Table des matières

Introduction 11

Chapitre 1. Maîtrise de la sécurité 13

1.1. Introduction 13
1.2. Sûreté de fonctionnement 13
1.2.1. Introduction 13
1.2.2. Entrave à la sûreté de fonctionnement 15
1.2.3. Exemple d'entrave 18
1.2.4. Etudes de démonstration de la sécurité 20
1.2.5. Bilan 23
1.3. Conclusion 23
1.4. Glossaire 23
1.5. Bibliographie 24

Chapitre 2. Système, sous-système, équipement et logiciel 25

2.1. Introduction 25
2.2. Système de contrôle et de commande 26
2.3. Système 29
2.4. Application logicielle 32
2.4.1. Qu'est-ce que le logiciel ? 32
2.4.2. Différents types de logiciel 32
2.4.3. L'application logicielle dans son contexte 33
2.5. Conclusion 34
2.6. Glossaire 34
2.7. Bibliographie 35

Chapitre 3. Système et certification 37

3.1. Introduction. 37
3.2. Contexte normatif 37
3.2.1. Normes génériques 38
3.2.1.1. Présentation 38
3.2.1.2. Niveaux de sécurité 39
3.2.1.3. Normes filles 40
3.2.2. Aspect ferroviaire. 40
3.2.2.1. Historique entre CENELEC et IEC 41
3.2.2.2. Le référentiel CENELEC 41
3.2.2.3. Présentation 41
3.2.2.4. Mise en œuvre 45
3.2.2.5. Sécurité *versus* disponibilité 46
3.2.2.6. Futur 47
3.2.2.7. Sécurité du logiciel. 47
3.2.3. Automobile. 50
3.2.4. Aéronautique. 52
3.2.4.1. Présentation 52
3.2.4.2. Niveau de sécurité du logiciel 55
3.2.5. Spatial. 55
3.3. Conclusion 56
3.4. Glossaire 56
3.5. Bibliographie. 57

Chapitre 4. Gestion du risque. 61

4.1. Introduction. 61
4.2. Définitions de base 61
4.3. Mise en sécurité 68
4.3.1. Qu'est-ce que la sécurité ?. 68
4.3.2. Maîtrise de la sécurité 70
4.3.3. Intégrité de la sécurité 77
4.3.4. Détermination du SIL 80
4.3.5. Table de SIL 85
4.3.6. Allocation des SIL 86
4.3.7. Gestion des SIL 86
4.3.8. Software SIL. 88
4.3.9. Processus itératif 89
4.3.10. Identification des exigences de sécurité 90
4.4. CEI/IEC 61508 et CEI/IEC 61511 92

4.4.1. Graphe de risque 92
4.4.2. LOPA 94
4.4.3. Bilan. 95
4.5. Conclusion 95
4.6. Glossaire 96
4.7. Bibliographie 97

Chapitre 5. Principe de sécurisation du matériel 101

5.1. Introduction. 101
5.2. Architecture sûre et/ou disponible 101
5.3. Réinitialisation d'une unité de traitement 102
5.4. Présentation des techniques de sécurisation 102
5.4.1. Détection d'erreurs 103
5.4.1.1. Concepts 103
5.4.1.2. Chien de garde 104
5.4.1.3. Autotests 105
5.4.1.4. Contrôles de cohérence 107
5.4.1.5. Bilan 109
5.4.2. Diversité 109
5.4.3. Redondance 110
5.4.3.1. Redondance d'exécution 111
5.4.3.2. Redondance informationnelle 114
5.4.3.3. Redondance du matériel 120
5.4.4. Reprise ou recouvrement d'erreur 135
5.4.4.1. Reprise 135
5.4.4.2. Poursuite 136
5.4.4.3. Bilan 136
5.4.5. Partitionnement 136
5.5. Conclusion 137
5.6. Bibliographie 138

Chapitre 6. Principe de sécurisation d'un logiciel 139

6.1. Introduction. 139
6.2. Techniques de sécurisation d'une application logicielle 139
6.2.1. La gestion des erreurs 140
6.2.1.1. Principes 140
6.2.1.2. Bilan 142
6.2.2. Le recouvrement d'erreur 142
6.2.2.1. Le recouvrement d'erreur par reprise 143

6.2.2.2. Le recouvrement d'erreur par poursuite 147
6.2.2.3. Bilan 148
6.2.3. La programmation défensive 148
6.2.3.1. Présentation 148
6.2.3.2. Principes 149
6.2.3.3. Bilan 155
6.2.4. La double exécution de l'application logicielle 155
6.2.4.1. Principes 155
6.2.4.2. Exemple 1 159
6.2.4.3. Exemple 2 160
6.2.4.4. Exemple 3 161
6.2.4.5. Exemple 4 163
6.2.4.6. Bilan 163
6.2.5. La redondance des données 163
6.2.5.1. Présentation 163
6.2.5.2. Généralisation 165
6.2.5.3. Bilan 167
6.3. D'autres diversités 167
6.3.1. La diversité temporelle 167
6.3.2. La diversité d'allocation en mémoire 168
6.4. Bilan général 168
6.5. Maîtrise de la qualité 169
6.5.1. Introduction 169
6.5.2. Réalisation d'une application logicielle 169
6.5.3. Cycle de réalisation 170
6.5.3.1. Cycle en V et autre cycle de réalisation 170
6.5.3.2. Vérification et validation 173
6.5.3.3. Bilan 174
6.6. Conclusion 174
6.7. Bibliographie 174

Chapitre 7. Certification 177

7.1. Introduction 177
7.2. Evaluation indépendante 177
7.3. Certification 178
7.4. Certification dans le ferroviaire 179
7.4.1. Obligations 179
7.4.2. Besoins 179
7.4.3. Mise en place d'une certification 180
7.4.4. Mise en œuvre 181

7.4.5. Maîtrise des évolutions 182
7.4.6. *Cross-acceptance* 186
7.4.7. Essais 187
7.5. Système à base d'automatismes 188
7.6. Aéronautique 188
7.7. Nucléaire 189
7.8. Automobile 189
7.9. Spatial 190
7.10. Dossier de sécurité 190
7.11. Conclusion 191
7.12. Glossaire 191
7.13. Bibliographie 192

Conclusion 195

Index 197