

Edition 1.0 2011-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Industrial communication networks—Profiles PREVIEW
Part 3-18: Functional safety fieldbuses - Additional specifications for CPF 18
(Standards.iten.al)

Réseaux de communication industriels — Profils Partie 3-18: Bus de terrain de sécurité fonctionnelle — Spécifications supplémentaires pour le CPF 1826562/iec-61784-3-18-2011





THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2011 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 la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

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 ARD PREVIEW

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 It also gives information on projects, withdrawn and replaced publications.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. $\underline{IEC~61784-3-18:2011}$

Electropedia: www.electropedia.org ds.iteh.ai/catalog/standards/sist/ac3332fb-bd87-40f1-9671

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: <u>www.iec.ch/webstore/custserv</u>

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

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) 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 CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

■ Catalogue des publications de la CEI: <u>www.iec.ch/searchpub/cur_fut-f.htm</u>

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,...). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

Just Published CEI: www.iec.ch/online news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

■ Electropedia: <u>www.electropedia.org</u>

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

■ Service Clients: <u>www.iec.ch/webstore/custserv/custserv_entry-f.htm</u>

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:

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



Edition 1.0 2011-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Industrial communication networks Aprofiles REVIEW
Part 3-18: Functional safety fieldbuses - Additional specifications for CPF 18

Réseaux de communication industriels - Profils

Partie 3-18: Bus de terrain de sécurité fonctionnelle - Spécifications supplémentaires pour le CPF 182 fc5 c2/iec-61784-3-18-2011

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE CODE PRIX

ICS 13.110, 25.040.40, 35.100.05

ISBN 978-2-88912-475-6

CONTENTS

1 Scope	FΟ	REW	ORD	5	
0.2 Patent declaration 99 1 Scope 10 2 Normative references 10 3 Terms, definitions, symbols, abbreviated terms and conventions 11 3.1 Terms and definitions 11 3.1.1 Common terms and definitions 15 3.2 Symbols and abbreviated terms 16 3.2.1 Common symbols and abbreviated terms 16 3.2.2 CPF 18: Additional symbols and abbreviated terms 17 3.3 Conventions 17 4 Overview of FSCP 18/1 (SafetyNET p™) 19 4.1 General 19 4.2 FSCP 18/1 19 5 General 20 5.1 External documents providing specifications for the profile 20 5.2 Safety functional requirements 21.d.s.tcl	0	Introduction			
1 Scope		0.1	General	7	
2 Normative references		0.2	Patent declaration	9	
3 Terms, definitions, symbols, abbreviated terms and conventions	1	Scop	pe	10	
3.1 Terms and definitions	2	Norn	native references	10	
3.1 Terms and definitions	3	Term	ns, definitions, symbols, abbreviated terms and conventions	11	
3.1.1 Common terms and definitions 3.1.2 CPF 18: Additional terms and definitions 3.2 Symbols and abbreviated terms 3.2.1 Common symbols and abbreviated terms 3.2.2 CPF 18: Additional symbols and abbreviated terms 3.2.2 CPF 18: Additional symbols and abbreviated terms 3.3 Conventions 17 4 Overview of FSCP 18/1 (SafetyNET p™) 4.1 General 4.2 FSCP 18/1 19 5 General 7 Safety functional requirements 19 5.1 External documents providing specifications for the profile 5.2 Safety functional requirements 12 T	Ū	•			
3.1.2 CPF 18: Additional terms and definitions 3.2 Symbols and abbreviated terms		0.1			
3.2 Symbols and abbreviated terms					
3.2.1 Common symbols and abbreviated terms 3.2.2 CPF 18: Additional symbols and abbreviated terms 17 3.3 Conventions 17 4 Overview of FSCP 18/1 (SafetyNET p™) 19 4.1 General 19 4.2 FSCP 18/1 19 5 General 19 5 General 19 5 General 19 5 Safety functional requirements lards item 20 5.1 External documents providing specifications for the profile 20 5.2 Safety functional requirements lards item 21 5.5 Relationships with FAL (and DLL PhL) sest/ac/332/b-bd87-40B-967I 22 5.5.1 General 25 5.5.2 Data Types 26 6 Safety communication layer structure 1.820II 25 5.5.1 General 27 5.5.2 Data Types 22 6.1 General elements 22 6.1 General elements 22 6.1.1 General elements 22 6.1.1 General 22 6.1.2 Safety pipct dictionary 22 6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety heartbeat (SHB) 22 6.1.5 Safety communication relation 23 6.2 Communication relation 23 6.3 Communication relation 24 7.1.1 General 24 7.1.2 Safety pDU format 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety pDU sembedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.3 Safety process data communication 30 7.4 Safety process data communication 30 7.5 Delay monitoring 31 8 Safety communication layer management (SALMT) 28 7.5 Delay monitoring 33 8 Safety communication layer management 34 8.1 Parameter handling		3.2			
3.2.2 CPF 18: Additional symbols and abbreviated terms		·-	•		
3.3 Conventions			•		
4.1 General 19 4.2 FSCP 18/1 19 5 General 20 5.1 External documents providing specifications for the profile 20 5.2 Safety functional requirements and Structure 2.18.201. 20 5.3 Safety measures 20 5.4 Safety communication layer structure 2.18.201. 21 5.5 Relationships with FAL (and DLL, Phily six acid3332ls bd87-400-9671. 22 5.5.1 General 22 5.5.2 Data Types 22 6 Safety communication layer services 22 6.1 General elements 22 6.1.1 General 22 6.1.2 Safety object dictionary 22 6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety process data object (SPDO) 22 6.1.5 Safety delay monitoring (SDM) 23 6.2 Communication layer protocol 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety proce		3.3	•		
4.1 General 19 4.2 FSCP 18/1 19 5 General 20 5.1 External documents providing specifications for the profile 20 5.2 Safety functional requirements and Structure 2.18.201. 20 5.3 Safety measures 20 5.4 Safety communication layer structure 2.18.201. 21 5.5 Relationships with FAL (and DLL, Phily six acid3332ls bd87-400-9671. 22 5.5.1 General 22 5.5.2 Data Types 22 6 Safety communication layer services 22 6.1 General elements 22 6.1.1 General 22 6.1.2 Safety object dictionary 22 6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety process data object (SPDO) 22 6.1.5 Safety delay monitoring (SDM) 23 6.2 Communication layer protocol 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety proce	4	Over	rview of FSCP 18/1 (SafetyNET p™)	19	
4.2 FSCP 18/1 19 5 General 20 5.1 External documents providing specifications for the profile 20 5.2 Safety functional requirements [ards.itch.ai] 20 5.3 Safety measures 20 5.4 Safety communication layer structure 1.18.2011 21 5.5 Relationships with FAL land DLL Phill sist/ac3332fb-bd87-40fl-9671- 22 5.5.1 General 22 5.5.2 Data Types 22 6 Safety communication layer services 22 6.1 General elements 22 6.1.1 General 22 6.1.2 Safety object dictionary 22 6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety delay monitoring (SDM) 23 6.2 Communication relation 23 7 Safety communication layer protocol 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety process data communication a Type 22 PDU 28 7.2					
5 General 20 5.1 External documents providing specifications for the profile 20 5.2 Safety functional requirements 20 5.3 Safety measures 20 5.4 Safety communication layer structure 18.2011 2.5 Relationships with FAL (and DLL) PhL) sist/ac3332lb-bd87-40f1-9671 22 5.5.1 General 7955c4265c2 ac-61784-3-18-2011 22 5.5.2 Data Types 22 6 Safety communication layer services 22 6.1 General elements 22 6.1.1 General elements 22 6.1.2 Safety object dictionary 22 6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety delay monitoring (SDM) 23 6.2 Communication relation 23 7 Safety communication layer protocol 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety process data communication 26 7.1.4 Safety process data communication					
5.2 Safety functional requirements and structure 3. IS20II. 20 5.3 Safety measures. 20 5.4 Safety communication layer structure 3. IS20II. 21 5.5 Relationships with FALCand DLC. Pht sist/ac3332fb-bd87-40fl-9671. 22 5.5.1 General	5				
5.2 Safety functional requirements and structure 3. IS20II. 20 5.3 Safety measures. 20 5.4 Safety communication layer structure 3. IS20II. 21 5.5 Relationships with FALCand DLC. Pht sist/ac3332fb-bd87-40fl-9671. 22 5.5.1 General		5 1	External documents providing specifications for the profile	20	
5.3 Safety measures 20 5.4 Safety communication layer structure 3-18:2011 21 5.5 Relationships with FAL (and DLS Pht Sstrac3332h-bd87-40f1-9671- 22 5.5.1 General 7953c42is52/rcc-61784-3-18-2011 22 5.5.2 Data Types 22 6 Safety communication layer services 22 6.1 General elements 22 6.1.1 General elements 22 6.1.2 Safety object dictionary 22 6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety heartbeat (SHB) 22 6.1.5 Safety delay monitoring (SDM) 23 6.2 Communication relation 23 7 Safety communication layer protocol 24 7.1 Safety PDU format 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety process data objects (SPDO) 24 7.1.4 Safety process data communication 30 7.4 Safety process data communication 30			Safety functional requirements lands iteh.ai	20	
5.4 Safety communication layer structure 3-18:2011 21 5.5 Relationships with FAL cand DLLS Phills/sst/ac33326-bd87-40f1-9671- 22 5.5.1 General 7953c42652/cc-61784-3-18-2011 22 5.5.2 Data Types 22 6 Safety communication layer services 22 6.1 General elements 22 6.1.1 General 22 6.1.2 Safety object dictionary 22 6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety heartbeat (SHB) 22 6.1.5 Safety delay monitoring (SDM) 23 6.2 Communication relation 23 7 Safety pout format 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety process data objects (SPDO) 24 7.1.4 Safety pous embedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.5 Delay monitoring 33 8 Safety communication layer management 34					
5.5 Relationships with PAL cand DLL Philips six a 3332h-bd87-40f1-9671- 22 5.5.1 General (1953-42 lecc-2) lecc-61784-3-18-2011 22 5.5.2 Data Types 22 6 Safety communication layer services 22 6.1 General elements 22 6.1.1 General 22 6.1.2 Safety object dictionary 22 6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety heartbeat (SHB) 22 6.1.5 Safety delay monitoring (SDM) 23 6.2 Communication relation 23 7 Safety communication layer protocol 24 7.1 Safety PDU format 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety heartbeat (SHB) 26 7.1.4 Safety PDUs embedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.5 Delay monitoring 33 8 Safety communication layer management 34 <td< td=""><td></td><td>•</td><td></td></td<>			•		
5.5.2 Data Types 22 6 Safety communication layer services 22 6.1 General elements 22 6.1.1 General 22 6.1.2 Safety object dictionary 22 6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety heartbeat (SHB) 22 6.1.5 Safety delay monitoring (SDM) 23 6.2 Communication relation 23 7 Safety communication layer protocol 24 7.1 Safety PDU format 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety heartbeat (SHB) 26 7.1.4 Safety PDUs embedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.3 Safety heartbeat 32 7.5 Delay monitoring 33 8 Safety communication layer management 34 8.1 Parameter handling 34		5.5	Relationships / withar Alterancatolog/stappards/sist/ac3332fb-bd87-40f1-9671-	22	
5.5.2 Data Types 22 6 Safety communication layer services 22 6.1 General elements 22 6.1.1 General 22 6.1.2 Safety object dictionary 22 6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety heartbeat (SHB) 22 6.1.5 Safety delay monitoring (SDM) 23 6.2 Communication relation 23 7 Safety communication layer protocol 24 7.1 Safety PDU format 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety heartbeat (SHB) 26 7.1.4 Safety PDUs embedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.3 Safety heartbeat 32 7.5 Delay monitoring 33 8 Safety communication layer management 34 8.1 Parameter handling 34			5.5.1 General	22	
6.1 General elements 22 6.1.1 General 22 6.1.2 Safety object dictionary 22 6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety heartbeat (SHB) 22 6.1.5 Safety delay monitoring (SDM) 23 6.2 Communication relation 23 7 Safety communication layer protocol 24 7.1 Safety PDU format 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety heartbeat (SHB) 26 7.1.4 Safety PDUs embedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.3 Safety heartbeat 32 7.5 Delay monitoring 33 8 Safety communication layer management 34 8.1 Parameter handling 34					
6.1.1 General 22 6.1.2 Safety object dictionary 22 6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety heartbeat (SHB) 22 6.1.5 Safety delay monitoring (SDM) 23 6.2 Communication relation 23 7 Safety communication layer protocol 24 7.1 Safety PDU format 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety heartbeat (SHB) 26 7.1.4 Safety PDUs embedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.3 Safety heartbeat 32 7.5 Delay monitoring 33 8 Safety communication layer management 34 8.1 Parameter handling 34	6	•			
6.1.2 Safety object dictionary 22 6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety heartbeat (SHB) 22 6.1.5 Safety delay monitoring (SDM) 23 6.2 Communication relation 23 7 Safety communication layer protocol 24 7.1 Safety PDU format 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety heartbeat (SHB) 26 7.1.4 Safety PDUs embedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.3 Safety process data communication 30 7.4 Safety heartbeat 32 7.5 Delay monitoring 33 8 Safety communication layer management 34 8.1 Parameter handling 34		6.1	General elements	22	
6.1.2 Safety object dictionary 22 6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety heartbeat (SHB) 22 6.1.5 Safety delay monitoring (SDM) 23 6.2 Communication relation 23 7 Safety communication layer protocol 24 7.1 Safety PDU format 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety heartbeat (SHB) 26 7.1.4 Safety PDUs embedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.3 Safety process data communication 30 7.4 Safety heartbeat 32 7.5 Delay monitoring 33 8 Safety communication layer management 34 8.1 Parameter handling 34					
6.1.3 Safety process data object (SPDO) 22 6.1.4 Safety heartbeat (SHB) 22 6.1.5 Safety delay monitoring (SDM) 23 6.2 Communication relation 23 7 Safety communication layer protocol 24 7.1 Safety PDU format 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety heartbeat (SHB) 26 7.1.4 Safety PDUs embedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.3 Safety process data communication 30 7.4 Safety heartbeat 32 7.5 Delay monitoring 33 8 Safety communication layer management 34 8.1 Parameter handling 34					
6.1.5 Safety delay monitoring (SDM) 23 6.2 Communication relation 23 7 Safety communication layer protocol 24 7.1 Safety PDU format 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety heartbeat (SHB) 26 7.1.4 Safety PDUs embedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.3 Safety process data communication 30 7.4 Safety heartbeat 32 7.5 Delay monitoring 33 8 Safety communication layer management 34 8.1 Parameter handling 34					
6.2 Communication relation 23 7 Safety communication layer protocol 24 7.1 Safety PDU format 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety heartbeat (SHB) 26 7.1.4 Safety PDUs embedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.3 Safety process data communication 30 7.4 Safety heartbeat 32 7.5 Delay monitoring 33 8 Safety communication layer management 34 8.1 Parameter handling 34			6.1.4 Safety heartbeat (SHB)	22	
7 Safety communication layer protocol 24 7.1 Safety PDU format 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety heartbeat (SHB) 26 7.1.4 Safety PDUs embedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.3 Safety process data communication 30 7.4 Safety heartbeat 32 7.5 Delay monitoring 33 8 Safety communication layer management 34 8.1 Parameter handling 34					
7.1 Safety PDU format 24 7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety heartbeat (SHB) 26 7.1.4 Safety PDUs embedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.3 Safety process data communication 30 7.4 Safety heartbeat 32 7.5 Delay monitoring 33 8 Safety communication layer management 34 8.1 Parameter handling 34		6.2	Communication relation	23	
7.1.1 General 24 7.1.2 Safety process data objects (SPDO) 24 7.1.3 Safety heartbeat (SHB) 26 7.1.4 Safety PDUs embedded in a Type 22 PDU 28 7.2 Safety communication layer management (SALMT) 28 7.3 Safety process data communication 30 7.4 Safety heartbeat 32 7.5 Delay monitoring 33 8 Safety communication layer management 34 8.1 Parameter handling 34	7	Safe	ty communication layer protocol	24	
7.1.2 Safety process data objects (SPDO)		7.1	Safety PDU format	24	
7.1.3 Safety heartbeat (SHB)			7.1.1 General	24	
7.1.4 Safety PDUs embedded in a Type 22 PDU			7.1.2 Safety process data objects (SPDO)	24	
7.2Safety communication layer management (SALMT)287.3Safety process data communication307.4Safety heartbeat327.5Delay monitoring338Safety communication layer management348.1Parameter handling34			7.1.3 Safety heartbeat (SHB)	26	
7.3Safety process data communication307.4Safety heartbeat327.5Delay monitoring338Safety communication layer management348.1Parameter handling34			7.1.4 Safety PDUs embedded in a Type 22 PDU	28	
7.4Safety heartbeat327.5Delay monitoring338Safety communication layer management348.1Parameter handling34		7.2	Safety communication layer management (SALMT)	28	
7.5 Delay monitoring		7.3	Safety process data communication	30	
8 Safety communication layer management		7.4	Safety heartbeat	32	
8.1 Parameter handling34		7.5	Delay monitoring	33	
	8	Safe	ty communication layer management	34	
8.2 Safety object dictionary34		8.1 Parameter handling			
		8.2	Safety object dictionary	34	

		8.2.1	General	34	
		8.2.2	Communication profile section	35	
		8.2.3	Standardized device profile section		
9	System requirements				
	9.1	Indicat	ors and switches	51	
		9.1.1	Indicator states and flash rates	51	
		9.1.2	Indicators		
		9.1.3	Switches		
	9.2	9			
	9.3		function response time		
		9.3.1	General		
		9.3.2	Determination of FSCP 18/1 time expectation behavior		
	0.4	9.3.3	Calculation of the worst case safety function response time		
	9.4		on of demands		
	9.5	9.5.1	aints for calculation of system characteristics Safety related constraints		
		9.5.1	Probabilistic considerations		
	9.6	· · · · · -	nance		
	9.7		manual		
10		•			
Δnr	ρν Δ	(informs	itive) Additional information for functional safety communication		
pro	files o	f CPF 1	8	57	
Anr	ex B	(informa	8 (standards.iteh.ai) Itive) Information for assessment of the functional safety		
con	nmuni	cation p	rofiles of CPF 18 <u>IEC 61784-3-18:2011</u>	58	
Bib	iogra	ohv	https://standards.iteh:ai/catalog/standards/sist/ac3332fb-bd87-40fl-9671	50	
	0 1	. ,	11. Ups//startuards.1tc11.a/catalog/startuards/sis/ac333210-006/-4011-90/1-		
	5 1	,	7953c42fe5c2/iec-61784-3-18-2011		
			7953c42fe5c2/iec-61784-3-18-2011		
Tab	ole 1 –	Object	7953c42fe5c2/iec-61784-3-18-2011 definition	18	
Tab Tab	ole 1 – ole 2 –	Object Safety	7953c42fe5c2/iec-61784-3-18-2011 definition	18	
Tab Tab Tab	ole 1 – ole 2 – ole 3 –	Object Safety Commi	7953c42fe5c2/iec-61784-3-18-2011 definition	18 18	
Tab Tab Tab	ole 1 – ole 2 – ole 3 – ole 4 –	Object Safety Commi	7953c42fe5c2/iec-61784-3-18-2011 definition	18 18 21	
Tab Tab Tab Tab	ole 1 – ole 2 – ole 3 – ole 4 – ole 5 –	Object Safety Commo SPDO SHB re	7953c42fe5c2/iec-61784-3-18-2011 definition	18 21 25	
Tab Tab Tab Tab Tab	ole 1 – ole 2 – ole 3 – ole 4 – ole 5 – ole 6 –	Object Safety Commo SPDO SHB re	7953c42fe5c2/iec-61784-3-18-2011 definition	18212526	
Tab Tab Tab Tab Tab	ole 1 – ole 2 – ole 3 – ole 4 – ole 5 – ole 6 –	Object Safety Commo SPDO SHB re SHB re	7953c42fe5c2/iec-61784-3-18-2011 definition	1821252627	
Tab Tab Tab Tab Tab Tab	ole 1 – ole 2 – ole 3 – ole 4 – ole 5 – ole 6 – ole 7 – ole 8 –	Object Safety Commo SPDO SHB re SHB re SHB sa	7953c42fe5c2/iec-61784-3-18-2011 definition PDU element definition unication errors and detection measures PDU structure equest PDU structure esponse PDU structure afety communication layer state encoding	182125262727	
Tab Tab Tab Tab Tab Tab Tab	ole 1 – ole 2 – ole 3 – ole 4 – ole 5 – ole 6 – ole 7 – ole 8 –	Object Safety Common SPDO SHB re SHB re SHB sa SALMT System	7953c42fe5c2/iec-61784-3-18-2011 definition	18212526272728	
Tab Tab Tab Tab Tab Tab Tab	ole 1 – ole 2 – ole 3 – ole 5 – ole 6 – ole 7 – ole 8 – ole 9 –	Object Safety Commo SPDO SHB re SHB sa SALMT System – State	definition	18212526272829	
Tab Tab Tab Tab Tab Tab Tab Tab	ole 1 – ole 2 – ole 3 – ole 4 – ole 5 – ole 6 – ole 8 – ole 9 – ole 10	Object Safety Commo SPDO SHB re SHB sa SALMT System - State - Syste	definition	182125262728293031	
Tab Tab Tab Tab Tab Tab Tab Tab	le 1 – le 2 – le 3 – le 4 – le 5 – le 6 – le 7 – le 8 – le 9 – le 10	Object Safety Common SPDO SHB re SHB sa SALMT System State System System System	definition PDU element definition unication errors and detection measures PDU structure exponse PDU structure afety communication layer state encoding commands states of SALMT state machine m states of RxSPDO state machine m states of RxSPDO state machine	182125262728293031	
Tab Tab Tab Tab Tab Tab Tab Tab Tab	ole 1 – ole 2 – ole 3 – ole 4 – ole 5 – ole 6 – ole 8 – ole 9 – ole 10 ole 11 ole 12	Object Safety Commo SPDO SHB re SHB sa SALMT System System Syste Syste State Timed	definition PDU element definition unication errors and detection measures PDU structure equest PDU structure esponse PDU structure afety communication layer state encoding commands a states of SALMT state machine transitions SALMT state machine m states of RxSPDO state machine transitions RxSPDO state machine		
Tab Tab Tab Tab Tab Tab Tab Tab Tab	ole 1 – ole 2 – ole 3 – ole 5 – ole 5 – ole 7 – ole 9 – ole 10 ole 11 ole 12 ole 13	Object Safety Common SPDO SHB re SHB sa SALMT System State State State State State State State State	definition		
Tab	le 1 – le 2 – le 3 – le 4 – le 5 – le 6 – le 7 – le 9 – le 10 le 11 le 12 le 13 le 14	Object Safety Common SPDO SHB resident SHB safety SHB safety SHB safety State State State State State State State State Object	definition PDU element definition unication errors and detection measures PDU structure quest PDU structure sponse PDU structure afety communication layer state encoding commands states of SALMT state machine transitions SALMT state machine m states of RxSPDO state machine transitions RxSPDO state machine outs		
Tab	ole 1 – ole 2 – ole 3 – ole 4 – ole 5 – ole 6 – ole 7 – ole 9 – ole 10 ole 11 ole 12 ole 13 ole 14 ole 15	Object Safety Common SPDO SHB re SHB sa SALMT System State System State State State State Device Device	definition		
Tab	le 1 – le 2 – le 3 – le 4 – le 5 – le 6 – le 7 – le 10 le 11 le 12 le 13 le 14 le 15 le 16	Object Safety Common SPDO SHB res SHB sa SALMT System System State State State State State Device Safety	definition		

Table 20 – Safety producer heartbeat parameter	39
Table 21 – Safety bus cycle times	42
Table 22 – SPDO timeout tolerance	43
Table 23 – Receive SPDO communication parameter	43
Table 24 – Transmit SPDO communication parameter	46
Table 25 – Mapping format	49
Table 26 – Receive SPDO mapping parameter	49
Table 27 – Transmit SPDO mapping parameter	50
Table 28 – Indicator states definiton	51
Table 29 – STATUS indicator states	51
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	7
Figure 2 – Relationships of IEC 61784-3 with other standards (process)	8
Figure 3 – FSCP 18/1 system	19
Figure 4 – FSCP 18/1 software architecture	21
Figure 5 – SPDO interaction model	23
Figure 6 – SHB interaction model	
Figure 7 – Safety process data object structure R.D. P.R.E.V.I.E.W.	24
Figure 8 – Safety heartbeat request structure	26
Figure 8 – Safety heartbeat request structure ds.item.ai) Figure 9 – Safety heartbeat response structure	26
Figure 10 – Safety PDU for FSCP 18/1 embedded in a Type 22 CDC data section	28
Figure 11 – SALMThistate machine hai/catalog/standards/sist/ac3332fb-bd87-40f1-9671-7953c42fe5c2/iec-61784-3-18-2011 Figure 12 – RxSPDO state machine	29
Figure 12 – RxSPDO state machine	31
Figure 13 – Heartbeat procedure	32
Figure 14 – Delay measurement principle	33
Figure 15 – Parameter handling	34
Figure 16 – Safety response time components	52
Figure 17 – Considered data fields for message size calculation	54
Figure 18 – Residual error rate	55

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18

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 the corresponding national or regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

 7953c42fe5c2/iec-61784-3-18-2011
- 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.

International Standard IEC 61784-3-18 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/PAS 61784-3-18 published in 2009. This first edition constitutes a technical revision.

The text of this standard is based on the following documents:

FDIS	Report on voting
65C/639/FDIS	65C/649/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.

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

A list of all parts of the IEC 61784-3 series, published under the general title *Industrial* communication networks – Profiles – Functional safety fieldbuses, can be found on the IEC website.

The committee has decided that the contents of this 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.

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.

iTeh STANDARD PREVIEW (standards.iteh.ai)

<u>IEC 61784-3-18:2011</u> https://standards.iteh.ai/catalog/standards/sist/ac3332fb-bd87-40f1-9671-7953c42fe5c2/iec-61784-3-18-2011

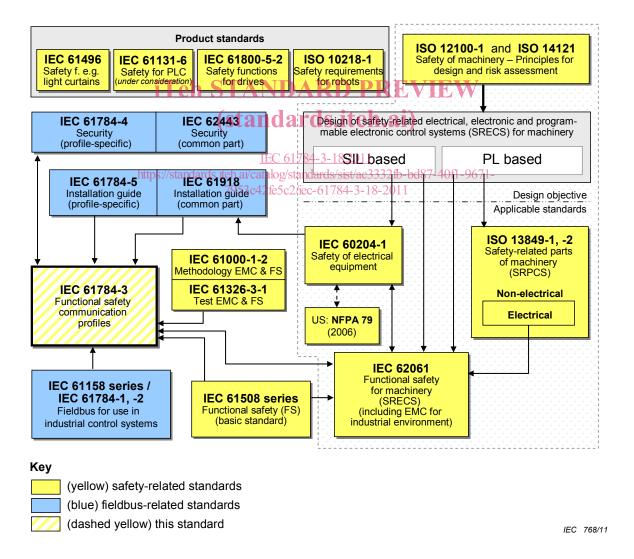
0 Introduction

0.1 General

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus many fieldbus enhancements are emerging, addressing not yet standardized areas such as real time, safety-related and security-related applications.

This standard explains the relevant principles for functional safety communications with reference to IEC 61508 series and specifies several safety communication layers (profiles and corresponding protocols) based on the communication profiles and protocol layers of IEC 61784-1, IEC 61784-2 and the IEC 61158 series. It does not cover electrical safety and intrinsic safety aspects.

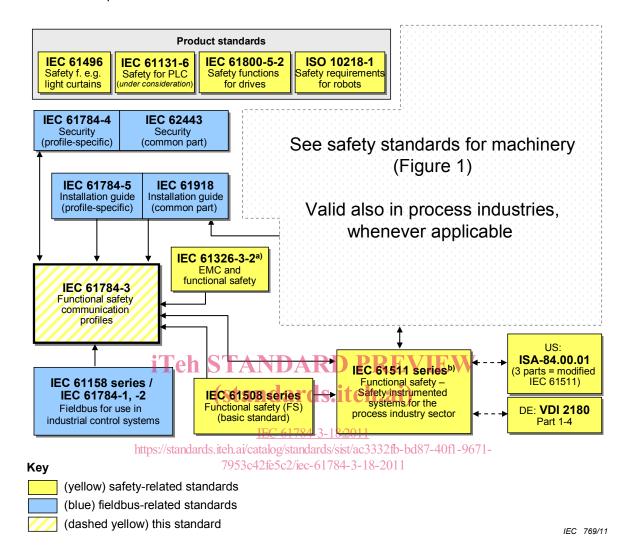
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



NOTE Subclauses 6.7.6.4 (high complexity) and 6.7.8.1.6 (low complexity) of IEC 62061 specify the relationship between PL (Category) and SIL.

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

Figure 2 shows the relationships between this standard and relevant safety and fieldbus standards in a process environment.



a For specified electromagnetic environments; otherwise IEC 61326-3-1.

Figure 2 – Relationships of IEC 61784-3 with other standards (process)

Safety communication layers which are implemented as parts of safety-related systems according to IEC 61508 series provide the necessary confidence in the transportation of messages (information) between two or more participants on a fieldbus in a safety-related system, or sufficient confidence of safe behaviour in the event of fieldbus errors or failures.

Safety communication layers specified in this standard do this in such a way that a fieldbus can be used for applications requiring functional safety up to the Safety Integrity Level (SIL) specified by its corresponding functional safety communication profile.

The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system – implementation of a functional safety communication profile in a standard device is not sufficient to qualify it as a safety device.

b EN ratified.

This standard describes:

- basic principles for implementing the requirements of IEC 61508 series for safetyrelated data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- individual description of functional safety profiles for several communication profile families in IEC 61784-1 and IEC 61784-2;
- safety layer extensions to the communication service and protocols sections of the IEC 61158 series.

0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning the functional safety communication profiles for family 18 as follows, where the [xx] notation indicates the holder of the patent right:

DE 10 2008 007 672.4-31 [PI] Verfahren und Vorrichtung zum Übertragen von Daten in einem Netzwerk

IEC takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the IEC that he/she is willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with IEC. Information may be obtained from

Information may be obtained from:

IEC 61784-3-18:2011

https://standards.iteh.ai/catalog/standards/sist/ac3332fb-bd87-40f1-9671-Pilz GmbH & G93cKG-5c2/iec-61784-3-18-2011

[PI]

Felix-Wankel-Str. 2 73760 Ostfildern **GERMANY**

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. IEC shall not be held responsible for identifying any or all such patent rights.

ISO (www.iso.org/patents) and IEC (http://www.iec.ch/tctools/patent_decl.htm) maintain online data bases of patents relevant to their standards. Users are encouraged to consult the data bases for the most up to date information concerning patents.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 18 of IEC 61784-2 and IEC 61158 Type 22. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer.

NOTE 1 It does not cover electrical safety and intrinsic safety aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres.

This part¹ defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series² for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery. **Teh STANDARD PREVIEW**

This part provides guidelines for both developers and assessors of compliant devices and systems.

NOTE 2 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system implementation of a functional safety communication profile according to this part in a standard device is not sufficient to qualify it as a safety device.

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 61158-3-22, Industrial communication networks — Fieldbus specifications — Part 3-22: Data-link layer service definition — Type 22 elements

IEC 61158-4-22, Industrial communication networks — Fieldbus specifications — Part 4-22: Data-link layer protocol specification — Type 22 elements

IEC 61158-5-22, Industrial communication networks — Fieldbus specifications — Part 5-22: Application layer service definition — Type 22 elements

IEC 61158-6-22, Industrial communication networks — Fieldbus specifications — Part 6-22: Application layer protocol specification — Type 22 elements

IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems

In the following pages of this standard, "this part" will be used for "this part of the IEC 61784-3 series".

² In the following pages of this standard, "IEC 61508" will be used for "IEC 61508 series".

IEC 61508-2:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

IEC 61784-2:2010, Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3

IEC 61784-3:2010, Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions

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

ISO/IEC 10731, Information technology — Open system interconnection — Basic reference model — Conventions for the definition of OSI services

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

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

3.1.1 Common terms and definitions DARD PREVIEW

3.1.1.1

availability

(standards.iteh.ai)

probability for an automated system that for a given period of time there are no unsatisfactory system conditions such as loss of production 84-3-18:2011

https://standards.iteh.ai/catalog/standards/sist/ac3332fb-bd87-40f1-9671-

3.1.1.2

7953c42fe5c2/iec-61784-3-18-2011

black channel

communication channel without available evidence of design or validation according to IEC 61508

3.1.1.3

communication channel

logical connection between two end-points within a communication system

3.1.1.4

communication system

arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498 application layer) from one application to another

3.1.1.5

connection

logical binding between two application objects within the same or different devices

3.1.1.6

Cyclic Redundancy Check (CRC)

<value> redundant data derived from, and stored or transmitted together with, a block of data in order to detect data corruption

<method> procedure used to calculate the redundant data

NOTE 1 Terms "CRC code" and "CRC signature", and labels such as CRC1, CRC2, may also be used in this standard to refer to the redundant data.

NOTE 2 See also [35], [36]³.

3.1.1.7

error

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

[IEC 61508-4:2010], [IEC 61158]

NOTE 1 Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

NOTE 2 Errors do not necessarily result in a failure or a fault.

3.1.1.8

failure

termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

NOTE 1 The definition in IEC 61508-4 is the same, with additional notes.

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.11, modified]

NOTE 2 Failure may be due to an error (for example, problem with hardware/software design or message disruption).

3.1.1.9

fault iTeh STANDARD PREVIEW

abnormal condition that may cause a reduction in, or loss of the capability of a functional unit to perform a required function (Standards.iten.ai)

NOTE IEV 191-05-01 defines "fault" as a state characterized by the inability to perform a required function, excluding the inability during a preventive amaintenance or other splanned actions, or due to lack of external resources.

7953c42fe5c2/iec-61784-3-18-2011

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.10, modified]

3.1.1.10

fieldbus

communication system based on serial data transfer and used in industrial automation or process control applications

3.1.1.11

frame

denigrated synonym for DLPDU

3.1.1.12

Frame Check Sequence (FCS)

redundant data derived from a block of data within a DLPDU (frame), using a hash function, and stored or transmitted together with the block of data, in order to detect data corruption

NOTE 1 An FCS can be derived using for example a CRC or other hash function.

NOTE 2 See also [35], [36].

3.1.1.13

hash function

(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

³ Figures in square brackets refer to the Bibliography.

NOTE 1 Hash functions can be used to detect data corruption.

NOTE 2 Common hash functions include parity, checksum or CRC.

[IEC/TR 62210, modified]

3.1.1.14

hazard

state or set of conditions of a system that, together with other related conditions will inevitably lead to harm to persons, property or environment

3.1.1.15

message

ordered series of octets intended to convey information

[ISO/IEC 2382-16.02.01, modified]

3.1.1.16

message sink

part of a communication system in which messages are considered to be received

[ISO/IEC 2382-16.02.03]

3.1.1.17

message source

part of a communication system from which messages are considered to originate

[ISO/IEC 2382-16.02.02]

(standards.iteh.ai)

3.1.1.18

nuisance trip

IEC 61784-3-18:2011

spurious trip with no harmful effect ai/catalog/standards/sist/ac3332fb-bd87-40f1-9671-953c42fe5c2/iec-61784-3-18-2011

NOTE Internal abnormal errors can be caused in communication systems such as wireless transmission, for example by too many retries in the presence of interferences.

3.1.1.19

performance level (PL)

discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

[ISO 13849-1]

3.1.1.20

redundancy

existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

[IEC 61508-4:2010, modified], [ISO/IEC 2382-14.01.12, modified]

3.1.1.21

risk

combination of the probability of occurrence of harm and the severity of that harm

NOTE For more discussion on this concept see Annex A of IEC 61508-5:2010.

[IEC 61508-4:2010], [ISO/IEC Guide 51:1999, definition 3.2]

3.1.1.22

safety communication layer (SCL)

communication layer that includes all the necessary measures to ensure safe transmission of data in accordance with the requirements of IEC 61508