Autonomie et sécurité des satellites

Quelques règles de base pour la conception et les opérations

Dominique SÉGUÉLA

04 Juin 2012

Quelques caractéristiques des systèmes orbitaux

Pas de maintenance en vol, ni préventive ni corrective

- l'architecture (fonctionnelle et matérielle) doit permettre des actions correctives
  - éléments redondants, Xstrapping,...
- contournements parfois possibles par modification du logiciel de vol

Une opérabilité limitée

- commandabilité limitée et observabilité parfois indirecte
- bien prévoir les points de mesures et de commande
  - utilisés à bord et/ou au sol
- visibilités discontinues
  - pas de possibilité de réaction rapide via une boucle sol

Des coûts élevés

- coût des satellites et des lancements
- problématique des débris

Pas de place pour l'improvisation

- risque de situation non contrôlée et irréversible conduisant à la perte du satellite
- procédures validées exhaustivement et gérées en configuration
- entraînement des opérateurs

Tous les satellites doivent être capables

- de détecter une panne de façon autonome
- de prendre une décision en fonction
  - de la nature de la panne
  - de son impact sur l'accomplissement de la mission
  - de son impact sur la sécurité du satellite

La décision dépend du niveau d'autonomie donné au satellite

Principe de base : on ne traite que les pannes « simples »

- on fait l'hypothèse que 2 événements indépendants ne peuvent pas se produire au même endroit au même moment (*probabilité quasi-nulle*)
  - l'AMDEC identifie les pannes (y compris celles de mode commun)

FDIR Failure Detection Isolation and Recovery
AMDEC Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité

Surveillance et gestion des anomalies (FDIR) : un des services de la commande/contrôle

La FDIR Système est distribuée entre le Sol et le Bord

Le rôle de la FDIR Système est :

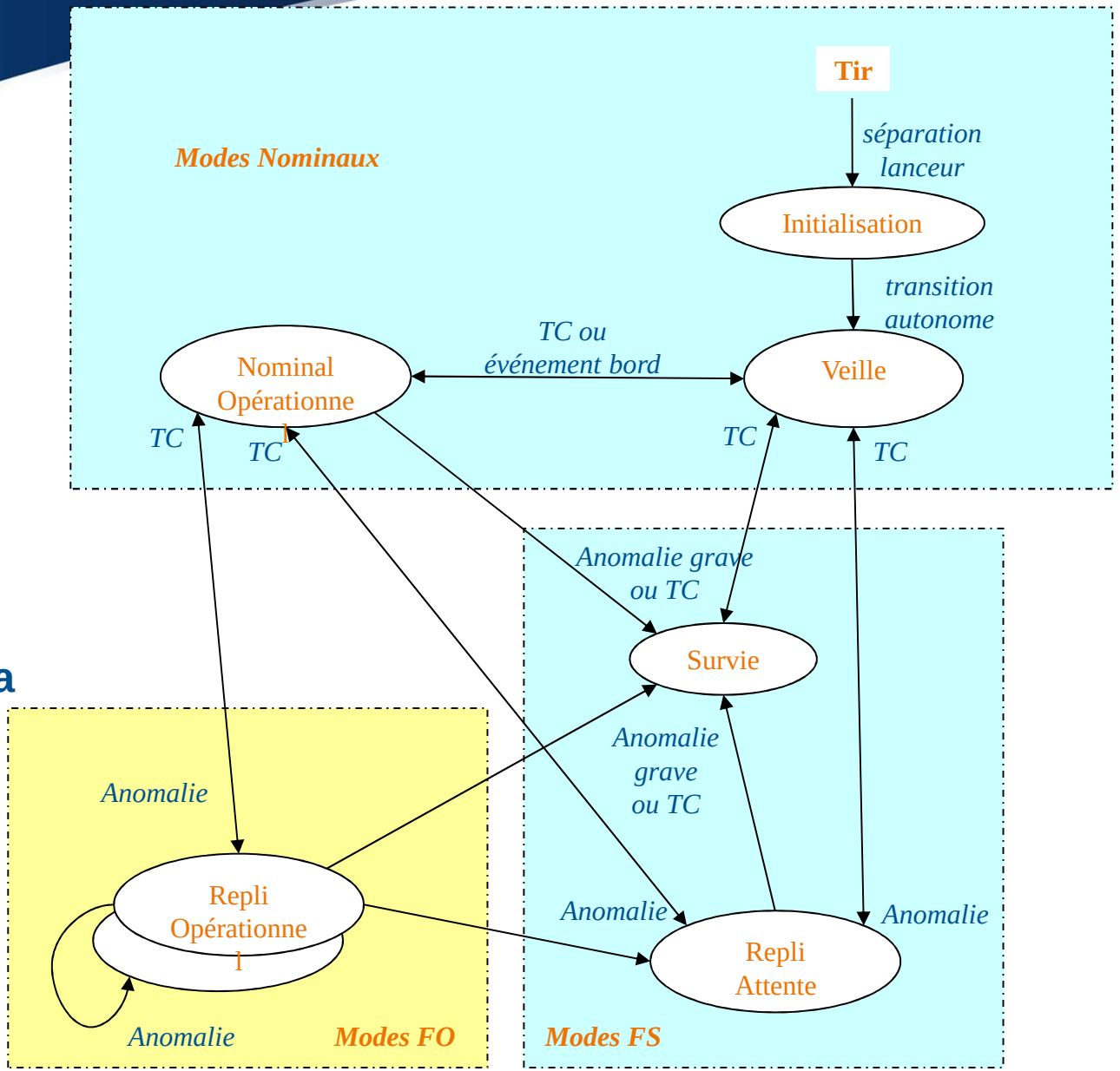
- la surveillance des paramètres et du fonctionnement
- la détection des anomalies
- le déclenchement éventuel d'actions (réponses), pour isoler l'anomalie
- la reconfiguration éventuelle des ressources actives
- le redémarrage, autonome ou pas, des fonctions
- les comptes-rendus du bord vers le sol

La surveillance et le gestion des anomalies et des pannes du Système ont :

- un objectif de robustesse, par la surveillance et gestion des anomalies de fonctionnement
- un objectif de performance par surveillance et gestion des anomalies sur des données (perte de données, perte de performances)

En général la priorité est donnée à l'objectif de robustesse, dont dépend le succès de la mission.

Exemple de diagramme des modes, des transitions et de la FDIR



FO = Fail-Operational
FS = Fail-Safe

Degrés de criticité des pannes

Niveau 4 : Alerte (*grave*) matériel

- passage en mode survie

Niveau 2/3 : Perte de performance

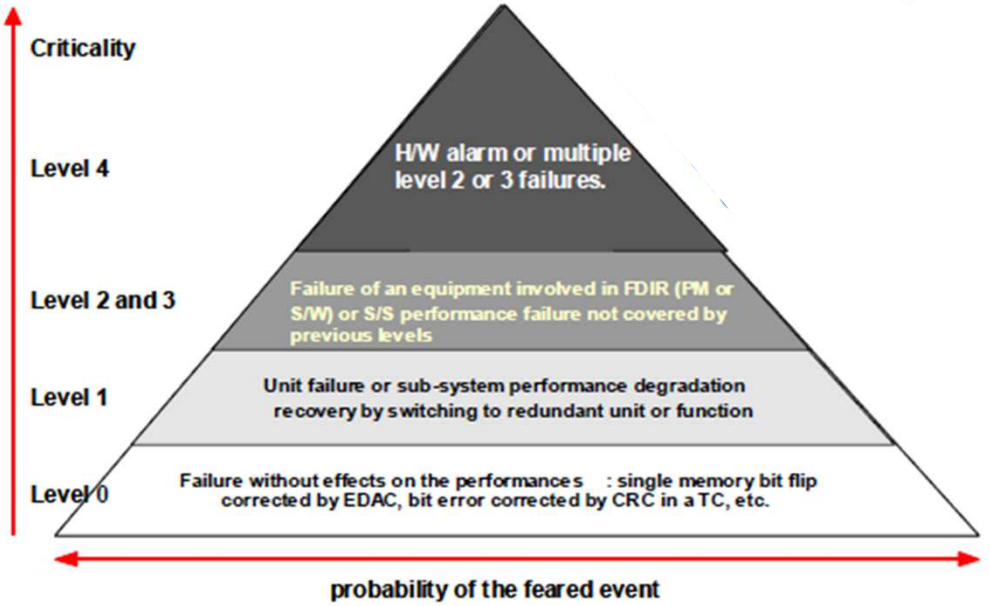
- passage en mode dégradé

Niveau 1 : Equipement / Instrument

- passage sur équipement/instrument redondant

Niveau 0 : interne équipement

- correction interne (transparente)



Mode survie

- le satellite est dans un état stable
- il peut y rester plusieurs jours sans dégradation
- seules les fonctions minimum sont assurées, avec des ressources aussi indépendantes que possible du mode normal
  - ✦ senseurs, actionneurs, logiciel,...
- la sortie de survie est gérée par le centre de contrôle

Traitement des pannes selon leur niveau de criticité

Niveau 0

- pannes détectées et corrigées localement et immédiatement, sans effet sur les performances
- entièrement décentralisé au niveau équipement (matériel ou logiciel)

Niveau 1

- pannes équipement corrigées par une commutation sur l'équipement ou la fonction redondante
- distribué au niveau équipement : détecté par l'équipement (implémentation matérielle), passivation réalisée par le logiciel centralisé qui gère la configuration des équipements

Niveau 2

- anomalies vues au niveau des chaînes fonctionnelles
- détectées et passivées par le logiciel applicatif de la chaîne fonctionnelle →changement de mode
  - chaîne fonctionnelle centralisée dans le calculateur central → traitement de l'anomalie de façon centralisée
  - chaîne fonctionnelle décentralisée dans un équipement dédié→ traitement de l'anomalie par cet équipement de façon décentralisée

Niveau 3

- anomalies majeures affectant le calculateur central
  - détection des anomalies matérielles par le watchdog HW (régulièrement réarmé par le logiciel central)
  - détection des anomalies logicielles réalisée par le watchdog SW
  - passivation réalisée par le module de reconfiguration, qui pour des raisons de sûreté de fonctionnement, est entièrement matériel

Niveau 4

- alarmes système ou accumulation d'anomalies de niveau inférieur
- générées de façon décentralisée (décharge batterie signalée par le système de puissance, dépointage anormal détecté par le SCAO, etc …)
- entièrement traitées par le module de reconfiguration (matériel) → passage en survie

Urgence

- toute panne qui compromet à court terme la bonne santé du satellite doit être détectée et passivée à bord en autonome
  - passivation = suppression des effets de la panne

Type de mission et exigences de disponibilité

- un système de télécommunication doit demeurer opérationnel en toutes circonstances
  - le satellite doit rester « fail-op » : coût ↗↗ et complexité ↗↗
- les missions d'observation de la Terre et les missions scientifiques sont moins exigeantes en disponibilité
  - on privilégie la robustesse du satellite et on accepte d'interrompre la mission

Phases de vie

- « fail safe » en routine
- « fail op » dans certaines phases critiques
  - ex : insertion dans l'orbite martienne

« Coût » de l'autonomie

Validation

- logiciel de vol plus complexe, combinatoire plus importante
- validation plus longue et plus complexe
- ↳ coût à comparer aux gains obtenus par l'autonomie
  - ✦ disponibilité, efficacité

Maîtrise du système

- connaître en permanence l'état du satellite
  - ✦ comprendre les décisions prises à bord
- pouvoir désactiver et/ou modifier facilement les mécanismes bord
  - ✦ correction d'erreur, évolution de l'environnement (ex: panne permanente)
- maintenir les compétences des opérateurs

→ N'implanter à bord que des mécanismes simples et robustes

Exemples

On privilégie la robustesse (cas d'un satellite d'observation de la Terre) → logique de « fail-safe »

- panne affectant uniquement la charge utile
  - la mission est interrompue
  - le satellite reste dans un état nominal
  - le segment sol investigue, corrige et reprogramme la mission
- panne affectant la plateforme
  - la mission est interrompue
  - si niveau 1, le satellite passe sur l'équipement redondant et reste en mode nominal
    - » le segment sol reprogramme la mission
  - si niveau 2 ou 3 (ou niveau 1 persistant), le satellite passe sur un mode de repli
  - si niveau 4, le satellite passe en survie
  - si niveau >1, le segment sol investigue, corrige et passe le satellite en mode nominal

On privilégie la disponibilité mission → logique de « fail-op »

- équipements en redondance chaude
- poursuite de la mission, éventuellement en mode dégradé

C1

Diapositive 10

C1 Avez-vous des infos sur le traitement de la FDIR sur les satellites de télécom commerciaux ?
CNES; 23/05/2012