

INTERNATIONAL STANDARD



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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2010 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembe
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 It also gives information on projects, withdrawn and replaced publications.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

Document generated by EVS



IEC 62439-1

Edition 1.0 2010-02

INTERNATIONAL STANDARD



**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

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	8
2 Normative references.....	8
3 Terms, definitions, abbreviations, acronyms, and conventions.....	9
3.1 Terms and definitions.....	9
3.2 Abbreviations and acronyms.....	16
3.3 Conventions.....	17
3.3.1 General conventions.....	17
3.3.2 Conventions for state machine definitions.....	17
3.3.3 Conventions for PDU specification.....	17
3.4 Reserved network addresses.....	18
4 Conformance requirements (normative).....	18
4.1 Conformance to redundancy protocols.....	18
4.2 Conformance tests.....	19
4.2.1 Concept.....	19
4.2.2 Methodology.....	19
4.2.3 Test conditions and test cases.....	20
4.2.4 Test procedure and measuring.....	20
4.2.5 Test report.....	20
5 Concepts for high availability automation networks (informative).....	21
5.1 Characteristics of application of automation networks.....	21
5.1.1 Resilience in case of failure.....	21
5.1.2 Classes of network redundancy.....	22
5.1.3 Redundancy maintenance.....	22
5.1.4 Comparison and indicators.....	23
5.2 Generic network system.....	24
5.2.1 Network elements.....	24
5.2.2 Topologies.....	26
5.2.3 Redundancy handling.....	32
5.2.4 Network recovery time.....	32
5.2.5 Diagnosis coverage.....	32
5.2.6 Failures.....	32
5.3 Safety.....	34
5.4 Security.....	34
6 Classification of networks (informative).....	34
6.1 Notation.....	34
6.2 Classification of robustness.....	35
7 Availability calculations for selected networks (informative).....	35
7.1 Definitions.....	35
7.2 Reliability models.....	36
7.2.1 Generic symmetrical reliability model.....	36
7.2.2 Simplified symmetrical reliability model.....	38
7.2.3 Asymmetric reliability model.....	38
7.3 Availability of selected structures.....	39
7.3.1 Single LAN without redundant leaves.....	39

7.3.2	Network without redundant leaves	40
7.3.3	Single LAN with redundant leaves	41
7.3.4	Network with redundant leaves	41
7.3.5	Considering second failures	42
7.4	Caveat	44
8	RSTP for High Availability Networks: configuration rules, calculation and measurement method for deterministic recovery time in a ring topology	44
8.1	General	44
8.2	Deployment and configuration rules for the ring topology	44
8.3	Calculations for fault recovery time in a ring	45
8.3.1	Dependencies and failure modes	45
8.3.2	Calculations for non-considered failure modes	45
8.3.3	Calculations for the considered failure modes	45
8.4	Timing measurement method	46
8.4.1	Measurement of T_{PA}	46
8.4.2	Measurement of T_L	47
8.4.3	Measurement of $(T_{TC} + T_F)$	48
8.4.4	System test example	50
	Bibliography	52
	Figure 1 – Conformance test overview	19
	Figure 2 – General network elements (tree topology)	24
	Figure 3 – Link Redundancy Entity in a Doubly Attached Node (DAN)	26
	Figure 4 – Example of tree topology	27
	Figure 5 – Example of linear topology	28
	Figure 6 – Example of ring topology	28
	Figure 7 – Example of a partially meshed topology	29
	Figure 8 – Example of fully meshed topology	30
	Figure 9 – Single LAN structure without redundant leaf links	30
	Figure 10 – Single LAN structure with redundant leaf links	31
	Figure 11 – Redundant LAN structure without redundant leaf links	31
	Figure 12 – Redundant LAN structure with redundant leaf links	31
	Figure 13 – General symmetrical fault model	37
	Figure 14 – Simplified fault model	38
	Figure 15 – Asymmetric fault model	39
	Figure 16 – Network with no redundancy	40
	Figure 17 – Network with no single point of failure	41
	Figure 18 – Network with resiliency to second failure	43
	Figure 19 – Test rig for T_{PA} measurement	47
	Figure 20 – Test rig for T_L measurement	48
	Figure 21 – Test rig for $(T_{TC} + T_F)$ measurement	49
	Figure 22 – Test rig for system test	50
	Table 1 – Examples of application grace time	21
	Table 2 – Examples of redundancy protocols	23

Table 3 – Code assignment for the <TYPE> field 34

Table 4 – Code assignment for the <PLCYleaf> field 34

Table 5 – Code assignment for the <TPLGY> field..... 35

Table 6 – Code assignment for the <ITYPE> field 35

This document is a preview generated by EVS

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.

This document is a preview generated by EVS

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>>