INTERNATIONAL STANDARD

ISO 13849-1

Second edition
2006-11-01

Safety of machinery — Safety-related parts of control systems —

Part 1: General principles for design

Sécurité des machines — Parties des systèmes de commande relatives à la sécurité —

Partie 1: Principes généraux de conception

Reference number
ISO 13849-1:2006(E)

© ISO 2006

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO 2006

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 ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Contents

Page

Foreword ... v

Introduction ... vi

1 Scope ... 1

2 Normative references ... 1

3 Terms, definitions, symbols and abbreviated terms ... 2
3.1 Terms and definitions ... 2
3.2 Symbols and abbreviated terms ... 8

4 Design considerations ... 9
4.1 Safety objectives in design ... 9
4.2 Strategy for risk reduction ... 11
4.2.1 General ... 11
4.2.2 Contribution to the risk reduction by the control system ... 11
4.3 Determination of required performance level (PL$_r$) ... 14
4.4 Design of SRP/CS ... 14
4.5 Evaluation of the achieved performance level PL and relationship with SIL ... 15
4.5.1 Performance level PL ... 15
4.5.2 Mean time to dangerous failure of each channel (MTTF$_d$) ... 17
4.5.3 Diagnostic coverage (DC) ... 18
4.5.4 Simplified procedure for estimating PL ... 18
4.6 Software safety requirements ... 21
4.6.1 General ... 21
4.6.2 Safety-related embedded software (SRESW) ... 21
4.6.3 Safety-related application software (SRASW) ... 22
4.6.4 Software-based parameterization ... 25
4.7 Verification that achieved PL meets PL$_r$ ... 26
4.8 Ergonomic aspects of design ... 26

5 Safety functions ... 26
5.1 Specification of safety functions ... 26
5.2 Details of safety functions ... 28
5.2.1 Safety-related stop function ... 28
5.2.2 Manual reset function ... 29
5.2.3 Start/restart function ... 29
5.2.4 Local control function ... 30
5.2.5 Muting function ... 30
5.2.6 Response time ... 30
5.2.7 Safety–related parameters ... 30
5.2.8 Fluctuations, loss and restoration of power sources ... 31

6 Categories and their relation to MTTF$_d$ of each channel, DC$_{avg}$ and CCF ... 31
6.1 General ... 31
6.2 Specifications of categories ... 32
6.2.1 General ... 32
6.2.2 Designated architectures ... 32
6.2.3 Category B ... 32
6.2.4 Category 1 ... 33
6.2.5 Category 2 ... 34
6.2.6 Category 3 ... 35
6.2.7 Category 4 ... 36
6.3 Combination of SRP/CS to achieve overall PL ... 39

© ISO 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale