CLAUSES TECHNIQUES - ACTION « COTS DE QUALITE : LOGICIELS CRITIQUES ET TEMPS REEL »

	Date et Signature
Préparé par	Danko ILIK (DTS/QGP/SQT)
Vérifié par	Pierre Mézard (DTS/QGP/SQT)
Autorisé par	Eric Fieux (DTS/QGP)

PARIS - Les Halles
SIÈGE
2, place Maurice Quentin
75039 Paris Cedex 01
T +33 (0)1 44 76 75 00

PARIS - Daumesnil
DIRECTION DES LANCEURS
52, rue Jacques Hillairet
75612 Paris Cedex
T +33 (0)1 80 97 71 11

TOULOUSE
CENTRE SPATIAL DE TOULOUSE
18, avenue Édouard Belin
31401 Toulouse Cedex 9
T +33 (0)5 61 27 31 31

GUYANE
CENTRE SPATIAL GUYANAIS
BP 726
97387 Kourou Cedex
T +594 (0)5 94 33 51 11

RCS Paris B 775 665 912
Siret 775 665 912 000 82
Code APE 731 Z
N° identification :
TVA FR 49 775 665 912

cnes.fr

ANALYSE DOCUMENTAIRE

Classification (+ qualification pour Diffusion Limitée) : Diffusion Limitée classe 2 CNES OCamlpro
Mots clés : logiciel, sur étagère, critique, temps réel, catalogue, méthodologie de développement
Rédacteurs : Danko ILIK (DTS/QGP/SQT)
Résumé : Le présent document constitue les clauses techniques relatives à l'obtention des recommandations techniques concernant des produits logiciels disponibles sur étagère et adaptés à l'utilisation dans un contexte temps réel ou critique.
Contrat : PPAQSE 2024-03
Version en ligne : https://confluence.cnes.fr/pages/viewpage.action?pageId=360057897

HISTORIQUE DES MODIFICATIONS

Issue	Date	Reason for change
1	10 janv. 2024	Draft initial
2	5 févr. 2024	Précision des sections 4.1. Entrées et 4.2. Sorties

DIFFUSION

Name	Organisation
Emmanuel Rougeaud	CNES DTS//SE
Bruno Vella	CNES IGQ///PR
Gwenaëlle Roland-Gosselin	CNES DF/GO/STS
Julien Blond	OCamlpro SAS
Fabrice Le Fessant	OCamlpro SAS

SOMMAIRE

1. Objet du document

Le présent document constitue les clauses techniques de l'activité PPAQSE 2024-03 relatives à l'obtention des recommandations techniques concernant des produits logiciels disponibles sur étagère et adaptés à l'utilisation dans un contexte temps réel ou critique.

Cette activité est pilotée par le service sûreté de fonctionnement des systèmes de transport spatial de la Direction du Transport Spatial du CNES (DTS/QGP/SQT).

2. Documents de référence

Sans objet

3. Contexte et description des travaux à réaliser

3.1. CONTEXTE

Le CNES opère ou participe au développement d'un certain nombre de systèmes critiques du point de vue de la sûreté de fonctionnement, du temps réel ou des ambiances, tels que des installations de lancement, des systèmes de sauvegarde vol, des lanceurs, des satellites, etc.

Des composants logiciels, et en particulier des composants sur étagère (COTS), sont de plus en plus proposés pour la réalisation de ces systèmes, remplaçant souvent des composants mécaniques ou électriques.

3.2. DESCRIPTION DES TRAVAUX A REALISER

Les objectifs de cette action sont :

- D'effectuer un état des lieux et une veille des ressources logicielles sur étagère, et des méthodologies de développement et de vérification employant des outils sur l'étagère, et utilisés ou utilisables dans un contexte critique.
- Faire une comparaison entre les différents ressources/méthodologies identifiées en identifiant les les forces et les faiblesses techniques et programmatiques (coûts, délais) liées à leur utilisation.
- Faire remonter des nouvelles technologies logiciels prometteuses et en particulier celles développées par les laboratoires ou entreprises françaises.

Le livrable attendu est une étude de synthèse abordant les objectifs ci-dessus.

4. Modalités d'exécution et interfaces

4.1. ENTREES

Pour la tâche à réaliser, le CNES indique dans ce paragraphe données nécessaires en entrée, c'est-à-dire les catégories et aspects dans le périmètre de l'étude, à savoir :

- Écosystèmes COTS (développement et vérification)
  - Écosystèmes bas niveau à couvrir :
    - ✓ C
    - ✓ C++
    - ✓ Ada

- ✓ Scade
- ✓ Ocaml
- ✓ Rust

- Aspects à couvrir pour chaque écosystème (critères de comparaison entre écosystèmes) :
  - ✓ Paradigme (impérative, fonctionnelle, orienté objet, synchrone, ...) et principales caractéristiques (ex. modèles d'allocation de la mémoire/tas/pile, limitation des effets de bord, ...)
  - ✓ Possibilité de (modéliser et) vérifier de propriétés de correction fonctionnelle, en particulier l'existence de :
    - ♦ Outils d'analyse statique cohérente (*sound static analysis*) garantissant l'absence d'erreurs de runtime, de WCET, de pile, de qualité numérique, etc.
    - ♦ Langages de formalisation de haut niveau (et extraction de code compilable)
    - ♦ Mécanismes inhérentes aux langages et éliminant des classes d'erreurs par construction (ex. typage forte/algébrique)
    - ♦ Outils de génération de tests ou de fuzzing
  - ✓ Existence de compilateurs alternatifs et maintenus, des outils débugueur, de outils de métaprogrammation (ex. générateurs de parseurs, dérivation automatique)
  - ✓ Diversité de librairies natives COTS existantes et existence d'une communauté de développeurs
  - ✓ Utilisabilité de binaires produits sans/avec un système d'exploitation
  - ✓ Interfaçage avec d'autres langages/ABIs
  - ✓ Utilisation précédente dans un contexte critique, si connue

Ces données d'entrée pourront être complétées au besoin et validées lors de la réunion de démarrage de l'activité.

4.2. SORTIES

Les livrables attendus sont :

- ➢ l'étude de synthèse mentionnée dans les sections "Description des travaux à réaliser",
- ➢ une présentation synthétique des travaux et des résultats, destinée à un public technique.

La licence de droit d'auteurs applicable aux livrables sera la licence "Creative Commons Attribution 3.0 France".

4.3. LANGUES DE TRAVAIL

Français

4.4. LIEU DE TRAVAIL ET DEPLACEMENTS

L'activité est à réaliser en dehors des locaux du CNES. Des interventions sont à prévoir au CNES sur le site de Paris Daumesnil (réunions de démarrage, avancement, clôture).

4.5. DELAIS

L'activité est à achever avant T0 + 12 semaines (T0 : démarrage des travaux).

4.6. MANAGEMENT

Le Titulaire doit mettre en place et maintenir un management et un système d'administration pour répondre à toutes les obligations liées aux prestations telles que définies par le présent cahier des charges. Les coûts de management et d'administration du Titulaire pour cette prestation doivent être couverts par le Titulaire au titre de ses frais généraux.

Le Titulaire prend en charge la formation professionnelle continue de son personnel.

Le Titulaire devra respecter les dispositions légales et réglementaires en matière d'horaires et de durée du travail.

4.7. FLEXIBILITE

Le Titulaire doit s'assurer de la bonne exécution de la prestation avec le souci permanent de la satisfaction du client CNES, avec la flexibilité nécessaire pour s'adapter aux exigences opérationnelles qui pourraient évoluer au cours de la durée du contrat.

4.8. EN CAS DE PROBLEME

Le Titulaire devra signaler au représentant du CNES par écrit tout problème majeur qui pourrait affecter la bonne exécution du contrat, au regard des exigences du CNES. Dans ce cas, les parties s'engagent à se rencontrer afin de prendre les mesures palliatives.

5. Interfaces

5.1. INTERFACES ENTRE LE CNES ET LE TITULAIRE

Le représentant de la Direction du Transport Spatial habilité à traiter les problèmes découlant du présent marché avec le représentant du Titulaire, dans la limite de leurs attributions, est le chef du service DTS/QGP/SQT.

L'interface opérationnelle désignée du Titulaire pour toutes les questions techniques, y compris celles relatives à la gestion quotidienne, est le service DTS/QGP/SQT.

Le Titulaire devra nommer un gestionnaire de contrat (ou RCI – Responsable Contrat Industriel) qui assurera l'interface avec le responsable CNES. Le RCI sera l'interface pour toutes les questions liées au management, à l'administration et les questions contractuelles en lien avec le support fourni. Le Titulaire indiquera, au plus tard à la notification du contrat, le nom du RCI et les représentants sur site qui assureront la gestion technique du marché en relation avec les représentants CNES.

Par ailleurs, le RCI du Titulaire, peut être amené à rencontrer le responsable achat en charge du marché (DAR/OAR/TSR) ou bien l'officier de sécurité et les responsables de la sécurité SSI de la DTS (DTS//SE).

5.2. PRINCIPAUX INTERLOCUTEURS INTERNES ET EXTERNES

Les principaux interlocuteurs pour cette activité sont les ingénieurs CNES du service de sûreté de fonctionnement (DTS/QGP/SQT).

6. Échéancier et lotissement prévisionnel

L'échéancier suivant est indicatif :

Lot	Événement	Livrable	Date
1	1	Livrables de l'étude	T0 + 12 semaines

Les réunions suivantes sont à prévoir : démarrage (T0), point d'avancement (T0+4 semaines), point de restitution préliminaire (T0+8semaines), point de restitution final (T0+12semaines)

Les attendus de chaque réunion seront précisés lors de la réunion de démarrage.

♦♦♦♦♦ FIN DU DOCUMENT ♦♦♦♦♦