

PUBLICLY AVAILABLE SPECIFICATION



Lifecycle requirements for functional safety and security for IACS



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2020 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

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 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.

Preview generated by EVS



IEC PAS 63325

Edition 1.0 2020-12

PUBLICLY AVAILABLE SPECIFICATION



Lifecycle requirements for functional safety and security for IACS

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040

ISBN 978-2-8322-8861-0

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

CONTENTS

FOREWORD.....	3
INTRODUCTION.....	5
1 Scope.....	6
2 Normative References.....	6
3 Terms, definitions and abbreviated terms.....	6
3.1 Terms and definitions.....	6
3.2 Abbreviated terms.....	8
4 Lifecycle stages.....	8
5 Management coordination requirement.....	8
5.1 General.....	8
5.2 Organization requirements.....	8
5.3 Management of change.....	9
6 Lifecycle requirements.....	9
6.1 Concept and scope.....	9
6.2 Risk assessment.....	10
6.2.1 General requirement.....	10
6.2.2 Hazard and Risk Analysis / Threat-vulnerability assessment.....	11
6.2.3 Risk criterion.....	11
6.2.4 Conflict resolution.....	12
6.3 Development and implementation.....	12
6.3.1 General.....	12
6.3.2 Response to system failures or security events.....	12
6.4 Operation and maintenance.....	13
6.5 Decommission.....	13
Annex A (informative) Measures that could be used in the coordination of safety and security in different stages.....	14
A.1 Risk assessment.....	14
A.2 Development and implementation.....	14
A.2.1 Physical compensation measures are necessary for access control.....	14
A.2.2 Segmentation into zones and perimeter protection.....	14
A.2.3 Safety and security communication protocol.....	14
A.2.4 Remote access control.....	15
A.2.5 Wireless access control.....	15
A.2.6 Device level.....	15
A.2.7 Control level.....	15
A.2.8 Integration of information security protection measures.....	16
A.2.9 Integration of safety and security monitoring.....	16
A.2.10 Monitoring of normal operation.....	16
A.2.11 Routine maintenance and inspection.....	17
A.2.12 Modification.....	17
Figure 1 – General process of risk assessment.....	11
Table 1 – Example of classification of all the systems and devices.....	10

INTERNATIONAL ELECTROTECHNICAL COMMISSION

LIFECYCLE REQUIREMENTS FOR FUNCTIONAL SAFETY AND SECURITY FOR IACS

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.

A PAS is an intermediate specification made available to the public and needing a lower level of consensus than an International Standard to be approved by vote (simple majority).

IEC PAS 63325 has been processed by IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this PAS is based on the following document:

This PAS was approved for publication by the P-members of the committee concerned as indicated in the following document

Draft PAS	Report on voting
65/813/DPAS	65/826/RVDPAS

Following publication of this PAS, which is a pre-standard publication, the technical committee or subcommittee concerned may transform it into an International Standard.

This PAS shall remain valid for an initial maximum period of 2 years starting from the publication date. The validity may be extended for a single period up to a maximum of 2 years, at the end of which it shall be published as another type of normative document, or shall be withdrawn.

IMPORTANT – The "colour inside" logo on the cover page of this document 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.

This document is a preview generated by EVS

INTRODUCTION

Safety and security are becoming increasingly interdependent. Traditional safety-related systems are not isolated any more, as required by connectivity and inter-operability, and threats and vulnerabilities can increase the probability of attacks to safety-related systems. IEC TR 63069 gives some top-level framework recommendations for functional safety and security.

This specification concentrates on how to consider the lifecycles for functional safety and security in different stages, optimizing risk assessment, improving efficiency of safety and security related activities included in engineering processes, avoiding conflicts between safety functions and security countermeasures. This document also will give some safety and security co-engineering guidelines to make the implications to systems more safe, more secure, and cost efficient.

This document is a preview generated by EVS

LIFECYCLE REQUIREMENTS FOR FUNCTIONAL SAFETY AND SECURITY FOR IACS

1 Scope

This PAS provides requirements and guidance for ensuring and assuring functional safety and security in different stages of the lifecycle. It will help the coordination of risk assessment, design and management and operation processes, avoiding conflicts between functional safety and security.

This specification does not aim to define a completely new lifecycle, but based on the functional safety lifecycle, security lifecycle and other state of the art engineering processes, it aims to provide requirements and suggestions to support coordination between functional safety and security.

The objective of this document is Industrial Automation Control Systems (IACS), including the Equipment Under Control (EUC) system and the safety-related system.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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

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

More definitions could refer to the IEC 62443 series and the IEC 61508 series.

3.1.1 conflict

situation when one or several safety measures and one or several security countermeasures are not in coordination with each other and one or several safety measures cannot achieve its required target performance

Note 1 to entry: This conflict definition is in the context of this document.

3.1.2 safety

freedom from unacceptable risk