
Table des matières

Chapitre 1. Introduction	13
1.1. Objectif	13
1.2. Rappel	15
1.3. Synthèse	16
1.4. Bibliographie	17
Chapitre 2. Du système au logiciel	19
2.1. Introduction	19
2.2. Système de contrôle et de commande	20
2.3. Système	24
2.4. Application logicielle	25
2.4.1. Qu'est-ce que le logiciel ?	25
2.4.2. Différents types de logiciels	28
2.4.3. L'application logicielle dans son contexte	28
2.5. Conclusion	29
2.6. Bibliographie	29
Chapitre 3. Normes ferroviaires	31
3.1. Introduction	31
3.2. Normes génériques	32
3.2.1. Présentation	32
3.2.2. Niveaux de sécurité	33
3.3. Historique entre CENELEC et IEC	34
3.4. Référentiel CENELEC	35
3.4.1. Présentation	35

3.4.2. Description	36
3.4.3. Mise en œuvre	39
3.4.4. Sécurité du logiciel	40
3.4.5. Sécurité <i>versus</i> disponibilité	40
3.5. Norme EN 50155	41
3.6. CENELEC 50128	43
3.6.1. Introduction	43
3.6.2. Gestion du SSIL	44
3.6.3. Comparaison des versions 2001 et 2011	46
3.7. Conclusion	47
3.8. Bibliographie	48

Chapitre 4. Risque et niveau de sécurité 51

4.1. Introduction	51
4.2. Définitions de base	51
4.3. Mise en sécurité	58
4.3.1. Qu'est-ce que la sécurité ?	58
4.3.2. Maîtrise de la sécurité	60
4.3.3. Intégrité de la sécurité	67
4.3.4. Détermination du SIL	70
4.3.5. Table de SIL	74
4.3.6. Allocation des SIL	75
4.3.7. Gestion des SIL	76
4.3.8. Software SIL	77
4.3.9. Processus itératif	78
4.3.10. Identification des exigences de sécurité	79
4.4. Dans les normes CEI/IEC 61508 et CEI/IEC 61511	80
4.4.1. Graphe de risque	82
4.4.2. LOPA	84
4.4.3. Bilan	85
4.5. Conclusion	85
4.6. Bibliographie	85

Chapitre 5. Assurance du logiciel 89

5.1. Introduction	89
5.2. Prérequis	89
5.3. Assurance qualité	89
5.3.1. Introduction	89
5.3.2. Management de l'assurance qualité	90

5.3.3. Réalisation d'une application logicielle	94
5.3.4. Plan d'assurance qualité du logiciel (PAQL).	96
5.4. Organisation	99
5.4.1. Organisation type	99
5.4.2. Gestion des compétences	101
5.5. Maîtrise de la gestion de la configuration	103
5.6. Management de l'assurance sécurité	104
5.7. Vérification et validation	106
5.7.1. Introduction	106
5.7.2. Vérification	108
5.7.3. Validation	122
5.8. Evaluation indépendante	123
5.9. Qualification des outils	124
5.10. Conclusion	124
5.11. Annexe A : liste des documents qualité à produire	125
5.12. Annexe B : structure d'un plan d'assurance qualité logiciel	125
5.13. Bibliographie	126
Chapitre 6. Management des exigences	129
6.1. Introduction.	129
6.2. Phase d'acquisition des exigences	130
6.2.1. Introduction	130
6.2.2. Elucidation des exigences	131
6.2.3. Processus d'analyse et de documentation.	138
6.2.4. Vérification et validation des exigences.	145
6.3. Spécification des exigences	147
6.3.1. Caractérisation des exigences	147
6.3.2. Caractérisation de la spécification des exigences	153
6.3.3. Expression des exigences	153
6.3.4. Validation des exigences.	157
6.4. Réalisation des exigences	158
6.4.1. Processus	158
6.4.2. Vérification	158
6.4.3. Traçabilité	160
6.4.4. Gestion des changements	163
6.5. Gestion des exigences.	166
6.5.1. Activités	166
6.5.2. Deux approches	168
6.5.3. Mise en place d'outils	168

6.6. Conclusion	170
6.7. Bibliographie	170
Chapitre 7. Préparation des données	173
7.1. Introduction	173
7.2. Rappel	174
7.3. Problématique	174
7.4. Système paramétré par les données	176
7.4.1. Introduction	176
7.4.2. Caractérisation des données	178
7.4.3. Inhibition de service	179
7.4.4. Synthèse	181
7.5. Du système au logiciel	182
7.5.1. Besoin	182
7.5.2. Ce que ne dit pas le référentiel CENELEC	184
7.6. Processus de préparation des données	186
7.6.1. Contexte	186
7.6.2. Présentation de la section 8 de la norme 50128:2011	187
7.7. Processus de préparation des données	191
7.7.1. Maîtrise du processus de préparation des données	191
7.7.2. Vérification	198
7.7.3. Phase de spécification	198
7.7.4. Phase d'architecture	203
7.7.5. Production des données	206
7.7.6. Intégration de l'application et acceptation des tests	211
7.7.7. Validation et évaluation de l'application	212
7.7.8. Procédure et outils de préparation de l'application	213
7.7.9. Développement du logiciel générique	213
7.8. Conclusion	214
7.9. Annexe A : documentation à produire	214
7.10. Bibliographie	215
Chapitre 8. Application générique	217
8.1. Introduction	217
8.2. Processus de réalisation d'une application logicielle	217
8.3. Réalisation d'une application générique	219
8.3.1. Phase de spécification	219
8.3.2. Phase d'architecture et de conception des composants	226

8.3.3. Phase de conception du composant	247
8.3.4. Phase de codage	252
8.3.5. Réalisation des tests de composant.	254
8.3.6. Phase d'intégration du logiciel	256
8.3.7. Phase de tests d'ensemble du logiciel	257
8.4. Petit retour d'expérience	259
8.5. Conclusion	260
8.6. Annexe A : langage Ada	260
8.7. Annexe B : langage C.	262
8.7.1. Introduction	262
8.7.2. Difficulté du C.	262
8.7.3. MISRA-C	263
8.7.4. Exemple de règle	264
8.8. Annexe C : langage orienté objet, présentation.	264
8.9. Annexe D : documentation à produire	267
8.10. Bibliographie	268
Chapitre 9. Modélisation et formalisation	271
9.1. Introduction.	271
9.2. Modélisation	271
9.2.1. Objectifs	271
9.2.2. Différents types de modélisation	273
9.2.3. Modèle	274
9.3. Prise en compte des techniques et méthodes formelles	275
9.3.1. Définitions	275
9.3.2. UML	278
9.4. Petite introduction aux méthodes formelles	278
9.4.1. Rappel	278
9.4.2. Utilisation dans le ferroviaire	280
9.4.3. Synthèse	285
9.5. Mise en œuvre des méthodes formelles	288
9.5.1. Processus classiques	288
9.5.2. Processus prenant en compte les méthodes formelles.	289
9.5.3. Problématique	291
9.6. Maintenance de l'application logicielle	293
9.7. Conclusion	293
9.8. Bibliographie	295

Chapitre 10. Qualification des outils	299
10.1. Introduction	299
10.2. Concept de qualification	299
10.2.1. Problématique	299
10.2.2. CENELEC 50128:2001	300
10.2.3. DO 178	302
10.2.4. IEC 61508	304
10.2.5. ISO 26262	304
10.3. CENELEC 50128:2011	305
10.3.1. Introduction.	305
10.3.2. Dossier de qualification	305
10.3.3. Processus de qualification	306
10.3.4. Mise en œuvre du processus de qualification	308
10.4. Adéquation au besoin	316
10.4.1. Méthode de conception	316
10.4.2. En cas d'incompatibilité	316
10.4.3. La génération de code.	317
10.5. Gestion des versions	317
10.5.1. Identification des versions	317
10.5.2. Analyse des défauts	318
10.5.3. Changement de version.	318
10.6. Processus de qualification	318
10.6.1. Dossier de qualification	318
10.6.2. Au final	319
10.6.3. Qualification des outils non commerciaux	319
10.7. Conclusion	319
10.8. Bibliographie	320
Chapitre 11. Maintenance et déploiement	321
11.1. Introduction	321
11.2. Besoins.	321
11.2.1. Gestion des défauts	321
11.2.2. Maîtrise des évolutions	322
11.3. Déploiement	324
11.3.1. Problématique	324
11.3.2. Mise en œuvre	324
11.3.3. En réalité	326
11.4. Maintenance du logiciel.	326

11.4.1. Problématique	326
11.4.2. Mise en œuvre	327
11.5. Ligne de produits	328
11.6. Conclusion	330
11.7. Annexe : documentation à produire	330
11.8. Bibliographie	330
Chapitre 12. Evaluation et certification	333
12.1. Introduction	333
12.2. Evaluation	333
12.2.1. Principes	333
12.2.2. CENELEC 50128:2011	336
12.3. <i>Cross-acceptance</i>	337
12.4. Certification	338
12.4.1. Certification de produit	338
12.4.2. Certification de logiciel	338
12.4.3. Maîtrise des évolutions	339
12.5. Conclusion	339
12.6. Annexe : documentation à produire	340
12.7. Bibliographie	340
Conclusion	341
Glossaire	343
Index	349