Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Application de la fiabilité sur le démonstrateur de lanceur de premier étage réutilisable CALLISTO

CALLISTO - Flight demonstrator for future reusable launcher reliability

OUTIN Coralie
CNES Direction du Transport Spatial
Paris
coralie.outin@cnes.fr

BIARD Arnaud
CNES Direction du Transport Spatial
Paris
arnaud.biard@cnes.fr

MAURIES Alain
CNES Direction du Transport Spatial
Toulouse
alain.mauries@cnes.fr

CHAVAGNAC Christophe
ARIANE GROUP
Les Mureaux
christophe.chavagnac@arianegroup.fr

DAVEZAC Marie-Lou
CNES Centre Spatial Guyanais
Kourou
marie-lou.davezac@cnes.fr

Résumé **- CALLISTO est un démonstrateur en vol de premier étage de lanceur réutilisable. Le défi est de développer les compétences des agences spatiales nationales (CNES, JAXA et DLR) nécessaires à la récupération puis réutilisation d'un étage de lanceur : la conception du véhicule et de ses produits, la mise au point du segment sol et des opérations post-vol de récupération et de réutilisation. Comme tout projet conduit depuis le CSG, la réglementation française sur les aspects sécurité s'applique pour (i) les opérations avant et après vol réalisées sur le site et (ii) la gestion de la sécurité des personnes et des biens pendant le vol. Les niveaux de fiabilité, disponibilité et maintenabilité à atteindre sont à l'appréciation des projets. Le projet CALLISTO a décidé de ne pas spécifier de niveau de fiabilité quantitatif à atteindre. Ce papier décrit donc comment la fiabilité est prise en compte pour (i) garantir un niveau de fiabilité et de sécurité lors des opérations au sol, (ii) permettre l'autorisation de vol et (iii) l'évaluation du niveau de sécurité en vol. Ce papier s'appuie sur des exemples d'application concret.**

Mots-clefs — CALLISTO, fiabilité, sécurité, aptitude au vol

Abstract **— The CALLISTO (Cooperative Action Leading to Launcher Innovation is Stage Toss-back Operations) vehicle is a flight demonstrator for future reusable launcher stages. CALLISTO's objective is to increase the competences of the three national space agencies (CNES, JAXA and DLR) in reusable launcher vehicle: design, ground segment, operations, vehicle toss back. For each vehicle launched from CSG, it is necessary to comply with French regulation for safety during both ground and flight opérations, the other dependability characteristics being the project issue. CALLISTO project decided to not look for quantitative reliability figure. This paper describes how the reliability is coped with to (i) demonstrate safety and reliability figures during ground operations, (ii) authorize flight and (iii) demonstrate relevant safety during flight. This paper is illustrated with application cases.**

Keywords — CALLISTO, reliability, safety, flight worthiness

I. INTRODUCTION

A. Présentation macroscopique du projet

CALLISTO (Cooperative Action Leading to Launcher Innovation in Stage TOss-back) est un projet de démonstrateur en vol pour un premier étage de lanceur réutilisable. Le projet est réalisé en coopération entre trois Etats représentés par leurs agences spatiales : le CNES (Centre National d'Etudes Spatiales) pour la France, le DLR (Deutsches Zentrum für Luft- und Raumfahrt) pour l'Allemagne et la JAXA (Japan Aerospace Exploration Agency) pour le Japon. Les vols seront réalisés au Centre Spatial Guyanais (CSG) qui opère, par ailleurs, des lanceurs commerciaux. Ce projet permet aux différents partenaires de monter en compétence dans le domaine des lanceurs réutilisables, de la définition du véhicule au opérations post-vol pour la récupération en incluant la mise au point des moyens sol.

Fig. 1. CALLISTO en quelques chiffres-clé

Les objectifs de CALLISTO sont multiples : le premier est de récupérer et remettre en vol un étage ayant déjà volé, le second étant d'évaluer les efforts de maintenance et, enfin, le dernier de préparer le CSG à l'arrivée de nouveaux opérateurs. Donc, in fine, l'objectif de CALLISTO n'est non pas de placer un objet en orbite mais de collecter des données en conditions réelles d'utilisation d'un 1er étage de lanceur réutilisable à décollage et atterrissage vertical.

CALLISTO réalisera jusqu'à dix vols sur une période de 6 mois avec ouverture progressive du domaine de vol, ce qui est une première pour un lanceur Européen.

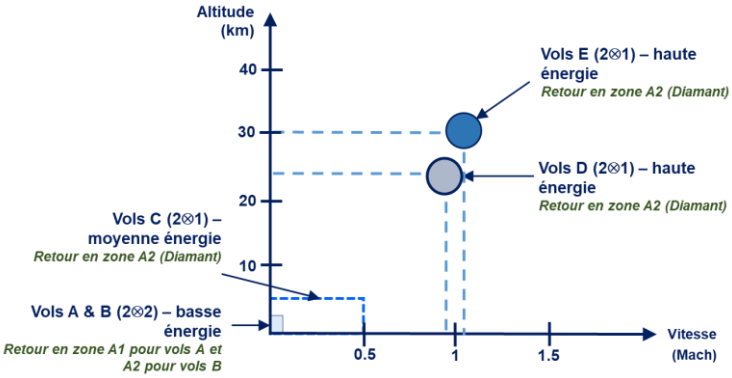

Fig. 2. Plan de vol incrémental CALLISTO

Le projet CALLISTO conduit à faire collaborer des équipes de plusieurs cultures différentes. Les différences culturelles s'expriment sur au moins 2 plans : sur le plan humain (histoire, langue, us et coutumes, …), mais aussi sur le plan technique (niveau d'expérience, d'un typage plus recherche ou plus industriel, …). Ces différences peuvent autant constituer un frein dans la bonne marche du projet et une inhomogénéité dans l'application des processus, qu'une force dans des visions et analyses complémentaires des risques pris.

B. Cadre réglementaire

Tout projet spatial doit être conforme à la réglementation française. La Réglementation Technique (RT) [1] fixe notamment les objectifs de sécurité à atteindre pour les opérations spatiales. Sans même parler de sa finalité (placer un objet en orbite), le domaine de vol de CALLISTO dont son altitude maximum ne permet pas de considérer les opérations CALLISTO comme des opérations spatiales. Néanmoins, CALLISTO étant le premier démonstrateur de réutilisation à voler depuis le territoire français, une évaluation de la conformité est réalisée pour *« l'exemple »*.

Un autre texte sert de cadre réglementaire : le REI (Règlement d'Exploitation des Installations) [2]. Ce texte est la référence pour la réalisation d'activités au CSG. Ce texte couvre toutes les opérations qui seront réalisées avant et après le décollage du véhicule (sachant qu'aujourd'hui les phases de réutilisation ne sont pas couvertes) ainsi que la définition d'éléments de sécurité du véhicule, notamment pour ce qui a trait à la Mission de Sauvegarde et d'Intervention (MSI) pendant le vol proprement dit.

En supplément, une partie de l'intégration et des tests sur le modèle de vol du véhicule étant réalisés au Japon, le règlement japonais JERG-0001 [3] s'applique. Il a été démontré que les risques rencontrés au CSG et au NTC (Noshiro Test Center – site où sont réalisés les essais à feu de la propulsion fusée) sont similaires :

- Risques techniques liés aux parties mécaniques, fluides et électriques,
- L'exposition à des conditions environnementales extérieures,
- Les opérations sur des fluides cryogéniques et les essais à feu,
- Les risques pyrotechniques seront quant à eux spécifiques au CSG. En effet, un système pyrotechnique, décrit au §IV.B.3) sera intégré au démonstrateur pour réaliser les essais en vol. Ce système permettra de neutraliser le véhicule en cas de danger.

Ces risques, bien qu'à une échelle différente, sont de même nature que ceux associés à des lanceurs opérationnels de plus grande masse/taille, nécessitant l'accord des autorités de sécurité pour l'autorisation d'opérer, voir [4].

Ces deux textes ont servi de référence pour la définition des objectifs de sécurité, déclinés dans les règles de conception du véhicule et les exigences des différents sous-systèmes.

II. Definition des objectifs de surete de fonctionnement vs Demonstrateurs

A. *Des idées reçues…*

Les objectifs de sûreté de fonctionnement initialement définis étaient issus de (i) le cadre réglementaire rappelé au chapitre ci-dessus pour la sécurité, (ii) le retour d'expérience sur des premiers vols pour la fiabilité et (iii) des objectifs d'immobilisation des ressources sur une durée exigée de campagne pour les objectifs de disponibilité. Les objectifs de maintenabilité découlent de la combinaison disponibilité/fiabilité.

La décision de ne pas chercher à atteindre un niveau de fiabilité quantifiée, hors les système de neutralisation (en vol) du véhicule, relève de :

- la difficulté à disposer de valeurs de fiabilité des équipements
  - l'évaluation de fiabilité quantitative n'est pas prise en compte dans les contrat des nouveaux développements, ce qui est le produit du cadre budgétaire très contraint pour un démonstrateur,
  - l'utilisation de COTS et donc la difficulté de disposer de valeurs de fiabilité (et représentatives des conditions d'utilisation de CALLISTO dans la cas où les données de fiabilité du fournisseur sont disponibles) ;

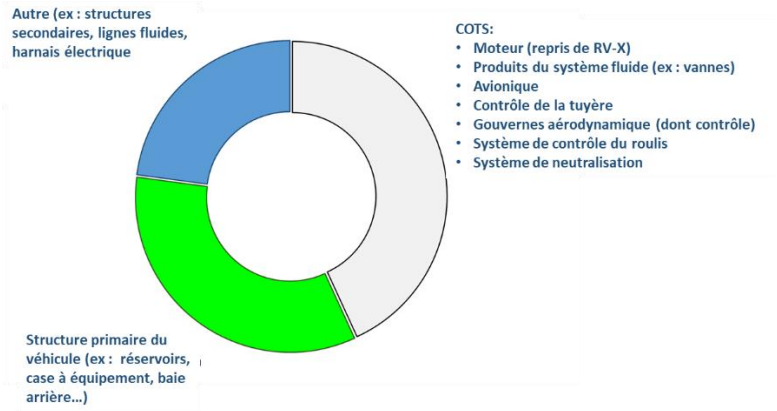

Fig. 3. Répartition entre COTS et produits spécifiques à CALLISTO

- la faible représentativité de la fiabilité sur un unique démonstrateur. Le papier en référence [5] souligne l'écart entre les fiabilités prévisionnelles calculées par les opérateurs de lancement pour les premiers vols et le nombre d'échecs réellement observé. La défiabilité prévisionnelle est le résultat de l'agrégation de défiabilités caractérisées au niveau produit par des méthodes hétérogènes (utilisation de base de données, tests de fiabilité accélérée, *etc.*). Elle n'inclue pas des sources de défiabilité comme les erreurs humaines en conception, en production ou en opération.

B. *…à l'application concrète*

Les objectifs de sûreté de fonctionnement finalement définis pour CALLISTO sont essentiellement qualitatifs et résumés dans le tableau ci-dessous. En parallèle, un objectif quantitatif de fiabilité pour le système de neutralisation est défini et son allocation est définie au paragraphe IV.B.1).

TABLE I. MATRICE D'ACCEPTATION DU RISQUE POUR CALLISTO

		Critère qualitatif		
		Tolérance à 2 défaillances	**Tolérance à 1 défaillance**	**Pas de tolérance à la défaillance**
Gravité	**Catastrophique – perte vie humaine ou dommage irréversible à l'environnement**	Acceptable	Non acceptable	Non acceptable
	Majeur – perte mission	Acceptable	Acceptable	• **Exigence de tolérance à la panne lors des opérations au sol** • **Acceptable en vol**
	Disponibilité	**Le système doit permettre la réalisation de 10 vols en 6 mois.**		
	Sans effet	Acceptable	Acceptable	Acceptable

Les analyses sûreté de fonctionnement sont définies dans un plan de sûreté de fonctionnement. Une analyse de risque englobant le véhicule et ses moyens sol (banc de contrôle, moyens fluides et mécaniques) synthétise tous les risques fiabilité et sécurité de CALLISTO. Cette méthode s'appuie sur le retour d'expérience Ariane et vérifie la cohérence entre les définitions du Segment sol et du véhicule. Cette méthode permet de vérifier qu'en cas de défaillance ou d'erreur humaine, le système de lancement resterait dans un état de sécurité.

Les analyses de risque CALLISTO se concentrent donc sur les deux aspects suivants :

- Risque catastrophique (e.g. décès d'une personne) : le système doit être tolérant à la double panne (critère FS/FS (Fail Safe));
- Risque critique (e.g. perte du véhicule ou de la mission) : le système doit être tolérant à la simple panne (N.B. : aucun objectif de tolérance à la panne en vol) (critère FS).

Pour chaque risque identifié, la conformité au critère FS/FS ou au critère FS est vérifié.

III. FIABILITE ET SECURITE LORS DES OPERATIONS AU SOL (AVANT ET APRES VOL)

A. Fiabilité lors des opérations au sol

Comme évoqué précédemment, le système doit être tolérant à la panne lors des opérations au sol. Pour rappel, le système CALLISTO est constitué d'un Segment Sol et du véhicule lui-même. Lors des opérations avant vol, les principes suivants sont donnés comme objectifs :

- **Une redondance simple vis-à-vis d'un évènement critique**, ce qui implique une remise en sécurité immédiate dès la première panne, au détriment de la disponibilité du système. Le système est donc dimensionné au juste besoin afin de permettre (i) la conformité du système à la tenue de l'exigence qualitative de fiabilité et (ii) des coûts maitrisés pour une installation qui aura une « faible » durée de vie (en comparaison des durées d'exploitation habituellement prévues pour des installations sol au CSG, environ 25 ans pour ARIANE 5 vs 12-18 mois pour CALLISTO au maximum). A titre d'exemple, l'architecture du banc de contrôle CALLISTO est dérivée du banc de contrôle ARIANE 6. En revanche, là où le banc de contrôle ARIANE 6 possède les redondances permettant le meilleur compromis entre disponibilité et sécurité pour permettre d'exclure un calculateur défaillant, le banc de contrôle CALLISTO en possède deux, ce qui impacte directement la disponibilité du système.

- **Le véhicule est dans un état stable en cas de perte de l'alimentation électrique**. Le véhicule ne possède pas de mécanismes permettant de détecter, d'isoler et de « réparer » une panne. Ce choix résulte des contraintes d'encombrement et masse propres à ce type de véhicule. Cela représenterait également un effort de développement logiciel rédhibitoire pour un programme de cette envergure.

Pour les opérations post-vol, la remise dans un état stable du véhicule ainsi que son état de santé (pour un futur vol) impose de reconnecter des servitudes fluide (hélium et azote gazeux) et de génération/distribution de puissance électrique. Tant que le véhicule n'est pas reconnecté, sa remise en sécurité n'est pas garantie. C'est pour cela que le critère « tolérance à une panne » ne s'applique plus dans les phases vol et atterrissage. Dans la plupart des cas, un évènement catastrophique survient après une panne ayant un impact sur la perte du lanceur. Le cas particulier de remise en sécurité du lanceur après vol est détaillé dans le paragraphe suivant car il a fallu déterminé une manière de remettre dans un état stable le véhicule tout en garantissant la sécurité des opérateurs amenés à s'approcher du véhicule à un moment ou à un autre.

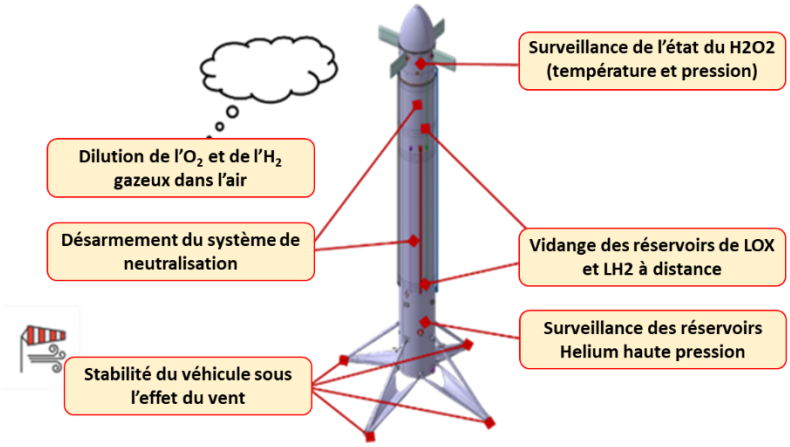

Fig. 4. Etat stable pour CALLISTO après vol

B. *Sécurité lors des opérations au sol*

Le niveau de sécurité à atteindre lors des opérations au sol est bien défini par le cadre réglementaire (REI) du CSG, à savoir la tenue du critère triple panne avant l'occurrence d'un évènement catastrophique (critère FS/FS), voir [4] et [7]. Il a été admis dans le projet et avec l'autorité en charge de la sécurité que la probabilité d'occurrence d'un évènement catastrophique à 10^{-6} par campagne est satisfait par la tolérance à trois défaillances indépendantes (système à risque et deux barrières). Dans les cas où il n'est pas possible de satisfaire au critère FS/FS, le personnel doit être interdit d'accès à la zone de danger.

Un cas d'application concret est la mise en œuvre des fluides cryogéniques. L'hydrogène et l'oxygène liquide (respectivement LH2 et LOX) étant intrinsèquement dangereux lorsqu'ils sont mis en présence (hydrogène explosif à faible concentration et montée en pression rapide, oxygène liquide facilement inflammable et compatibilité limitée avec les matériaux), les opérations sont réalisées à distance dès que l'hydrogène et l'oxygène liquides sont mis en œuvre simultanément pour la phase de remplissage des réservoirs du véhicule.

Avant vol, le véhicule est connecté au système fluide sol (cryogénie, azote gazeux et hélium gazeux) et électrique (alimentation électrique et flux de données Ethernet). Après vol, il est nécessaire de remettre le lanceur dans un état stable (décrit dans la Fig. 4) avant d'autoriser l'accès aux personnels. Il est en particulier nécessaire de (i) éviter l'accumulation d'hydrogène dans les compartiments véhicule en les ventilant (azote gazeux) et (ii) éviter un effet geyser dans le réservoir oxygène en ventilant le système fluide (hélium gazeux).

La remise en sécurité d'un lanceur après vol est une première pour le CNES qui peut néanmoins s'appuyer partiellement sur la connaissance de remises en sécurité après décollage avorté. Pour remettre en sécurité le véhicule après vol, le CNES a décidé d'utiliser un robot opéré à distance pour les servitudes nécessaires : les fluides (hélium et azote) ainsi que l'énergie électrique et la communication. Le robot permet donc la remise en sécurité de CALLISTO (fiabilité) tout en garantissant la sécurité des personnes qui sont en dehors des zones d'effet du véhicule.

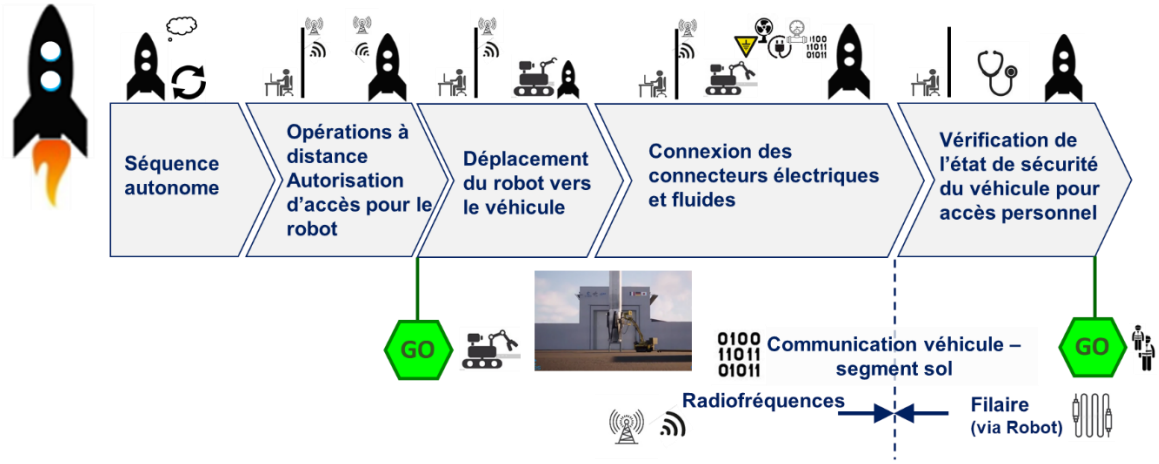

Fig. 5. Principe de remise en sécurité avec le robot

IV. FIABILITE ET SECURITE EN VOL

A. *Fiabilité*

1) *Généralités*

Comme mentionné précédemment, aucun critère quantitatif de fiabilité n'est spécifié. Les contraintes d'encombrement-masse et financiers de ce type de véhicule ne permettent pas de redonder les chaines fonctionnelles (à différencier des chaines sécuritaires pour le vol qui sont détaillées au paragraphe IV.B.3). Une panne simple sur une des chaines fonctionnelles (poussée moteur, guidage-navigation-contrôle, alimentation électrique) entraîne dans la quasi-totalité des cas une perte du véhicule.

Pour donner un niveau de confiance suffisant pour permettre l'autorisation de partir en vol, trois approches sont mises en place :

- Une analyse de robustesse pour permettre de vérifier la tolérance à certains cas de pannes. Par exemple, le véhicule dispose d'un moyen de pilotage-contrôle d'attitude utilisé pour tout ou partie au cours du vol par actionnement d'un jeu de tuyères actionnées en fonction du mouvement à contrer ou générer en tangage, lacet ou roulis.. Le véhicule disposant de 8 tuyères, ces analyses de robustesse permettront d'évaluer la tolérance à la perte d'une ou plusieurs tuyères sur la bonne poursuite de la phase vol en cours ou suivante. Les cas de panne à analyser ont été déterminés grâce à l'analyse de risque en vol. L'analyse de robustesse sera effectuée via l'exploitation du simulateur de vol,
- Le test des différentes fonctions de manière incrémentale et avec des conditions d'environnement de plus en plus exigeantes avec des essais au sol qui permettent de dérisquer les phases de vol (par exemple l'extension des pieds ou les tirs à feu) et l'ouverture incrémentale du domaine de vol (altitude et vitesse – voir Fig. 2 plus haut). Ainsi, les fonctions critiques seront d'abord testées dans des conditions où les risques sont limitées pour le véhicule, avant d'être utilisées opérationnellement,
- L'aptitude au vol qui consiste à fournir une synthèse des risques résiduels de perte de la mission sur la base des aléas rencontrés tout au long du développement du véhicule (conception, fabrication, essais au sol). La perte de la mission se définit comme le scénario où au moins un endommagement du segment sol et/ou du véhicule conduit à la perte d'une majorité des paramètres mesurés en vol et/ou à des réparations des sous-ensembles Véhicule ou du Segment sol, dépassant au final la capacité du projet en termes de planning et/ou de coût.

2) Focus sur l'aptitude au vol

Le processus d'aptitude au vol est un processus historiquement appliqué depuis les premières missions spatiales (cf. [6]). Pour une mission spatiale, il a pour but d'aboutir à l'autorisation d'engager les dernières opérations conduisant au décollage du lanceur avec sa charge utile. La figure ci-après décrit ce processus adapté pour le projet CALLISTO en précisant les acteurs, les points clés (flèches) ainsi que les documents successivement associés.

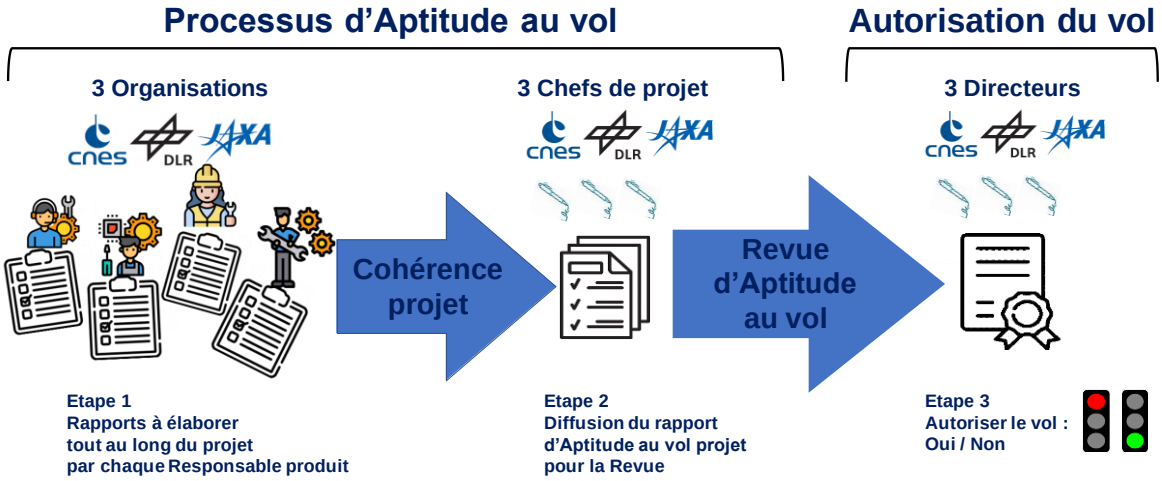

Fig. 6. Processus d'aptitude au vol

L'objet de ce processus est de fournir en entrée de la Revue d'Aptitude au Vol un rapport permettant d'évaluer les risques résiduels sur le véhicule à l'issue des activités menées depuis le début du projet. Ce rapport est une synthèse de l'ensemble des écarts majeurs rencontrés durant les phases, de définition et de vérification des exigences du véhicule, de fabrication et d'intégration des éléments, de préparation des campagnes d'essais et de vol et de mise en œuvre finale avant vol.

Ainsi, le non-respect des référentiels applicables pour ces phases du projet génère des écarts formellement couverts par des anomalies et des dérogations. Celles-ci sont traitées selon le processus et les dispositions du plan Qualité du projet pour en évaluer les risques résiduels i.e. constat, analyse, action corrective éventuelle, impact résiduel sur le vol et acceptabilité. Sur ces bases, chaque responsable de produit du véhicule, ou de produit du segment sol directement interfacé avec le véhicule, établit son rapport de synthèse des écarts avec ses justifications d'acceptabilité (cf. Fig.5). La compilation de ces bilans individuels, dont la cohérence est analysée et validée au niveau du système véhicule, sera la base du rapport d'aptitude au vol proposé pour revue et autorisation de vol.

En synthèse, un processus d'aptitude au vol classique est appliqué sur le projet de démonstrateur CALLISTO ; cependant, compte tenu de l'implication de 3 agences avec des responsabilités croisées et multiples pour la fourniture des produits du véhicule et du segment sol, il a été jugé nécessaire d'émettre un plan d'aptitude au vol dédié pour préciser les étapes du processus et garantir une homogénéité de traitement par toutes les parties prenantes. Comme pour toute mission spatiale, il s'appuie majoritairement sur les processus d'Assurance Qualité et de Sûreté de Fonctionnement permettant d'identifier tout écart au référentiel et d'en évaluer son impact sur la réussite du vol.

B. Sécurité des personnes et des biens

1) Généralités

La réglementation fixe des objectifs de sécurité à atteindre pour les risques catastrophiques lors des lancements : la probabilité de faire au moins une victime au sol doit être inférieure à 2.10^{-5}. Ce risque global est ensuite décliné sur CALLISTO (voir Fig. 7) et les différents contributeurs participant à cet évènement redouté :

- Défaillance du système de neutralisation, détaillée au §IV.B.3),
- Défaillance du véhicule détaillée au §IV.B.2).

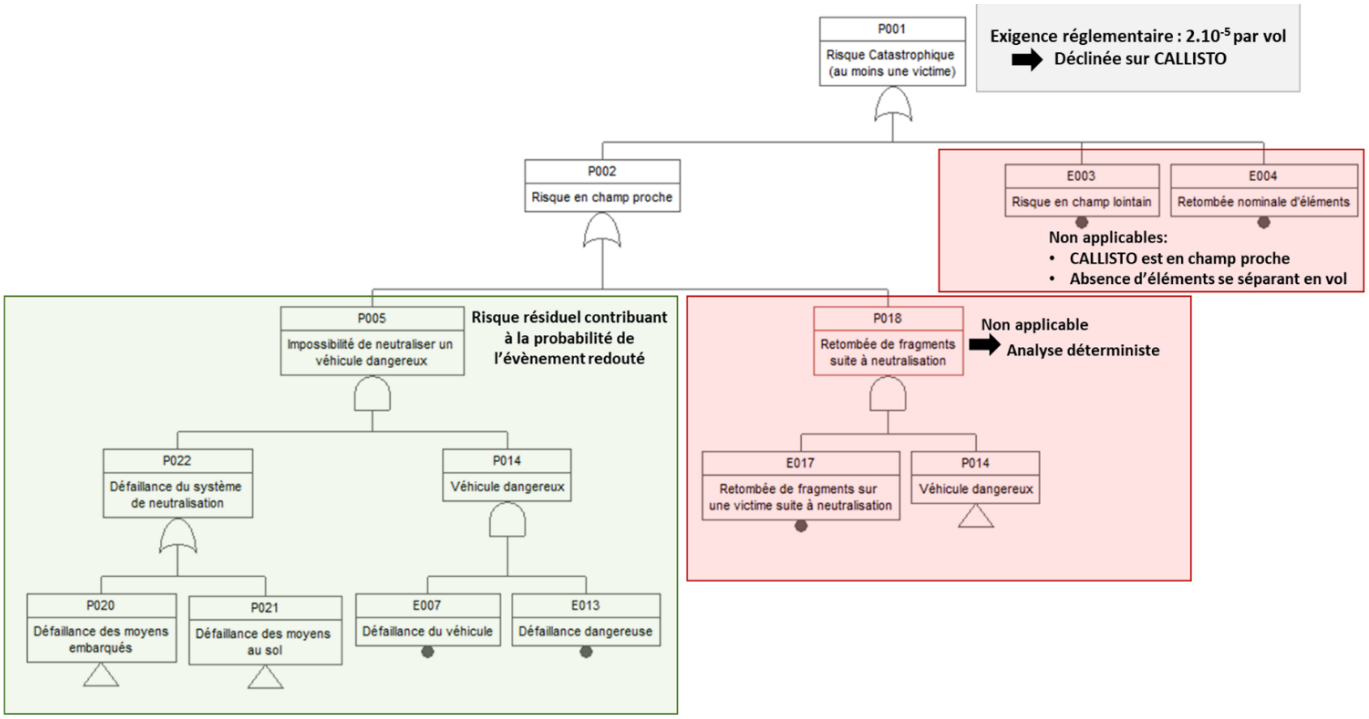

Fig. 7. Allocations de sécurité pour CALLISTO

La retombée de fragments suite à une neutralisation du véhicule est analysée de manière déterministe. La méthode appliquée à CALLISTO est expliquée dans [7].

2) Fiabilité du véhicule au profil de la sécurité

Malgré l'absence de niveau de fiabilité déposé pour CALLISTO ou d'exigence de fiabilité, il a été néanmoins nécessaire de définir un niveau de fiabilité du véhicule pour en dériver une allocation pour le système de neutralisation lui-même.

Dans les phases préliminaires du projet, une approché dérivée de la FAA (Federal Aviation Agency) [8] et basée sur une loi binomiale a été appliquée. Les hypothèses principales étant qu'un seul véhicule est utilisé (et donc ne rencontre que des succès). Chaque classe de vol étant différente, les niveaux inférieurs de fiabilité sont à considérer (intervalle de confiance à 60%).

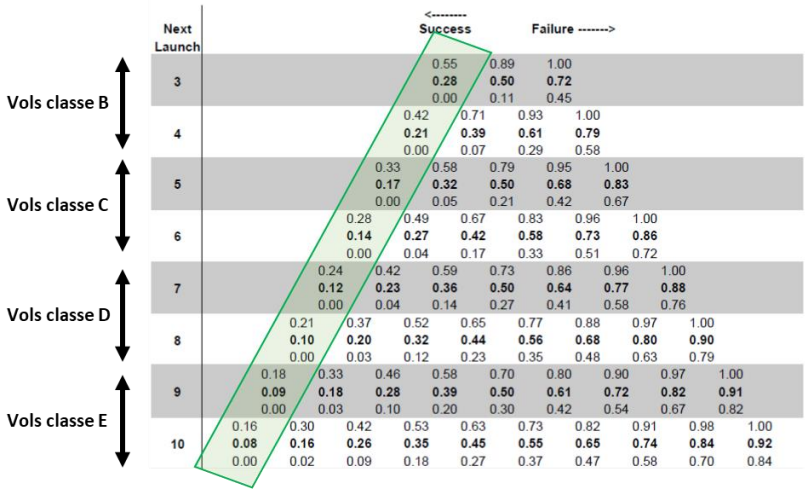

Fig. 8. Méthode d'évaluation de la fiabilité issue de la FAA

En 2023, la méthode définie dans le papier en référence [5] a été utilisée pour évaluer un niveau de fiabilité empirique pour CALLISTO. L'objectif était de vérifier que le niveau de fiabilité alloué au système de neutralisation restait cohérent de la fiabilité du lanceur avec cette nouvelle méthode. La méthode de calcul de la fiabilité empirique prend en considération l'historique des échecs et des réussites des systèmes comparables au système de transport spatial étudié (ici CALLISTO). A partir du retour d'expérience de projets similaires, un échantillon de véhicules suborbitaux réutilisables a été constitué. Cet échantillon est différent selon le type de vol : vols à basse et moyenne énergie (Grasshopper, Nebula 1, *etc.*) ou vols à haute énergie (Starship, *etc.*). Bien que le retour d'expérience était limité pour l'application à CALLISTO (absences de démonstrateur avec le même système propulsif, peu de vols à haute énergie, absence de démonstrateurs ayant fait une campagne entière, *etc.*), la méthode a été adaptée pour déterminer une fiabilité empirique de notre démonstrateur. Ce niveau de fiabilité est bien inférieur à la fiabilité calculée avec la méthode décrite en Fig. 8 mais n'a pas dénoncé l'allocation de fiabilité du système de neutralisation.

3) Fiabilité du système de neutralisation

Pour répondre à une exigence du REI, le système de neutralisation CALLISTO est le seul système pour lequel un niveau de fiabilité quantitatif doit être évalué/démontré. Ce système de neutralisation s'appuie sur deux contributeurs, un système embarqué et un système au sol (Segment Sol).

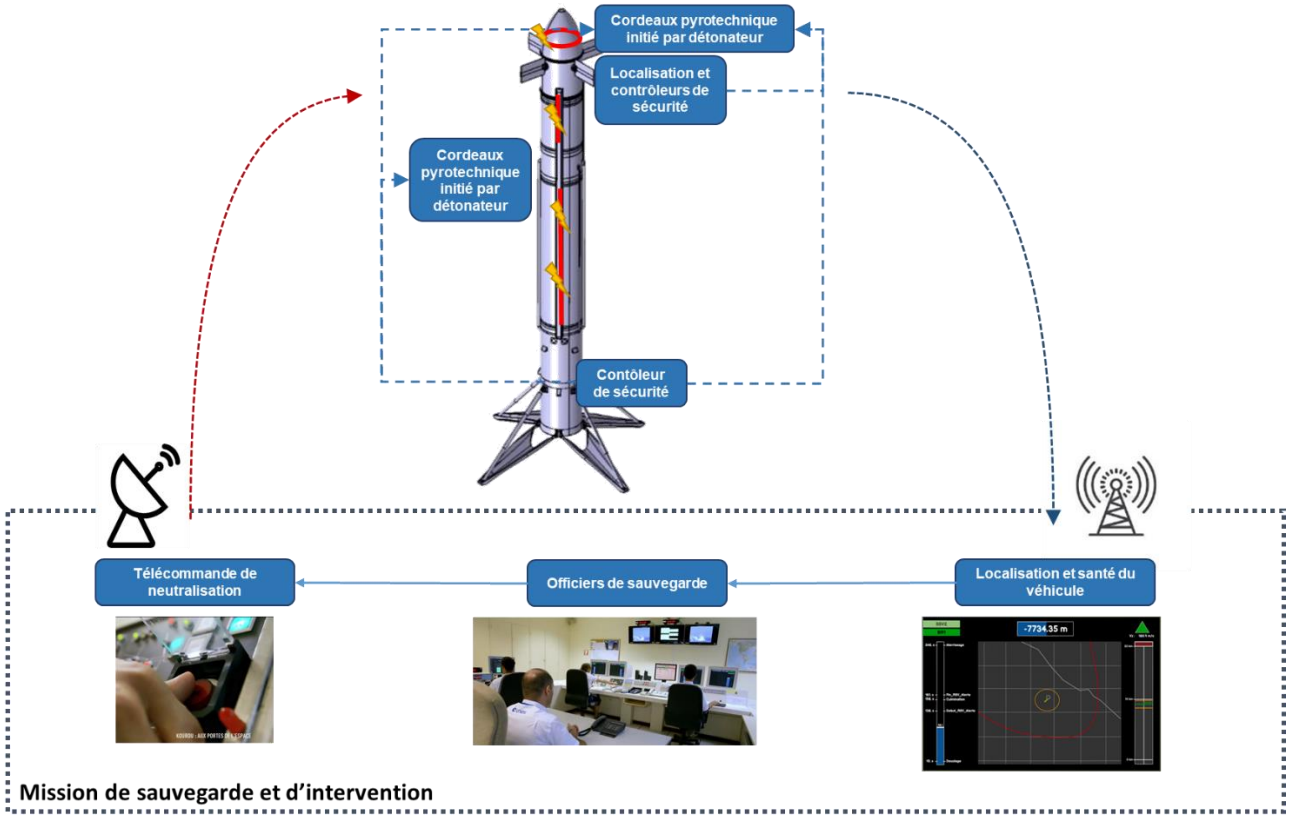

Fig. 9. Architecture du système de neutralisation

CALLISTO s'appuiera sur des moyens du CSG utilisés pour effectuer la sauvegarde en vol d'autres systèmes de lancement. Par conséquent, les radars de localisation, les stations de télémétrie, la télécommande de neutralisation et la salle sauvegarde seront réutilisées. Quelques adaptations limitées seront faites pour opérer CALLISTO (par exemple l'IHM utilisée pour l'aide à la décision des responsables sauvegarde vol, cf. [7] et [9]). La logique opérationnelle, c'est-à-dire les critères de neutralisation, influence quant à elle la fiabilité et la sécurité du véhicule : elle permet de privilégier soit une neutralisation à tort, soit une non neutralisation d'un véhicule dangereux.

En revanche, le système de neutralisation embarqué sur le véhicule, lui, est à définir et développer en respectant les exigences du REI : (i) ségrégation des éléments fonctionnels et sécuritaires et (ii) deux chaines indépendantes pour permettre la neutralisation. Des choix de conception ont été pris au vu des spécificités de CALLISTO :

- le système de localisation adaptable au fil de l'ouverture de l'enveloppe de vol. Une localisation qui s'appuie sur des radars pour les premiers vols jusqu'à une localisation basée sur des systèmes GNSS,
- Utilisation de COTS (Commercial Off-The-Shelf) pour permettre la miniaturisation des antennes,
- Le développement de contrôleurs de sécurité permettant la communication avec le système de localisation sol et réception de télécommande ainsi que l'intégration de critères autonomes de neutralisation,
- Un système de communication entièrement numérique.

Le projet CALLISTO est responsable du système de neutralisation embarqué et par conséquent de sa fiabilité. Celle-ci est calculée en utilisant le guide FIDES [10] ou la MIL-HDBK-217F [11], pour les systèmes électriques et le guide du GTPS n°11F pour les systèmes pyrotechniques [12].

V. Limitations et perspectives

Ce papier a permis de faire un bilan synthétique de comment est prise en compte la fiabilité, avec des exemples. Le choix de suppression de fiabilité en 2021 entraine des conséquences notamment au stade RCD.

A. Acceptation de non-conformités

Il est spécifié que le système doit être tolérant à la panne lors des opérations au sol. Dans le cas où ce critère n'est pas respecté (e.g., un seul robot pour réaliser des opérations critiques sur le lanceur), l'acceptation d'une non-conformité ne peut se baser simplement sur des critères quantitatifs, en comparant la fiabilité d'une panne du système non conforme à la fiabilité du véhicule par exemple. La fiabilité peut être calculée pour comparer deux solutions techniques, mais n'est pas à utiliser comme fiabilité de référence. L'accent est mis sur la qualification et la validation des systèmes avant leur utilisation (e.g. vérifications de bon fonctionnement pour les systèmes électriques, contrôles d'étanchéité pour les systèmes fluides).

B. Ouverture du domaine de vol et fiabilité

Comme expliqué précédemment, sans objectif quantitatif de fiabilité en vol, l'évaluation de la réussite mission repose sur le processus d'Assurance Qualité (en dehors des analyses de robustesse rappelées au §IV.A.1) qui recense les écarts à un référentiel, sans pouvoir garantir le niveau de fiabilité associé à ce référentiel. Ce niveau sera constaté en fin de développement avant le vol.

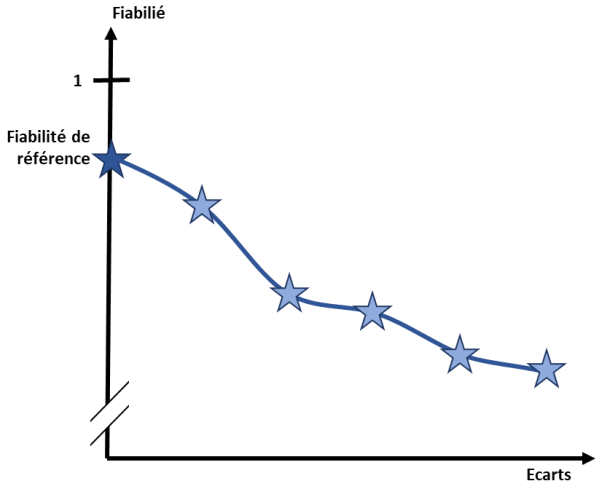

Fig. 10. Evolution de la fiabilité de CALLISTO en fonction des écarts au référentiel (pas à l'échelle)

Cette démarche est acceptée du fait d'une part qu'il s'agit d'un démonstrateur (niveau d'investissement financier limité) et d'autre part que le domaine de vol sera exploré de manière incrémentale vol après vol (cf. §IV.A.1). Cette approche permet ainsi de gagner en robustesse et fiabilité, en soumettant initialement le véhicule à des environnements peu sollicitants - vols à basse

énergie), et en corrigeant pour le vol suivant les anomalies constatées lors du vol précédent. Basée sur la méthode définie dans la référence [5] et appliquée sur CALLISTO (§IV.B.2), l'évolution attendue de la fiabilité empirique de CALLISTO est la suivante.

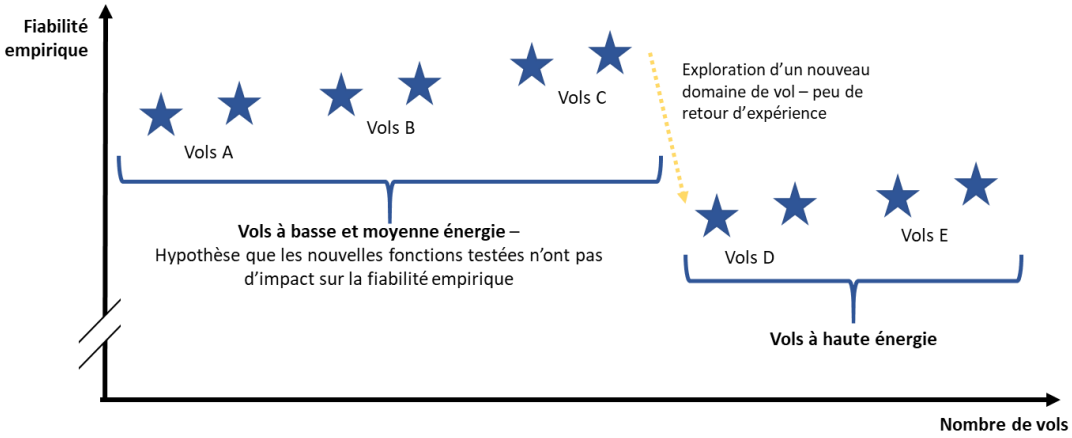

Fig. 11. Evolution de la fiabilité empirique de CALLISTO en fonction des vols (pas à l'échelle)

VI. Conclusion

Les analyses de sûreté de fonctionnement pour CALLISTO s'appuient sur des méthodes génériques et éprouvées d'analyse et d'identification des risques.

Le choix de ne pas s'appuyer sur un critère de fiabilité quantitative conduit à mettre en place une méthode pour analyser la sécurité en vol et de définir dans une phase amont du projet le processus d'aptitude au vol, qui a pour but de maîtriser la défiabilité induite par chaque aléa rencontré depuis le début du projet.

Pour ce projet, le processus d'« aptitude au vol » est rendu d'autant plus nécessaire que la maturité des produits est très inhomogène (du produit sur étagères au protoflight), qu'aucune probabilité de réussite mission n'est spécifiée et que le projet fait coopérer des équipes issues de cultures différentes. On peut ajouter que c'est l'exemplaire de vol (unique) du véhicule qui servira à la fois à des essais de vérification & validation avant vol (essais à feu statique par exemple) et les vols eux-mêmes, bien sûr

Au final, les résultats des travaux de sûreté de fonctionnement, ainsi que ceux issus des processus d'assurance qualité constituent les principales bases de la décision d'aller en vol.

References

[1] Loi sur les opérations spatiales. Loi n°2008-518. Dernière version 26 février 2022

[2] Arrêté portant réglementation de l'exploitation des installation du centre spatial guyanais. N°2010-1 du 9 décembre 2010

[3] JAXA JMR/JERG Common Technical Documentation - https://sma.jaxa.jp/en/TechDoc/index.html

[4] P. Mézard, Dr. N. Cesco, N. Praly, D. Monchaux, T. Clauzon, J. Desmariaux. CALLISTO – A safety demonstration of future reusable launcher stages from CSG. 9th European conference for aeronautics and space science (EUCASS). Juillet 2022

[5] M-L. Davezac, M. Malherbe. Méthode de calcul de la fiabilité empirique des lanceurs. Lambda Mu 24. Octobre 2024

[6] A. Biard, H. Martens, Y. Tajima, Y. Saito, C. Chavagnac, A. Mauries. CALLISTO – Flight Worthiness process : how to prepare the tripartite go to flight decision? 10th European conference for aeronautics and space science (EUCASS). Juillet 2023

[7] C. Outin, P. Mézard, C. Chavagnac, M. Kurela, F. Tinto, N. Praly, M. Zemoura. CALLISTO – A safety opportunity for new space launchers operated from CSG. International association for the advancement of space safety Conference. Mai 2023

[8] FAA Guide to Probability of Failure Analysis for New Expendable Launch Vehicles. Federal Aviation Agency. 2005

[9] S. Steere, E. Barboni, C. Martinie, D. Navarre, P. Palanque, D. Rodriguez-Hernando, F. Tinto. Operator-center & model-based design for critical HMIs: application to the new CSG operations center for reusable launchers. GBSF 2022, 6th to 8th December 2022

[10] Union Technique de l'Electricité. Méthodologie de fiabilité pour les systèmes électroniques. UTE C80-811. Edition A. Janvier 2011

[11] US Department of Defense (Janvier 1990). MIL-HDBK-217F: Reliability prediction of electronic equipment.

[12] Commission "Fiabilité" GTPS (Octobre 2012). Méthode statistique des Essais durcis. Recommandation pour obtenir et assurer la fiabilité des produits pyrotechniques en conception.