La sûreté de fonctionnement

Didier Buchs

Objectif de la sûreté de fonctionnement

Spécifier, concevoir, réaliser et exploiter des systèmes où la faute est naturelle, prévue et tolérable.

Concepts de base et terminologie

sûreté de fonctionnement = confiance justifiée dans le service délivré

service = comportement perçu par ses utilisateurs (humains où physiques)

Attributs de la sûreté de fonctionnement:

- Disponibilité (prêt à l'utilisation)
- Fiabilité (continuité du service)
- Sécurité-innocuité (non-occurence de défaillance catastrophique)
- Sécurité-confidentialité (manipulation non-autorisées des informations)

- Intégrité (non-occurence d'altérations inapropriées de l'information)
- Maintenabilité (aptitude aux réparations)

Terminologie de l'origine des entraves à la sûreté:

- défaillances (spécification non respectée, déviation du service par rapport à la fonction)
- spécification ou fonction (description du service attendu)
- erreur (état pouvant entraîner une défaillance)
- faute (cause d'une erreur)

faute ⟶ erreur ⟶ défaillance ⟶ ...

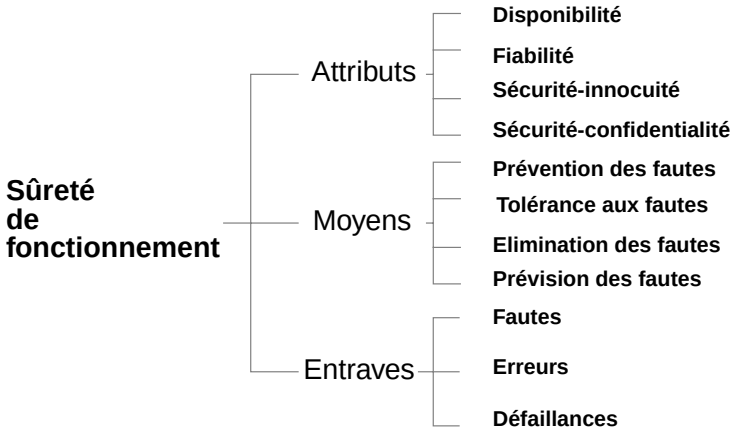
Comment tenir compte de la sûreté de fonctionnement ?

Méthode de développement destinées a:

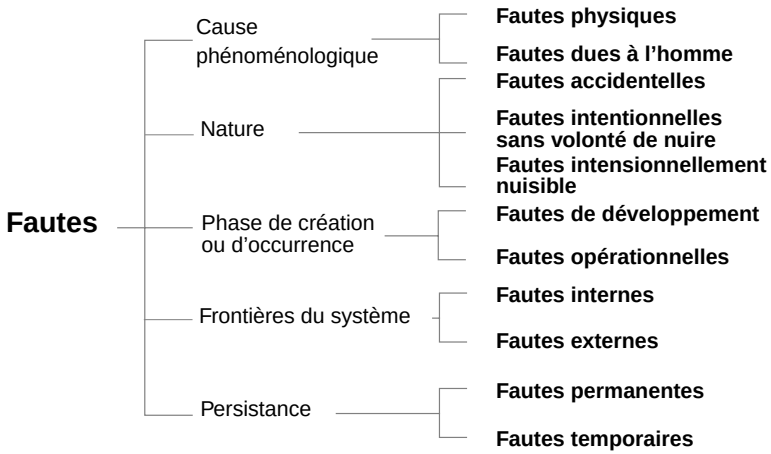
- la prévention des fautes
- la tolérance aux fautes
- l'élimination des fautes
- la prévision des fautes

Caractéristiques principales: la combinaison de ces techniques assure l'obtention de la sureté de fonctionnement.

Sûreté de fonctionnement



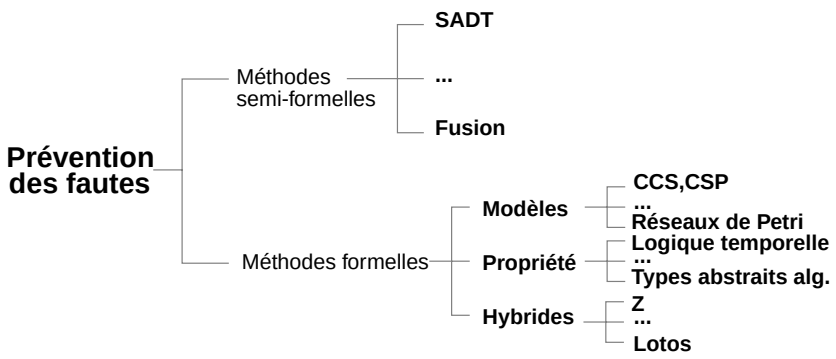
Quelles fautes peuvent survenir ?

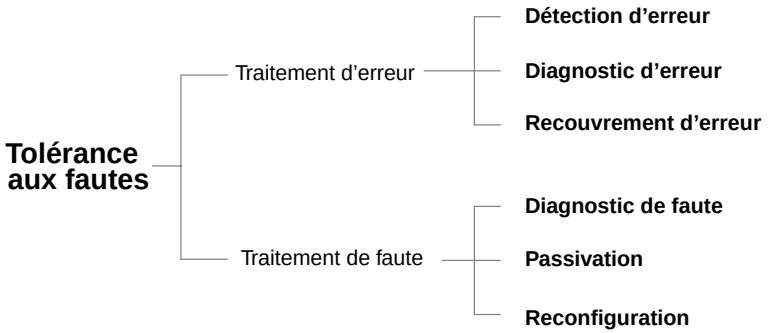


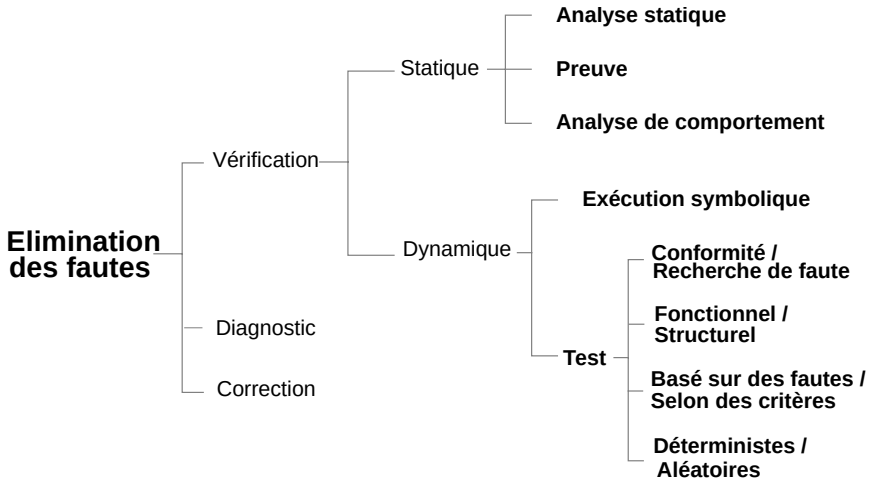
Fautes dues à l'homme

- Fautes de conception
- Fautes d'interaction
- Logiques malignes
- Intrusions

Moyens pour la sûreté de fonctionnement







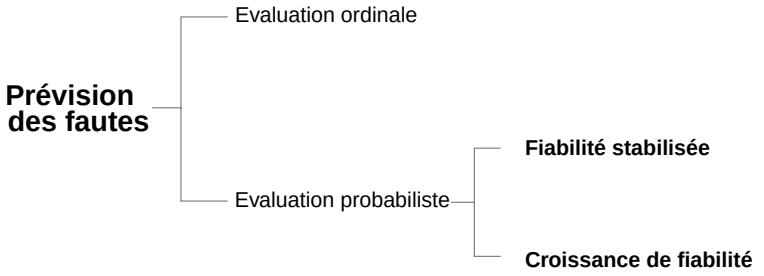
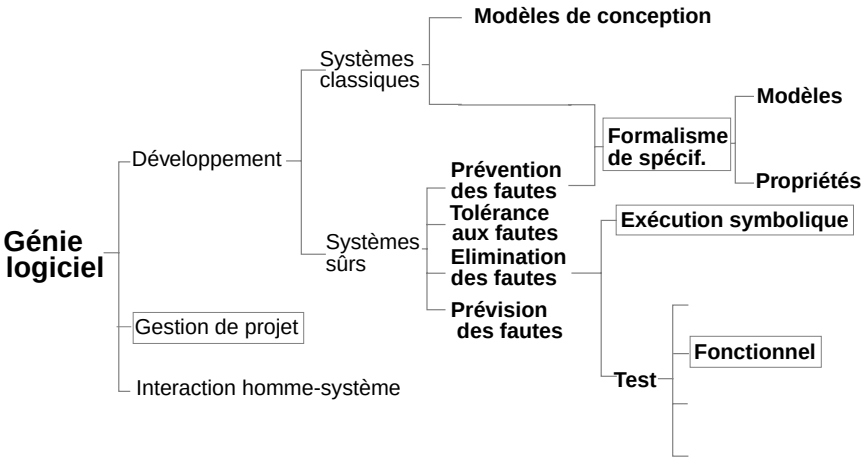


Diagramme du cours



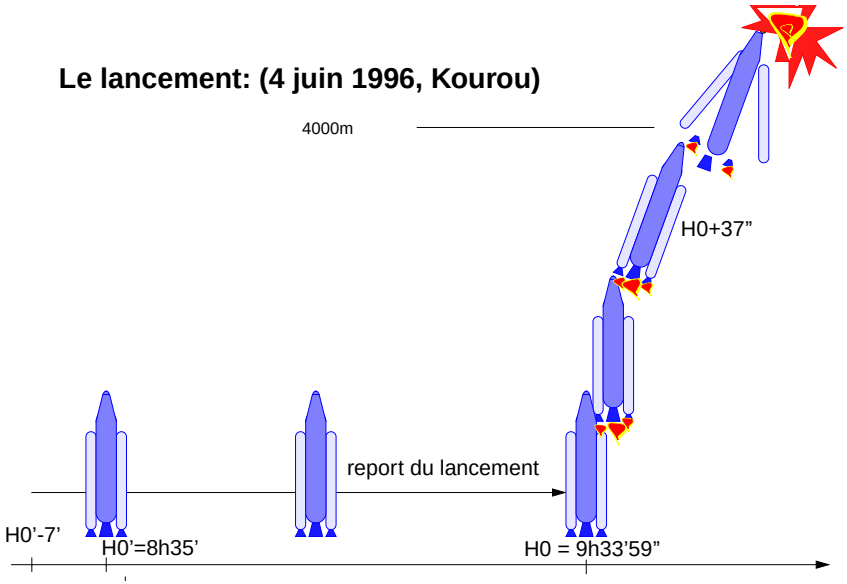
Un exemple concret de catastrophe: Ariane 501

Référence: Rapport de la commission d'inspection (J.L. Lions chairman) 19 juillet 1996.

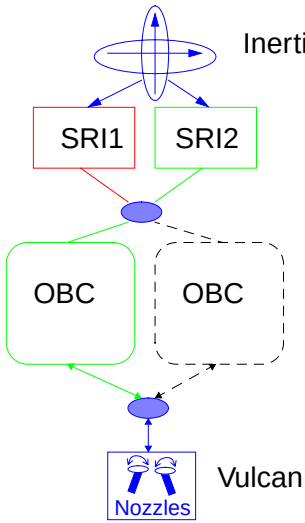
Cahier des charges de la commission:

- Déterminer les causes de l'échec du lancement
- Critiquer les procédures de test de qualifications et d'acceptations
- Déterminer les moyens pour remédier à ce problème et éventuellement en découvrir d'autres.

Le lancement: (4 juin 1996, Kourou)



Configuration du système



Caractéristiques principales du système

- Haut degré de duplication des composants pour augmenter la fiabilité
- L'altitude et les déplacements spaciaux sont mesurés par les SRI.
- Les deux SRI ont même soft et hard et opèrent en parallèle
- Un SRI est actif tandis que l'autre est en attente active
- En cas de problème d'un SRI l'autre est employé immédiatement à sa place.
- Les SRI de Ariane 5 sont identique aux SRI de Ariane 4
- Il y a deux OBC, dont un est actif et l'autre est de secours
- Les données des SRI sont transmises au OBC par l'intermédiaire d'un bus de donnée
- L'OBC contrôle les déviateurs de jets (nozzles) par l'intermédiaire d'actuateurs et de servo-valves.

Suite des événements (vers le passé)

- Désintégration du lanceur à H0 + 39s (charge aérodynamiques trop importantes à cause de l'angle de 20 degré pris par la fusée)
- Angle d'attaque causée par une déflection complète des déviateurs de jets.
- La déflection à été commandée par l'OBC sur la base de données transmises par le SRI actif (SRI2). Ces données ne contenaient pas de données de vol correctes. Il s'agissait en fait de motifs de diagnostiques du SRI 2, qui ont été interprétée comme données de vol.
- SRI2 fournis des informations éronnées car l'unité déclare une erreur due à une exception logiciel.
- L'OBC ne peut commuter le SRI2 sur le SRI1 car le SRI1 à cesser de fonctionner pour la même raison que SRI2 lors du cycle précédant.
- L'exception logiciel du SRI a été causée par une

conversion 64 bits FP -> 16 bits Signed Integer hors représentation possible. L'exception est une erreur d'opérande. L'instruction de conversion (Ada) n'était pas protégée (bien que d'autres instructions le fussent).
- L'erreur c'est produite dans une portion de code qui ne sert qu'au réglage de la plate-forme à inertie. Durant le décollage cette fonction ne sert à rien.
- La fonction de réglage est opérationnelle pour 50 secondes après le démarrage du mode de vol des SRI qui à lieu à H0 -3s pour Ariane 5. Cette fonction est donc opérationnelle pendant env. 40s durant le vol (c'est une spécification de Ariane 4 et non de Ariane 5).
- L'erreur d'opérande c'est produit à cause d'une valeur particulièrement élevée de la fonction d'ajustement appelée BH (Horizontal Bias), correspondant à la vitesse horizontale ressentie par la plate-forme. Cette valeur était différente pour Ariane 5 que pour Ariane 4 à cause d'une différence de principe de trajectoire.

Commentaires

Cause technique de la catastrophe: manque de protection de la conversion, ce qui a causé l'arrêt de l'ordinateur du SRI.

Choix technologiques de programmation: Toutes les conversions ne sont pas protégées, car il y avait un objectif de ne pas avoir une surcharge de plus de 80% de temps pour ces activités.

Le choix des variables à protégé à été motivées pour 7 variables, mais finalement pour des raisons obscures seulement 4 variables ont été protégées.

Une des raisons de ne pas protéger ces trois variables réside dans des limites physiques ou des marges de sécurité très larges (ce qui était un raisonnement erroné pour BH).

Ces choix ont été faits d'un commun accord entre les partenaires du projet.

Il n'y a pas de preuves que des données de la trajectoire aient - été utilisée pour analyser le comportement de ces variables et qu'il a été conjointement admis de ne pas inclure les données de la trajectoire d'Ariane 5 dans le cahier des charges du SRI.

Choix technologiques de conception de la gestion d'erreurs:

Malgré cette erreur, la mission n'a pas échoué pour cette raison uniquement. La spécification du système de gestion d'exception a été lui-même une cause de l'échec. Celle-ci dit qu'en cas d'exception le système doit indiquer sur le bus cet échec et le stocker sur une EEPROM (qui a été retrouvée pour Ariane 501). Finalement le SRI doit être stoppé.

C'est donc l'arrêt du SRI qui a été fatal. La raison de ce choix est que ces exceptions sont censées refléter un problème hardware, ce qui dans ce cas est raisonnable puisque le système de sauvegarde doit alors entrer en service.

Il est clair que malgré l'erreur flagrante de conception logiciel, des mécanismes peuvent être introduits pour atténuer ce genre de problèmes.

- Le SRI aurait pu continuer à fournir sa meilleure

estimation des informations nécessaires.

- Il y a une raison de préoccupation qu'une exception logiciel cause un arrêt du processeur dans des équipements critiques. La perte d'une fonction logiciel est dangereuses car le même logiciel est utilisé dans les deux SRI.

Choix technologiques de conception de la procedure de recalage:

La raison de la poursuite de la procédure de recalage après le décollage est due à des choix anciens de la gamme Ariane. En particulier lié à des problèmes lors de report de lancement, ce qui permet juste un décalage de la fenêtre de tir sans recommencer toute la longue procédure de réinitiallisation. Ces principes n'ont pas vraiment de raison d'être pour Ariane 5 qui a adopté d'autres procédures d'initialisation.

Cette procédure n'a également pas de raison d'être pour des raisons de principes même de l'ajustement qui est une opération qui doit être faite lorsque la fusée est immobilisée.

Commentaires généraux

La commission souligne le fait qu'une défaillance logiciel à une nature très différente qu'une défaillance matérielle. Le logiciel est flexible et expressif et encourage des cahier des charges complexes mais en contre-partie conduit à des réalisations complexes qui sont difficiles à certifier.

Le point de vue pris lors de la conception du système est qu'un logiciel doit être considéré comme correct jusqu'a ce qu'il soit en faute. La commission propose le contraire, le logiciel doit être supposé erronés jusqu'a ce que l'application de la meilleure méthode connue ait démontré qu'il soit correct.

Procédure de test et de qualification

Procédure de qualification du système de Vol:

- Qualification des équipements
- Qualification du logiciel (Logiciel embarqué)
- Intégration d'étage
- test de validation du système

Le test du SRI comme boite noire est impossible pour des raisons physiques, uniquement l'injection de données des accéléromètres correspondantes à la trajectoire de vol est possible.

Ces tests n'ont pas été effectués à cause de l'absence des données de vols de Ariane 5 dans le cahier des charges.

La spécification des SRI n'inclut pas de restriction

opérationnelles liées à des choix d'implémentations. De telles déclarations de limitations, qui doivent être obligatoires pour chaque éléments critiques de la mission, auraient servis à découvrir que le système n'était pas compatible avec la trajectoire de Ariane 5.

Une phase complète de test par simulation à été développée pour détecter les problèmes généraux de vols (diverses trajectoires acceptables, pannes des équipements et procédures de récupérations, ...). De nombreux équipements étaient intégré physiquement lors de ce test. Les deux SRI ne l'étaient pas et étaient remplacés par des modules logiciels.

Les tests d'intégrations des SRI n'étaient à ce niveau que des tests de bas niveau des capacités électriques et de transmission du bus de données.

Le choix de ne pas intégrer les SRI dans la boucle de test était du à la complexité de cette tache. Des considérations de précision des équipements de tests ont également conduit à remplacer les SRI par des simulations logiciels (la précision dans ce test n'était pas le point crucial).

La commission souligne que l'objectif à ce niveau de test d'intégration n'est pas seulement de vérifier les interfaces mais est de voir que l'ensemble des composants fonctionnent ensembles. Il y avait un risque majeur de penser que le bon fonctionnement pour Ariane 4, ne demandait pas de test d'intégration pour Ariane 5.

Recommandations de la commission

R1: La fonction d'ajustement doit-être coupée dès le décollage.

R2: Préparer des moyens de tests plus réalistes, injecter des données réalistes et réaliser un test en boucle fermée complet. Une simulation complète doit être faite avant chaque mission. Augmenter la couverture de test.

R3: Ne pas autorisé qu'un quelconque capteur arrête d'envoyer ses données.

R4: Organiser pour chaque système incluant du logiciel une procédure de qualification. Fournir des informations claire sur les restrictions d'utilisations.

R5: Revoir chaque logiciel de vol et en particulier:

- Identifier chaque suppositions faites par le code
- Vérifier les valeurs que peuvent prendre toutes les variables des logiciels

R6: Partout ou cela est possible, n'utiliser les exceptions que pour les fonctionnalités de sauvegardes.

R7: Fournir plus de données à la télémétrie pour la panne de chaque composants, ainsi les équipements de sauvegarde d'informations seront moins essentiels.

R8: Reconsidérer les composants critiques, inclure les fautes logiciels.

R9: Inclure des personnes extérieures au projet pour les tests.

R10: Inclure les données de trajectoire dans les spécifications

R11: Revoir la couverture de test

R12: Attribuer le même soin aux documents de justification du code qu'au code lui-même.

R13: Etablir une équipe qui prépare la procédure de qualification, établir des règles claires qui établisse cette qualifications à travers des procédures de haute qualité de spécification, vérification et test du logiciel.

R14: Augmenter la clarté de l'organisation de la coopération entre les partenaires du projet Ariane 5, établir des contacts entre ingénieurs qui s'affranchissent des aspects hiérarchies.

Remarques finales:

Une série de fautes de gestion du projet ont conduits à la catastrophe:

- Erreurs logiciels mal prises en compte dans la réalisation du système
- Limites de l'implémentation mal fixées, confusion entre les spécifications de Ariane 4 et 5.
- Test d'intégration incorrect

Réutilisation mal réussie car:

- Spécification mal établie
- Limites de l'implémentation mal définie
- Tests trop limités