## **Contents**

Forewo	ord		•	•	•	•	٠	•		•	•		•	V
Acknov	vled	gement	s .	•				•				•	•	vi
Introdu	ıctioi	n	• ~	•										xiii
СН	APTE	R 1 A	GUII									ΓΑΤ	ION	
		OF C	MITIC	AL '	COIV	IPU 1	CN	31	311	EIVIS	•			
Part 1	Abo	out this	Guide	eline										
	1.1	Scope .												4
		Intende												4
	1.3	Main To	pics	•				•			•			4
		Tailorin												4
		Relation												5
	1.6		ces.	•		٠			•				٠	6
	1.7													6
	1.8	Structur	e and	Conte	ent of	the	Guid	lelin	e	•	•	•	٠	7
Part 2	Dog	cumenta	ation	Guid	lelino	е								
	Top	ic 1: Ma	anagen	nent I	Docu	nent	atior	1						9
	1.1	Docume	entatio	n stru	icture									10
	1.2	Docume	entatio	n star	ndard	S								10
	1.3	2000												11
	Topic 2: System Requirements Specification (SRS)												13	
		ic 3: Sy:												13
	3.1	The syst	tem .											14
	3.2	Hardwa	re .						•					19
	3.3	Softwar	е.											23
	3.4	System	operat	ion a	nd use	er ası	nects	:	_		_	_		32

viii Contents

	rop	ic 4. Teenine	ai gappoi	DUC	unich	latio	**		•	•	•	33
	4.1	Verification,	validatior	and t	est pl	ans						36
	4.2	Record of ver	rification	activiti	ies ¯							36
	4.3	Project development	opment re	eport							_	44
	Top	ic 5: Project i	Managem	ent D	ocum	enta	tion					45
	5 1	End-product	specificat	ion				•	•	•	•	46
	5.2	Technical and	roach do	cumet	1f	•	•	•	•	•	•	46
	5.2	Verification, Record of ver Project develor ic 5: Project End-product Technical app	rintions	cumei	11	•	•	•	•	•	•	47
	5.3	Dicks and fall	haak doo	umant	•	•	•	•	•	•	•	47
	J.4	Nisks and fan	dia	umem ( +	S 1.	•	•	•	•	•	•	47
	3.3	Activity describes and fall Dependency Bar charts Budgets	uiagrams,	netwo	PΓK	•	•	٠	•	•	•	48
	5.6	Bar charts .		•	•			•	•	•	•	48
	5.7	Budgets .		•				٠				49
	5.8	Project mana	gement a	nd qua	ality p	olans	(PM	IQP)				49
	Top	Bar charts Budgets Project mana ic 6: Mainten Introduction Maintenance Maintenance Maintenance Maintenance Maintenance ic 7: Operation System overv Operator into Tasks and pro	ance Do	cumen	tatior	1						54
	6.1	Introduction										54
	6.2	Maintenance	organisat	ion								55
	6.3	Maintenance	procedur	es .								57
	6.4	Maintenance	provision	is.		•	•	•	•	•	•	60
_	6.5	Maintenance	equipme	nt	•	•	•	•	•	•	•	60
	Ton	ic 7: Operati	onal Doc	umant	ation	•	•	•	•	•	•	61
	7 1	Custom susmi	ian Doc	umem	auon	•	•	•	•	•	•	
	7.1	System overv	iew .	•	•	•	•	•	•	•	•	61
	7.2	Operator inte	erraces .	•	•	٠	•	•	•	٠	•	61
	7.3	Tasks and pro Operator resp	ocedures	٠.		٠.	•	•	•	•	•	62
	7.4	Operator resp	ponsibilit	es and	dema	ands	•					63
	Top	ic 8: Additio	nal Equip	ment	and S	oftw	are l	Docu	ımen	tatio	n	63
	8.1	Introduction Management Development Verification a										64
	8.2	Management	tools .									64
	8.3	Development	docume	ntatior	ı tool	S						65
	8.4	Verification a	nd valida	tion to	ools	_						65
	8.5	Operation to	ols		- 010	•	•	•	•	•	•	66
	8.6	Operation to Interfaces with	th other s	vstem	and	evte	rnal	cone	train	te.	•	67
	0.0	Additional de	ni Ullici s	tion	and	CAIC	ınaı	COIIS	ti aiii	ıs	•	68
	0.7	Additional do	Jeumenta	HOII	•	•	•	•	•	•	•	OC
СН		ER 2 A GU System re									OF	
art 1	Ab	out this Guid	deline									
	1.1	Scope Intended Aud Main Topics Tailoring . Terms and D Existing Req		•	•	٠	•			•	•	72
	1.2	Intended Au	dience .		•	•	•	•		•		72
	1.3	Main Topics										72
	1.4	Tailoring .			•							72
	1.5	Terms and D	efinitions									73
	1.6	Existing Rea	uirement	s Speci	ificati	on P	racti	ce				74
	17	Structure of	an SRS	-1				-	-		-	75
	1 Q	Structure of a Relationship	of this D	ocuma	nt to	Oth	22 Ct	anda	rde	٠	٠	75
		Deferences	or uns D	ocume	111 10	Otti	JI 31	anua	102	•	•	7:
	1.9	References.		•	•						•	/:

Contents ix

Part 2	Abo	out System Requirements Specifications	s (SR	Ss)										
	2.1	Importance of SRSs				76								
	2.2	Purpose				77								
	2.3	Form	-	•		77								
	2.4	Areas Subject to Customer Requirements	•		•	77								
	2.5	Stability	•	•	•	77								
	2.6	Quality What is a Good SPS	•	•	•	78								
	2.7	Standard SDS Outline	•	•										
	2.8		•	•	•	81								
	2.8	Life-Cycle of an SKS	•	•	•	81								
Part 3	The Form of a System Requirements Specification													
	3.0	Title				82								
	3.1	Contents												
	3.2	Introduction	•	•	•	84								
	3 3	About this Document	•	•	•	84								
	3.4	Introduction About this Document Definitions of Terms Used in this Document Target System in Context Target System Requirements Target System Environment Requirements Development Project Requirements Development Project Environment Requirement Acceptance Test Plans and Criteria References	•	•	•	87								
	3.5	Target System in Context	•	•	•	87								
	3.5	Target System Dequirements	•	•	•	0/								
	2.7	Target System Environment Descriptions	•	•	•	88								
	2.7	Development Project Benefit Requirements.	•	•	•	101								
	3.8	Development Project Requirements	•	•	•	105								
	3.9	Development Project Environment Requireme	nts	•		108								
	3.10	Acceptance Test Plans and Criteria	•	•		109								
	3.11	References				110								
	3.12	Appendices	•	•	•	111								
CH	APTE	R 3 A GUIDELINE FOR THE DEVELO CRITICAL SOFTWARE	PME	NT	O	F								
Part 1		out this Guideline												
	1.1	Scope				114								
	1.2	Intended Audience				114								
	1.3	Main Topics				115								
	1.4	Tailoring	•	•	•	115								
	1.5	Structure of the Guideline	•	•	•	115								
	1.5	offacture of the Guideline	•	•	•	115								
Part 2	About the Development of Critical Software													
	2.1					116								
	2.2	Approach to Software Design				117								
	2.3	The Development Process				118								
	2.4	Appropriate Programming Language and Com	niler	•	•	118								
	2.5	The Development Process				119								
<b>5</b> .														
Part 3		ailed Guideline for the Design and Cons critical Software	truct	ion										
						101								
		Design and Construction Procedures												
	3.Z	Structuring of Software				128								

x Contents

	3.3	Program Detailed Language	Self Che	cks									138
	3.4	Detailed	Design a	and Co	oding								142
	3.5	Language	e-Depen	dent C	onsid	erati	ons						149
Part 4	Lan	guage, 1	ransla	tor ar	nd Lii	nkag	je E	dito	r				
-	4.1	General Error Ha Data and					,						153
	42	Error Ha	ndling										154
	43	Data and	Variabl	e Han	dling		•	•	•	•	•		154
	4.4	Timing A	snects	o man	GIII.5	•	•	•	•	•	·		
	7.7	Tilling 2	ispects.	•	•	•	•	•	•	•	•	•	10 ,
,	· LI A D	TER 4	A GUI	DEI II	NE E	ΛP	THE	: n	EC1/	281	V VID		
		JCTION											
r	ODC	CHON	COM							NEL	AIL	U	
			COIVI	OIL			_1710	•					
Part 1	Δha	ut this (	Suidali	na									
I al Ci	1.1	Introduct					_						157
		Caras	non .	•	•	•	•	•	•	•	•	•	158
	1.2	Scope . Intended Main Top	, , , , , , , , , , , , , , , , , , ,	•	•	•	•	•	•	•	٠	•	
	1.3	Intended	Audien	ce .	•	•	•	٠	•	•	٠	٠	158
	1.4	Main To	pics .	•	•	•	•	•	•	•	•		158
	1.5	Existing Relations	Practice	•	•	•	•	• .	•	•	•	•	159
	1.6	Relations	ship of t	nis Do	cume	nt to	othe	er St	anda	rds			159
	1.7	Reference	es										159
	1.8	Reference List of A	bbreviat	ions		•							160
	0.7												
Part 2		e Hardw											
	2.1	Aim . Methods Types of		•		•	•		•		•		161
	2.2	Methods											162
	2.3	Types of	Failures										164
	2.4	Possibilit	ies for F	ail-Sat	fe Sys	tems	, Inc	ludii	ng C	ompi	uters		166
	2.5	A Qualit	ative Sa	fety In	vestig	ation	n on	the 1	nflu	ence	of an	ıd	
		Protectiv	e Measu	res ag	ainst ]	Failu	res						173
	2.6	A Quant	itative S	afety l	nvest	igatio	on oi	n the	Infl	nenc	e of		
	2.0	Failure-I											
													182
	2.7	Complete Special P	eness .	for E	nilura	Dota	natio		•	•	•	•	214
		Special F	Tograms	o Cho	allule	Dec	cuo	11	•	•	•	•	222
	2.8	Verificat	ion of th	e Che	CKING	Prog	rams	S .				•	222
	2.9	Compara	itive Dis	cussio	n oi ti	ne va	anou	is Sy	stem	is iro	m a		
		Fail-Safe New Dev	Point o	View	•	•	٠	•	•	•	•	٠	228
	2.10	New Dev	velopme	nts .	•	•	•	•	•	•	•	٠	231
CHA		R 5 A										/NI	)
	VAL	DATION	I OF C	RITIC	AL C	:OM	PU'	TER	SY	STE	MS		
Part 1	۸h	out this (	Guidali	na									
raili													222
	1.1	Scope .			•	•	•	•	•	•	•	٠	233
	1.2	Intended	Augien	ce .									234

Contents xi

	1.3	Assumptions		234
	1.4	The Verification and Validation Process .		235
	1.5	The Verification and Validation Plan		236
Part 2	The	Verification and Validation Activities		
raitz	2.1			237
	2.2	Design Verification	•	237
	2.3	Code Verification	•	
		Code Verification	•	242
	2.4	Code Verification Report	•	245
	2.5	Hardware/Software Integration Verification	•	245
	2.6	Integration Verification Report Computer System Validation	•	247
	2.7	Computer System Validation		247
	2.8	System Validation Report		248
	2.9	Post-Certification Software—Change Verification	n and	i
		Validation		249
	2.10	Related Standards and Guidelines		249
CHA	PTE	R 6 TECHNIQUES FOR THE VERIFICA	TION	J AND
CHA	<b>\</b> FIL	VALIDATION OF CRITICAL SOFTWAR		AND
		VALIDATION OF CHITICAL SOFTWARE	_	
Part 1	Abo	out this Guideline		
	1 1	Score		252
	1.2	Intended Audience	•	252
	1.2	Classification	•	253
	1.3	Scope	•	253
	1.4	Tormat of the Survey	•	255
Part 2	A S	urvey of Software Verification and Valid	atior	1
	Tec	hniques		
	2.1	Method Class 1: Analysis Techniques		254
	2.2	Method Class 2: Testing Techniques		
	2.3		Ī	267
	2.4			271
	2.5	Method Class 4: Tests of Databases		277
	2.5	References	•	211
Glossa	iry .			279
Appen	dix 1		the	
		Production of these Guidelines	•	283
Annon	div 1	Companies of the EWICS TC3 March		205
Appen	UIX Z	Companies of the EWICS TC7 Member	5	285
Index				287