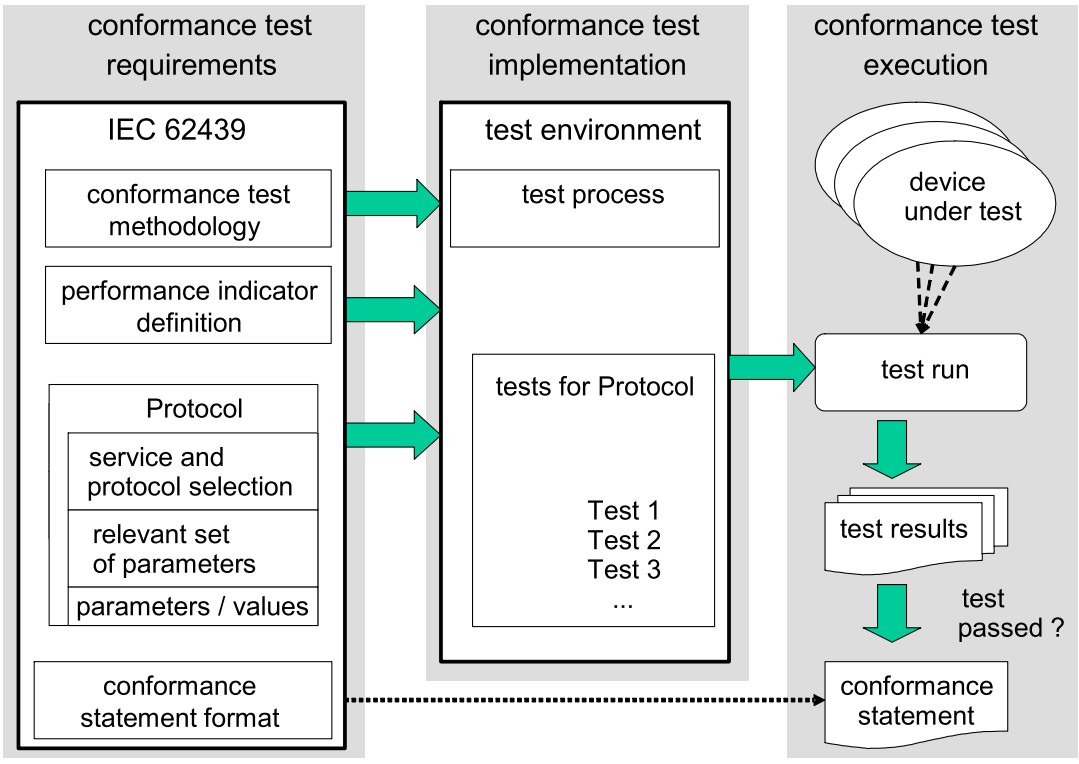


Figure 1 – Conformance test overview

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;

Copyright International Electrotechnical Commission

- 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.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

5.2 Generic network system

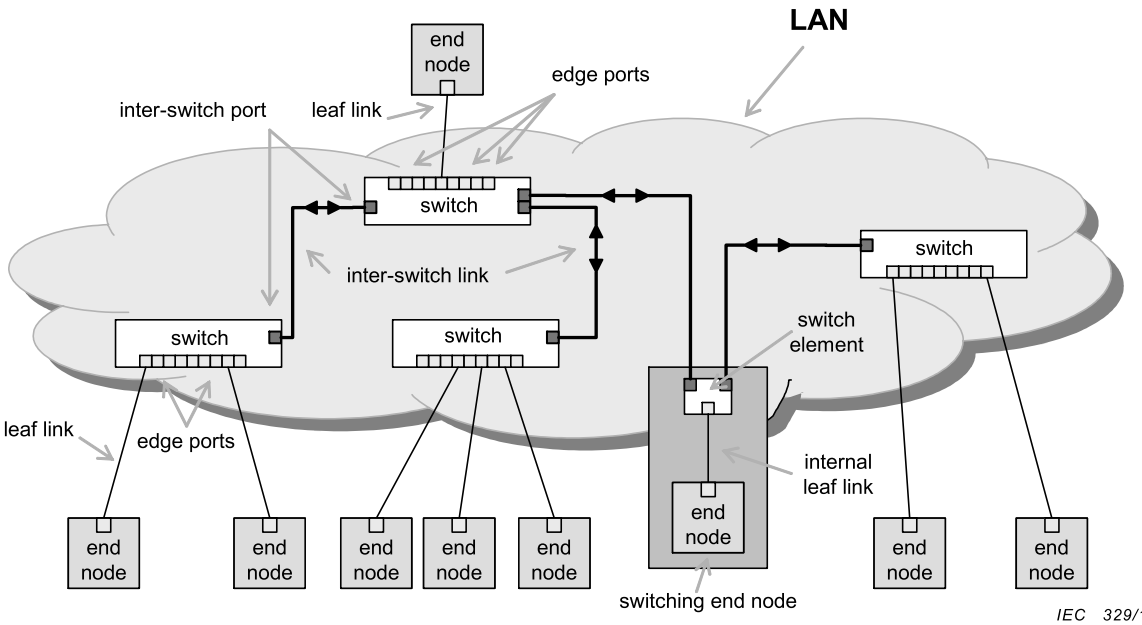
5.2.1 Network elements

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.

Copyright International Electrotechnical Commission

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.

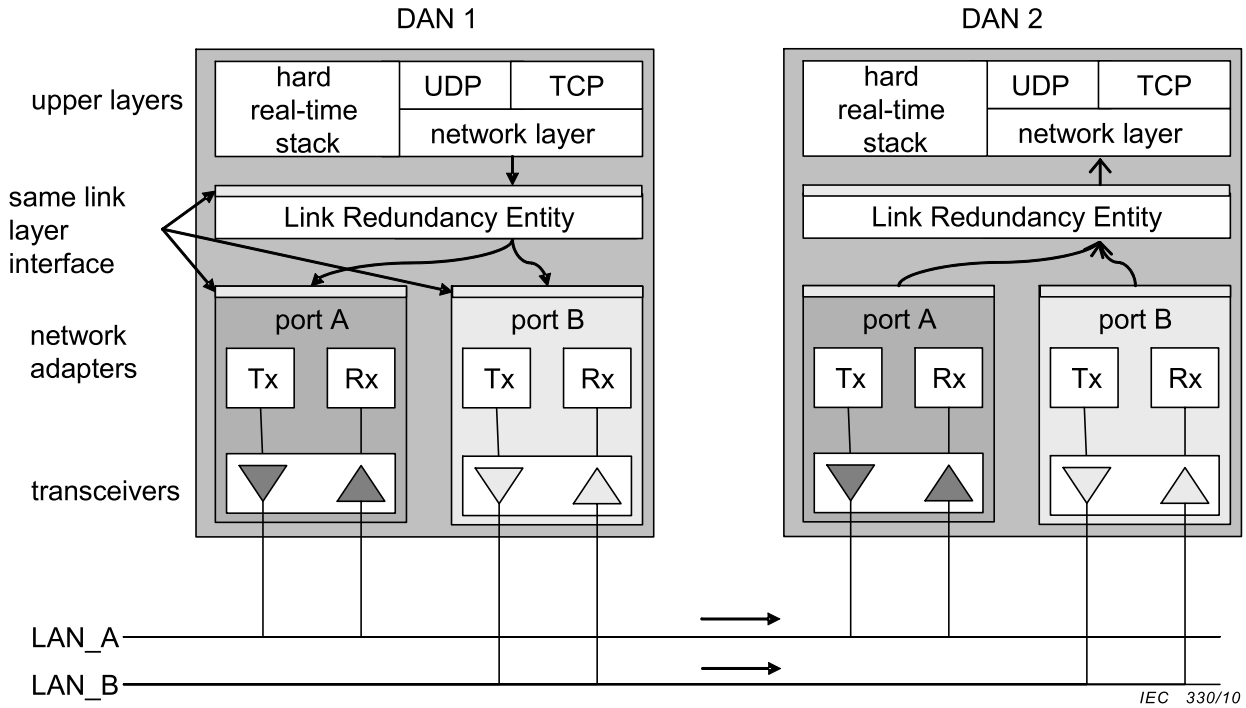


Figure 3 – Link Redundancy Entity in a Doubly Attached Node (DAN)

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).

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

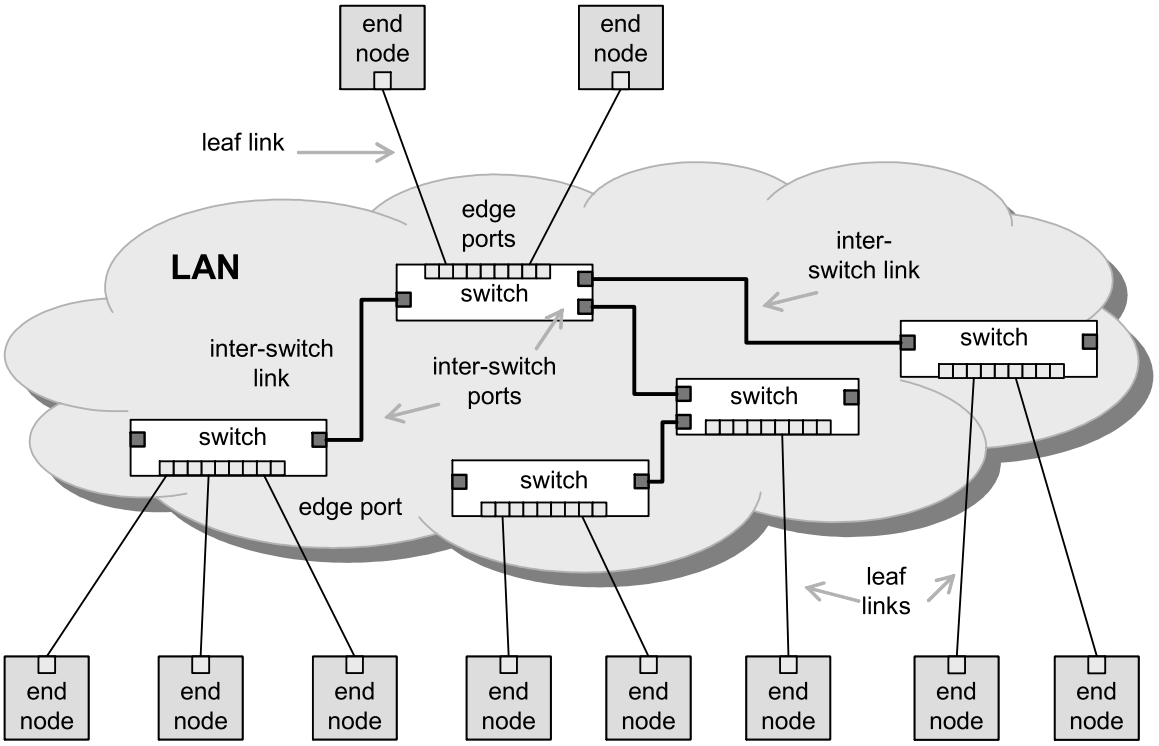


Figure 4 – Example of tree topology

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.

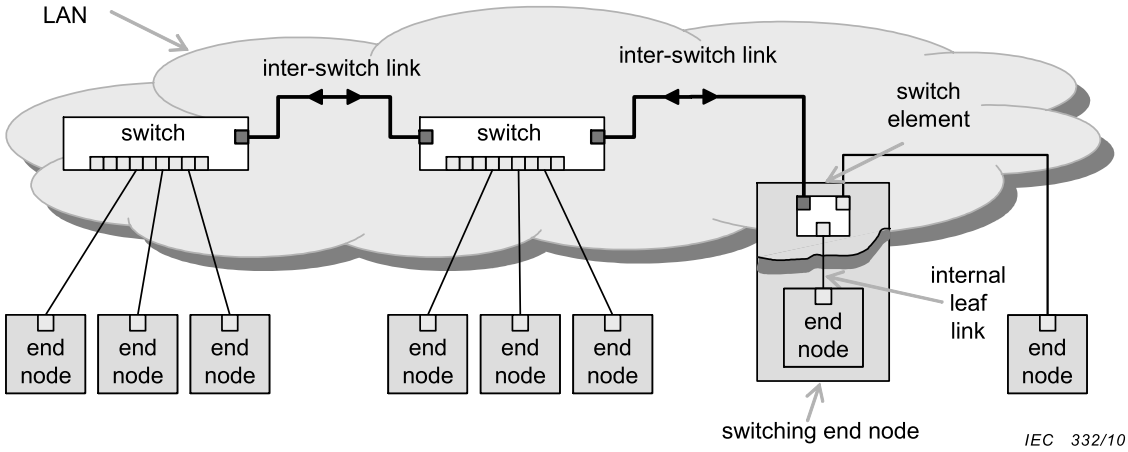


Figure 5 – Example of linear topology

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.

Copyright International Electrotechnical Commission

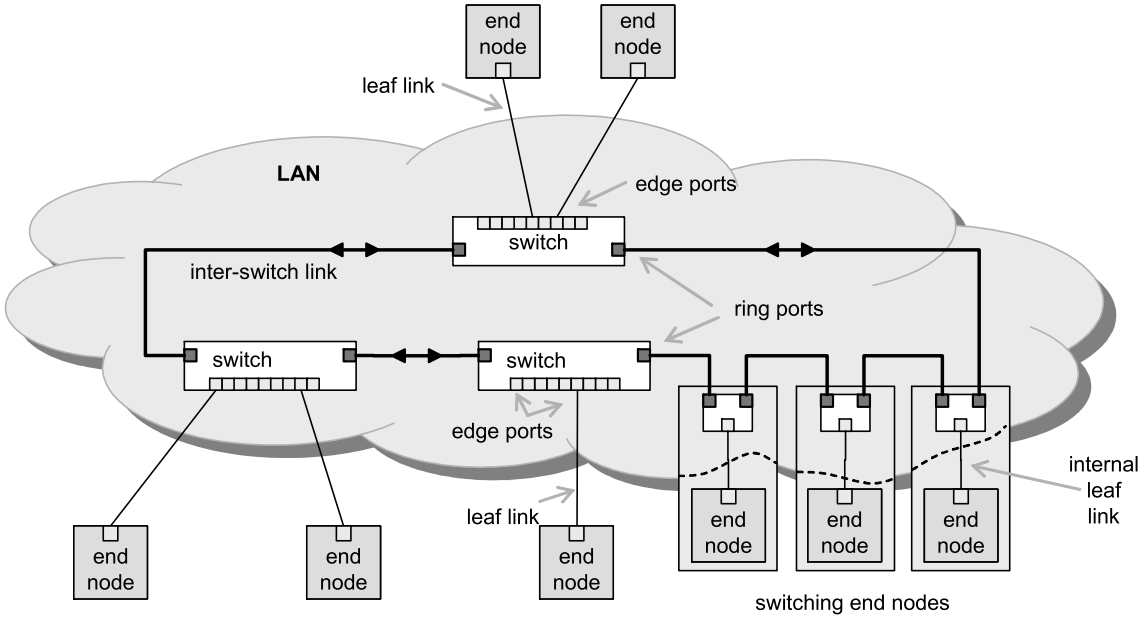


Figure 6 – Example of ring topology

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.

Copyright International Electrotechnical Commission

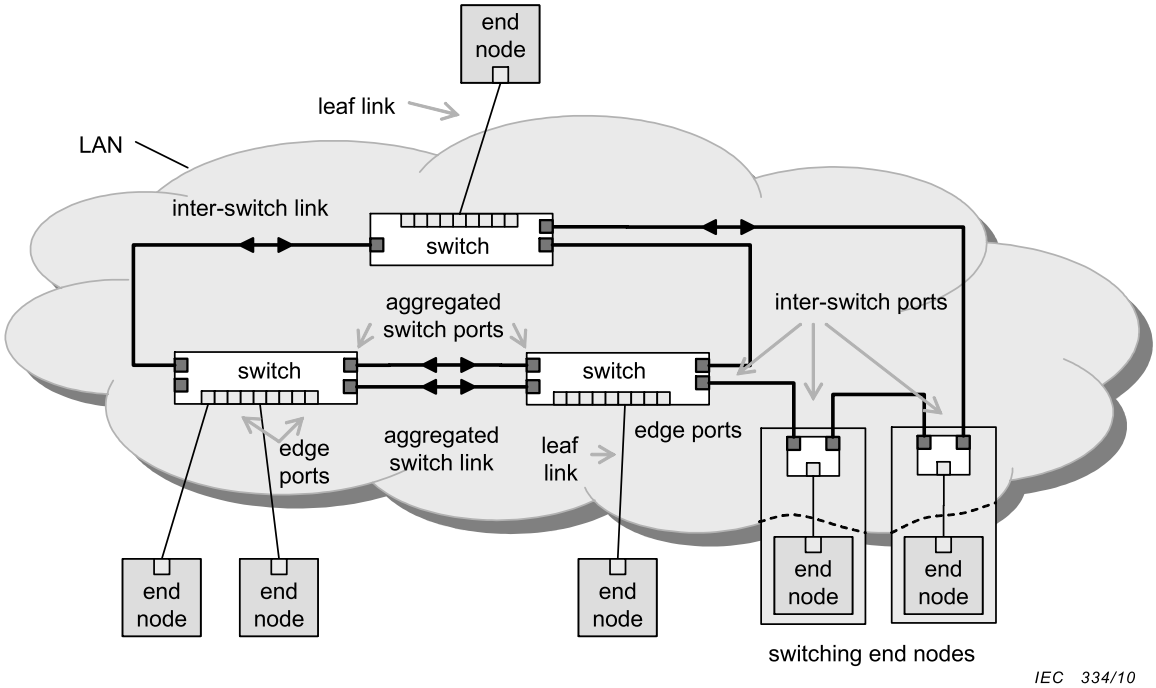


Figure 7 – Example of a partially meshed topology

5.2.2.3.3 Fully meshed topology

In a fully meshed topology, every switch has more than two inter-switch links.

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.

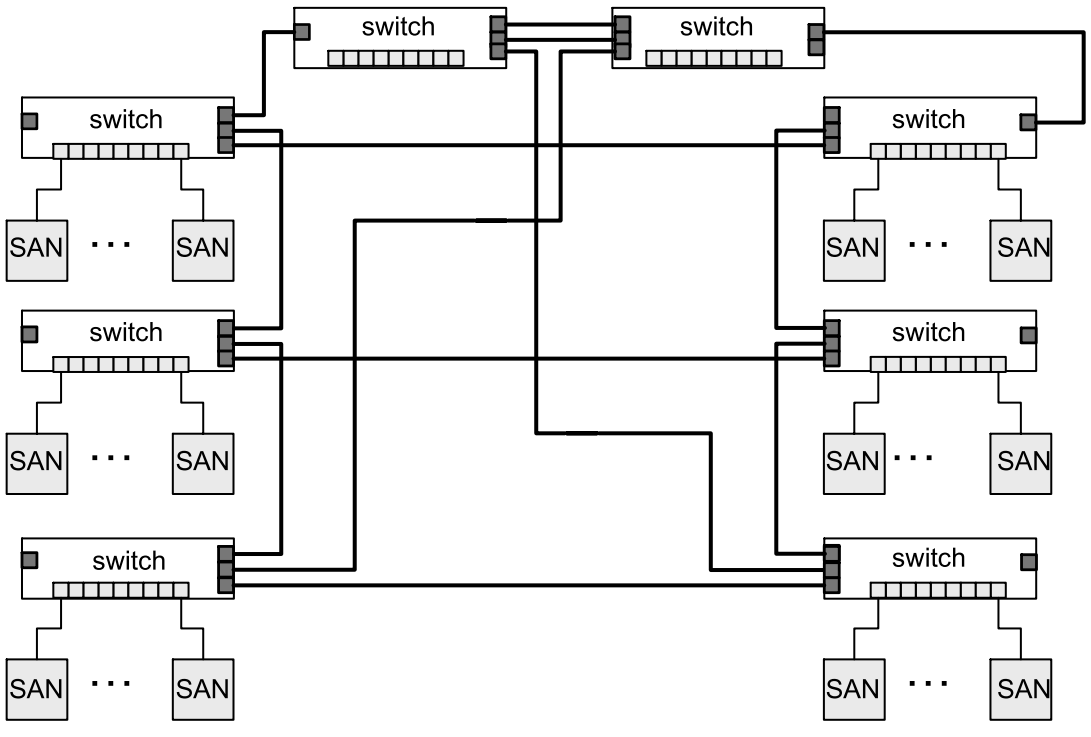


Figure 8 – Example of fully meshed topology

Copyright International Electrotechnical Commission

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).

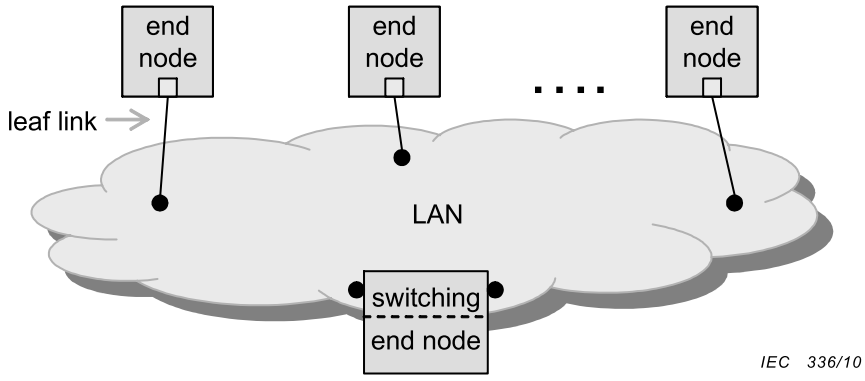


Figure 9 – Single LAN structure without redundant leaf links

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.

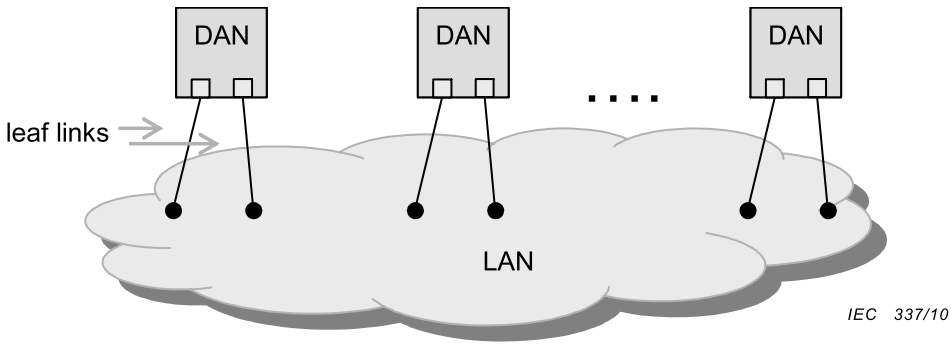


Figure 10 – Single LAN structure with redundant leaf links

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.

Copyright International Electrotechnical Commission

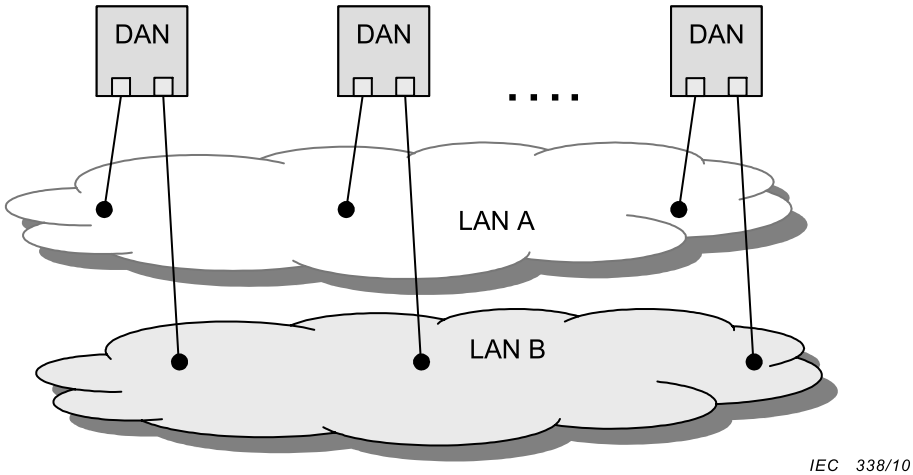


Figure 11 – Redundant LAN structure without redundant leaf links

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.

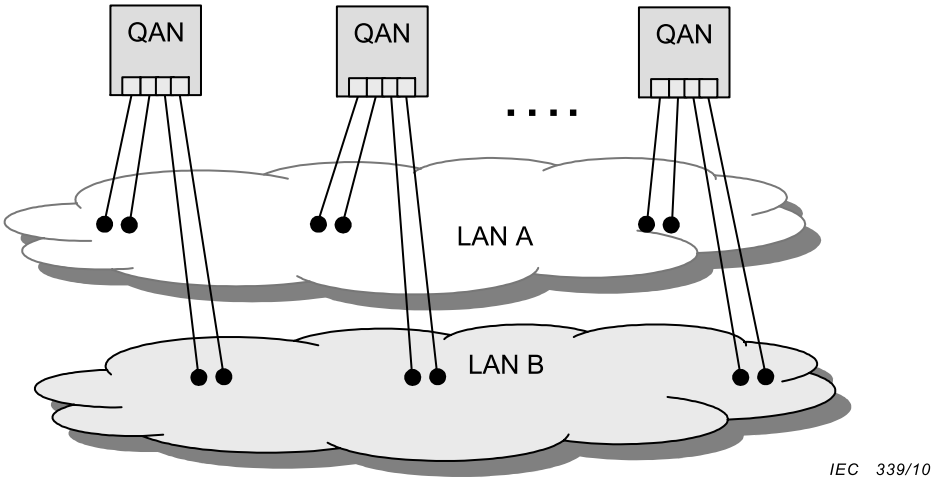


Figure 12 – Redundant LAN structure with redundant leaf links

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 IEV 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.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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

Copyright International Electrotechnical Commission

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;

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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:

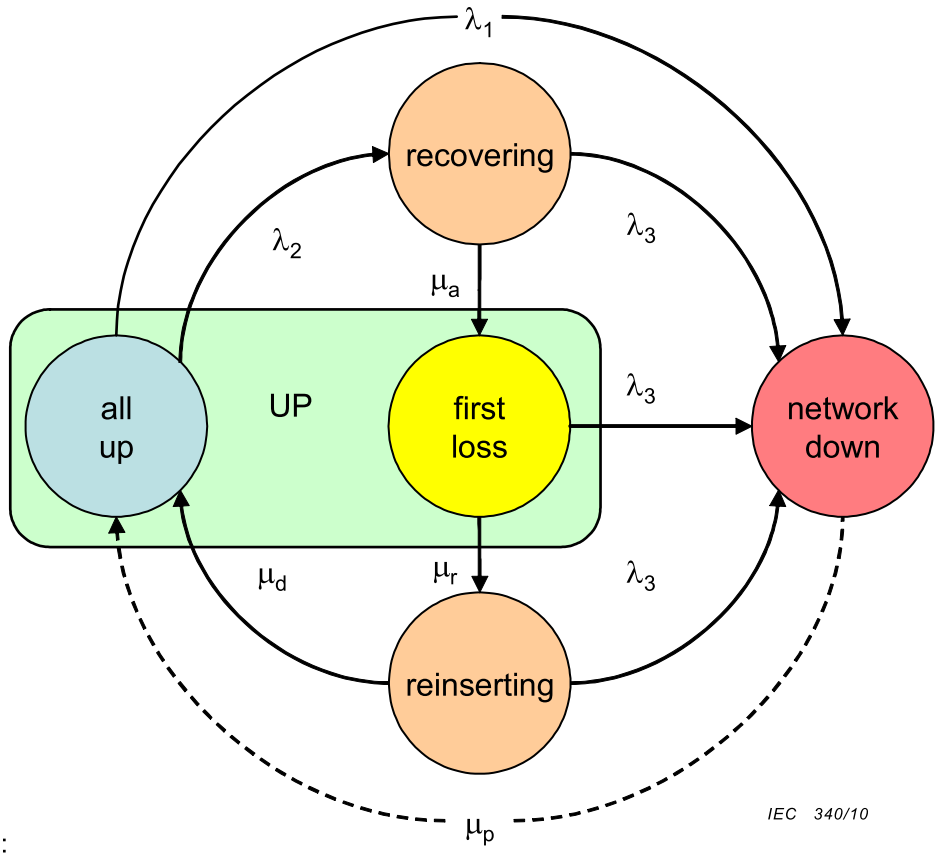
$$\lambda_S = 1 / \text{MTTFswitch} = 1/100 \text{ years}$$

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

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)

Copyright International Electrotechnical Commission

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.

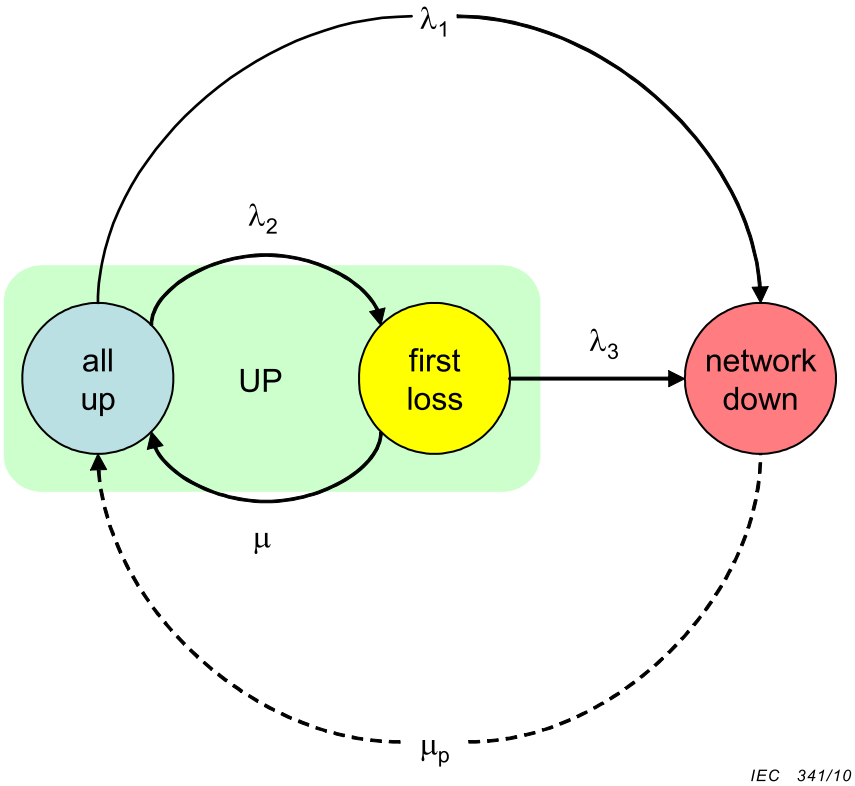


Figure 14 – Simplified fault model

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

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

Copyright International Electrotechnical Commission

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.

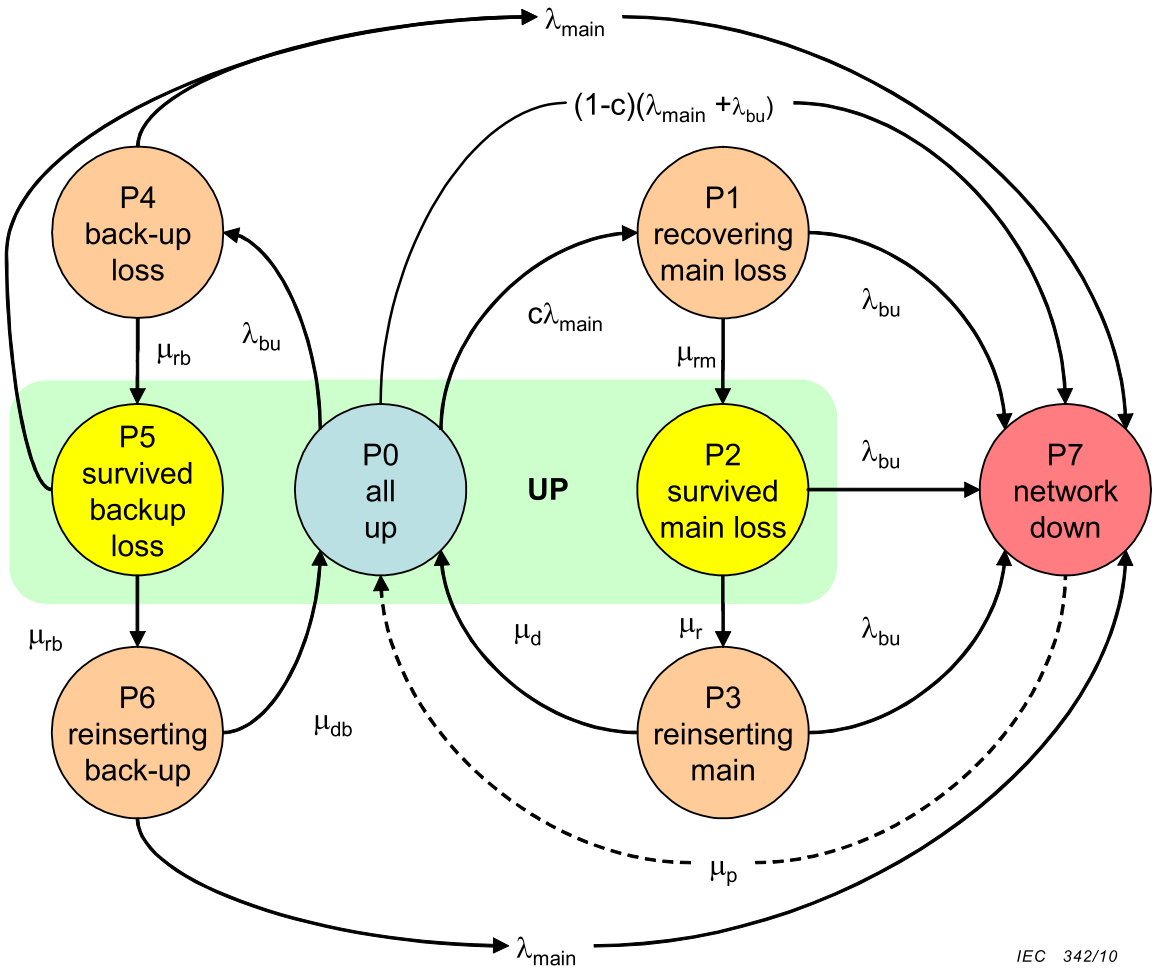


Figure 15 – Asymmetric fault model

Copyright International Electrotechnical Commission

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.

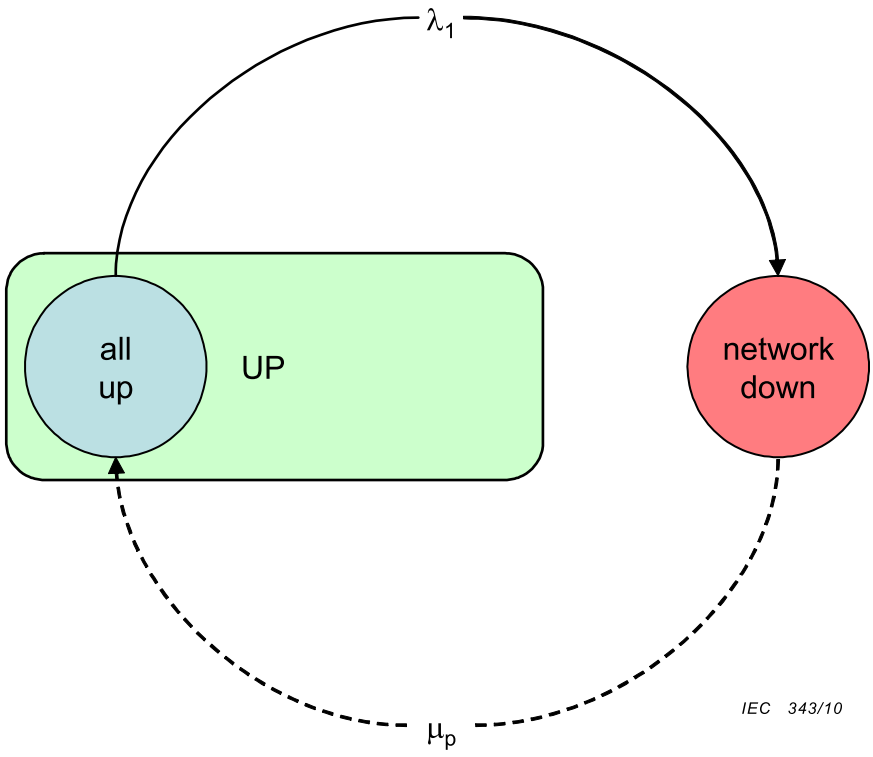


Figure 16 – Network with no redundancy

Therefore, the MTTFN simplifies into Equation (3).

$$\text{MTTFN} = \frac{1}{\lambda_1} \tag{3}$$

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

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):

Copyright International Electrotechnical Commission

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

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.

Copyright International Electrotechnical Commission

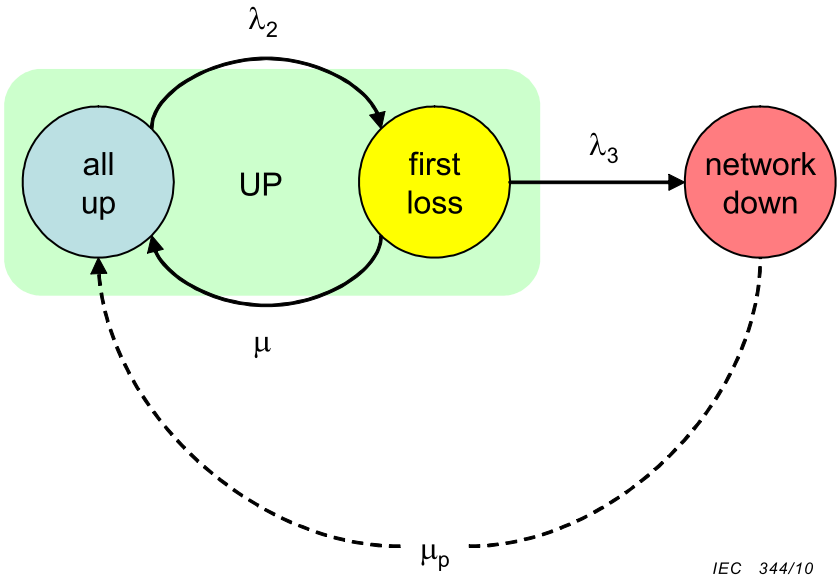


Figure 17 – Network with no single point of failure

The MTTFN simplifies to Equation (5):

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

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 MTTFS 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.

Copyright International Electrotechnical Commission

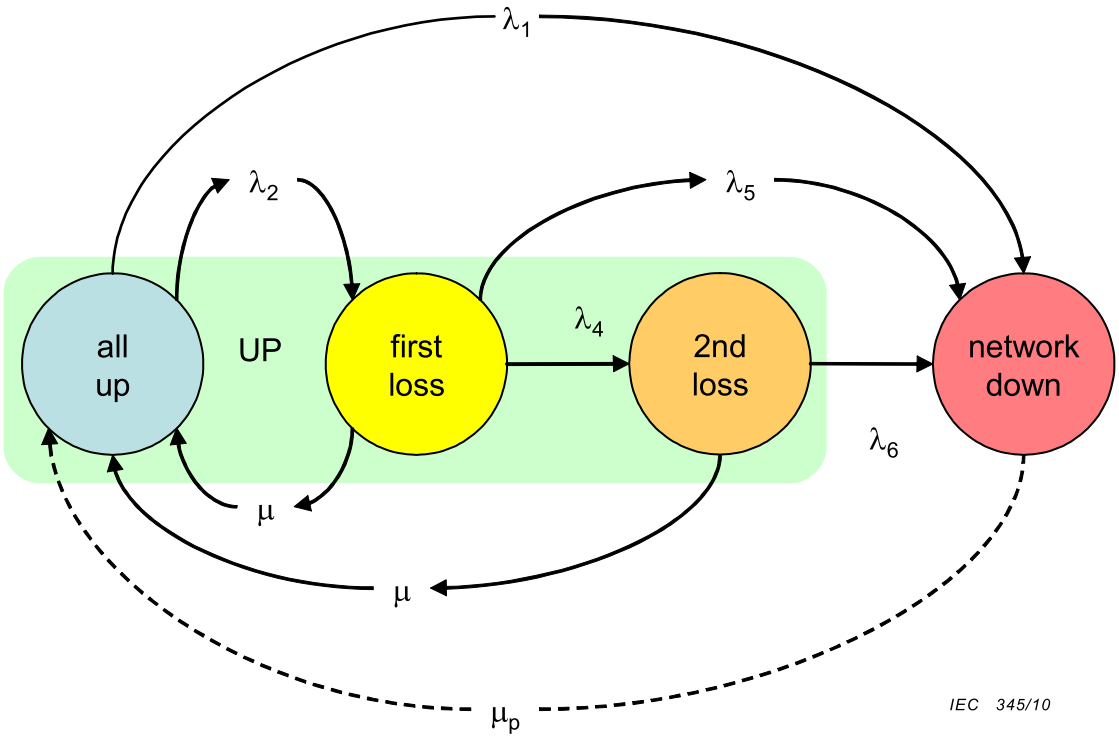


Figure 18 – Network with resiliency to second failure

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).

$$MTTFN = \frac{(\mu + \lambda_2 + \lambda_4 + \lambda_5) + \frac{\lambda_2 \lambda_4}{\mu + \lambda_6}}{\lambda_1(\mu + \lambda_4 + \lambda_5) + \lambda_2\left(\lambda_5 + \lambda_4\left(\frac{1}{1 + \frac{\mu}{\lambda_6}}\right)\right)} \quad \mu >> \sum(\lambda_i) \quad \approx \quad \frac{1}{\lambda_1 + \frac{\lambda_2^2 f}{\mu}} \tag{6}$$

Copyright International Electrotechnical Commission

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 λ_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~~ predictible 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.

Copyright International Electrotechnical Commission

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:

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

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

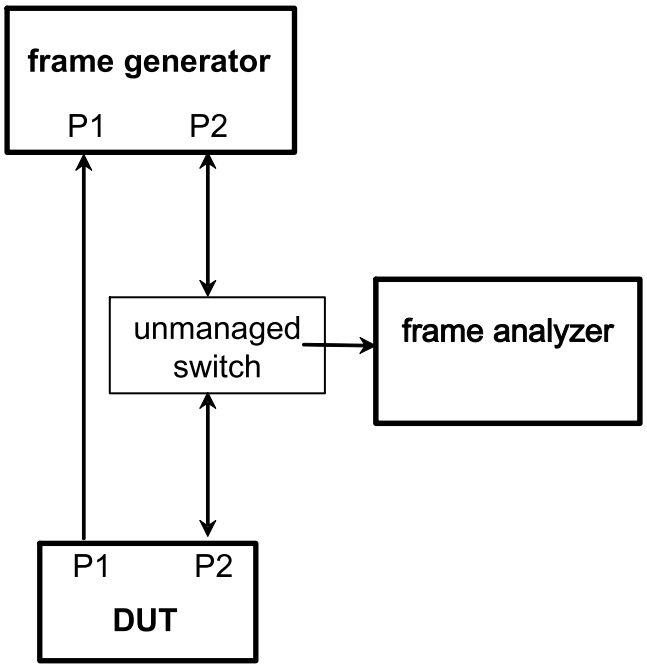


Figure 19 –Test rig for T_{PA} measurement

b) Configure DUT so that the connected ports ‘AdminEdge’ and ‘AutoEdge’ parameters are set to FALSE.

c) Configure the frame generator’s Port2 to send a Proposal BPDU (i.e. with the “proposal” flag set and “root bridge ID” better than DUT’s).

d) Configure frame generator’s Port1 only to maintain an Ethernet link but not to send any frames. This port will simulate another RSTP switch to which the DUT will propagate a proposal.

e) Configure the frame analyzer to capture frames received from the unmanaged switch.

8.4.1.3 Procedure

The procedure is as follows:

a) verify that DUT has elected itself as “root”.

b) start capturing frames in frame analyzer.

c) transmit a single BPDU from frame generator.

d) stop capturing frames.

e) verify that DUT sent “agreement” BPDU in response to the “proposal” BPDU.

f) measure the time interval between the “proposal” BvPDU and the first “agreement” BPDU.

8.4.2 Measurement of T_L

8.4.2.1 Measurement

This test is actually measuring (T_L + T_{Proc}) time. Given that T_{Proc} has been measured by the previous test, T_L is deduced from (T_L + T_{Proc}).

8.4.2.2 Setup

Configure the system as follows:

a) build the network as shown in Figure 20.

Copyright International Electrotechnical Commission

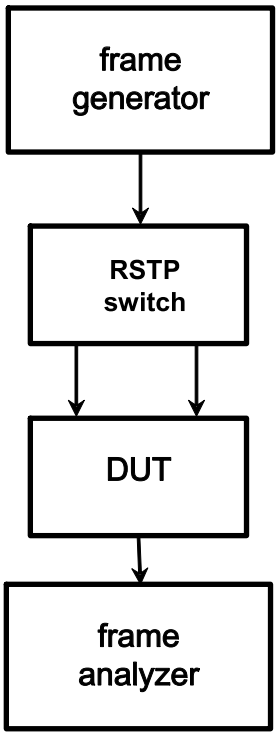


Figure 20 –Test rig for T_L measurement

b) set the RSTP switch “Bridge priority” parameter to 0 to force it to be the elected “root”.

c) configure the frame generator to send a continuous stream of arbitrary frames at a rate of at least 4 000 frames-per-second to allow time measurement resolution of 0,25 ms.

d) configure the frame analyzer to capture frames received from DUT.

8.4.2.3 Procedure

The procedure is as follows:

a) verify that the RSTP switch has been elected “root”.

b) verify that one of the DUT ports has a “root forwarding” status and the other port has an “alternate discarding” status.

c) start transmitting from the frame generator.

d) start capturing frames.

e) verify that frames are received by the frame analyzer.

f) break the link attached to the DUT’s “root” port. This will cause DUT to failover to its “alternate” port.

g) verify that frames are received by the frame analyzer.

h) stop capturing frames.

i) measure for how long frame receiving was disrupted.

8.4.3 Measurement of (T_{TC} + T_F)

8.4.3.1 Setup

Configure the test rig as follows:

a) build the test network as shown in Figure 21.

Copyright International Electrotechnical Commission

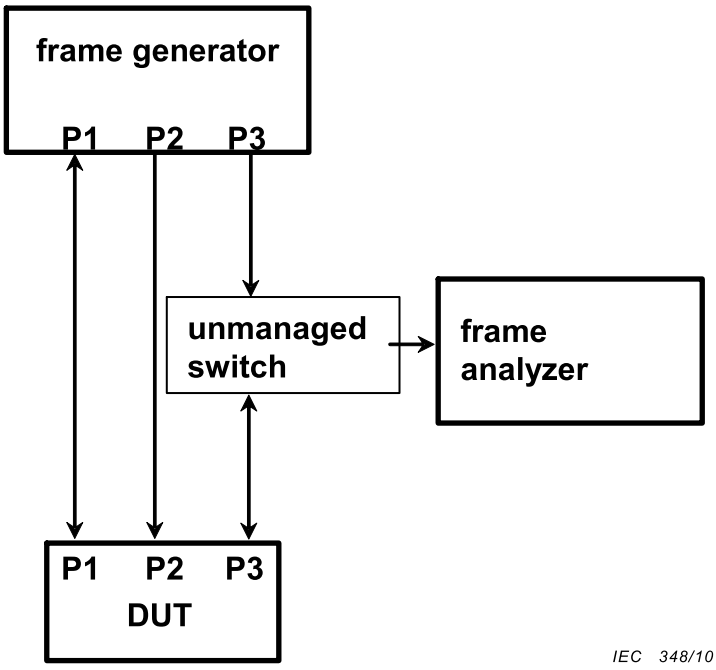


Figure 21 –Test rig for (T_{TC} + T_F) measurement

b) set DUT's Port1 and Port3 'AutoEdge' and 'AdminEdge' parameters to FALSE.

c) set DUT's Port2 'AutoEdge' parameter to FALSE and 'AdminEdge' parameter to TRUE.

d) configure the frame generator's Port1 to send a single arbitrary frame.

e) configure the frame generator's Port2 to send a continuous stream of frames to the destination MAC address of Port2 at a rate of at least 4 000 frames-per-second to allow time measurement resolution of 0,25 ms.

f) configure the frame generator's Port3 to send a single "agreement + topology change" BPDU.

g) configure the frame analyzer to capture frames received from the unmanaged switch.

8.4.3.2 Procedure

The procedure is as follows:

a) verify that DUT has elected itself as "root".

b) transmit a single frame out of the frame generator's Port1. This will make that DUT's Port1 learns the frame source MAC address.

c) start transmitting a continuous stream out of the frame generator's Port2.

d) start capturing frames in the frame analyzer.

e) verify that the stream is not forwarded out of DUT's Port3 (it is only forwarded out of DUT's Port1).

f) send a single BPDU from the frame generator's Port3. This will cause the DUT to flash its MAC address table and start flooding the traffic stream out of Port3 so it will be captured by the frame analyzer.

g) stop capturing frames.

h) verify that the DUT started flooding out of Port3 in response to the "topology change" BPDU.

i) measure the time interval between the "topology change" BPDU and the first stream frame.

j) repeat a) … i) for 10 different randomly chosen values of the source MAC address used by the frame generator's Port1 (and thus the destination MAC address used by the frame generator's Port2) and chose the maximum value among all measurements.

Copyright International Electrotechnical Commission

8.4.4 System test example

8.4.4.1 Setup

Configure the system as follows:

a) build a switch ring of 20-40 switches which comply with the IEEE 802.1D:2004 RSTP specification as shown in Figure 22.

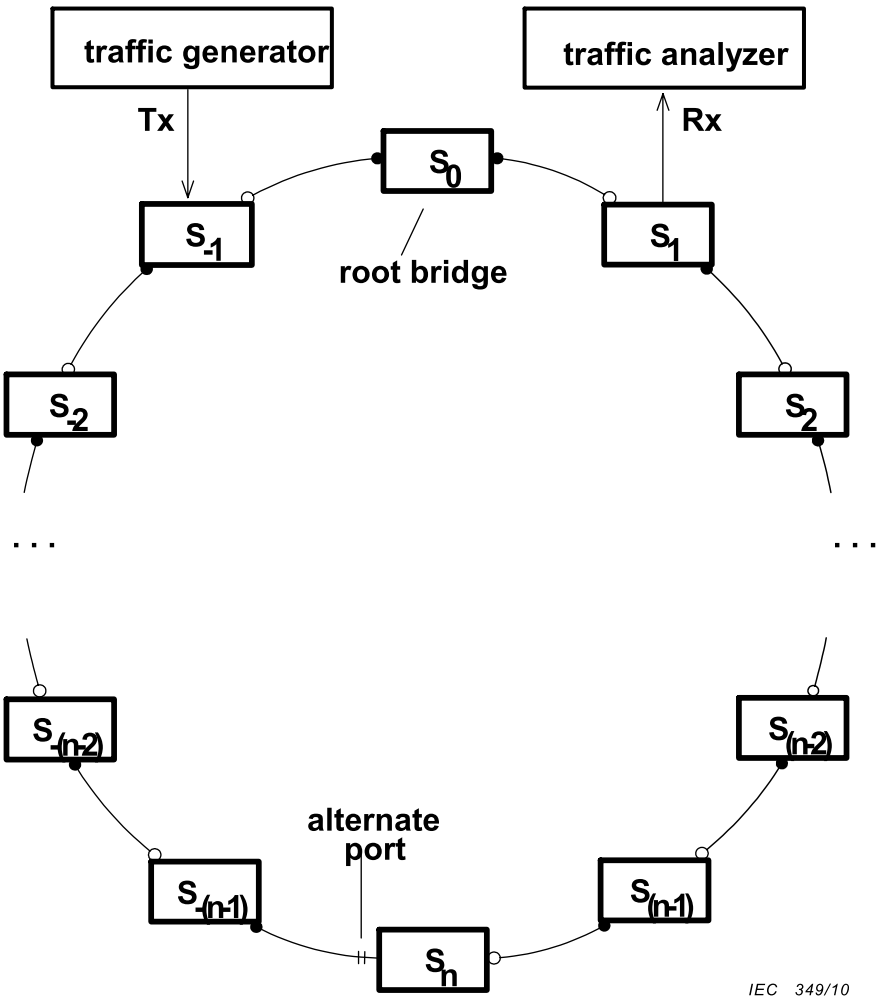


Figure 22 –Test rig for system test

b) ensure that all links comply with the deployment requirements specified in 8.2.

c) configure the traffic generator to send frames destined to the Rx port's MAC address out of its Tx port. Transmission rate should be chosen high enough so that a fault recovery time could be calculated based on a number of lost packets with a millisecond resolution.

d) configure the traffic generator to send low rate (e.g. once in a few seconds) arbitrary frames out of its Rx port with the Rx port's source MAC address (so that switches would learn it).

e) configure the traffic analyzer to display Tx and Rx frame counters.

f) set all switches RSTP parameters to default values. Verify that all switches have their "bridge priority" set to 32 768.

g) set switch S_0 "bridge priority" to 0, so that S_0 will be elected a root switch.

h) set switch S_1 "bridge priority" to 4 096, so that S_1 will be the next best root candidate after S_0.

Copyright International Electrotechnical Commission

8.4.4.2 Procedure

The procedure is as follows:

a) verify that alternate port is on the S_n switch, S_n–$S_{-(n-1)}$ link.

b) start transmitting low rate dummy frames out of traffic Rx port. Verify that switches S_{-1}, S_0 and S_1 learned the Rx port's MAC address.

c) start transmitting frames out of the Tx port. Verify that the Rx counter is incrementing along with the Tx counter and no traffic is lost.

d) break the S_0–S_1 link.

e) verify that the Rx counter is incrementing (i.e. connectivity has recovered).

f) stop transmitting out of the Tx port.

g) read the Tx and Rx counters and calculate number of lost frames.

h) calculate the fault recovery time using formula t = (number of lost frames) / (frame rate).

8.5 RSTP topology limits and maximum recovery time

NOTE In the next edition of IEC 62439-1, this new Subclause 8.5 will be renumbered as 8.2.

8.5.1 RSTP protocol parameters

This subclause explains the RSTP protocol parameters that impact network recovery times and shows how a specific topology and protocol configuration influence them. First, RSTP-specific terms are defined. Then, basic guidelines on network design are given and finally a method to determine an approximation of an upper bond worst case network reconfiguration time for meshed RSTP networks is given.

This subclause particularly deals with RSTP networks that are composed of more than a single ring. For a single Ethernet ring running RSTP, the network reconfiguration time can be determined as 8.2 shows. However, the subsequent statements concerning RSTP parameters are also applicable in a ring network.

8.5.2 RSTP-specific terms and definitions

NOTE These terms are inherited from IEEE 802.1D.

8.5.2.1 Transmission Hold Count (TxHoldCount)

Each port of an RSTP bridge includes a counter TxHoldCount. This counter starts at zero and is incremented for each BPDU the port sends. A timer decrements every second the counter. If TxHoldCount reaches the maximum value, no further BPDU are transmitted over that port until the counter has been decremented again, regardless of the importance of the BPDU to network reconfiguration. The default maximum value of TxHoldCount is 6 and the maximum configurable number is 10.

8.5.2.2 Bridge Max Age

Each RSTP bridge includes a parameter Bridge Max Age that should be configured to the same value in each bridge. Bridge Max Age defines the maximum total number of "physical hops" or links between the root bridge and any bridge participating in the same RSTP network. Its default value is 20 and it can be configured to from 6 to a maximum of 40. In special cases, Bridge Max Age is configured differently in some bridges.

Because Bridge Max Age defines the maximum extension of an RSTP network, it is sometimes referred to as "network diameter". But "Bridge Max Age" and the actually usable network diameter are not synonymous, see 8.5.2.4.

Copyright International Electrotechnical Commission

8.5.2.3 Message Age

Each BPDU includes a parameter Message Age. Upon reception of a BPDU, a bridge increments Message Age and afterwards compares it to its “Bridge Max Age”. If Message Age is larger than Bridge Max Age, the bridge discards the BPDU and ignores the information it carries.

The root bridge starts by sending BPDUs with Message Age = 0. The first bridge after the root bridge (and subsequent bridges until Message Age reaches Bridge Max Age) receives the BPDU, increment “Message Age” by 1, compares it to the “Bridge Max Age” and transmit BPDUs with the updated information.

8.5.2.4 Network diameter and radius

The “diameter” in an RSTP network is the number of bridges on the longest active path in a network tree between the two bridges that are the farthest away from each other. The diameter does not necessarily correspond to the RSTP parameter Bridge Max Age (see Figure 23).

The ”radius” in a RSTP network is the number of bridges from (and including) the active root bridge to the bridge that is the farthest away from this active root in the topology. This is the length (in hops) of the longuest path over which the RSTP protocol information needs to be forwarded (see Figure 23). The maximum supported radius by RSTP can be defined as:

max. radius = Bridge Max Age + 1.

The radius is important to determine worst case topologies. In a worst case fault situation (without an engineered network and consciously placed root bridges), upon failure of a root bridge, the farthest away leaf might be the backup root bridge, which might become the next root. In this case, the diameter of the network can become the radius and it becomes the actual path that the RSTP information to the individual bridges has to travel. (See Figure 23)

NOTE RSTP BPDUs are only transmitted on the link between two directly connected bridges. Each bridge consumes and produces these BPDUs, but the RSTP information which they carry travels distinct paths through the network (in a stable network state without reconfiguration).

Copyright International Electrotechnical Commission

8.5.3 Example of a small RSTP tree

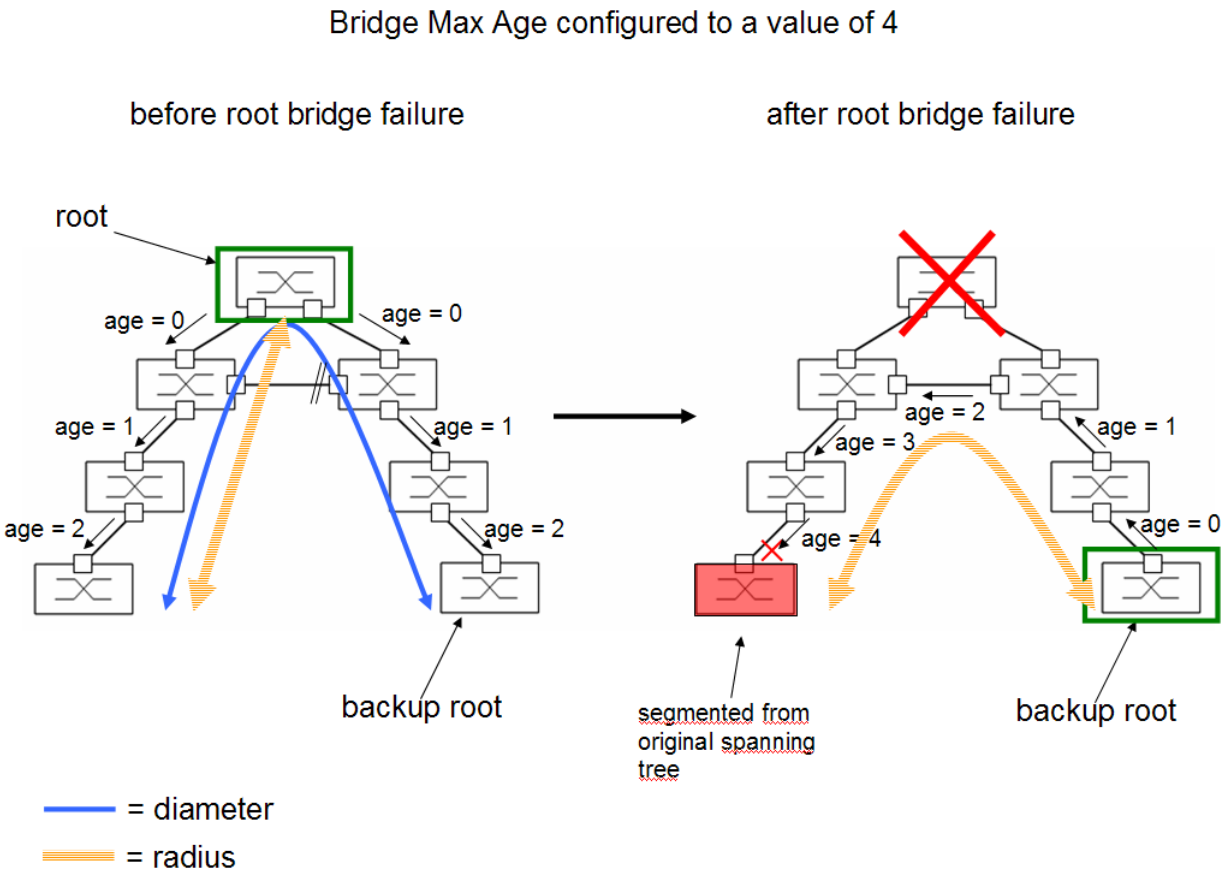


Figure 23 – Diameter and Bridge Max Age

NOTE 1 The RSTP parameter Bridge Max Age has been assigned the value 4 for the sake of this example although 802.1D does not allow a value lower than 6.

In the example of Figure 23, at first, the network without a failure is in a stable condition with Bridge Max Age = 4 and because the actual radius is 4 (the RSTP configuration could support a maximum radius of 5). The diameter is 7, from one leaf in one branch to the other leaf in the other branch, via the root bridge. Because the root bridge is the root element of a balanced tree, Bridge Max Age = 4 is sufficient for all bridges to receive RSTP BPDUs from the same RSTP root.

A root bridge failure and an unfavorable backup root election changes that. After a root bridge failure, the redundant link that was formerly blocked is activated. The diameter is now 6. At the same time, the radius is also increased to 6. Because one of the leaves of the original branches has now become the root bridge, the Bridge Max Age of 4 is not sufficient for the RSTP root information to reach all bridges of the network, because the RSTP information now has to travel the whole diameter, which is now equivalent to the radius. Thus, the last bridge is segmented, as indicated in Figure 23. This bridge discards the BPDU, because the Message Age has exceeded the configured Bridge Max Age.

To engineer stable and high performance networks, it is necessary to observe and understand the difference between the network diameter and the radius, respectively the Bridge Max Age parameter. The Bridge Max Age parameter is kept as high as necessary not to segment any device in a worst case fault scenario and as low as possible to minimize the network recovery time as shown in the following subclauses. The network radius determines the necessary Bridge Max Age value for each considered topology. The Bridge Max Age can be kept low by

Copyright International Electrotechnical Commission

positionning both root bridge and backup root bridge at a central position in the network, e.g. on the main ring of a hierarchical multi-ring topology.

NOTE 2 Another method, which is not covered in this document, is to configure different Bridge Max Age values on root and backup root bridge, according to their respective positions in the network.

8.5.4 Assumption on TxHoldCount

Calculation or approximation of an upper bond reconfiguration time is made under the assumption that the Transmit Hold Count (TxHoldCount) is never reached and no BPDU necessary for fast reconfiguration of the network is lost.

This however can occur in practice, especially during network reconfiguration. As soon as the TxHoldCount of one bridge port becomes “saturated”, all bridges connected to the saturated port won’t receive any BPDUs any more until the TxHoldCount has been decremented. If the dropped BPDUs are vital for network reconfiguration, the network reconfiguration time can be extended by several seconds. This assumption is of high practical relevance and is considered as the biggest threat to the network reconfiguration time of RSTP networks.

8.5.5 Worst case topology and radius determination

Because the worst case radius and the lowest possible Bridge Max Age parameter are correlated, determining the worst case radius is important in determining the upper bond worst case reconfiguration time.

In an arbitrarily meshed network, the reconfigured links of the network in steady state after reconfiguration can be predicted prior to the failure, but as the protocol is based on reception and sending BPDUs in each individual bridge, race conditions can occur during reconfiguration. Therefore the maximum reconfiguration time can only be given as a worst case bound based on the maximum reaction time of each bridge and the maximum number of hops allowed by the protocol.

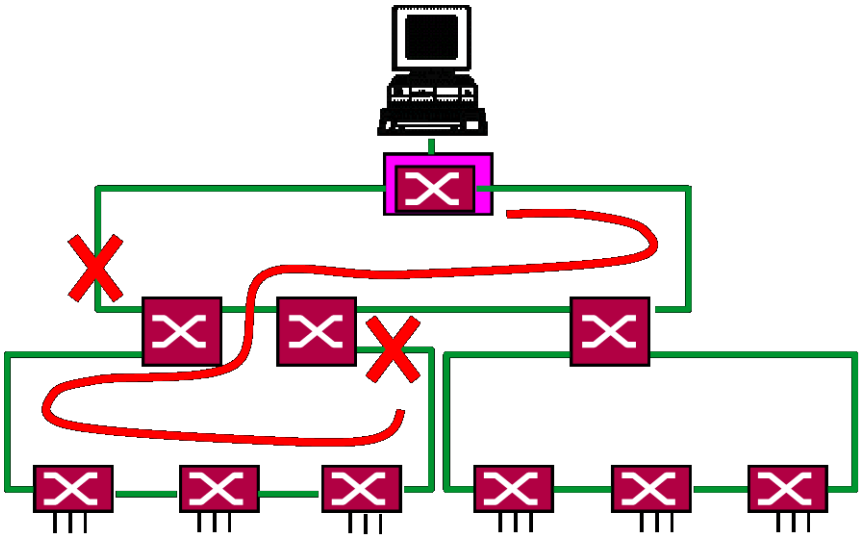
In addition, some media such as 1000Tx present large link failure detection times. Indeed, auto-negotiation disabled on fiber Gigabit links may jeopardize RSTP failover time in case of link failure.

NOTE Malicious failures such as a bridge unable to forward payload frames but still exchanging BPDUs with its neighbors cannot be considered in the calculations.

When designing a network that operates with RSTP, the network radius from the root-bridge location and from the backup root location to the farthest away leaf bridge has to be calculated.

This radius calculation also considers a worst case failure, because failures in the topology can increase the radius. As an example, Figure 24 shows the root bridge and the backup root bridge located on the main ring. The worst case radius for this specific topology is reached by two simultaneous failures positioned as Figure 24 shows, which is 7 for the indicated root.

Copyright International Electrotechnical Commission



IEC 954/12

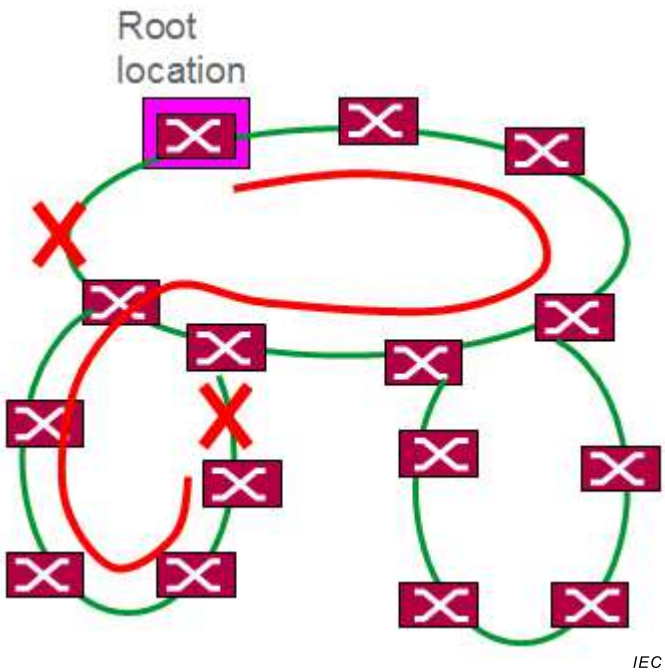
Figure 24 – Worst path determination

Once the worst case radius value for a worst case failure scenario in the network topology has been determined, Bridge Max Age should be configured to exactly this number - 1. This minimizes the upper bond reconfiguration time of the network, since a lower Bridge Max Age limits the time that BPDUs circulate in the network.

8.5.6 Method to determine the worst case radius in case of a ring-ring architecture

In a ring of rings topology, the main ring is made of “N” bridges + 2 × “M” bridges that connect “M” sub-rings redundantly, each made of “R” bridges (excluding the bridge to connect on the main ring).

Figure 25 shows an example of a main ring (N = 3) with two sub-rings (M = 2) connected redundantly via a total of four bridges (two per sub-ring) to the main ring, with R = 4.



IEC 955/12

Figure 25 – Example ring-ring topology

Copyright International Electrotechnical Commission

Root bridge and backup root bridge remain on the main ring (this is ensured by configuring the RSTP priority of root and backup root on the main ring with a better priority value than any other bridge in the sub-rings).

Only one failure at the main ring and one failure at the sub-ring are considered. Sustaining one failure in the main ring and simultaneously a second failure in a sub-ring is a corner case.

Then the worst case radius (i.e. the Bridge Max Age that needs to be configured which is equivalent to the worst case radius - 1) is:

$$\text{worst case radius} = N + 2 \times M + R$$

$$\text{Bridge Max Age} = (\text{worst case radius} - 1) = N + 2 \times M + R - 1$$

where

“R” is the number of bridges in the sub-ring with the highest number of devices;

“N” is the number of bridges in the main ring (excluding the bridges that connect the sub-rings);

“M” is the number of bridges in the main ring that connect the main ring to the sub-rings.

In the diagram above, considering that N=3, M=2, R=4, the worst case radius = 11.

Thus, the RSTP protocol parameter “Bridge Max Age” should be configured to a value of 10 to optimize network recovery times.

8.5.7 Worst case radius of an optimized multilayer architecture

With a large number of bridges, the network topology should be optimized in order not to reach the Bridge Max Age limit and to keep worst case reconfiguration times low.

A simple solution is to consider a multilayer topology, consisting of “L” layers, as shown in Figure 26:

Copyright International Electrotechnical Commission

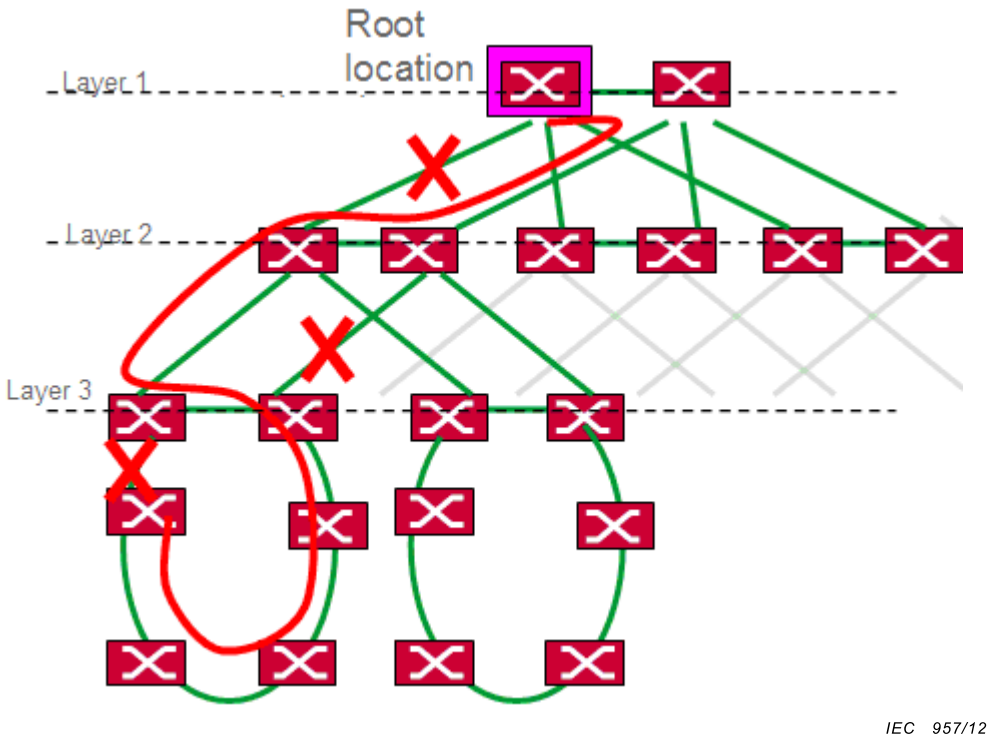


Figure 26 – Example multilayer topology

The upper layer is made of 2 main bridges which are set to be the root/backup root bridges. (Priority value of these bridges is expected to be set consequently to the highest and second to highest priority).

The maximum size of layer 3 is defined by sub-rings made of “R” bridges. The parameter “R” excludes the bridges that connect the individual layer 3 subring to layer 2, which is taken into the calculation through the parameter “L”.

Only one failure per layer is considered.

Then the worst case radius is equal to:

$$\text{worst case radius} = (2 \times L) + R$$

In the above diagram, L=3, R=4, and therefore, worst case radius = 10. This results in a Bridge Max Age parameter of 9.

The interesting point is that this result is not dependant on the number of branch-offs per layers, and this topology is possibly able to support a large number of nodes with a low Bridge Max Age parameter. The limitation is the maximum number of ports of the bridges used at each layer: A large number of physical ports is detrimental to RSTP performance on bridges.

8.5.8 Approximated upper bond reconfiguration time for RSTP networks

The RSTP root bridge failure is the worst case scenario aftecting reconfiguration time. The upper bond reconfiguration time is the time needed for recovery after a root bridge failure. The recovery time for link failures or non-root bridge failures will not exceed the root bridge failure recovery time. Since it is the worst case scenario, the recovery time subsequently is estimated for a root bridge failure.

Copyright International Electrotechnical Commission

When considering the network reconfiguration time of a meshed RSTP network, three distinct phases can be identified:

– Aging phase: The phase in which the fault in the network is detected and in which multiple root information (old and new root priority vectors) are still present in the network. The old root information can still circulate around in the network until the Message Age in the BPDUs reaches the Bridge Max Age value. Only after the old root priority vector from the failed root bridge has been completely eliminated from the network, can the backup root priority vector prevail. The aging phase is therefore the time from the fault to the moment, when the old root BPDU priority vector is eliminated and, in a worst case situation, any other, inferior new temporary root vector reaches the backup root bridge and triggers the converging phase.

– Converging phase: The phase in which the backup root broadcasts its new root vector to the network and is no longer disturbed by old root vector information. The converging phase immediately starts after the aging phase and ends when the bridge farthest away from the new backup root has received the new root information.

– Flushing phase: After the reconfiguration of the active topology, several bridges could flush their filtering databases to make certain that the new communication paths are learned properly. RSTP uses Topology Change (TC) BPDUs to initiate flushing. With a worst case assumption, this phase begins immediately after the converging phase and ends after the Topology Change notification from the bridge farthest away from the root has reached the root bridge.

NOTE When a root bridge fails, usually more than one bridge claims root. But as the backup root has the best remaining priority, its priority vector quickly (one single priority propagation through the topology) prevails against the other temporary root bridges. But in a worst case scenario, the better priority vector from the old root may still “circulate” around much longer. This is, therefore, the limiting element that defines the length of the aging phase.

The total upper bond reconfiguration time Trec of a meshed RSTP network can therefore be approximated as:

$$Trec = TL + Tage + Tconv + Tflush$$

where:

Tage = 2 × Bridge Max Age × TPA;

Tconv = worst case radius × TPA;

Tflush = worst case radius × TTC;

TL is the maximum time required by a bridge to detect a link failure (depends on the link type);

TPA is the maximum time required by a pair of bridges to perform RSTP Proposal Agreement handshaking; equal to the sum of the BPDU processing times in both bridges of the pair. TPA values may differ from vendor to vendor and from product to product;

TTC is the time an Ethernet bridge needs to process an RSTP topology change.

Typical values for “fast RSTP” implementation:

TPA = 5 ms when the vendor claims a 5 ms/hop recovery time

TL = 4-6 ms for 100BASE-TX and 100BASE-FX links

= 20 ms for 1000BASE-X links

= 700 ms for 1000BASE-T links (defined by the ISO/IEC 8802-3)

Copyright International Electrotechnical Commission

This approximation shows that it is beneficial for the total recovery time to set the Bridge Max Age parameter as high as necessary to support the given topology (with respect to possible failures), but as low as possible to minimize its impact on the network recovery time.

This approximation of recovery time covers the worst case scenario, the root bridge failure. When comparing the likeliness of a root bridge failure to the likeliness of a non-root or link failure, a root bridge failure is far more unlikely (when similar failure probabilities for all participating devices and media are assumed) because for each root bridge there is a large number of media connections and non-root bridges that may fail before.

Therefore, the typical recovery time will be faster than the worst case recovery time that can be approximated by this clause, but this cannot be counted on.

NOTE There may be an additional effect when a bridge with multiple ports connected to the RSTP network is becoming a part of the active topology (especially when this device is elected root), that the sending of BPDUs on the multiple ports is not totally simultaneous. This may be complicated further with different media on these multiple ports. The reconfiguration time may be stretched by this effect.

Copyright International Electrotechnical Commission

Bibliography

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

IEC/TR 61158-1, *Industrial communication networks – Fieldbus specifications – Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series*

IEC/TR 61158-6 (all parts), *Industrial communication networks – Fieldbus specifications – Part 6: Symmetrical pair/quad cables with transmission characteristics up to 1 000 MHz – Work area wiring*

IEC 61588, *Precision clock synchronization protocol for networked measurement and control systems*

IEC 61784-2:2007, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*

IEC 61918:2007, *Industrial communication networks – Installation of communication networks in industrial premises*

IEC 62439-2, *Industrial communication networks – High availability automation networks – Part 2: Media Redundancy Protocol (MRP)*

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

IEC 62439-4, *Industrial communication networks – High availability automation networks – Part 4: Cross-network Redundancy Protocol (CRP)*

IEC 62439-5, *Industrial communication networks – High availability automation networks – Part 5: Beacon Redundancy Protocol (BRP)*

IEC 62439-6, *Industrial communication networks – High availability automation networks – Part 6: Distributed Redundancy Protocol (DRP)*

IEC 62439-7, *Industrial communication networks – High availability automation networks – Part 7: Ring-based Redundancy Protocol (RRP)*

ISO/IEC 2382 (all parts), *Information technology – Vocabulary*

ISO/IEC 9646 (all parts), *Information technology – Open Systems Interconnection – Conformance testing methodology and framework*

ISO/IEC 10731, *Information technology – Open Systems Interconnection – Basic Reference Model – Conventions for the definition of OSI services*

ISO/IEC 11801:2002, *Information technology – Generic cabling for customer premises*
Amendment 1 (2008)

ISO/IEC 15802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Common specifications – Part 3 : Media Access Control (MAC) Bridges*

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

Copyright International Electrotechnical Commission

PUSTYLNIK M., ZAFIROVIC-VUKOTIC, M., MOORE, R., *Performance of the Rapid Spanning Tree Protocol in Ring Network Topology, Rugged Com. Inc.*
http://www.ruggedcom.com/pdfs/white_%20papers/performance_of_rapid_spanning_tree_protocol_in_ring_network_topology.pdf

Copyright International Electrotechnical Commission

SOMMAIRE

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX INDUSTRIELS DE COMMUNICATION – RÉSEAUX D'AUTOMATISME À HAUTE DISPONIBILITÉ–

Partie 1: Concepts généraux et méthodes de calcul

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.

2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.

3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.

4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.

5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.

6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.

7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.

8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.

9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

DÉGAGEMENT DE RESPONSABILITÉ
Cette version consolidée n'est pas une Norme IEC officielle, elle a été préparée par commodité pour l'utilisateur. Seules les versions courantes de cette norme et de son(ses) amendement(s) doivent être considérées comme les documents officiels.

Cette version consolidée de l'IEC 62439-1 porte le numéro d'édition 1.2. Elle comprend la première édition (2010-02) [documents 65C/583/FDIS et 65C/589/RVD], son amendement 1 (2012-06) [documents 65C/684/FDIS et 65C/691/RVD] et son amendement 2 (2016-02) [documents 65C/834/FDIS et 65C/841/RVD]. Le contenu technique est identique à celui de l'édition de base et à ses amendements.

Copyright International Electrotechnical Commission

Dans cette version Redline, une ligne verticale dans la marge indique où le contenu technique est modifié par les amendements 1 et 2. Les ajouts sont en vert, les suppressions sont en rouge, barrées. Une version Finale avec toutes les modifications acceptées est disponible dans cette publication.

La Norme internationale IEC 62439-1 a été établie par le sous-comité 65C: Réseaux industriels, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'IEC 62439 (2008):

– ajout d'une méthode de calcul pour le protocole RSTP (Rapid Spanning Tree Protocol, IEEE 802.1Q),
– ajout de deux nouveaux protocoles de redondance: HSR (High-availability Seamless Redundancy) et DRP (Distributed Redundancy Protocol),
– déplacement des Articles 1 à 4 (Introduction, Définitions, Aspects généraux) et des Annexes (taxinomie, calcul de disponibilité) dans l'IEC 62439-1, qui servent à présent de base aux autres documents,
– déplacement de l'Article 5 (MRP) dans l'IEC 62439-2 avec peu de modifications éditoriales,
– déplacement de l'Article 6 (PRP) dans l'IEC 62439-3 avec peu de modifications éditoriales,
– déplacement de l'Article 7 (CRP) dans l'IEC 62439-4 avec peu de modifications éditoriales, et
– déplacement de l'Article 8 (BRP) dans l'IEC 62439-5 avec peu de modifications éditoriales,
– ajout d'une méthode de calcul du temps de reprise maximal du protocole RSTP dans une configuration restreinte (anneau) dans l'IEC 62439-1 (Article 8),
– ajout de spécifications du protocole HSR (High-availability Seamless Redundancy), qui partage les principes du protocole PRP dans l'IEC 62439-3 (Article 5), et
– introduction du protocole DRP (IEC 62439-6).

La version française de cette norme n'a pas été soumise au vote.

Cette publication a été rédigée selon les Directives de l'ISO/IEC, Partie 2.

Une liste de la série IEC 62439 est disponible sous le titre général "*Réseaux industriels de communication – Réseaux de haute disponibilité pour l'automation"* sur le site Web de l'IEC.

Le comité a décidé que le contenu de la publication de base et de ses amendements ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

Copyright International Electrotechnical Commission

INTRODUCTION

La série IEC 62439 spécifie les principes pertinents relatifs aux réseaux haute disponibilité satisfaisant aux exigences des réseaux d'automatisation industriels.

À l'état exempt de panne du réseau, les protocoles de la série IEC 62439 assurent une communication de données fiable et conforme à l'ISO/IEC 8802-3 (IEEE 802.3) et préservent le caractère déterministe des communications de données en temps réel. En cas de panne, de retrait et d'insertion d'un composant, ils assurent des temps de reprise déterministes.

Ces protocoles conservent la totalité des fonctions de communication Ethernet classiques telles qu'elles sont utilisées dans le monde professionnel, de sorte que le logiciel impliqué reste applicable.

Le marché a besoin de plusieurs solutions réseau, présentant chacune des caractéristiques de performance et des capacités fonctionnelles différentes, correspondant aux diverses exigences d'application. Ces solutions prennent en charge différents mécanismes et topologies de redondance qui sont présentés dans l'IEC 62439-1 et spécifiés dans les autres parties de la série IEC 62439. L'IEC 62439-1 distingue également les différentes solutions, en donnant à l'utilisateur des lignes directrices.

La série IEC 62439 se conforme à la structure et aux termes généraux de la série IEC 61158.

Copyright International Electrotechnical Commission

RÉSEAUX INDUSTRIELS DE COMMUNICATION – RÉSEAUX D'AUTOMATISME À HAUTE DISPONIBILITÉ–

Partie 1: Concepts généraux et méthodes de calcul

1 Domaine d'application

La série IEC 62439 s'applique aux réseaux de haute disponibilité pour l'automatisation reposant sur la technologie 8802-3 (IEEE 802.3) (Ethernet) de l'ISO/IEC.

La présente partie de la série IEC 62439 spécifie

- les éléments communs et les définitions pour d'autres parties de la série IEC 62439;
- la spécification d'essai de conformité (normative);
- un système de classification pour les caractéristiques de réseau (informative);
- une méthodologie pour l'estimation de la disponibilité du réseau (informative);
- les règles de configuration, la méthode de calcul et de mesure pour un temps de reprise déterministe dans le protocole RSTP.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60050-191:1990, *Vocabulaire Électrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service*

IEC 61158 (toutes les parties), *Réseaux de communication industriels – Spécifications des bus de terrain*

IEC 61158-6-10, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-10: Spécification de protocole de couche application – Éléments de Type 10*

ISO/IEC 8802-3:2000, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseaux locaux et métropolitains – Prescriptions spécifiques – Partie 3: Accès multiple par surveillance du signal et détection de collision (CSMA/CD) et spécifications pour la couche physique*

IEEE 802.1Q*, IEEE standards for local and metropolitan area network. Virtual bridged local area networks (disponible en anglais seulement)*

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

IETF RFC 791, *Internet Protocol (Protocole Internet)*; disponible à l'adresse <http://www.ietf.org>

Copyright International Electrotechnical Commission

3 Termes, définitions, abréviations, acronymes et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'IEC 60050-191 ainsi que les suivants s'appliquent.

3.1.1
disponibilité
aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens nécessaires est assurée

NOTE 1 La disponibilité dépend de la fiabilité, de la maintenabilité et de la logistique de maintenance.

NOTE 2 Les moyens extérieurs nécessaires, autres que la logistique de maintenance, n'influencent pas la disponibilité de l'entité.

[VEI 191-02-05]

3.1.2
canal
connexion de couche 2 entre deux nœuds d'extrémité, qui consiste en un ou plusieurs chemins (pour la redondance) entre les nœuds d'extrémité

3.1.3
défaillance en mode commun
défaillance qui affecte tous les éléments redondants pour une fonction donnée en même temps

3.1.4
défaillance complète
défaillance qui entraîne l'inaptitude complète d'une entité à accomplir toutes les fonctions requises

[VEI 191-04-20]

3.1.5
connexion
relation logique entre deux nœuds

3.1.6
couverture
probabilité qu'une défaillance est découverte dans un délai assez court pour que la redondance puisse y faire face, exprimant également le pourcentage de défaillances rattrapées par la redondance par rapport au nombre total de défaillances

3.1.7
commutation à la volée (cut-through)
technologie dans laquelle un nœud de commutation commence à émettre une trame reçue avant que cette trame ne soit complètement reçue

3.1.8
défaillance par dégradation
défaillance qui est à la fois une défaillance progressive et une défaillance partielle

[VEI 191-04-22]

Copyright International Electrotechnical Commission

3.1.9
sûreté de fonctionnement
ensemble des propriétés qui décrivent la performance de disponibilité et les facteurs qui la conditionnent: fiabilité, maintenabilité et logistique de maintenance

NOTE La sûreté de fonctionnement est une notion générale sans caractère quantitatif.

[VEI 191-02-03]

3.1.10
appareil
entité physique connectée au réseau composé d'éléments de communication et éventuellement d'autres éléments fonctionnels

NOTE Les appareils sont par exemple des nœuds, des routeurs et des commutateurs.

3.1.11
nœud à double association
nœud qui dispose de deux ports pour des fins de fonctionnement redondant

3.1.12
port d'extrémité
port d'un commutateur connecté à une liaison en feuille

3.1.13
nœud d'extrémité
nœud qui est producteur ou consommateur de données d'application

NOTE Pour les besoins de la série IEC 62439, des spécifications supplémentaires sont données en 0.

3.1.14
erreur
écart ou discordance entre une valeur ou condition calculée, observée ou mesurée et la valeur ou condition spécifiée ou théoriquement correcte

NOTE 1 Une erreur peut être causée par un élément défectueux, par exemple une erreur de calcul faite par un ordinateur en panne.

NOTE 2 Le terme français “erreur” ("error" en anglais) peut aussi désigner "une erreur humaine" ("mistake" en anglais) (voir VEI 191-05-25).

[VEI 191-05-24, modifiée]

3.1.15
défaillance
cessation de l’aptitude d’une entité à accomplir une fonction requise

NOTE 1 Après une défaillance d’une entité, cette entité est en état de panne.

NOTE 2 Une défaillance est un passage d'un état à un autre, par opposition à une panne, qui est un état.

NOTE 3 La notion de défaillance, telle qu'elle est définie, ne s'applique pas à une entité constituée seulement de logiciel.

[VEI 191-04-01]

3.1.16
panne
état d'une entité inapte à accomplir une fonction requise, non comprise l'inaptitude due à la maintenance préventive ou à d'autres actions programmées ou due à un manque de moyens extérieurs

Copyright International Electrotechnical Commission

NOTE Une panne est souvent la conséquence d'une défaillance de l'entité elle-même, mais elle peut exister sans défaillance préalable.

[VEI 191-05-01]

3.1.17
temps de reprise de panne
temps à partir de l'événement de panne jusqu'à l'instant où le réseau retrouve sa fonction de communication requise en présence de la panne

NOTE Suite à un rétablissement après une panne, le réseau fonctionne en mode dégradé utilisant certains des éléments de redondance, ce qui réduit la tolérance aux pannes, et peut ne pas être en mesure d'effectuer un rétablissement après une deuxième panne.

3.1.18
trame
unité de transmission de données sur un MAC (Media Access Control, Commande d'Accès au Support) ISO/IEC 8802-3 qui transmet une unité de données de protocole (PDU) entre les utilisateurs de service MAC

[IEEE 802.1Q, modifiée]

3.1.19
taux de défaillance (instantané)
limite, si elle existe, du quotient de la probabilité conditionnelle que l'instant d'une défaillance d'un élément non réparée se situe dans un intervalle de temps donné (t, t + Δt) et la durée de cet intervalle de temps, Δt, lorsque Δt tend vers zéro, sachant que l'élément n'est pas tombé en panne jusqu'au début de l'intervalle de temps

[VEI 191-12-02]

NOTE Le taux de défaillance est le nombre inverse du MTTF lorsque le taux de défaillance est constant sur la durée de vie d'un élément.

3.1.20
maille inter-étage
liaison entre deux commutateurs

3.1.21
port inter-étage
port d'un commutateur connecté à un autre commutateur via une maille inter-étage

3.1.22
LAN
domaine de diffusion de couche 2 dans lequel les adresses MAC sont uniques et peuvent être traitées à partir de tout autre appareil appartenant à ce domaine de diffusion

NOTE 1 Un VLAN permet le multiplexage de plusieurs réseaux LAN sur la même infrastructure réseau.

NOTE 2 Dans le cadre de la redondance, un réseau peut être constitué de plusieurs réseaux LAN fonctionnant en redondance, auquel cas il est appelé un réseau LAN redondant.

3.1.23
liaison en feuille
liaison entre un nœud d'extrémité et le LAN

NOTE Pour les besoins de la série IEC 62439, des spécifications supplémentaires sont données en 5.2.1.3.

3.1.24
topologie linéaire
topologie où les commutateurs sont connectés en série, avec deux commutateurs connectés chacun à un seul autre commutateur et tous les autres commutateurs connectés à deux autres commutateurs (soit, connectés sous la forme d'une ligne)

Copyright International Electrotechnical Commission

NOTE 1 Cette topologie correspond à celle d'un anneau ouvert.

NOTE 2 Cette configuration est parfois nommée “configuration en chaîne”. La série IEC 62439 n'utilise pas le terme “en chaîne (daisy chain)” à cause d'une éventuelle confusion avec le terme “guirlande (daisy chain)” utilisé ailleurs pour les bus. Du point de vue de câblage, les deux configurations exigent deux mises en œuvre différentes.

[IEC 61918, 3.1.39, modifiée]

3.1.25
liaison
connexion généralement duplex, physique, point-à-point entre deux nœuds adjacents.

[ISO/IEC 11801, 3.1.51, modifiée]

NOTE Le terme “liaison” est différent de "bus", qui est un support physique de diffusion.

3.1.26
entité de redondance de liaison
entité au niveau de la couche 2 qui cache la redondance de port des couches supérieures, en transmettant aux couches supérieures les trames reçues à partir des ports redondants actifs comme si elles provenaient d'un port simple, et en transmettant aux ports redondants actifs une trame provenant des couches supérieures

3.1.27
unité de données de service de liaison
données transportées dans une couche protocolaire à la couche supérieure

NOTE L'unité de données de service de liaison dans une trame Ethernet représente le contenu de la trame située entre le champ Longueur/Type et la séquence de contrôle de trame.

3.1.28
taux moyen de défaillance
moyenne du taux de défaillance instantané sur un intervalle de temps donné $\lambda(t_1, t_2)$.

[VEI 191-12-03]

NOTE La série IEC 62439 utilise le terme “taux de défaillance” pour signifier “taux moyen de défaillance” défini par le VEI 191-12-03.

3.1.29
moyenne de temps de bon fonctionnement
MTBF
espérance mathématique de la durée de bon fonctionnement

[VEI 191-12-09]

3.1.30
durée moyenne de fonctionnement avant défaillance
MTTF
espérance mathématique de la durée de fonctionnement avant défaillance

[VEI 191-12-07]

3.1.31
moyenne des temps pour la tâche de réparation
MTTR
espérance mathématique des temps pour la tâche de réparation

[VEI 191-13-08, modifiée]

3.1.32
topologie en maille
topologie où chaque nœud est connecté à trois mailles inter-étage ou plus

Copyright International Electrotechnical Commission

3.1.33
message
série ordonnée d'octets, destinée à véhiculer des informations

NOTE Normalement utilisé pour transmettre des informations entre des homologues sur la couche Application.

[IEC 61784-2, 3.1.14]

3.1.34
réseau
système de communication constitué de nœuds d'extrémité, de liaisons en feuille et d'un ou plusieurs LAN

NOTE Un réseau peut avoir plusieurs LAN pour des fins de redondance.

3.1.35
nœud
entité du réseau connectée à une ou plusieurs liaisons

NOTE Les nœuds peuvent être soit un commutateur soit un nœud d'extrémité soit les deux.

[IEC 61784-2, 3.1.16, modifiée]

3.1.36
défaillance partielle
défaillance qui entraîne l'inaptitude d'une entité à accomplir certaines fonctions requises mais pas toutes

3.1.37
chemin
ensemble de liaisons et de commutateurs liés en série

NOTE Il peut y avoir deux ou plusieurs chemins entre deux commutateurs pour assurer la redondance.

3.1.38
installation
système qui dépend de la disponibilité du réseau d'automatisation à exploiter

EXEMPLE Les installations peuvent être des centrales électriques, des imprimantes, des systèmes de fabrication, des postes, des véhicules.

3.1.39
port
point de connexion d'un nœud au réseau

[ISO/IEC 8802-3, modifiée]

NOTE 1 Cette définition est différente d'un port TCP ou d'un port UDP, qui sont qualifiés explicitement dans la série IEC 62439, si nécessaire.

NOTE 2 Un port inclut une mise en œuvre de couche 1 et de couche 2.

3.1.40
reprise
événement lorsque le réseau redevient capable d'assurer sa fonction de communication requise après une interruption

NOTE Des exemples d'interruptions pourraient être une panne ou le retrait et la réinsertion d'un composant.

3.1.41
temps de reprise
durée de rétablissement
durée entre l'interruption et la reprise

Copyright International Electrotechnical Commission

3.1.42
redondance
existence, dans une entité, de plus d'un moyen pour accomplir une fonction requise

[VEI 191-15-01]

NOTE Dans la série IEC 62439, l'existence de plus d'un chemin (consistant en liaisons et commutateurs) entre nœuds d'extrémité.

3.1.43
temps de rétablissement de remise en état
temps pour rétablir la configuration du réseau originale ou précédant la panne y compris les états d'exploitation et de gestion d'origine dans chaque appareil

3.1.44
fiabilité
aptitude d'un élément à remplir une fonction requise dans des conditions déterminées et pendant un intervalle de temps donné

[VEI 191-02-06]

NOTE 1 Il est généralement admis que l'élément soit en état de remplir cette fonction requise au début de l'intervalle de temps.

NOTE 2 Le terme "fiabilité" est aussi employé comme une mesure de la performance de la fiabilité (voir VEI 191-12-01).

3.1.45
réparation
mesure prise pour le rétablissement de la situation spécifiée

3.1.46
temps de reprise de réparation
durée de rétablissement de réparation
retard entre le début de l'action de réparation et l'achèvement de la réparation de l'élément défectueux de telle sorte que le réseau retrouve, et sa fonction de communication requise, et sa capacité requise de résistance aux pannes.

NOTE 1 Ce délai comprend tout temps d'arrêt du réseau provoqué par le processus de réparation, par exemple une panne de réseau pour remplacer un commutateur à plusieurs bons ports et un seul port défectueux.

NOTE 2 Ce délai n'inclut pas le temps de remise en état du réseau de son mode de fonctionnement de secours au mode de fonctionnement d'origine.

3.1.47
liaison d'un anneau
liaison qui connecte deux commutateurs d'un anneau

3.1.48
port d'un anneau
port d'un commutateur auquel une liaison d'anneau est liée

3.1.49
topologie en anneau
topologie où chaque nœud est connecté en série à deux autres nœuds

NOTE 1 Les nœuds sont connectés les uns aux autres sous la forme logique d'un cercle.

NOTE 2 Les trames sont transmises séquentiellement entre des nœuds actifs, chaque nœud étant capable d'examiner ou de modifier la trame avant de la transmettre.

Copyright International Electrotechnical Commission

3.1.50
robustesse
comportement du réseau face aux défaillances

3.1.51
pont racine
commutateur ayant la valeur la plus faible d'un paramètre identificateur de pont RSTP dans le réseau

[IEEE 802.1D]

3.1.52
route
chemin de communication couche 3 entre deux nœuds

3.1.53
critère de défaillance unique
capacité d'un système qui inclut des composants redondants afin de maintenir toute sa fonctionnalité suite à une défaillance d'un de ses composants, avant la maintenance ou le rétablissement automatique

3.1.54
point unique de défaillance
composant dont la défaillance pourrait provoquer une défaillance du système et n'est pas compensée par la redondance ou une autre procédure opérationnelle

NOTE Un point unique de défaillance provoque une défaillance en mode commun. Elle peut être provoquée par une erreur de conception dans les éléments redondants ou par une cause extérieure qui affecte tous les éléments redondants de la même manière, par exemple, température extrême.

3.1.55
nœud à une seule association
nœud qui dispose d'un seul port à un LAN

3.1.56
redondance en attente
redondance telle qu'une partie seulement des moyens d'accomplir une fonction requise est utilisée, le reste n'étant utilisé qu'en cas de besoin

[VEI 191-15-03]

NOTE Elle est également appelée «redondance dynamique».

3.1.57
topologie en étoile
topologie où tous les appareils sont connectés à un nœud central

3.1.58
commutation avec enregistrement et retransmission (store-and-forward)
technologie dans laquelle un nœud de commutation commence à émettre une trame reçue seulement après que cette trame est complètement reçue

3.1.59
commutateur
nœud commutateur
pont MAC tel que défini dans l'IEEE 802.1D

NOTE Le terme “commutateur” est utilisé en tant que synonyme pour le terme “nœud commutateur”.

Copyright International Electrotechnical Commission

3.1.60
nœud d'extrémité de commutation
un nœud d'extrémité et un commutateur combinés dans un seul appareil

3.1.61
défaillance systématique
défaillance liée de façon déterministe à une certaine cause, qui ne peut être éliminée que par une modification de la conception ou du processus de fabrication, par les procédures opérationnelles, par la documentation ou par d'autres facteurs pertinents

NOTE 1 La maintenance corrective sans modification n'éliminera pas en général la cause de la défaillance.

NOTE 2 Une défaillance systématique peut être induite par la simulation de la cause de la défaillance.

[VEI 191-04-19]

3.1.62
topologie
configuration des positions relatives et des interconnexions des nœuds individuels du réseau

[issue de l'IEC 61918, 3.1.67]

NOTE D'autres aspects tels que le délai, l'atténuation et les classes de support physique, relatifs aux chemins qui connectent les nœuds du réseau sont aussi parfois considérés comme des propriétés de la topologie.

3.1.63
topologie en arbre
topologie dans laquelle deux nœuds ont seulement un chemin entre eux et au moins un commutateur est lié à plus de deux mailles inter-étage

3.1.64
partie jonction
partie d'un LAN commuté qui achemine le trafic à plusieurs nœuds d'extrémité

3.1.65
entité de couche supérieure
parties de la pile protocolaire immédiatement au-dessus de la couche traitant la redondance

3.1.66
temps de reprise dans les conditions les plus défavorables
temps de reprise maximal prévu parmi toutes les pannes et pour toutes les configurations autorisées

NOTE Ce retard est important pour un concepteur de réseau pour indiquer quels sont les aspects du réseau qui nécessitent un traitement spécial pour réduire au maximum les interruptions de communication.

3.1.67
pont
dispositif connectant des segments LAN au niveau de la couche 2 conformément à l'IEEE 802.1D

NOTE Les termes "commutateur" et "pont" sont considérés comme synonymes, le terme "pont" est utilisé dans le contexte des normes telles que RSTP (IEEE 802.1D), PTP (IEC 61588) ou IEC 62439-3 (PRP & HSR).

3.1.68
temps de rétablissement du réseau
délai écoulé entre la première défaillance d'un composant ou d'un média au sein du réseau et la fin de la reconfiguration du réseau et à partir duquel tous les dispositifs qui sont encore en mesure de participer à la communication du réseau sont à nouveau capables d'atteindre tous les autres dispositifs dans le réseau

Copyright International Electrotechnical Commission

NOTE Lorsqu'un protocole de contrôle de redondance du réseau (comme RSTP) reconfigure le réseau en raison d'une défaillance, certaines parties du réseau peuvent être toujours disponibles et les ruptures de communication peuvent varier dans le temps et dans l'espace sur l'ensemble du réseau. Dans les calculs, seul le scénario le plus défavorable est pris en compte.

3.2 Abréviations et acronymes

BRP Beacon Redundancy Protocol (Protocole de redondance à balise), IEC 62439-5

BPDU Bridge management Protocol Data Unit (Unité de données de protocole de gestion de pont), conformément à l'IEEE 802.1D

CRP Cross-network Redundancy Protocol (Protocole de redondance inter-réseau), voir IEC 62439-4

DAN Doubly Attached Node (Noeud à double association)

DRP Distributed Redundancy Protocol (Protocole de redondance distribuée), voir IEC 62439-6

DUT Device Under Test (Appareil en essai)

HSR High-availability Seamless Redundancy (Redondance transparente de haute disponibilité), voir IEC 62439-3

IP Internet Protocol, couche 3 de la pile Protocole Internet

IT ou TI Information Technology ou Technologie de l'information

LAN Local Area Network (Réseau local)

LRE Link Redundancy Entity (Entité de redondance de liaison)

MAC Media Access Control (Commande d'accès au support)

MRP Medium Redundancy Protocol (Protocole de redondance du support), voir IEC 62439-2

MTBF Mean Time Between Failure (Temps moyen entre défaillances)

MTTF Mean Time To Failure (Durée moyenne de fonctionnement avant défaillance)

MTTFN Mean Time To Failure of Network (Durée moyenne de fonctionnement avant défaillance du réseau)

MTTFS Mean Time To Failure of System (Durée moyenne de fonctionnement avant défaillance du système)

MTTR Mean Time To Repair (Durée moyenne de panne)

MTTRP Mean Time To Repair Plant (Durée moyenne de panne installation)

OUI Organizational Unique Identifier (Identificateur propre à une organisation)

PDU Protocol Data Unit (Unité de données de protocole)

PICS Protocol Implementation Conformance Statement (Déclaration de conformité de mise en œuvre de protocole)

PRP Parallel Redundancy Protocol (Protocole de redondance parallèle), voir IEC 62439-3

QAN Quadruply Attached Node (Nœud à quadruple association)

RFC Request For Comments de l'Internet Society (Demande de commentaires de l'Internet Society)

Copyright International Electrotechnical Commission

RRP Ring-based Redundancy Protocol (Protocole de redondance pour réseau en anneau), voir IEC 62439-7

RSTP Rapid Spanning Tree Protocol (Protocole arborescence rapide), voir IEEE 802.1D

SAN Singly Attached Node (Nœud à une seule association)

SRP Serial Redundancy Protocol (Protocole de redondance série), voir IEC 62439-3

STP Spanning Tree Protocol (Protocole d'arborescence, Protocole spanning tree)

TCP Transmission Control Protocol (Protocole de commande de transport), couche 4 de la pile Protocole Internet

UDP User Datagram Protocol (Protocole de datagramme utilisateur), couche 4 de la pile Protocole Internet

3.3 Conventions

3.3.1 Conventions générales

Les protocoles spécifiés dans la série IEC 62439 suivent la structure définie dans l'IEC/TR 61158-1.

Les directives générales sont spécifiées dans l'IEC 61158-6-10, 3.7.

3.3.2 Conventions pour les définitions des diagrammes d'états

La série IEC 62439 suit les conventions utilisées dans l'IEC 61158-6-10, 3.8. Ce qui suit est un résumé.

- Chaque état est décrit par une table, avec une rangée séparée pour chaque transition qui peut provoquer un changement d'état.
- Les transitions sont définies comme des événements qui peuvent transporter des arguments et être assujettis à des conditions.
- Le champ d'action exprime l'action qui se déroule dans le cas où l'événement est déclenché.
- Pour des raisons d'espace, l'événement et les actions sont placés dans la même cellule.
- La colonne de droite indique le prochain état dans lequel on pénètre après la fin de l'action.

3.3.3 Conventions pour la spécification de PDU

Les PDU sont décrites conformément à la spécification RFC 791, Annexe B.

En particulier:

- les bits, les octets et les matrices sont numérotés à partir de 0;
- La convention "Ordre des Octets du Réseau" (big-endian (gros boutiste), octet de poids fort en premier) est observée.

L'IEC 61158-6-10 distingue le bit "identification" du bit "offset".

EXEMPLE Dans une chaîne binaire de 8 bits, le bit le plus à droite (Bit de poids faible) est étiqueté bit 0, mais son bit "offset" est mis à 7 dans l'octet de chaîne de bits.

Lors de la spécification d'objets de données plutôt que de PDU, le bit "identification" selon la série IEC 61158-6 est utilisé. Par conséquent, les bits d'une chaîne binaire sont spécifiés dans l'ordre croissant du bit "identification", bien qu'ils soient émis dans l'ordre inverse.

Copyright International Electrotechnical Commission

3.4 Adresses réseau réservées

Ce qui suit est un récapitulatif des adresses réseau réservées pour les besoins de la série IEC 62439, tandis que les valeurs requises sont spécifiées dans les parties respectives de la série IEC 62439.

Pour les besoins de la série IEC 62439, l'identificateur OUI 00-15-4E a été réservé par l'IEEE. Toutes les bandes ayant cet identificateur OUI sont réservées pour la série IEC 62439. Les bandes suivantes sont affectées:

- MRP (voir IEC 62439-2) utilise 00-15-4E, bande 00-00-xx.
- PRP (voir IEC 62439-3) utilise 00-15-4E, bande 00-01-xx.
- HSR (voir IEC 62439-3) utilise 0x892F.
- CRP (voir IEC 62439-4) utilise une adresse MAC multidiffusion IP.
- BRP (voir IEC 62439-5) utilise 00-15-4E, bande 00-02-xx.
- DRP (voir IEC 62439-6) utilise 00-15-4E, bande 00-03-xx.
- RRP (voir IEC 62439-7) utilise 00 E0 91 02 05 99.

Pour les besoins de la série IEC 62439, les Ethertypes suivants (voir IEEE 802a) ont été réservés par l'IEEE:

- MRP (voir IEC 62439-2) utilise 0x88E3.
- PRP (voir IEC 62439-3) utilise 0x88FB.
- CRP (voir IEC 62439-4) utilise 0x0800 (IP) avec un port UDP 3622.
- BRP (voir IEC 62439-5) utilise 0x80E1.
- DRP (voir IEC 62439-6) utilise 0x8907.
- RRP (voir IEC 62439-7) utilise 0x88FE.

4 Exigences de conformité (normative)

4.1 Conformité aux protocoles de redondance

Une déclaration de conformité avec une partie de la série IEC 62439 doit être énoncée comme:

- une conformité à l'IEC 62439-2 (MRP), ou
- une conformité à l'IEC 62439-3 (PRP), ou
- une conformité à l'IEC 62439-4 (CRP), ou
- une conformité à l'IEC 62439-5 (BRP),
- une conformité à l'IEC 62439-6 (DRP),
- une conformité à l'IEC 62439-7 (RRP).

Une déclaration de conformité doit être accompagnée d'une documentation justificative appropriée telle que définie en 4.2. Les protocoles et options pris en charge doivent être spécifiés comme PICS, au format:

Options PICS_62439-X_supported.

EXEMPLE PICS_62439-5_BlockingSupported.

Copyright International Electrotechnical Commission

4.2 Essais de conformité

4.2.1 Concept

Le concept de cet essai de conformité est de vérifier les fonctions d'un appareil en essai (DUT) par rapport à un ensemble cohérent d'indicateurs dans les conditions simulées les plus défavorables. L'essai de conformité doit assurer l'interopérabilité des appareils qui revendiquent la conformité avec le même protocole.

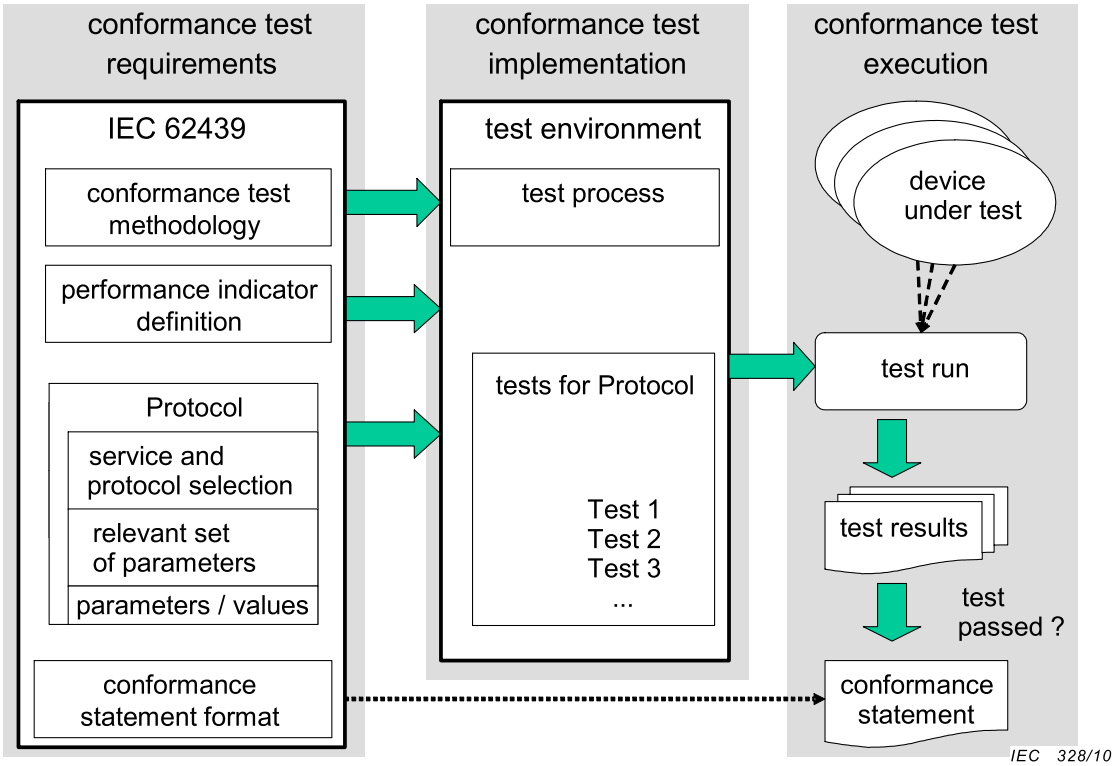
La série IEC 62439 contient des spécifications qui doivent être observées par différents acteurs:

- le constructeur d'appareils qui conçoit et met en essai une interface compatible;
- le gestionnaire de réseau qui définit la topologie;
- l'utilisateur du réseau qui respecte les limites d'utilisation.

Un appareil vendu comme étant entièrement conforme à un protocole de la série IEC 62439 peut avoir une performance inférieure si les règles de configuration de réseau ne sont pas respectées quand il est utilisé.

La Figure 1 donne une vue d'ensemble de l'essai de conformité lié aux protocoles de la série IEC 62439.

NOTE La mise en œuvre et l'exécution de l'essai de conformité ne sont pas définies dans la série IEC 62439.



Légende

Anglais	Français
Conformance test requirements	Exigences d'essai de conformité
Conformance test implementation	Mise en œuvre d'essai de conformité
Conformance test execution	Exécution d'essai de conformité
Conformance test methodology	Méthodologie d'essai de conformité
Performance indicator definition	Définition d'indicateur de performance
Protocol	Protocole

Copyright International Electrotechnical Commission

Anglais	Français
Service and protocol selection	Sélection de service et protocole
Relevant set of parameters	Ensemble pertinent de paramètres
Parameters / values	Paramètres / valeurs
Conformance statement format	Format de déclaration de conformité
Test environment	Environnement d'essai
Test process	Processus d'essai
Tests for Protocol	Essais pour protocole
Test 1	Essai 1
Test 2	Essai 2
Test 3	Essai 3
Device under test	Appareil en essai
Test run	Déroulement d'essai
Test results	Résultats d'essai
Test passed?	Essai réussi?
Conformance statement	Déclaration de conformité

Figure 1 – Vue d'ensemble de l'essai de conformité

4.2.2 Méthodologie

Les scénarios d'essai doivent être développés de manière que les essais puissent être répétés. Les résultats des essais doivent être documentés et doivent être utilisés comme la base pour la déclaration de conformité.

Les essais de conformité d'un appareil doivent inclure, le cas échéant, la vérification

- de l'exactitude de la fonctionnalité spécifiée,
- des valeurs des indicateurs liés au réseau,
- des valeurs des indicateurs liés à l'appareil.

Les valeurs des indicateurs de performance du protocole et de l'appareil en essai doivent être utilisées.

NOTE 1 Une description d'un processus d'essai de conformité est donnée dans la série ISO/IEC 9646.

NOTE 2 Il est supposé que la qualité des scénarios d'essai garantisse l'interopérabilité d'un appareil soumis à l'essai. Si des irrégularités sont signalées, les scénarios d'essai seront adaptés en conséquence.

4.2.3 Conditions et scénarios d'essai

Les conditions et les scénarios d'essai doivent être définis et documentés sur la base d'un protocole de redondance spécifique. Cela doit inclure les indicateurs suivants, le cas échéant:

- nombre de nœuds;
- topologie de réseau;
- le nombre de commutateurs entre les nœuds;
- le type de trafic.

Pour chaque indicateur mesuré, les documents relatifs aux conditions et aux scénarios d'essai doivent être établis et doivent décrire:

- le but d'essai;
- le montage d'essai;

Copyright International Electrotechnical Commission

- la procédure d'essai;
- les critères de conformité.

Le montage d'essai décrit le réglage de l'équipement nécessaire pour effectuer l'essai, y compris les équipements de mesure, l'appareil en essai, les équipements auxiliaires, le schéma d'interconnexion et les conditions environnementales d'essai.

Des parties de l'environnement d'essai peuvent être émulées ou simulées. Les effets de l'émulation ou de la simulation doivent être documentés.

La procédure d'essai décrit comment il convient d'effectuer l'essai, ce qui inclut également une description d'un ensemble spécifique d'indicateurs nécessaires pour effectuer cet essai. Les critères de conformité définissent les résultats des essais acceptés en tant que conformité avec cet essai.

4.2.4 Procédure d'essai et mesures

Les indicateurs mesurés doivent inclure, le cas échéant:

- le temps de reprise de la redondance,
- l'impact d'une surcharge de redondance en fonctionnement normal.

La procédure d'essai doit être basée sur les principes de 4.2.3.

La séquence de mesure des actions pour effectuer un essai doit être fournie.

Le nombre d'essais indépendants doit être fourni.

La méthode utilisée pour calculer le résultat de l'essai à partir des essais indépendants doit être fournie, le cas échéant.

4.2.5 Rapport d'essai

Le rapport d'essai doit contenir suffisamment d'informations permettant de répéter l'essai.

Le rapport d'essai doit contenir au moins

a) la référence à la méthodologie d'essai de conformité selon 4.2.2,
b) la référence aux définitions des indicateurs de performance,
c) la référence au protocole de redondance de la série IEC 62439,
d) une description de l'environnement de l'essai de conformité, y compris les émulateurs de réseau, les équipements de mesure et la personne ou l'organisation responsable de l'exécution de l'essai, ainsi que la date de l'essai,
e) une description de l'appareil en essai, son fabricant et la version matérielle et logicielle,
f) le nombre et le type d'appareils connectés au réseau ainsi que la topologie,
g) une référence aux spécifications des scénarios d'essai,
h) les valeurs mesurées,
i) un énoncé relatif à la conformité au protocole de redondance.

Copyright International Electrotechnical Commission

5 Concepts pour des réseaux d'automatisme à haute disponibilité (informative)

5.1 Caractéristiques d'application des réseaux d'automatisation

5.1.1 Résilience en cas de défaillance

Les installations comptent sur le bon fonctionnement du système d'automatisation. Les installations tolèrent une dégradation du système d'automatisation pendant un court laps de temps seulement, appelé temps de grâce. Il convient que le temps de reprise du réseau soit plus court que le temps de grâce du moment où l'application nécessite généralement d'effectuer des tâches supplémentaires (liées au protocole et au traitement de données, en attendant le prochain cycle de communication programmée, etc.) avant que l'installation revienne à l'état totalement opérationnel. Les applications peuvent être distinguées par leur temps de grâce, comme le montre le Tableau 1.

Tableau 1 – Exemples de temps de grâce d'applications

Applications	Temps de grâce type s
Automatisation non critique, par exemple systèmes d'entreprises	20
Gestion d'automatisation, par exemple fabrication, automatisation discrète	2
Automatisation générale, par exemple automatisation de processus, centrales électriques	0,2
Automatisation à temps critique, par exemple transmissions synchronisées	0,020

Certaines installations ont des exigences plus strictes quand elles doivent fonctionner en continu, n'ayant pas de période de repos pendant laquelle l'installation peut être maintenue ou reconfigurée. Dans ce cas, le temps de grâce est valable pour l'exigence la plus stricte, par exemple dictée par le remplacement à chaud de parties de l'équipement.

Les systèmes d'automatisation peuvent contenir de la redondance pour faire face aux défaillances. Les méthodes diffèrent sur la façon de gérer la redondance, mais leur facteur de performance clé est le temps de reprise, c'est-à-dire le temps nécessaire pour rétablir le fonctionnement après l'apparition d'une interruption. Si le temps de reprise dépasse le temps de grâce de l'installation, les mécanismes de protection lancent un arrêt (en mode sûr), ce qui peut entraîner une perte importante de la production et de la disponibilité opérationnelle des installations.

Une caractéristique clé du rétablissement est son déterminisme, c'est-à-dire la garantie que le temps de reprise reste en dessous d'une certaine valeur, tant que les hypothèses de base (défaillance unique à la fois, pas de mode commun de défaillance, moins d'une extension maximale du système) sont satisfaites. Un réseau offre un rétablissement déterministe s'il est possible de calculer un temps de rétablissement maximum fini d'une topologie donnée, en cas de défaillance simple.

Chaque fois que l'exploitation dépend de la fonction correcte du réseau d'automatisation, il peut être nécessaire d'augmenter la disponibilité du réseau.

L'augmentation de la disponibilité en augmentant la fiabilité des éléments ou en améliorant la maintenance est en dehors du domaine d'application de la série IEC 62439. La série IEC 62439 considère uniquement les protocoles qui introduisent de la redondance et reconfigurent automatiquement les éléments redondants du réseau en cas de défaillance.

Copyright International Electrotechnical Commission

5.1.2 Classes de redondance de réseau

5.1.2.1 Généralités

La série IEC 62439 considère deux classes de redondance de réseau:

a) redondance gérée au sein du réseau;

b) redondance gérée dans les nœuds d'extrémité.

NOTE La série IEC 62439 ne considère pas la redondance des nœuds d'extrémité eux-mêmes, c'est-à-dire l'utilisation de nœuds d'extrémité redondants, puisque cela est hautement spécifique à une application.

5.1.2.2 Redondance gérée au sein du réseau

La redondance au sein d'un réseau a été appliquée aux réseaux étendus et aux bus de terrain traditionnels.

Les routeurs de couche 3 (non pris en compte dans la série IEC 62439) calculent les routes alternatives à la suite de défaillances de liaison. Les protocoles correspondants ont bien fait leurs preuves comme partie intégrante de la pile IP, mais le temps de reprise est de l'ordre de dizaines de secondes, voire de l'ordre de minutes, en fonction de la topologie. Ces temps de reprise sont tolérés uniquement par les applications les plus bénignes.

Les réseaux d'automatisation fonctionnent généralement dans un seul réseau local (LAN), c'est-à-dire les messages opérationnels sont acheminés à travers les répéteurs de la couche 1 ou les commutateurs de la couche 2, mais ne traversent pas les routeurs. Les messages partagés avec le monde extérieur via les routeurs ou les pare-feux existent bien, mais ils sont considérés comme non critiques.

Classiquement, la redondance au sein d'un réseau LAN est assurée par les protocoles qui réagissent à la perte de liaisons et de commutateurs par la reconfiguration du LAN, en utilisant des liaisons et des commutateurs redondants, tels que le protocole RSTP (Rapid Spanning Tree Protocol) conformément à l'IEEE 802.1D.

Les protocoles de redondance améliorés de couche 2 se basent sur les mêmes principes que RSTP, mais fournissent une reprise plus rapide en exploitant l'hypothèse que le réseau d'automatisation ait une topologie en anneau. Les nœuds d'extrémité sont des nœuds d'automatisation non modifiés.

5.1.2.3 Redondance gérée dans les nœuds d'extrémité

D'autres améliorations des temps de reprise nécessitent la gestion de la redondance dans les nœuds d'extrémité, en équipant les nœuds d'extrémité par plusieurs liaisons de communication redondantes. En général, les nœuds d'extrémité à double association fournissent une redondance suffisante. Dans ce type de redondance, aucune hypothèse n'est faite concernant les commutateurs dans le LAN.

Pour les applications à temps critique telles que les transmissions synchronisées, l'exploitation parallèle des réseaux disjoints fournit un rétablissement sans raccord, mais nécessite une duplication complète du réseau. Certaines installations critiques nécessitent également des nœuds à double association, afin de faire face à une défaillance d'une liaison en feuille, même si elles ne nécessitent pas de temps de reprise très court.

5.1.3 Maintenance de la redondance

La redondance peut être affectée par des pannes latentes, ce qui peut être détecté par les essais. L'intervalle d'essai permet d'estimer la disponibilité. Tous les protocoles fournissent les moyens pour mettre en essai les composants redondants ou de rechange et signaler les défaillances détectées à la gestion du réseau.

Copyright International Electrotechnical Commission

5.1.4 Comparaison et indicateurs

Les protocoles spécifiés dans la série IEC 62439 offrent:

- un temps de reprise maximal, déterministe et garanti (qui peut dépendre de la topologie),
- la transparence de la communication réelle vers l'application en toutes circonstances, et
- pour les nœuds à double association, l'interopérabilité avec les appareils à une seule association (matériel TI courant disponible dans le commerce).

Le Tableau 2 compare certaines caractéristiques de quelques protocoles de redondance, commandés par le temps de reprise.

Tableau 2 – Exemples de protocoles de redondance

Protocole	Solution	Perte de trame	Protocole de redondance	Association de nœuds d'extrémité	Topologie de réseau	Temps de reprise pour les défaillances considérées
IP	Routage IP	Oui	Dans le réseau	Simple	Simple maillée	> 30 s typique non déterministe
STP	IEEE 802.1D	Oui	Dans le réseau	Simple	Simple maillée	> 20 s typique non déterministe
RSTP	IEEE 802.1D	Oui	Dans le réseau	Simple	Simple maillée, anneau	Peut être déterministe conformément aux règles de l'Article 8
CRP	IEC 62439-4	Oui	Dans les nœuds d'extrémité	Simple et double	Doublement maillée, à connexion croisée	1 s au pire des cas pour 512 nœuds d'extrémité
DRP	IEC 62439-6	Oui	Dans le réseau	Simple et double	Anneau, double anneau	100 ms au pire des cas pour 50 commutateurs
MRP	IEC 62439-2	Oui	Dans le réseau	Simple	Anneau, maillé	500 ms, 200 ms, 30 ms ou 10 ms le cas le plus défavorable pour 50 commutateurs en fonction de l'ensemble des paramètres et de la typologie du réseau
BRP	IEC 62439-5	Oui	Dans les nœuds ~~d'extrémité~~ terminaux	Double	Doublement maillée, connectée	~~4,8~~ 8,88 ms le cas le plus défavorable pour ~~500~~ 100 nœuds ~~d'extrémité~~ terminaux
RRP	IEC 62439-7	Oui	Dans les nœuds terminaux	Double (nœuds terminaux de commutation)	En anneau simple	8 ms dans 100BASEX, 4 ms dans 1000BASEX
PRP	IEC 62439-3	Non	Dans les nœuds d'extrémité	Double	Doublement maillée, indépendante	0 s
HSR	IEC 62439-3	Non	Dans les nœuds d'extrémité	Double	Anneau, maillée	0 s

NOTE Pour les protocoles de redondance spécifiés dans la série IEC 62439, les temps de reprise dans le Tableau 2 sont garantis si l'on utilise les configurations et les paramètres spécifiés dans la partie associée de la série IEC 62439. Des temps de reprise plus rapides peuvent être réalisés en utilisant des réglages et des paramètres différents, et ce, sous la responsabilité de l'utilisateur.

Copyright International Electrotechnical Commission

Les indicateurs pour les différentes solutions incluent, le cas échéant:

- le temps de reprise de panne,
- le temps de reprise de réparation,
- la durée de rétablissement de remise en état,
- temps de reprise dans les conditions les plus défavorables,
- l'impact sur le fonctionnement normal.

Les cas de panne comportent:

- défaillance du gestionnaire de réseau actif courant (s'il existe) suivie par une réparation et un rétablissement;
- défaillance de la source courante du temps de réseau (si elle existe) suivie par une réparation et un rétablissement.

Le paragraphe 5.2 généralise les considérations ci-dessus et introduit un schéma de classification.

5.2 Système du réseau générique

5.2.1 Éléments du réseau

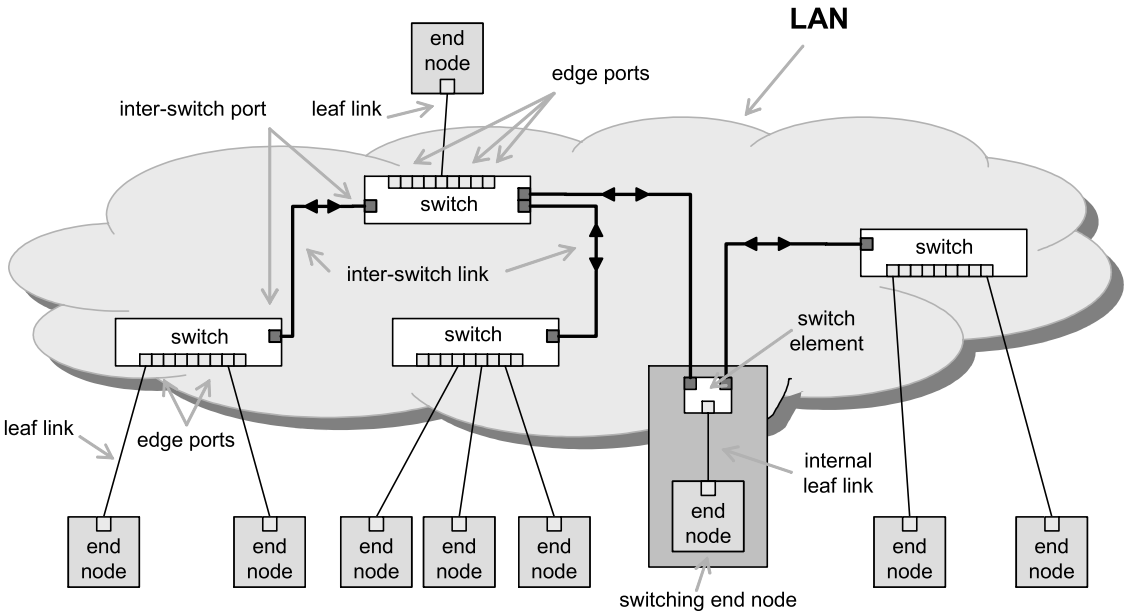
5.2.1.1 Généralités

Le réseau générique est modélisé avec les éléments fonctionnels énumérés ci-dessous et représentés dans la Figure 2.

- Nœuds d'extrémité
- Liaisons en feuille
- Commutateurs (avec ports d'extrémité et ports inter-étage)
- Mailles inter-étage
- Nœuds d'extrémité de commutation

Le LAN se constitue de tous les composants du réseau, excepté les nœuds d'extrémité et les liaisons en feuille.

Copyright International Electrotechnical Commission



NOTE Les ports d'extrémité sont ombrés en gris clair, les ports inter-étage sont ombrés en gris foncé, les mailles inter-étage sont dessinées avec un trait épais, les liaisons en feuille sont dessinées avec un trait fin.

Légende

Anglais	Français
Inter switch port	Port inter-étage
Leaf link	Liaison en feuille
Edge ports	Ports d'extrémité
Switch	Commutateur
Inter switch link	Maille inter-étage
Switch element	Élément de commutateur
Internal leaf link	Liaison en feuille interne
End node	Nœud d'extrémité
Switching end node	Nœud d'extrémité de commutation

Figure 2 – Éléments du réseau général (topologie en arbre)

5.2.1.2 Nœud d'extrémité

Un nœud d'extrémité nécessite un port de connexion au LAN pour son fonctionnement normal.

Le port de connexion d'un nœud d'extrémité est connecté à un port d'extrémité d'un commutateur dans un LAN par une liaison en feuille.

5.2.1.3 Liaison en feuille

Une liaison en feuille connecte un nœud d'extrémité au LAN.

Cette connexion peut être interne à un appareil, dans le cas où l'appareil combine le nœud d'extrémité et le commutateur ou la fonctionnalité LRE (nœud d'extrémité de commutation dans la Figure 2).

5.2.1.4 Maille inter-étage

Une maille inter-étage connecte les commutateurs dans un LAN.

Copyright International Electrotechnical Commission

Différentes mailles inter-étage peuvent exister entre deux commutateurs en vue d'augmenter la disponibilité.

5.2.1.5 Commutateurs

Les commutateurs sont des éléments de connexion de couche 2 tels que définis dans l'IEEE 802.1D.

NOTE Les ponts conformément à l'IEEE 802.1D sont nommés commutateurs dans la série IEC 62439.

Les commutateurs sont connectés les uns aux autres par des mailles inter-étage.

Un commutateur est connecté à une liaison en feuille par le biais d'un port d'extrémité.

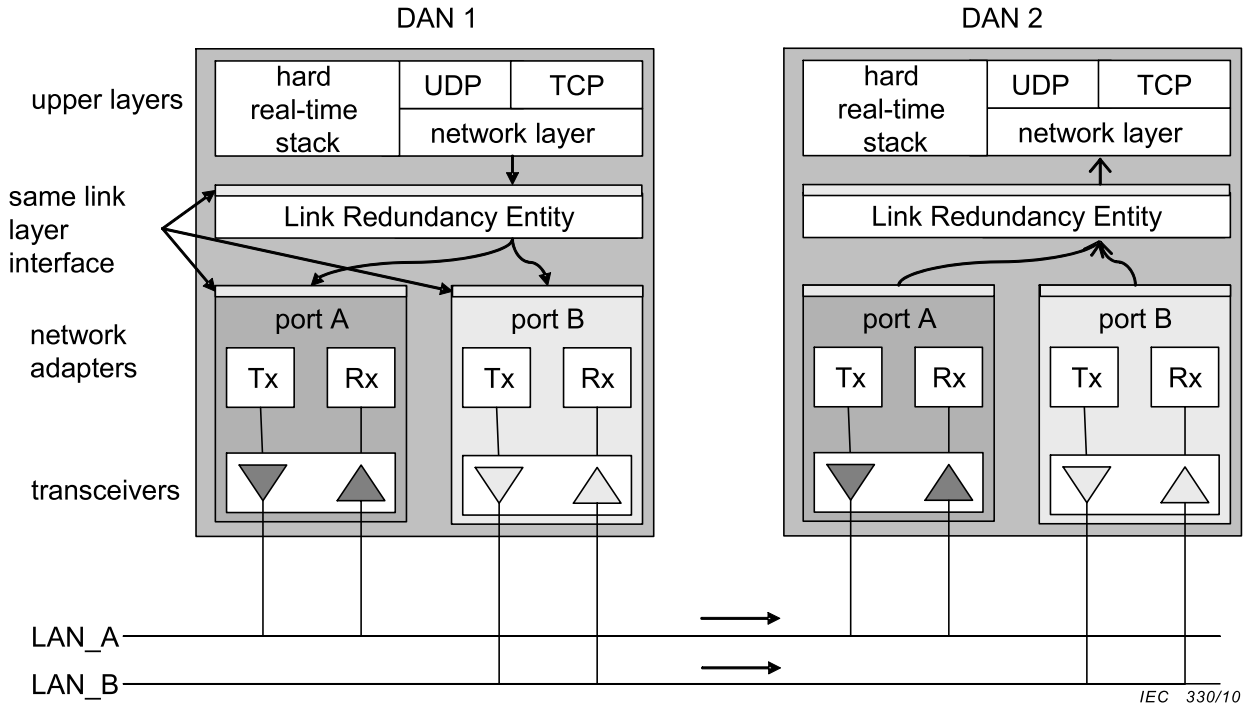
5.2.1.6 Nœud d'extrémité de commutation

Un élément du commutateur peut être mis en œuvre dans la même partie de l'équipement physique comme étant le nœud d'extrémité. Bien que cela fasse apparaitre le nœud d'extrémité comme un nœud à double association, en interne le principe de fonctionnement est différent, car il n'y a pas besoin d'une entité de redondance de liaison parce que l'élément du commutateur joue ce rôle.

5.2.1.7 Nœuds d'extrémité à associations multiples

Les nœuds d'extrémité peuvent avoir plusieurs ports de connexion pour la redondance. Les ports de connexion d'un nœud d'extrémité peuvent être connectés au même réseau LAN ou à différents réseaux LAN.

Les nœuds d'extrémité à plusieurs associations nécessitent une entité de redondance de liaison (LRE, Link Redundancy Entity) dans leur pile de communication afin de masquer la redondance de l'application, comme le montre la Figure 3.



Légende

Anglais	Français
Upper layers	Couches supérieures

Copyright International Electrotechnical Commission

Anglais	Français
Hard real-time stack	Pile temps réel matérielle
Network layer	Couche réseau
Same link layer interface	Même interface liaison de données
Link redundancy entity	Entité de redondance de liaison
Network adapters	Adaptateurs réseau
Port A	Port A
Port B	Port B
Transceivers	Émetteurs-récepteurs

Figure 3 – Entité de redondance de liaison dans un nœud à double association (DAN)

Un nœud d'extrémité connecté à un ou deux LAN du même réseau par le biais de deux liaisons en feuille est un nœud à double association (DAN, Doubly Attached Node).

Un nœud d'extrémité connecté à un ou plusieurs LAN du même réseau par le biais de quatre liaisons en feuille est un nœud à quadruple association (QAN, Quadruply Attached Node).

NOTE Les nœuds d'extrémité utilisant différents ports de communication pour les réseaux indépendants ne sont pas considérés ici, les considérations s'appliquent à chaque réseau séparément.

5.2.2 Topologies

5.2.2.1 Généralités

La redondance dans le réseau considère la présence de plus d'éléments de réseau que nécessaire (commutateurs, liaisons) pour le fonctionnement, afin d'empêcher la perte de la communication provoquée par une défaillance. À cet effet, il y a plus d'un chemin physique entre deux nœuds d'extrémité.

L'IEC 61918 spécifie différentes sortes de topologies physiques de base, certaines de celles-ci étant utilisées par la série IEC 62439 pour définir différentes topologies.

a) Topologies sans redondance
   - Topologie en arbre (Figure 4);
   - Topologie linéaire (Figure 5).

b) Topologies avec des liaisons redondantes
   - Topologie en anneau (Figure 6);
   - Topologie partiellement maillée (Figure 7);
   - Topologie entièrement maillée (Figure 8).

Il existe quatre structures de haut niveau:

- LAN simple sans liaisons en feuille redondantes (voir 5.2.2.4.1);
- LAN simple avec liaisons en feuille redondantes (voir 5.2.2.4.2);
- LAN redondants sans liaisons en feuille redondantes (voir 5.2.2.4.3);
- LAN redondants avec liaisons en feuille redondantes (voir 5.2.2.4.4).

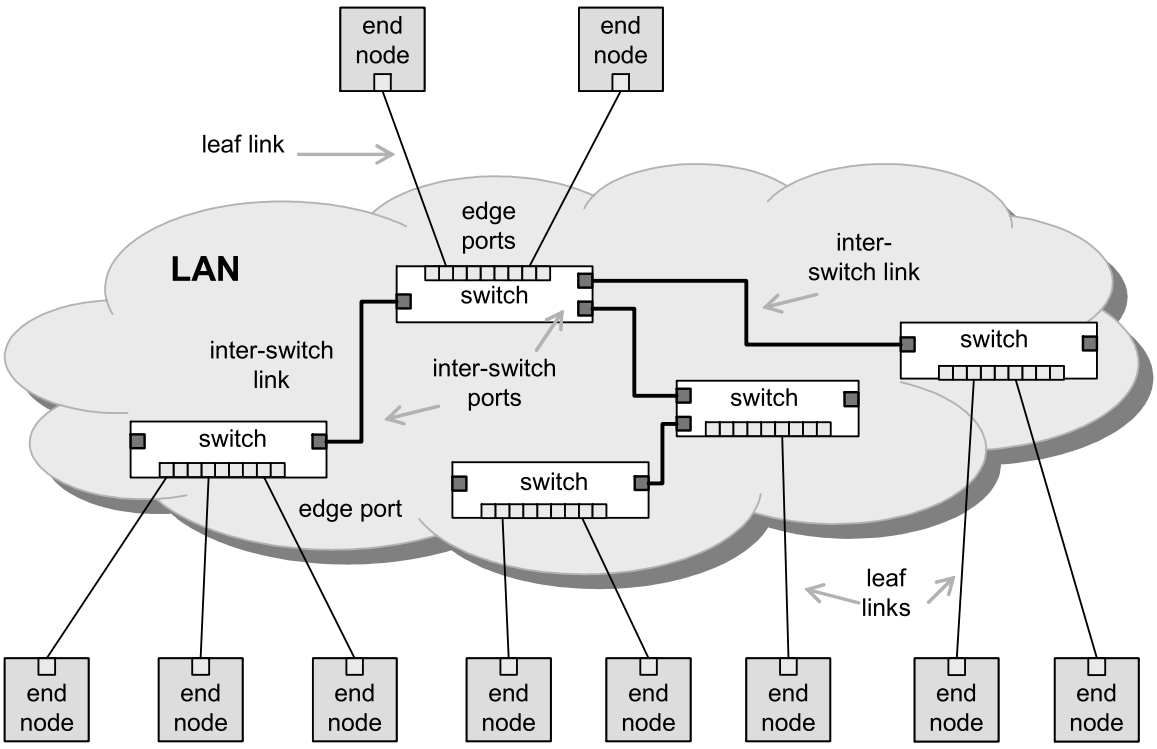
Lorsque la redondance est gérée dans le LAN, les nœuds d'extrémité peuvent être connectés par une simple association. Dans le cas d'une défaillance de commutateur ou de la liaison en feuille, ces nœuds d'extrémité peuvent perdre la communication.

Copyright International Electrotechnical Commission

5.2.2.2 Topologies sans redondance

5.2.2.2.1 Topologie en arbre

Dans une topologie en arbre, au moins un commutateur dispose de plus de deux mailles inter-étage et il n'y a qu'un seul chemin entre deux appareils quelconques. La Figure 4 montre un exemple d'une topologie en arbre.



IEC 331/10

Légende

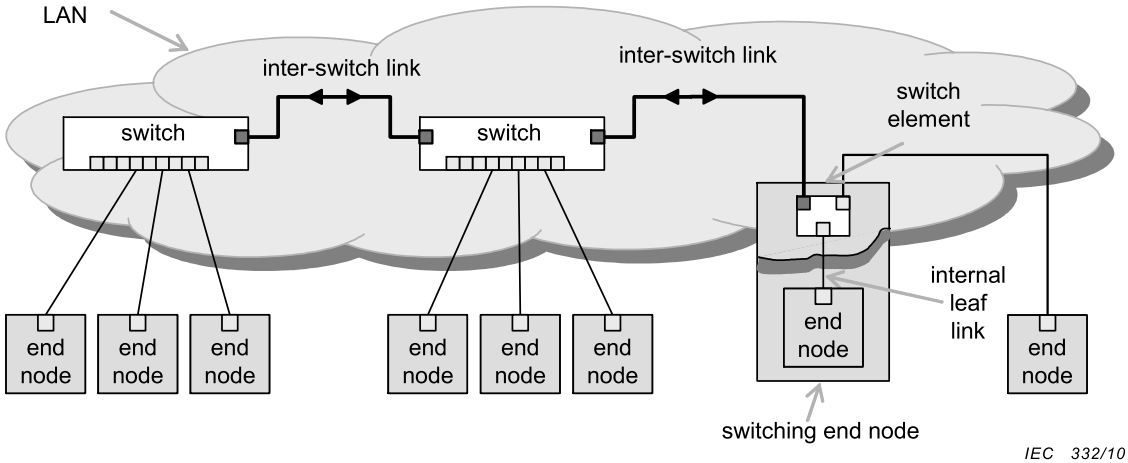
Anglais	Français
End node	Nœud d'extrémité
Leaf link	Liaison en feuille
Edge ports	Ports d'extrémité
Inter switch port	Port inter-étage
Inter switch link	Maille inter-étage
Switch	Commutateur

Figure 4 – Exemple d'une topologie en arbre

5.2.2.2.2 Topologie linéaire

Dans une topologie linéaire, tous les commutateurs sont connectés les uns aux autres en ligne et aucun nœud ne dispose de plus de deux mailles inter-étage, mais les deux nœuds situés à l'extrémité de la ligne n'ont qu'une seule maille inter-étage. La Figure 5 montre un exemple d'une topologie linéaire.

Copyright International Electrotechnical Commission



Légende

Anglais	Français
Inter switch link	Maille inter-étage
Switch	Commutateur
Switch element	Élément de commutateur
Internal leaf link	Liaison en feuille interne
End node	Nœud d'extrémité
Switching end node	Nœud d'extrémité de commutation

Figure 5 – Exemple d'une topologie linéaire

NOTE Un nœud peut être un nœud d'extrémité de commutation, comme montré dans le deuxième nœud d'extrémité à partir de la droite de la Figure 5.

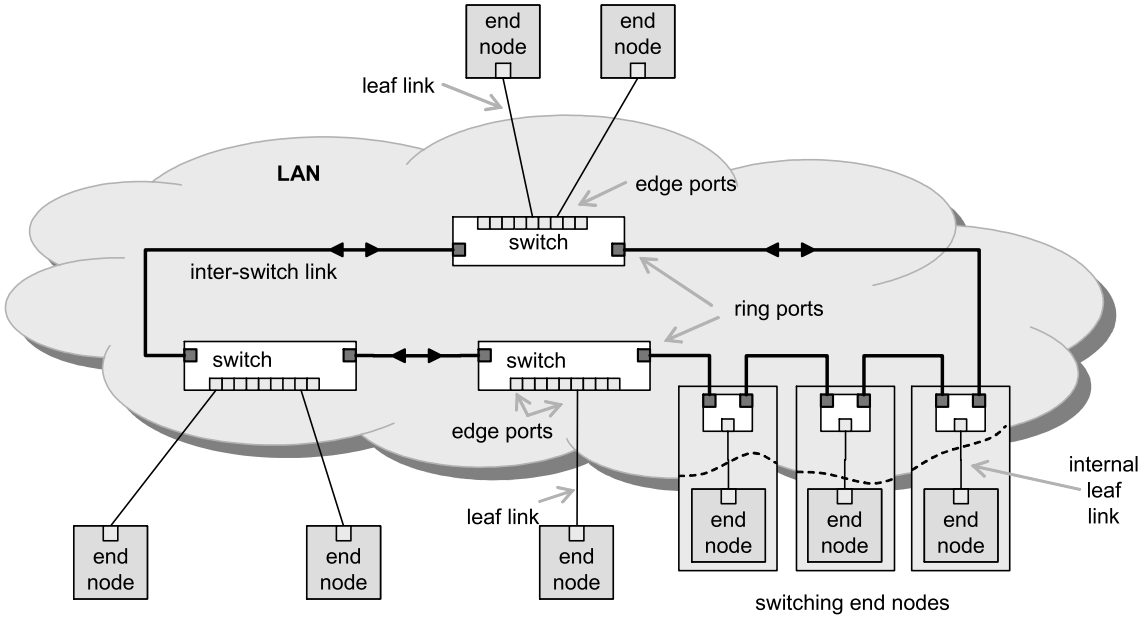
5.2.2.3 Topologies avec des liaisons redondantes

5.2.2.3.1 Topologie en anneau

NOTE Cette topologie s'applique à la redondance du RSTP (voir Article 7), du MRP (IEC 62439-2) et du DRP (IEC 62439-6).

Dans une topologie en anneau, chaque commutateur possède deux mailles inter-étage et deux nœuds d'extrémité quelconques ont deux chemins entre eux lorsque tous les composants sont opérationnels. La Figure 6 montre un exemple d'une topologie en anneau.

Copyright International Electrotechnical Commission



Légende

Anglais	Français
End node	Nœud d'extrémité
Leaf link	Liaison en feuille
Edge ports	Ports d'extrémité
Switch	Commutateur
Inter switch link	Maille inter-étage
Ring ports	Ports d'anneau
Internal leaf link	Liaison en feuille interne
Switching end node	Nœud d'extrémité de commutation

Figure 6 – Exemple d'une topologie en anneau

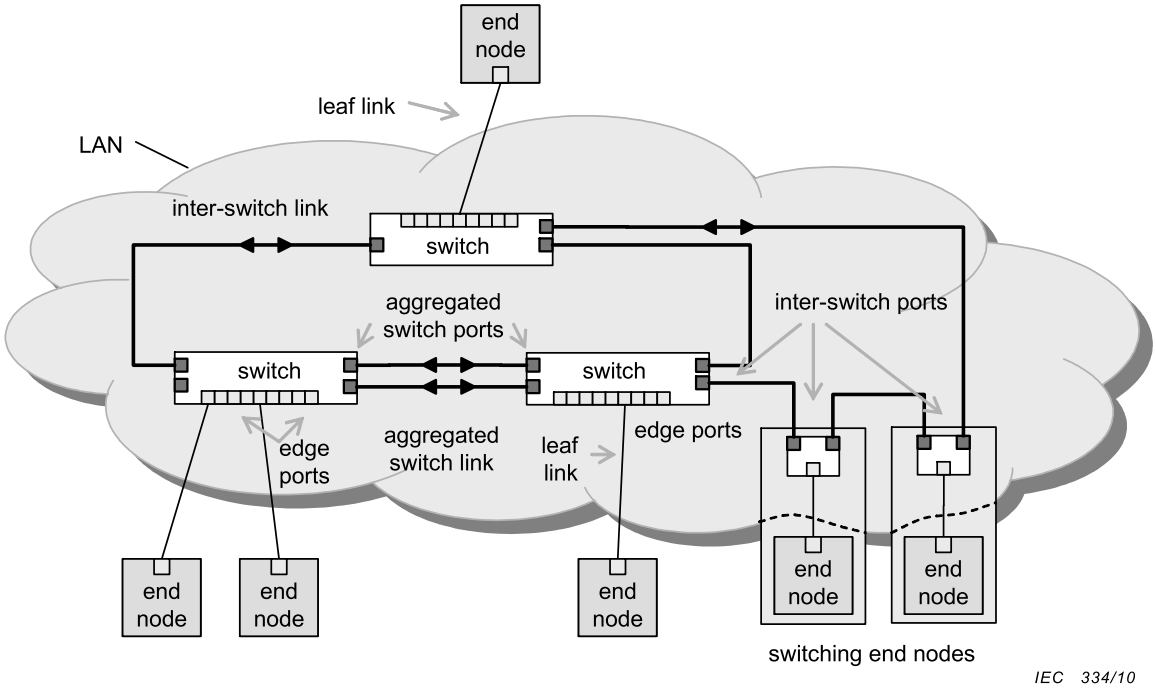
Une topologie en anneau présente une boucle dans le LAN qui pourrait conduire à des inondations causées par des trames en circulation permanente. Les protocoles tels que le protocole RSTP (Rapid Spanning Tree) et le protocole MRP (Media Redundancy Protocol) assurent que les commutateurs maintiennent une topologie linéaire logique lors de l'initialisation, l'exploitation et la reconfiguration.

Si un commutateur ou une maille inter-étage tombe en panne, le commutateur est exclu de l'anneau, et une nouvelle topologie linéaire logique est établie. Cependant, les nœuds d'extrémité connectés à un commutateur en panne perdent la connectivité.

5.2.2.3.2 Topologie partiellement maillée

Dans une topologie partiellement maillée, au moins un commutateur possède plus de deux mailles inter-étage et il existe plus d'un chemin entre quelques appareils. La Figure 7 montre un exemple d'une topologie partiellement maillée.

Copyright International Electrotechnical Commission



Légende

Anglais	Français
End node	Nœud d'extrémité
Leaf link	Liaison en feuille
Inter switch link	Maille inter-étage
Switch	Commutateur
Aggregated switch ports	Ports de commutateur d'agrégation
Inter-switch ports	Ports inter-étage
Edge ports	Ports d'extrémité
Aggregated switch link	Liaison de commutateur d'agrégation
Switching end nodes	Nœuds d'extrémité de commutation

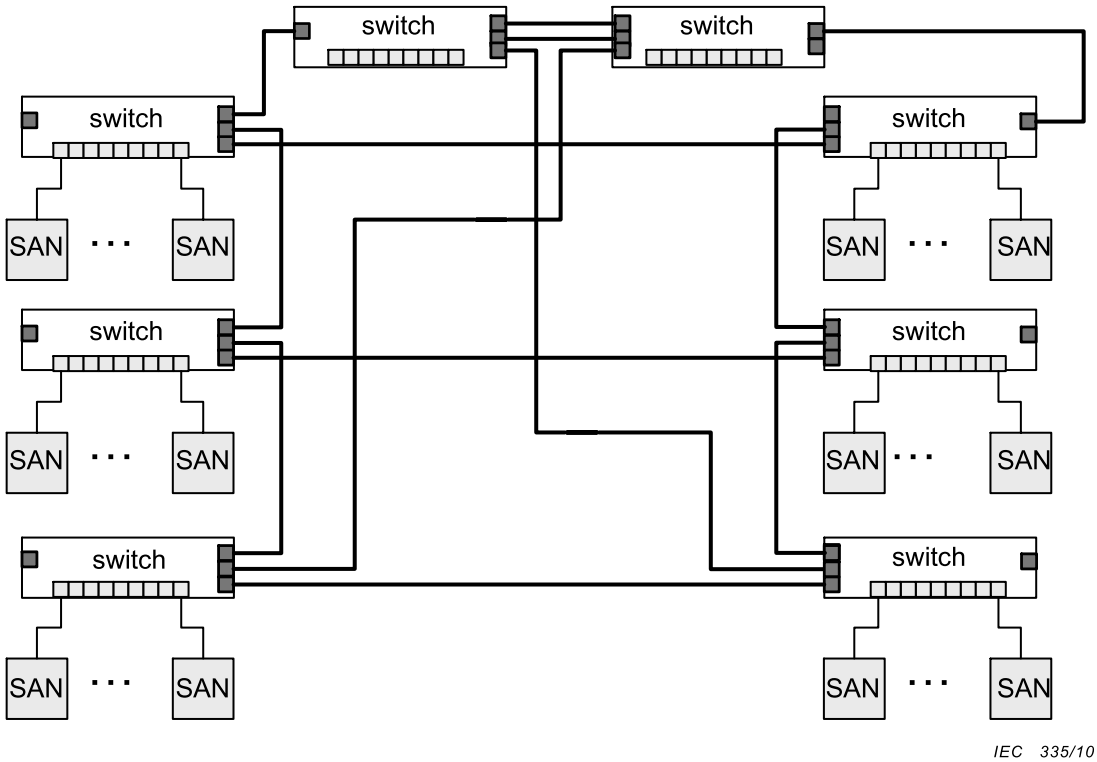
Figure 7 – Exemple d'une topologie partiellement maillée

5.2.2.3.3 Topologie entièrement maillée

Dans une topologie entièrement maillée, chaque commutateur possède plusieurs mailles inter-étage.

Dans une topologie entièrement maillée, la défaillance d'une maille inter-étage ou d'un commutateur peut être tolérée. Cependant, les nœuds d'extrémité connectés à un commutateur en panne perdent la connectivité. La Figure 8 montre un exemple d'une topologie entièrement maillée.

Copyright International Electrotechnical Commission



Légende

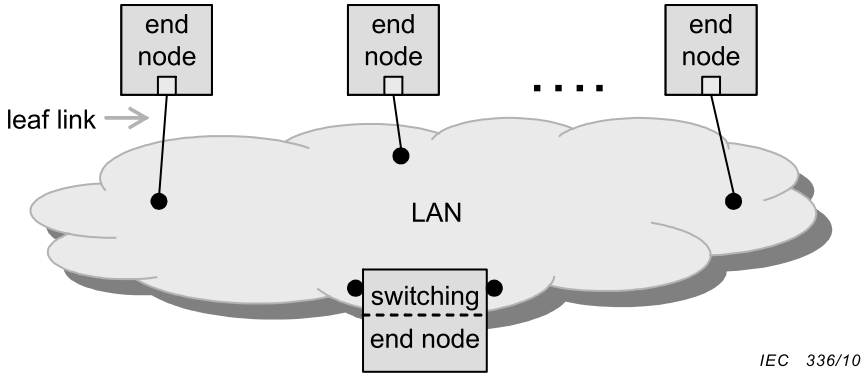
Anglais	Français
Switch	Commutateur

Figure 8 – Exemple d'une topologie entièrement maillée

5.2.2.4 Structures de haut niveau de réseaux

5.2.2.4.1 LAN simple sans liaisons en feuille redondantes

Cette topologie possède un seul chemin entre deux nœuds (voir Figure 9).



Légende

Anglais	Français
End node	Nœud d'extrémité
Leaf link	Liaison en feuille
Switching end node	Nœud d'extrémité de commutation

Figure 9 – Structure de LAN simple sans liaisons en feuille redondantes

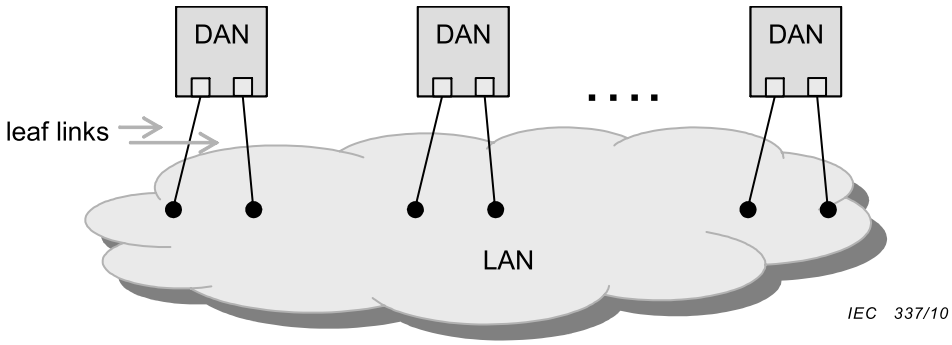
Des exemples de cette topologie sont la topologie en arbre et la topologie linéaire (voir Figure 4 et Figure 5).

Copyright International Electrotechnical Commission

5.2.2.4.2 LAN simple avec feuilles redondantes

NOTE Cette topologie s'applique, par exemple, à des nœuds comportant un commutateur RSTP ou un sous-ensemble de ceux-ci.

Les nœuds à double association (DAN) sont connectés au même LAN par le biais des liaisons en feuille. Chaque port d'extrémité peut appartenir au même commutateur ou à différents commutateurs. La Figure 10 montre un exemple.



Légende

Anglais	Français
Leaf links	Liaisons en feuille

Figure 10 – Structure de LAN simple avec liaisons en feuille redondantes

5.2.2.4.3 Réseau sans feuilles redondantes

NOTE Cette topologie s'applique au PRP (voir IEC 62439-3), au CRP (voir IEC 62439-4) et au BRP (voir IEC 62439-5).

Dans ce type de topologie, les chemins ne se chevauchent pas. Les liaisons en feuille redondantes sont connectées à des LAN différents. Un exemple est montré à la Figure 11.

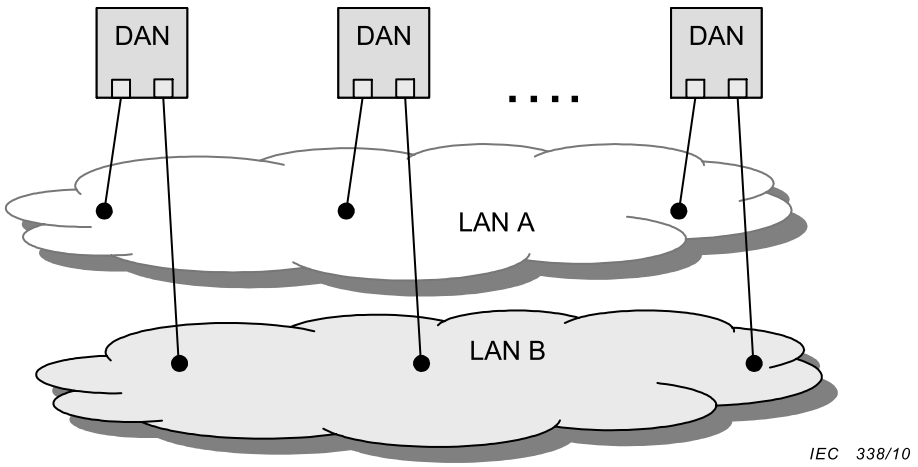


Figure 11 – Structure de LAN redondant sans liaisons en feuille redondantes

5.2.2.4.4 LAN redondant avec liaisons en feuille redondantes

Les liaisons en feuille redondantes sont connectées à la fois au même LAN et à des LAN différents. Les nœuds sont des nœuds à association quadruple (QAN). Un exemple est montré à la Figure 12.

Copyright International Electrotechnical Commission

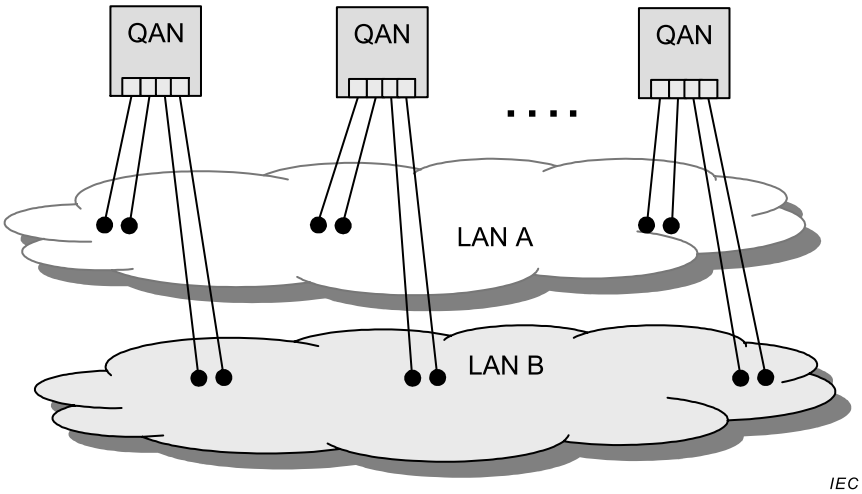


Figure 12 – Structure de LAN redondant avec liaisons en feuille redondantes

5.2.3 Gestion de la redondance

5.2.3.1 Mode secours

En mode secours, seul l'un des chemins redondants est choisi comme chemin en service alors que les autres chemins restent en veille.

Si le chemin en service devient indisponible, un autre chemin le remplace.

Durant le temps écoulé depuis la perte du chemin en service jusqu'au début de fonctionnement du chemin de secours, des messages peuvent être perdus et, par conséquent, la voie est considérée être en état déconnecté.

NOTE Le VEI appelle ce type de redondance, une redondance “en attente (stand-by)” ou “passive”. Le terme «redondance dynamique» est également utilisé.

5.2.3.2 Mode alterné (actif)

En mode alterné, les chemins redondants sont utilisés en alternance, de manière aléatoire ou selon des modèles réguliers, et les messages sont émis par l'intermédiaire de l'un des chemins redondants.

Si l'on détecte que l'un des chemins redondants est en état déconnecté, ce chemin cesse d'être utilisé pendant que les autres chemins continuent à être utilisés en alternance.

Ce mode permet de vérifier la disponibilité des composants en permanence et augmente ainsi la couverture.

5.2.3.3 Fonctionnement parallèle (actif)

En fonctionnement parallèle, les messages sont émis par l'intermédiaire de tous les chemins redondants disponibles.

Le nœud d'extrémité destinataire sélectionne l'un des messages reçus.

NOTE Le terme “redondance statique” ou “work-by” est aussi utilisé.

5.2.4 Temps de reprise du réseau

Le temps de reprise du réseau est appelé temps de reprise ("recovery time") dans la série IEC 62439 parce que la série IEC 62439 traite seulement les réseaux. La définition donnée en 3.1.41 s'applique.

Copyright International Electrotechnical Commission

5.2.5 Couverture de diagnostic

Les pannes sont détectées par des mécanismes de détection d'erreurs qui détectent seulement un pourcentage des pannes. La couverture est la probabilité que les mécanismes de diagnostic détectent une erreur dans un délai permettant le rétablissement avant que d'autres mécanismes ne prennent l'action de protéger l'installation ou avant que l'installation ne subisse de dommages.

5.2.6 Défaillances

5.2.6.1 Sortes de défaillances

Il existe trois sortes de défaillances:

- défaillance passagère,
- défaillance de composant et
- défaillance systématique.

Elles affectent les éléments suivants:

- les nœuds d'extrémité,
- les liaisons en feuille,
- les commutateurs,
- les mailles inter-étage.

5.2.6.2 Défaillance passagère

Une défaillance passagère, comme les interférences électromagnétiques, provoque des erreurs passagères qui laissent le matériel essentiellement intact, mais en perturbent la fonction. Dans ce cas, la partie défaillante peut être automatiquement réintégrée après des essais automatiques. De tels mécanismes sont partiellement mis en œuvre dans les protocoles de redondance spécifiés dans la série IEC 62439.

NOTE Les interférences EM peuvent devenir des défaillances systématiques.

5.2.6.3 Défaillance de composant

La défaillance d'un composant peut être partielle ou complète. Seules les défaillances complètes de composants (non temporaires, non parasites) sont prises en compte dans la série IEC 62439.

5.2.6.4 Défaillance systématique

Une défaillance systématique affecte plusieurs composants redondants en même temps; il s'agit par conséquent d'un point unique de défaillance. Les erreurs de configuration appartiennent aussi à cette catégorie. Les protocoles de redondance spécifiés dans la série IEC 62439 ne considèrent pas les défaillances systématiques mais permettent d'en détecter quelques-unes.

NOTE La diversité de la conception est éventuellement en mesure de réduire l'impact de défaillance systématique.

5.2.6.5 Défaillance d'un nœud d'extrémité

La défaillance d'un nœud d'extrémité est en dehors du domaine d'application de la série IEC 62439.

5.2.6.6 Défaillance d'une liaison en feuille

La défaillance d'une liaison en feuille est provoquée par:

Copyright International Electrotechnical Commission

- la défaillance du port de connexion d'un nœud d'extrémité,
- la défaillance du câble d'une liaison en feuille, ou
- la défaillance du port d'extrémité.

5.2.6.7 Défaillance d'un commutateur

Un commutateur se compose d'une fonctionnalité commutateur cœur (par exemple processeur, alimentation) et d'un nombre de ports.

Pour des besoins de calcul, une défaillance de commutateur ne considère que la défaillance de la fonction commutateur cœur.

La défaillance d'un port d'extrémité du commutateur est considérée comme une défaillance de la liaison en feuille.

La défaillance d'un port inter-étage du commutateur est considérée comme une défaillance de maille inter-étage.

5.2.6.8 Défaillance d'une maille inter-étage

La défaillance de maille inter-étage est provoquée par:

- la défaillance du port inter-étage ou
- la défaillance du câble de la maille inter-étage.

5.3 Sûreté

La série IEC 62439 ne considère pas les aspects de sûreté, par exemple, l'intégrité.

NOTE Même si la sûreté n'est pas directement traitée, une haute fiabilité est une caractéristique souhaitable dans un système de sûreté.

5.4 Sécurité

La série IEC 62439 ne considère pas les problématiques de sécurité (par exemple l'aspect privé, l'authentification).

6 Classification de réseaux (informative)

6.1 Notation

La structure de réseau relative à un réseau hautement disponible est exprimée par la notation suivante:

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

où

TYPE	indique le type de structure redondante de haut niveau;
NUMsn	indique le nombre de LAN redondants;
PLCYleaf	indique la politique de la redondance de liaison en feuille;
NUMleaf	indique le nombre de feuilles redondantes;
TPLGY	indique la topologie LAN.

EXEMPLE “A1N1RB” représente un réseau en anneau simple sans redondance de liaison en feuille.

Le champ <TYPE> est défini dans le Tableau 3.

Copyright International Electrotechnical Commission

Tableau 3 – Affectation de code pour le champ <TYPE>

Code	Structure redondante de haut niveau
A	Structure de LAN simple sans feuilles redondantes
B	Structure de LAN simple avec feuilles redondantes
C	Structure de LAN redondants sans feuilles redondantes
D	Structure de LAN redondants avec feuilles redondantes

Le champ <PLCYleaf> est défini dans le Tableau 4.

Tableau 4 – Affectation de code pour le champ <PLCYleaf>

Code	Politique relative à la redondance de liaison en feuille
P	Fonctionnement parallèle
A	Fonctionnement alterné
B	Fonctionnement secours
O	Autre politique redondante
N	N'est pas applicable ou pas de redondance de liaison en feuille

Le champ <TPLGY> est défini dans le Tableau 5.

Tableau 5 – Affectation de code pour le champ <TPLGY>

Code	Topologie LAN
S	Topologie simplex
R	Topologie en anneau
P	Topologie partiellement maillée
M	Topologie entièrement maillée
O	Autre topologie

6.2 Classification de robustesse

La robustesse d'un réseau hautement disponible est exprimée par la notation suivante:

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

où

ITYPE indique l'impact à considérer;

NUMleaf indique le nombre de défaillances des liaisons en feuille, acceptable pour le fonctionnement du réseau;

NUMtrunk indique le nombre de défaillances des mailles inter-étage, acceptable pour le fonctionnement du réseau;

NUMsw indique le nombre de défaillances des commutateurs, acceptable pour le fonctionnement du réseau.

Le champ <ITYPE> est défini dans le Tableau 6.

Copyright International Electrotechnical Commission

Tableau 6 – Affectation de code pour le champ <ITYPE>

code	Impact pour la classification de robustesse
N	Aucun impact n'est observé
R	Chaque nœud d'extrémité est capable de communiquer avec tous les autres nœuds d'extrémité, mais il y a une certaine période d'interruption
L	Un nombre limité de nœuds d'extrémité n'est pas en mesure de communiquer, mais d'autres nœuds d'extrémité sont en mesure de communiquer en présence d'une certaine interruption

EXEMPLE "R-L0T1S0" signifie que la défaillance d'une maille inter-étage n'affecte pas l'exploitation du réseau, sauf pour une certaine période d'interruption, mais la défaillance d'une liaison en feuille ou d'un commutateur n'est pas résolue par la redondance.

7 Calculs de disponibilité pour les réseaux sélectionnés (informative)

7.1 Définitions

Le réseau est considéré comme fonctionnel si chaque nœud d'extrémité est capable de communiquer avec tout autre nœud d'extrémité dans le réseau. Il est supposé que l'installation devienne indisponible si le réseau d'automatisation ne fonctionne pas.

NOTE 1 Cette définition peut être assouplie si une dégradation progressive est envisagée, mais cela dépend de l'application et n'est pas considérée ici.

La disponibilité du réseau est définie comme étant la fraction de temps pendant laquelle le réseau est fonctionnel, durant toute sa durée de vie. Le MTTF du réseau est la durée moyenne à partir d'un bon état initial jusqu'à la défaillance d'un composant. Supposons que la disponibilité est haute, le MTTF est légèrement égal au temps moyen entre défaillances (MTBF, Mean Time Between Failures), qui est le temps moyen entre les appels de maintenance.

Puisque la durée de vie du réseau est beaucoup plus longue que le MTTF, le chiffre qui décrit le mieux le comportement du réseau dans des conditions de panne est la durée moyenne de fonctionnement avant défaillance du réseau ou MTTFN.

La disponibilité du réseau est ainsi déduite en Équation (1):

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

où

MTTFN est la durée moyenne de fonctionnement avant défaillance du réseau, et

MTTRN (Mean Time To Repair Network) est la moyenne des temps pour la tâche de réparation.

NOTE 2 La disponibilité de l'installation est plus faible car il y a d'autres causes de défaillance à part celle du réseau et car le temps de restaurer l'installation après une défaillance du réseau est plus important que le temps de réparer le réseau.

Les taux de défaillance des éléments suivants sont considérés en cas d'utilisation:

λ_L = taux de défaillance des liaisons en feuille y compris les deux ports;

λ_S = taux de défaillance des commutateurs cœur, sans considérer les ports;

λ_T = taux de défaillance des mailles inter-étage y compris les deux ports.

Copyright International Electrotechnical Commission

NOTE 3 Le taux de défaillance s'applique au réseau uniquement, la fiabilité de l'application dans un appareil n'est pas considéré.

NOTE 4 Pour les besoins de calculs dans les exemples suivants, un exemple de réseau est considéré et consiste, dans le cas non redondant, de 5 commutateurs à 8 ports chacun, connectés en anneau. Les taux de défaillance types des éléments qui sont utilisés dans les exemples suivants sont:

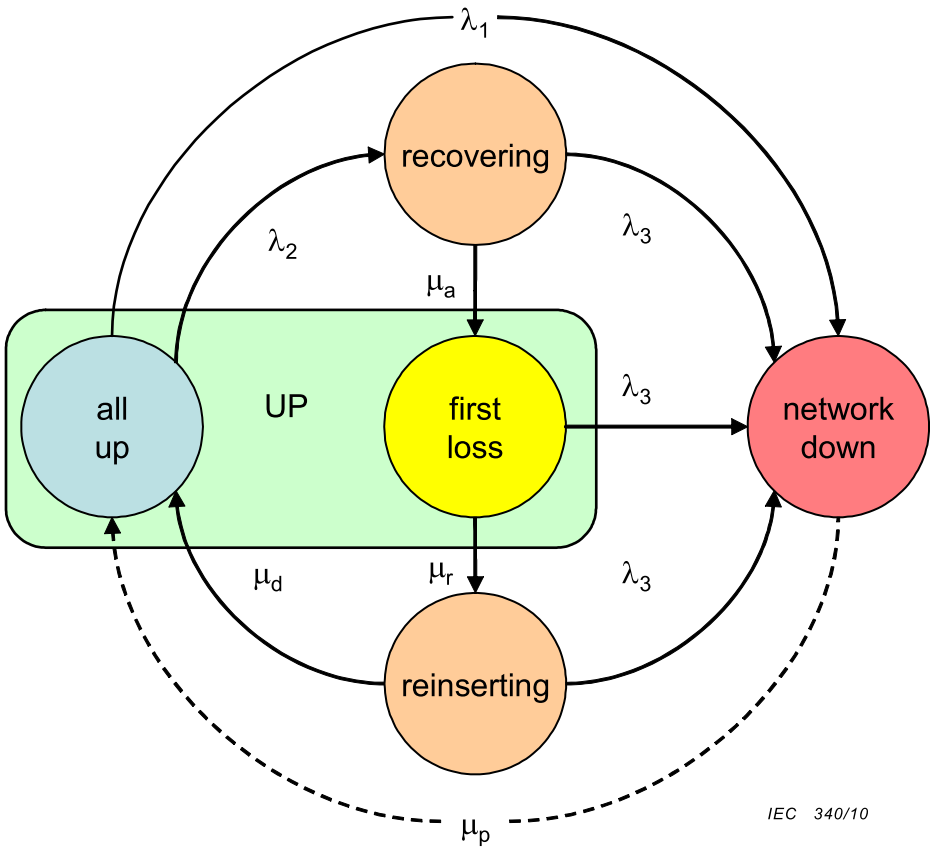
$$\lambda_S = 1 / \text{MTTFswitch} = 1/100 \text{ ans}$$

$$\lambda_L = \lambda_T = 1 / \text{MTTFlink} = 1/50 \text{ ans (liaison cuivre ou optique)}$$

7.2 Modèles de fiabilité

7.2.1 Modèle de fiabilité générique symétrique

Le modèle général de panne d'un réseau composé de parties redondantes et non redondantes est montré à la Figure 13. Ce modèle symétrique suppose que les rôles d'une unité principale et de son unité de secours ("stand-by" ou "work-by") soient interchangeables; c'est-à-dire qu'une fois que le réseau fonctionne avec l'unité de secours, il n'est pas nécessaire de basculer vers l'ancienne unité principale après la réparation.



Légende

Anglais	Français
Recovering	Rétablissement
All up	Tout en fonctionnement
First loss	Première perte
Network down	Réseau en panne
Reinserting	Réinsertion

Figure 13 – Modèle de panne générique symétrique

Copyright International Electrotechnical Commission

Les transitions sont:

λ_1 = taux de défaillance des composants non redondants
(y compris le point unique de défaillance et la probabilité d'un rétablissement non réussi)

λ_2 = taux de défaillance des composants redondants
(pour lesquels il existe une redondance et le rétablissement est réussi)

λ_3 = taux de défaillance des composants restants

μ_a = taux de rétablissement automatique
(durée entre l'apparition d'une panne et son rétablissement)

μ_d = taux d'interruption
(temps moyen d'interruption du réseau causée par la réinsertion)

μ_r = taux de rétablissement
(durée entre l'apparition d'une panne et la restauration de la redondance, inclut la réparation en ligne)

μ_p = taux de réparation de l'installation
(durée depuis l'apparition d'une panne non récupérable jusqu'à ce que l'installation soit remontée de nouveau)

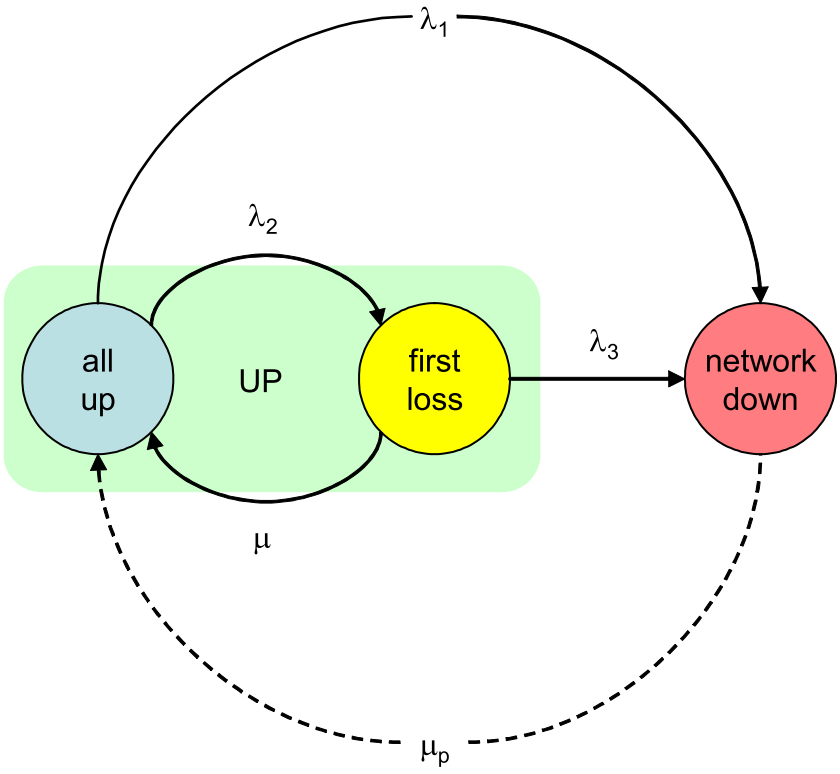
NOTE Les pannes inaperçues sont prises en compte dans μ_r et λ_1 plutôt que par l'introduction d'un état supplémentaire.

Ce modèle observe deux courtes interruptions: sur une première défaillance, il y a un temps court de reprise de panne pour activer la redondance; après la réparation, il y a un temps court de reprise de réinsertion de redondance pour restaurer le fonctionnement redondant. Tant que ces interruptions restent en dessous du temps d'interruption acceptable, elles n'affectent pas les calculs de disponibilité.

7.2.2 Modèle de fiabilité simplifié symétrique

Supposons que le réseau passe un temps très court dans les états de "rétablissement" et de "réinsertion", ces états peuvent être regroupés dans l'état "première perte", comme le montre la Figure 14.

Copyright International Electrotechnical Commission



Légende

Anglais	Français
All up	Tout en fonctionnement
First loss	Première perte
Network down	Réseau en panne

Figure 14 – Modèle de panne simplifié

La solution générale du modèle simplifié est exprimée dans l'Équation (2):

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

où

λ_2 est le taux de défaillance des composants redondants;
λ_3 est le taux de défaillance des composants restants;
μ est le taux de réparation.

Il serait en principe nécessaire d'introduire des transitions et des états relatifs à la défaillance des commutateurs et à la défaillance des liaisons. Cependant, puisque le réseau est constitué d'un grand nombre d'éléments et les taux de défaillance des commutateurs et des liaisons ne sont pas trop différents, un seul état "première défaillance" peut être utilisé.

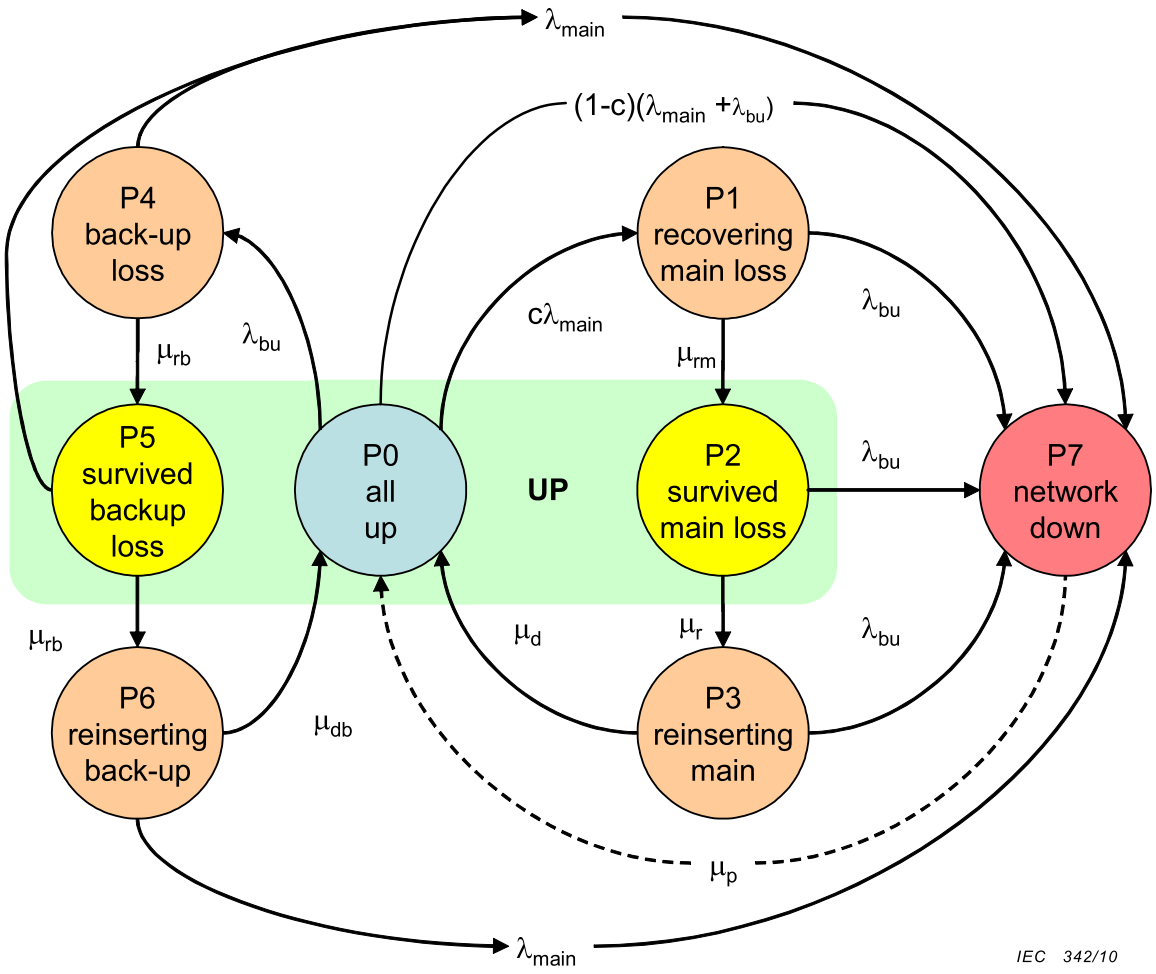
7.2.3 Modèle de fiabilité asymétrique

Dans de nombreux cas, le rôle principal et le rôle de secours ne sont pas interchangeables. Une redondance complète n'est rétablie que lorsque l'unité principale d'origine est de nouveau en place. Par conséquent, le modèle asymétrique considère plus d'interruptions, comme le montre la Figure 15. Les transitions de ce modèle ne sont pas détaillées car ce modèle est inclus seulement pour rappeler d'envisager d'éventuelles interruptions supplémentaires. Comme dans le cas précédent, les états d'interruption P1, P2, P4 et P6

Copyright International Electrotechnical Commission

n'ont aucune influence sur les calculs de la sûreté de fonctionnement tant que leur durée reste inférieure au temps d'interruption maximal acceptable.

NOTE Par analogie, considérer une voiture où la roue de secours est utilisée en cas d'urgence seulement et est destinée uniquement à atteindre en toute sécurité le prochain garage. Quand un pneu est crevé, deux changements de pneu sont nécessaires afin de rétablir le fonctionnement normal. En revanche, lorsque la roue de secours est identique à celle qu'elle remplace, une seule interruption est nécessaire.



Légende

Anglais	Français
P4 Backup loss	P4 Perte du secours
P1 Recovering main loss	P1 Rétablissement de la perte principale
P5 Survived backup loss	P5 Survit à une perte du secours
P0 All up	P0 Tout en bon fonctionnement
UP	EN BON FONCTIONNEMENT
P2 Survived main loss	P2 Survit à une perte du principal
P7 Network down	P7 Réseau en panne
P6 Reinserting backup	P6 Réinsertion du secours
P3 Reinserting main	P3 Réinsertion du principal

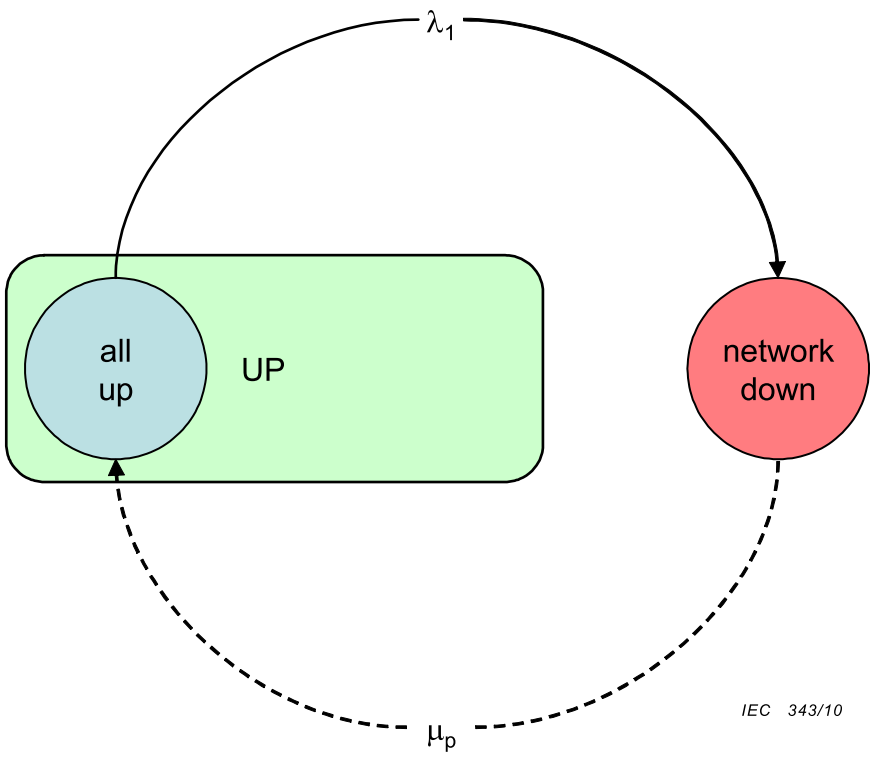
Figure 15 – Modèle de panne asymétrique

Copyright International Electrotechnical Commission

7.3 Disponibilité des structures sélectionnées

7.3.1 LAN simple sans feuilles redondantes

Dans un réseau non redondant, la défaillance d'un élément quelconque entraîne la défaillance du réseau, comme le montre la Figure 16 .



Légende

Anglais	Français
All up	Tout en bon fonctionnement
UP	En bon fonctionnement
Network down	Réseau en panne

Figure 16 – Réseau sans redondance

Par conséquent, le MTTFN se simplifie en Équation (3).

$$MTTFN = \frac{1}{\lambda_1} \tag{3}$$

où $\lambda_1 = \Sigma (\lambda_L + \lambda_S + \lambda_T)$

EXEMPLE Pour l'exemple de réseau (5 commutateurs, 40 liaisons en feuille, 5 mailles inter-étage)

MTTFN = 1,05 an et

MTTF = 1,05 an.

7.3.2 Réseau sans feuilles redondantes

Dans l'hypothèse où le taux de réparation est beaucoup plus élevé que le taux de défaillance, seule la fiabilité des liaisons en feuille importe et l'Équation (3) se réduit à l'Équation (4):

Copyright International Electrotechnical Commission

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

où $\lambda_1 = \Sigma (\lambda_L)$, sachant que tous les commutateurs et les mailles inter-étage sont redondants.

Cela signifie que, si le taux de réparation est assez élevé (MTTR en quelques jours par rapport à quelques années de MTTF), la fiabilité est entièrement dictée par les parties non redondantes du réseau et que la redondance permet simplement de négliger les éléments redondants dans le calcul du MTTFN.

EXEMPLE Pour l'exemple de réseau (5 commutateurs, 40 liaisons en feuille non redondantes, 6 mailles inter-étage)

MTTFN = 1,17 an

MTTF = 1,03 an.

NOTE Dans le cas de nœuds d'extrémité de commutation, le MTTFN est beaucoup plus élevé, car les liaisons en feuille sont internes aux nœuds et sont prises en compte dans le taux de défaillance des nœuds.

7.3.3 LAN simple avec feuilles redondantes

Dans ce cas, le taux de défaillance des liaisons en feuille peut être ignoré. Comme le nombre de ports par commutateur est supposé être constant, le nombre de commutateurs est doublé.

EXEMPLE Pour l'exemple de réseau (10 commutateurs, 80 liaisons en feuille redondantes, 11 mailles inter-étage redondantes):

MTTFN = 9,78 an

MTTF = 0,52 an.

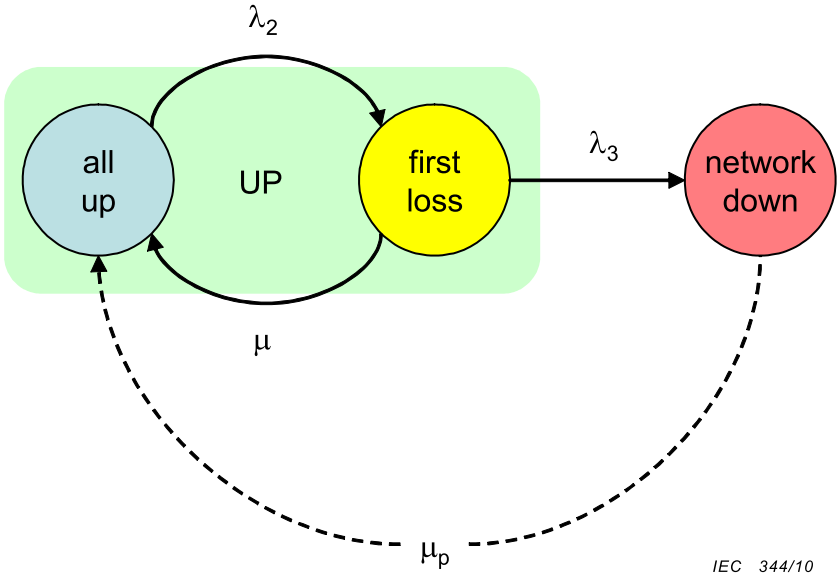
NOTE 1 Cela montre que l'augmentation de la fiabilité obtenue par une double association de nœuds est réduite par le nombre croissant de commutateurs qui sont nécessaires. Le MTTF double par rapport au cas non redondant puisque le nombre de liaisons et de ports a doublé. Par conséquent, cette structure n'a de sens que dans le contexte d'une dégradation progressive, où les appareils importants possèdent une association redondante, mais ne nécessitent pas de connectivité avec tous les nœuds d'extrémité.

NOTE 2 Dans le cas de nœuds d'extrémité de commutation, le MTTFN est beaucoup plus élevé, car les liaisons en feuille sont internes aux nœuds et leur non-fiabilité est considérée dans le taux de défaillance des nœuds.

7.3.4 Réseau avec feuilles redondantes

Supposons que tous les éléments du réseau soient redondants, le taux de défaillance λ_1 est réduit à un point unique de défaillance et aux défaillances de rétablissement/réinsertion. Si celles-ci peuvent être négligées par une conception appropriée, le modèle de fiabilité est donné à la Figure 17.

Copyright International Electrotechnical Commission



Légende

Anglais	Français
All up	Tout en bon fonctionnement
UP	EN BON FONCTIONNEMENT
First loss	Première perte
Network down	Réseau en panne

Figure 17 – Réseau sans point unique de défaillance

Le MTTFN se simplifie en Équation (5):

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

où $\lambda_2 = \Sigma (\lambda_L + \lambda_S + \lambda_T)$ et $\lambda_3 = \lambda_2/2$

Le taux de défaillance λ_3 des éléments restants est supposé être la moitié de celui du réseau entier, puisque les secondes défaillances du LAN déjà dégradé n'affectent pas le fonctionnement.

Le MTTFN est légèrement augmenté par rapport au cas non redondant deux fois le rapport du taux de réparation sur le taux de défaillance, ce qui est généralement élevé, par exemple MTTR = 24 heures par rapport au MTTF = 1 an.

EXEMPLE Pour l'exemple de réseau (2 × 5 commutateurs, 2 × 40 liaisons en feuille, 2 × 6 mailles inter-étage):

MTTFN = 196 an.

MTTF = 0,58 an.

NOTE 1 Cela montre que même si le réseau est entièrement redondant, la disponibilité est encore limitée et que la duplication du réseau provoque le double d'un taux de maintenance élevé, puisqu'il y a deux fois plus d'éléments pouvant tomber en panne.

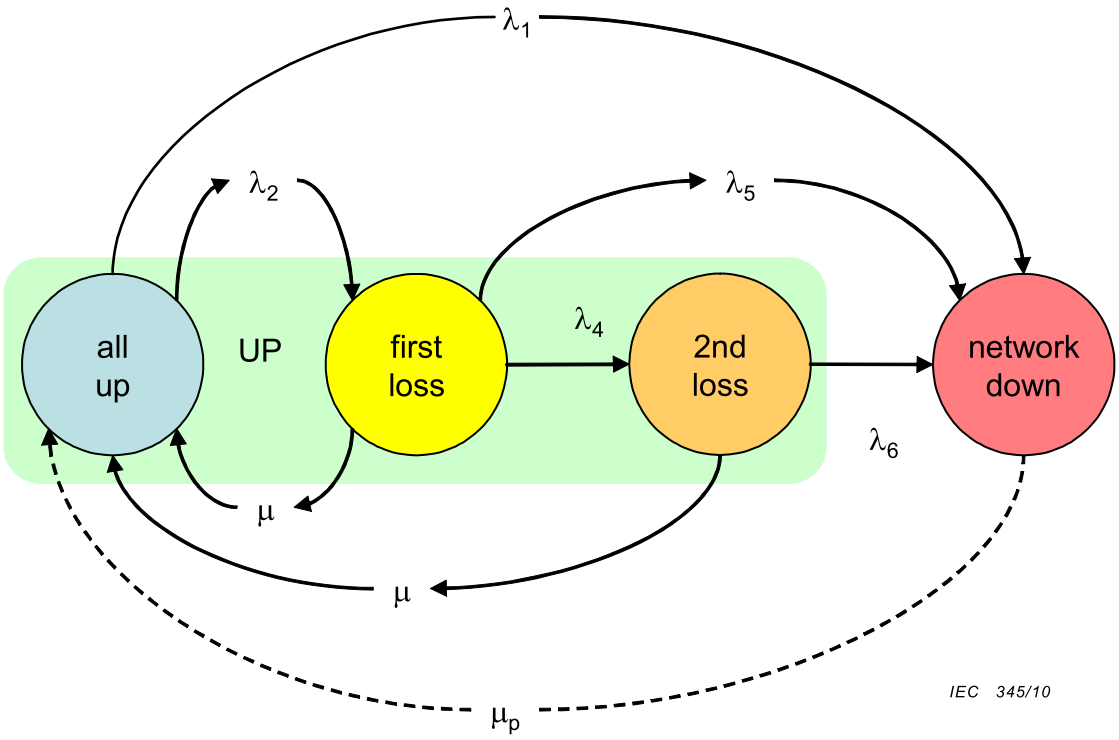
NOTE 2 Ce MTTFN qui paraît élevé a été calculé en négligeant les erreurs de mode commun. Si l'on considère la fiabilité de l'ensemble du système d'automatisation, le taux de défaillance du nœud d'extrémité domine le MTTFS et il convient d'envisager la redondance du nœud d'extrémité. Même un simple élément non redondant ou une cause commune de défaillance comme une erreur de logiciel abaisse fortement le MTTFN.

Copyright International Electrotechnical Commission

7.3.5 Considération de secondes défaillances

Le calcul ci-dessus est pessimiste car il suppose qu'une deuxième défaillance perturbe le reste du réseau avec une probabilité de 100 %. Cela est vrai pour les commutateurs lorsque le LAN ne dispose pas de redondance à l'intérieur, mais ce n'est pas le cas pour les liaisons en feuille puisque la probabilité d'une deuxième défaillance perturbant le même nœud d'extrémité n'est pas donnée par Σ (λ_L), mais simplement par λ_L.

Pour une estimation plus précise, le diagramme de transition de la Figure 18 peut être utilisé.



Légende

Anglais	Français
All up	Tout en bon fonctionnement
UP	EN BON FONCTIONNEMENT
First loss	Première perte
2nd loss	Deuxième perte
Network down	Réseau en panne

Figure 18 – Réseau avec une résilience à la deuxième défaillance

Les transitions sont:

λ_1 = taux de défaillance des composants non redondants
(y compris le point unique de défaillance et la probabilité d'un rétablissement non réussi).

λ_2 = taux de défaillance des composants redondants
(pour lesquels il existe une redondance et le rétablissement est réussi).

λ_4 = taux de défaillance des composants restants qui n'entraînent pas de perte du réseau.

λ_5 = taux de défaillance des composants restants qui entraînent une perte du réseau
(la somme de λ_4 et λ_5 est approximativement égale à λ_2, ainsi $\lambda_5 = f\lambda_2$,
où f est la probabilité que la deuxième erreur entraîne une défaillance du réseau.

λ_6 = taux de défaillance des composants restants après une deuxième défaillance.

Copyright International Electrotechnical Commission

μ = taux de rétablissement
(durée entre l'apparition d'une panne jusqu'à la restauration de la redondance, inclut la réparation en ligne)

μ_p = taux de réparation de l'installation
(durée entre l'apparition d'une panne non récupérable jusqu'à ce que l'installation fonctionne de nouveau).

le MTTFN du réseau est donnée par l'Équation (6).

$$MTTFN = \frac{(\mu + \lambda_2 + \lambda_4 + \lambda_5) + \frac{\lambda_2 \lambda_4}{\mu + \lambda_6}}{\lambda_1(\mu + \lambda_4 + \lambda_5) + \lambda_2\left(\lambda_5 + \lambda_4\left(\frac{1}{1 + \frac{\mu}{\lambda_6}}\right)\right)} \quad \mu >> \sum(\lambda_i) \approx \frac{1}{\lambda_1 + \frac{\lambda_2^2 f}{\mu}} \tag{6}$$

Supposons que les défaillances de mode commun (λ_1) puissent être négligées, le MTTFN est légèrement amélioré par rapport à la structure de la Figure 14 comme étant le rapport entre les secondes défaillances récupérables et les secondes défaillances non récupérables, λ_4 sur λ_5, ce rapport dépendant de la topologie.

Le taux de défaillance depuis la deuxième perte jusqu'à la défaillance du réseau n'influence pas significativement le résultat, puisque le système passe très peu de sa durée de vie dans l'état de deuxième perte, si le taux de réparation est élevé.

EXEMPLE Avec λ_1= 0 (pas de mode commun de défaillance), $\lambda_2 = \Sigma (\lambda_L + \lambda_S + \lambda_T)$, λ_4 = 0,9 λ_2, λ_5 = 0,1 λ_2 (1 panne sur dix n'est pas récupérable), $\lambda_6 = \lambda_2$.

MTTFN = 1 868 an.

7.4 Mise en garde

Il convient d'utiliser ces calculs comme une mise en garde que la redondance n'est pas en mesure de résoudre tous les problèmes de fiabilité et que l'hypothèse de base que le réseau est opérationnel lorsque tous les nœuds peuvent communiquer avec tous les autres nœuds, peut être relâchée dans des cas particuliers.

8 RSTP pour des réseaux à haute disponibilité: règles de configuration, méthode de calcul et de mesure pour un temps de rétablissement ~~déterministe~~ prévisible

NOTE Dans le contexte du présent Article, le terme “pont” est utilisé à la place de “commutateur”, respectivement “ponter” au lieu de “commuter”.

8.1 Généralités

Le protocole RSTP (Rapid Spanning Tree Protocol) tel que spécifié dans la norme IEEE 802.1D offre une prévention contre les boucles et une gestion de la redondance pour une topologie arbitraire des réseaux Ethernet commutés.

Le protocole RSTP fournit un rétablissement de deux types de pannes de réseau

a) une défaillance de maille inter-étage et
b) une défaillance de commutateur, qui peut être de deux types, en fonction du rôle du commutateur au moment de sa panne:

Copyright International Electrotechnical Commission

1) une défaillance d'un commutateur non-racine que le RSTP traite comme une défaillance de maille inter-étage ou
2) une défaillance d'un commutateur racine que le RSTP traite par la reconfiguration du réseau.

Bien que le protocole RSTP comprenne un algorithme efficace pour le rétablissement du réseau, le temps de reprise réel de la panne dépend de la topologie et de la mise en œuvre du RSTP.

En général, le protocole RSTP fournit un temps de reprise déterministe même dans une topologie arbitrairement maillée en cas de défaillance d'une liaison ou de défaillance d'un commutateur non-racine. Toutefois, en cas de défaillance d'un commutateur racine, il est difficile de prévoir le temps de reprise dans une topologie arbitrairement maillée.

En revanche, lorsque la topologie est limitée à un anneau, le temps de reprise d'une panne par RSTP est déterministe dans tous les scénarios et peut être calculé, à condition que les caractéristiques de performance de synchronisation du RSTP relatives aux commutateurs soient connues.

Le présent paragraphe spécifie la topologie en anneau de référence, la méthode de calcul pour calculer le temps de reprise relatif à cette topologie de référence, la méthode de mesure des caractéristiques de performance de synchronisation pertinentes d'une mise en œuvre du protocole RSTP et la forme sous laquelle il convient qu'elles soient divulguées.

8.2 Règles de déploiement et de configuration pour la topologie en anneau

Pour obtenir un temps de reprise déterministe, et pour les besoins des calculs suivants, les règles de configuration suivantes doivent être respectées:

- La topologie du réseau doit être limitée à un seul anneau de N appareils.
- Comme l'exigent les spécifications du RSTP, N doit être inférieur ou égal à 40.
- Les ports d'anneau doivent être activés pour le fonctionnement du RSTP.
- Les ports n'appartenant pas à l'anneau ne doivent pas être activés pour le fonctionnement du RSTP.
- Toutes les liaisons doivent être configurées pour opérer en mode bilatéral simultané (full-duplex).
- Les convertisseurs de supports, s'ils sont utilisés en connexions inter-étage, doivent fonctionner en mode de liaison transparent.
- Les commutateurs doivent être configurés de sorte qu'ils n'utilisent pas la classe de service la plus haute disponible à l'exception des BPDU ou, si cela n'est pas possible, au moins 10 % de la bande passante de la classe de service la plus haute disponible doit être réservé pour les BPDU.

NOTE La désactivation des ports n'appartenant pas à l'anneau pour RSTP a pour conséquence que les boucles connectées aux ports n'appartenant pas à l'anneau ne seront pas évitées par RSTP.

8.3 Calculs pour le temps de reprise de panne dans un anneau

8.3.1 Dépendances et modes de défaillance

Le temps de reprise de panne par RSTP dépend des facteurs suivants:

- l'emplacement du point de défaillance lié au(x) port(s) de rejet qui termine(nt) la/les branche(s) d'arbre recouvrant,
- la combinaison des paramètres de configuration du RSTP dans différents commutateurs dans le(s) segment(s) affectés du réseau.

Les modes de défaillance suivants sont considérés:

Copyright International Electrotechnical Commission

- perte d'une maille inter-étage,
- perte d'un nœud dans le rôle non-racine,
- perte d'un nœud dans le rôle racine.

RSTP dépend de la détection de l'état de la liaison.

8.3.2 Calculs pour les modes de défaillance non considérés

Si une défaillance se produit de telle sorte qu'aucune erreur de liaison n'est détectée et qu'aucune BPDU n'est envoyée, le temps de reprise s'élèvera à une valeur qui est trois fois le temps "Hellotime", qui est actuellement spécifié comme un minimum de 1 s dans l'IEEE 802.1D: 2004.

NOTE Les mécanismes pour prévenir cette situation sont possibles, mais ne sont pas exigés dans l'IEEE 802.1D.

8.3.3 Calculs pour les modes de défaillance considérés

Les formules ci-dessous présentent la limite supérieure du temps de reprise de panne dans un réseau en anneau:

- $T_L + N*max(T_{PA} , (T_{TC}+T_F))$ – pour une défaillance de mailles inter-étage et une défaillance de commutateurs non-racine
- $T_L + 2*N*T_{PA}$ – pour une défaillance de commutateurs racine

où:

N est le nombre de commutateurs dans l'anneau;

T_L est le temps requis par un commutateur pour détecter une défaillance de liaison;

T_{PA} est le temps requis par une paire de commutateurs pour effectuer l'établissement de liaison "Proposition-Accord" (Proposal-Agreement) du protocole RSTP; égal à la somme des temps de traitement de la BPDU dans les deux commutateurs de la paire ;

T_{TC} est le temps requis par une paire de commutateurs pour propager une BPDU de changement de topologie; égal à la somme des temps de traitement de la BPDU dans les deux commutateurs de la paire;

NOTE 1 T_{TC} est approximativement la moitié de T_{PA} puisqu'aucun acquittement n'est impliqué.

T_F est le temps requis par un commutateur pour vider sa table d'adresses MAC.

Un autre paramètre non utilisé dans les formules ci-dessus est défini pour les mesures de synchronisation:

T_{Proc} est le temps de traitement du RSTP, c'est-à-dire le temps requis pour traiter un cycle entier de diagrammes d'états RSTP.

NOTE 2 T_{PA} est en fait la somme du temps de traitement descendant (“downlink”) d'un commutateur et le temps de traitement ascendant (“uplink”) du commutateur adjacent (générant une BPDU "Proposal" (Proposition), traitant la BPDU "Proposal" et générant une BPDU "Agreement" (Accord), et traitant la BPDU "Agreement"). Un cycle entier de diagrammes d'états RSTP inclut les temps de traitement “ascendant” et “descendant” d'un commutateur, c'est-à-dire approximativement $T_{Proc} = T_{PA}$.

EXEMPLE Pour atteindre un temps de reprise de 130 ms dans un anneau de 40 appareils, pour tous les commutateurs, il convient que le temps T_L soit inférieur à 10 ms pour des liaisons 100Base-TX et 100Base-FX et que le temps T_{PA} et la somme ($T_{TC} + T_F$) soient inférieurs à 3 ms.

NOTE 3 Cela requiert que le port du commutateur matériel prenne en charge la détection rapide de défaillance de liaison, telle que spécifiée par l'ISO/IEC 8802-3 (IEEE 802.3).

NOTE 4 Les liaisons 1000Base-T ne peuvent pas être utilisées pour les connexions inter-étage dans cette application en raison de leur important temps de détection de défaillance de liaison.

NOTE 5 Cela peut être assuré en donnant la priorité aux tâches de surveillance des liaisons et de traitement du microprogramme RSTP et par la vitesse du processeur et la mise en œuvre du microprogramme RSTP appropriés.

Copyright International Electrotechnical Commission

8.4 Méthode de mesure de la synchronisation (timing)

8.4.1 Mesure de T_{PA}

8.4.1.1 Mesure

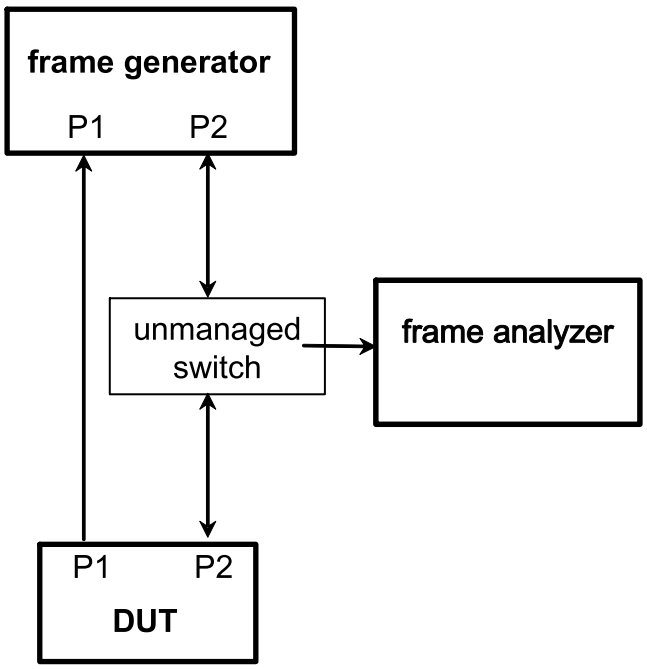
Il est impossible de mesurer séparément certaines valeurs de temps définies ci-dessus. Par conséquent, certains essais mesurent une combinaison de plusieurs valeurs de temps, de sorte que le temps en question peut être calculé à partir de la valeur mesurée.

Cet essai mesure en fait le temps T_{Proc} mais T_{Proc} est égal à T_{PA}, comme expliqué en 8.3.3.

8.4.1.2 Configuration

Configurer le système comme suit:

a) Construire le réseau d'essai comme montré à la Figure 19.



Légende

Anglais	Français
Frame generator	Générateur de trames
Frame analyzer	Analyseur de trames
Unmanaged switch	Commutateur non géré
DUT	Appareil en essai

Figure 19 – Banc d'essai pour mesure de T_{PA}

b) Configurer l'appareil en essai de sorte que les paramètres 'AdminEdge' et 'AutoEdge' des ports connectés sont mis à "FALSE".

c) Configurer le Port2 du générateur de trames pour envoyer une BPDU "Proposal" (c'est-à-dire avec le fanion "proposal" défini et "root bridge ID" meilleur que celui de l'appareil en essai).

d) Configurer le Port1 du générateur de trames seulement pour maintenir une liaison Ethernet mais pas pour envoyer toutes les trames. Ce port simulera un autre commutateur RSTP auquel l'appareil en essai propagera une proposition.

Copyright International Electrotechnical Commission

e) Configurer l'analyseur de trames pour capturer les trames reçues à partir du commutateur non géré.

8.4.1.3 Procédure

La procédure est comme suit:

a) vérifier que l'appareil en essai s'est choisi comme "racine".

b) commencer à capturer les trames dans l'analyseur de trames.

c) émettre une seule BPDU à partir du générateur de trames.

d) arrêter de capturer les trames.

e) vérifier que l'appareil en essai a envoyé une BPDU "agreement" en réponse à la BPDU "proposal".

f) mesurer l'intervalle de temps entre la BvPDU "proposal" et la première BPDU "agreement".

8.4.2 Mesure de T_L

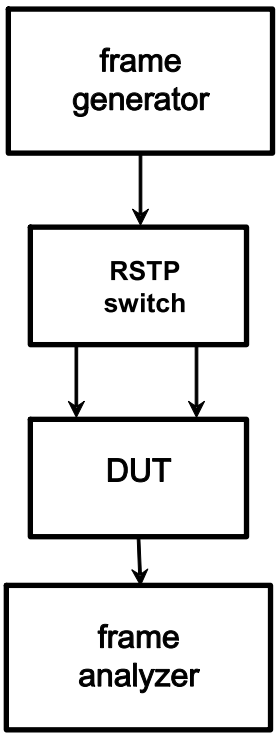
8.4.2.1 Mesure

Cet essai mesure en fait le temps (T_L + T_{Proc}). Sachant que T_{Proc} a été mesuré par l'essai précédent, T_L est déduit de (T_L + T_{Proc}).

8.4.2.2 Configuration

Configurer le système comme suit:

a) construire le réseau comme montré à la Figure 20.



IEC 347/10

Légende

Anglais	Français
Frame generator	Générateur de trames
RSTP switch	Commutateur RSTP
DUT	Appareil en essai

Copyright International Electrotechnical Commission

Anglais	Français
Frame analyzer	Analyseur de trames

Figure 20 – Banc d'essai pour mesure de T_L

b) mettre le paramètre “Bridge priority” du commutateur RSTP à 0 afin de le forcer à être élu comme “racine”.

c) configurer le générateur de trames pour envoyer un flux continu de trames arbitraires à un débit minimal de 4 000 trames par seconde afin de permettre une résolution de mesure de temps de 0,25 ms.

d) configurer l'analyseur de trames pour capturer les trames reçues à partir de l’appareil en essai.

8.4.2.3 Procédure

La procédure est comme suit:

a) vérifier que le commutateur RSTP a été choisi comme “racine”.

b) vérifier que l'un des ports de l’appareil en essai a un statut “root forwarding” (transmission racine) et l'autre port a un statut “alternate discarding” (rejet remplaçant).

c) commencer à émettre à partir du générateur de trames.

d) commencer à capturer les trames.

e) vérifier que les trames sont reçues par l'analyseur de trames.

f) couper la liaison associée au port “root” de l’appareil en essai. Cela mènera l’appareil en essai à basculer vers son port “alternate”.

g) vérifier que les trames sont reçues par l'analyseur de trames.

h) arrêter de capturer les trames.

i) mesurer pour combien de temps la réception de trames a été perturbée.

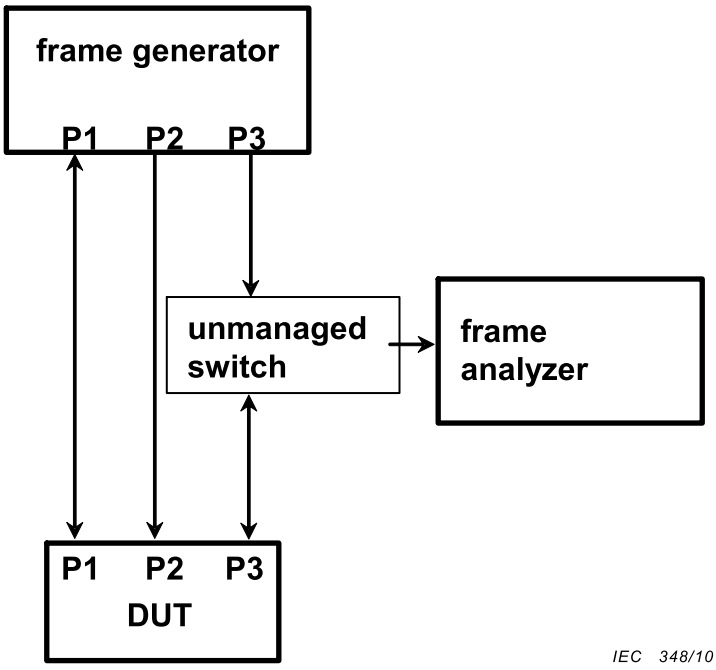
8.4.3 Mesure de (T_{TC} + T_F)

8.4.3.1 Configuration

Configurer le banc d'essai comme suit:

a) construire le réseau d'essai comme montré à la Figure 21.

Copyright International Electrotechnical Commission



Légende

Anglais	Français
Frame generator	Générateur de trames
Frame analyzer	Analyseur de trames
Unmanaged switch	Commutateur non géré
DUT	Appareil en essai

Figure 21 – Banc d'essai pour mesure de (T_{TC} + T_F)

b) mettre les paramètres ‘AutoEdge’ et ‘AdminEdge’ du Port1 et du Port3 de l’appareil en essai à FALSE.

c) mettre le paramètre ‘AutoEdge’ du Port2 de l’appareil en essai à FALSE et le paramètre ‘AdminEdge’ à TRUE.

d) configurer le Port1 du générateur de trames pour envoyer une seule trame arbitraire.

e) configurer le Port2 du générateur de trames pour envoyer un flux continu de trames à l'adresse MAC destination du Port2 à un débit minimal de 4 000 trames par seconde afin de permettre une résolution de mesure de temps de 0,25 ms.

f) configurer le Port3 du générateur de trames pour envoyer une seule BPDU “agreement + topology change” (“accord + changement de topologie”).

g) configurer l'analyseur de trames pour capturer les trames reçues à partir du commutateur non géré.

8.4.3.2 Procédure

La procédure est comme suit:

a) vérifier que l’appareil en essai s'est élu lui-même comme “racine”.

b) émettre une seule trame à partir du Port1 du générateur de trames. Cela permettra que le Port1 de l’appareil en essai apprenne l'adresse MAC source de la trame.

c) commencer à émettre un flux continu à partir du Port2 du générateur de trames.

d) commencer à capturer les trames dans l'analyseur de trames.

e) vérifier que le flux n'est pas transmis à partir du Port3 de l’appareil en essai (il est transmis uniquement à partir du Port1 de l’appareil en essai).

Copyright International Electrotechnical Commission

f) envoyer une seule BPDU à partir du Port3 du générateur de trames. Cela entraînera l'appareil en essai à purger sa table d'adresses MAC et commencer à inonder le flux de trafic à partir du Port3, ainsi il sera capturé par l'analyseur de trames.

g) arrêter de capturer les trames.

h) vérifier que l'appareil en essai a commencé à inonder le flux à partir du Port3 en réponse à la BPDU "changement de topologie".

i) mesurer l'intervalle de temps entre la BPDU "changement de topologie" et la première trame de flux.

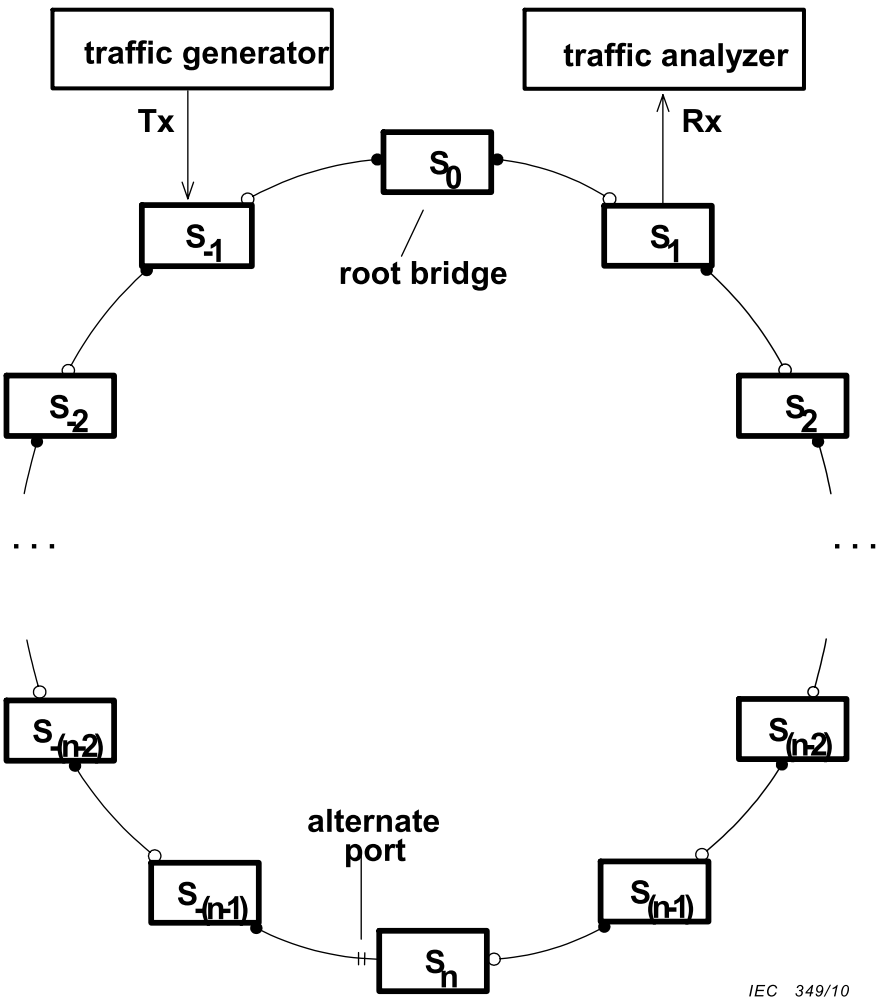
j) répéter a) ... i) pour 10 valeurs différentes choisies aléatoirement de l'adresse MAC source utilisée par le Port1 du générateur de trames (et donc l'adresse MAC destination utilisée par le Port2 du générateur de trames) et choisir la valeur maximale parmi toutes les mesures.

8.4.4 Exemple d'essai de système

8.4.4.1 Configuration

Configurer le système comme suit:

a) construire un anneau de commutateurs, composé de 20-40 commutateurs se conformant à la spécification IEEE 802.1D:2004 RSTP comme montré à la Figure 22.



Légende

Anglais	Français
Traffic generator	Générateur de trafic

Copyright International Electrotechnical Commission

Anglais	Français
Traffic analyzer	Analyseur de trafic
Root bridge	Pont racine
Alternate port	Port remplaçant

Figure 22 – Banc d'essai pour l'essai du système

b) s'assurer que toutes les liaisons sont conformes aux exigences de déploiement spécifiées en 8.2.

c) configurer le générateur de trafic pour envoyer des trames destinées à l'adresse MAC du port Rx à partir de son port Tx. Il convient de choisir le débit de transmission suffisamment élevé pour que temps de reprise de panne puisse être calculé sur la base d'un nombre de paquets perdus avec une résolution de l'ordre de milliseconde.

d) configurer le générateur de trafic pour envoyer des trames arbitraires de faible débit (par exemple une fois en quelques secondes) à partir de son port Rx avec l'adresse MAC source du port Rx (afin que les commutateurs l'apprennent).

e) configurer l'analyseur de trafic pour afficher les compteurs de trames Tx et Rx.

f) mettre tous les paramètres RSTP des commutateurs aux valeurs par défaut. Vérifier que tous les commutateurs ont leur "bridge priority" mis à 32 768.

g) mettre à 0 le "bridge priority" S_0 du commutateur, afin que S_0 soit élu comme un commutateur racine.

h) mettre à 4 096 le "bridge priority" S_1 du commutateur, afin que S_1 soit le meilleur prochain candidat racine après S_0.

8.4.4.2 Procédure

La procédure est comme suit:

a) vérifier que le port remplaçant est sur le commutateur S_n, sur la liaison S_n–$S_{-(n-1)}$.

b) commencer à émettre à faible débit des trames fictives à partir du port de trafic Rx. Vérifier que les commutateurs S_{-1}, S_0 et S_1 ont appris l'adresse MAC du port Rx.

c) commencer à émettre des trames à partir du port Tx. Vérifier que le compteur Rx s'incrémente avec le compteur Tx et qu'aucun trafic n'est perdu.

d) couper la liaison S_0–S_1.

e) vérifier que le compteur Rx s'incrémente (c'est-à-dire la connectivité a été rétablie).

f) arrêter d'émettre à partir du port Tx.

g) lire les compteurs Tx et Rx et calculer le nombre de trames perdues.

h) calculer le temps de reprise de panne en utilisant la formule t = (nombre de trames perdues) / (débit de trames).

8.5 Limites de topologie RSTP et temps de rétablissement maximal

NOTE Dans la prochaine édition de l'IEC 62439-1, ce nouveau Paragraphe sera renuméroté 8.2.

8.5.1 Paramètres du protocole RSTP

Le présent paragraphe explique les paramètres du protocole RSTP ayant une influence sur les temps de rétablissement maximaux et décrit comment une configuration spécifique de topologie et de protocole les influence. Les termes spécifiques à RSTP sont d'abord définis. Des lignes directrices de base relatives à la conception du réseau sont ensuite données, tandis qu'une méthode de détermination d'une approximation d'un temps de reconfiguration de réseau de limite supérieure le plus défavorable pour des réseaux maillés RSTP est fournie.

Le présent paragraphe traite en particulier des réseaux RSTP composés de plus d'un anneau. Pour un seul anneau Ethernet fonctionnant sur RSTP, le temps de reconfiguration du réseau

Copyright International Electrotechnical Commission

peut être déterminé comme le montre le 8.2. Cependant, les énoncés suivants concernant des paramètres RSTP s'appliquent également dans un réseau en anneau.

8.5.2 Termes et définitions spécifiques à RSTP

NOTE Ces termes sont tirés de l'IEEE 802.1D.

8.5.2.1 Délai de transmission (TxHoldCount)

Chaque port d'un pont RSTP comprend un compteur TxHoldCount. Ce compteur démarre à zéro et est incrémenté à chaque envoi de BPDU par le port. Une minuterie décrémente le compteur à chaque seconde. Si TxHoldCount atteint la valeur maximale, aucune autre BPDU n'est transmise sur ce port jusqu'à ce que le compteur soit décrémenté à nouveau, quelle que soit l'importance de la BPDU pour la reconfiguration du réseau. La valeur maximale par défaut de TxHoldCount est de 6 et le numéro configurable maximal est de 10.

8.5.2.2 Bridge Max Age

Chaque pont RSTP comprend un paramètre Bridge Max Age qu'il convient de configurer à une valeur identique dans chacun des ponts. Bridge Max Age définit le nombre total maximal de “bonds physiques” ou de liaisons entre le pont racine et tour pont participant au même réseau RSTP. Sa valeur par défaut est de 20 et peut être configurée de 6 à une valeur maximale de 40. Dans certains cas particuliers, Bridge Max Age est configuré de manière différente dans certains ponts.

Etant donné que Bridge Max Age définit l'extension maximale d'un réseau RSTP, il est souvent appelé “diamètre du réseau”. Cependant, le terme “Bridge Max Age” et le diamètre du réseau réellement utilisable ne sont pas synonymes, voir 8.5.2.4.

8.5.2.3 Message Age

Chaque BPDU comprend un paramètre Message Age. A réception d'une BPDU, un pont incrémente Message Age puis le compare à son propre “Bridge Max Age”. Si le paramètre Message Age est supérieur à Bridge Max Age, le pont rejette la BPDU et ignore les informations qu'elle contient.

Le pont racine commence par envoyer des BPDU avec Message Age = 0. Le premier pont situé après le pont racine (ainsi que les ponts suivants jusqu'à ce que le paramètre Message Age atteigne Bridge Max Age) reçoit la BPDU, incrémente “Message Age” de 1, le compare au paramètre “Bridge Max Age” puis transmet les BPDU accompagnées des informations mises à jour.

8.5.2.4 Diamètre et rayon du réseau

Le “diamètre” du réseau RSTP est le nombre de ponts sur le chemin actif le plus long d'une arborescence réseau entre deux ponts les plus éloignés entre eux. Le diamètre ne correspond pas nécessairement au paramètre RSTP Bridge Max Age (voir Figure 23).

Le ”rayon” d'un réseau RSTP correspond au nombre de ponts à partir (et comprenant) du pont racine actif vers le pont le plus éloigné de cette racine active dans la topologie. Il s'agit de la longueur (en sauts) du chemin le plus long sur lequel il est nécessaire de transférer les informations du protocole RSTP (voir Figure 23). Le rayon maximum pris en charge par RSTP peut être défini comme:

rayon max. = Bridge Max Age + 1.

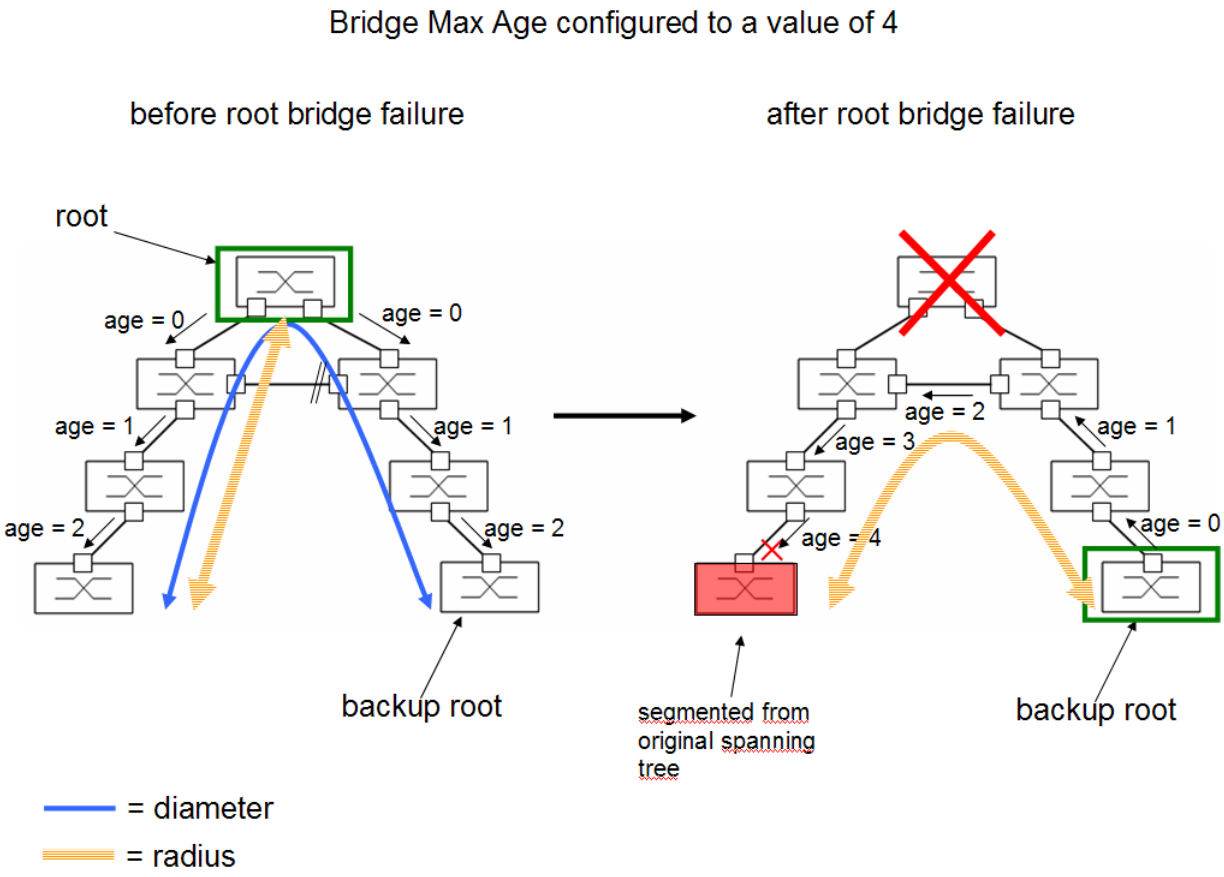
Le rayon est indispensable pour déterminer les topologies les plus défavorables. Dans des conditions de défaillance les plus défavorables (en l'absence d'un réseau technique et de ponts racines placés avec attention), en cas de défaillance d'un pont racine, la feuille la plus éloignée pourrait être le pont racine de secours, susceptible de devenir la racine suivante.

Copyright International Electrotechnical Commission

Dans ce cas, le diamètre du réseau peut devenir le rayon et devient le chemin réel que les informations RSTP doivent parcourir pour se rendre vers les ponts individuels. (Voir Figure 23)

NOTE Les BPDU RSTP sont uniquement transmises sur la liaison située entre deux ponts directement connectés. Chacun des ponts consomme et produit ces BPDU, mais les informations RSTP qu'ils transportent parcourent divers chemins à travers le réseau (dans un état de réseau stable et sans reconfiguration).

8.5.3 Exemple d'arborescence RSTP de petite taille



IEC 953/12

Légende

Anglais	Français
Bridge Max Age configured to a value of 4	Paramètre Bridge Max Age configuré sur une valeur de 4
Before root bridge failure	Avant la défaillance d'un pont racine
After root bridge failure	Après la défaillance d'un pont racine
Root	Racine
Backup root	Racine de secours
Age	Âge
Segmented from original spanning tree	Segmenté de l'arborescence d'origine
Diameter	Diamètre
Radius	Rayon

Figure 23 – Diamètre et Bridge Max Age

NOTE 1 La valeur de 4 a été attribuée au paramètre RSTP Bridge Max Age pour les besoins du présent exemple même si 802.1D ne permet pas une valeur inférieure à 6.

Copyright International Electrotechnical Commission

Dans l'exemple de la Figure 23, le réseau sans défaillance se trouve d'abord dans une condition stable avec Bridge Max Age = 4 et parce que le rayon réel est de 4 (la configuration RSTP pourrait supporter un rayon maximal de 5). Le diamètre est de 7, d'une feuille d'une branche à l'autre feuille située dans l'autre branche, via le pont racine. Etant donné que le pont racine est l'élément racine d'une arborescence équilibrée, Bridge Max Age = 4 suffit pour tous les ponts afin de recevoir les BPDU RSTP à partir de la même racine RSTP.

Une défaillance de pont racine et un choix de racine de secours défavorable changent ce processus. Après la défaillance d'un pont racine, la liaison redondante précédemment bloquée est activée. Le diamètre est désormais de 6. Parallèlement, le rayon est également augmenté pour atteindre 6. Etant donné que l'une des feuilles des branches d'origine est désormais devenue le pont racine, le paramètre Bridge Max Age de 4 ne suffit plus pour que les informations racines RSTP atteignent tous les ponts du réseau, car les informations RSTP doivent alors parcourir l'ensemble du diamètre, maintenant équivalent au rayon. Par conséquent, le dernier pont est segmenté, comme indiqué dans la Figure 23. Ce pont rejette la BPDU, car le paramètre Message Age a dépassé le paramètre configuré Bridge Max Age.

Pour concevoir des réseaux stables et haute performance, il est nécessaire d'observer et de comprendre la différence entre le diamètre du réseau et le rayon, respectivement le paramètre Bridge Max Age. Ce dernier est maintenu à une valeur aussi élevée que nécessaire afin de ne pas segmenter de dispositif dans le scénario de défaillance le plus défavorable et à une valeur la plus faible possible afin de réduire au maximum le temps de rétablissement du réseau tel que décrit dans les paragraphes suivants. Le rayon du réseau détermine la valeur Bridge Max Age nécessaire pour chacune des topologies considérées. Le paramètre Bridge Max Age peut être maintenu à une valeur faible en positionnant à la fois le pont racine et le pont racine de secours dans une position centrale au sein du réseau, par exemple sur l'anneau principal d'une topologie hiérarchique multi-anneaux.

NOTE 2 Une autre méthode, qui n'est pas traitée dans le présent document, consiste à configurer différentes valeurs Bridge Max Age sur le pont racine et sur le pont racine de secours, conformément à leurs positions respectives dans le réseau.

8.5.4 Hypothèse relative à TxHoldCount

Le calcul ou l'approximation d'un temps de reconfiguration de limite supérieure est effectué à partir de l'hypothèse selon laquelle le paramètre Transmit Hold Count (TxHoldCount) n'est jamais atteint et qu'aucune BPDU nécessaire à une reconfiguration rapide du réseau n'est perdue.

Ceci peut cependant se produire en pratique, notamment pendant la reconfiguration du réseau. Dès que le paramètre TxHoldCount d'un port de pont est “saturé”, aucun des ponts reliés au port saturé ne recevra plus de BPDU jusqu'à ce TxHoldCount ait été décrémenté. Si les BPDU rejetées sont essentielles à la reconfiguration du réseau, le temps de rétablissement du réseau peut être rallongé de plusieurs secondes. Cette hypothèse est d'une importance pratique majeure et est considérée comme la plus grande menace pour le temps de reconfiguration du réseau des réseaux RSTP.

8.5.5 Topologie la plus défavorable et détermination du rayon

Etant donné que le rayon le plus défavorable et le paramètre Bridge Max Age le plus faible possible sont corrélés, la détermination du rayon le plus défavorable est importante pour déterminer le temps de reconfiguration de limite supérieure le plus défavorable.

Dans un réseau maillé arbitrairement, les liaisons reconfigurées du réseau en régime établi après reconfiguration peuvent être prévues avant la défaillance, mais étant donné que le protocole est basé sur la réception et l'envoi de BPDU dans chaque pont individuel, des conditions de concurrence peuvent avoir lieu pendant la reconfiguration. Par conséquent, le temps de reconfiguration maximal ne peut être donné que comme une limite la plus défavorable basée sur le temps de réaction maximal de chaque pont et sur le nombre maximal de sauts autorisés par le protocole.

Copyright International Electrotechnical Commission

En outre, certains supports tels que 1000Tx présentent des temps de détection de défaillance de liaison importants. Ainsi, l'auto-négociation désactivée sur des liaisons à fibre Gigabit peut compromettre le temps de défaillance RSTP en cas de défaillance de liaison.

NOTE Des défaillances malveillantes, par exemple un pont incapable de transférer des trames de données utiles mais qui échange toujours des BPDU avec ses voisins, ne peuvent être prises en compte dans les calculs.

Lors de la conception d'un réseau fonctionnant avec RSTP, le rayon du réseau à partir de l'emplacement du pont racine et de l'emplacement de la racine de secours vers le pont de la feuille la plus éloignée doit être calculé.

Ce calcul de rayon tient également compte d'une défaillance la plus défavorable, car des défaillances de topologie peuvent augmenter le rayon. Par exemple, la Figure 24 illustre le pont racine et le pont racine de secours situés sur l'anneau principal. Le rayon le plus défavorable pour cette topologie spécifique est atteint par deux défaillances simultanées positionnées comme le montre Figure 24, et s'élève à 7 pour la racine indiquée.

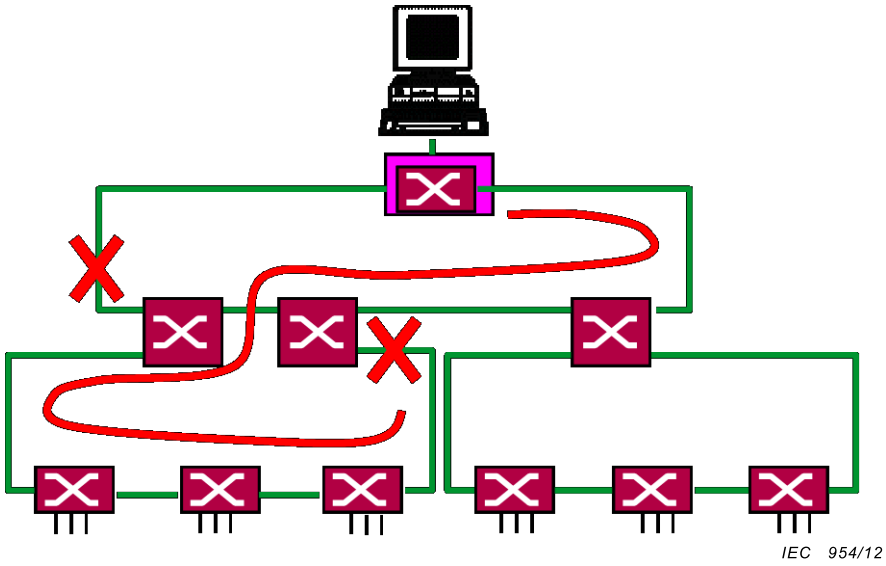


Figure 24 – Détermination du chemin le plus défavorable

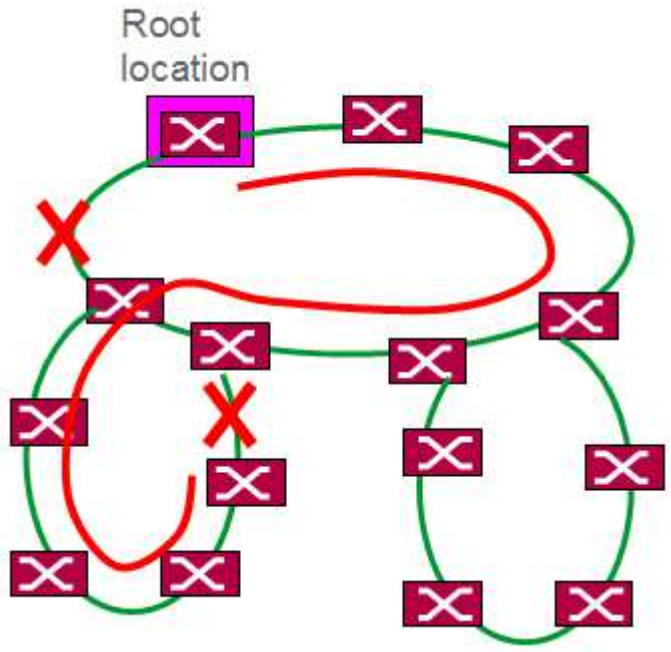
Une fois déterminée la valeur du rayon le plus défavorable pour un scénario de défaillance la plus défavorable dans la topologie de réseau, il convient de configurer Bridge Max Age précisément au nombre - 1. Ceci permet de réduire au maximum le temps de reconfiguration de limite supérieure du réseau, puisqu'un paramètre Bridge Max Age plus faible limite le temps de parcours des BPDU dans le réseau.

8.5.6 Méthode de détermination du rayon le plus défavorable en cas d'architecture anneau-anneau

Dans une topologie d'anneau à anneaux, l'anneau principal se compose de “N” ponts + 2 × “M” ponts qui relient “M” sous-anneaux de manière redondante, chacun étant composé de “R” ponts (à l'exception du pont utilisé pour relier à l'anneau principal).

La Figure 25 donne un exemple d'anneau principal (N = 3) doté de deux sous-anneaux (M = 2) reliés de manière redondante via un total de quatre ponts (deux par sous-anneau) à l'anneau principal, avec R = 4.

Copyright International Electrotechnical Commission



IEC 956/12

Légende

Anglais	Français
Root location	Emplacement de la racine

Figure 25 – Exemple de topologie anneau-anneau

Le pont racine et le pont racine de secours restent sur l'anneau principal (cette position est garantie en configurant la priorité RSTP de la racine et de la racine de secours sur l'anneau principal avec une valeur de priorité supérieure à tout autre pont dans les sous-anneaux).

Une seule défaillance au niveau de l'anneau principal et une défaillance au niveau du sous-anneau sont prises en compte. Le support simultané d'une défaillance sur l'anneau principal et d'une deuxième défaillance sur un sous-anneau est un cas limite.

Le rayon le plus défavorable (c'est-à-dire que le paramètre Bridge Max Age qui nécessite une configuration et qui est équivalent au rayon le plus défavorable - 1) est alors:

$$\text{rayon le plus défavorable} = N + 2 \times M + R$$

$$\text{Bridge Max Age} = (\text{rayon le plus défavorable} - 1) = N + 2 \times M + R - 1$$

où

“R” est le nombre de ponts dans le sous-anneau et possédant le plus grand nombre de dispositifs;

“N” est le nombre de ponts dans l'anneau principal (à l'exception des ponts qui relient les sous-anneaux);

“M” est le nombre de ponts sur l'anneau principal qui relient l'anneau principal aux sous-anneaux.

Dans le schéma ci-dessus, on tient compte de N=3, M=2, R=4, le rayon le plus défavorable étant = 11.

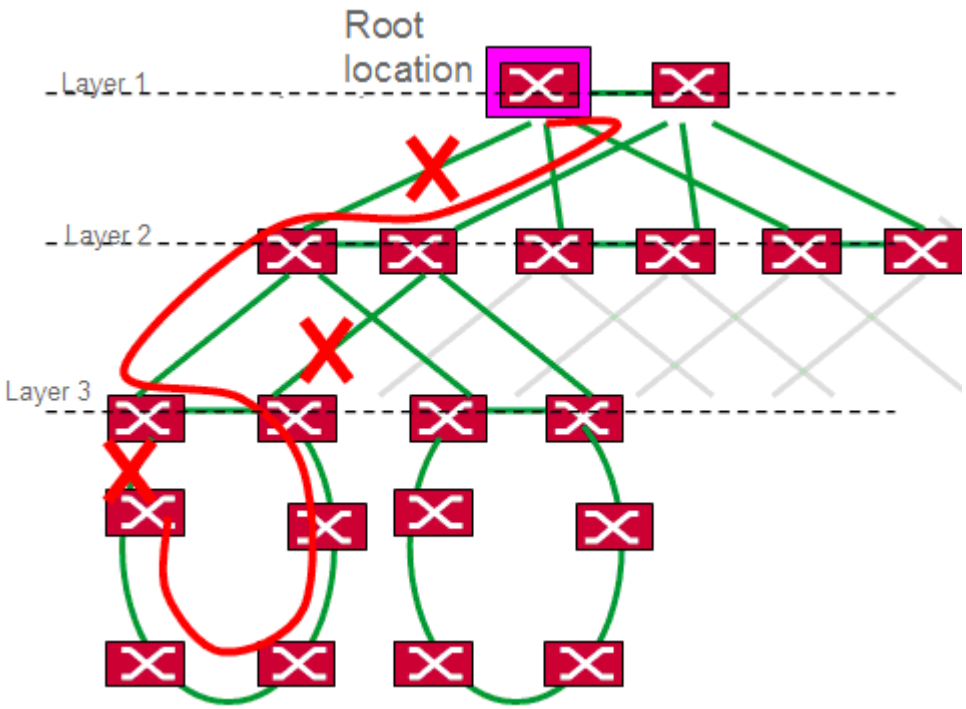
Par conséquent, il convient de configurer le paramètre de protocole RSTP “Bridge Max Age” à une valeur de 10 afin d'optimiser les temps de rétablissement du réseau.

Copyright International Electrotechnical Commission

8.5.7 Rayon le plus défavorable d'une architecture multicouche optimisée

Avec un grand nombre de ponts, il convient d'optimiser la topologie du réseau afin de ne pas atteindre la limite Bridge Max Age et de maintenir les temps de reconfiguration les plus défavorables à un niveau bas.

Une solution simple consiste à considérer une topologie multicouche, composée de “L” couches, comme illustré dans la Figure 26:



IEC 957/12

Légende

Anglais	Français
Root location	Emplacement de la racine
Layer	Couche

Figure 26 – Exemple de topologie multicouche

La couche supérieure est composée de 2 ponts principaux qui sont définis pour être les ponts racines/ponts racines de secours. (Il est prévu que la valeur de priorité de ces ponts soit définie en conséquence à la priorité la plus élevée et à la deuxième priorité la plus élevée).

La taille maximale de la couche 3 est définie par des sous-anneaux composés de “R” ponts. Le paramètre “R” exclut les ponts reliant le sous-anneau individuel de couche 3 à la couche 2, qui est intégré au calcul grâce au paramètre “L”.

Une seule défaillance par couche est prise en compte.

Le rayon le plus défavorable est alors égal à:

$$\text{rayon le plus défavorable} = (2 \times L) + R$$

Dans le schéma ci-dessus, L=3, R=4, et par conséquent le rayon le plus défavorable = 10. Ceci donne lieu à un paramètre Bridge Max Age de 9.

Copyright International Electrotechnical Commission

Le point d'intérêt est que ce résultat ne dépend pas du nombre de dérivations par couche, et cette topologie est éventuellement en mesure de prendre en charge un grand nombre de nœuds avec un faible paramètre Bridge Max Age. La limite est le nombre maximal de ports des ponts utilisés au niveau de chaque couche: Un grand nombre de ports physiques est préjudiciable aux performances RSTP sur les ponts.

8.5.8 Temps de reconfiguration approximatif de limite supérieure destiné aux réseaux RSTP

La défaillance du pont racine RSTP est le scénario le plus défavorable affectant le temps de reconfiguration. Le temps de reconfiguration de limite supérieure est le temps nécessaire au rétablissement après une défaillance du pont racine. Le temps de rétablissement des défaillances de liaisons ou des défaillances de ponts qui ne sont pas à la racine ne sera pas supérieur au temps de rétablissement d'une défaillance de pont racine. Etant donné qu'il s'agit du scénario le plus défavorable, le temps de rétablissement est par conséquent estimé pour une défaillance du pont racine.

Lorsque l'on considère le temps de reconfiguration du réseau d'un réseau RSTP maillé, trois phases distinctes peuvent être identifiées:

– Phase de vieillissement: Phase au cours de laquelle la défaillance du réseau est détectée et où de multiples informations racines (anciens et nouveaux vecteurs de priorité de racine) sont encore présentes au sein du réseau. Les anciennes informations racines peuvent encore circuler au sein du réseau jusqu'à ce que le paramètre Message Age des BPDU atteigne la valeur Bridge Max Age. Une fois l'ancien vecteur de priorité de racine issu du pont racine défectueux complètement éliminé du réseau seulement, le vecteur de priorité de racine de secours peut être prépondérant. La phase de vieillissement est ainsi le temps à partir de la défaillance jusqu'au moment où l'ancien vecteur de priorité BPDU racine est éliminé et, dans une situation la plus défavorable, lorsque tout autre nouveau vecteur racine temporaire inférieur atteint le pont racine de secours et déclenche la phase de convergence.

– Phase de convergence: La phase au cours de laquelle la racine de secours diffuse son nouveau vecteur racine au réseau et n'est plus perturbée par des informations de l'ancien vecteur racine. La phase de convergence débute immédiatement après la phase de vieillissement et se termine lorsque le pont le plus éloigné de la nouvelle racine de secours a reçu les informations de la nouvelle racine.

– Phase de vidange: Après la reconfiguration de la topologie active, plusieurs ponts peuvent vider leurs bases de données filtrantes pour s'assurer que les nouveaux chemins de communication sont correctement appris. RSTP utilise des BPDU de changement de topologie (TC) pour initier la vidange. Dans l'hypothèse du cas le plus défavorable, cette phase débute immédiatement après la phase de convergence et se termine lorsque la notification de changement de topologie à partir du pont le plus éloigné de la racine a atteint le pont racine.

NOTE Lors d'une défaillance de pont racine, souvent plus d'un pont revendique une racine. Cependant, lorsque la racine de secours présente la meilleure priorité restante, son vecteur de priorité est rapidement (une seule propagation de priorité au sein de la topologie) prépondérant par rapport aux ponts racines temporaires. Toutefois, en cas de scénario le plus défavorable, le meilleur vecteur de priorité issu de l'ancienne racine peut encore “circuler” plus longtemps. Par conséquent, il s'agit de l'élément limite qui définit la longueur de la phase de vieillissement.

Le temps total de reconfiguration de limite supérieure Trec d'un réseau RSTP maillé peut par conséquent être estimé sous la forme:

$$Trec = TL + Tage + Tconv + Tflush$$

où

Tage = 2 × Bridge Max Age × TPA;

Tconv = rayon le plus défavorable × TPA;

Tflush = rayon le plus défavorable × TTC;

Copyright International Electrotechnical Commission

TL est le temps maximal requis par un pont pour détecter une défaillance de liaison (dépend du type de liaison);

TPA est le temps maximal requis par une paire de ponts pour établir une liaison d'accord de proposition RSTP; égal à la somme des temps de traitement BPDU des deux ponts de la paire. Les valeurs TPA peuvent varier d'un fournisseur à un autre et d'un produit à un autre;

TTC est le temps nécessaire à un pont Ethernet pour traiter un changement de topologie RSTP.

Valeurs types d'une implémentation “RSTP rapide”:

TPA = 5 ms lorsque le fournisseur exige 5 ms/saut de temps de rétablissement

TL = 4-6 ms pour des liaisons 100BASE-TX et 100BASE-FX

= 20 ms pour des liaisons 1000BASE-X

= 700 ms pour des liaisons 1000BASE-T (définies par l'ISO/IEC 8802-3)

Cette approximation montre qu'il est avantageux pour le temps total de rétablissement de définir le paramètre Bridge Max Age à une valeur aussi élevée que nécessaire pour prendre en charge la topologie donnée (par rapport aux éventuelles défaillances), mais aussi faible que possible afin de réduire au maximum son impact sur le temps de rétablissement du réseau.

Cette approximation du temps de rétablissement couvre le scénario le plus défavorable, à savoir la défaillance du pont racine. En comparant la probabilité d'une défaillance du pont racine à la probabilité d'une défaillance d'un pont qui ne se trouve pas à la racine ou d'une liaison, une défaillance du pont racine est nettement moins probable (si l'on suppose des probabilités de défaillance similaires pour tous les dispositifs et supports participant) car pour chaque pont racine, un grand nombre de connexions de support et de ponts non-racines peut présenter une défaillance avant.

Par conséquent, le temps de rétablissement type sera plus rapide que le temps de rétablissement du cas le plus défavorable susceptible d'être estimé par le présent article, mais ceci ne peut être pris en compte.

NOTE On peut assister à une conséquence supplémentaire lorsqu'un pont doté de plusieurs ports connectés au réseau RSTP fait partie de la topologie active (en particulier lorsque ce dispositif est la racine), à savoir que l'envoi de BPDU sur les multiples ports n'est pas totalement simultané. Ce phénomène peut être d'autant plus compliqué si différents supports sont présents sur ces multiples ports. Le temps de reconfiguration peut alors être rallongé par cet effet.

Copyright International Electrotechnical Commission

Bibliographie

IEC 61158 (toutes les parties), *Réseaux de communication industriels – Spécifications des bus de terrain*

IEC/TR 61158-1, *Industrial communication networks – Fieldbus specifications – Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series (disponible en anglais seulement)*

IEC/TR 61158-6 (all parts), *Industrial communication networks – Fieldbus specifications – Part 6: Symmetrical pair/quad cables with transmission characteristics up to 1 000 MHz – Work area wiring (disponible en anglais seulement)*

IEC 61588, *Precision clock synchronization protocol for networked measurement and control systems*

IEC 61784-2:2007, *Réseaux de communication industriels – Profils – Partie 2: Profils de bus de terrain complémentaires pour les réseaux en temps réel selon l'ISO/IEC 8802-3*

IEC 61918:2007, *Industrial communication networks – Installation of communication networks in industrial premises*

IEC 62439-2, *Réseaux industriels de communication – Réseaux de haute disponibilité pour l'automation – Partie 2: Protocole de redondance du support (MRP)*

IEC 62439-3, *Réseaux de communication industriels – Réseaux d'automatisme à haute disponibilité – Partie 3: Protocole de redondance parallèle (PRP) et redondance transparente de haute disponibilité (HSR)*

IEC 62439-4, *Réseaux de communication industriels – Réseaux d'automatisme à haute disponibilité – Partie 4: Protocole de Redondance à réseau Croisé (CRP)*

IEC 62439-5, *Réseaux de communication industriels – Réseaux d'automatisme à haute disponibilité – Partie 5: Protocole de redondance à balise (BRP)*

IEC 62439-6, *Réseaux industriels de communication – Réseaux de haute disponibilité pour l'automation – Partie 6: Protocole de redondance distribuée (DRP)*

IEC 62439-7, *Réseaux de communication industriels – Réseaux de haute disponibilité pour l'automation – Partie 7: Protocole de redondance pour réseau en anneau (RRP)*

ISO/IEC 2382 (toutes les parties), *Technologies de l'information – Vocabulaire*

ISO/IEC 9646 (toutes les parties), *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Cadre général et méthodologie des tests de conformité*

ISO/IEC 10731, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Modèle de référence de base – Conventions pour la définition des services OSI*

ISO/IEC 11801:2002, *Technologies de l'information – Câblage générique des locaux d'utilisateurs*
Amendement 1 (2008)

ISO/IEC 15802-3, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseaux locaux et métropolitains – Spécifications communes – Partie 3: Ponts du Contrôle d'accès au support*

Copyright International Electrotechnical Commission

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

PUSTYLNIK M., ZAFIROVIC-VUKOTIC, M., MOORE, R., *Performance of the Rapid Spanning Tree Protocol in Ring Network Topology, Rugged Com. Inc.*
http://www.ruggedcom.com/pdfs/white_%20papers/performance_of_rapid_spanning_tree_protocol_in_ring_network_topology.pdf

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

IEC 62439-1

Edition 1.2 2016-02

FINAL VERSION

VERSION FINALE

colour inside

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

IEC 62439-1:2010-02+AMD1:2012-06+AMD2:2016-02 CSV(en-fr)
Copyright International Electrotechnical Commission

CONTENTS

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

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.

This Final version does not show where the technical content is modified by amendments 1 and 2. A separate Redline version with all changes highlighted is available in this publication.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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>

Copyright International Electrotechnical Commission

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]

Copyright International Electrotechnical Commission

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 IEV 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]

Copyright International Electrotechnical Commission

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 + Δt) 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.

Copyright International Electrotechnical Commission

[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.

Copyright International Electrotechnical Commission

[IEC 61784-2, 3.1.14]

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.

Copyright International Electrotechnical Commission

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 IEV 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]

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

[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

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

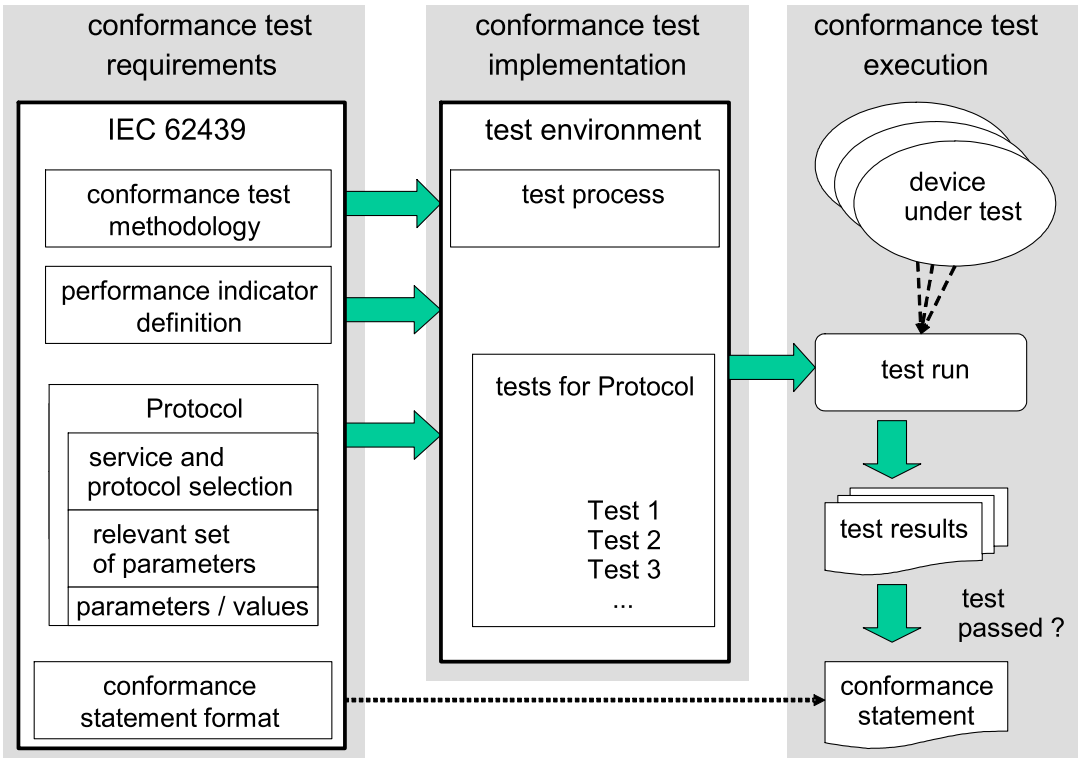


Figure 1 – Conformance test overview

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;

Copyright International Electrotechnical Commission

- 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.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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	8,88 ms worst case for 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.

Copyright International Electrotechnical Commission

5.2 Generic network system

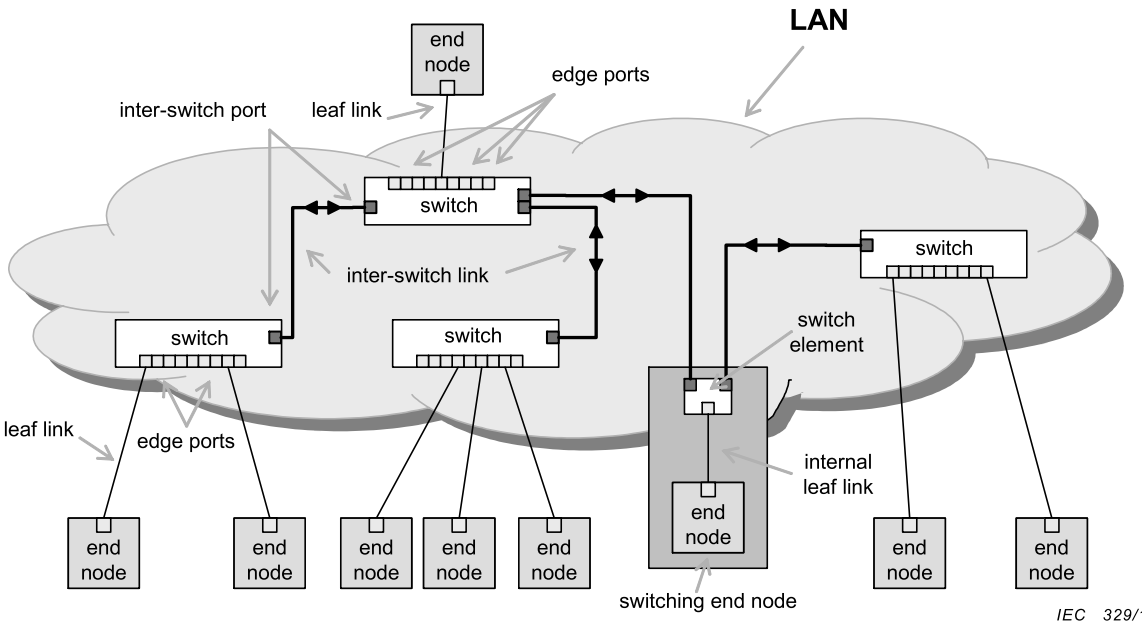
5.2.1 Network elements

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.

Copyright International Electrotechnical Commission

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.

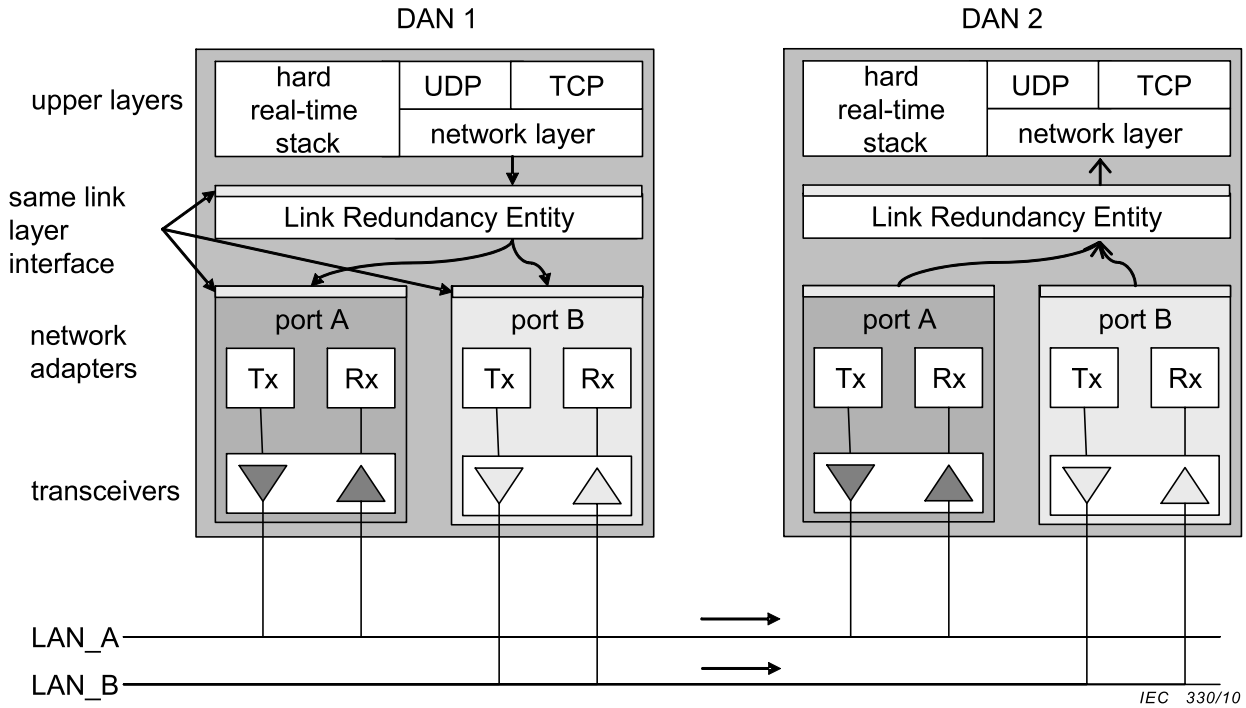


Figure 3 – Link Redundancy Entity in a Doubly Attached Node (DAN)

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).

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

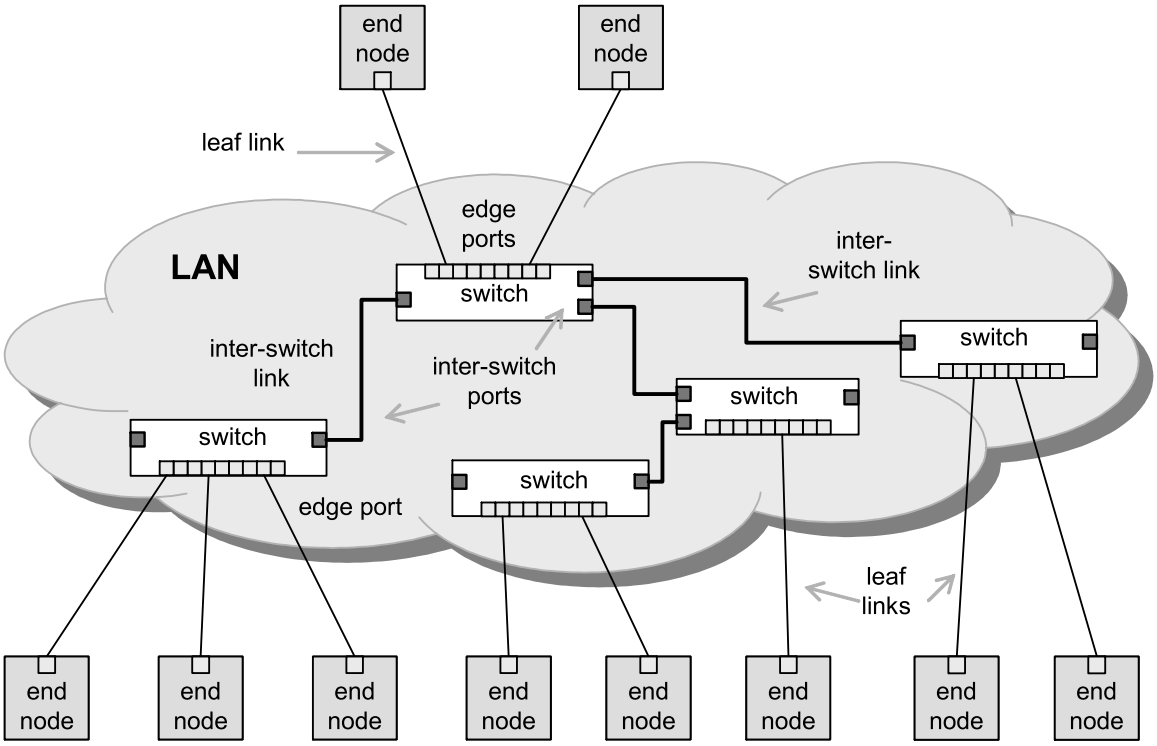


Figure 4 – Example of tree topology

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.

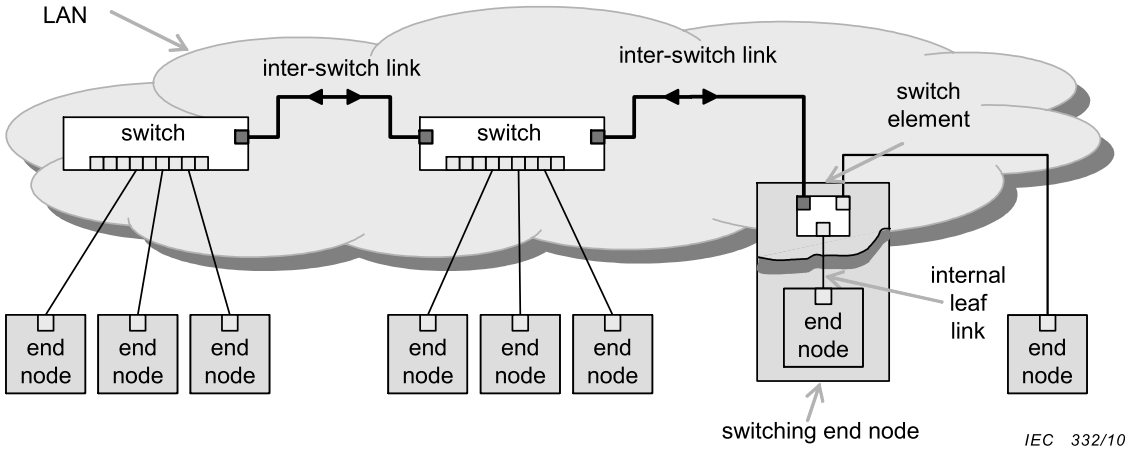


Figure 5 – Example of linear topology

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.

Copyright International Electrotechnical Commission

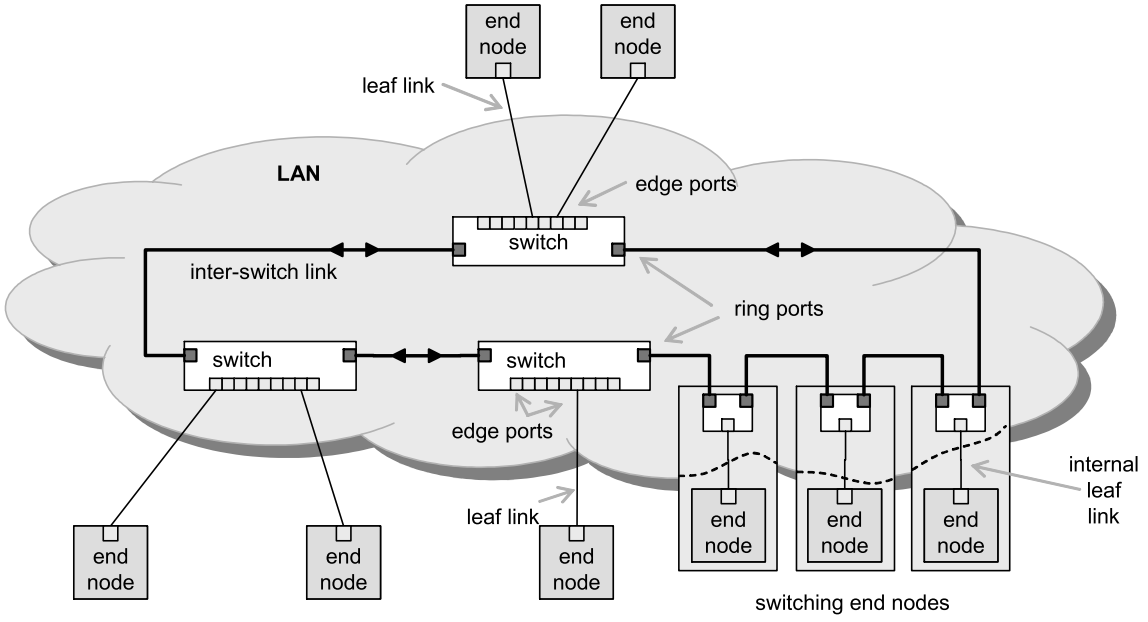


Figure 6 – Example of ring topology

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.

Copyright International Electrotechnical Commission

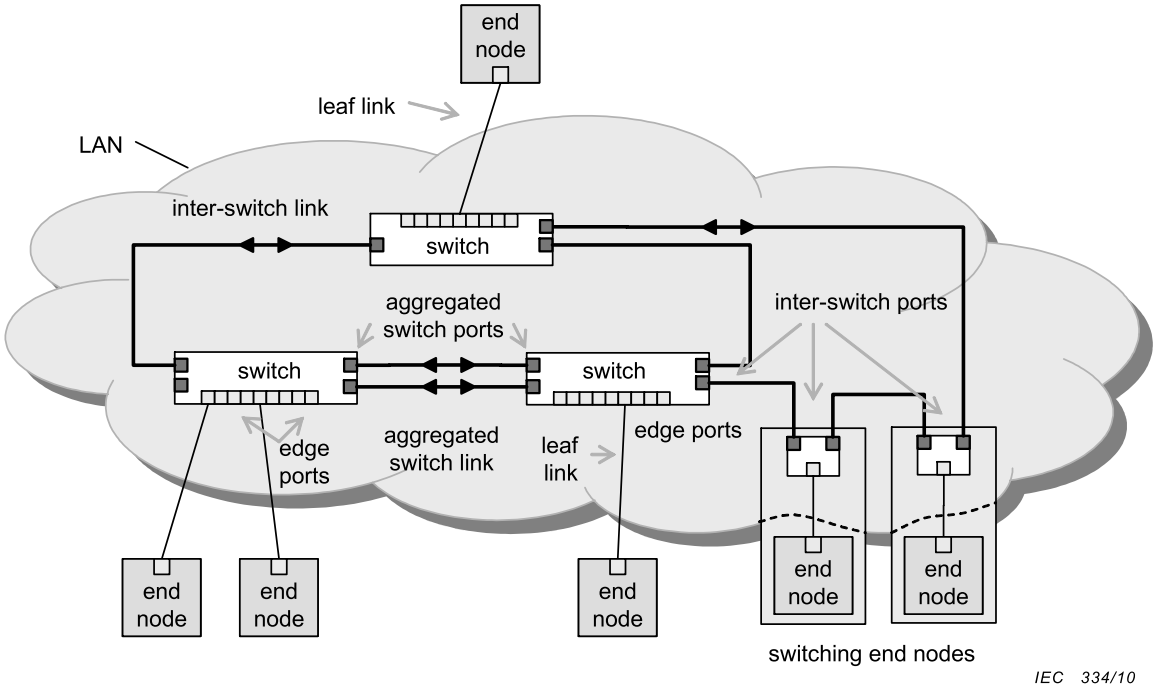


Figure 7 – Example of a partially meshed topology

5.2.2.3.3 Fully meshed topology

In a fully meshed topology, every switch has more than two inter-switch links.

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.

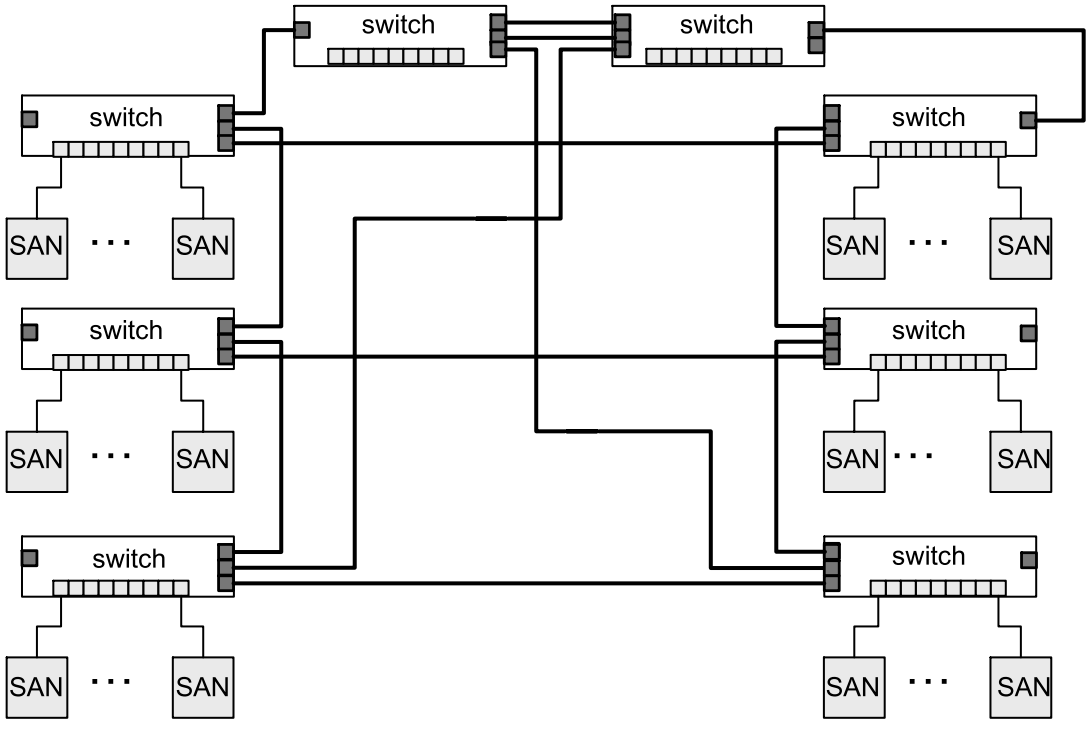


Figure 8 – Example of fully meshed topology

Copyright International Electrotechnical Commission

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).

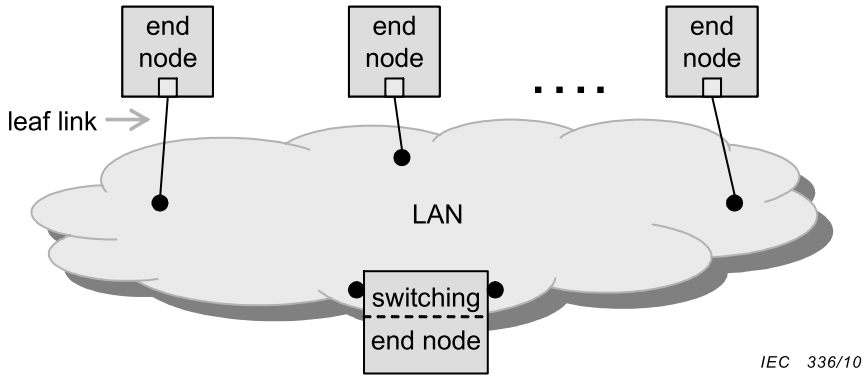


Figure 9 – Single LAN structure without redundant leaf links

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.

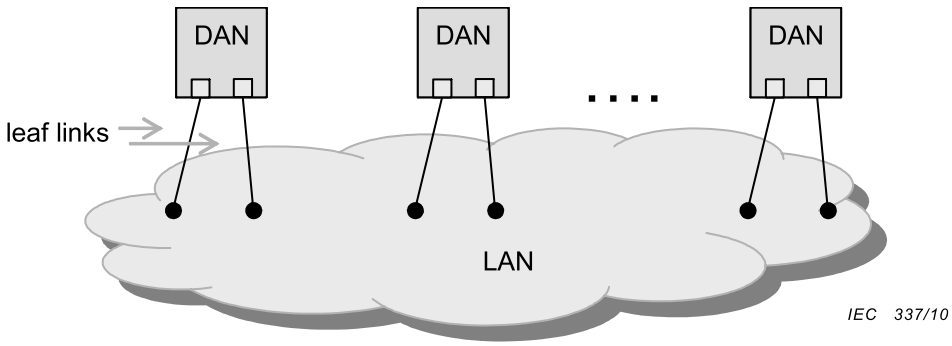


Figure 10 – Single LAN structure with redundant leaf links

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.

Copyright International Electrotechnical Commission

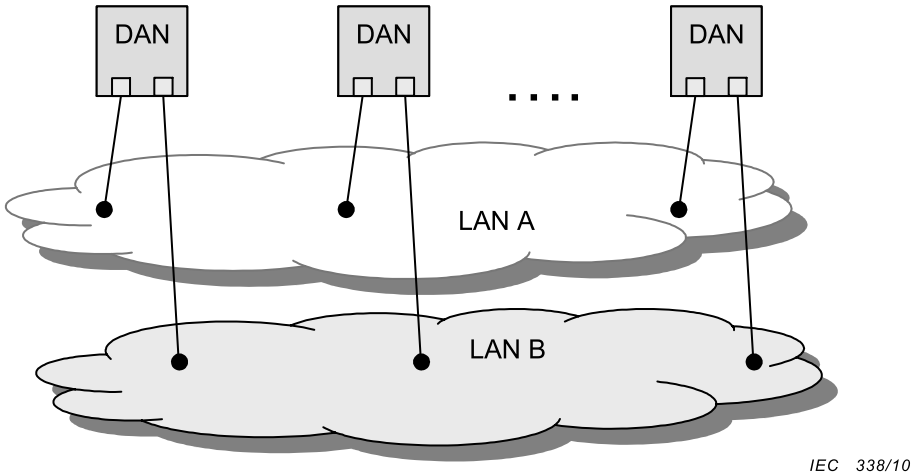


Figure 11 – Redundant LAN structure without redundant leaf links

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.

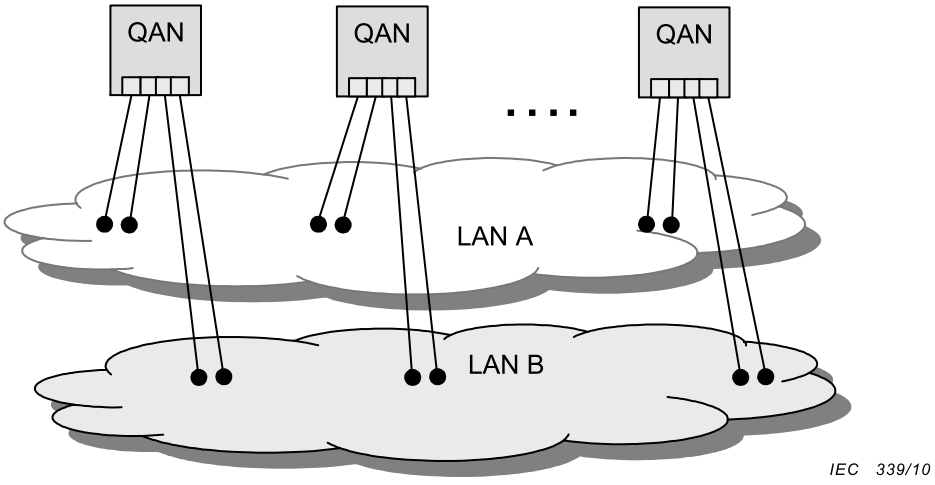


Figure 12 – Redundant LAN structure with redundant leaf links

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 IEV 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.

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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

Copyright International Electrotechnical Commission

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;

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

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:

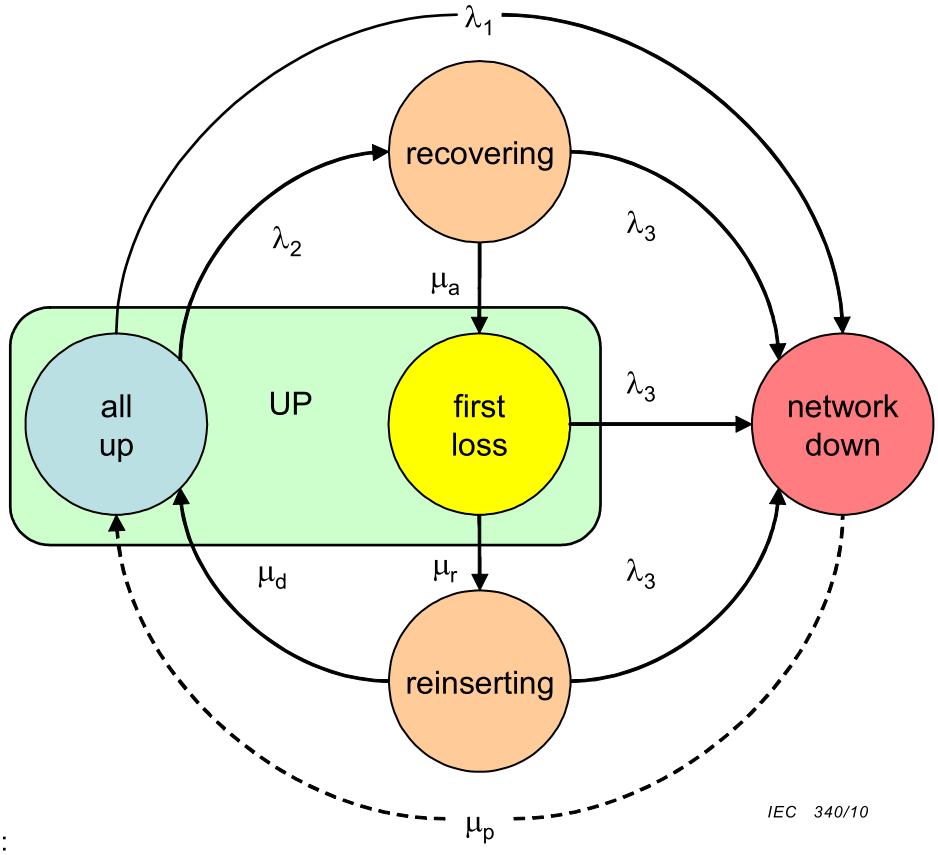
$$\lambda_S = 1 / \text{MTTFswitch} = 1/100 \text{ years}$$

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

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)

Copyright International Electrotechnical Commission

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.

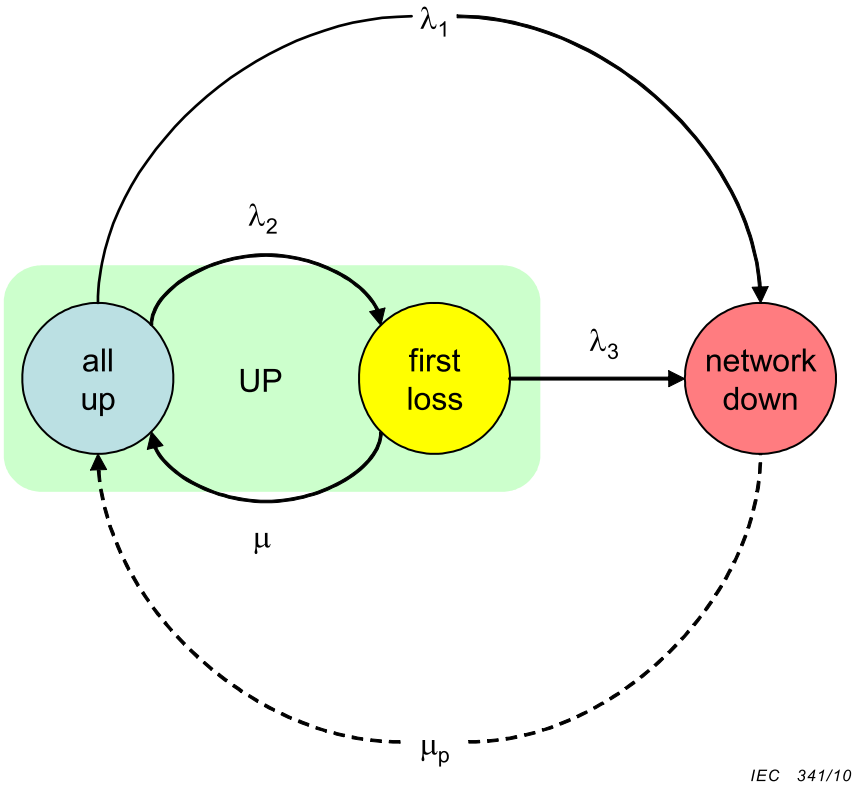


Figure 14 – Simplified fault model

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

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

Copyright International Electrotechnical Commission

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.

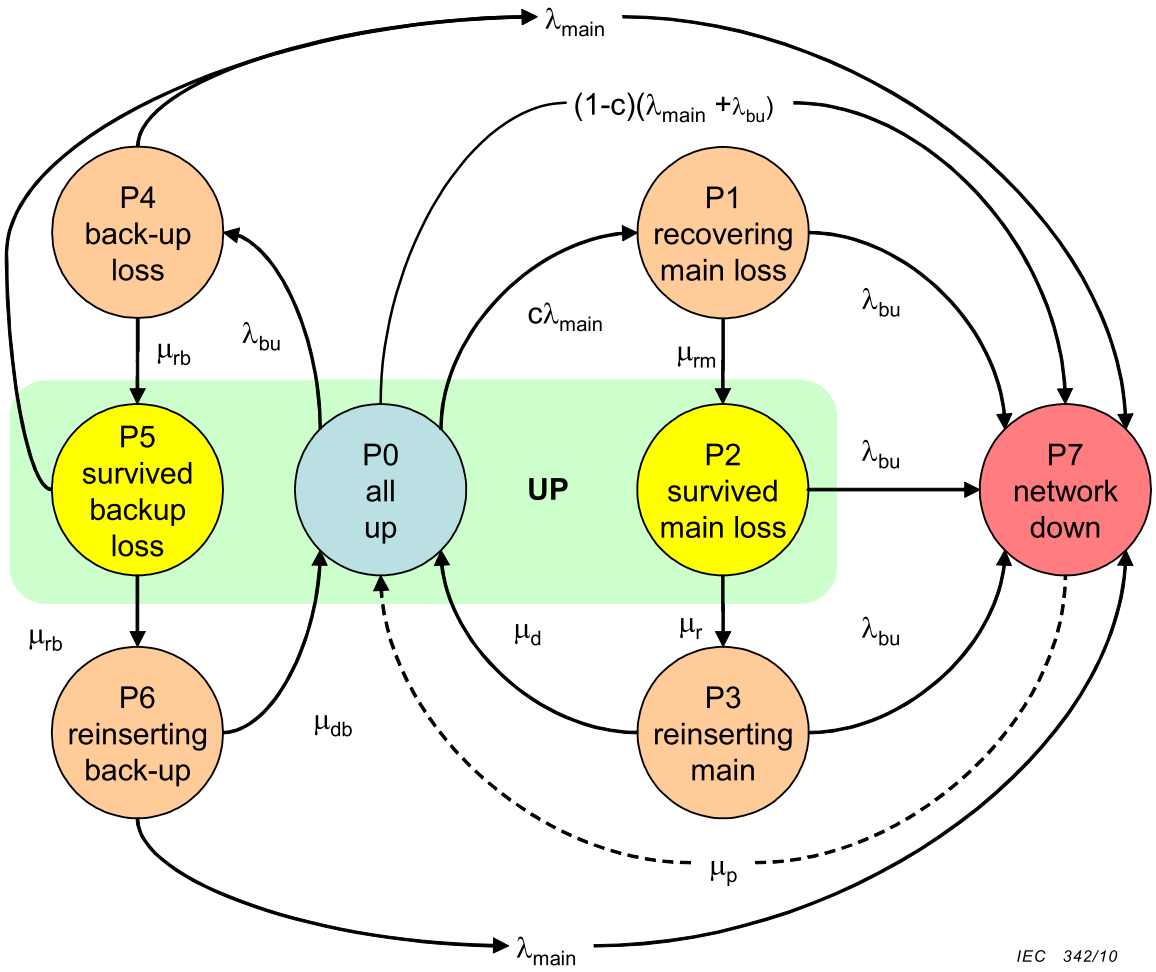


Figure 15 – Asymmetric fault model

Copyright International Electrotechnical Commission

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.

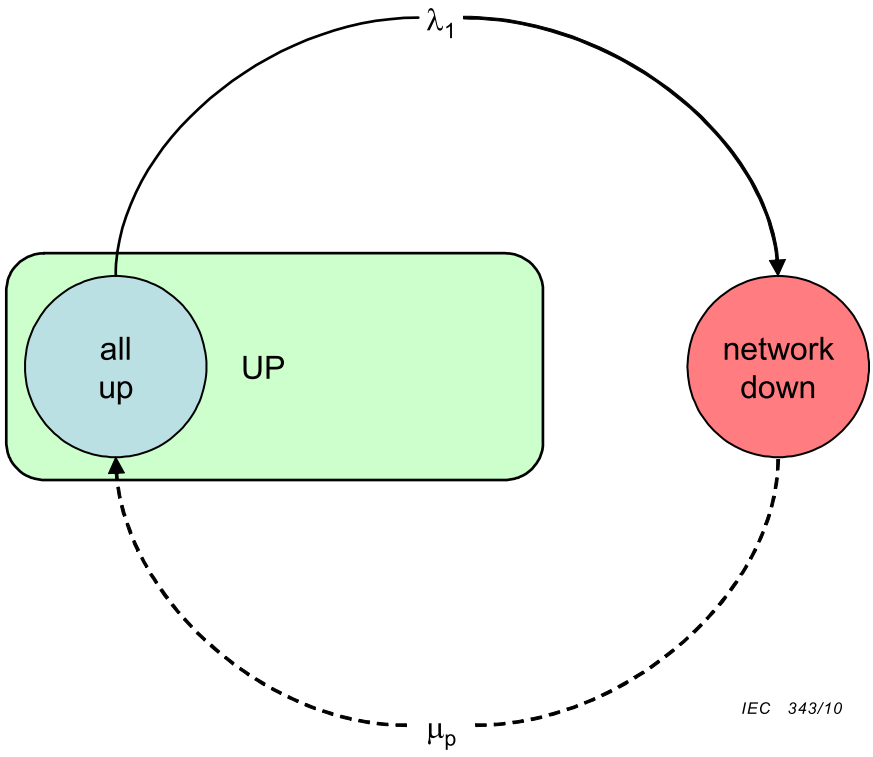


Figure 16 – Network with no redundancy

Therefore, the MTTFN simplifies into Equation (3).

$$\text{MTTFN} = \frac{1}{\lambda_1} \tag{3}$$

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

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):

Copyright International Electrotechnical Commission

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

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.

Copyright International Electrotechnical Commission

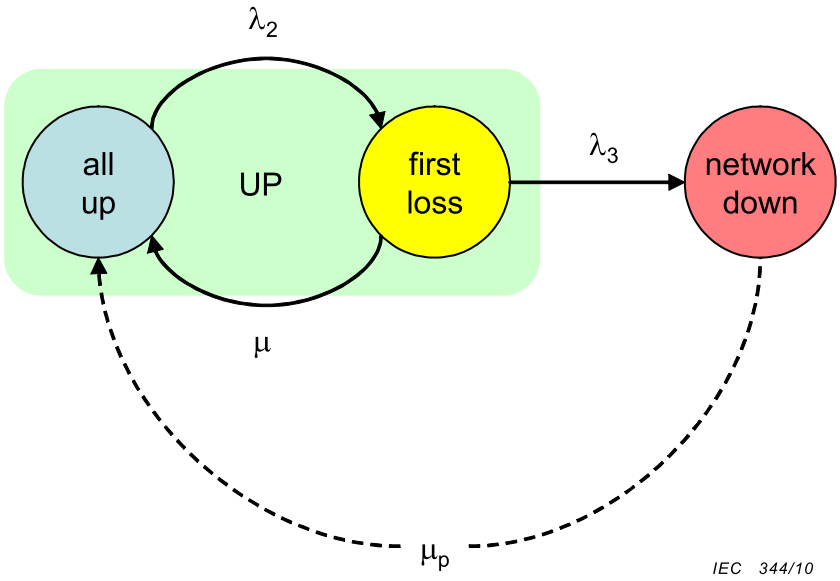


Figure 17 – Network with no single point of failure

The MTTFN simplifies to Equation (5):

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

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 MTTFS 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.

Copyright International Electrotechnical Commission

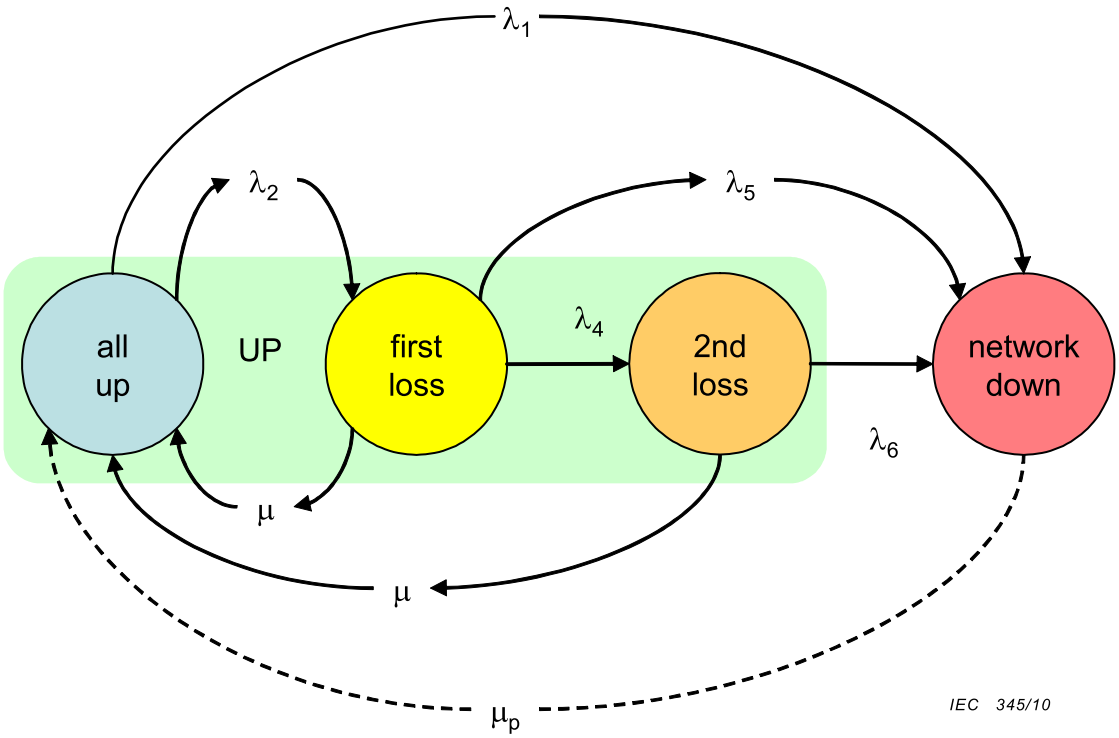


Figure 18 – Network with resiliency to second failure

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).

$$MTTFN = \frac{(\mu + \lambda_2 + \lambda_4 + \lambda_5) + \frac{\lambda_2 \lambda_4}{\mu + \lambda_6}}{\lambda_1(\mu + \lambda_4 + \lambda_5) + \lambda_2\left(\lambda_5 + \lambda_4\left(\frac{1}{1 + \frac{\mu}{\lambda_6}}\right)\right)} \quad \mu >> \sum(\lambda_i) \quad \approx \quad \frac{1}{\lambda_1 + \frac{\lambda_2^2 f}{\mu}} \tag{6}$$

Copyright International Electrotechnical Commission

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 λ_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 predictible recovery time

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:

Copyright International Electrotechnical Commission

- 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:

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

Copyright International Electrotechnical Commission

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.

Copyright International Electrotechnical Commission

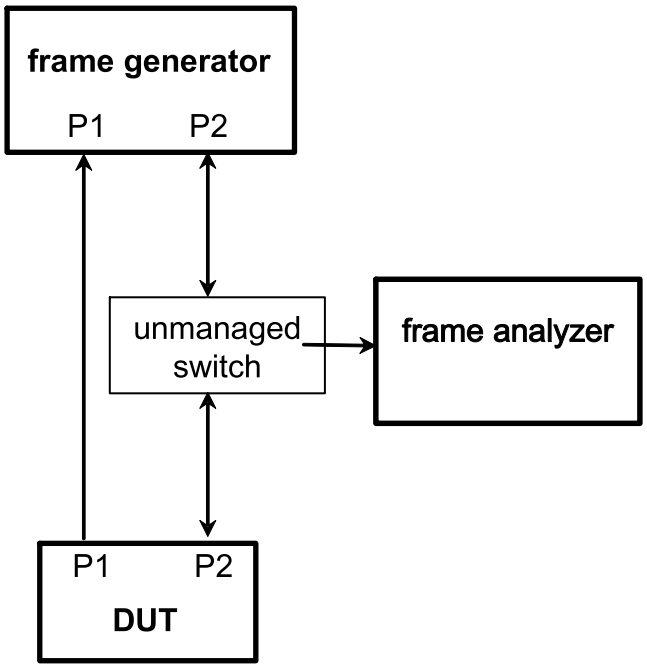


Figure 19 –Test rig for T_{PA} measurement

b) Configure DUT so that the connected ports ‘AdminEdge’ and ‘AutoEdge’ parameters are set to FALSE.

c) Configure the frame generator’s Port2 to send a Proposal BPDU (i.e. with the “proposal” flag set and “root bridge ID” better than DUT’s).

d) Configure frame generator’s Port1 only to maintain an Ethernet link but not to send any frames. This port will simulate another RSTP switch to which the DUT will propagate a proposal.

e) Configure the frame analyzer to capture frames received from the unmanaged switch.

8.4.1.3 Procedure

The procedure is as follows:

a) verify that DUT has elected itself as “root”.

b) start capturing frames in frame analyzer.

c) transmit a single BPDU from frame generator.

d) stop capturing frames.

e) verify that DUT sent “agreement” BPDU in response to the “proposal” BPDU.

f) measure the time interval between the “proposal” BvPDU and the first “agreement” BPDU.

8.4.2 Measurement of T_L

8.4.2.1 Measurement

This test is actually measuring (T_L + T_{Proc}) time. Given that T_{Proc} has been measured by the previous test, T_L is deduced from (T_L + T_{Proc}).

8.4.2.2 Setup

Configure the system as follows:

a) build the network as shown in Figure 20.

Copyright International Electrotechnical Commission

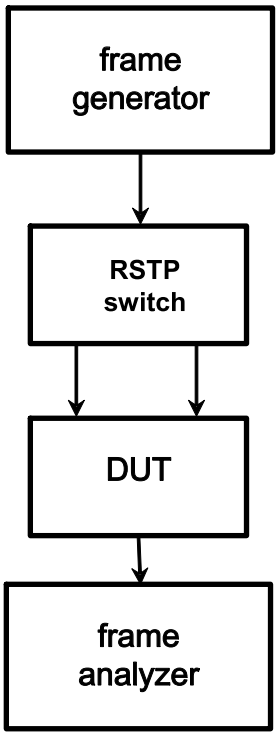


Figure 20 –Test rig for T_L measurement

b) set the RSTP switch “Bridge priority” parameter to 0 to force it to be the elected “root”.

c) configure the frame generator to send a continuous stream of arbitrary frames at a rate of at least 4 000 frames-per-second to allow time measurement resolution of 0,25 ms.

d) configure the frame analyzer to capture frames received from DUT.

8.4.2.3 Procedure

The procedure is as follows:

a) verify that the RSTP switch has been elected “root”.

b) verify that one of the DUT ports has a “root forwarding” status and the other port has an “alternate discarding” status.

c) start transmitting from the frame generator.

d) start capturing frames.

e) verify that frames are received by the frame analyzer.

f) break the link attached to the DUT’s “root” port. This will cause DUT to failover to its “alternate” port.

g) verify that frames are received by the frame analyzer.

h) stop capturing frames.

i) measure for how long frame receiving was disrupted.

8.4.3 Measurement of (T_{TC} + T_F)

8.4.3.1 Setup

Configure the test rig as follows:

a) build the test network as shown in Figure 21.

Copyright International Electrotechnical Commission

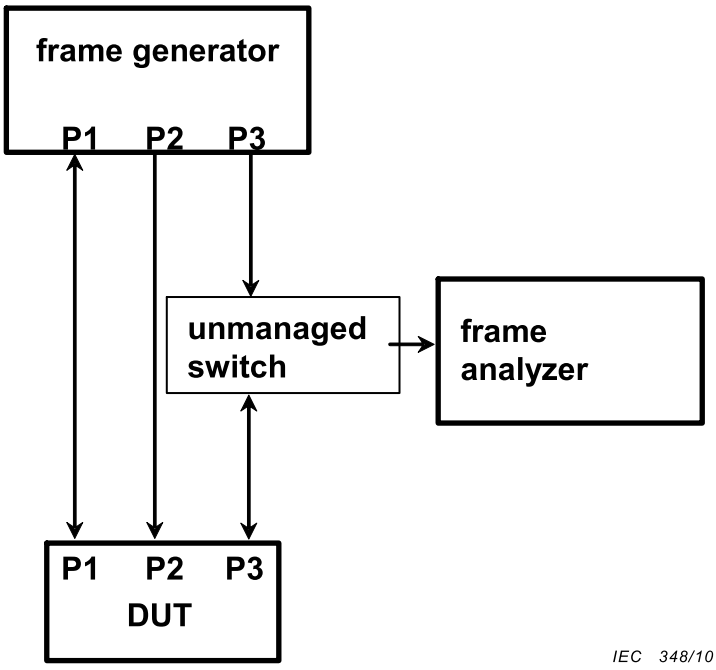


Figure 21 –Test rig for (T_{TC} + T_F) measurement

b) set DUT's Port1 and Port3 'AutoEdge' and 'AdminEdge' parameters to FALSE.

c) set DUT's Port2 'AutoEdge' parameter to FALSE and 'AdminEdge' parameter to TRUE.

d) configure the frame generator's Port1 to send a single arbitrary frame.

e) configure the frame generator's Port2 to send a continuous stream of frames to the destination MAC address of Port2 at a rate of at least 4 000 frames-per-second to allow time measurement resolution of 0,25 ms.

f) configure the frame generator's Port3 to send a single "agreement + topology change" BPDU.

g) configure the frame analyzer to capture frames received from the unmanaged switch.

8.4.3.2 Procedure

The procedure is as follows:

a) verify that DUT has elected itself as "root".

b) transmit a single frame out of the frame generator's Port1. This will make that DUT's Port1 learns the frame source MAC address.

c) start transmitting a continuous stream out of the frame generator's Port2.

d) start capturing frames in the frame analyzer.

e) verify that the stream is not forwarded out of DUT's Port3 (it is only forwarded out of DUT's Port1).

f) send a single BPDU from the frame generator's Port3. This will cause the DUT to flash its MAC address table and start flooding the traffic stream out of Port3 so it will be captured by the frame analyzer.

g) stop capturing frames.

h) verify that the DUT started flooding out of Port3 in response to the "topology change" BPDU.

i) measure the time interval between the "topology change" BPDU and the first stream frame.

j) repeat a) … i) for 10 different randomly chosen values of the source MAC address used by the frame generator's Port1 (and thus the destination MAC address used by the frame generator's Port2) and chose the maximum value among all measurements.

Copyright International Electrotechnical Commission

8.4.4 System test example

8.4.4.1 Setup

Configure the system as follows:

a) build a switch ring of 20-40 switches which comply with the IEEE 802.1D:2004 RSTP specification as shown in Figure 22.

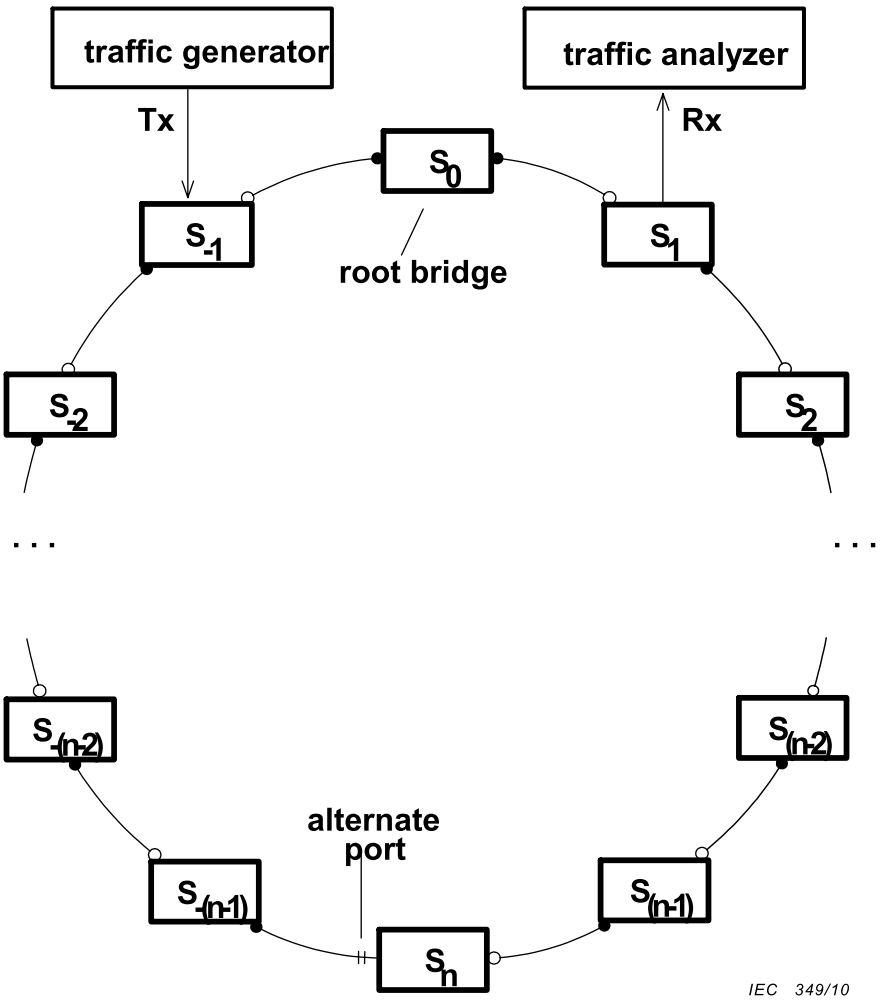


Figure 22 –Test rig for system test

b) ensure that all links comply with the deployment requirements specified in 8.2.

c) configure the traffic generator to send frames destined to the Rx port's MAC address out of its Tx port. Transmission rate should be chosen high enough so that a fault recovery time could be calculated based on a number of lost packets with a millisecond resolution.

d) configure the traffic generator to send low rate (e.g. once in a few seconds) arbitrary frames out of its Rx port with the Rx port's source MAC address (so that switches would learn it).

e) configure the traffic analyzer to display Tx and Rx frame counters.

f) set all switches RSTP parameters to default values. Verify that all switches have their "bridge priority" set to 32 768.

g) set switch S_0 "bridge priority" to 0, so that S_0 will be elected a root switch.

h) set switch S_1 "bridge priority" to 4 096, so that S_1 will be the next best root candidate after S_0.

Copyright International Electrotechnical Commission

8.4.4.2 Procedure

The procedure is as follows:

a) verify that alternate port is on the S_n switch, S_n–$S_{-(n-1)}$ link.

b) start transmitting low rate dummy frames out of traffic Rx port. Verify that switches S_{-1}, S_0 and S_1 learned the Rx port's MAC address.

c) start transmitting frames out of the Tx port. Verify that the Rx counter is incrementing along with the Tx counter and no traffic is lost.

d) break the S_0–S_1 link.

e) verify that the Rx counter is incrementing (i.e. connectivity has recovered).

f) stop transmitting out of the Tx port.

g) read the Tx and Rx counters and calculate number of lost frames.

h) calculate the fault recovery time using formula t = (number of lost frames) / (frame rate).

8.5 RSTP topology limits and maximum recovery time

NOTE In the next edition of IEC 62439-1, this new Subclause 8.5 will be renumbered as 8.2.

8.5.1 RSTP protocol parameters

This subclause explains the RSTP protocol parameters that impact network recovery times and shows how a specific topology and protocol configuration influence them. First, RSTP-specific terms are defined. Then, basic guidelines on network design are given and finally a method to determine an approximation of an upper bond worst case network reconfiguration time for meshed RSTP networks is given.

This subclause particularly deals with RSTP networks that are composed of more than a single ring. For a single Ethernet ring running RSTP, the network reconfiguration time can be determined as 8.2 shows. However, the subsequent statements concerning RSTP parameters are also applicable in a ring network.

8.5.2 RSTP-specific terms and definitions

NOTE These terms are inherited from IEEE 802.1D.

8.5.2.1 Transmission Hold Count (TxHoldCount)

Each port of an RSTP bridge includes a counter TxHoldCount. This counter starts at zero and is incremented for each BPDU the port sends. A timer decrements every second the counter. If TxHoldCount reaches the maximum value, no further BPDU are transmitted over that port until the counter has been decremented again, regardless of the importance of the BPDU to network reconfiguration. The default maximum value of TxHoldCount is 6 and the maximum configurable number is 10.

8.5.2.2 Bridge Max Age

Each RSTP bridge includes a parameter Bridge Max Age that should be configured to the same value in each bridge. Bridge Max Age defines the maximum total number of "physical hops" or links between the root bridge and any bridge participating in the same RSTP network. Its default value is 20 and it can be configured to from 6 to a maximum of 40. In special cases, Bridge Max Age is configured differently in some bridges.

Because Bridge Max Age defines the maximum extension of an RSTP network, it is sometimes referred to as "network diameter". But "Bridge Max Age" and the actually usable network diameter are not synonymous, see 8.5.2.4.

Copyright International Electrotechnical Commission

8.5.2.3 Message Age

Each BPDU includes a parameter Message Age. Upon reception of a BPDU, a bridge increments Message Age and afterwards compares it to its “Bridge Max Age”. If Message Age is larger than Bridge Max Age, the bridge discards the BPDU and ignores the information it carries.

The root bridge starts by sending BPDUs with Message Age = 0. The first bridge after the root bridge (and subsequent bridges until Message Age reaches Bridge Max Age) receives the BPDU, increment “Message Age” by 1, compares it to the “Bridge Max Age” and transmit BPDUs with the updated information.

8.5.2.4 Network diameter and radius

The “diameter” in an RSTP network is the number of bridges on the longest active path in a network tree between the two bridges that are the farthest away from each other. The diameter does not necessarily correspond to the RSTP parameter Bridge Max Age (see Figure 23).

The ”radius” in a RSTP network is the number of bridges from (and including) the active root bridge to the bridge that is the farthest away from this active root in the topology. This is the length (in hops) of the longuest path over which the RSTP protocol information needs to be forwarded (see Figure 23). The maximum supported radius by RSTP can be defined as:

max. radius = Bridge Max Age + 1.

The radius is important to determine worst case topologies. In a worst case fault situation (without an engineered network and consciously placed root bridges), upon failure of a root bridge, the farthest away leaf might be the backup root bridge, which might become the next root. In this case, the diameter of the network can become the radius and it becomes the actual path that the RSTP information to the individual bridges has to travel. (See Figure 23)

NOTE RSTP BPDUs are only transmitted on the link between two directly connected bridges. Each bridge consumes and produces these BPDUs, but the RSTP information which they carry travels distinct paths through the network (in a stable network state without reconfiguration).

Copyright International Electrotechnical Commission

8.5.3 Example of a small RSTP tree

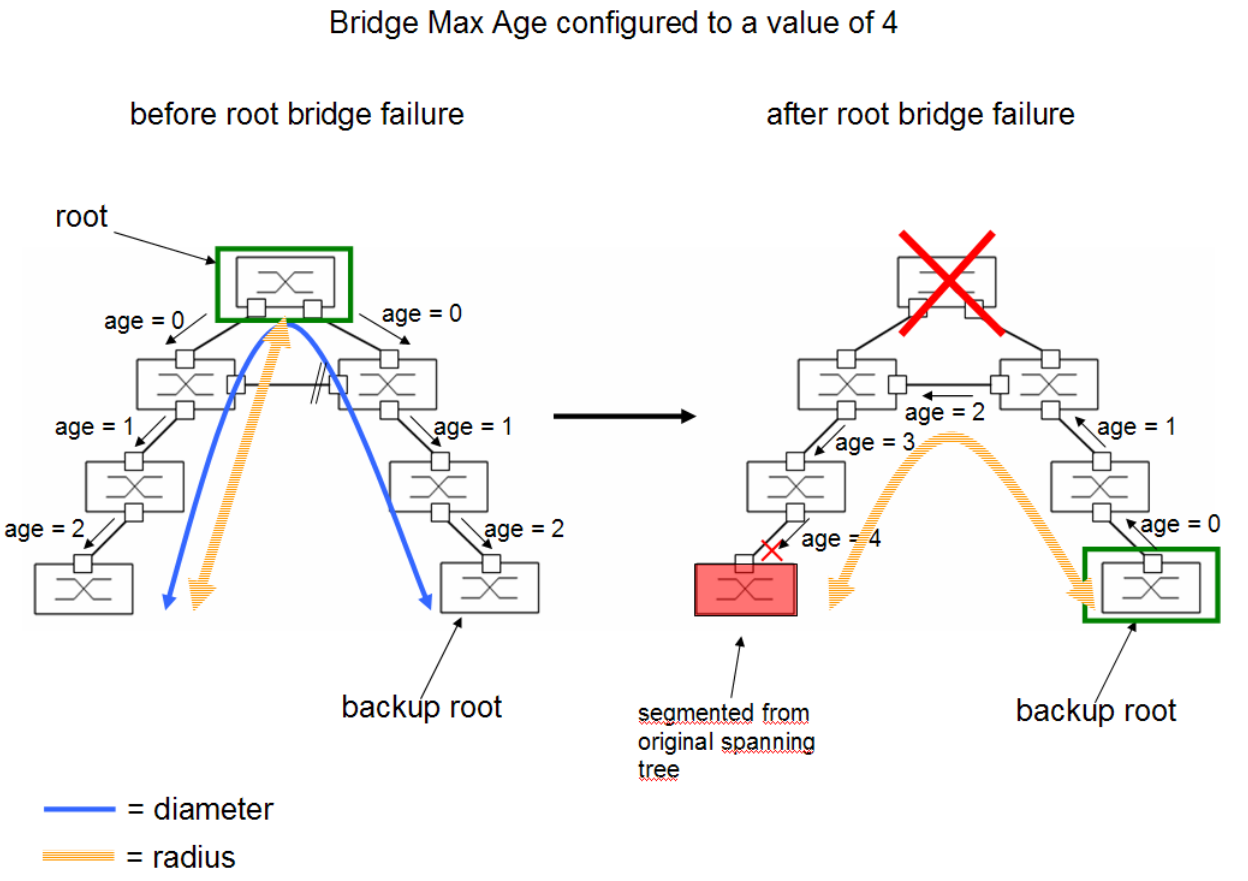


Figure 23 – Diameter and Bridge Max Age

NOTE 1 The RSTP parameter Bridge Max Age has been assigned the value 4 for the sake of this example although 802.1D does not allow a value lower than 6.

In the example of Figure 23, at first, the network without a failure is in a stable condition with Bridge Max Age = 4 and because the actual radius is 4 (the RSTP configuration could support a maximum radius of 5). The diameter is 7, from one leaf in one branch to the other leaf in the other branch, via the root bridge. Because the root bridge is the root element of a balanced tree, Bridge Max Age = 4 is sufficient for all bridges to receive RSTP BPDUs from the same RSTP root.

A root bridge failure and an unfavorable backup root election changes that. After a root bridge failure, the redundant link that was formerly blocked is activated. The diameter is now 6. At the same time, the radius is also increased to 6. Because one of the leaves of the original branches has now become the root bridge, the Bridge Max Age of 4 is not sufficient for the RSTP root information to reach all bridges of the network, because the RSTP information now has to travel the whole diameter, which is now equivalent to the radius. Thus, the last bridge is segmented, as indicated in Figure 23. This bridge discards the BPDU, because the Message Age has exceeded the configured Bridge Max Age.

To engineer stable and high performance networks, it is necessary to observe and understand the difference between the network diameter and the radius, respectively the Bridge Max Age parameter. The Bridge Max Age parameter is kept as high as necessary not to segment any device in a worst case fault scenario and as low as possible to minimize the network recovery time as shown in the following subclauses. The network radius determines the necessary Bridge Max Age value for each considered topology. The Bridge Max Age can be kept low by

Copyright International Electrotechnical Commission

positionning both root bridge and backup root bridge at a central position in the network, e.g. on the main ring of a hierarchical multi-ring topology.

NOTE 2 Another method, which is not covered in this document, is to configure different Bridge Max Age values on root and backup root bridge, according to their respective positions in the network.

8.5.4 Assumption on TxHoldCount

Calculation or approximation of an upper bond reconfiguration time is made under the assumption that the Transmit Hold Count (TxHoldCount) is never reached and no BPDU necessary for fast reconfiguration of the network is lost.

This however can occur in practice, especially during network reconfiguration. As soon as the TxHoldCount of one bridge port becomes “saturated”, all bridges connected to the saturated port won’t receive any BPDUs any more until the TxHoldCount has been decremented. If the dropped BPDUs are vital for network reconfiguration, the network reconfiguration time can be extended by several seconds. This assumption is of high practical relevance and is considered as the biggest threat to the network reconfiguration time of RSTP networks.

8.5.5 Worst case topology and radius determination

Because the worst case radius and the lowest possible Bridge Max Age parameter are correlated, determining the worst case radius is important in determining the upper bond worst case reconfiguration time.

In an arbitrarily meshed network, the reconfigured links of the network in steady state after reconfiguration can be predicted prior to the failure, but as the protocol is based on reception and sending BPDUs in each individual bridge, race conditions can occur during reconfiguration. Therefore the maximum reconfiguration time can only be given as a worst case bound based on the maximum reaction time of each bridge and the maximum number of hops allowed by the protocol.

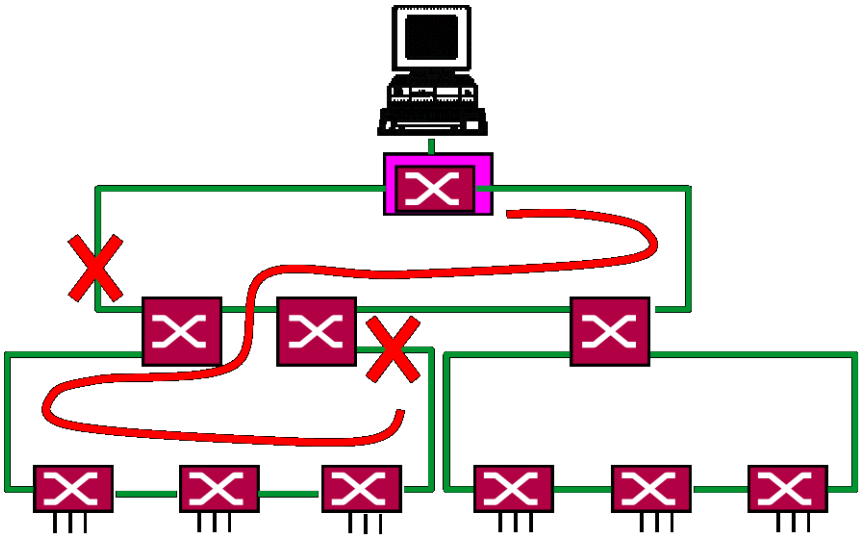
In addition, some media such as 1000Tx present large link failure detection times. Indeed, auto-negotiation disabled on fiber Gigabit links may jeopardize RSTP failover time in case of link failure.

NOTE Malicious failures such as a bridge unable to forward payload frames but still exchanging BPDUs with its neighbors cannot be considered in the calculations.

When designing a network that operates with RSTP, the network radius from the root-bridge location and from the backup root location to the farthest away leaf bridge has to be calculated.

This radius calculation also considers a worst case failure, because failures in the topology can increase the radius. As an example, Figure 24 shows the root bridge and the backup root bridge located on the main ring. The worst case radius for this specific topology is reached by two simultaneous failures positioned as Figure 24 shows, which is 7 for the indicated root.

Copyright International Electrotechnical Commission



IEC 954/12

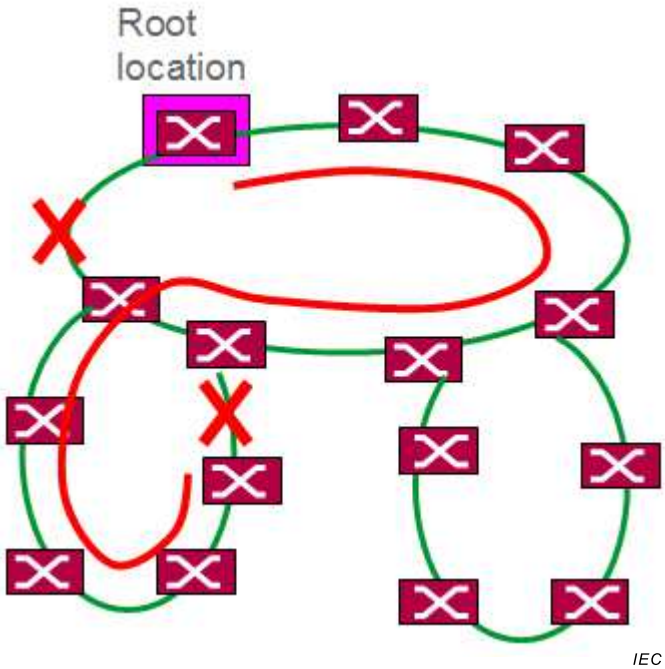
Figure 24 – Worst path determination

Once the worst case radius value for a worst case failure scenario in the network topology has been determined, Bridge Max Age should be configured to exactly this number - 1. This minimizes the upper bond reconfiguration time of the network, since a lower Bridge Max Age limits the time that BPDUs circulate in the network.

8.5.6 Method to determine the worst case radius in case of a ring-ring architecture

In a ring of rings topology, the main ring is made of “N” bridges + 2 × “M” bridges that connect “M” sub-rings redundantly, each made of “R” bridges (excluding the bridge to connect on the main ring).

Figure 25 shows an example of a main ring (N = 3) with two sub-rings (M = 2) connected redundantly via a total of four bridges (two per sub-ring) to the main ring, with R = 4.



IEC 955/12

Figure 25 – Example ring-ring topology

Copyright International Electrotechnical Commission

Root bridge and backup root bridge remain on the main ring (this is ensured by configuring the RSTP priority of root and backup root on the main ring with a better priority value than any other bridge in the sub-rings).

Only one failure at the main ring and one failure at the sub-ring are considered. Sustaining one failure in the main ring and simultaneously a second failure in a sub-ring is a corner case.

Then the worst case radius (i.e. the Bridge Max Age that needs to be configured which is equivalent to the worst case radius - 1) is:

$$\text{worst case radius} = N + 2 \times M + R$$

$$\text{Bridge Max Age} = (\text{worst case radius} - 1) = N + 2 \times M + R - 1$$

where

“R” is the number of bridges in the sub-ring with the highest number of devices;

“N” is the number of bridges in the main ring (excluding the bridges that connect the sub-rings);

“M” is the number of bridges in the main ring that connect the main ring to the sub-rings.

In the diagram above, considering that N=3, M=2, R=4, the worst case radius = 11.

Thus, the RSTP protocol parameter “Bridge Max Age” should be configured to a value of 10 to optimize network recovery times.

8.5.7 Worst case radius of an optimized multilayer architecture

With a large number of bridges, the network topology should be optimized in order not to reach the Bridge Max Age limit and to keep worst case reconfiguration times low.

A simple solution is to consider a multilayer topology, consisting of “L” layers, as shown in Figure 26:

Copyright International Electrotechnical Commission

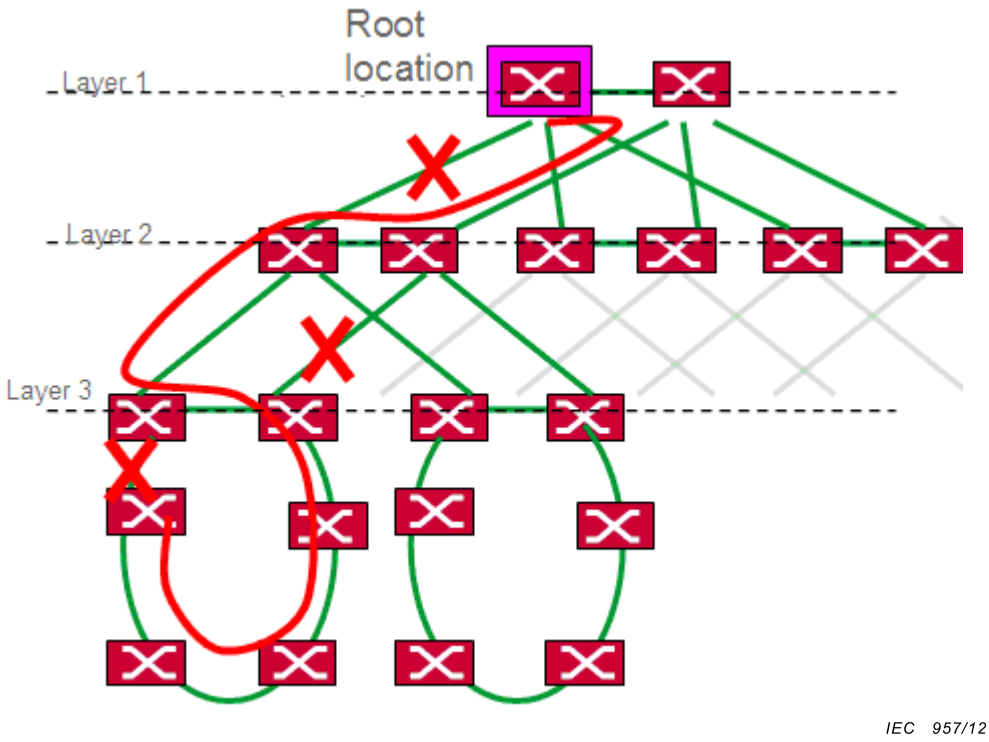


Figure 26 – Example multilayer topology

The upper layer is made of 2 main bridges which are set to be the root/backup root bridges. (Priority value of these bridges is expected to be set consequently to the highest and second to highest priority).

The maximum size of layer 3 is defined by sub-rings made of “R” bridges. The parameter “R” excludes the bridges that connect the individual layer 3 subring to layer 2, which is taken into the calculation through the parameter “L”.

Only one failure per layer is considered.

Then the worst case radius is equal to:

$$\text{worst case radius} = (2 \times L) + R$$

In the above diagram, L=3, R=4, and therefore, worst case radius = 10. This results in a Bridge Max Age parameter of 9.

The interesting point is that this result is not dependant on the number of branch-offs per layers, and this topology is possibly able to support a large number of nodes with a low Bridge Max Age parameter. The limitation is the maximum number of ports of the bridges used at each layer: A large number of physical ports is detrimental to RSTP performance on bridges.

8.5.8 Approximated upper bond reconfiguration time for RSTP networks

The RSTP root bridge failure is the worst case scenario aftecting reconfiguration time. The upper bond reconfiguration time is the time needed for recovery after a root bridge failure. The recovery time for link failures or non-root bridge failures will not exceed the root bridge failure recovery time. Since it is the worst case scenario, the recovery time subsequently is estimated for a root bridge failure.

Copyright International Electrotechnical Commission

When considering the network reconfiguration time of a meshed RSTP network, three distinct phases can be identified:

– Aging phase: The phase in which the fault in the network is detected and in which multiple root information (old and new root priority vectors) are still present in the network. The old root information can still circulate around in the network until the Message Age in the BPDUs reaches the Bridge Max Age value. Only after the old root priority vector from the failed root bridge has been completely eliminated from the network, can the backup root priority vector prevail. The aging phase is therefore the time from the fault to the moment, when the old root BPDU priority vector is eliminated and, in a worst case situation, any other, inferior new temporary root vector reaches the backup root bridge and triggers the converging phase.

– Converging phase: The phase in which the backup root broadcasts its new root vector to the network and is no longer disturbed by old root vector information. The converging phase immediately starts after the aging phase and ends when the bridge farthest away from the new backup root has received the new root information.

– Flushing phase: After the reconfiguration of the active topology, several bridges could flush their filtering databases to make certain that the new communication paths are learned properly. RSTP uses Topology Change (TC) BPDUs to initiate flushing. With a worst case assumption, this phase begins immediately after the converging phase and ends after the Topology Change notification from the bridge farthest away from the root has reached the root bridge.

NOTE When a root bridge fails, usually more than one bridge claims root. But as the backup root has the best remaining priority, its priority vector quickly (one single priority propagation through the topology) prevails against the other temporary root bridges. But in a worst case scenario, the better priority vector from the old root may still “circulate” around much longer. This is, therefore, the limiting element that defines the length of the aging phase.

The total upper bond reconfiguration time Trec of a meshed RSTP network can therefore be approximated as:

$$Trec = TL + Tage + Tconv + Tflush$$

where:

Tage = 2 × Bridge Max Age × TPA;

Tconv = worst case radius × TPA;

Tflush = worst case radius × TTC;

TL is the maximum time required by a bridge to detect a link failure (depends on the link type);

TPA is the maximum time required by a pair of bridges to perform RSTP Proposal Agreement handshaking; equal to the sum of the BPDU processing times in both bridges of the pair. TPA values may differ from vendor to vendor and from product to product;

TTC is the time an Ethernet bridge needs to process an RSTP topology change.

Typical values for “fast RSTP” implementation:

TPA = 5 ms when the vendor claims a 5 ms/hop recovery time

TL = 4-6 ms for 100BASE-TX and 100BASE-FX links

= 20 ms for 1000BASE-X links

= 700 ms for 1000BASE-T links (defined by the ISO/IEC 8802-3)

Copyright International Electrotechnical Commission

This approximation shows that it is beneficial for the total recovery time to set the Bridge Max Age parameter as high as necessary to support the given topology (with respect to possible failures), but as low as possible to minimize its impact on the network recovery time.

This approximation of recovery time covers the worst case scenario, the root bridge failure. When comparing the likeliness of a root bridge failure to the likeliness of a non-root or link failure, a root bridge failure is far more unlikely (when similar failure probabilities for all participating devices and media are assumed) because for each root bridge there is a large number of media connections and non-root bridges that may fail before.

Therefore, the typical recovery time will be faster than the worst case recovery time that can be approximated by this clause, but this cannot be counted on.

NOTE There may be an additional effect when a bridge with multiple ports connected to the RSTP network is becoming a part of the active topology (especially when this device is elected root), that the sending of BPDUs on the multiple ports is not totally simultaneous. This may be complicated further with different media on these multiple ports. The reconfiguration time may be stretched by this effect.

Copyright International Electrotechnical Commission

Bibliography

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

IEC/TR 61158-1, *Industrial communication networks – Fieldbus specifications – Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series*

IEC/TR 61158-6 (all parts), *Industrial communication networks – Fieldbus specifications – Part 6: Symmetrical pair/quad cables with transmission characteristics up to 1 000 MHz – Work area wiring*

IEC 61588, *Precision clock synchronization protocol for networked measurement and control systems*

IEC 61784-2:2007, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*

IEC 61918:2007, *Industrial communication networks – Installation of communication networks in industrial premises*

IEC 62439-2, *Industrial communication networks – High availability automation networks – Part 2: Media Redundancy Protocol (MRP)*

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

IEC 62439-4, *Industrial communication networks – High availability automation networks – Part 4: Cross-network Redundancy Protocol (CRP)*

IEC 62439-5, *Industrial communication networks – High availability automation networks – Part 5: Beacon Redundancy Protocol (BRP)*

IEC 62439-6, *Industrial communication networks – High availability automation networks – Part 6: Distributed Redundancy Protocol (DRP)*

IEC 62439-7, *Industrial communication networks – High availability automation networks – Part 7: Ring-based Redundancy Protocol (RRP)*

ISO/IEC 2382 (all parts), *Information technology – Vocabulary*

ISO/IEC 9646 (all parts), *Information technology – Open Systems Interconnection – Conformance testing methodology and framework*

ISO/IEC 10731, *Information technology – Open Systems Interconnection – Basic Reference Model – Conventions for the definition of OSI services*

ISO/IEC 11801:2002, *Information technology – Generic cabling for customer premises*
Amendment 1 (2008)

ISO/IEC 15802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Common specifications – Part 3 : Media Access Control (MAC) Bridges*

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

Copyright International Electrotechnical Commission

PUSTYLNIK M., ZAFIROVIC-VUKOTIC, M., MOORE, R., *Performance of the Rapid Spanning Tree Protocol in Ring Network Topology, Rugged Com. Inc.*
http://www.ruggedcom.com/pdfs/white_%20papers/performance_of_rapid_spanning_tree_protocol_in_ring_network_topology.pdf

_____

Copyright International Electrotechnical Commission

SOMMAIRE

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX INDUSTRIELS DE COMMUNICATION – RÉSEAUX D'AUTOMATISME À HAUTE DISPONIBILITÉ–

Partie 1: Concepts généraux et méthodes de calcul

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.

2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.

3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.

4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.

5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.

6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.

7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.

8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.

9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

DÉGAGEMENT DE RESPONSABILITÉ
Cette version consolidée n'est pas une Norme IEC officielle, elle a été préparée par commodité pour l'utilisateur. Seules les versions courantes de cette norme et de son(ses) amendement(s) doivent être considérées comme les documents officiels.

Cette version consolidée de l'IEC 62439-1 porte le numéro d'édition 1.2. Elle comprend la première édition (2010-02) [documents 65C/583/FDIS et 65C/589/RVD], son amendement 1 (2012-06) [documents 65C/684/FDIS et 65C/691/RVD] et son amendement 2 (2016-02) [documents 65C/834/FDIS et 65C/841/RVD]. Le contenu technique est identique à celui de l'édition de base et à ses amendements.

Copyright International Electrotechnical Commission

Cette version Finale ne montre pas les modifications apportées au contenu technique par les amendements 1 et 2. Une version Redline montrant toutes les modifications est disponible dans cette publication.

La Norme internationale IEC 62439-1 a été établie par le sous-comité 65C: Réseaux industriels, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'IEC 62439 (2008):

– ajout d'une méthode de calcul pour le protocole RSTP (Rapid Spanning Tree Protocol, IEEE 802.1Q),
– ajout de deux nouveaux protocoles de redondance: HSR (High-availability Seamless Redundancy) et DRP (Distributed Redundancy Protocol),
– déplacement des Articles 1 à 4 (Introduction, Définitions, Aspects généraux) et des Annexes (taxinomie, calcul de disponibilité) dans l'IEC 62439-1, qui servent à présent de base aux autres documents,
– déplacement de l'Article 5 (MRP) dans l'IEC 62439-2 avec peu de modifications éditoriales,
– déplacement de l'Article 6 (PRP) dans l'IEC 62439-3 avec peu de modifications éditoriales,
– déplacement de l'Article 7 (CRP) dans l'IEC 62439-4 avec peu de modifications éditoriales, et
– déplacement de l'Article 8 (BRP) dans l'IEC 62439-5 avec peu de modifications éditoriales,
– ajout d'une méthode de calcul du temps de reprise maximal du protocole RSTP dans une configuration restreinte (anneau) dans l'IEC 62439-1 (Article 8),
– ajout de spécifications du protocole HSR (High-availability Seamless Redundancy), qui partage les principes du protocole PRP dans l'IEC 62439-3 (Article 5), et
– introduction du protocole DRP (IEC 62439-6).

La version française de cette norme n'a pas été soumise au vote.

Cette publication a été rédigée selon les Directives de l'ISO/IEC, Partie 2.

Une liste de la série IEC 62439 est disponible sous le titre général "*Réseaux industriels de communication – Réseaux de haute disponibilité pour l'automation"* sur le site Web de l'IEC.

Le comité a décidé que le contenu de la publication de base et de ses amendements ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

Copyright International Electrotechnical Commission

INTRODUCTION

La série IEC 62439 spécifie les principes pertinents relatifs aux réseaux haute disponibilité satisfaisant aux exigences des réseaux d'automatisation industriels.

À l'état exempt de panne du réseau, les protocoles de la série IEC 62439 assurent une communication de données fiable et conforme à l'ISO/IEC 8802-3 (IEEE 802.3) et préservent le caractère déterministe des communications de données en temps réel. En cas de panne, de retrait et d'insertion d'un composant, ils assurent des temps de reprise déterministes.

Ces protocoles conservent la totalité des fonctions de communication Ethernet classiques telles qu'elles sont utilisées dans le monde professionnel, de sorte que le logiciel impliqué reste applicable.

Le marché a besoin de plusieurs solutions réseau, présentant chacune des caractéristiques de performance et des capacités fonctionnelles différentes, correspondant aux diverses exigences d'application. Ces solutions prennent en charge différents mécanismes et topologies de redondance qui sont présentés dans l'IEC 62439-1 et spécifiés dans les autres parties de la série IEC 62439. L'IEC 62439-1 distingue également les différentes solutions, en donnant à l'utilisateur des lignes directrices.

La série IEC 62439 se conforme à la structure et aux termes généraux de la série IEC 61158.

Copyright International Electrotechnical Commission

RÉSEAUX INDUSTRIELS DE COMMUNICATION – RÉSEAUX D'AUTOMATISME À HAUTE DISPONIBILITÉ–

Partie 1: Concepts généraux et méthodes de calcul

1 Domaine d'application

La série IEC 62439 s'applique aux réseaux de haute disponibilité pour l'automatisation reposant sur la technologie 8802-3 (IEEE 802.3) (Ethernet) de l'ISO/IEC.

La présente partie de la série IEC 62439 spécifie

- les éléments communs et les définitions pour d'autres parties de la série IEC 62439;
- la spécification d'essai de conformité (normative);
- un système de classification pour les caractéristiques de réseau (informative);
- une méthodologie pour l'estimation de la disponibilité du réseau (informative);
- les règles de configuration, la méthode de calcul et de mesure pour un temps de reprise déterministe dans le protocole RSTP.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60050-191:1990, *Vocabulaire Électrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service*

IEC 61158 (toutes les parties), *Réseaux de communication industriels – Spécifications des bus de terrain*

IEC 61158-6-10, *Réseaux de communication industriels – Spécifications des bus de terrain – Partie 6-10: Spécification de protocole de couche application – Éléments de Type 10*

ISO/IEC 8802-3:2000, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseaux locaux et métropolitains – Prescriptions spécifiques – Partie 3: Accès multiple par surveillance du signal et détection de collision (CSMA/CD) et spécifications pour la couche physique*

IEEE 802.1Q*, IEEE standards for local and metropolitan area network. Virtual bridged local area networks (disponible en anglais seulement)*

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

IETF RFC 791, *Internet Protocol (Protocole Internet)*; disponible à l'adresse <http://www.ietf.org>

Copyright International Electrotechnical Commission

3 Termes, définitions, abréviations, acronymes et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'IEC 60050-191 ainsi que les suivants s'appliquent.

3.1.1
disponibilité
aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens nécessaires est assurée

NOTE 1 La disponibilité dépend de la fiabilité, de la maintenabilité et de la logistique de maintenance.

NOTE 2 Les moyens extérieurs nécessaires, autres que la logistique de maintenance, n'influencent pas la disponibilité de l'entité.

[VEI 191-02-05]

3.1.2
canal
connexion de couche 2 entre deux nœuds d'extrémité, qui consiste en un ou plusieurs chemins (pour la redondance) entre les nœuds d'extrémité

3.1.3
défaillance en mode commun
défaillance qui affecte tous les éléments redondants pour une fonction donnée en même temps

3.1.4
défaillance complète
défaillance qui entraîne l'inaptitude complète d'une entité à accomplir toutes les fonctions requises

[VEI 191-04-20]

3.1.5
connexion
relation logique entre deux nœuds

3.1.6
couverture
probabilité qu'une défaillance est découverte dans un délai assez court pour que la redondance puisse y faire face, exprimant également le pourcentage de défaillances rattrapées par la redondance par rapport au nombre total de défaillances

3.1.7
commutation à la volée (cut-through)
technologie dans laquelle un nœud de commutation commence à émettre une trame reçue avant que cette trame ne soit complètement reçue

3.1.8
défaillance par dégradation
défaillance qui est à la fois une défaillance progressive et une défaillance partielle

[VEI 191-04-22]

Copyright International Electrotechnical Commission

3.1.9
sûreté de fonctionnement
ensemble des propriétés qui décrivent la performance de disponibilité et les facteurs qui la conditionnent: fiabilité, maintenabilité et logistique de maintenance

NOTE La sûreté de fonctionnement est une notion générale sans caractère quantitatif.

[VEI 191-02-03]

3.1.10
appareil
entité physique connectée au réseau composé d'éléments de communication et éventuellement d'autres éléments fonctionnels

NOTE Les appareils sont par exemple des nœuds, des routeurs et des commutateurs.

3.1.11
nœud à double association
nœud qui dispose de deux ports pour des fins de fonctionnement redondant

3.1.12
port d'extrémité
port d'un commutateur connecté à une liaison en feuille

3.1.13
nœud d'extrémité
nœud qui est producteur ou consommateur de données d'application

NOTE Pour les besoins de la série IEC 62439, des spécifications supplémentaires sont données en 0.

3.1.14
erreur
écart ou discordance entre une valeur ou condition calculée, observée ou mesurée et la valeur ou condition spécifiée ou théoriquement correcte

NOTE 1 Une erreur peut être causée par un élément défectueux, par exemple une erreur de calcul faite par un ordinateur en panne.

NOTE 2 Le terme français “erreur” ("error" en anglais) peut aussi désigner "une erreur humaine" ("mistake" en anglais) (voir VEI 191-05-25).

[VEI 191-05-24, modifiée]

3.1.15
défaillance
cessation de l’aptitude d’une entité à accomplir une fonction requise

NOTE 1 Après une défaillance d’une entité, cette entité est en état de panne.

NOTE 2 Une défaillance est un passage d'un état à un autre, par opposition à une panne, qui est un état.

NOTE 3 La notion de défaillance, telle qu'elle est définie, ne s'applique pas à une entité constituée seulement de logiciel.

[VEI 191-04-01]

3.1.16
panne
état d'une entité inapte à accomplir une fonction requise, non comprise l'inaptitude due à la maintenance préventive ou à d'autres actions programmées ou due à un manque de moyens extérieurs

Copyright International Electrotechnical Commission

NOTE Une panne est souvent la conséquence d'une défaillance de l'entité elle-même, mais elle peut exister sans défaillance préalable.

[VEI 191-05-01]

3.1.17
temps de reprise de panne
temps à partir de l'événement de panne jusqu'à l'instant où le réseau retrouve sa fonction de communication requise en présence de la panne

NOTE Suite à un rétablissement après une panne, le réseau fonctionne en mode dégradé utilisant certains des éléments de redondance, ce qui réduit la tolérance aux pannes, et peut ne pas être en mesure d'effectuer un rétablissement après une deuxième panne.

3.1.18
trame
unité de transmission de données sur un MAC (Media Access Control, Commande d'Accès au Support) ISO/IEC 8802-3 qui transmet une unité de données de protocole (PDU) entre les utilisateurs de service MAC

[IEEE 802.1Q, modifiée]

3.1.19
taux de défaillance (instantané)
limite, si elle existe, du quotient de la probabilité conditionnelle que l'instant d'une défaillance d'un élément non réparée se situe dans un intervalle de temps donné (t, t + Δt) et la durée de cet intervalle de temps, Δt, lorsque Δt tend vers zéro, sachant que l'élément n'est pas tombé en panne jusqu'au début de l'intervalle de temps

[VEI 191-12-02]

NOTE Le taux de défaillance est le nombre inverse du MTTF lorsque le taux de défaillance est constant sur la durée de vie d'un élément.

3.1.20
maille inter-étage
liaison entre deux commutateurs

3.1.21
port inter-étage
port d'un commutateur connecté à un autre commutateur via une maille inter-étage

3.1.22
LAN
domaine de diffusion de couche 2 dans lequel les adresses MAC sont uniques et peuvent être traitées à partir de tout autre appareil appartenant à ce domaine de diffusion

NOTE 1 Un VLAN permet le multiplexage de plusieurs réseaux LAN sur la même infrastructure réseau.

NOTE 2 Dans le cadre de la redondance, un réseau peut être constitué de plusieurs réseaux LAN fonctionnant en redondance, auquel cas il est appelé un réseau LAN redondant.

3.1.23
liaison en feuille
liaison entre un nœud d'extrémité et le LAN

NOTE Pour les besoins de la série IEC 62439, des spécifications supplémentaires sont données en 5.2.1.3.

3.1.24
topologie linéaire
topologie où les commutateurs sont connectés en série, avec deux commutateurs connectés chacun à un seul autre commutateur et tous les autres commutateurs connectés à deux autres commutateurs (soit, connectés sous la forme d'une ligne)

Copyright International Electrotechnical Commission

NOTE 1 Cette topologie correspond à celle d'un anneau ouvert.

NOTE 2 Cette configuration est parfois nommée “configuration en chaîne”. La série IEC 62439 n'utilise pas le terme “en chaîne (daisy chain)” à cause d'une éventuelle confusion avec le terme “guirlande (daisy chain)” utilisé ailleurs pour les bus. Du point de vue de câblage, les deux configurations exigent deux mises en œuvre différentes.

[IEC 61918, 3.1.39, modifiée]

3.1.25
liaison
connexion généralement duplex, physique, point-à-point entre deux nœuds adjacents.

[ISO/IEC 11801, 3.1.51, modifiée]

NOTE Le terme “liaison” est différent de "bus", qui est un support physique de diffusion.

3.1.26
entité de redondance de liaison
entité au niveau de la couche 2 qui cache la redondance de port des couches supérieures, en transmettant aux couches supérieures les trames reçues à partir des ports redondants actifs comme si elles provenaient d'un port simple, et en transmettant aux ports redondants actifs une trame provenant des couches supérieures

3.1.27
unité de données de service de liaison
données transportées dans une couche protocolaire à la couche supérieure

NOTE L'unité de données de service de liaison dans une trame Ethernet représente le contenu de la trame située entre le champ Longueur/Type et la séquence de contrôle de trame.

3.1.28
taux moyen de défaillance
moyenne du taux de défaillance instantané sur un intervalle de temps donné $\lambda(t_1, t_2)$.

[VEI 191-12-03]

NOTE La série IEC 62439 utilise le terme “taux de défaillance” pour signifier “taux moyen de défaillance” défini par le VEI 191-12-03.

3.1.29
moyenne de temps de bon fonctionnement
MTBF
espérance mathématique de la durée de bon fonctionnement

[VEI 191-12-09]

3.1.30
durée moyenne de fonctionnement avant défaillance
MTTF
espérance mathématique de la durée de fonctionnement avant défaillance

[VEI 191-12-07]

3.1.31
moyenne des temps pour la tâche de réparation
MTTR
espérance mathématique des temps pour la tâche de réparation

[VEI 191-13-08, modifiée]

3.1.32
topologie en maille
topologie où chaque nœud est connecté à trois mailles inter-étage ou plus

Copyright International Electrotechnical Commission

3.1.33
message
série ordonnée d'octets, destinée à véhiculer des informations

NOTE Normalement utilisé pour transmettre des informations entre des homologues sur la couche Application.

[IEC 61784-2, 3.1.14]

3.1.34
réseau
système de communication constitué de nœuds d'extrémité, de liaisons en feuille et d'un ou plusieurs LAN

NOTE Un réseau peut avoir plusieurs LAN pour des fins de redondance.

3.1.35
nœud
entité du réseau connectée à une ou plusieurs liaisons

NOTE Les nœuds peuvent être soit un commutateur soit un nœud d'extrémité soit les deux.

[IEC 61784-2, 3.1.16, modifiée]

3.1.36
défaillance partielle
défaillance qui entraîne l'inaptitude d'une entité à accomplir certaines fonctions requises mais pas toutes

3.1.37
chemin
ensemble de liaisons et de commutateurs liés en série

NOTE Il peut y avoir deux ou plusieurs chemins entre deux commutateurs pour assurer la redondance.

3.1.38
installation
système qui dépend de la disponibilité du réseau d'automatisation à exploiter

EXEMPLE Les installations peuvent être des centrales électriques, des imprimantes, des systèmes de fabrication, des postes, des véhicules.

3.1.39
port
point de connexion d'un nœud au réseau

[ISO/IEC 8802-3, modifiée]

NOTE 1 Cette définition est différente d'un port TCP ou d'un port UDP, qui sont qualifiés explicitement dans la série IEC 62439, si nécessaire.

NOTE 2 Un port inclut une mise en œuvre de couche 1 et de couche 2.

3.1.40
reprise
événement lorsque le réseau redevient capable d'assurer sa fonction de communication requise après une interruption

NOTE Des exemples d'interruptions pourraient être une panne ou le retrait et la réinsertion d'un composant.

3.1.41
temps de reprise
durée de rétablissement
durée entre l'interruption et la reprise

Copyright International Electrotechnical Commission

3.1.42
redondance
existence, dans une entité, de plus d'un moyen pour accomplir une fonction requise

[VEI 191-15-01]

NOTE Dans la série IEC 62439, l'existence de plus d'un chemin (consistant en liaisons et commutateurs) entre nœuds d'extrémité.

3.1.43
temps de rétablissement de remise en état
temps pour rétablir la configuration du réseau originale ou précédant la panne y compris les états d'exploitation et de gestion d'origine dans chaque appareil

3.1.44
fiabilité
aptitude d'un élément à remplir une fonction requise dans des conditions déterminées et pendant un intervalle de temps donné

[VEI 191-02-06]

NOTE 1 Il est généralement admis que l'élément soit en état de remplir cette fonction requise au début de l'intervalle de temps.

NOTE 2 Le terme "fiabilité" est aussi employé comme une mesure de la performance de la fiabilité (voir VEI 191-12-01).

3.1.45
réparation
mesure prise pour le rétablissement de la situation spécifiée

3.1.46
temps de reprise de réparation
durée de rétablissement de réparation
retard entre le début de l'action de réparation et l'achèvement de la réparation de l'élément défectueux de telle sorte que le réseau retrouve, et sa fonction de communication requise, et sa capacité requise de résistance aux pannes.

NOTE 1 Ce délai comprend tout temps d'arrêt du réseau provoqué par le processus de réparation, par exemple une panne de réseau pour remplacer un commutateur à plusieurs bons ports et un seul port défectueux.

NOTE 2 Ce délai n'inclut pas le temps de remise en état du réseau de son mode de fonctionnement de secours au mode de fonctionnement d'origine.

3.1.47
liaison d'un anneau
liaison qui connecte deux commutateurs d'un anneau

3.1.48
port d'un anneau
port d'un commutateur auquel une liaison d'anneau est liée

3.1.49
topologie en anneau
topologie où chaque nœud est connecté en série à deux autres nœuds

NOTE 1 Les nœuds sont connectés les uns aux autres sous la forme logique d'un cercle.

NOTE 2 Les trames sont transmises séquentiellement entre des nœuds actifs, chaque nœud étant capable d'examiner ou de modifier la trame avant de la transmettre.

Copyright International Electrotechnical Commission

3.1.50
robustesse
comportement du réseau face aux défaillances

3.1.51
pont racine
commutateur ayant la valeur la plus faible d'un paramètre identificateur de pont RSTP dans le réseau

[IEEE 802.1D]

3.1.52
route
chemin de communication couche 3 entre deux nœuds

3.1.53
critère de défaillance unique
capacité d'un système qui inclut des composants redondants afin de maintenir toute sa fonctionnalité suite à une défaillance d'un de ses composants, avant la maintenance ou le rétablissement automatique

3.1.54
point unique de défaillance
composant dont la défaillance pourrait provoquer une défaillance du système et n'est pas compensée par la redondance ou une autre procédure opérationnelle

NOTE Un point unique de défaillance provoque une défaillance en mode commun. Elle peut être provoquée par une erreur de conception dans les éléments redondants ou par une cause extérieure qui affecte tous les éléments redondants de la même manière, par exemple, température extrême.

3.1.55
nœud à une seule association
nœud qui dispose d'un seul port à un LAN

3.1.56
redondance en attente
redondance telle qu'une partie seulement des moyens d'accomplir une fonction requise est utilisée, le reste n'étant utilisé qu'en cas de besoin

[VEI 191-15-03]

NOTE Elle est également appelée «redondance dynamique».

3.1.57
topologie en étoile
topologie où tous les appareils sont connectés à un nœud central

3.1.58
commutation avec enregistrement et retransmission (store-and-forward)
technologie dans laquelle un nœud de commutation commence à émettre une trame reçue seulement après que cette trame est complètement reçue

3.1.59
commutateur
nœud commutateur
pont MAC tel que défini dans l'IEEE 802.1D

NOTE Le terme “commutateur” est utilisé en tant que synonyme pour le terme “nœud commutateur”.

Copyright International Electrotechnical Commission

3.1.60
nœud d'extrémité de commutation
un nœud d'extrémité et un commutateur combinés dans un seul appareil

3.1.61
défaillance systématique
défaillance liée de façon déterministe à une certaine cause, qui ne peut être éliminée que par une modification de la conception ou du processus de fabrication, par les procédures opérationnelles, par la documentation ou par d'autres facteurs pertinents

NOTE 1 La maintenance corrective sans modification n'éliminera pas en général la cause de la défaillance.

NOTE 2 Une défaillance systématique peut être induite par la simulation de la cause de la défaillance.

[VEI 191-04-19]

3.1.62
topologie
configuration des positions relatives et des interconnexions des nœuds individuels du réseau

[issue de l'IEC 61918, 3.1.67]

NOTE D'autres aspects tels que le délai, l'atténuation et les classes de support physique, relatifs aux chemins qui connectent les nœuds du réseau sont aussi parfois considérés comme des propriétés de la topologie.

3.1.63
topologie en arbre
topologie dans laquelle deux nœuds ont seulement un chemin entre eux et au moins un commutateur est lié à plus de deux mailles inter-étage

3.1.64
partie jonction
partie d'un LAN commuté qui achemine le trafic à plusieurs nœuds d'extrémité

3.1.65
entité de couche supérieure
parties de la pile protocolaire immédiatement au-dessus de la couche traitant la redondance

3.1.66
temps de reprise dans les conditions les plus défavorables
temps de reprise maximal prévu parmi toutes les pannes et pour toutes les configurations autorisées

NOTE Ce retard est important pour un concepteur de réseau pour indiquer quels sont les aspects du réseau qui nécessitent un traitement spécial pour réduire au maximum les interruptions de communication.

3.1.67
pont
dispositif connectant des segments LAN au niveau de la couche 2 conformément à l'IEEE 802.1D

NOTE Les termes "commutateur" et "pont" sont considérés comme synonymes, le terme "pont" est utilisé dans le contexte des normes telles que RSTP (IEEE 802.1D), PTP (IEC 61588) ou IEC 62439-3 (PRP & HSR).

3.1.68
temps de rétablissement du réseau
délai écoulé entre la première défaillance d'un composant ou d'un média au sein du réseau et la fin de la reconfiguration du réseau et à partir duquel tous les dispositifs qui sont encore en mesure de participer à la communication du réseau sont à nouveau capables d'atteindre tous les autres dispositifs dans le réseau

Copyright International Electrotechnical Commission

NOTE Lorsqu'un protocole de contrôle de redondance du réseau (comme RSTP) reconfigure le réseau en raison d'une défaillance, certaines parties du réseau peuvent être toujours disponibles et les ruptures de communication peuvent varier dans le temps et dans l'espace sur l'ensemble du réseau. Dans les calculs, seul le scénario le plus défavorable est pris en compte.

3.2 Abréviations et acronymes

BRP Beacon Redundancy Protocol (Protocole de redondance à balise), IEC 62439-5

BPDU Bridge management Protocol Data Unit (Unité de données de protocole de gestion de pont), conformément à l'IEEE 802.1D

CRP Cross-network Redundancy Protocol (Protocole de redondance inter-réseau), voir IEC 62439-4

DAN Doubly Attached Node (Noeud à double association)

DRP Distributed Redundancy Protocol (Protocole de redondance distribuée), voir IEC 62439-6

DUT Device Under Test (Appareil en essai)

HSR High-availability Seamless Redundancy (Redondance transparente de haute disponibilité), voir IEC 62439-3

IP Internet Protocol, couche 3 de la pile Protocole Internet

IT ou TI Information Technology ou Technologie de l'information

LAN Local Area Network (Réseau local)

LRE Link Redundancy Entity (Entité de redondance de liaison)

MAC Media Access Control (Commande d'accès au support)

MRP Medium Redundancy Protocol (Protocole de redondance du support), voir IEC 62439-2

MTBF Mean Time Between Failure (Temps moyen entre défaillances)

MTTF Mean Time To Failure (Durée moyenne de fonctionnement avant défaillance)

MTTFN Mean Time To Failure of Network (Durée moyenne de fonctionnement avant défaillance du réseau)

MTTFS Mean Time To Failure of System (Durée moyenne de fonctionnement avant défaillance du système)

MTTR Mean Time To Repair (Durée moyenne de panne)

MTTRP Mean Time To Repair Plant (Durée moyenne de panne installation)

OUI Organizational Unique Identifier (Identificateur propre à une organisation)

PDU Protocol Data Unit (Unité de données de protocole)

PICS Protocol Implementation Conformance Statement (Déclaration de conformité de mise en œuvre de protocole)

PRP Parallel Redundancy Protocol (Protocole de redondance parallèle), voir IEC 62439-3

QAN Quadruply Attached Node (Nœud à quadruple association)

RFC Request For Comments de l'Internet Society (Demande de commentaires de l'Internet Society)

Copyright International Electrotechnical Commission

RRP Ring-based Redundancy Protocol (Protocole de redondance pour réseau en anneau), voir IEC 62439-7

RSTP Rapid Spanning Tree Protocol (Protocole arborescence rapide), voir IEEE 802.1D

SAN Singly Attached Node (Nœud à une seule association)

SRP Serial Redundancy Protocol (Protocole de redondance série), voir IEC 62439-3

STP Spanning Tree Protocol (Protocole d'arborescence, Protocole spanning tree)

TCP Transmission Control Protocol (Protocole de commande de transport), couche 4 de la pile Protocole Internet

UDP User Datagram Protocol (Protocole de datagramme utilisateur), couche 4 de la pile Protocole Internet

3.3 Conventions

3.3.1 Conventions générales

Les protocoles spécifiés dans la série IEC 62439 suivent la structure définie dans l'IEC/TR 61158-1.

Les directives générales sont spécifiées dans l'IEC 61158-6-10, 3.7.

3.3.2 Conventions pour les définitions des diagrammes d'états

La série IEC 62439 suit les conventions utilisées dans l'IEC 61158-6-10, 3.8. Ce qui suit est un résumé.

- Chaque état est décrit par une table, avec une rangée séparée pour chaque transition qui peut provoquer un changement d'état.
- Les transitions sont définies comme des événements qui peuvent transporter des arguments et être assujettis à des conditions.
- Le champ d'action exprime l'action qui se déroule dans le cas où l'événement est déclenché.
- Pour des raisons d'espace, l'événement et les actions sont placés dans la même cellule.
- La colonne de droite indique le prochain état dans lequel on pénètre après la fin de l'action.

3.3.3 Conventions pour la spécification de PDU

Les PDU sont décrites conformément à la spécification RFC 791, Annexe B.

En particulier:

- les bits, les octets et les matrices sont numérotés à partir de 0;
- La convention "Ordre des Octets du Réseau" (big-endian (gros boutiste), octet de poids fort en premier) est observée.

L'IEC 61158-6-10 distingue le bit "identification" du bit "offset".

EXEMPLE Dans une chaîne binaire de 8 bits, le bit le plus à droite (Bit de poids faible) est étiqueté bit 0, mais son bit "offset" est mis à 7 dans l'octet de chaîne de bits.

Lors de la spécification d'objets de données plutôt que de PDU, le bit "identification" selon la série IEC 61158-6 est utilisé. Par conséquent, les bits d'une chaîne binaire sont spécifiés dans l'ordre croissant du bit "identification", bien qu'ils soient émis dans l'ordre inverse.

Copyright International Electrotechnical Commission

3.4 Adresses réseau réservées

Ce qui suit est un récapitulatif des adresses réseau réservées pour les besoins de la série IEC 62439, tandis que les valeurs requises sont spécifiées dans les parties respectives de la série IEC 62439.

Pour les besoins de la série IEC 62439, l'identificateur OUI 00-15-4E a été réservé par l'IEEE. Toutes les bandes ayant cet identificateur OUI sont réservées pour la série IEC 62439. Les bandes suivantes sont affectées:

- MRP (voir IEC 62439-2) utilise 00-15-4E, bande 00-00-xx.
- PRP (voir IEC 62439-3) utilise 00-15-4E, bande 00-01-xx.
- HSR (voir IEC 62439-3) utilise 0x892F.
- CRP (voir IEC 62439-4) utilise une adresse MAC multidiffusion IP.
- BRP (voir IEC 62439-5) utilise 00-15-4E, bande 00-02-xx.
- DRP (voir IEC 62439-6) utilise 00-15-4E, bande 00-03-xx.
- RRP (voir IEC 62439-7) utilise 00 E0 91 02 05 99.

Pour les besoins de la série IEC 62439, les Ethertypes suivants (voir IEEE 802a) ont été réservés par l'IEEE:

- MRP (voir IEC 62439-2) utilise 0x88E3.
- PRP (voir IEC 62439-3) utilise 0x88FB.
- CRP (voir IEC 62439-4) utilise 0x0800 (IP) avec un port UDP 3622.
- BRP (voir IEC 62439-5) utilise 0x80E1.
- DRP (voir IEC 62439-6) utilise 0x8907.
- RRP (voir IEC 62439-7) utilise 0x88FE.

4 Exigences de conformité (normative)

4.1 Conformité aux protocoles de redondance

Une déclaration de conformité avec une partie de la série IEC 62439 doit être énoncée comme:

- une conformité à l'IEC 62439-2 (MRP), ou
- une conformité à l'IEC 62439-3 (PRP), ou
- une conformité à l'IEC 62439-4 (CRP), ou
- une conformité à l'IEC 62439-5 (BRP),
- une conformité à l'IEC 62439-6 (DRP),
- une conformité à l'IEC 62439-7 (RRP).

Une déclaration de conformité doit être accompagnée d'une documentation justificative appropriée telle que définie en 4.2. Les protocoles et options pris en charge doivent être spécifiés comme PICS, au format:

Options PICS_62439-X_supported.

EXEMPLE PICS_62439-5_BlockingSupported.

Copyright International Electrotechnical Commission

4.2 Essais de conformité

4.2.1 Concept

Le concept de cet essai de conformité est de vérifier les fonctions d'un appareil en essai (DUT) par rapport à un ensemble cohérent d'indicateurs dans les conditions simulées les plus défavorables. L'essai de conformité doit assurer l'interopérabilité des appareils qui revendiquent la conformité avec le même protocole.

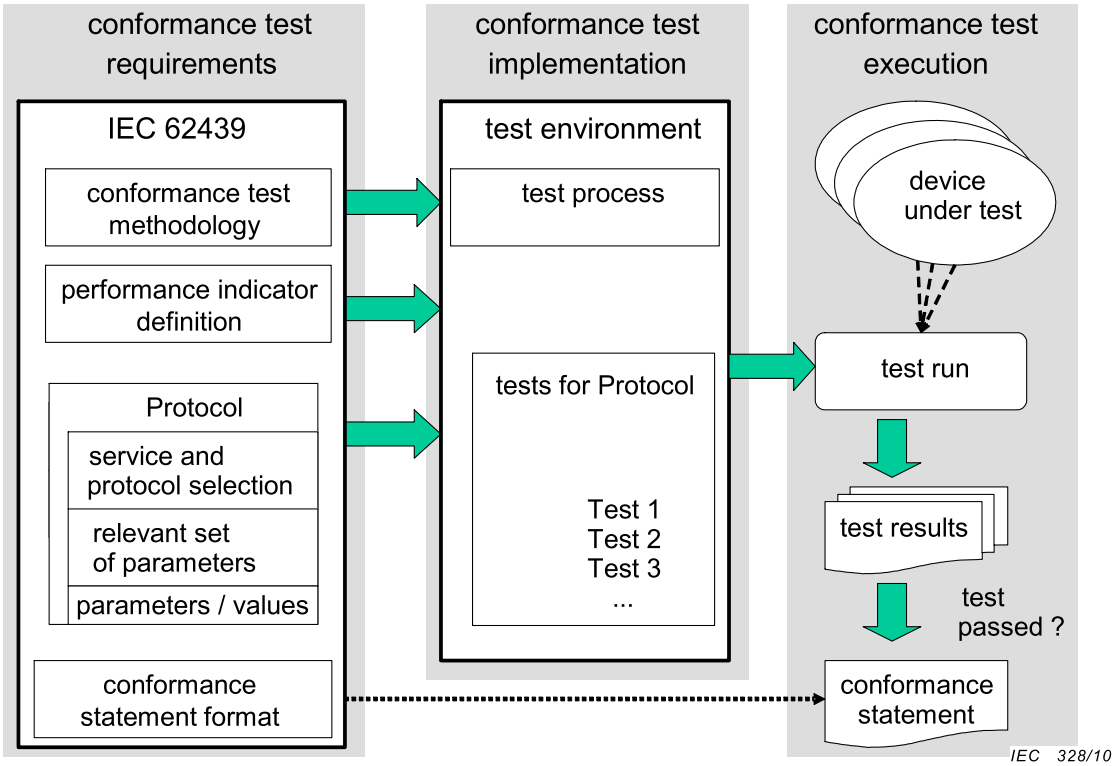
La série IEC 62439 contient des spécifications qui doivent être observées par différents acteurs:

- le constructeur d'appareils qui conçoit et met en essai une interface compatible;
- le gestionnaire de réseau qui définit la topologie;
- l'utilisateur du réseau qui respecte les limites d'utilisation.

Un appareil vendu comme étant entièrement conforme à un protocole de la série IEC 62439 peut avoir une performance inférieure si les règles de configuration de réseau ne sont pas respectées quand il est utilisé.

La Figure 1 donne une vue d'ensemble de l'essai de conformité lié aux protocoles de la série IEC 62439.

NOTE La mise en œuvre et l'exécution de l'essai de conformité ne sont pas définies dans la série IEC 62439.



Légende

Anglais	Français
Conformance test requirements	Exigences d'essai de conformité
Conformance test implementation	Mise en œuvre d'essai de conformité
Conformance test execution	Exécution d'essai de conformité
Conformance test methodology	Méthodologie d'essai de conformité
Performance indicator definition	Définition d'indicateur de performance
Protocol	Protocole

Copyright International Electrotechnical Commission

Anglais	Français
Service and protocol selection	Sélection de service et protocole
Relevant set of parameters	Ensemble pertinent de paramètres
Parameters / values	Paramètres / valeurs
Conformance statement format	Format de déclaration de conformité
Test environment	Environnement d'essai
Test process	Processus d'essai
Tests for Protocol	Essais pour protocole
Test 1	Essai 1
Test 2	Essai 2
Test 3	Essai 3
Device under test	Appareil en essai
Test run	Déroulement d'essai
Test results	Résultats d'essai
Test passed?	Essai réussi?
Conformance statement	Déclaration de conformité

Figure 1 – Vue d'ensemble de l'essai de conformité

4.2.2 Méthodologie

Les scénarios d'essai doivent être développés de manière que les essais puissent être répétés. Les résultats des essais doivent être documentés et doivent être utilisés comme la base pour la déclaration de conformité.

Les essais de conformité d'un appareil doivent inclure, le cas échéant, la vérification

- de l'exactitude de la fonctionnalité spécifiée,
- des valeurs des indicateurs liés au réseau,
- des valeurs des indicateurs liés à l'appareil.

Les valeurs des indicateurs de performance du protocole et de l'appareil en essai doivent être utilisées.

NOTE 1 Une description d'un processus d'essai de conformité est donnée dans la série ISO/IEC 9646.

NOTE 2 Il est supposé que la qualité des scénarios d'essai garantisse l'interopérabilité d'un appareil soumis à l'essai. Si des irrégularités sont signalées, les scénarios d'essai seront adaptés en conséquence.

4.2.3 Conditions et scénarios d'essai

Les conditions et les scénarios d'essai doivent être définis et documentés sur la base d'un protocole de redondance spécifique. Cela doit inclure les indicateurs suivants, le cas échéant:

- nombre de nœuds;
- topologie de réseau;
- le nombre de commutateurs entre les nœuds;
- le type de trafic.

Pour chaque indicateur mesuré, les documents relatifs aux conditions et aux scénarios d'essai doivent être établis et doivent décrire:

- le but d'essai;
- le montage d'essai;

Copyright International Electrotechnical Commission

- la procédure d'essai;
- les critères de conformité.

Le montage d'essai décrit le réglage de l'équipement nécessaire pour effectuer l'essai, y compris les équipements de mesure, l'appareil en essai, les équipements auxiliaires, le schéma d'interconnexion et les conditions environnementales d'essai.

Des parties de l'environnement d'essai peuvent être émulées ou simulées. Les effets de l'émulation ou de la simulation doivent être documentés.

La procédure d'essai décrit comment il convient d'effectuer l'essai, ce qui inclut également une description d'un ensemble spécifique d'indicateurs nécessaires pour effectuer cet essai. Les critères de conformité définissent les résultats des essais acceptés en tant que conformité avec cet essai.

4.2.4 Procédure d'essai et mesures

Les indicateurs mesurés doivent inclure, le cas échéant:

- le temps de reprise de la redondance,
- l'impact d'une surcharge de redondance en fonctionnement normal.

La procédure d'essai doit être basée sur les principes de 4.2.3.

La séquence de mesure des actions pour effectuer un essai doit être fournie.

Le nombre d'essais indépendants doit être fourni.

La méthode utilisée pour calculer le résultat de l'essai à partir des essais indépendants doit être fournie, le cas échéant.

4.2.5 Rapport d'essai

Le rapport d'essai doit contenir suffisamment d'informations permettant de répéter l'essai.

Le rapport d'essai doit contenir au moins

a) la référence à la méthodologie d'essai de conformité selon 4.2.2,
b) la référence aux définitions des indicateurs de performance,
c) la référence au protocole de redondance de la série IEC 62439,
d) une description de l'environnement de l'essai de conformité, y compris les émulateurs de réseau, les équipements de mesure et la personne ou l'organisation responsable de l'exécution de l'essai, ainsi que la date de l'essai,
e) une description de l'appareil en essai, son fabricant et la version matérielle et logicielle,
f) le nombre et le type d'appareils connectés au réseau ainsi que la topologie,
g) une référence aux spécifications des scénarios d'essai,
h) les valeurs mesurées,
i) un énoncé relatif à la conformité au protocole de redondance.

Copyright International Electrotechnical Commission

5 Concepts pour des réseaux d'automatisme à haute disponibilité (informative)

5.1 Caractéristiques d'application des réseaux d'automatisation

5.1.1 Résilience en cas de défaillance

Les installations comptent sur le bon fonctionnement du système d'automatisation. Les installations tolèrent une dégradation du système d'automatisation pendant un court laps de temps seulement, appelé temps de grâce. Il convient que le temps de reprise du réseau soit plus court que le temps de grâce du moment où l'application nécessite généralement d'effectuer des tâches supplémentaires (liées au protocole et au traitement de données, en attendant le prochain cycle de communication programmée, etc.) avant que l'installation revienne à l'état totalement opérationnel. Les applications peuvent être distinguées par leur temps de grâce, comme le montre le Tableau 1.

Tableau 1 – Exemples de temps de grâce d'applications

Applications	Temps de grâce type s
Automatisation non critique, par exemple systèmes d'entreprises	20
Gestion d'automatisation, par exemple fabrication, automatisation discrète	2
Automatisation générale, par exemple automatisation de processus, centrales électriques	0,2
Automatisation à temps critique, par exemple transmissions synchronisées	0,020

Certaines installations ont des exigences plus strictes quand elles doivent fonctionner en continu, n'ayant pas de période de repos pendant laquelle l'installation peut être maintenue ou reconfigurée. Dans ce cas, le temps de grâce est valable pour l'exigence la plus stricte, par exemple dictée par le remplacement à chaud de parties de l'équipement.

Les systèmes d'automatisation peuvent contenir de la redondance pour faire face aux défaillances. Les méthodes diffèrent sur la façon de gérer la redondance, mais leur facteur de performance clé est le temps de reprise, c'est-à-dire le temps nécessaire pour rétablir le fonctionnement après l'apparition d'une interruption. Si le temps de reprise dépasse le temps de grâce de l'installation, les mécanismes de protection lancent un arrêt (en mode sûr), ce qui peut entraîner une perte importante de la production et de la disponibilité opérationnelle des installations.

Une caractéristique clé du rétablissement est son déterminisme, c'est-à-dire la garantie que le temps de reprise reste en dessous d'une certaine valeur, tant que les hypothèses de base (défaillance unique à la fois, pas de mode commun de défaillance, moins d'une extension maximale du système) sont satisfaites. Un réseau offre un rétablissement déterministe s'il est possible de calculer un temps de rétablissement maximum fini d'une topologie donnée, en cas de défaillance simple.

Chaque fois que l'exploitation dépend de la fonction correcte du réseau d'automatisation, il peut être nécessaire d'augmenter la disponibilité du réseau.

L'augmentation de la disponibilité en augmentant la fiabilité des éléments ou en améliorant la maintenance est en dehors du domaine d'application de la série IEC 62439. La série IEC 62439 considère uniquement les protocoles qui introduisent de la redondance et reconfigurent automatiquement les éléments redondants du réseau en cas de défaillance.

Copyright International Electrotechnical Commission

5.1.2 Classes de redondance de réseau

5.1.2.1 Généralités

La série IEC 62439 considère deux classes de redondance de réseau:

a) redondance gérée au sein du réseau;

b) redondance gérée dans les nœuds d'extrémité.

NOTE La série IEC 62439 ne considère pas la redondance des nœuds d'extrémité eux-mêmes, c'est-à-dire l'utilisation de nœuds d'extrémité redondants, puisque cela est hautement spécifique à une application.

5.1.2.2 Redondance gérée au sein du réseau

La redondance au sein d'un réseau a été appliquée aux réseaux étendus et aux bus de terrain traditionnels.

Les routeurs de couche 3 (non pris en compte dans la série IEC 62439) calculent les routes alternatives à la suite de défaillances de liaison. Les protocoles correspondants ont bien fait leurs preuves comme partie intégrante de la pile IP, mais le temps de reprise est de l'ordre de dizaines de secondes, voire de l'ordre de minutes, en fonction de la topologie. Ces temps de reprise sont tolérés uniquement par les applications les plus bénignes.

Les réseaux d'automatisation fonctionnent généralement dans un seul réseau local (LAN), c'est-à-dire les messages opérationnels sont acheminés à travers les répéteurs de la couche 1 ou les commutateurs de la couche 2, mais ne traversent pas les routeurs. Les messages partagés avec le monde extérieur via les routeurs ou les pare-feux existent bien, mais ils sont considérés comme non critiques.

Classiquement, la redondance au sein d'un réseau LAN est assurée par les protocoles qui réagissent à la perte de liaisons et de commutateurs par la reconfiguration du LAN, en utilisant des liaisons et des commutateurs redondants, tels que le protocole RSTP (Rapid Spanning Tree Protocol) conformément à l'IEEE 802.1D.

Les protocoles de redondance améliorés de couche 2 se basent sur les mêmes principes que RSTP, mais fournissent une reprise plus rapide en exploitant l'hypothèse que le réseau d'automatisation ait une topologie en anneau. Les nœuds d'extrémité sont des nœuds d'automatisation non modifiés.

5.1.2.3 Redondance gérée dans les nœuds d'extrémité

D'autres améliorations des temps de reprise nécessitent la gestion de la redondance dans les nœuds d'extrémité, en équipant les nœuds d'extrémité par plusieurs liaisons de communication redondantes. En général, les nœuds d'extrémité à double association fournissent une redondance suffisante. Dans ce type de redondance, aucune hypothèse n'est faite concernant les commutateurs dans le LAN.

Pour les applications à temps critique telles que les transmissions synchronisées, l'exploitation parallèle des réseaux disjoints fournit un rétablissement sans raccord, mais nécessite une duplication complète du réseau. Certaines installations critiques nécessitent également des nœuds à double association, afin de faire face à une défaillance d'une liaison en feuille, même si elles ne nécessitent pas de temps de reprise très court.

5.1.3 Maintenance de la redondance

La redondance peut être affectée par des pannes latentes, ce qui peut être détecté par les essais. L'intervalle d'essai permet d'estimer la disponibilité. Tous les protocoles fournissent les moyens pour mettre en essai les composants redondants ou de rechange et signaler les défaillances détectées à la gestion du réseau.

Copyright International Electrotechnical Commission

5.1.4 Comparaison et indicateurs

Les protocoles spécifiés dans la série IEC 62439 offrent:

- un temps de reprise maximal, déterministe et garanti (qui peut dépendre de la topologie),
- la transparence de la communication réelle vers l'application en toutes circonstances, et
- pour les nœuds à double association, l'interopérabilité avec les appareils à une seule association (matériel TI courant disponible dans le commerce).

Le Tableau 2 compare certaines caractéristiques de quelques protocoles de redondance, commandés par le temps de reprise.

Tableau 2 – Exemples de protocoles de redondance

Protocole	Solution	Perte de trame	Protocole de redondance	Association de nœuds d'extrémité	Topologie de réseau	Temps de reprise pour les défaillances considérées
IP	Routage IP	Oui	Dans le réseau	Simple	Simple maillée	> 30 s typique non déterministe
STP	IEEE 802.1D	Oui	Dans le réseau	Simple	Simple maillée	> 20 s typique non déterministe
RSTP	IEEE 802.1D	Oui	Dans le réseau	Simple	Simple maillée, anneau	Peut être déterministe conformément aux règles de l'Article 8
CRP	IEC 62439-4	Oui	Dans les nœuds d'extrémité	Simple et double	Doublement maillée, à connexion croisée	1 s au pire des cas pour 512 nœuds d'extrémité
DRP	IEC 62439-6	Oui	Dans le réseau	Simple et double	Anneau, double anneau	100 ms au pire des cas pour 50 commutateurs
MRP	IEC 62439-2	Oui	Dans le réseau	Simple	Anneau, maillé	500 ms, 200 ms, 30 ms ou 10 ms le cas le plus défavorable pour 50 commutateurs en fonction de l'ensemble des paramètres et de la typologie du réseau
BRP	IEC 62439-5	Oui	Dans les nœuds terminaux	Double	Doublement maillée, connectée	8,88 ms le cas le plus défavorable pour 100 nœuds terminaux
RRP	IEC 62439-7	Oui	Dans les nœuds terminaux	Double (nœuds terminaux de commutation)	En anneau simple	8 ms dans 100BASEX, 4 ms dans 1000BASEX
PRP	IEC 62439-3	Non	Dans les nœuds d'extrémité	Double	Doublement maillée, indépendante	0 s
HSR	IEC 62439-3	Non	Dans les nœuds d'extrémité	Double	Anneau, maillée	0 s

NOTE Pour les protocoles de redondance spécifiés dans la série IEC 62439, les temps de reprise dans le Tableau 2 sont garantis si l'on utilise les configurations et les paramètres spécifiés dans la partie associée de la série IEC 62439. Des temps de reprise plus rapides peuvent être réalisés en utilisant des réglages et des paramètres différents, et ce, sous la responsabilité de l'utilisateur.

Les indicateurs pour les différentes solutions incluent, le cas échéant:

Copyright International Electrotechnical Commission

- le temps de reprise de panne,
- le temps de reprise de réparation,
- la durée de rétablissement de remise en état,
- temps de reprise dans les conditions les plus défavorables,
- l'impact sur le fonctionnement normal.

Les cas de panne comportent:

- défaillance du gestionnaire de réseau actif courant (s'il existe) suivie par une réparation et un rétablissement;
- défaillance de la source courante du temps de réseau (si elle existe) suivie par une réparation et un rétablissement.

Le paragraphe 5.2 généralise les considérations ci-dessus et introduit un schéma de classification.

5.2 Système du réseau générique

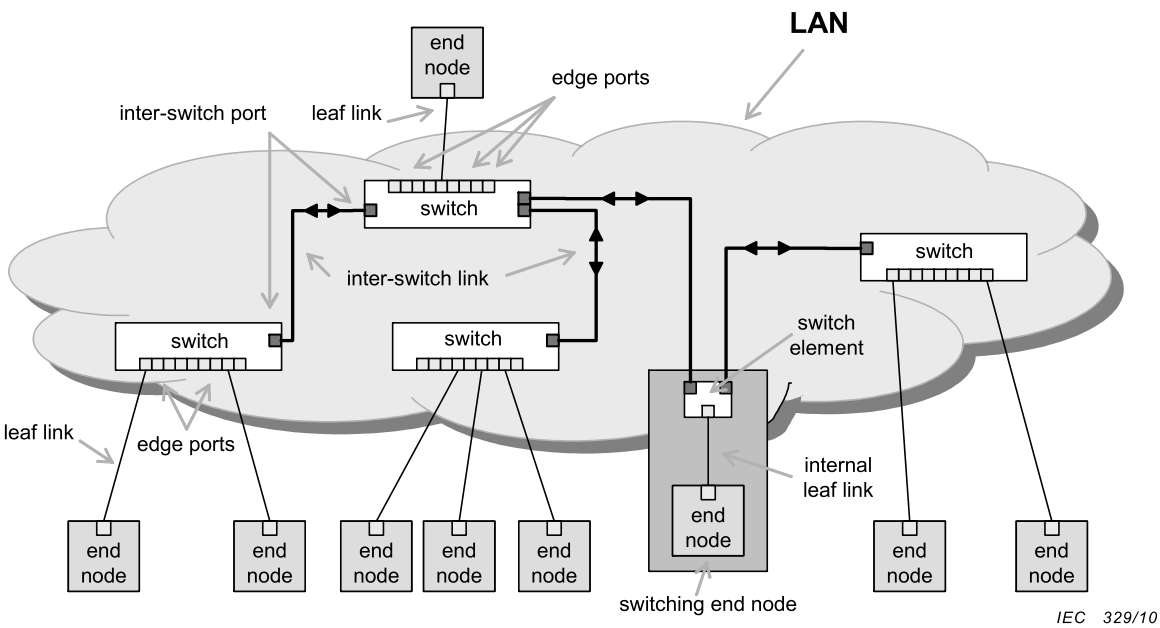
5.2.1 Éléments du réseau

5.2.1.1 Généralités

Le réseau générique est modélisé avec les éléments fonctionnels énumérés ci-dessous et représentés dans la Figure 2.

- Nœuds d'extrémité
- Liaisons en feuille
- Commutateurs (avec ports d'extrémité et ports inter-étage)
- Mailles inter-étage
- Nœuds d'extrémité de commutation

Le LAN se constitue de tous les composants du réseau, excepté les nœuds d'extrémité et les liaisons en feuille.



NOTE Les ports d'extrémité sont ombrés en gris clair, les ports inter-étage sont ombrés en gris foncé, les mailles inter-étage sont dessinées avec un trait épais, les liaisons en feuille sont dessinées avec un trait fin.

Copyright International Electrotechnical Commission

Légende

Anglais	Français
Inter switch port	Port inter-étage
Leaf link	Liaison en feuille
Edge ports	Ports d'extrémité
Switch	Commutateur
Inter switch link	Maille inter-étage
Switch element	Élément de commutateur
Internal leaf link	Liaison en feuille interne
End node	Nœud d'extrémité
Switching end node	Nœud d'extrémité de commutation

Figure 2 – Éléments du réseau général (topologie en arbre)

5.2.1.2 Nœud d'extrémité

Un nœud d'extrémité nécessite un port de connexion au LAN pour son fonctionnement normal.

Le port de connexion d'un nœud d'extrémité est connecté à un port d'extrémité d'un commutateur dans un LAN par une liaison en feuille.

5.2.1.3 Liaison en feuille

Une liaison en feuille connecte un nœud d'extrémité au LAN.

Cette connexion peut être interne à un appareil, dans le cas où l'appareil combine le nœud d'extrémité et le commutateur ou la fonctionnalité LRE (nœud d'extrémité de commutation dans la Figure 2).

5.2.1.4 Maille inter-étage

Une maille inter-étage connecte les commutateurs dans un LAN.

Différentes mailles inter-étage peuvent exister entre deux commutateurs en vue d'augmenter la disponibilité.

5.2.1.5 Commutateurs

Les commutateurs sont des éléments de connexion de couche 2 tels que définis dans l'IEEE 802.1D.

NOTE Les ponts conformément à l'IEEE 802.1D sont nommés commutateurs dans la série IEC 62439.

Les commutateurs sont connectés les uns aux autres par des mailles inter-étage.

Un commutateur est connecté à une liaison en feuille par le biais d'un port d'extrémité.

5.2.1.6 Nœud d'extrémité de commutation

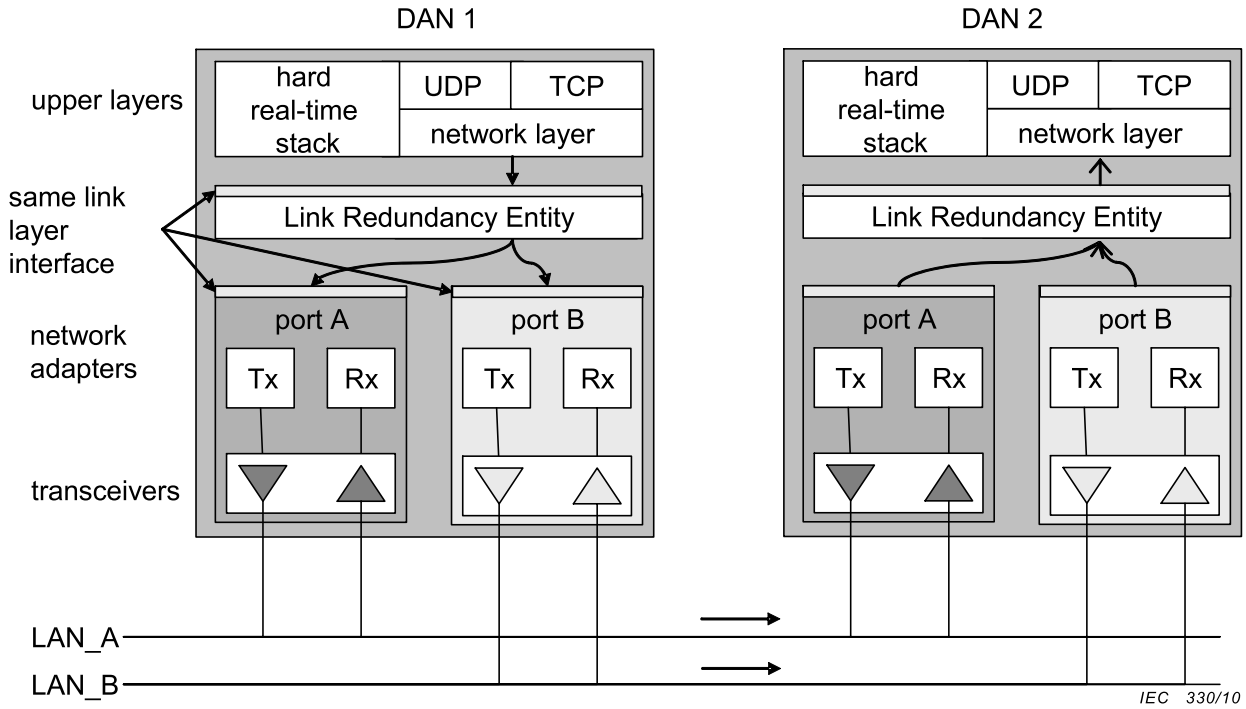
Un élément du commutateur peut être mis en œuvre dans la même partie de l'équipement physique comme étant le nœud d'extrémité. Bien que cela fasse apparaitre le nœud d'extrémité comme un nœud à double association, en interne le principe de fonctionnement est différent, car il n'y a pas besoin d'une entité de redondance de liaison parce que l'élément du commutateur joue ce rôle.

Copyright International Electrotechnical Commission

5.2.1.7 Nœuds d'extrémité à associations multiples

Les nœuds d'extrémité peuvent avoir plusieurs ports de connexion pour la redondance. Les ports de connexion d'un nœud d'extrémité peuvent être connectés au même réseau LAN ou à différents réseaux LAN.

Les nœuds d'extrémité à plusieurs associations nécessitent une entité de redondance de liaison (LRE, Link Redundancy Entity) dans leur pile de communication afin de masquer la redondance de l'application, comme le montre la Figure 3.



Légende

Anglais	Français
Upper layers	Couches supérieures
Hard real-time stack	Pile temps réel matérielle
Network layer	Couche réseau
Same link layer interface	Même interface liaison de données
Link redundancy entity	Entité de redondance de liaison
Network adapters	Adaptateurs réseau
Port A	Port A
Port B	Port B
Transceivers	Émetteurs-récepteurs

Figure 3 – Entité de redondance de liaison dans un nœud à double association (DAN)

Un nœud d'extrémité connecté à un ou deux LAN du même réseau par le biais de deux liaisons en feuille est un nœud à double association (DAN, Doubly Attached Node).

Un nœud d'extrémité connecté à un ou plusieurs LAN du même réseau par le biais de quatre liaisons en feuille est un nœud à quadruple association (QAN, Quadruply Attached Node).

NOTE Les nœuds d'extrémité utilisant différents ports de communication pour les réseaux indépendants ne sont pas considérés ici, les considérations s'appliquent à chaque réseau séparément.

Copyright International Electrotechnical Commission

5.2.2 Topologies

5.2.2.1 Généralités

La redondance dans le réseau considère la présence de plus d'éléments de réseau que nécessaire (commutateurs, liaisons) pour le fonctionnement, afin d'empêcher la perte de la communication provoquée par une défaillance. À cet effet, il y a plus d'un chemin physique entre deux nœuds d'extrémité.

L'IEC 61918 spécifie différentes sortes de topologies physiques de base, certaines de celles-ci étant utilisées par la série IEC 62439 pour définir différentes topologies.

a) Topologies sans redondance
   - Topologie en arbre (Figure 4);
   - Topologie linéaire (Figure 5).

b) Topologies avec des liaisons redondantes
   - Topologie en anneau (Figure 6);
   - Topologie partiellement maillée (Figure 7);
   - Topologie entièrement maillée (Figure 8).

Il existe quatre structures de haut niveau:

- LAN simple sans liaisons en feuille redondantes (voir 5.2.2.4.1);
- LAN simple avec liaisons en feuille redondantes (voir 5.2.2.4.2);
- LAN redondants sans liaisons en feuille redondantes (voir 5.2.2.4.3);
- LAN redondants avec liaisons en feuille redondantes (voir 5.2.2.4.4).

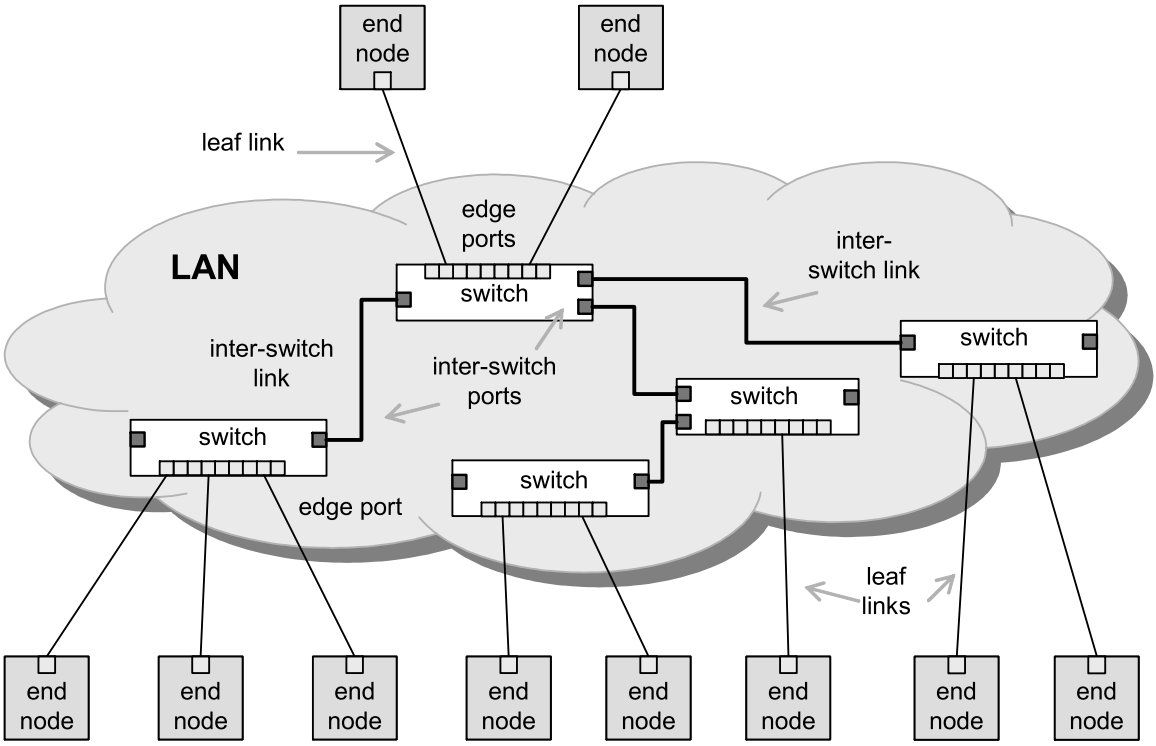
Lorsque la redondance est gérée dans le LAN, les nœuds d'extrémité peuvent être connectés par une simple association. Dans le cas d'une défaillance de commutateur ou de la liaison en feuille, ces nœuds d'extrémité peuvent perdre la communication.

5.2.2.2 Topologies sans redondance

5.2.2.2.1 Topologie en arbre

Dans une topologie en arbre, au moins un commutateur dispose de plus de deux mailles inter-étage et il n'y a qu'un seul chemin entre deux appareils quelconques. La Figure 4 montre un exemple d'une topologie en arbre.

Copyright International Electrotechnical Commission



Légende *IEC 331/10*

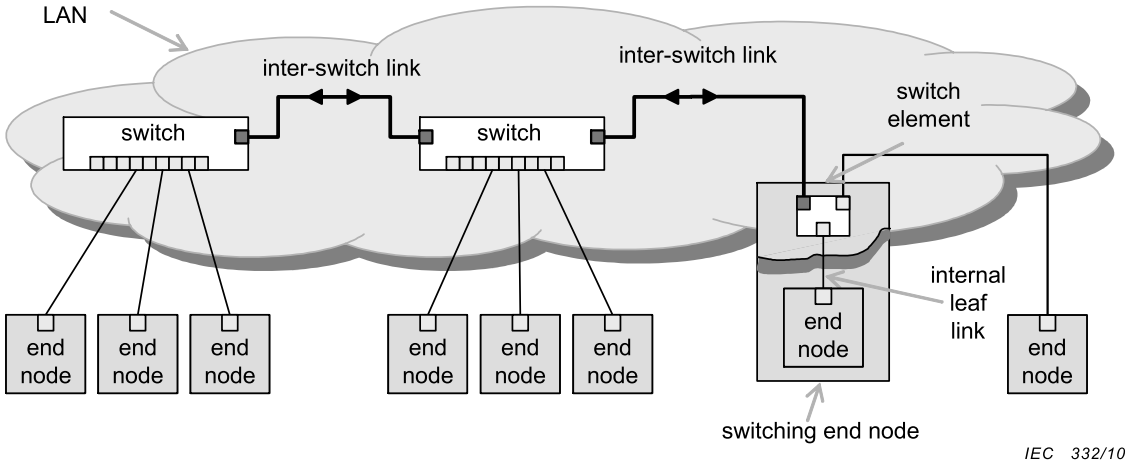
Anglais	Français
End node	Nœud d'extrémité
Leaf link	Liaison en feuille
Edge ports	Ports d'extrémité
Inter switch port	Port inter-étage
Inter switch link	Maille inter-étage
Switch	Commutateur

Figure 4 – Exemple d'une topologie en arbre

5.2.2.2.2 Topologie linéaire

Dans une topologie linéaire, tous les commutateurs sont connectés les uns aux autres en ligne et aucun nœud ne dispose de plus de deux mailles inter-étage, mais les deux nœuds situés à l'extrémité de la ligne n'ont qu'une seule maille inter-étage. La Figure 5 montre un exemple d'une topologie linéaire.

Copyright International Electrotechnical Commission



Légende

Anglais	Français
Inter switch link	Maille inter-étage
Switch	Commutateur
Switch element	Élément de commutateur
Internal leaf link	Liaison en feuille interne
End node	Nœud d'extrémité
Switching end node	Nœud d'extrémité de commutation

Figure 5 – Exemple d'une topologie linéaire

NOTE Un nœud peut être un nœud d'extrémité de commutation, comme montré dans le deuxième nœud d'extrémité à partir de la droite de la Figure 5.

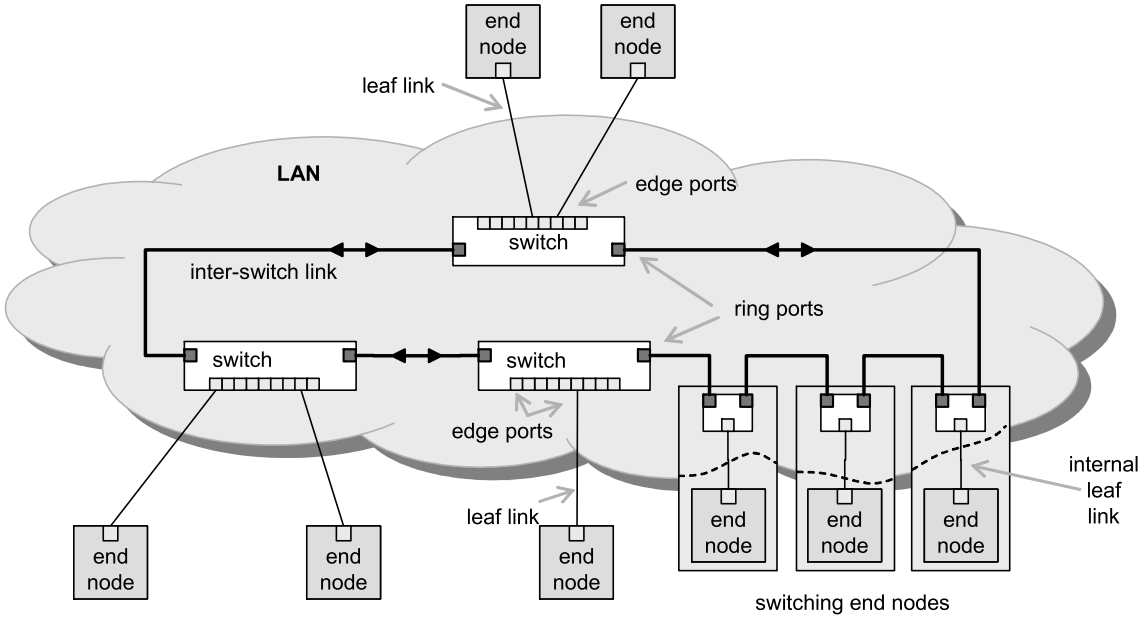
5.2.2.3 Topologies avec des liaisons redondantes

5.2.2.3.1 Topologie en anneau

NOTE Cette topologie s'applique à la redondance du RSTP (voir Article 7), du MRP (IEC 62439-2) et du DRP (IEC 62439-6).

Dans une topologie en anneau, chaque commutateur possède deux mailles inter-étage et deux nœuds d'extrémité quelconques ont deux chemins entre eux lorsque tous les composants sont opérationnels. La Figure 6 montre un exemple d'une topologie en anneau.

Copyright International Electrotechnical Commission



Légende

Anglais	Français
End node	Nœud d'extrémité
Leaf link	Liaison en feuille
Edge ports	Ports d'extrémité
Switch	Commutateur
Inter switch link	Maille inter-étage
Ring ports	Ports d'anneau
Internal leaf link	Liaison en feuille interne
Switching end node	Nœud d'extrémité de commutation

Figure 6 – Exemple d'une topologie en anneau

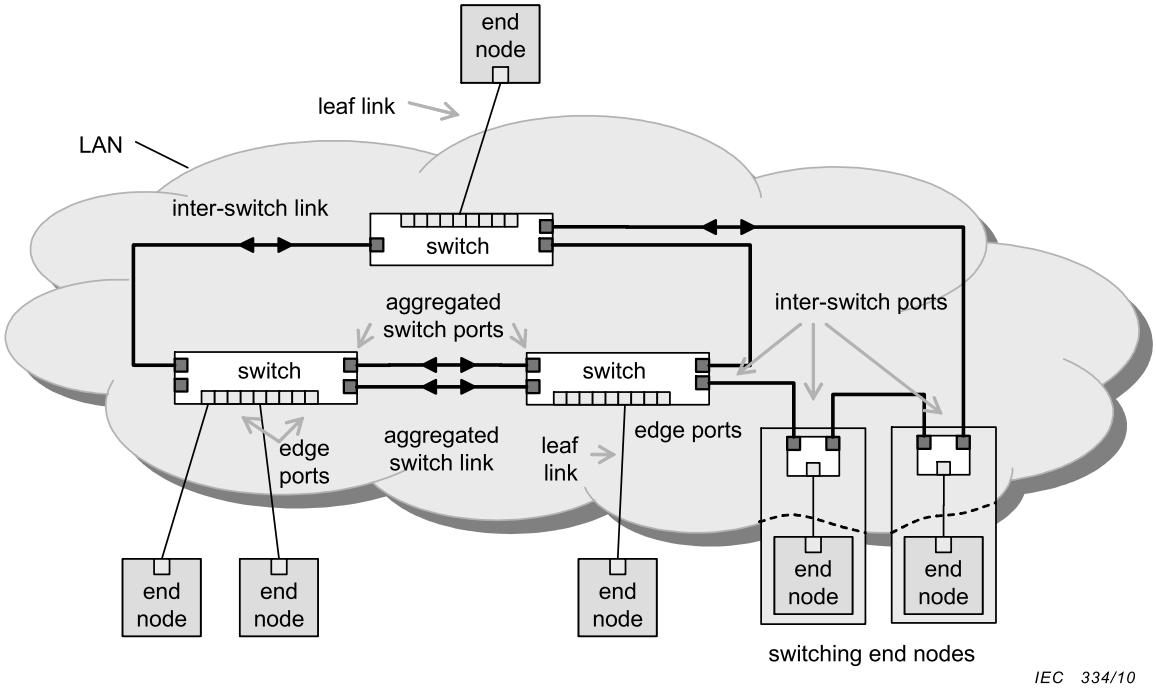
Une topologie en anneau présente une boucle dans le LAN qui pourrait conduire à des inondations causées par des trames en circulation permanente. Les protocoles tels que le protocole RSTP (Rapid Spanning Tree) et le protocole MRP (Media Redundancy Protocol) assurent que les commutateurs maintiennent une topologie linéaire logique lors de l'initialisation, l'exploitation et la reconfiguration.

Si un commutateur ou une maille inter-étage tombe en panne, le commutateur est exclu de l'anneau, et une nouvelle topologie linéaire logique est établie. Cependant, les nœuds d'extrémité connectés à un commutateur en panne perdent la connectivité.

5.2.2.3.2 Topologie partiellement maillée

Dans une topologie partiellement maillée, au moins un commutateur possède plus de deux mailles inter-étage et il existe plus d'un chemin entre quelques appareils. La Figure 7 montre un exemple d'une topologie partiellement maillée.

Copyright International Electrotechnical Commission



Légende

Anglais	Français
End node	Nœud d'extrémité
Leaf link	Liaison en feuille
Inter switch link	Maille inter-étage
Switch	Commutateur
Aggregated switch ports	Ports de commutateur d'agrégation
Inter-switch ports	Ports inter-étage
Edge ports	Ports d'extrémité
Aggregated switch link	Liaison de commutateur d'agrégation
Switching end nodes	Nœuds d'extrémité de commutation

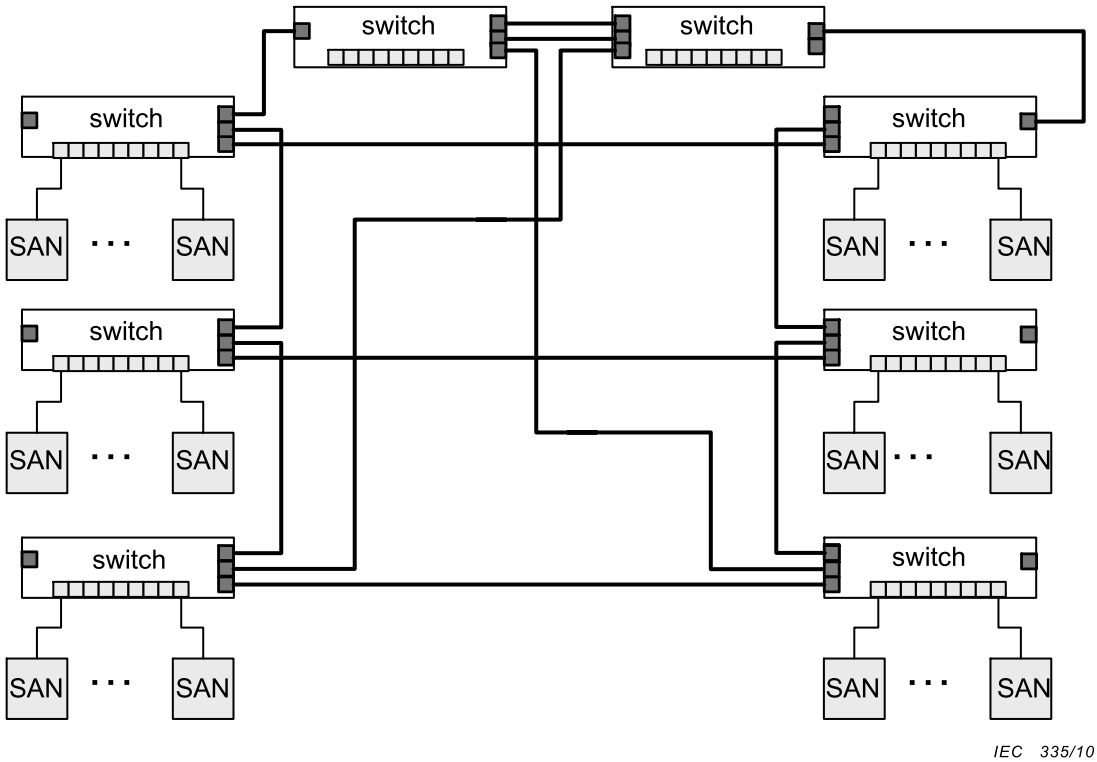
Figure 7 – Exemple d'une topologie partiellement maillée

5.2.2.3.3 Topologie entièrement maillée

Dans une topologie entièrement maillée, chaque commutateur possède plusieurs mailles inter-étage.

Dans une topologie entièrement maillée, la défaillance d'une maille inter-étage ou d'un commutateur peut être tolérée. Cependant, les nœuds d'extrémité connectés à un commutateur en panne perdent la connectivité. La Figure 8 montre un exemple d'une topologie entièrement maillée.

Copyright International Electrotechnical Commission



Légende

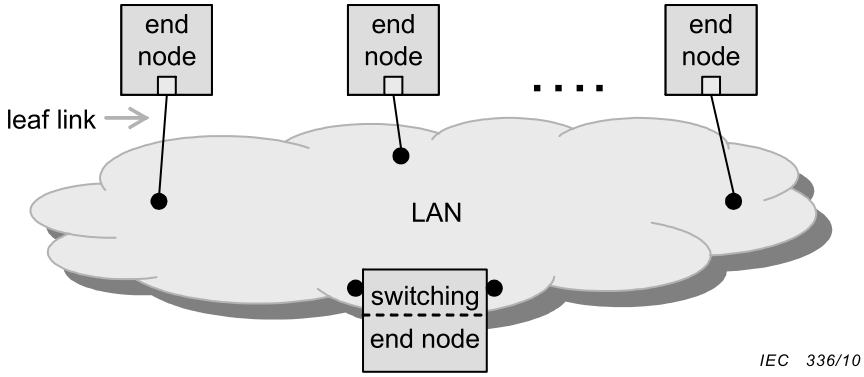
Anglais	Français
Switch	Commutateur

Figure 8 – Exemple d'une topologie entièrement maillée

5.2.2.4 Structures de haut niveau de réseaux

5.2.2.4.1 LAN simple sans liaisons en feuille redondantes

Cette topologie possède un seul chemin entre deux nœuds (voir Figure 9).



Légende

Anglais	Français
End node	Nœud d'extrémité
Leaf link	Liaison en feuille
Switching end node	Nœud d'extrémité de commutation

Figure 9 – Structure de LAN simple sans liaisons en feuille redondantes

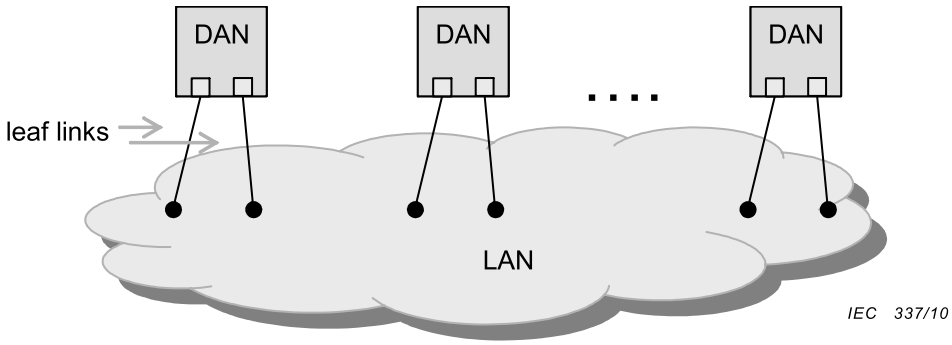
Des exemples de cette topologie sont la topologie en arbre et la topologie linéaire (voir Figure 4 et Figure 5).

Copyright International Electrotechnical Commission

5.2.2.4.2 LAN simple avec feuilles redondantes

NOTE Cette topologie s'applique, par exemple, à des nœuds comportant un commutateur RSTP ou un sous-ensemble de ceux-ci.

Les nœuds à double association (DAN) sont connectés au même LAN par le biais des liaisons en feuille. Chaque port d'extrémité peut appartenir au même commutateur ou à différents commutateurs. La Figure 10 montre un exemple.



Légende

Anglais	Français
Leaf links	Liaisons en feuille

Figure 10 – Structure de LAN simple avec liaisons en feuille redondantes

5.2.2.4.3 Réseau sans feuilles redondantes

NOTE Cette topologie s'applique au PRP (voir IEC 62439-3), au CRP (voir IEC 62439-4) et au BRP (voir IEC 62439-5).

Dans ce type de topologie, les chemins ne se chevauchent pas. Les liaisons en feuille redondantes sont connectées à des LAN différents. Un exemple est montré à la Figure 11.

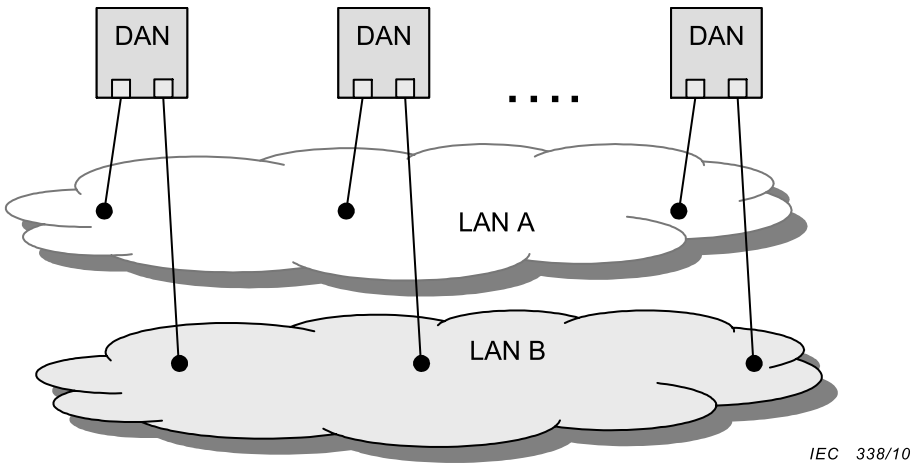


Figure 11 – Structure de LAN redondant sans liaisons en feuille redondantes

5.2.2.4.4 LAN redondant avec liaisons en feuille redondantes

Les liaisons en feuille redondantes sont connectées à la fois au même LAN et à des LAN différents. Les nœuds sont des nœuds à association quadruple (QAN). Un exemple est montré à la Figure 12.

Copyright International Electrotechnical Commission

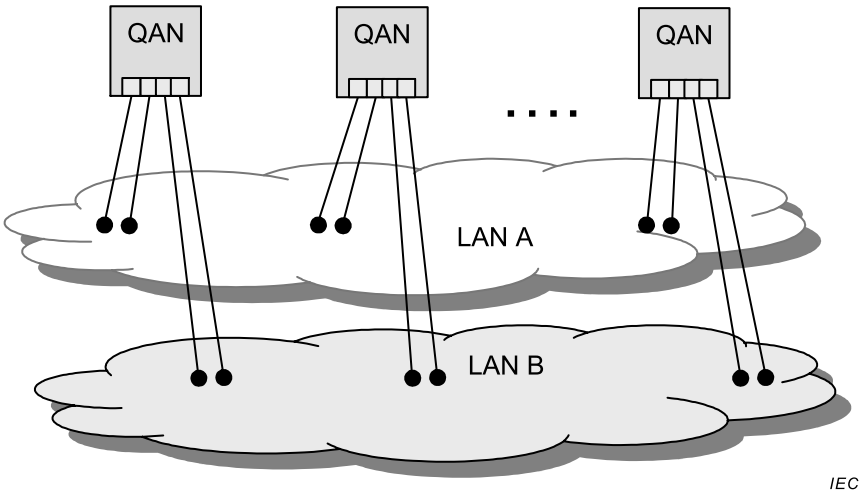


Figure 12 – Structure de LAN redondant avec liaisons en feuille redondantes

5.2.3 Gestion de la redondance

5.2.3.1 Mode secours

En mode secours, seul l'un des chemins redondants est choisi comme chemin en service alors que les autres chemins restent en veille.

Si le chemin en service devient indisponible, un autre chemin le remplace.

Durant le temps écoulé depuis la perte du chemin en service jusqu'au début de fonctionnement du chemin de secours, des messages peuvent être perdus et, par conséquent, la voie est considérée être en état déconnecté.

NOTE Le VEI appelle ce type de redondance, une redondance “en attente (stand-by)” ou “passive”. Le terme «redondance dynamique» est également utilisé.

5.2.3.2 Mode alterné (actif)

En mode alterné, les chemins redondants sont utilisés en alternance, de manière aléatoire ou selon des modèles réguliers, et les messages sont émis par l'intermédiaire de l'un des chemins redondants.

Si l'on détecte que l'un des chemins redondants est en état déconnecté, ce chemin cesse d'être utilisé pendant que les autres chemins continuent à être utilisés en alternance.

Ce mode permet de vérifier la disponibilité des composants en permanence et augmente ainsi la couverture.

5.2.3.3 Fonctionnement parallèle (actif)

En fonctionnement parallèle, les messages sont émis par l'intermédiaire de tous les chemins redondants disponibles.

Le nœud d'extrémité destinataire sélectionne l'un des messages reçus.

NOTE Le terme “redondance statique” ou “work-by” est aussi utilisé.

5.2.4 Temps de reprise du réseau

Le temps de reprise du réseau est appelé temps de reprise ("recovery time") dans la série IEC 62439 parce que la série IEC 62439 traite seulement les réseaux. La définition donnée en 3.1.41 s'applique.

Copyright International Electrotechnical Commission

5.2.5 Couverture de diagnostic

Les pannes sont détectées par des mécanismes de détection d'erreurs qui détectent seulement un pourcentage des pannes. La couverture est la probabilité que les mécanismes de diagnostic détectent une erreur dans un délai permettant le rétablissement avant que d'autres mécanismes ne prennent l'action de protéger l'installation ou avant que l'installation ne subisse de dommages.

5.2.6 Défaillances

5.2.6.1 Sortes de défaillances

Il existe trois sortes de défaillances:

- défaillance passagère,
- défaillance de composant et
- défaillance systématique.

Elles affectent les éléments suivants:

- les nœuds d'extrémité,
- les liaisons en feuille,
- les commutateurs,
- les mailles inter-étage.

5.2.6.2 Défaillance passagère

Une défaillance passagère, comme les interférences électromagnétiques, provoque des erreurs passagères qui laissent le matériel essentiellement intact, mais en perturbent la fonction. Dans ce cas, la partie défaillante peut être automatiquement réintégrée après des essais automatiques. De tels mécanismes sont partiellement mis en œuvre dans les protocoles de redondance spécifiés dans la série IEC 62439.

NOTE Les interférences EM peuvent devenir des défaillances systématiques.

5.2.6.3 Défaillance de composant

La défaillance d'un composant peut être partielle ou complète. Seules les défaillances complètes de composants (non temporaires, non parasites) sont prises en compte dans la série IEC 62439.

5.2.6.4 Défaillance systématique

Une défaillance systématique affecte plusieurs composants redondants en même temps; il s'agit par conséquent d'un point unique de défaillance. Les erreurs de configuration appartiennent aussi à cette catégorie. Les protocoles de redondance spécifiés dans la série IEC 62439 ne considèrent pas les défaillances systématiques mais permettent d'en détecter quelques-unes.

NOTE La diversité de la conception est éventuellement en mesure de réduire l'impact de défaillance systématique.

5.2.6.5 Défaillance d'un nœud d'extrémité

La défaillance d'un nœud d'extrémité est en dehors du domaine d'application de la série IEC 62439.

5.2.6.6 Défaillance d'une liaison en feuille

La défaillance d'une liaison en feuille est provoquée par:

Copyright International Electrotechnical Commission

- la défaillance du port de connexion d'un nœud d'extrémité,
- la défaillance du câble d'une liaison en feuille, ou
- la défaillance du port d'extrémité.

5.2.6.7 Défaillance d'un commutateur

Un commutateur se compose d'une fonctionnalité commutateur cœur (par exemple processeur, alimentation) et d'un nombre de ports.

Pour des besoins de calcul, une défaillance de commutateur ne considère que la défaillance de la fonction commutateur cœur.

La défaillance d'un port d'extrémité du commutateur est considérée comme une défaillance de la liaison en feuille.

La défaillance d'un port inter-étage du commutateur est considérée comme une défaillance de maille inter-étage.

5.2.6.8 Défaillance d'une maille inter-étage

La défaillance de maille inter-étage est provoquée par:

- la défaillance du port inter-étage ou
- la défaillance du câble de la maille inter-étage.

5.3 Sûreté

La série IEC 62439 ne considère pas les aspects de sûreté, par exemple, l'intégrité.

NOTE Même si la sûreté n'est pas directement traitée, une haute fiabilité est une caractéristique souhaitable dans un système de sûreté.

5.4 Sécurité

La série IEC 62439 ne considère pas les problématiques de sécurité (par exemple l'aspect privé, l'authentification).

6 Classification de réseaux (informative)

6.1 Notation

La structure de réseau relative à un réseau hautement disponible est exprimée par la notation suivante:

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

où

TYPE	indique le type de structure redondante de haut niveau;
NUMsn	indique le nombre de LAN redondants;
PLCYleaf	indique la politique de la redondance de liaison en feuille;
NUMleaf	indique le nombre de feuilles redondantes;
TPLGY	indique la topologie LAN.

EXEMPLE “A1N1RB” représente un réseau en anneau simple sans redondance de liaison en feuille.

Le champ <TYPE> est défini dans le Tableau 3.

Copyright International Electrotechnical Commission

Tableau 3 – Affectation de code pour le champ <TYPE>

Code	Structure redondante de haut niveau
A	Structure de LAN simple sans feuilles redondantes
B	Structure de LAN simple avec feuilles redondantes
C	Structure de LAN redondants sans feuilles redondantes
D	Structure de LAN redondants avec feuilles redondantes

Le champ <PLCYleaf> est défini dans le Tableau 4.

Tableau 4 – Affectation de code pour le champ <PLCYleaf>

Code	Politique relative à la redondance de liaison en feuille
P	Fonctionnement parallèle
A	Fonctionnement alterné
B	Fonctionnement secours
O	Autre politique redondante
N	N'est pas applicable ou pas de redondance de liaison en feuille

Le champ <TPLGY> est défini dans le Tableau 5.

Tableau 5 – Affectation de code pour le champ <TPLGY>

Code	Topologie LAN
S	Topologie simplex
R	Topologie en anneau
P	Topologie partiellement maillée
M	Topologie entièrement maillée
O	Autre topologie

6.2 Classification de robustesse

La robustesse d'un réseau hautement disponible est exprimée par la notation suivante:

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

où

ITYPE indique l'impact à considérer;

NUMleaf indique le nombre de défaillances des liaisons en feuille, acceptable pour le fonctionnement du réseau;

NUMtrunk indique le nombre de défaillances des mailles inter-étage, acceptable pour le fonctionnement du réseau;

NUMsw indique le nombre de défaillances des commutateurs, acceptable pour le fonctionnement du réseau.

Le champ <ITYPE> est défini dans le Tableau 6.

Copyright International Electrotechnical Commission

Tableau 6 – Affectation de code pour le champ <ITYPE>

code	Impact pour la classification de robustesse
N	Aucun impact n'est observé
R	Chaque nœud d'extrémité est capable de communiquer avec tous les autres nœuds d'extrémité, mais il y a une certaine période d'interruption
L	Un nombre limité de nœuds d'extrémité n'est pas en mesure de communiquer, mais d'autres nœuds d'extrémité sont en mesure de communiquer en présence d'une certaine interruption

EXEMPLE "R-L0T1S0" signifie que la défaillance d'une maille inter-étage n'affecte pas l'exploitation du réseau, sauf pour une certaine période d'interruption, mais la défaillance d'une liaison en feuille ou d'un commutateur n'est pas résolue par la redondance.

7 Calculs de disponibilité pour les réseaux sélectionnés (informative)

7.1 Définitions

Le réseau est considéré comme fonctionnel si chaque nœud d'extrémité est capable de communiquer avec tout autre nœud d'extrémité dans le réseau. Il est supposé que l'installation devienne indisponible si le réseau d'automatisation ne fonctionne pas.

NOTE 1 Cette définition peut être assouplie si une dégradation progressive est envisagée, mais cela dépend de l'application et n'est pas considérée ici.

La disponibilité du réseau est définie comme étant la fraction de temps pendant laquelle le réseau est fonctionnel, durant toute sa durée de vie. Le MTTF du réseau est la durée moyenne à partir d'un bon état initial jusqu'à la défaillance d'un composant. Supposons que la disponibilité est haute, le MTTF est légèrement égal au temps moyen entre défaillances (MTBF, Mean Time Between Failures), qui est le temps moyen entre les appels de maintenance.

Puisque la durée de vie du réseau est beaucoup plus longue que le MTTF, le chiffre qui décrit le mieux le comportement du réseau dans des conditions de panne est la durée moyenne de fonctionnement avant défaillance du réseau ou MTTFN.

La disponibilité du réseau est ainsi déduite en Équation (1):

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

où

MTTFN est la durée moyenne de fonctionnement avant défaillance du réseau, et

MTTRN (Mean Time To Repair Network) est la moyenne des temps pour la tâche de réparation.

NOTE 2 La disponibilité de l'installation est plus faible car il y a d'autres causes de défaillance à part celle du réseau et car le temps de restaurer l'installation après une défaillance du réseau est plus important que le temps de réparer le réseau.

Les taux de défaillance des éléments suivants sont considérés en cas d'utilisation:

λ_L = taux de défaillance des liaisons en feuille y compris les deux ports;

λ_S = taux de défaillance des commutateurs cœur, sans considérer les ports;

λ_T = taux de défaillance des mailles inter-étage y compris les deux ports.

Copyright International Electrotechnical Commission

NOTE 3 Le taux de défaillance s'applique au réseau uniquement, la fiabilité de l'application dans un appareil n'est pas considéré.

NOTE 4 Pour les besoins de calculs dans les exemples suivants, un exemple de réseau est considéré et consiste, dans le cas non redondant, de 5 commutateurs à 8 ports chacun, connectés en anneau. Les taux de défaillance types des éléments qui sont utilisés dans les exemples suivants sont:

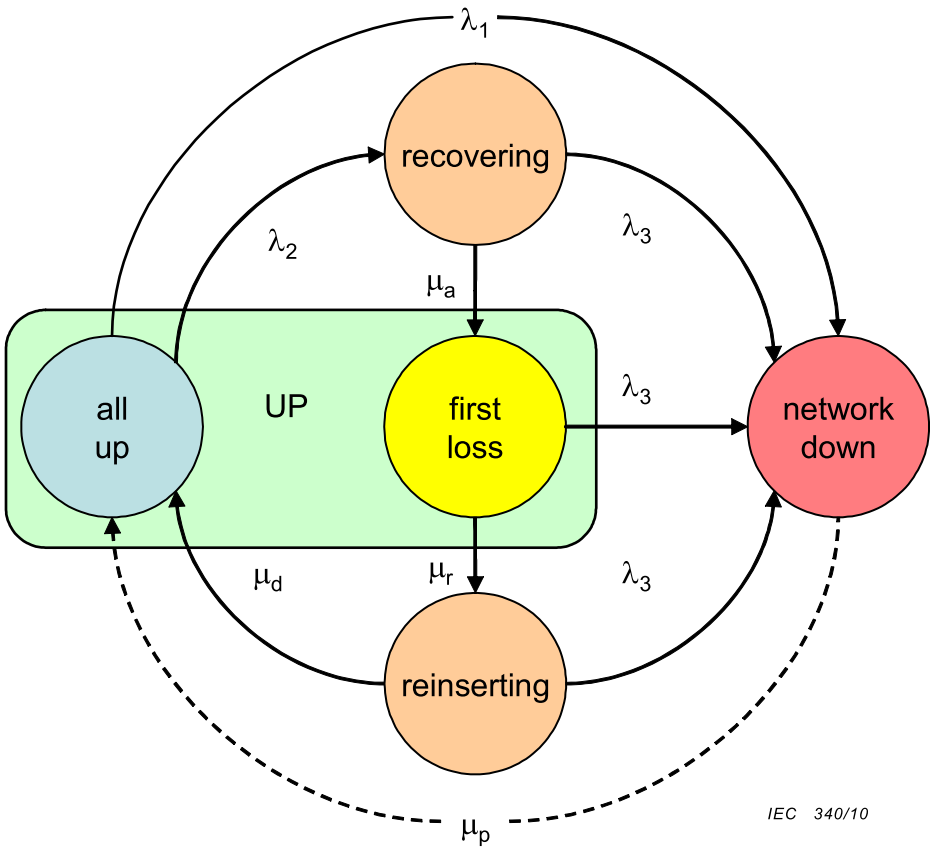
$$\lambda_S = 1 / \text{MTTFswitch} = 1/100 \text{ ans}$$

$$\lambda_L = \lambda_T = 1 / \text{MTTFlink} = 1/50 \text{ ans (liaison cuivre ou optique)}$$

7.2 Modèles de fiabilité

7.2.1 Modèle de fiabilité générique symétrique

Le modèle général de panne d'un réseau composé de parties redondantes et non redondantes est montré à la Figure 13. Ce modèle symétrique suppose que les rôles d'une unité principale et de son unité de secours ("stand-by" ou "work-by") soient interchangeables; c'est-à-dire qu'une fois que le réseau fonctionne avec l'unité de secours, il n'est pas nécessaire de basculer vers l'ancienne unité principale après la réparation.



Légende

Anglais	Français
Recovering	Rétablissement
All up	Tout en fonctionnement
First loss	Première perte
Network down	Réseau en panne
Reinserting	Réinsertion

Figure 13 – Modèle de panne générique symétrique

Copyright International Electrotechnical Commission

Les transitions sont:

λ_1 = taux de défaillance des composants non redondants
(y compris le point unique de défaillance et la probabilité d'un rétablissement non réussi)

λ_2 = taux de défaillance des composants redondants
(pour lesquels il existe une redondance et le rétablissement est réussi)

λ_3 = taux de défaillance des composants restants

μ_a = taux de rétablissement automatique
(durée entre l'apparition d'une panne et son rétablissement)

μ_d = taux d'interruption
(temps moyen d'interruption du réseau causée par la réinsertion)

μ_r = taux de rétablissement
(durée entre l'apparition d'une panne et la restauration de la redondance, inclut la réparation en ligne)

μ_p = taux de réparation de l'installation
(durée depuis l'apparition d'une panne non récupérable jusqu'à ce que l'installation soit remontée de nouveau)

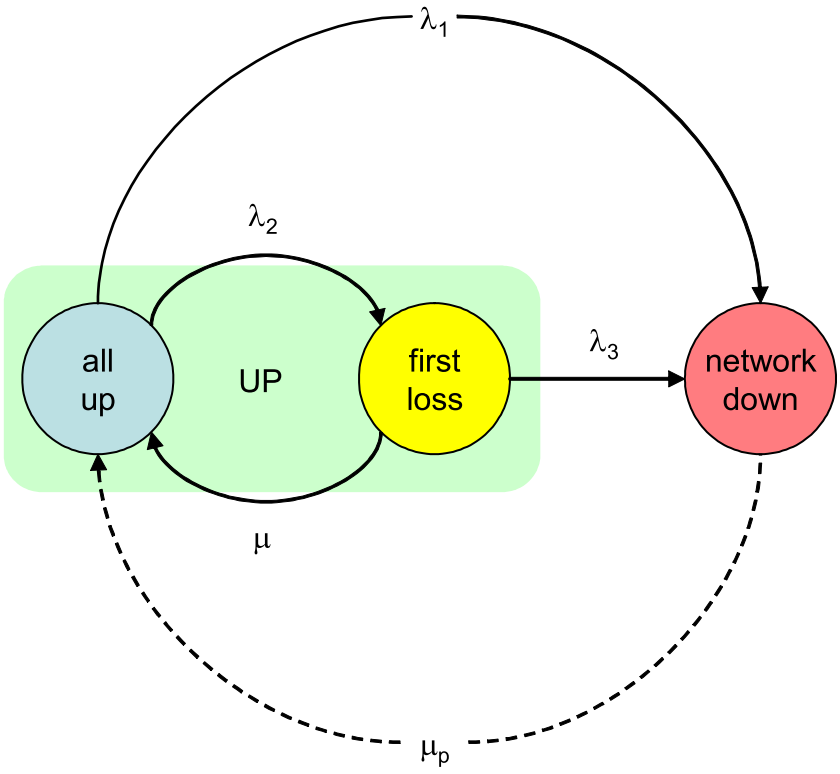
NOTE Les pannes inaperçues sont prises en compte dans μ_r et λ_1 plutôt que par l'introduction d'un état supplémentaire.

Ce modèle observe deux courtes interruptions: sur une première défaillance, il y a un temps court de reprise de panne pour activer la redondance; après la réparation, il y a un temps court de reprise de réinsertion de redondance pour restaurer le fonctionnement redondant. Tant que ces interruptions restent en dessous du temps d'interruption acceptable, elles n'affectent pas les calculs de disponibilité.

7.2.2 Modèle de fiabilité simplifié symétrique

Supposons que le réseau passe un temps très court dans les états de "rétablissement" et de "réinsertion", ces états peuvent être regroupés dans l'état "première perte", comme le montre la Figure 14.

Copyright International Electrotechnical Commission



Légende

Anglais	Français
All up	Tout en fonctionnement
First loss	Première perte
Network down	Réseau en panne

Figure 14 – Modèle de panne simplifié

La solution générale du modèle simplifié est exprimée dans l'Équation (2):

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

où

λ_2 est le taux de défaillance des composants redondants;
λ_3 est le taux de défaillance des composants restants;
μ est le taux de réparation.

Il serait en principe nécessaire d'introduire des transitions et des états relatifs à la défaillance des commutateurs et à la défaillance des liaisons. Cependant, puisque le réseau est constitué d'un grand nombre d'éléments et les taux de défaillance des commutateurs et des liaisons ne sont pas trop différents, un seul état "première défaillance" peut être utilisé.

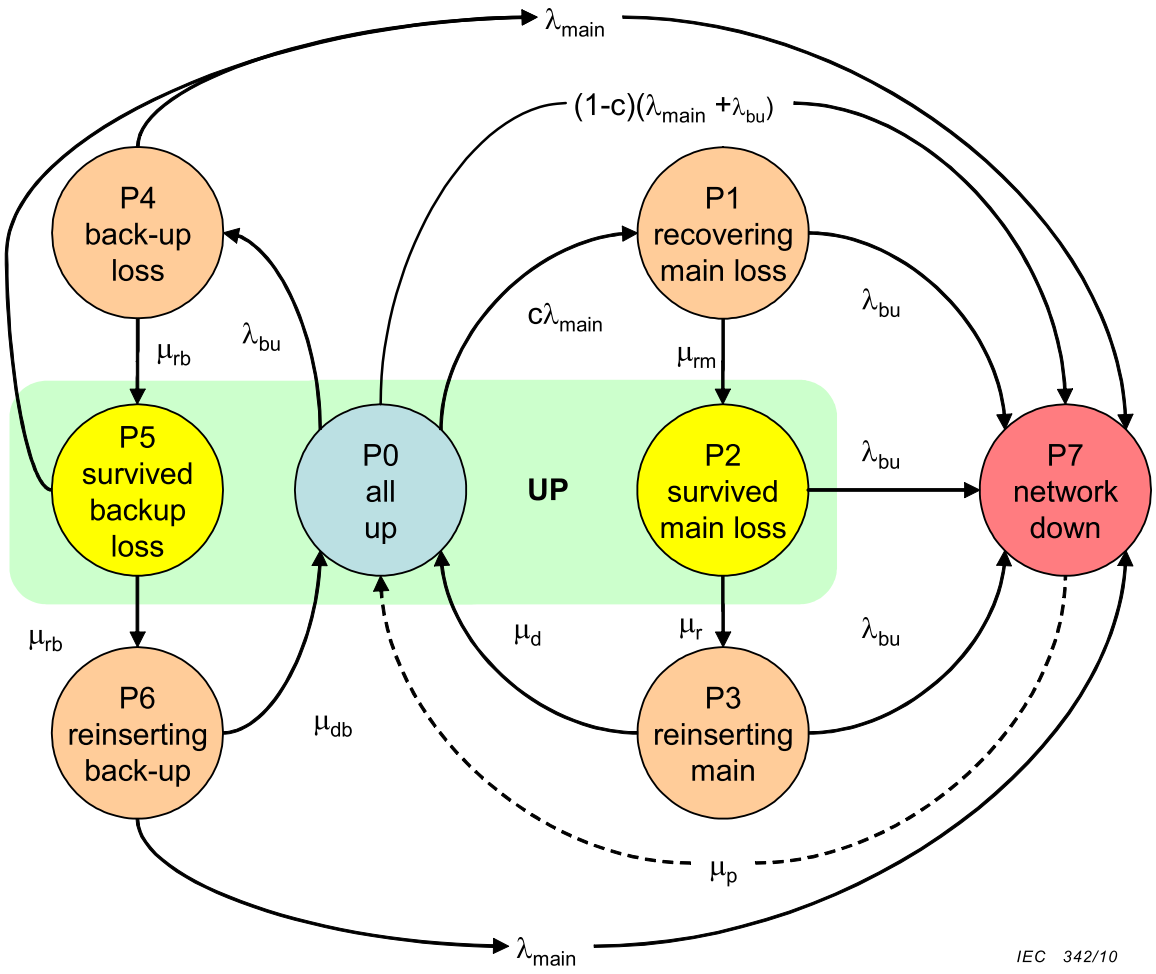
7.2.3 Modèle de fiabilité asymétrique

Dans de nombreux cas, le rôle principal et le rôle de secours ne sont pas interchangeables. Une redondance complète n'est rétablie que lorsque l'unité principale d'origine est de nouveau en place. Par conséquent, le modèle asymétrique considère plus d'interruptions, comme le montre la Figure 15. Les transitions de ce modèle ne sont pas détaillées car ce modèle est inclus seulement pour rappeler d'envisager d'éventuelles interruptions supplémentaires. Comme dans le cas précédent, les états d'interruption P1, P2, P4 et P6

Copyright International Electrotechnical Commission

n'ont aucune influence sur les calculs de la sûreté de fonctionnement tant que leur durée reste inférieure au temps d'interruption maximal acceptable.

NOTE Par analogie, considérer une voiture où la roue de secours est utilisée en cas d'urgence seulement et est destinée uniquement à atteindre en toute sécurité le prochain garage. Quand un pneu est crevé, deux changements de pneu sont nécessaires afin de rétablir le fonctionnement normal. En revanche, lorsque la roue de secours est identique à celle qu'elle remplace, une seule interruption est nécessaire.



Légende

Anglais	Français
P4 Backup loss	P4 Perte du secours
P1 Recovering main loss	P1 Rétablissement de la perte principale
P5 Survived backup loss	P5 Survit à une perte du secours
P0 All up	P0 Tout en bon fonctionnement
UP	EN BON FONCTIONNEMENT
P2 Survived main loss	P2 Survit à une perte du principal
P7 Network down	P7 Réseau en panne
P6 Reinserting backup	P6 Réinsertion du secours
P3 Reinserting main	P3 Réinsertion du principal

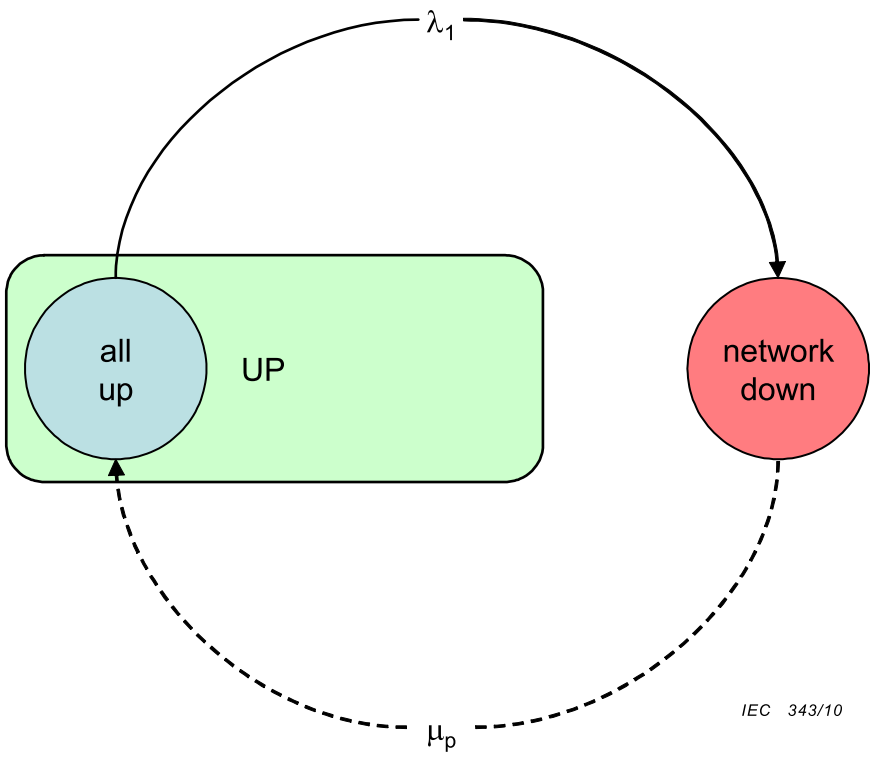
Figure 15 – Modèle de panne asymétrique

Copyright International Electrotechnical Commission

7.3 Disponibilité des structures sélectionnées

7.3.1 LAN simple sans feuilles redondantes

Dans un réseau non redondant, la défaillance d'un élément quelconque entraîne la défaillance du réseau, comme le montre la Figure 16 .



Légende

Anglais	Français
All up	Tout en bon fonctionnement
UP	En bon fonctionnement
Network down	Réseau en panne

Figure 16 – Réseau sans redondance

Par conséquent, le MTTFN se simplifie en Équation (3).

$$MTTFN = \frac{1}{\lambda_1} \tag{3}$$

où $\lambda_1 = \Sigma (\lambda_L + \lambda_S + \lambda_T)$

EXEMPLE Pour l'exemple de réseau (5 commutateurs, 40 liaisons en feuille, 5 mailles inter-étage)

MTTFN = 1,05 an et

MTTF = 1,05 an.

7.3.2 Réseau sans feuilles redondantes

Dans l'hypothèse où le taux de réparation est beaucoup plus élevé que le taux de défaillance, seule la fiabilité des liaisons en feuille importe et l'Équation (3) se réduit à l'Équation (4):

Copyright International Electrotechnical Commission

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

où $\lambda_1 = \Sigma (\lambda_L)$, sachant que tous les commutateurs et les mailles inter-étage sont redondants.

Cela signifie que, si le taux de réparation est assez élevé (MTTR en quelques jours par rapport à quelques années de MTTF), la fiabilité est entièrement dictée par les parties non redondantes du réseau et que la redondance permet simplement de négliger les éléments redondants dans le calcul du MTTFN.

EXEMPLE Pour l'exemple de réseau (5 commutateurs, 40 liaisons en feuille non redondantes, 6 mailles inter-étage)

MTTFN = 1,17 an

MTTF = 1,03 an.

NOTE Dans le cas de nœuds d'extrémité de commutation, le MTTFN est beaucoup plus élevé, car les liaisons en feuille sont internes aux nœuds et sont prises en compte dans le taux de défaillance des nœuds.

7.3.3 LAN simple avec feuilles redondantes

Dans ce cas, le taux de défaillance des liaisons en feuille peut être ignoré. Comme le nombre de ports par commutateur est supposé être constant, le nombre de commutateurs est doublé.

EXEMPLE Pour l'exemple de réseau (10 commutateurs, 80 liaisons en feuille redondantes, 11 mailles inter-étage redondantes):

MTTFN = 9,78 an

MTTF = 0,52 an.

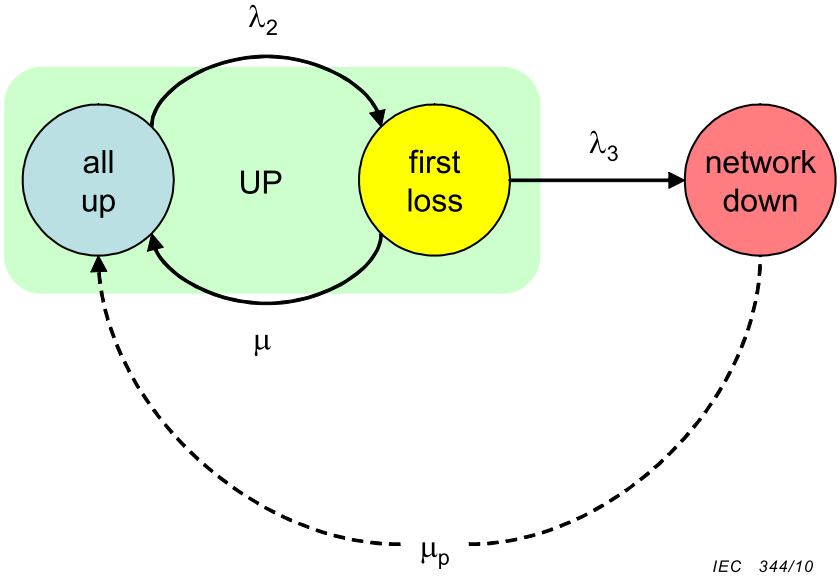
NOTE 1 Cela montre que l'augmentation de la fiabilité obtenue par une double association de nœuds est réduite par le nombre croissant de commutateurs qui sont nécessaires. Le MTTF double par rapport au cas non redondant puisque le nombre de liaisons et de ports a doublé. Par conséquent, cette structure n'a de sens que dans le contexte d'une dégradation progressive, où les appareils importants possèdent une association redondante, mais ne nécessitent pas de connectivité avec tous les nœuds d'extrémité.

NOTE 2 Dans le cas de nœuds d'extrémité de commutation, le MTTFN est beaucoup plus élevé, car les liaisons en feuille sont internes aux nœuds et leur non-fiabilité est considérée dans le taux de défaillance des nœuds.

7.3.4 Réseau avec feuilles redondantes

Supposons que tous les éléments du réseau soient redondants, le taux de défaillance λ_1 est réduit à un point unique de défaillance et aux défaillances de rétablissement/réinsertion. Si celles-ci peuvent être négligées par une conception appropriée, le modèle de fiabilité est donné à la Figure 17.

Copyright International Electrotechnical Commission



Légende

Anglais	Français
All up	Tout en bon fonctionnement
UP	EN BON FONCTIONNEMENT
First loss	Première perte
Network down	Réseau en panne

Figure 17 – Réseau sans point unique de défaillance

Le MTTFN se simplifie en Équation (5):

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

où $\lambda_2 = \Sigma (\lambda_L + \lambda_S + \lambda_T)$ et $\lambda_3 = \lambda_2/2$

Le taux de défaillance λ_3 des éléments restants est supposé être la moitié de celui du réseau entier, puisque les secondes défaillances du LAN déjà dégradé n'affectent pas le fonctionnement.

Le MTTFN est légèrement augmenté par rapport au cas non redondant deux fois le rapport du taux de réparation sur le taux de défaillance, ce qui est généralement élevé, par exemple MTTR = 24 heures par rapport au MTTF = 1 an.

EXEMPLE Pour l'exemple de réseau (2 × 5 commutateurs, 2 × 40 liaisons en feuille, 2 × 6 mailles inter-étage):

MTTFN = 196 an.

MTTF = 0,58 an.

NOTE 1 Cela montre que même si le réseau est entièrement redondant, la disponibilité est encore limitée et que la duplication du réseau provoque le double d'un taux de maintenance élevé, puisqu'il y a deux fois plus d'éléments pouvant tomber en panne.

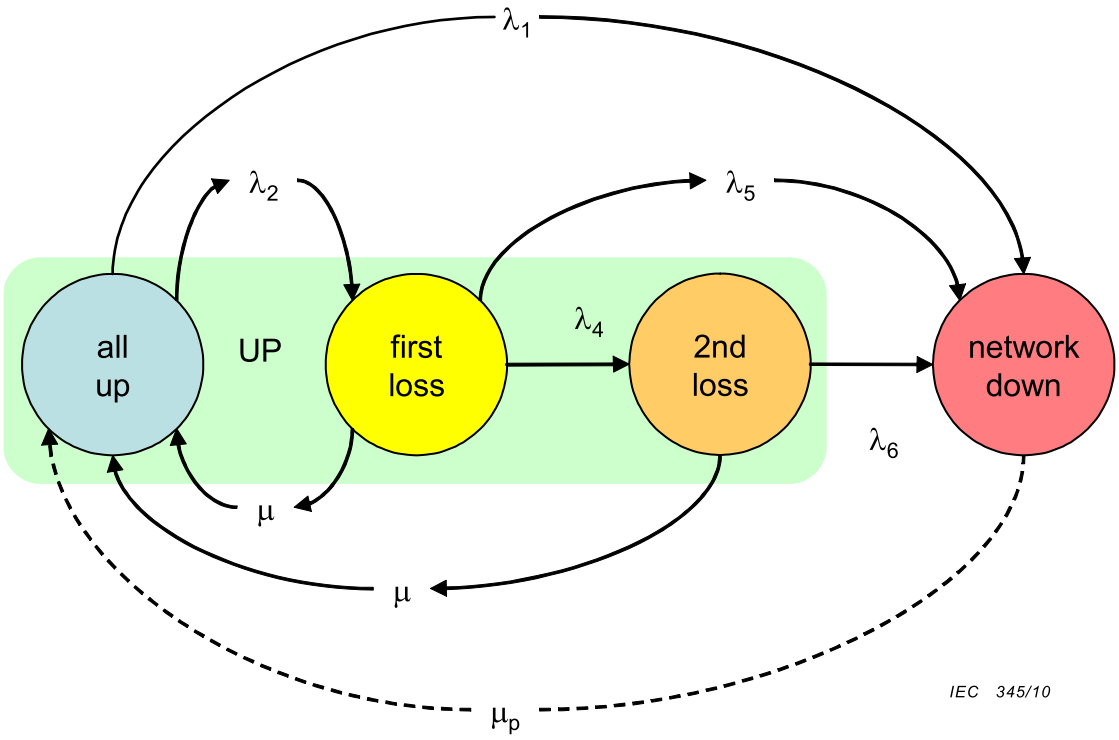
NOTE 2 Ce MTTFN qui paraît élevé a été calculé en négligeant les erreurs de mode commun. Si l'on considère la fiabilité de l'ensemble du système d'automatisation, le taux de défaillance du nœud d'extrémité domine le MTTFS et il convient d'envisager la redondance du nœud d'extrémité. Même un simple élément non redondant ou une cause commune de défaillance comme une erreur de logiciel abaisse fortement le MTTFN.

Copyright International Electrotechnical Commission

7.3.5 Considération de secondes défaillances

Le calcul ci-dessus est pessimiste car il suppose qu'une deuxième défaillance perturbe le reste du réseau avec une probabilité de 100 %. Cela est vrai pour les commutateurs lorsque le LAN ne dispose pas de redondance à l'intérieur, mais ce n'est pas le cas pour les liaisons en feuille puisque la probabilité d'une deuxième défaillance perturbant le même nœud d'extrémité n'est pas donnée par Σ (λ_L), mais simplement par λ_L.

Pour une estimation plus précise, le diagramme de transition de la Figure 18 peut être utilisé.



Légende

Anglais	Français
All up	Tout en bon fonctionnement
UP	EN BON FONCTIONNEMENT
First loss	Première perte
2nd loss	Deuxième perte
Network down	Réseau en panne

Figure 18 – Réseau avec une résilience à la deuxième défaillance

Les transitions sont:

λ_1 = taux de défaillance des composants non redondants
(y compris le point unique de défaillance et la probabilité d'un rétablissement non réussi).

λ_2 = taux de défaillance des composants redondants
(pour lesquels il existe une redondance et le rétablissement est réussi).

λ_4 = taux de défaillance des composants restants qui n'entraînent pas de perte du réseau.

λ_5 = taux de défaillance des composants restants qui entraînent une perte du réseau
(la somme de λ_4 et λ_5 est approximativement égale à λ_2, ainsi $\lambda_5 = f\lambda_2$,
où f est la probabilité que la deuxième erreur entraîne une défaillance du réseau.

λ_6 = taux de défaillance des composants restants après une deuxième défaillance.

Copyright International Electrotechnical Commission

μ = taux de rétablissement
(durée entre l'apparition d'une panne jusqu'à la restauration de la redondance, inclut la réparation en ligne)

μ_p = taux de réparation de l'installation
(durée entre l'apparition d'une panne non récupérable jusqu'à ce que l'installation fonctionne de nouveau).

le MTTFN du réseau est donnée par l'Équation (6).

$$MTTFN = \frac{(\mu + \lambda_2 + \lambda_4 + \lambda_5) + \frac{\lambda_2 \lambda_4}{\mu + \lambda_6}}{\lambda_1(\mu + \lambda_4 + \lambda_5) + \lambda_2\left(\lambda_5 + \lambda_4\left(\frac{1}{1 + \frac{\mu}{\lambda_6}}\right)\right)} \quad \mu >> \sum(\lambda_i) \approx \frac{1}{\lambda_1 + \frac{\lambda_2^2 f}{\mu}} \tag{6}$$

Supposons que les défaillances de mode commun (λ_1) puissent être négligées, le MTTFN est légèrement amélioré par rapport à la structure de la Figure 14 comme étant le rapport entre les secondes défaillances récupérables et les secondes défaillances non récupérables, λ_4 sur λ_5, ce rapport dépendant de la topologie.

Le taux de défaillance depuis la deuxième perte jusqu'à la défaillance du réseau n'influence pas significativement le résultat, puisque le système passe très peu de sa durée de vie dans l'état de deuxième perte, si le taux de réparation est élevé.

EXEMPLE Avec λ_1= 0 (pas de mode commun de défaillance), $\lambda_2 = \Sigma (\lambda_L + \lambda_S + \lambda_T)$, λ_4 = 0,9 λ_2, λ_5 = 0,1 λ_2 (1 panne sur dix n'est pas récupérable), $\lambda_6 = \lambda_2$.

MTTFN = 1 868 an.

7.4 Mise en garde

Il convient d'utiliser ces calculs comme une mise en garde que la redondance n'est pas en mesure de résoudre tous les problèmes de fiabilité et que l'hypothèse de base que le réseau est opérationnel lorsque tous les nœuds peuvent communiquer avec tous les autres nœuds, peut être relâchée dans des cas particuliers.

8 RSTP pour des réseaux à haute disponibilité: règles de configuration, méthode de calcul et de mesure pour un temps de rétablissement prévisible

NOTE Dans le contexte du présent Article, le terme “pont” est utilisé à la place de “commutateur”, respectivement “ponter” au lieu de “commuter”.

8.1 Généralités

Le protocole RSTP (Rapid Spanning Tree Protocol) tel que spécifié dans la norme IEEE 802.1D offre une prévention contre les boucles et une gestion de la redondance pour une topologie arbitraire des réseaux Ethernet commutés.

Le protocole RSTP fournit un rétablissement de deux types de pannes de réseau

a) une défaillance de maille inter-étage et
b) une défaillance de commutateur, qui peut être de deux types, en fonction du rôle du commutateur au moment de sa panne:

Copyright International Electrotechnical Commission

1) une défaillance d'un commutateur non-racine que le RSTP traite comme une défaillance de maille inter-étage ou
2) une défaillance d'un commutateur racine que le RSTP traite par la reconfiguration du réseau.

Bien que le protocole RSTP comprenne un algorithme efficace pour le rétablissement du réseau, le temps de reprise réel de la panne dépend de la topologie et de la mise en œuvre du RSTP.

En général, le protocole RSTP fournit un temps de reprise déterministe même dans une topologie arbitrairement maillée en cas de défaillance d'une liaison ou de défaillance d'un commutateur non-racine. Toutefois, en cas de défaillance d'un commutateur racine, il est difficile de prévoir le temps de reprise dans une topologie arbitrairement maillée.

En revanche, lorsque la topologie est limitée à un anneau, le temps de reprise d'une panne par RSTP est déterministe dans tous les scénarios et peut être calculé, à condition que les caractéristiques de performance de synchronisation du RSTP relatives aux commutateurs soient connues.

Le présent paragraphe spécifie la topologie en anneau de référence, la méthode de calcul pour calculer le temps de reprise relatif à cette topologie de référence, la méthode de mesure des caractéristiques de performance de synchronisation pertinentes d'une mise en œuvre du protocole RSTP et la forme sous laquelle il convient qu'elles soient divulguées.

8.2 Règles de déploiement et de configuration pour la topologie en anneau

Pour obtenir un temps de reprise déterministe, et pour les besoins des calculs suivants, les règles de configuration suivantes doivent être respectées:

- La topologie du réseau doit être limitée à un seul anneau de N appareils.
- Comme l'exigent les spécifications du RSTP, N doit être inférieur ou égal à 40.
- Les ports d'anneau doivent être activés pour le fonctionnement du RSTP.
- Les ports n'appartenant pas à l'anneau ne doivent pas être activés pour le fonctionnement du RSTP.
- Toutes les liaisons doivent être configurées pour opérer en mode bilatéral simultané (full-duplex).
- Les convertisseurs de supports, s'ils sont utilisés en connexions inter-étage, doivent fonctionner en mode de liaison transparent.
- Les commutateurs doivent être configurés de sorte qu'ils n'utilisent pas la classe de service la plus haute disponible à l'exception des BPDU ou, si cela n'est pas possible, au moins 10 % de la bande passante de la classe de service la plus haute disponible doit être réservé pour les BPDU.

NOTE La désactivation des ports n'appartenant pas à l'anneau pour RSTP a pour conséquence que les boucles connectées aux ports n'appartenant pas à l'anneau ne seront pas évitées par RSTP.

8.3 Calculs pour le temps de reprise de panne dans un anneau

8.3.1 Dépendances et modes de défaillance

Le temps de reprise de panne par RSTP dépend des facteurs suivants:

- l'emplacement du point de défaillance lié au(x) port(s) de rejet qui termine(nt) la/les branche(s) d'arbre recouvrant,
- la combinaison des paramètres de configuration du RSTP dans différents commutateurs dans le(s) segment(s) affectés du réseau.

Les modes de défaillance suivants sont considérés:

Copyright International Electrotechnical Commission

- perte d'une maille inter-étage,
- perte d'un nœud dans le rôle non-racine,
- perte d'un nœud dans le rôle racine.

RSTP dépend de la détection de l'état de la liaison.

8.3.2 Calculs pour les modes de défaillance non considérés

Si une défaillance se produit de telle sorte qu'aucune erreur de liaison n'est détectée et qu'aucune BPDU n'est envoyée, le temps de reprise s'élèvera à une valeur qui est trois fois le temps "Hellotime", qui est actuellement spécifié comme un minimum de 1 s dans l'IEEE 802.1D: 2004.

NOTE Les mécanismes pour prévenir cette situation sont possibles, mais ne sont pas exigés dans l'IEEE 802.1D.

8.3.3 Calculs pour les modes de défaillance considérés

Les formules ci-dessous présentent la limite supérieure du temps de reprise de panne dans un réseau en anneau:

- $T_L + N*max(T_{PA} , (T_{TC}+T_F))$ – pour une défaillance de mailles inter-étage et une défaillance de commutateurs non-racine
- $T_L + 2*N*T_{PA}$ – pour une défaillance de commutateurs racine

où:

N est le nombre de commutateurs dans l'anneau;

T_L est le temps requis par un commutateur pour détecter une défaillance de liaison;

T_{PA} est le temps requis par une paire de commutateurs pour effectuer l'établissement de liaison "Proposition-Accord" (Proposal-Agreement) du protocole RSTP; égal à la somme des temps de traitement de la BPDU dans les deux commutateurs de la paire ;

T_{TC} est le temps requis par une paire de commutateurs pour propager une BPDU de changement de topologie; égal à la somme des temps de traitement de la BPDU dans les deux commutateurs de la paire;

NOTE 1 T_{TC} est approximativement la moitié de T_{PA} puisqu'aucun acquittement n'est impliqué.

T_F est le temps requis par un commutateur pour vider sa table d'adresses MAC.

Un autre paramètre non utilisé dans les formules ci-dessus est défini pour les mesures de synchronisation:

T_{Proc} est le temps de traitement du RSTP, c'est-à-dire le temps requis pour traiter un cycle entier de diagrammes d'états RSTP.

NOTE 2 T_{PA} est en fait la somme du temps de traitement descendant (“downlink”) d'un commutateur et le temps de traitement ascendant (“uplink”) du commutateur adjacent (générant une BPDU "Proposal" (Proposition), traitant la BPDU "Proposal" et générant une BPDU "Agreement" (Accord), et traitant la BPDU "Agreement"). Un cycle entier de diagrammes d'états RSTP inclut les temps de traitement “ascendant” et “descendant” d'un commutateur, c'est-à-dire approximativement $T_{Proc} = T_{PA}$.

EXEMPLE Pour atteindre un temps de reprise de 130 ms dans un anneau de 40 appareils, pour tous les commutateurs, il convient que le temps T_L soit inférieur à 10 ms pour des liaisons 100Base-TX et 100Base-FX et que le temps T_{PA} et la somme ($T_{TC} + T_F$) soient inférieurs à 3 ms.

NOTE 3 Cela requiert que le port du commutateur matériel prenne en charge la détection rapide de défaillance de liaison, telle que spécifiée par l'ISO/IEC 8802-3 (IEEE 802.3).

NOTE 4 Les liaisons 1000Base-T ne peuvent pas être utilisées pour les connexions inter-étage dans cette application en raison de leur important temps de détection de défaillance de liaison.

NOTE 5 Cela peut être assuré en donnant la priorité aux tâches de surveillance des liaisons et de traitement du microprogramme RSTP et par la vitesse du processeur et la mise en œuvre du microprogramme RSTP appropriés.

Copyright International Electrotechnical Commission

8.4 Méthode de mesure de la synchronisation (timing)

8.4.1 Mesure de T_{PA}

8.4.1.1 Mesure

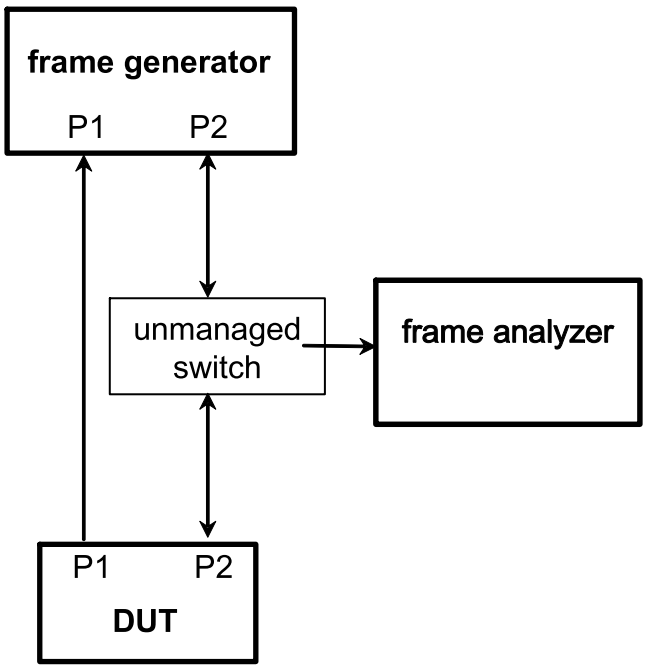
Il est impossible de mesurer séparément certaines valeurs de temps définies ci-dessus. Par conséquent, certains essais mesurent une combinaison de plusieurs valeurs de temps, de sorte que le temps en question peut être calculé à partir de la valeur mesurée.

Cet essai mesure en fait le temps T_{Proc} mais T_{Proc} est égal à T_{PA}, comme expliqué en 8.3.3.

8.4.1.2 Configuration

Configurer le système comme suit:

a) Construire le réseau d'essai comme montré à la Figure 19.



Légende

Anglais	Français
Frame generator	Générateur de trames
Frame analyzer	Analyseur de trames
Unmanaged switch	Commutateur non géré
DUT	Appareil en essai

Figure 19 – Banc d'essai pour mesure de T_{PA}

b) Configurer l'appareil en essai de sorte que les paramètres 'AdminEdge' et 'AutoEdge' des ports connectés sont mis à "FALSE".

c) Configurer le Port2 du générateur de trames pour envoyer une BPDU "Proposal" (c'est-à-dire avec le fanion "proposal" défini et "root bridge ID" meilleur que celui de l'appareil en essai).

d) Configurer le Port1 du générateur de trames seulement pour maintenir une liaison Ethernet mais pas pour envoyer toutes les trames. Ce port simulera un autre commutateur RSTP auquel l'appareil en essai propagera une proposition.

Copyright International Electrotechnical Commission

e) Configurer l'analyseur de trames pour capturer les trames reçues à partir du commutateur non géré.

8.4.1.3 Procédure

La procédure est comme suit:

a) vérifier que l'appareil en essai s'est choisi comme "racine".
b) commencer à capturer les trames dans l'analyseur de trames.
c) émettre une seule BPDU à partir du générateur de trames.
d) arrêter de capturer les trames.
e) vérifier que l'appareil en essai a envoyé une BPDU "agreement" en réponse à la BPDU "proposal".
f) mesurer l'intervalle de temps entre la BvPDU "proposal" et la première BPDU "agreement".

8.4.2 Mesure de T_L

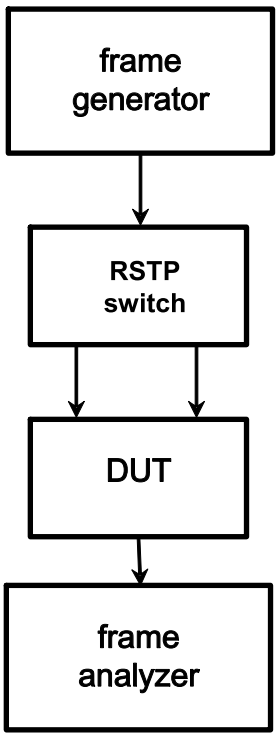
8.4.2.1 Mesure

Cet essai mesure en fait le temps (T_L + T_{Proc}). Sachant que T_{Proc} a été mesuré par l'essai précédent, T_L est déduit de (T_L + T_{Proc}).

8.4.2.2 Configuration

Configurer le système comme suit:

a) construire le réseau comme montré à la Figure 20.



IEC 347/10

Légende

Anglais	Français
Frame generator	Générateur de trames
RSTP switch	Commutateur RSTP

Copyright International Electrotechnical Commission

Anglais	Français
DUT	Appareil en essai
Frame analyzer	Analyseur de trames

Figure 20 – Banc d'essai pour mesure de T_L

b) mettre le paramètre “Bridge priority” du commutateur RSTP à 0 afin de le forcer à être élu comme “racine”.

c) configurer le générateur de trames pour envoyer un flux continu de trames arbitraires à un débit minimal de 4 000 trames par seconde afin de permettre une résolution de mesure de temps de 0,25 ms.

d) configurer l'analyseur de trames pour capturer les trames reçues à partir de l’appareil en essai.

8.4.2.3 Procédure

La procédure est comme suit:

a) vérifier que le commutateur RSTP a été choisi comme “racine”.

b) vérifier que l'un des ports de l’appareil en essai a un statut “root forwarding” (transmission racine) et l'autre port a un statut “alternate discarding” (rejet remplaçant).

c) commencer à émettre à partir du générateur de trames.

d) commencer à capturer les trames.

e) vérifier que les trames sont reçues par l'analyseur de trames.

f) couper la liaison associée au port “root” de l’appareil en essai. Cela mènera l’appareil en essai à basculer vers son port “alternate”.

g) vérifier que les trames sont reçues par l'analyseur de trames.

h) arrêter de capturer les trames.

i) mesurer pour combien de temps la réception de trames a été perturbée.

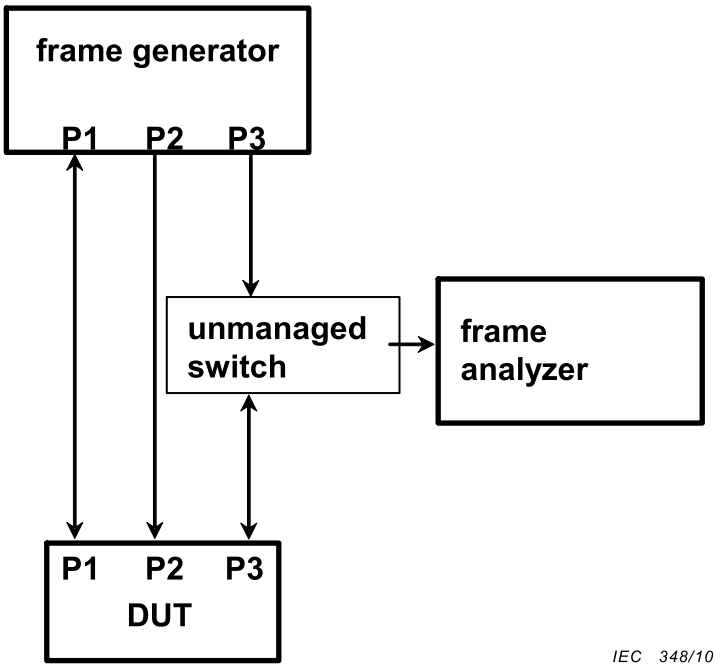
8.4.3 Mesure de (T_{TC} + T_F)

8.4.3.1 Configuration

Configurer le banc d'essai comme suit:

a) construire le réseau d'essai comme montré à la Figure 21.

Copyright International Electrotechnical Commission



Légende

Anglais	Français
Frame generator	Générateur de trames
Frame analyzer	Analyseur de trames
Unmanaged switch	Commutateur non géré
DUT	Appareil en essai

Figure 21 – Banc d'essai pour mesure de (T_{TC} + T_F)

b) mettre les paramètres ‘AutoEdge’ et ‘AdminEdge’ du Port1 et du Port3 de l’appareil en essai à FALSE.

c) mettre le paramètre ‘AutoEdge’ du Port2 de l’appareil en essai à FALSE et le paramètre ‘AdminEdge’ à TRUE.

d) configurer le Port1 du générateur de trames pour envoyer une seule trame arbitraire.

e) configurer le Port2 du générateur de trames pour envoyer un flux continu de trames à l'adresse MAC destination du Port2 à un débit minimal de 4 000 trames par seconde afin de permettre une résolution de mesure de temps de 0,25 ms.

f) configurer le Port3 du générateur de trames pour envoyer une seule BPDU “agreement + topology change” (“accord + changement de topologie”).

g) configurer l'analyseur de trames pour capturer les trames reçues à partir du commutateur non géré.

8.4.3.2 Procédure

La procédure est comme suit:

a) vérifier que l’appareil en essai s'est élu lui-même comme “racine”.

b) émettre une seule trame à partir du Port1 du générateur de trames. Cela permettra que le Port1 de l’appareil en essai apprenne l'adresse MAC source de la trame.

c) commencer à émettre un flux continu à partir du Port2 du générateur de trames.

d) commencer à capturer les trames dans l'analyseur de trames.

e) vérifier que le flux n'est pas transmis à partir du Port3 de l’appareil en essai (il est transmis uniquement à partir du Port1 de l’appareil en essai).

Copyright International Electrotechnical Commission

f) envoyer une seule BPDU à partir du Port3 du générateur de trames. Cela entraînera l'appareil en essai à purger sa table d'adresses MAC et commencer à inonder le flux de trafic à partir du Port3, ainsi il sera capturé par l'analyseur de trames.

g) arrêter de capturer les trames.

h) vérifier que l'appareil en essai a commencé à inonder le flux à partir du Port3 en réponse à la BPDU "changement de topologie".

i) mesurer l'intervalle de temps entre la BPDU "changement de topologie" et la première trame de flux.

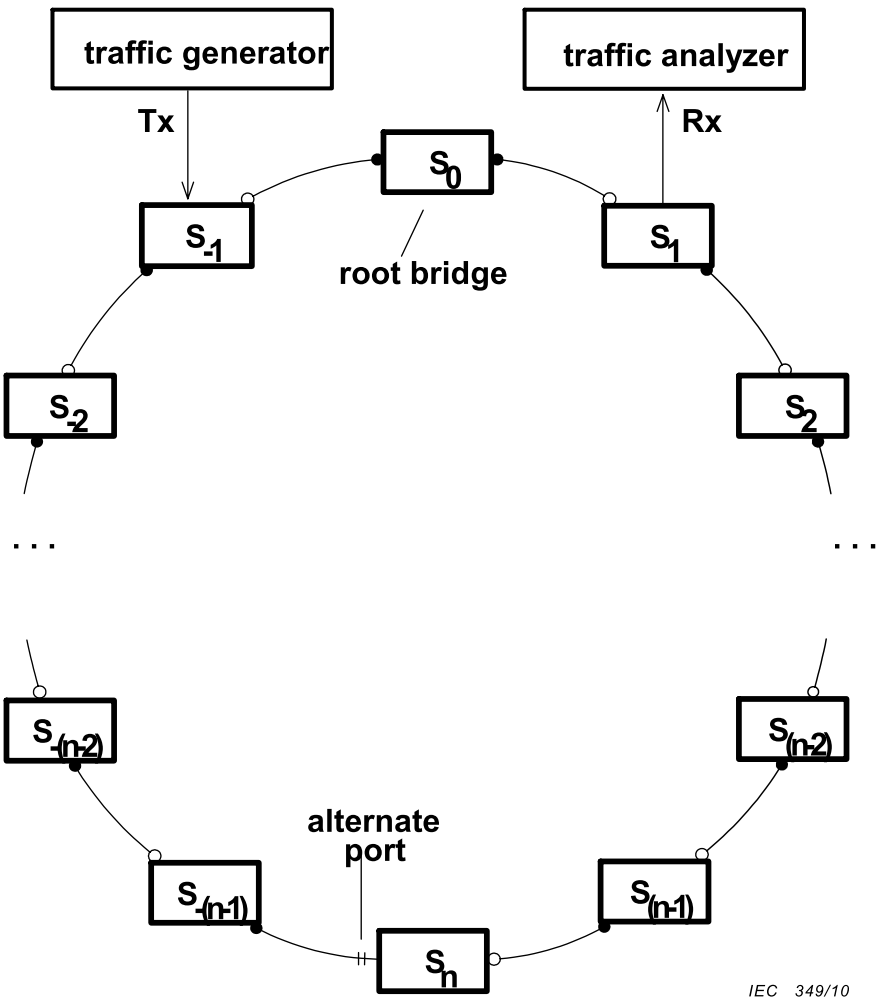
j) répéter a) ... i) pour 10 valeurs différentes choisies aléatoirement de l'adresse MAC source utilisée par le Port1 du générateur de trames (et donc l'adresse MAC destination utilisée par le Port2 du générateur de trames) et choisir la valeur maximale parmi toutes les mesures.

8.4.4 Exemple d'essai de système

8.4.4.1 Configuration

Configurer le système comme suit:

a) construire un anneau de commutateurs, composé de 20-40 commutateurs se conformant à la spécification IEEE 802.1D:2004 RSTP comme montré à la Figure 22.



Légende

Anglais	Français
Traffic generator	Générateur de trafic

Copyright International Electrotechnical Commission

Anglais	Français
Traffic analyzer	Analyseur de trafic
Root bridge	Pont racine
Alternate port	Port remplaçant

Figure 22 – Banc d'essai pour l'essai du système

b) s'assurer que toutes les liaisons sont conformes aux exigences de déploiement spécifiées en 8.2.

c) configurer le générateur de trafic pour envoyer des trames destinées à l'adresse MAC du port Rx à partir de son port Tx. Il convient de choisir le débit de transmission suffisamment élevé pour que temps de reprise de panne puisse être calculé sur la base d'un nombre de paquets perdus avec une résolution de l'ordre de milliseconde.

d) configurer le générateur de trafic pour envoyer des trames arbitraires de faible débit (par exemple une fois en quelques secondes) à partir de son port Rx avec l'adresse MAC source du port Rx (afin que les commutateurs l'apprennent).

e) configurer l'analyseur de trafic pour afficher les compteurs de trames Tx et Rx.

f) mettre tous les paramètres RSTP des commutateurs aux valeurs par défaut. Vérifier que tous les commutateurs ont leur "bridge priority" mis à 32 768.

g) mettre à 0 le "bridge priority" S_0 du commutateur, afin que S_0 soit élu comme un commutateur racine.

h) mettre à 4 096 le "bridge priority" S_1 du commutateur, afin que S_1 soit le meilleur prochain candidat racine après S_0.

8.4.4.2 Procédure

La procédure est comme suit:

a) vérifier que le port remplaçant est sur le commutateur S_n, sur la liaison S_n–$S_{-(n-1)}$.

b) commencer à émettre à faible débit des trames fictives à partir du port de trafic Rx. Vérifier que les commutateurs S_{-1}, S_0 et S_1 ont appris l'adresse MAC du port Rx.

c) commencer à émettre des trames à partir du port Tx. Vérifier que le compteur Rx s'incrémente avec le compteur Tx et qu'aucun trafic n'est perdu.

d) couper la liaison S_0–S_1.

e) vérifier que le compteur Rx s'incrémente (c'est-à-dire la connectivité a été rétablie).

f) arrêter d'émettre à partir du port Tx.

g) lire les compteurs Tx et Rx et calculer le nombre de trames perdues.

h) calculer le temps de reprise de panne en utilisant la formule t = (nombre de trames perdues) / (débit de trames).

8.5 Limites de topologie RSTP et temps de rétablissement maximal

NOTE Dans la prochaine édition de l'IEC 62439-1, ce nouveau Paragraphe sera renuméroté 8.2.

8.5.1 Paramètres du protocole RSTP

Le présent paragraphe explique les paramètres du protocole RSTP ayant une influence sur les temps de rétablissement maximaux et décrit comment une configuration spécifique de topologie et de protocole les influence. Les termes spécifiques à RSTP sont d'abord définis. Des lignes directrices de base relatives à la conception du réseau sont ensuite données, tandis qu'une méthode de détermination d'une approximation d'un temps de reconfiguration de réseau de limite supérieure le plus défavorable pour des réseaux maillés RSTP est fournie.

Le présent paragraphe traite en particulier des réseaux RSTP composés de plus d'un anneau. Pour un seul anneau Ethernet fonctionnant sur RSTP, le temps de reconfiguration du réseau

Copyright International Electrotechnical Commission

peut être déterminé comme le montre le 8.2. Cependant, les énoncés suivants concernant des paramètres RSTP s'appliquent également dans un réseau en anneau.

8.5.2 Termes et définitions spécifiques à RSTP

NOTE Ces termes sont tirés de l'IEEE 802.1D.

8.5.2.1 Délai de transmission (TxHoldCount)

Chaque port d'un pont RSTP comprend un compteur TxHoldCount. Ce compteur démarre à zéro et est incrémenté à chaque envoi de BPDU par le port. Une minuterie décrémente le compteur à chaque seconde. Si TxHoldCount atteint la valeur maximale, aucune autre BPDU n'est transmise sur ce port jusqu'à ce que le compteur soit décrémenté à nouveau, quelle que soit l'importance de la BPDU pour la reconfiguration du réseau. La valeur maximale par défaut de TxHoldCount est de 6 et le numéro configurable maximal est de 10.

8.5.2.2 Bridge Max Age

Chaque pont RSTP comprend un paramètre Bridge Max Age qu'il convient de configurer à une valeur identique dans chacun des ponts. Bridge Max Age définit le nombre total maximal de “bonds physiques” ou de liaisons entre le pont racine et tour pont participant au même réseau RSTP. Sa valeur par défaut est de 20 et peut être configurée de 6 à une valeur maximale de 40. Dans certains cas particuliers, Bridge Max Age est configuré de manière différente dans certains ponts.

Etant donné que Bridge Max Age définit l'extension maximale d'un réseau RSTP, il est souvent appelé “diamètre du réseau”. Cependant, le terme “Bridge Max Age” et le diamètre du réseau réellement utilisable ne sont pas synonymes, voir 8.5.2.4.

8.5.2.3 Message Age

Chaque BPDU comprend un paramètre Message Age. A réception d'une BPDU, un pont incrémente Message Age puis le compare à son propre “Bridge Max Age”. Si le paramètre Message Age est supérieur à Bridge Max Age, le pont rejette la BPDU et ignore les informations qu'elle contient.

Le pont racine commence par envoyer des BPDU avec Message Age = 0. Le premier pont situé après le pont racine (ainsi que les ponts suivants jusqu'à ce que le paramètre Message Age atteigne Bridge Max Age) reçoit la BPDU, incrémente “Message Age” de 1, le compare au paramètre “Bridge Max Age” puis transmet les BPDU accompagnées des informations mises à jour.

8.5.2.4 Diamètre et rayon du réseau

Le “diamètre” du réseau RSTP est le nombre de ponts sur le chemin actif le plus long d'une arborescence réseau entre deux ponts les plus éloignés entre eux. Le diamètre ne correspond pas nécessairement au paramètre RSTP Bridge Max Age (voir Figure 23).

Le ”rayon” d'un réseau RSTP correspond au nombre de ponts à partir (et comprenant) du pont racine actif vers le pont le plus éloigné de cette racine active dans la topologie. Il s'agit de la longueur (en sauts) du chemin le plus long sur lequel il est nécessaire de transférer les informations du protocole RSTP (voir Figure 23). Le rayon maximum pris en charge par RSTP peut être défini comme:

rayon max. = Bridge Max Age + 1.

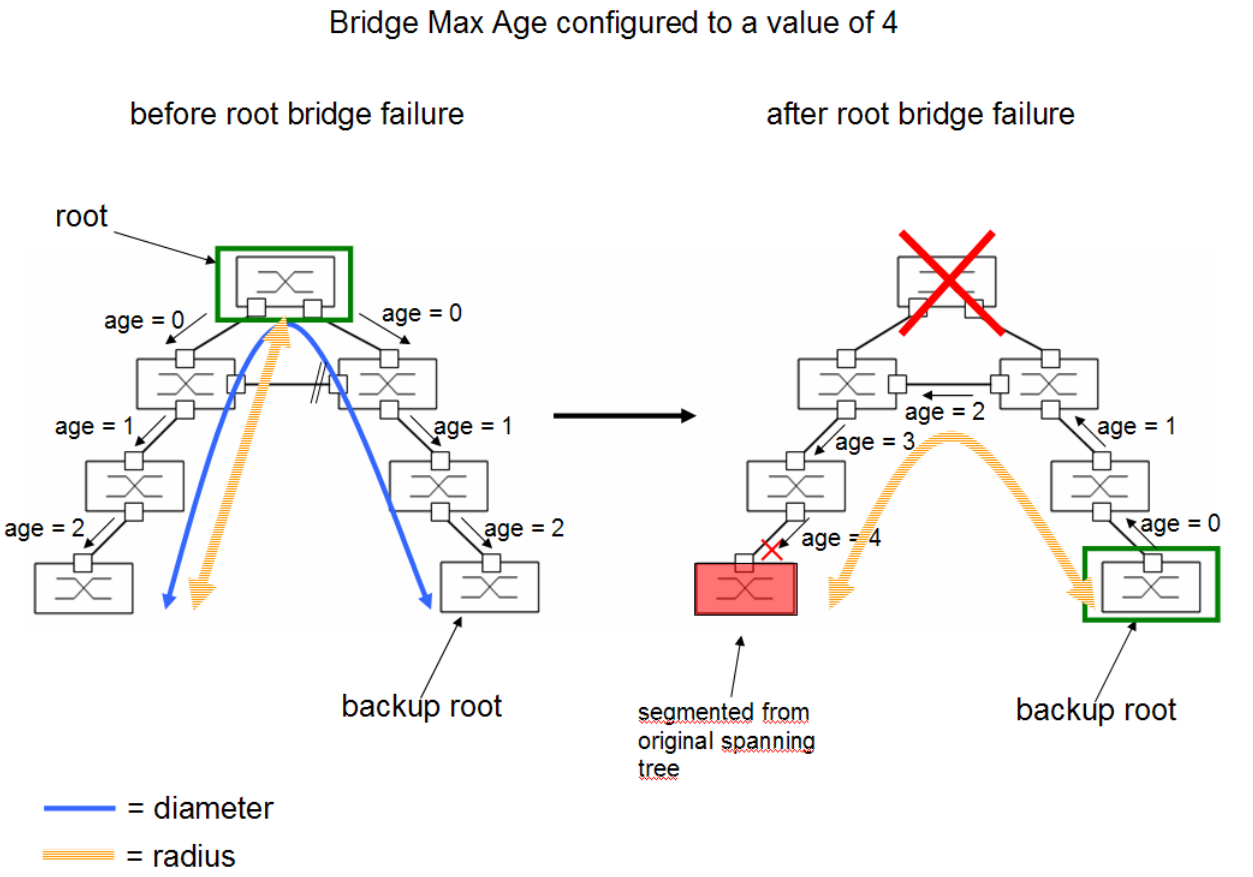
Le rayon est indispensable pour déterminer les topologies les plus défavorables. Dans des conditions de défaillance les plus défavorables (en l'absence d'un réseau technique et de ponts racines placés avec attention), en cas de défaillance d'un pont racine, la feuille la plus éloignée pourrait être le pont racine de secours, susceptible de devenir la racine suivante.

Copyright International Electrotechnical Commission

Dans ce cas, le diamètre du réseau peut devenir le rayon et devient le chemin réel que les informations RSTP doivent parcourir pour se rendre vers les ponts individuels. (Voir Figure 23)

NOTE Les BPDU RSTP sont uniquement transmises sur la liaison située entre deux ponts directement connectés. Chacun des ponts consomme et produit ces BPDU, mais les informations RSTP qu'ils transportent parcourent divers chemins à travers le réseau (dans un état de réseau stable et sans reconfiguration).

8.5.3 Exemple d'arborescence RSTP de petite taille



IEC 953/12

Légende

Anglais	Français
Bridge Max Age configured to a value of 4	Paramètre Bridge Max Age configuré sur une valeur de 4
Before root bridge failure	Avant la défaillance d'un pont racine
After root bridge failure	Après la défaillance d'un pont racine
Root	Racine
Backup root	Racine de secours
Age	Âge
Segmented from original spanning tree	Segmenté de l'arborescence d'origine
Diameter	Diamètre
Radius	Rayon

Figure 23 – Diamètre et Bridge Max Age

NOTE 1 La valeur de 4 a été attribuée au paramètre RSTP Bridge Max Age pour les besoins du présent exemple même si 802.1D ne permet pas une valeur inférieure à 6.

Copyright International Electrotechnical Commission

Dans l'exemple de la Figure 23, le réseau sans défaillance se trouve d'abord dans une condition stable avec Bridge Max Age = 4 et parce que le rayon réel est de 4 (la configuration RSTP pourrait supporter un rayon maximal de 5). Le diamètre est de 7, d'une feuille d'une branche à l'autre feuille située dans l'autre branche, via le pont racine. Etant donné que le pont racine est l'élément racine d'une arborescence équilibrée, Bridge Max Age = 4 suffit pour tous les ponts afin de recevoir les BPDU RSTP à partir de la même racine RSTP.

Une défaillance de pont racine et un choix de racine de secours défavorable changent ce processus. Après la défaillance d'un pont racine, la liaison redondante précédemment bloquée est activée. Le diamètre est désormais de 6. Parallèlement, le rayon est également augmenté pour atteindre 6. Etant donné que l'une des feuilles des branches d'origine est désormais devenue le pont racine, le paramètre Bridge Max Age de 4 ne suffit plus pour que les informations racines RSTP atteignent tous les ponts du réseau, car les informations RSTP doivent alors parcourir l'ensemble du diamètre, maintenant équivalent au rayon. Par conséquent, le dernier pont est segmenté, comme indiqué dans la Figure 23. Ce pont rejette la BPDU, car le paramètre Message Age a dépassé le paramètre configuré Bridge Max Age.

Pour concevoir des réseaux stables et haute performance, il est nécessaire d'observer et de comprendre la différence entre le diamètre du réseau et le rayon, respectivement le paramètre Bridge Max Age. Ce dernier est maintenu à une valeur aussi élevée que nécessaire afin de ne pas segmenter de dispositif dans le scénario de défaillance le plus défavorable et à une valeur la plus faible possible afin de réduire au maximum le temps de rétablissement du réseau tel que décrit dans les paragraphes suivants. Le rayon du réseau détermine la valeur Bridge Max Age nécessaire pour chacune des topologies considérées. Le paramètre Bridge Max Age peut être maintenu à une valeur faible en positionnant à la fois le pont racine et le pont racine de secours dans une position centrale au sein du réseau, par exemple sur l'anneau principal d'une topologie hiérarchique multi-anneaux.

NOTE 2 Une autre méthode, qui n'est pas traitée dans le présent document, consiste à configurer différentes valeurs Bridge Max Age sur le pont racine et sur le pont racine de secours, conformément à leurs positions respectives dans le réseau.

8.5.4 Hypothèse relative à TxHoldCount

Le calcul ou l'approximation d'un temps de reconfiguration de limite supérieure est effectué à partir de l'hypothèse selon laquelle le paramètre Transmit Hold Count (TxHoldCount) n'est jamais atteint et qu'aucune BPDU nécessaire à une reconfiguration rapide du réseau n'est perdue.

Ceci peut cependant se produire en pratique, notamment pendant la reconfiguration du réseau. Dès que le paramètre TxHoldCount d'un port de pont est “saturé”, aucun des ponts reliés au port saturé ne recevra plus de BPDU jusqu'à ce TxHoldCount ait été décrémenté. Si les BPDU rejetées sont essentielles à la reconfiguration du réseau, le temps de rétablissement du réseau peut être rallongé de plusieurs secondes. Cette hypothèse est d'une importance pratique majeure et est considérée comme la plus grande menace pour le temps de reconfiguration du réseau des réseaux RSTP.

8.5.5 Topologie la plus défavorable et détermination du rayon

Etant donné que le rayon le plus défavorable et le paramètre Bridge Max Age le plus faible possible sont corrélés, la détermination du rayon le plus défavorable est importante pour déterminer le temps de reconfiguration de limite supérieure le plus défavorable.

Dans un réseau maillé arbitrairement, les liaisons reconfigurées du réseau en régime établi après reconfiguration peuvent être prévues avant la défaillance, mais étant donné que le protocole est basé sur la réception et l'envoi de BPDU dans chaque pont individuel, des conditions de concurrence peuvent avoir lieu pendant la reconfiguration. Par conséquent, le temps de reconfiguration maximal ne peut être donné que comme une limite la plus défavorable basée sur le temps de réaction maximal de chaque pont et sur le nombre maximal de sauts autorisés par le protocole.

Copyright International Electrotechnical Commission

En outre, certains supports tels que 1000Tx présentent des temps de détection de défaillance de liaison importants. Ainsi, l'auto-négociation désactivée sur des liaisons à fibre Gigabit peut compromettre le temps de défaillance RSTP en cas de défaillance de liaison.

NOTE Des défaillances malveillantes, par exemple un pont incapable de transférer des trames de données utiles mais qui échange toujours des BPDU avec ses voisins, ne peuvent être prises en compte dans les calculs.

Lors de la conception d'un réseau fonctionnant avec RSTP, le rayon du réseau à partir de l'emplacement du pont racine et de l'emplacement de la racine de secours vers le pont de la feuille la plus éloignée doit être calculé.

Ce calcul de rayon tient également compte d'une défaillance la plus défavorable, car des défaillances de topologie peuvent augmenter le rayon. Par exemple, la Figure 24 illustre le pont racine et le pont racine de secours situés sur l'anneau principal. Le rayon le plus défavorable pour cette topologie spécifique est atteint par deux défaillances simultanées positionnées comme le montre Figure 24, et s'élève à 7 pour la racine indiquée.

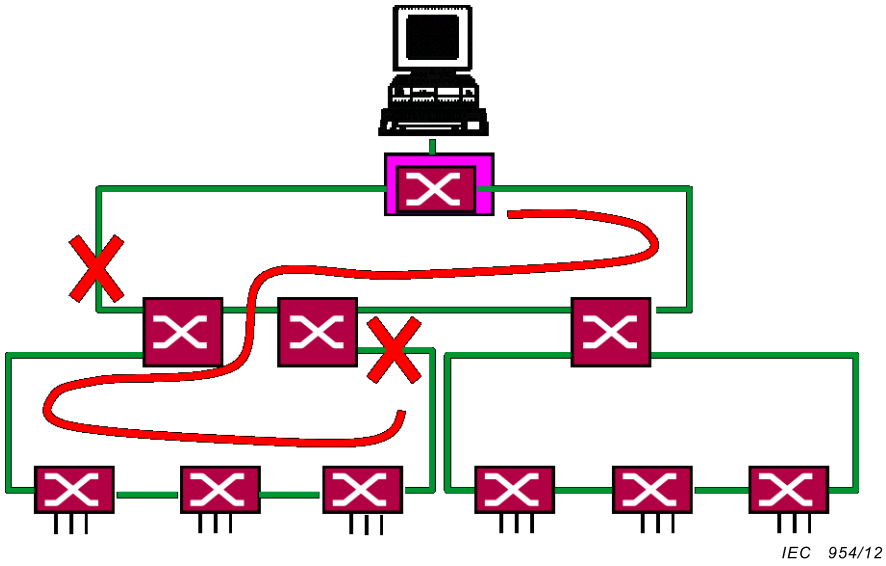


Figure 24 – Détermination du chemin le plus défavorable

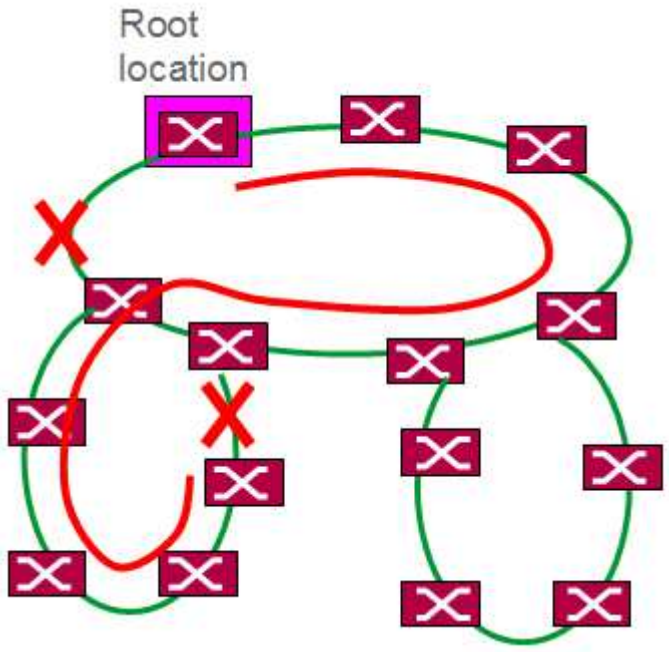
Une fois déterminée la valeur du rayon le plus défavorable pour un scénario de défaillance la plus défavorable dans la topologie de réseau, il convient de configurer Bridge Max Age précisément au nombre - 1. Ceci permet de réduire au maximum le temps de reconfiguration de limite supérieure du réseau, puisqu'un paramètre Bridge Max Age plus faible limite le temps de parcours des BPDU dans le réseau.

8.5.6 Méthode de détermination du rayon le plus défavorable en cas d'architecture anneau-anneau

Dans une topologie d'anneau à anneaux, l'anneau principal se compose de “N” ponts + 2 × “M” ponts qui relient “M” sous-anneaux de manière redondante, chacun étant composé de “R” ponts (à l'exception du pont utilisé pour relier à l'anneau principal).

La Figure 25 donne un exemple d'anneau principal (N = 3) doté de deux sous-anneaux (M = 2) reliés de manière redondante via un total de quatre ponts (deux par sous-anneau) à l'anneau principal, avec R = 4.

Copyright International Electrotechnical Commission



IEC 956/12

Légende

Anglais	Français
Root location	Emplacement de la racine

Figure 25 – Exemple de topologie anneau-anneau

Le pont racine et le pont racine de secours restent sur l'anneau principal (cette position est garantie en configurant la priorité RSTP de la racine et de la racine de secours sur l'anneau principal avec une valeur de priorité supérieure à tout autre pont dans les sous-anneaux).

Une seule défaillance au niveau de l'anneau principal et une défaillance au niveau du sous-anneau sont prises en compte. Le support simultané d'une défaillance sur l'anneau principal et d'une deuxième défaillance sur un sous-anneau est un cas limite.

Le rayon le plus défavorable (c'est-à-dire que le paramètre Bridge Max Age qui nécessite une configuration et qui est équivalent au rayon le plus défavorable - 1) est alors:

$$\text{rayon le plus défavorable} = N + 2 \times M + R$$

$$\text{Bridge Max Age} = (\text{rayon le plus défavorable} - 1) = N + 2 \times M + R - 1$$

où

“R” est le nombre de ponts dans le sous-anneau et possédant le plus grand nombre de dispositifs;

“N” est le nombre de ponts dans l'anneau principal (à l'exception des ponts qui relient les sous-anneaux);

“M” est le nombre de ponts sur l'anneau principal qui relient l'anneau principal aux sous-anneaux.

Dans le schéma ci-dessus, on tient compte de N=3, M=2, R=4, le rayon le plus défavorable étant = 11.

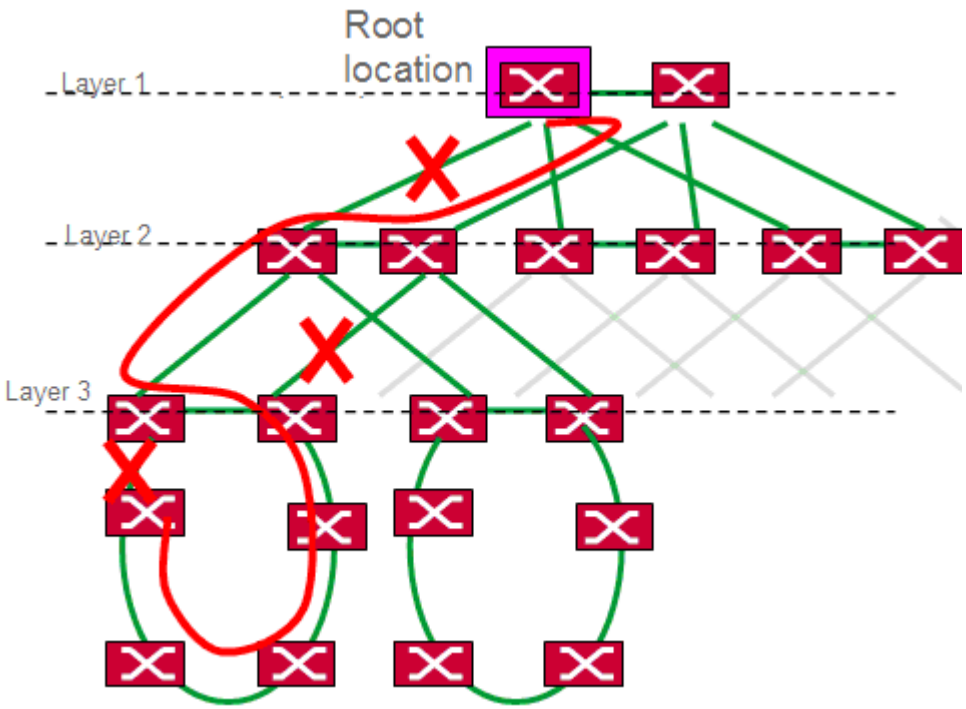
Par conséquent, il convient de configurer le paramètre de protocole RSTP “Bridge Max Age” à une valeur de 10 afin d'optimiser les temps de rétablissement du réseau.

Copyright International Electrotechnical Commission

8.5.7 Rayon le plus défavorable d'une architecture multicouche optimisée

Avec un grand nombre de ponts, il convient d'optimiser la topologie du réseau afin de ne pas atteindre la limite Bridge Max Age et de maintenir les temps de reconfiguration les plus défavorables à un niveau bas.

Une solution simple consiste à considérer une topologie multicouche, composée de “L” couches, comme illustré dans la Figure 26:



IEC 957/12

Légende

Anglais	Français
Root location	Emplacement de la racine
Layer	Couche

Figure 26 – Exemple de topologie multicouche

La couche supérieure est composée de 2 ponts principaux qui sont définis pour être les ponts racines/ponts racines de secours. (Il est prévu que la valeur de priorité de ces ponts soit définie en conséquence à la priorité la plus élevée et à la deuxième priorité la plus élevée).

La taille maximale de la couche 3 est définie par des sous-anneaux composés de “R” ponts. Le paramètre “R” exclut les ponts reliant le sous-anneau individuel de couche 3 à la couche 2, qui est intégré au calcul grâce au paramètre “L”.

Une seule défaillance par couche est prise en compte.

Le rayon le plus défavorable est alors égal à:

$$\text{rayon le plus défavorable} = (2 \times L) + R$$

Dans le schéma ci-dessus, L=3, R=4, et par conséquent le rayon le plus défavorable = 10. Ceci donne lieu à un paramètre Bridge Max Age de 9.

Copyright International Electrotechnical Commission

Le point d'intérêt est que ce résultat ne dépend pas du nombre de dérivations par couche, et cette topologie est éventuellement en mesure de prendre en charge un grand nombre de nœuds avec un faible paramètre Bridge Max Age. La limite est le nombre maximal de ports des ponts utilisés au niveau de chaque couche: Un grand nombre de ports physiques est préjudiciable aux performances RSTP sur les ponts.

8.5.8 Temps de reconfiguration approximatif de limite supérieure destiné aux réseaux RSTP

La défaillance du pont racine RSTP est le scénario le plus défavorable affectant le temps de reconfiguration. Le temps de reconfiguration de limite supérieure est le temps nécessaire au rétablissement après une défaillance du pont racine. Le temps de rétablissement des défaillances de liaisons ou des défaillances de ponts qui ne sont pas à la racine ne sera pas supérieur au temps de rétablissement d'une défaillance de pont racine. Etant donné qu'il s'agit du scénario le plus défavorable, le temps de rétablissement est par conséquent estimé pour une défaillance du pont racine.

Lorsque l'on considère le temps de reconfiguration du réseau d'un réseau RSTP maillé, trois phases distinctes peuvent être identifiées:

– Phase de vieillissement: Phase au cours de laquelle la défaillance du réseau est détectée et où de multiples informations racines (anciens et nouveaux vecteurs de priorité de racine) sont encore présentes au sein du réseau. Les anciennes informations racines peuvent encore circuler au sein du réseau jusqu'à ce que le paramètre Message Age des BPDU atteigne la valeur Bridge Max Age. Une fois l'ancien vecteur de priorité de racine issu du pont racine défectueux complètement éliminé du réseau seulement, le vecteur de priorité de racine de secours peut être prépondérant. La phase de vieillissement est ainsi le temps à partir de la défaillance jusqu'au moment où l'ancien vecteur de priorité BPDU racine est éliminé et, dans une situation la plus défavorable, lorsque tout autre nouveau vecteur racine temporaire inférieur atteint le pont racine de secours et déclenche la phase de convergence.
– Phase de convergence: La phase au cours de laquelle la racine de secours diffuse son nouveau vecteur racine au réseau et n'est plus perturbée par des informations de l'ancien vecteur racine. La phase de convergence débute immédiatement après la phase de vieillissement et se termine lorsque le pont le plus éloigné de la nouvelle racine de secours a reçu les informations de la nouvelle racine.
– Phase de vidange: Après la reconfiguration de la topologie active, plusieurs ponts peuvent vider leurs bases de données filtrantes pour s'assurer que les nouveaux chemins de communication sont correctement appris. RSTP utilise des BPDU de changement de topologie (TC) pour initier la vidange. Dans l'hypothèse du cas le plus défavorable, cette phase débute immédiatement après la phase de convergence et se termine lorsque la notification de changement de topologie à partir du pont le plus éloigné de la racine a atteint le pont racine.

NOTE Lors d'une défaillance de pont racine, souvent plus d'un pont revendique une racine. Cependant, lorsque la racine de secours présente la meilleure priorité restante, son vecteur de priorité est rapidement (une seule propagation de priorité au sein de la topologie) prépondérant par rapport aux ponts racines temporaires. Toutefois, en cas de scénario le plus défavorable, le meilleur vecteur de priorité issu de l'ancienne racine peut encore “circuler” plus longtemps. Par conséquent, il s'agit de l'élément limite qui définit la longueur de la phase de vieillissement.

Le temps total de reconfiguration de limite supérieure Trec d'un réseau RSTP maillé peut par conséquent être estimé sous la forme:

$$Trec = TL + Tage + Tconv + Tflush$$

où

Tage = 2 × Bridge Max Age × TPA;

Tconv = rayon le plus défavorable × TPA;

Tflush = rayon le plus défavorable × TTC;

Copyright International Electrotechnical Commission

TL est le temps maximal requis par un pont pour détecter une défaillance de liaison (dépend du type de liaison);

TPA est le temps maximal requis par une paire de ponts pour établir une liaison d'accord de proposition RSTP; égal à la somme des temps de traitement BPDU des deux ponts de la paire. Les valeurs TPA peuvent varier d'un fournisseur à un autre et d'un produit à un autre;

TTC est le temps nécessaire à un pont Ethernet pour traiter un changement de topologie RSTP.

Valeurs types d'une implémentation “RSTP rapide”:

TPA = 5 ms lorsque le fournisseur exige 5 ms/saut de temps de rétablissement

TL = 4-6 ms pour des liaisons 100BASE-TX et 100BASE-FX

= 20 ms pour des liaisons 1000BASE-X

= 700 ms pour des liaisons 1000BASE-T (définies par l'ISO/IEC 8802-3)

Cette approximation montre qu'il est avantageux pour le temps total de rétablissement de définir le paramètre Bridge Max Age à une valeur aussi élevée que nécessaire pour prendre en charge la topologie donnée (par rapport aux éventuelles défaillances), mais aussi faible que possible afin de réduire au maximum son impact sur le temps de rétablissement du réseau.

Cette approximation du temps de rétablissement couvre le scénario le plus défavorable, à savoir la défaillance du pont racine. En comparant la probabilité d'une défaillance du pont racine à la probabilité d'une défaillance d'un pont qui ne se trouve pas à la racine ou d'une liaison, une défaillance du pont racine est nettement moins probable (si l'on suppose des probabilités de défaillance similaires pour tous les dispositifs et supports participant) car pour chaque pont racine, un grand nombre de connexions de support et de ponts non-racines peut présenter une défaillance avant.

Par conséquent, le temps de rétablissement type sera plus rapide que le temps de rétablissement du cas le plus défavorable susceptible d'être estimé par le présent article, mais ceci ne peut être pris en compte.

NOTE On peut assister à une conséquence supplémentaire lorsqu'un pont doté de plusieurs ports connectés au réseau RSTP fait partie de la topologie active (en particulier lorsque ce dispositif est la racine), à savoir que l'envoi de BPDU sur les multiples ports n'est pas totalement simultané. Ce phénomène peut être d'autant plus compliqué si différents supports sont présents sur ces multiples ports. Le temps de reconfiguration peut alors être rallongé par cet effet.

Copyright International Electrotechnical Commission

Bibliographie

IEC 61158 (toutes les parties), *Réseaux de communication industriels – Spécifications des bus de terrain*

IEC/TR 61158-1, *Industrial communication networks – Fieldbus specifications – Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series (disponible en anglais seulement)*

IEC/TR 61158-6 (all parts), *Industrial communication networks – Fieldbus specifications – Part 6: Symmetrical pair/quad cables with transmission characteristics up to 1 000 MHz – Work area wiring (disponible en anglais seulement)*

IEC 61588, *Precision clock synchronization protocol for networked measurement and control systems*

IEC 61784-2:2007, *Réseaux de communication industriels – Profils – Partie 2: Profils de bus de terrain complémentaires pour les réseaux en temps réel selon l'ISO/IEC 8802-3*

IEC 61918:2007, *Industrial communication networks – Installation of communication networks in industrial premises*

IEC 62439-2, *Réseaux industriels de communication – Réseaux de haute disponibilité pour l'automation – Partie 2: Protocole de redondance du support (MRP)*

IEC 62439-3, *Réseaux de communication industriels – Réseaux d'automatisme à haute disponibilité – Partie 3: Protocole de redondance parallèle (PRP) et redondance transparente de haute disponibilité (HSR)*

IEC 62439-4, *Réseaux de communication industriels – Réseaux d'automatisme à haute disponibilité – Partie 4: Protocole de Redondance à réseau Croisé (CRP)*

IEC 62439-5, *Réseaux de communication industriels – Réseaux d'automatisme à haute disponibilité – Partie 5: Protocole de redondance à balise (BRP)*

IEC 62439-6, *Réseaux industriels de communication – Réseaux de haute disponibilité pour l'automation – Partie 6: Protocole de redondance distribuée (DRP)*

IEC 62439-7, *Réseaux de communication industriels – Réseaux de haute disponibilité pour l'automation – Partie 7: Protocole de redondance pour réseau en anneau (RRP)*

ISO/IEC 2382 (toutes les parties), *Technologies de l'information – Vocabulaire*

ISO/IEC 9646 (toutes les parties), *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Cadre général et méthodologie des tests de conformité*

ISO/IEC 10731, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Modèle de référence de base – Conventions pour la définition des services OSI*

ISO/IEC 11801:2002, *Technologies de l'information – Câblage générique des locaux d'utilisateurs*
Amendement 1 (2008)

ISO/IEC 15802-3, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseaux locaux et métropolitains – Spécifications communes – Partie 3: Ponts du Contrôle d'accès au support*

Copyright International Electrotechnical Commission

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

PUSTYLNIK M., ZAFIROVIC-VUKOTIC, M., MOORE, R., *Performance of the Rapid Spanning Tree Protocol in Ring Network Topology, Rugged Com. Inc.*
http://www.ruggedcom.com/pdfs/white_%20papers/performance_of_rapid_spanning_tree_protocol_in_ring_network_topology.pdf

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch

Copyright International Electrotechnical Commission