



TECHNICAL REPORT

**Functional safety – Safety instrumented systems for the process industry sector –
Part 4: Explanation and rationale for changes in IEC 61511-1 from Edition 1 to
Edition 2**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110, ICS 25.040.01

ISBN 978-2-8322-7870-3

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

CONTENTS

CONTENTS	2
FOREWORD	5
INTRODUCTION	7
1 Scope	8
2 Normative references	8
3 Terms, definitions and abbreviated terms	8
3.1 Terms and definitions	8
3.2 Abbreviated terms	9
4 Background	10
5 Management of functional safety (IEC 61511-1 Ed. 2 Clause 5)	10
5.1 Why is this clause important?	10
5.2 Common misconceptions	10
5.3 What was changed from Ed. 1 to Ed. 2 and why?	11
5.3.1 Existing systems	11
5.3.2 Change management	11
5.3.3 Performance metrics and quality assurance	11
5.3.4 Competency	12
5.3.5 More requirements for functional safety product and service providers	12
5.4 Summary on how	12
6 Safety life cycle (IEC 61511-1 Ed. 2 Clause 6)	12
6.1 Why is this clause important?	12
6.2 Common misconceptions	12
6.3 What was changed from Ed. 1 to Ed. 2 and why?	13
6.4 Summary on how	13
7 Verification (IEC 61511-1 Ed. 2 Clause 7)	13
7.1 Why is this clause important?	13
7.2 Common misconceptions	13
7.3 What was changed from Ed. 1 to Ed. 2 and why?	13
7.4 Summary on how	13
8 Hazard and risk analysis (IEC 61511-1 Ed. 2 Clause 8)	13
8.1 Why is this clause important?	13
8.2 Common misconceptions	14
8.3 What was changed from Ed. 1 to Ed. 2 and why?	14
8.4 Summary on how	15
9 Allocation of safety functions to protection layers (IEC 61511-1 Ed. 2 Clause 9)	15
9.1 Why is this clause important?	15
9.2 Common misconceptions	15
9.3 What was changed from Ed. 1 to Ed. 2 and why?	16
9.3.1 Limits on BPCS protection layers	16
9.3.2 Requirements for claiming RRF > 10 000 in total for instrumented safeguards	16
9.4 Summary on how	16
10 SIS safety requirements specification (IEC 61511-1 Ed. 2 Clause 10)	17
10.1 Why is this clause important?	17
10.2 Common misconceptions	17
10.3 What was changed from Ed. 1 to Ed. 2 and why?	18

10.4	Summary on how	18
11	Design and engineering (IEC 61511-1 Ed. 2 Clause 11)	18
11.1	Why is this clause important?	18
11.2	Common misconceptions	18
11.3	What was changed from Ed. 1 to Ed. 2 and why?.....	19
11.3.1	Hardware fault tolerance.....	19
11.3.2	Security risk requirements	20
11.3.3	Safety manual	20
11.3.4	Requirements for system behaviour on detection of a fault	20
11.3.5	Limitations on field device communication design	21
11.4	Summary on how	21
12	Application program development (IEC 61511-1 Ed. 2 Clause 12)	21
12.1	Why is this clause important?	21
12.2	Common misconceptions	22
12.3	What was changed from Ed. 1 to Ed. 2 and why?.....	22
12.4	Summary on how	22
13	Factory acceptance test (IEC 61511-1 Ed. 2 Clause 13)	22
13.1	Why is this clause important?	22
13.2	Common misconceptions	23
13.3	What was changed from Ed. 1 to Ed. 2 and why?.....	23
13.4	Summary on how	23
14	Installation (IEC 61511-1 Ed. 2 Clause 14)	23
14.1	Why is this clause important?	23
14.2	Common misconceptions	24
14.3	What was changed from Ed. 1 to Ed. 2 and why?.....	24
14.4	Summary on how	24
15	Validation (IEC 61511-1 Ed. 2 Clause 15).....	24
15.1	Why is this clause important?	24
15.2	Common misconceptions	24
15.3	What was changed from Ed. 1 to Ed. 2 and why?.....	24
15.4	Summary on how	24
16	Operation and maintenance (IEC 61511-1 Ed. 2 Clause 16)	25
16.1	Why is this clause important?	25
16.2	Common misconceptions	25
16.3	What was changed from Ed. 1 to Ed. 2 and why?.....	26
16.3.1	Fault detection, bypassing, and compensating measures.....	26
16.3.2	Proof testing after repair and change	26
16.4	Summary on how	26
17	Modification (IEC 61511-1 Ed. 2 Clause 17)	26
17.1	Why is this clause important?	26
17.2	Common misconceptions	26
17.3	What was changed from Ed. 1 to Ed. 2 and why?.....	27
	Planning for and completing change	27
17.4	Summary on how	27
18	Decommissioning (IEC 61511-1 Ed. 2 Clause 18).....	27
18.1	Why is this clause important?	27
18.2	Common misconceptions	27