

CONTENTS

FOREWORD	9
INTRODUCTION	11
1 Scope	13
2 Normative references	13
3 Terms, definitions, abbreviated terms, acronyms and conventions	13
3.1 Terms and definitions.....	13
3.2 Abbreviated terms and acronyms	16
3.3 Conventions.....	17
4 Zone, conduit and risk assessment requirements	17
4.1 Overview.....	17
4.2 ZCR 1: Identify the SUC.....	19
4.2.1 ZCR 1.1: Identify the SUC perimeter and access points	19
4.3 ZCR 2: Initial cyber security risk assessment	19
4.3.1 ZCR 2.1: Perform initial cyber security risk assessment	19
4.4 ZCR 3: Partition the SUC into zones and conduits	19
4.4.1 Overview	19
4.4.2 ZCR 3.1: Establish zones and conduits	20
4.4.3 ZCR 3.2: Separate business and IACS assets	20
4.4.4 ZCR 3.3: Separate safety related assets	20
4.4.5 ZCR 3.4: Separate temporarily connected devices	21
4.4.6 ZCR 3.5: Separate wireless devices	21
4.4.7 ZCR 3.6: Separate devices connected via external networks	21
4.5 ZCR 4: Risk comparison	21
4.5.1 Overview	21
4.5.2 ZCR 4.1: Compare initial risk to tolerable risk.....	21
4.6 ZCR 5: Perform a detailed cyber security risk assessment	22
4.6.1 Overview	22
4.6.2 ZCR 5.1: Identify threats	23
4.6.3 ZCR 5.2: Identify vulnerabilities.....	24
4.6.4 ZCR 5.3: Determine consequence and impact	24
4.6.5 ZCR 5.4: Determine unmitigated likelihood.....	25
4.6.6 ZCR 5.5: Determine unmitigated cyber security risk	25
4.6.7 ZCR 5.6: Determine SL-T.....	25
4.6.8 ZCR 5.7: Compare unmitigated risk with tolerable risk.....	26
4.6.9 ZCR 5.8: Identify and evaluate existing countermeasures	26
4.6.10 ZCR 5.9: Reevaluate likelihood and impact	26
4.6.11 ZCR 5.10: Determine residual risk.....	27
4.6.12 ZCR 5.11: Compare residual risk with tolerable risk	27
4.6.13 ZCR 5.12: Identify additional cyber security countermeasures	27
4.6.14 ZCR 5.13: Document and communicate results	28

4.7	ZCR 6: Document cyber security requirements, assumptions and constraints	28
4.7.1	Overview	28
4.7.2	ZCR 6.1: Cyber security requirements specification	28
4.7.3	ZCR 6.2: SUC description	29
4.7.4	ZCR 6.3: Zone and conduit drawings	29
4.7.5	ZCR 6.4: Zone and conduit characteristics	29
4.7.6	ZCR 6.5: Operating environment assumptions	31
4.7.7	ZCR 6.6: Threat environment	31
4.7.8	ZCR 6.7: Organizational security policies	31
4.7.9	ZCR 6.8: Tolerable risk	31
4.7.10	ZCR 6.9: Regulatory requirements	32
4.8	ZCR 7: Asset owner approval	32
4.8.1	Overview	32
4.8.2	ZCR 7.1: Attain asset owner approval	32
	Annex A (informative) Security levels	33
	Annex B (informative) Risk matrices	35
	BIBLIOGRAPHY	38
	Figure 1 – Parts of the ISA-62443 series	11
	Figure 2 – Workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk	18
	Figure 3 – Detailed cyber security risk assessment workflow per zone or conduit	23
	Table B.1 – Example of a 3 x 5 risk matrix	35
	Table B.2 – Example of likelihood scale	35
	Table B.3 – Example of consequence or severity scale	36
	Table B.4 – Example of a simple 3 x 3 risk matrix	36
	Table B.5 – Example of a 5 x 5 risk matrix	37
	Table B.6 – Example of a 3 x 4 matrix	37