IEC 62439-1

Edition 1.0 2010-02

INTERNATIONAL STANDARD

colour inside

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

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

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 It also gives information on projects, withdrawn and replaced publications.

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

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

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

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

IEC 62439-1

Edition 1.0 2010-02

INTERNATIONAL STANDARD

colour inside

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE XA

ICS 25.040, 35.040

ISBN 978-2-88910-704-9

CONTENTS

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.

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

This standard cancels and replaces IEC 62439 published in 2008. This first edition constitutes a technical revision.

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 text of this standard is based on the following documents:

FDIS	Report on voting
65C/583/FDIS	65C/589/RVD

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

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.

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

INDUSTRIAL COMMUNICATION NETWORKS – HIGH AVAILABILITY AUTOMATION NETWORKS –

Part 1: General concepts and calculation methods

1 Scope

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

This part of the IEC 62439 series specifies

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

2 Normative references

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

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

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

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

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

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

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

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

3 Terms, definitions, abbreviations, acronyms, and conventions

3.1 Terms and definitions

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

3.1.1
availability (performance)
ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided

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

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

[IEV 191-02-05]

3.1.2
channel
layer 2 connection between two end nodes which consists of one or more paths (for redundancy) between end nodes

3.1.3
common mode failure
failure that affects all redundant elements for a given function at the same time

3.1.4
complete failure
failure which results in the complete inability of an item to perform all required functions

[IEV 191-04-20]

3.1.5
connection
logical relationship between two nodes

3.1.6
coverage
probability that a failure is discovered within a time short enough for redundancy to handle it, also expressing the percentage of failures caught up by redundancy vs. total number of failures

3.1.7
cut-through switching
a technology in which a switching node starts transmitting a received frame before this frame has been fully received

3.1.8
degradation failure
failure which is both a gradual failure and a partial failure

[IEV 191-04-22]

3.1.9
dependability
collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance

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

[IEV 191-02-03]

3.1.10
device
physical entity connected to the network composed of communication element and possibly other functional elements

NOTE Devices are for instance nodes, routers and switches.

3.1.11
doubly attached node
node that has two ports for the purpose of redundant operation

3.1.12
edge port
port of a switch connected to a leaf link

3.1.13
end node
node which is producer or consumer of application data

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

3.1.14
error
discrepancy between a computed, observed or measured value or condition and the specified or theoretically correct value or condition

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

NOTE 2 The French term “erreur” may also designate a mistake (see 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]

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.

[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 λ(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.