

Table des matières

Introduction	11
Chapitre 1. Système, équipement et logiciel	15
1.1. Introduction.	15
1.2. Impact sur la sûreté de fonctionnement	15
1.3. Système de contrôle et de commande	17
1.4. Système	22
1.5. Processus de réalisation.	25
1.6. Sécurité : du système au logiciel	27
1.7. Application logicielle	30
1.7.1. Qu'est-ce que le logiciel ?	30
1.7.2. Générique, spécifique ou dédiée	31
1.7.3. Différents types de logiciels.	31
1.7.4. Différents types d'utilisation	32
1.8. Conclusion	32
1.9. Glossaire	33
1.10. Bibliographie	34
Chapitre 2. Application logicielle	35
2.1. Introduction.	35
2.2. Application logicielle <i>versus</i> logiciel.	35
2.3. L'application logicielle dans son contexte.	38
2.3.1. Cadre général	38
2.3.2. Réutilisabilité, maintenabilité et continuité de service	39
2.3.3. Architecture modulaire.	41

2.4. Logiciel générique et logiciel paramétré	42
2.5. Module et composant	46
2.6. Composant réutilisé et COTS	51
2.7. Ligne de produit	52
2.8. Conclusion	54
2.9. Glossaire	54
2.10. Bibliographie	55

Chapitre 3. Principe de la sûreté de fonctionnement 57

3.1. Introduction	57
3.2. Sûreté de fonctionnement	58
3.2.1. Concepts de base	58
3.2.2. Entrave à la sûreté de fonctionnement	59
3.2.3. Moyen	64
3.2.4. Exemple d'entrave	65
3.2.5. Classification des fautes	67
3.2.6. Adaptation aux applications logicielles	68
3.3. Description des erreurs du logiciel	73
3.4. Mise en sécurité d'une application logicielle	73
3.4.1. L'évitement des fautes	74
3.4.2. L'élimination des fautes	75
3.4.3. La tolérance aux fautes	75
3.4.4. La prévision des fautes	76
3.4.5. Bilan	77
3.5. Conclusion	77
3.6. Glossaire	78
3.7. Bibliographie	78

Chapitre 4. Maîtrise de la sécurité d'une application logicielle . . . 81

4.1. Introduction	81
4.2. Approche générale	83
4.3. Danger, événement redouté, accident, risque	84
4.3.1. Définitions	84
4.4. Sécurité du système	90
4.4.1. Définition	90
4.4.2. Maîtrise de la sécurité	93
4.4.3. Intégrité de la sécurité	99

4.4.4. Gestion des SIL	102
4.4.5. Niveau d'intégrité de la sécurité	103
4.4.6. Cycle global de la sécurité.	107
4.5. Plan d'assurance sécurité.	113
4.6. Dossier de sécurité.	113
4.6.1. Structure du dossier de sécurité.	113
4.6.2. Contraintes exportées.	114
4.6.3. Produit	115
4.7. Fiabilité, disponibilité et maintenabilité	116
4.7.1. Besoin.	116
4.7.2. De la problématique particulière de l'utilisation de composants sur étagère.	117
4.7.3. Plan de FDM.	118
4.8. Système critique	118
4.9. Conclusion	119
4.10. Annexe : plan d'assurance sécurité	119
4.11. Glossaire.	120
4.12. Bibliographie	121
Chapitre 5. Sécurité d'une application logicielle.	125
5.1. Introduction.	125
5.2. Approche générale.	127
5.2.1. Fiabilité du logiciel	127
5.2.2. Disponibilité	129
5.2.3. Maintenance	130
5.2.4. Sécurité	130
5.2.5. Impact du logiciel.	132
5.3. Niveau de sécurité.	133
5.4. Activité de démonstration de la sécurité d'une application logicielle	134
5.4.1. Analyse de sécurité	134
5.4.2. Analyse du code.	140
5.4.3. Respect des exigences de sécurité	142
5.4.4. Analyse des anomalies.	143
5.5. Conclusion	143
5.6. Plan type d'un PASL	144
5.7. Glossaire	145
5.8. Bibliographie.	146

Chapitre 6. Technique de sécurisation d'une application logicielle	149
6.1. Introduction	149
6.2. Techniques de sécurisation d'une application logicielle	150
6.2.1. Introduction	150
6.2.2. La gestion des erreurs	150
6.2.3. Le recouvrement d'erreurs.	153
6.2.4. La programmation défensive	159
6.2.5. La double exécution de l'application logicielle	167
6.2.6. La redondance des données	175
6.3. D'autres diversités.	178
6.3.1. La diversité temporelle.	179
6.3.2. La diversité d'allocation en mémoire	179
6.4. Conclusion	179
6.5. Glossaire	180
6.6. Bibliographie.	181
Chapitre 7. Evaluation et certification.	183
7.1. Introduction.	183
7.2. Produit.	184
7.3. Evaluation.	184
7.4. Certification	188
7.4.1. Certification de produit	188
7.4.2. Evaluation et certification de logiciel	190
7.4.3. <i>Cross-acceptance</i>	192
7.4.4. Maîtrise des évolutions.	192
7.4.5. Essais	193
7.5. Conclusion	195
7.6. Glossaire	195
7.7. Bibliographie.	196
Chapitre 8. Plusieurs domaines et différents référentiels normatifs	199
8.1. Introduction.	199
8.2. Présentation des standards par domaine	199
8.2.1. Système E/E/EP	199
8.2.2. Domaine ferroviaire	204
8.2.3. Aéronautique.	212

8.2.4. Spatial	215
8.2.5. Nucléaire	216
8.2.6. Automobile.	216
8.3. Quelques contraintes	220
8.4. Niveau de sécurité	220
8.5. Conclusion	221
8.6. Glossaire	221
8.7. Bibliographie	222
Chapitre 9. Maîtrise de la qualité	227
9.1. Introduction	227
9.2. Amélioration continue	228
9.3. Management, mais aussi contrôle de la qualité	229
9.4. Maîtrise de la qualité	229
9.4.1. Introduction	229
9.4.2. ISO 9000	230
9.4.3. ISO 9001	230
9.4.4. Autres	233
9.4.5. Manuel d'assurance qualité, MAQ	237
9.4.6. Qualité projet	238
9.5. Qu'est-ce que la qualité d'une application logicielle ?	239
9.6. Réalisation d'une application logicielle	240
9.7. Qualité logiciel	241
9.7.1. Caractéristiques d'une application logicielle	241
9.7.2. Objectif qualité	242
9.8. Mesure de la complexité d'une application logicielle	246
9.9. Cycle de réalisation	246
9.9.1. Introduction	246
9.9.2. Différents cycles de vie	247
9.9.3. Cycle en V	249
9.9.4. Vérification et validation	251
9.10. Vocabulaire et mode d'expression	252
9.11. Organisation	252
9.11.1. Introduction.	252
9.11.2. Organisation type	253
9.11.3. Gestion des compétences.	255
9.12. Maîtrise de la gestion de la configuration	258
9.13. Management de l'assurance sécurité	259
9.14. Plan d'assurance qualité du logiciel (PAQL)	261
9.15. Gestion des anomalies.	263

9.16. Maintenance d'une application logicielle	266
9.17. Conclusion	266
9.18. Annexe : structure d'un plan d'assurance qualité logiciel	267
9.19. Glossaire.	268
9.20. Bibliographie	269
Chapitre 10. Management des exigences	271
10.1. Introduction	271
10.2. Phase d'acquisition des exigences.	272
10.2.1. Introduction.	272
10.2.2. Elucidation des exigences	273
10.2.3. Processus d'analyse et de documentation	280
10.2.4. Vérification et validation des exigences	287
10.3. Spécification des exigences	290
10.3.1. Caractérisation des exigences	290
10.3.2. Caractérisation de la spécification des exigences	295
10.3.3. Expression des exigences	295
10.3.4. Validation des exigences	300
10.4. Réalisation des exigences.	300
10.4.1. Processus	300
10.4.2. Vérification.	301
10.4.3. Traçabilité	302
10.4.4. Gestion des changements.	306
10.5. Gestion des exigences	309
10.5.1. Activités.	309
10.5.2. Deux approches	310
10.5.3. Mise en place d'outils.	311
10.6. Conclusion	313
10.7. Glossaire.	313
10.8. Bibliographie	314
Conclusion.	317
Index	319