SQUALE : CRITÈRES D'ÉVALUATION DE LA SÛRETÉ DE FONCTIONNEMENT

Yves Deswarte et Mohamed Kaâniche
LAAS-CNRS
7, avenue du Colonel Roche
31077 Toulouse cedex 4

Pierre Corneillie
CR2A-DI
19, avenue Dubonnet
92411 Courbevoie cedex

Paul Benoit
Matra Transport International
48-56 rue Barbès
92542 Montrouge cedex

Résumé
L'objectif de SQUALE est de développer des critères d'évaluation permettant d'obtenir une confiance justifiée qu'un système atteindra bien, pendant sa vie opérationnelle et au cours de son retrait de service, les objectifs de sûreté de fonctionnement qui lui ont été fixés. Par rapport aux méthodes classiques d'évaluation (critères d'évaluation de la sécurité informatique, normes pour la conception, le développement et la validation de systèmes critiques), les critères de SQUALE se distinguent par leur indépendance par rapport aux domaines d'application et aux secteurs industriels, leur prise en compte de l'ensemble des attributs de la sûreté de fonctionnement et leur progressivité en fonction d'exigences plus ou moins sévères. Pour valider l'approche et affiner les critères, une première expérimentation est en cours pour évaluer le système de commande de la ligne de métro automatique METEOR, et une autre expérimentation va être lancée sur un système de Bouygues Telecom.

Introduction

L'utilisation croissante de l'informatique dans tous les secteurs industriels conduit à spécifier et concevoir des systèmes adaptés aux besoins des applications visées, qu'il s'agisse d'exigences fonctionnelles (précision des résultats, temps de réponse, facilité d'utilisation, etc.) ou d'exigences de sûreté de fonctionnement (disponibilité, confidentialité, maintenabilité, etc.), le tout au moindre coût. Se pose alors la question de savoir si le système ainsi conçu ou choisi satisfait ces exigences. Pour ce qui concerne les aspects fonctionnels, il suffit en général de mener une campagne d'essais en mettant le système dans des conditions aussi proches que possible des limites prévues. Ceci est beaucoup plus difficile pour les aspects de sûreté de fonctionnement, puisqu'il n'est en général pas possible de mettre le système dans toutes les situations de fautes pour lesquelles on a fixé des exigences, qu'il s'agisse de fautes physiques, de fautes de conception, de fautes d'interaction ou de malveillances.

Pour les applications critiques, c'est-à-dire celles pour lesquelles une défaillance du système informatique serait susceptible d'entraîner des catastrophes, on peut obtenir une confiance suffisante dans le fonctionnement du système en imposant des méthodes de développement et de validation adaptées. Dans la plupart des secteurs concernés (ferroviaire, nucléaire, avionique, etc.), il existe des normes préconisant quelles méthodes utiliser et avec quel niveau de rigueur ou de détail. De même, si on s'intéresse à la sécurité vis-à-vis des malveillances, il existe des critères d'évaluation, tels que les ITSEC [1] qui permettent d'estimer la capacité du système à faire face à des menaces éventuelles. Mais ceci ne concerne principalement que deux des aspects de la sûreté de fonctionnement : la sécurité-innocuité (*safety* en anglais) et la sécurité-confidentialité (*security* en anglais) [2].

Or le plus souvent, il est nécessaire de prendre en compte d'autres attributs de la sûreté de fonctionnement comme la disponibilité ou la maintenabilité. Ainsi par exemple, dans les transports ferroviaires ou aériens, la sécurité des passagers est primordiale, mais la disponibilité peut aussi être critique vis-à-vis de la rentabilité du système. Il est donc important d'être capable de vérifier si le système satisfait toutes ses exigences de sûreté de fonctionnement. L'approche présentée ici est développée dans le projet SQUALE[1] (*Security, Safety and Quality Evaluation for Dependable Systems*, projet européen du Programme ACTS (*Advanced Communications, Technologies and Services*). L'objectif du projet est de développer des critères d'évaluation permettant d'obtenir une confiance justifiée qu'un système atteindra bien, pendant sa vie opérationnelle et au cours de son retrait de service, l'ensemble des objectifs de sûreté de fonctionnement qui lui ont été fixés. Ces critères sont génériques dans le sens où ils ne visent pas un secteur d'application donné, mais au contraire doivent être suffisamment souples pour ne pas exiger un travail supplémentaire important pour évaluer et certifier des systèmes conformément aux normes de leur domaine.

La première partie de cet article est consacrée à l'état de l'art en matière d'évaluation de la sécurité-confidentialité et de la sécurité-innocuité. Dans la deuxième partie, les critères de SQUALE sont présentés et leur expérimentation dans le cadre du système METEOR est décrite dans la troisième partie, ainsi que les leçons que nous avons pu en tirer.

1. État de l'art

L'évaluation et la certification des systèmes informatiques présentant des exigences de sûreté de fonctionnement a donné naissance à plusieurs normes et documents normatifs aux niveaux national, européen et international. On peut distinguer deux classes d'approches : celles ciblant la sécurité-confidentialité (regroupant à la fois la confidentialité, l'intégrité et la disponibilité, souvent appelée «sécurité des systèmes d'information») et celles

[1] Les partenaires actuels du projet SQUALE sont CR2A-DI (F), contractant principal, Admiral (Royaume-Uni), IABG (Allemagne), le LAAS-CNRS (F), Matra Transport International (F) et Bouygues Telecom (F),

focalisant sur les autres attributs de la sûreté de fonctionnement, essentiellement la sécurité-innocuité (c'est-à-dire la sécurité vis-à-vis des défaillances catastrophiques). La première classe a donné naissance aux critères d'évaluation TCSEC, ITSEC, etc. qui sont exposés dans la section 1.1. Ces critères ne sont pas spécifiques d'un domaine d'application donné, mais restent néanmoins axés sur les besoins de sécurité des systèmes d'information. En ce qui concerne la deuxième classe, chaque domaine d'application a développé ses propres normes. C'est le cas par exemple des domaines de l'avionique et des transports ferroviaires (section 1.2). Ces différentes normes présentent plusieurs points communs, ce qui montre le besoin de développer une démarche d'évaluation générique. Une telle démarche est considérée dans la norme CEI 1508 (section 1.3).

1.1. Critères d'évaluation de la sécurité-confidentialité

Pour comparer la capacité de divers systèmes informatiques à faire face à des malveillances, on utilise généralement des *critères d'évaluation*.

Les premiers critères ont été définis par le Department of Defense (DoD) des États-Unis dans ce qui est couramment appelé le *Livre Orange* ou TCSEC (*Trusted Computer System Evaluation Criteria*) [3], et dans les livres de diverses couleurs qui l'accompagnent, comme le *Livre Rouge* ou TNI (*Trusted Network Interpretation of the TCSEC*) [4]. Ces critères, basés à la fois sur des listes de fonctions de sécurité à remplir et sur les techniques employées pour la vérification, conduisent à classer les systèmes en 7 catégories (dans un ordre croissant de sécurité : D, C1, C2, B1, B2, B3, A1). Ces critères visaient à satisfaire d'abord les besoins du DoD, c'est-à-dire qu'ils privilégient la confidentialité plutôt que l'intégrité qui est le souci principal des systèmes dits «commerciaux». Depuis, deux agences fédérales américaines, le NIST (*National Institute of Standards and Technology*) et la NSA (*National Security Agency*), ont diffusé l'ébauche d'une nouvelle norme, les *critères fédéraux* [5], susceptible de remplacer le Livre Orange et ses dérivés. Le premier objectif des critères fédéraux est de mieux prendre en compte les divers aspects de la sécurité (confidentialité, intégrité et disponibilité), même si ce qui concerne la disponibilité est moins élaboré que ce qui concerne la confidentialité et l'intégrité : ainsi, la section réservée à la tolérance aux fautes n'est pas rédigée. L'évaluation par les critères fédéraux porte sur des «produits», c'est-à-dire sur des éléments isolés, plutôt que sur des «systèmes», c'est-à-dire des produits dans leur environnement d'exploitation. Contrairement au Livre Orange, les critères fédéraux séparent explicitement les *aspects fonctionnels*, les *aspects liés au développement* et les *aspects d'assurance* (ou vérification), chacun de ces aspects étant évalués avec différents niveaux. Néanmoins, 7 exemples d'*assurance packages* sont donnés en annexe, correspondant à 7 niveaux de sécurité dans un ordre croissant et regroupant des niveaux de fonctionnalité, de méthodes de développement et de vérification «homogènes». De plus, des «profils de protection» de différents niveaux sont proposés pour des classes d'applications typiques telles que les systèmes commerciaux ou les systèmes militaires.

En fait, cette volonté de séparer les exigences concernant les fonctionnalités de celles concernant la vérification était déjà présente dans les critères *harmonisés*[2] européens, ou ITSEC (*Information Technology Evaluation Criteria*) [1]. Dix *classes de fonctionnalités* y sont prédéfinies, dont les cinq premières reprennent les fonctionnalités des catégories C1 à B3 du Livre Orange (dans le Livre Orange, les fonctionnalités A1 sont identiques à celles de B3, et pour la catégorie D, rien n'est exigé puisqu'elle correspond aux systèmes n'ayant pas obtenu le niveau d'évaluation visé). Cinq autres classes de fonctionnalités sont définies pour les systèmes à haute intégrité, à haute disponibilité, à haute intégrité pour les transmissions, à haute confidentialité pour les transmissions et enfin pour les réseaux à hautes intégrité et confidentialité. Mais d'autres combinaisons de fonctionnalités peuvent être définies si le besoin s'en fait sentir pour un système ou une application particuliers. Pour ce qui concerne la vérification, 6 niveaux d'*assurance de conformité* sont définis, notés de E1 à E6, du moins exigeant au plus exigeant. Ces niveaux se distinguent en particulier par le niveau de détail de l'application des techniques de vérification et par le niveau de formalisation du développement. Des critères d'*assurance d'efficacité* sont également définis pour évaluer la pertinence et la cohésion des fonctionnalités, la résistance des mécanismes, la vulnérabilité de la construction ainsi que des critères liés à l'exploitation : facilité d'emploi et vulnérabilité en exploitation. Pour être évalué par les ITSEC, le système doit être décrit par une «cible d'évaluation» (*Target of Evaluation*, ou TOE) qui comprend : une définition de la politique de sécurité, une spécification des fonctions dédiées à la sécurité et des mécanismes de sécurité requis, ainsi que l'identification du niveau d'assurance visé. Un manuel d'évaluation des ITSEC, l'ITSEM (*Information Technology Evaluation Manual*), est paru [6]. Il précise en particulier les rôles des différents partenaires d'une évaluation : le commanditaire (ou sponsor) qui demande l'évaluation, le développeur du système à évaluer, les évaluateurs et l'organisme de certification. Le sponsor peut également être le vendeur ou le développeur du système, ou encore l'utilisateur, mais les évaluateurs doivent être indépendants du sponsor et du développeur.

Plus récemment, un comité (*Common Criteria Editorial Board* ou CCEB) a été constitué pour proposer des «critères communs», qui seraient le résultat de l'harmonisation des critères les plus récents. Participent à ce comité le Canada, la Grande-Bretagne, l'Allemagne, la France et, pour les Etats-Unis, le NIST et la NSA. Une première version de ces critères est parue en janvier 1996 [7]. On y retrouve le principe de la séparation entre les critères de fonctionnalité et ceux d'assurance (ou vérification), mais aussi les notions de cible d'évaluation définie par les ITSEC et de profils de protection présents dans

[2] Ces critères européens sont le résultat de l'harmonisation des ébauches de critères nationaux allemands, britanniques, français et hollandais. Ils sont soutenus par la Commission Européenne.

les critères fédéraux et les critères canadiens.

1.2. Normes de certification par domaines

Avionique civile : La certification des systèmes embarqués dans les avions civils fait l'objet d'une réglementation très contraignante. Vis-à-vis de la sûreté de fonctionnement, l'accent est mis sur la sécurité-innocuité. La démarche générale repose sur un processus d'analyse de la sécurité-innocuité (intégrant des études de risques préliminaires, fonctionnelles et architecturales) qui consiste à analyser les fonctions et l'architecture des systèmes avioniques et à identifier leurs modes de défaillance. Ces derniers sont classés par rapport à une échelle de sévérité (vis-à-vis des conséquences de ces défaillances sur la sécurité des vols et des passagers), définie par les règlements de navigation internationaux, qui comprend cinq niveaux : catastrophique, dangereuse, majeure, mineure, et sans effet. La criticité d'un système est alors déterminée par la plus forte sévérité de ses modes de défaillance. On définit cinq niveaux de criticité notés A, B, C, D, et E par ordre décroissant. Cette classification détermine le niveau d'assurance (ou de certification) que le système doit satisfaire. Pour chacun de ces niveaux, un ensemble de critères et de preuves sont requis. Cette philosophie est appliquée de façon itérative à différents niveaux de description des systèmes. Le document ARP 4754 [8] définit les exigences de certification pour des systèmes avioniques complexes en focalisant sur les phases de définition des exigences de haut niveau jusqu'à l'allocation des exigences aux systèmes matériels et logiciels. La norme DO 178B [9] est consacrée aux logiciels embarqués, et les exigences de certification pour les systèmes matériels embarqués sont en cours de préparation.

La norme DO 178B est basée sur une démarche orientée processus. On distingue trois types de processus dans le cycle de vie du logiciel : le processus de développement qui comprend la spécification, la conception, le codage et l'intégration ; les processus intégraux qui comprennent la vérification, la gestion de configuration, l'assurance qualité ainsi que la coordination pour la certification ; et le processus de planification qui coordonne le processus de développement et les processus intégraux. La norme accepte que plusieurs cycles de vie puissent être envisagés, mais impose que des critères de transition entre les processus du cycle de vie soient clairement établis. Pour chaque processus et chaque niveau d'assurance, les objectifs sont définis et une description des données du cycle de vie permettant de démontrer que les objectifs sont satisfaits est également fournie. Pour certains niveaux d'assurance, certains objectifs relatifs à la vérification et à l'assurance qualité doivent être atteints en respectant des critères d'indépendance vis-à-vis des développeurs ; le niveau de rigueur pour la gestion de configuration peut également varier. La norme n'impose aucune méthode pour atteindre les objectifs fixés. C'est à la charge du postulant à la certification d'apporter les preuves que les méthodes employées permettent de répondre aux objectifs. Notons enfin, que la norme recommande, sans imposer, des stratégies de tolérance aux fautes qui peuvent être employées pour la détection et le confinement des erreurs, par exemple : partitionnement, diversification, programmation défensive… Pour la diversification, des critères d'indépendance dans le développement de versions dissimilaires sont également requis.

Transports ferroviaires : La prise en compte de la sûreté de fonctionnement dans le développement des systèmes ferroviaires européens est couverte par un ensemble de documents de normalisation qui sont en cours de préparation. La norme EN 50126 [10] décrit les procédures à mettre en œuvre durant le cycle de vie d'un système ferroviaire (depuis la définition des concepts jusqu'au retrait définitif du service) et les activités à mener pour assurer d'une part, la disponibilité, la fiabilité et la maintenabilité, et d'autre part, la sécurité-innocuité. Pour chaque phase du cycle de vie, la norme définit les objectifs de la phase, les exigences à satisfaire et les données en entrée et en sortie pour les activités de sûreté de fonctionnement. Des tâches de vérification et de validation sont intégrées à chaque phase pour s'assurer de la satisfaction des objectifs et exigences définis pour le système. Une phase d'acceptation du système avant sa mise en exploitation est explicitement identifiée dans le cycle de vie proposé. La procédure de mise en œuvre et d'évaluation de la sécurité-innocuité repose sur la notion de risque, son évaluation et sa maîtrise. Le niveau de risque tolérable pour un chemin de fer dépend des critères de sécurité fixés par l'Autorité de Tutelle nationale en matière de sécurité, ou en accord avec celle-ci. L'évaluation et la maîtrise des risques en vue de satisfaire ces critères est de la responsabilité de la Société d'Exploitation Ferroviaire. Une échelle de sévérité des modes de défaillance (appelés situations dangereuses) à quatre niveaux (catastrophique, critique, marginal, insignifiant), combinée à une échelle de graduation de la fréquence d'occurrence de ces défaillances à six niveaux (fréquent, probable, occasionnel, rare, improbable, invraisemblable) permet de définir une matrice de classement des risques. Quatre catégories de risque sont définies (inacceptable, indésirable, acceptable, négligeable) et les actions à appliquer pour chaque catégorie sont spécifiées. Par exemple, tout risque inacceptable doit être éliminé. La norme utilise le concept de niveaux d'intégrité pour caractériser le niveau de confiance que l'on cherche à obtenir et à prouver pour les fonctions de sécurité. La définition de ces niveaux est liée à la probabilité d'occurrence d'événements indésirables pouvant affecter ces fonctions. La norme recommande de ne pas utiliser plus de quatre niveaux d'intégrité. Les recommandations pour des architectures, méthodes outils et techniques permettant d'obtenir le niveau de confiance correspondant à un niveau d'intégrité donné, font l'objet d'autres normes spécifiques, par exemple la norme EN 50128 [11] en ce qui concerne les systèmes logiciels et la norme ENV 50129 [12] pour les systèmes matériels.

Dans la norme EN 50128, on distingue quatre niveaux d'intégrité du logiciel pour les fonctions de sécurité, notés de 1 à 4 par ordre croissant ; un niveau 0 est rajouté pour identifier les fonctions non sécuritaires. Vis-à-vis du choix des techniques et méthodes, et des documentations à fournir afin de prouver le niveau d'intégrité visé, la norme donne en annexe une liste avec des recommanda-

tions du type : obligatoire, hautement recommandé, recommandé, non recommandé, interdit, sans avis. La norme ne distingue pas, pour le choix de ces méthodes et techniques, entre les niveaux 1 et 2, ni entre les niveaux 3 et 4. Cependant, la norme n'interdit pas le choix d'autres méthodes moyennant une justification de leur utilisation en fonction du niveau d'intégrité visé. Une philosophie similaire est adoptée dans la norme ENV 50129.

Notons enfin que ces normes exigent une justification du niveau de compétence, de formation, d'expérience et de qualification de toutes les personnes intervenant dans le processus global de développement et d'évaluation des systèmes ferroviaires. De plus, pour chaque niveau d'intégrité, des critères d'indépendance entre les personnes intervenant dans la gestion de projet, la conception et réalisation, la vérification, la validation, et l'évaluation du système sont définis dans les normes EN 50128 et ENV 50129.

1.3. Norme CEI 1508

La norme CEI 1508 [13] propose une approche générique, non spécifique d'un domaine d'application particulier, pour la spécification, la mise en œuvre et l'évaluation de la sécurité-innocuité de systèmes dits E/E/SEP (systèmes Électriques / Électroniques / Électroniques Programmables) qui comportent des systèmes informatiques. La démarche proposée s'articule autour d'un modèle de cycle de vie pour la sécurité-innocuité décrivant les principales activités à mener pour définir les exigences de sécurité, les mettre en œuvre et s'assurer du respect de ces exigences tout au long du cycle de vie du système. La norme ne spécifie pas qui doit avoir la responsabilité de la mise en œuvre de ces activités. Cependant, des exigences relatives à la compétence des personnes intervenant dans ce processus sont requises. Pour chaque phase du modèle de cycle de vie pour la sécurité-innocuité, la norme décrit les objectifs à atteindre, la portée de ces objectifs, les exigences à satisfaire, les données en entrée et les délivrables à fournir à la fin de la phase pour prouver que les exigences sont satisfaites. Chaque phase doit être conclue par une activité de vérification répondant aux exigences préalablement définies dans le plan de vérification. L'intégration des différents sous-systèmes de sécurité doit faire l'objet d'une validation globale permettant de vérifier que le système dans sa globalité satisfait les exigences de sécurité-innocuité. La spécification de ces exigences qui se traduit par la définition des fonctions de sécurité et des niveaux d'intégrité correspondants, est basée sur un processus d'identification, d'analyse et de maîtrise de risques. Quatre niveaux d'intégrité sont définis et des objectifs quantifiés sont associés à chaque niveau en termes de probabilités maximales d'occurrence de modes de défaillance affectant la fonction de sécurité considérée. La norme décrit également la procédure d'évaluation de la sécurité-innocuité qui doit être mise en œuvre pour apprécier dans quelle mesure les fonctions de sécurité-innocuité telles qu'elles sont mises en œuvre dans le système satisfont les objectifs et exigences définis par la norme. Un plan d'évaluation doit être établi au terme de la phase d'analyse préliminaire des risques. L'évaluation doit prendre en compte toutes les phases du cycle de vie général de la sécurité-innocuité. Elle peut être effectuée soit après chaque phase, soit après un certain nombre de phases en s'assurant que les risques identifiés ne peuvent pas se manifester avant qu'une telle évaluation ne soit appliquée. Des critères d'indépendance des évaluateurs vis-à-vis des développeurs (pris au sens large, c'est-à-dire concepteurs, responsables d'activité de vérification ou de validation, etc.) sont spécifiés en fonction de la phase de cycle de vie, de l'activité considérée, et des niveaux d'intégrité visés. Trois niveaux d'indépendance sont distingués : personne indépendante, service indépendant, organisation indépendante. Par exemple, une personne indépendante est une personne distinctement séparée de celles impliquées dans les activités de développement, et qui n'a pas de responsabilité directe dans ces activités. Pour le niveau d'intégrité le plus élévé, la norme exige que l'évaluation soit effectuée par une organisation distincte et séparée, de par sa gestion et ses autres ressources, de celles responsables du développement du système. Notons que des critères d'indépendance similaires sont aussi requis pour les activités de validation du logiciel, mais aucun critère d'indépendance n'est mentionné pour la validation du matériel. La norme admet que le degré de satisfaction des exigences et objectifs prescrits (degré de rigueur) dépend de plusieurs facteurs (niveau d'intégrité, nature des modes de défaillance potentiels, mécanismes de réduction de risque mis en œuvre, etc.). Des tableaux sont présentés dans la norme pour sélectionner les techniques et méthodes recommandées. Si une méthode classée comme hautement recommandée n'est pas utilisée, il faut détailler les raisons pour lesquelles elle a été écartée. Dans certains cas ou plusieurs choix sont proposés, une seule technique ou méthode parmi l'ensemble est requise. Ces recommandations sont faites pour chaque activité du cycle de vie et concernent les types d'architectures, les méthodes de spécification, de conception, de vérification, etc. Pour les systèmes matériels, des objectifs quantitatifs pour la couverture minimale des mécanismes de tolérance aux fautes sont spécifiés.

2. Description des critères SQUALE

Comme la norme CEI 1508 ou les ITSEC, les critères de SQUALE [14] se veulent indépendants du secteur d'application. Mais ils se veulent également génériques par la prise en compte de l'ensemble des attributs de la sûreté de fonctionnement.

2.1. Rôles des différents intervenants dans une évaluation

Dans une évaluation utilisant les critères de SQUALE, il convient de distinguer différents intervenants (cf. figure 1) :

Le commanditaire (ou sponsor) : C'est celui qui demande et finance l'évaluation. Ce peut être le fournisseur d'un système, le client, ou un organisme responsable de la sécurité. C'est lui aussi qui recevra le rapport d'évaluation.

Le développeur : C'est celui qui est responsable de la réalisation du système, suivant les préconisations du responsable de l'assurance qualité.

Le responsable de l'assurance qualité : Il émet des préconisations au développeur sur le processus de réalisation. Il est responsable des activités de vérification et de validation et fournit aux évaluateurs les justifications demandées par les critères.

L'évaluateur : Il vérifie que les exigences des critères sont bien satisfaites (d'après les justifications fournies par le responsable de l'assurance qualité) et réalise des activités complémentaires d'analyse de risques, de vérification et de validation sur le produit (par exemple, des tests de pénétration). Au vu des résultats, il rédige le rapport d'évaluation.

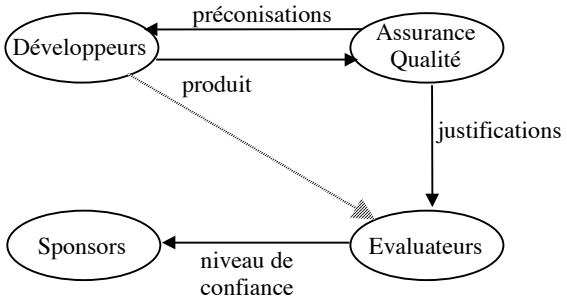

Figure 1. Relations entre les intervenants d'une évaluation

En fait, les activités de vérification et de validation peuvent être réparties entre développeur, responsable de l'assurance qualité et évaluateur.

Dans certains cas, il faut prendre en compte d'autres partenaires qui normalement n'interviennent pas directement dans l'évaluation. Il peut s'agir d'organismes de certification qui, au vu du rapport d'évaluation (par un organisme d'évaluation habilité), émettra un certificat autorisant l'exploitation du système. Il peut également s'agir des utilisateurs finals (les passagers d'un système de transport, par exemple).

2.2. Phases de l'évaluation et cycle de développement

L'application des critères de SQUALE prend en compte l'ensemble du cycle de vie du système (de l'expression des besoins jusqu'au démantèlement du système), mais ne repose pas sur un modèle de cycle de vie ou de développement particulier. Cependant le modèle de référence repose sur l'hypothèse que tout cycle de vie comprend les phases de construction, de service opérationnel et de retrait de service. Ces trois phases principales du cycle de vie sont scindées en étapes, qui en particulier pour la phase de construction sont calquées sur les niveaux de décomposition du système (sous-systèmes, composants, éléments, etc.) qui définissent habituellement les modules gérés en configuration. Chaque niveau de décomposition du système délimite une étape de construction dans laquelle on distingue une tâche de conception, une tâche d'implémentation et une tâche de vérification. Le projet SQUALE a ainsi déterminé un canevas élémentaire de construction de la sûreté de fonctionnement des systèmes, qui est utilisé par récurrence à chaque niveau de conception et sur lequel viennent se greffer les activités d'évaluation décomposées en quatre processus (figure 2) : évaluation des exigences de sûreté de fonctionnement, vérification de conformité, validation, évaluation du système d'assurance qualité.

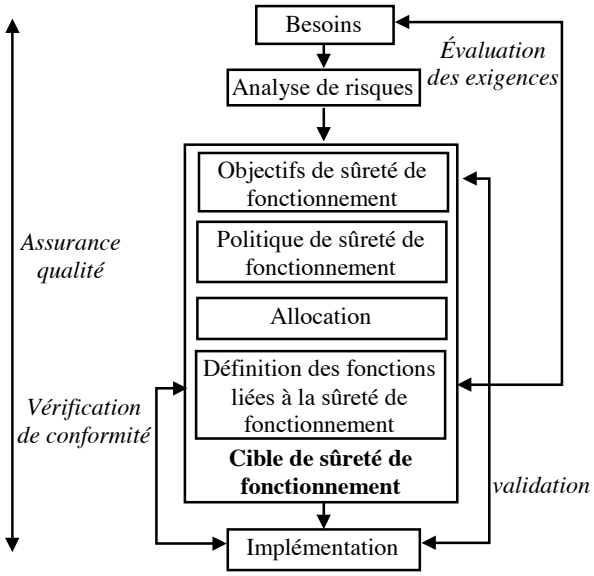

Figure 2. Activités d'évaluation

L'évaluation des exigences de sûreté de fonctionnement examine les objectifs de sûreté, la politique et les stratégies qui ont été choisies pour satisfaire les exigences, et détermine leur pertinence à contrer les risques du système.

La vérification de conformité est la vérification de l'implémentation des fonctions du système, et l'un des buts est de vérifier que les mesures de prévention des fautes, de tolérance aux fautes, de prévision des fautes, et d'élimination des fautes ont été prises tout au long du cycle de développement.

La validation détermine la pertinence de l'implémentation des fonctions liées à la sûreté de fonctionnement du système, ce qui inclut l'efficacité des mécanismes utilisés pour contrer les fautes et risques potentiels, la facilité d'emploi du système, la validité et la représentativité des hypothèses de fautes, et l'analyse des vulnérabilités résiduelles du système tel que construit.

L'évaluation du système d'assurance qualité consiste à s'assurer que les méthodes, outils et processus utilisés pendant le développement, l'exploitation opérationnelle et la maintenance sont adéquats pour atteindre les objectifs de sûreté de fonctionnement, et que les contrôles prévus dans le plan d'assurance qualité ont été réalisés.

2.3. Cible de sûreté de fonctionnement

La cible de sûreté de fonctionnement est un document qui sert de guide de référence pour l'évaluation du système,

et qui est développé dans une version initiale dans la toute première phase de développement du système, préalablement au démarrage des activités d'évaluation. Les évaluateurs se servent de ce document pour identifier les objectifs de sûreté de fonctionnement, les risques et leur cotation, la politique de sûreté, l'allocation des fonctions aux parties du système, et enfin pour définir les activités d'évaluation et leur déroulement. Dans le cas d'un système complexe, le document est complété à chaque étape d'une phase principale. Ce document est équivalent à la cible d'évaluation pour les critères ITSEC ou au dossier de sécurité pour les normes de sécurité-innocuité.

La cible de sûreté de fonctionnement est constituée :

- de la description du système et de son environnement, contenant la description des interfaces du système (interfaces avec d'autres systèmes, interfaces avec l'environnement physique, interfaces hommes-machines, interface avec l'organisation, etc.), les hypothèses sur l'environnement relatives aux risques (identifiant les risques éliminés par les conditions d'environnement) ;

- des résultats de l'analyse de risques qui identifient ce que le système doit préserver et contre quoi il doit être protégé ; cette d'analyse procure une liste de menaces et d'événements indésirables pour le système et pour son environnement, les hypothèses faites pour chaque menace, les cotations de sévérité de chaque menace et la description des méthodes de cotation ;

- des objectifs pour chaque attribut de sûreté de fonctionnement (disponibilité, confidentialité, fiabilité, intégrité, sécurité-innocuité et maintenabilité) ; l'activité a pour but de réduire si nécessaire le niveau de sévérité des risques à un niveau acceptable pour le système et son environnement ;

- de la politique et des stratégies de mise en œuvre de sûreté de fonctionnement qui fixent les normes, règles et procédures d'implémentation des mesures de sûreté de manière à satisfaire les objectifs ;

- de l'allocation de la sûreté de fonctionnement, en définissant le rôle de chaque sous-système (matériel, logiciel, humain, etc.) de l'architecture, de justifier les choix et de spécifier les composants ;

- de l'identification des fonctions liées à la sûreté de fonctionnement et de leurs spécifications ;

- la définition du profil de sûreté de fonctionnement requis pour chaque fonction et chaque composant lié à la sûreté ;

- le plan d'évaluation qui décrit les activités d'évaluation à réaliser et les méthodes d'évaluation à employer, choisies en fonction des attributs de sûreté de fonctionnement du composant, du niveau de confiance à atteindre et de la phase du cycle de vie ; le plan préliminaire préparé dans le cadre de la cible de sûreté de fonctionnement est complété au fur et à mesure de l'avancement de l'évaluation selon le canevas établi par la décomposition récurrente du système.

2.4. Profil de sûreté de fonctionnement

Pour un système, les exigences peuvent amener à définir tout ou partie des attributs de la sûreté de fonctionnement (disponibilité, confidentialité, fiabilité, intégrité, sécurité-innocuité et maintenabilité) et, l'importance de chacun d'eux peut ne pas être uniforme. Ainsi, un système peut n'avoir que des exigences de sécurité-innocuité et de maintenabilité, ces dernières étant d'importance moindre que les premières. Dans le cadre des critères SQUALE, on associe à chaque attribut de la sûreté de fonctionnement un niveau de confiance visé variant entre 1 et 4 : 1 représente le niveau de confiance le plus bas, et 4 le niveau le plus élevé. Un niveau 0 est aussi défini pour indiquer l'absence d'exigence sur un attribut. Par exemple, un système pourrait se voir affecter un « profil de sûreté de fonctionnement » correspondant à la combinaison de niveaux de confiance visés suivante : A1, C0, R3, I3, S3, M2 correspondant à des niveaux 1, 0, 3, 3, 3 et 2 respectivement pour la disponibilité, la confidentialité, la fiabilité, l'intégrité, la sécurité-innocuité et la maintenabilité.

Disponibilité	A1-A4
Confidentialité	C1-C4
Fiabilité	R1-R4
Intégrité	I1-I4
Sécurité-innocuité	S1-S4
Maintenabilité	M1-M4

2.5. Activités d'évaluation

Les activités d'évaluation définies dans le cadre des critères SQUALE sont regroupées en quatre processus :

- évaluation des exigences de sûreté,
- vérification de conformité,
- validation,
- évaluation de l'assurance qualité.

Évaluation des exigences de sûreté de fonctionnement : L'évaluation des exigences de sûreté de fonctionnement a pour objectif de valider les résultats de l'étape de définition des exigences de sûreté. L'activité est décomposée en une identification des risques, une cotation des risques et une analyse préliminaire des risques. L'identification des risques détermine les causes (interactions avec le système) qui peuvent entraîner des conséquences inacceptables pour le système et son environnement et de limiter les investigations par la prise en compte d'hypothèses. La cotation des risques consiste à apprécier le niveau d'apparition des causes de façon à définir les objectifs et le profil de sûreté de fonctionnement. L'analyse préliminaire de risque valide les exigences du système et sert de référence aux activités de vérification et de validation de la réalisation. L'analyse préliminaire de risques est une évaluation de la politique, des principes, de l'architecture et de la définition des fonctions contribuant à la sûreté de fonctionnement pour réaliser les objectifs définis lors de l'étape de cotation des risques.

Vérification de conformité : La vérification de conformité a pour objectif de s'assurer que chaque niveau de décomposition des systèmes contribuant à la sûreté de fonctionnement a été mis en œuvre de façon correcte conformément à ses spécifications, et que les spécifications de bas niveau sont cohérentes avec les spécifications de niveau supérieur. Ce processus est réalisé de facon itérative depuis la phase de définition des spécifications de haut niveau des fonctions contribuant à la sûreté de fonctionnement jusqu'à l'intégration finale du système global et sa mise en service. La vérification doit porter également sur les procédures d'exploitation opérationnelle, de maintenance et de démantèlement du système.

Les activités de vérification de conformité doivent assurer que les hypothèses concernant les fautes et erreurs sont prises en compte correctement dans l'implémentation des fonctions contribuant à la sûreté de fonctionnement. Une attention particulière doit être apportée à la vérification du raffinement de ces hypothèses et à l'exactitude de la mise en œuvre des mécanismes de détection et de recouvrement d'erreurs. Les objectifs de la vérification de conformité sont atteints par l'utilisation d'un ensemble d'activités d'inspections, de revues, de test, par l'emploi de méthodes formelles et d'analyses comportementales. Ces activités de vérification sont réalisées principalement par le développeur du système en synchronisme avec les phases du cycle de vie et en accord avec un plan de vérification accepté par les évaluateurs. Le rôle des évaluateurs est d'analyser et de vérifier les justifications et preuves fournies vis-à-vis de leur adéquation, complétude, et cohérence. Ces vérifications concernent aussi bien les procédures appliquées que les résultats obtenus. Les évaluateurs peuvent être amenés à faire des vérifications supplémentaires à leur discrétion, ou par exemple, à soumettre des jeux de test au fournisseur qui aura la charge de les exécuter et d'amener la preuve que ces tests complémentaires sont concluants.

Validation : L'objectif des activités de validation est de s'assurer que le système est conforme à ses objectifs. Le problème principal est que les objectifs ne peuvent pas toujours être traduits en exigences ou en spécifications du système directement implémentables qui pourraient être analysées par les activités de vérification. Ainsi la tâche principale est une évaluation que le système ne possède pas d'effet de bord non spécifiés, qui sans contredire les spécifications du système, lui donne un comportement qui pourrait avoir des conséquences intolérables.

Ainsi les activités de validation essayent de prendre en compte le fait que les spécifications d'un système sont incomplètes par rapport à l'ensemble des objectifs, que les hypothèses prises pendant les phases de spécification et de conception ne peuvent être identifiées complètement et que celles faites lors de la construction, la phase opérationnelle ou le démantèlement peuvent être erronées.

Les méthodes de validation recommandées comprennent les évaluations probabilistes, les analyses de pénétration, les AMDEC, les arbres de fautes, les analyses de causes communes, les analyses de canaux cachés, etc.

Évaluation de l'assurance qualité : La confiance dans un système repose non seulement sur l'évaluation du système tel que construit et de ses produits associés mais aussi sur l'évaluation des processus utilisés pour son développement et dans sa phase de fonctionnement opérationnel. L'objectif de l'évaluation du système d'assurance qualité est de s'assurer que les procédures utilisées lors du développement, de l'exploitation et du démantèlement du système sont d'un niveau de qualité approprié au niveau de confiance requis pour le système. Cette évaluation est menée par audits et inspection de documents pour les sujets concernant, la gestion de projet et son organisation, la gestion de configuration et des modifications, les procédures de développement, les procédures de mise en service, de fonctionnement opérationnel, de retrait de service, l'examen des revues, la justification des compétences, etc.

2.6. Évaluation des activités de vérification et de validation

Les critères SQUALE définissent pour les activités d'évaluation des niveaux de rigueur (RL), de détail (DL) et d'indépendance (IL) plus ou moins élevés (les niveaux RL, DL et IL vont de 1 à 3) en fonction des niveaux de confiance visés dans le profil de sûreté de fonctionnement.

Le niveau d'indépendance fixe le lien organisationnel entre les évaluateurs d'une activité et le développeur du système, et est coté depuis l'indépendance de l'évaluateur dans l'organisation de l'entreprise (personne indépendante, service indépendant) jusqu'à la totale indépendance qui peut être obtenue par un laboratoire d'évaluation extérieur à l'entrepreneur (organisation indépendante).

Le niveau de détail fixe les phases du cycle de vie au cours desquelles les activités d'évaluation doivent être réalisées et les exigences sur le contenu des fournitures de sortie de phase délivrées par le développeur aux évaluateurs.

Le niveau de rigueur détermine la manière avec laquelle les activités d'évaluation doivent être réalisées, le degré de justification qui doit être fourni par le développeur (par exemple, l'adéquation d'une méthode ou d'un outil, l'efficacité d'une méthode de tests…), et enfin fixe le niveau de preuves à apporter (couverture des tests), ou encore fixe le degré d'utilisation d'une méthode d'analyse ou de conception (méthodes formelles).

Les définitions des niveaux de rigueur et de détails sont spécifiques à chaque méthode recommandée par les critères SQUALE. Les critères fournissent pour chaque activité d'évaluation la définition de chacun des trois niveaux de rigueur et de détail, les relations entre les méthodes d'évaluation et les attributs de la sûreté de fonctionnement et finalement, les relations entre le profil de sûreté de fonctionnement et les niveaux de rigueur, de détail et d'indépendance.

3. Expérimentation des critères sur METEOR

3.1. Description du système

La nouvelle ligne de métro parisienne METEOR (METro Est-Ouest Rapide) se développe, dans sa première tranche, entre Tolbiac-Nationale au sud-est et Madeleine au nord-ouest en desservant deux nœuds importants du réseau parisien, la gare de Lyon et Châtelet. Elle est dimensionnée à terme pour un trafic de 40 000 voyageurs par heure et par sens avec un intervalle entre deux trains de 85 secondes aux heures de pointe. Cette ligne est pilotée par un nouveau Système d'Automatisation de l'Exploitation des Trains, le SAET, développé par Matra Transport International. Ce système à automatisme intégral autorise la circulation de trains sans conducteur ni accompagnateur. Il est conçu pour répondre à de fortes contraintes permettant d'assurer une très grande qualité de service, une grande souplesse d'exploitation et une facilité d'adaptation à l'environnement (trains non équipés transitant parmi des trains en automatisme intégral par exemple).

Le SAET est architecturé en quatre sous-systèmes : le Pilote Automatique et Signalisation (PA-SIG), le Poste de Conduite Centralisé (PCC), les façades de quai (FQ), et les moyens audiovisuels (MA).

Le PA-SIG commande la marche des trains et gère les arrêts en station en contrôlant la fermeture et l'ouverture des portes du train et des portes palières. Il effectue en sécurité le contrôle de la vitesse des trains, la commande de l'énergie de traction, la commande des itinéraires, la commande des portes et le suivi des alarmes « voyageurs ». Le Pilote Automatique est une architecture multiprocesseurs répartie. Il comporte le PA Ligne (PAL), les PA Sol (PAS) répartis le long de la ligne et les PA Embarqués (PAE) à bord des trains. Le PAL et les PAS dialoguent entre eux et avec le PCT (Poste de Commande et de contrôle de Trafic) via un réseau de transmission à haut débit. Le PAS communique avec les PAE sur la section qu'il gère via la transmission continue.

Le PCC permet aux opérateurs d'exploitation de superviser et de réguler à distance la circulation des trains et de contrôler le bon fonctionnement des fonctions essentielles du réseau. Pour assurer ses fonctions, l'opérateur dispose d'un Tableau de Contrôle Optique (TCO) qui lui fournit l'état en temps réel du réseau ainsi que de terminaux informatiques et de platines de commandes pour agir sur l'état du système. Il a aussi à sa disposition des moniteurs vidéo lui donnant les images des quais et de l'intérieur des rames et des moyens de communication phoniques avec les voyageurs dans les trains ou sur les quais ou avec le personnel d'exploitation et de maintenance.

Les façades de quai assurent la protection des voyageurs contre tout risque de chute sur la voie. Les échanges quai/train sont autorisés par l'ouverture des portes palières lorsque le train est correctement arrêté à quai. Dans ce cas, les portes des trains et les portes palières sont en regard. En cas de dysfonctionnement, des portes de secours autorisent l'évacuation des passagers du train lorsque celui-ci est mal positionné à quai.

Les moyens audiovisuels assurent la protection des voyageurs par une surveillance et une communication directe des voyageurs avec les opérateurs du PCC. Les moyens de communication sont fiabilisés et satisfont une grande disponibilité.

3.2. Cible de l'évaluation

Dans le cadre du projet SQUALE, l'étude de cas proposée pour éprouver les critères d'évaluation et le processus de certification est le sous-ensemble du SAET permettant le contrôle et la supervision du système. Il permet la commande et la transmission des ordres opérateur aux trains, les opérations d'exploitation telles que l'ajout ou le retrait de trains, le changement de programmes d'exploitation et la remontée d'informations du système vers les opérateurs ainsi que les alarmes. La « cible de sûreté de fonctionnement » comprend (cf. figure 3) :

- les opérateurs au PCC,
- les terminaux opérateur assurant l'interface homme-machine,
- le TCO qui visualise en temps réel l'état de la ligne et la position des trains,
- le PCT qui gère les commandes opérateur et les informations d'exploitation ou de maintenance,
- le PTCS (Platine des TéléCommandes Sécurisées) qui permet à l'opérateur de valider les commandes sécuritaires,
- le PAL qui transmet les commandes sécurisées aux équipements (PAS ou PAE via le PAS),
- le réseau de transmission à haut débit qui permet l'échange de messages entre les différents équipements connectés (PCT, PAL, PAS).

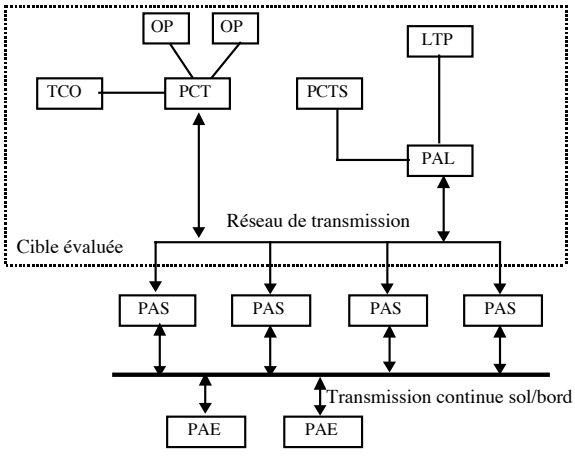

Figure 3. Architecture générale du SAET de METEOR

Le système doit satisfaire de fortes exigences de sûreté de fonctionnement. Les équipements sont redondés pour assurer une haute disponibilité du système. La sécurité du pilote automatique est assurée par l'utilisation de la technique du processeur codé déjà éprouvée dans le cadre du projet SACEM [15]. La sécurisation des commandes

sécuritaires s'appuie sur le principe de sécurité contrôlée avec une validation de la commande par l'opérateur à partir d'une platine réalisée en sécurité intrinsèque (PTCS).

3.3. Profil de sûreté de fonctionnement

Le profil de sûreté de fonctionnement du système de télécommande de la ligne METEOR a été fixé par les résultats de l'analyse de risques à S4, A3, I3, M3, R2 et C1.

L'analyse de risques, à partir de la définition des types de risques pour le système et son environnement (personnes, équipements, financiers, etc.) a déterminé leur influence sur chacun des six attributs de la sûreté de fonctionnement en cotant la sévérité de l'influence du risque sur chaque attribut de la sûreté de fonctionnement pour chaque cas de défaillance répertorié. Le maximum de la note de sévérité sur l'ensemble des cas de défaillance analysés donne pour chaque attribut le niveau de confiance à atteindre et par combinaison le profil de sûreté de fonctionnement. Liés aux risques d'accident des personnes transportées ou du personnel d'intervention, les objectifs de sûreté de fonctionnement sont élevés (S4), et sont en accord avec la norme EN 50128 du secteur ferroviaire.

Les objectifs de disponibilité (A3), d'intégrité (I3) et de maintenabilité (M3) sont forts car ils prennent en compte des contraintes quantitatives sur le matériel et le logiciel (temps de réparation, taux de disponibilité, MTBF, etc.), mais aussi les répercussions sur la qualité du service voyageur (interruption partielle ou totale de service, respect des horaires, etc.). L'attribut de fiabilité reste d'un niveau moyen (R2) car son influence sur la qualité du service est du second ordre. Les objectifs de confidentialité (C1) sont faibles car les menaces ne concernent que les informations sur les incidents du service voyageur.

3.4. Retours de l'expérience

L'application des critères SQUALE sur la référence du développement du système de télécommande de METEOR pour leur validation montre leur bonne applicabilité à un système industriel complexe ; cependant certaines améliorations doivent être apportées afin de les rendre plus souples, de lever des ambiguïtés et des redondances.

Une souplesse des critères devrait être introduite par un processus d'ajustement qui permettrait au développeur d'utiliser des techniques d'analyse, de test, etc. équivalentes à celles préconisées par les critères. Ce processus d'ajustement devrait également permettre de négocier avec le développeur le contenu des fournitures en utilisant au maximum celles qui sont définies dans le cycle de vie du système, mais pour cela doit être complété par des spécifications en termes de couple objet-contenu des dites fournitures pour chaque niveau de profil de sûreté. Des redondances dans les tâches imposées par les critères doivent être éliminées, car par exemple, contenues à la fois dans les tâches imposées par le système d'assurance qualité et comme tâche d'évaluation propre.

Des précisions de terminologie doivent être apportées, soit pour éviter des interprétations divergentes, soit pour préciser des concepts et notions qui ont été étendues ou restreintes par rapport aux définitions couramment admises dans les communautés de la sûreté et de la sécurité. D'autres précisions doivent lever les doutes sur les responsabilités des acteurs de l'évaluation, pour définir les limites des tâches de chacun, qui pourraient être modulées (ajustement), en autorisant l'alternative de réaliser une tâche technique soit par un laboratoire spécialisé, soit par le développeur, seul le contrôle de la tâche restant de la responsabilité de l'évaluateur.

Finalement, afin de rendre les critères plus facilement applicables dans les différents secteurs industriels (aéronautique, ferroviaire, nucléaire, télécommunications, etc.) une étude aura pour objectif d'indiquer les directives pour adapter les critères en concordance avec les normes sectorielles et sera complétée par quelques cas d'espèce (DO178B, CEI1508, ITSEC/ITSEM...).

Conclusion

Au vu des résultats de cette première expérimentation, il est donc possible d'apporter certaines améliorations aux critères de SQUALE. Une autre expérimentation devrait commencer prochainement dans un cadre très différent : il ne s'agit plus d'un système déjà réalisé, mais au contraire d'un système en cours de définition chez Bouygues Telecom. De plus, les exigences de ce système sont beaucoup moins sévères que celles de METEOR et devraient porter davantage sur la sécurité-confidentialité que sur la sécurité-innocuité. Cette deuxième expérimentation devrait permettre de vérifier (voire d'améliorer) la gradation des critères de SQUALE.

Une nouvelle version des critères de SQUALE, incluant ces améliorations ainsi que des directives pour l'utilisation de ces critères dans le cadre de certifications en fonction des normes existantes, devrait être publiée en septembre 1998.

Références

[1] *ITSEC: Information Technology Security Evaluation Criteria*, Office for Official Publications of the European Communities, Luxembourg, 1991, ISBN 92-826-3004-8.

[2] J.-C. Laprie, J. Arlat, J.-P. Blanquart, A. Costes, Y. Crouzet, Y. Deswarte, J.-C. Fabre, H. Guillermain, M. Kaâniche, K. Kanoun, C. Mazet, D. Powell, C. Rabéjac, P. Thévenod, *Guide de la Sûreté de Fonctionnement*, Cépaduès Éditions, 2ème édition, 1996, 370 p., ISBN 2.85428.382.1.

[3] TCSEC: *Department of Defense Trusted Computer System Evaluation Criteria*, U.S. Department of Defense, 1985.

[4] TNI: *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria*, National Computer Security Center, NCSC-TG-005, 31 July 1987.

[5] NIST-NSA, *Federal Criteria for Information Technology Security*, *Version 1.0*. 1992, National Institute of Standards and Technology (NIST) and National Security Agency (NSA).

[6] *ITSEM: Information Technology Security Evaluation Manual — Provisional Harmonized Methodology,* Office for Official Publications of the European Communities, Luxembourg, September 1993, ISBN 92-826-7087-2.

[7] CCEB, *Common Criteria for Information Technology Security Evaluation* - Version 1.0, 31 January 1996, Common Criteria Editorial Board.

[8] *Certification Considerations for Highly-Integrated or Complex Aircraft Systems*, ARP 4754, Society of Automotive Engineers (SAE), Inc. 1995.

[9] *Considérations sur le logiciel en vue de la certification des systèmes et équipements de bord*, DO 178B/ED12B, Radio Technical Commission for Aeronautics (RTCA), European Organization for Civil Aviation Electronics (EUROCAE) 1992.

[10] CENELEC EN 50126, *Applications ferroviaires : Spécification et démonstration de la fiabilité, de la maintenabilité et de la sécurité (FDMS)*, Comité Européen de Normalisation Électrotechnique (CENELEC) 1997.

[11] CENELEC EN 50128, *Applications aux chemins de fer : Logiciels pour systèmes de commande et de protection ferroviaire*, Comité Européen de Normalisation Électrotechnique (CENELEC), janvier 1997.

[12] CENELEC ENV 50129, *Applications aux chemins de fer : Systèmes électroniques de sécurité pour la signalisation*, Comité Européen de Normalisation Électrotechnique (CENELEC), avril 1997.

[13] CEI 1508, *Sûreté fonctionnelle : Systèmes relatifs à la sûreté*, *Parties 1 à 7*, 1995, Commission Électronique Internationale (CEI).

[14] Pierre Corneillie, Yves Deswarte, Alan Hawes, Mohamed Kaâniche, Helmut Kurth, Tim Manning, Sylvain Moreau, Angelika Steinacker, *SQUALE — Definition of draft criteria for the assessment of dependable systems*, Rapport LAAS n°97166, Contrat ACTS SQUALE, Project AC097, mai 1997, 138p. — également disponible à <http://www.research.ec.org/squale/>.

[15] Jean Martin, Sonia Wartski et Christian Galivel, "Le processeur codé : un nouveau concept appliqué à la sécurité des systèmes de transports", *Revue Générale de Chemins de Fer*, juin 1990, pp.29-35.