CLAUSES TECHNIQUES - ACTION PPAQSE 2025-02 - SYSTEMES D'EXPLOITATION LOGICIELS CRITIQUES ET TEMPS REEL

		Date et signature
Rédigé par	**Danko ILIK (DTS/QGP/SQT)**	Ilik Danko Signature numérique de Ilik Danko Date : 2025.02.14 09:13:59 +01'00'
Validé par	**Pierre MEZARD (DTS/QGP/SQT)**	Signature numérique de Mezard Pierre Date : 2025.02.18 12:54:16 +01'00'
Application autorisée par	**Caroline AUSSILHOU (DTS/QGP)**	Aussilhou Caroline Signature numérique de Aussilhou Caroline Date : 2025.02.18 13:27:34 +01'00'

PAGE D'ANALYSE DOCUMENTAIRE

Classification (+ qualification pour Diffusion Limitée) : **Non Sensible**		
Contrôle Export : **non** *Si votre document est soumis à contrôle export, merci de vous rapprocher de votre responsable Contrôle Export pour voir les marquages supplémentaires à apporter sur le document.*		
Mots clés :		
Rédacteurs : **Danko ILIK (DTS/QGP/SQT)**		
Résumé : Le présent document constitue les clauses techniques de l'activité PPAQSE 2025-02 relatives à l'obtention des recommandations techniques concernant des systèmes d'exploitation disponibles sur étagère et adaptés à l'utilisation dans un contexte temps réel ou critique.		
Documents rattachés : N/A		
Resp. Gest. Conf. : N/A		
Gestion en configuration :	A dater du : **Date de parution**	Par :
Contrat : **PPAQSE 2025-02**		
Nombre total de pages : 8 / Nombre de pages liminaires 4		
Version en ligne : https://confluence.cnes.fr/pages/viewpage.action?pageId=634295826		
Logiciel(s) hôte : Word MS-Office		

HISTORIQUE DES MODIFICATIONS

Edition	Date	Justification
1	03/02/2025	Version initiale + Prise en compte des remarques de DTN/STS/SEL

SOMMAIRE

1. Objet du document

Le présent document constitue les clauses techniques de l'activité PPAQSE 2025-02 relatives à l'obtention des recommandations techniques concernant des systèmes d'exploitation 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 et qualité des systèmes de transport spatial de la Direction du Transport Spatial du CNES (DTS/QGP/SQT).

2. Documents de référence

[DR1] OcamlPRO et CNES. Ecosystèmes COTS de développement et de vérification des logiciels critiques et temps réel. Référence: DLA-SF-0000000-194-QGP. Version: a4b0da4

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. Parmi ces composants, les système d'exploitation prennent une place importante.

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, concernant les systèmes d'exploitation (dans un sens large incluant les hyperviseurs*, runtimes* s'exécutant en mode *bare metal*, et unikernels), et utilisés ou utilisables dans un contexte critique.
- Faire une comparaison entre les différents ressources identifiées en identifiant 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. EXIGENCES

EXIG-1 Les **systèmes d'exploitation** à couvrir dans l'étude sont les suivantes (donnés par ordre alphabétique) :

- KVM
- Linux (pour un *patch* temps réel choisi par le prestataire)
- MirageOS
- PikeOS
- ProvenVisor
- RTEMS
- seL4
- XEN
- XtratuM

EXIG-2 Les **aspects** à couvrir pour chaque système d'exploitation, représentant aussi les critères de comparaison entre systèmes d'exploitation, dans l'étude sont les suivantes (donnés par ordre d'importance) :

1. Type de l'OS (hyperviseur type 1, type 2, OS classique, unikernel) et ses particularités
2. Architectures matérielles supportées ; support multi-coeur
3. Propriétés temps-réel et multi-tâche (caractéristiques, cout du *context switch*, gestion de la mémoire cache)
4. Mécanismes de détection ou de tolérance aux pannes disponibles (voir EXIG-3)
5. Pour les hyperviseurs, possibilité (en pratique ou en théorie) d'exécuter un language runtime en mode bare metal, pour les langages C, Ada, Ocaml et Rust (cf étude PPAQSE 2024 [DR1])
6. OS activement développé/supporté, nombre d'années en existence
7. Licences disponibles, informations (si existantes) de brevets
8. Estimation d'étendue de la couverture en pilotes (pilotes matériels, pilotes de protocoles (ex. IP, PTP, TLS), ...)
9. Poids du code propre à l'OS (SLOC, ...), hors *daemons* de service optionnels
10. Temps de démarrage (hors *daemons* de service optionnels), si connu (ordre de grandeur)

EXIG-3 Les **mécanismes de détection ou de tolérance aux pannes** à couvrir pour chaque système d'exploitation dans l'étude sont les suivantes (donnés par ordre d'importance) :

1. Partitionnement temps et/ou mémoire (caractéristiques, mécanismes de communication entre partitions)
2. Corruption de la mémoire (détection, scrubbing, pilotes mémoire ECC)
3. Perte du flux d'exécution
4. *Monitoring* et *profiling* (ex. linux perf)
5. *Watchdogs* matériels et logiciels
6. *Interrupt masking*
7. Alimentation électrique non nominale
8. Événements thermiques (ex. CPU *throttling*)

4.2. EXIGENCES MINIMALES

Dans le cadre de la présente mise en concurrence, l'offre du Candidat doit respecter des exigences minimales, telles que spécifiées ci-après :

- Le Candidat choisira au moins 6 systèmes d'exploitation à couvrir, parmi ceux donnés dans EXIG-1, ou parmi d'autres systèmes existants quand ils sont activement maintenus et disponibles sur l'étagère (COTS)
- Le Candidat traitera au moins les 7 premiers aspects de l'EXIG-2, avec la possibilité de modifier/préciser leur stipulations, et pourra proposer des aspects supplémentaire, non nécessairement parties de l'EXIG-2, qu'il estime pertinents à l'objet de l'étude
- Le Candidat traitera au moins les 4 premiers aspects de l'EXIG-3, avec la possibilité de modifier/préciser leur stipulations, et pourra proposer des mécanismes supplémentaires, non nécessairement partie de l'EXIG-3, qu'il estime pertinents à l'objet de l'étude

4.3. SORTIES

Les livrables attendus sont :

- l'étude de synthèse mentionnée dans la section "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".

4.4. LANGUES DE TRAVAIL

Français

4.5. 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).

4.6. DELAIS

L'activité est à achever avant T0 + 20 semaines (T0 : démarrage des travaux).

4.7. 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.

4.8. 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.

4.9. 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 et qualité des systèmes de transport spatial (DTS/QGP/SQT).

6. Échéancier et lotissement prévisionnel

L'échéancier suivant est indicatif :

Lot	Événement	Livrable	Date
1	1	Livrables de l'étude	T0 + 20 semaines

Les réunions suivantes sont à prévoir : démarrage (T0), point d'avancement (T0+4 semaines), point d'avancement (T0+12 semaines), point de restitution préliminaire (T0+16 semaines), point de restitution final (T0+20semaines)

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

♦♦♦♦♦ FIN DU DOCUMENT ♦♦♦♦♦