

Sécuriser l'espace :

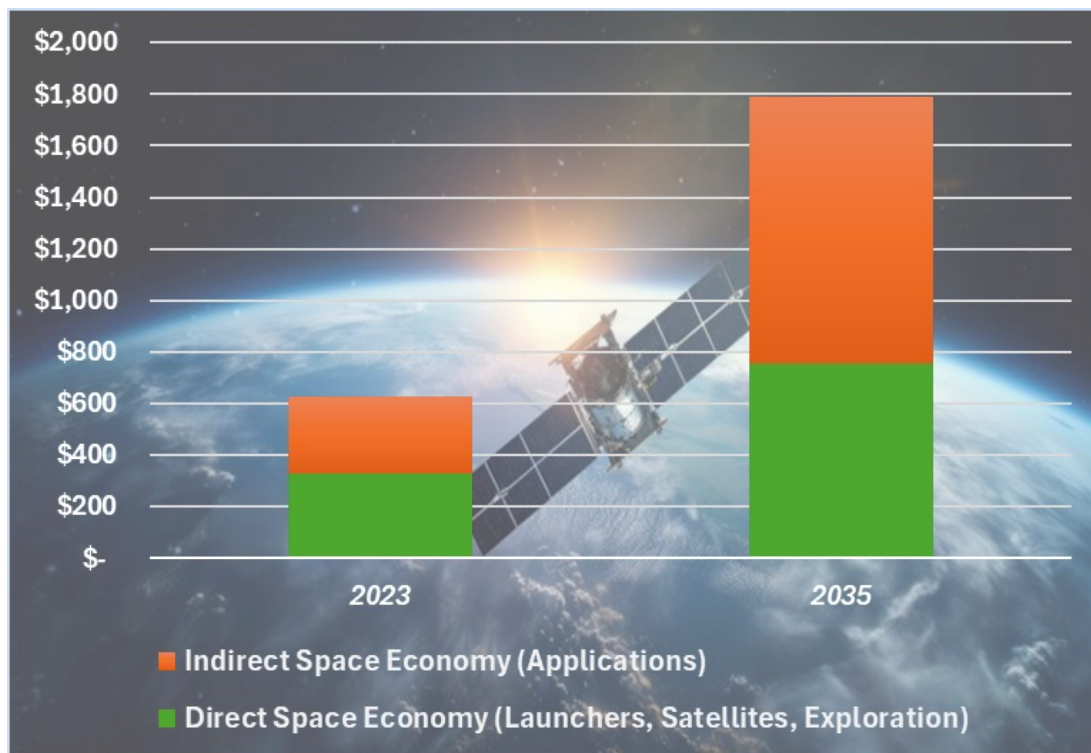
La prochaine frontière pour les infrastructures critiques

Par Scott Wakelin - Senior Product Manager pour l'unité commerciale des communications de Microchip

Aujourd'hui et à l'avenir, les systèmes spatiaux jouent un rôle de plus en plus important dans nos vies. Ils nous aident à nous orienter, nous informent sur la météo et nous connectent les uns aux autres. De plus, ils constituent une partie essentielle de notre infrastructure de sécurité nationale.

L'ampleur et l'étendue de l'économie spatiale mondiale témoignent de son importance. Le Forum économique mondial prévoit que les investissements directs dans les infrastructures spatiales (satellites, lanceurs, rovers, exploration) passeront de **330 milliards de dollars en 2023 à 755 milliards de dollars en 2035**. Sur la même période, l'économie indirecte dérivée de l'espace passera de **300 milliards à plus de 1 000 milliards de dollars**. L'espace est désormais profondément ancré dans le tissu de notre quotidien.

Figure 1 Global Space Economy (\$B)



Source: Space: The \$1.8 Trillion Opportunity for Global Economic Growth, World Economic Forum

Figure 1 : Économie spatiale mondiale (\$B)

Source : "Space: Les 1800 Milliards d'opportunités pour une Croissance Economique Globale

Malgré cela, l'accent a peu été mis sur la nécessité de sécuriser l'espace. Les méthodes de cyber sécurité couramment utilisées pour les applications terrestres sont rares dans l'espace. Au lieu de cela, la sécurité des systèmes spatiaux – qu'il s'agisse de satellites, de lanceurs ou de rovers/at-terrisseurs – repose souvent sur une combinaison d'obscurité et d'éloignement physique. Comme la cybersécurité ne figure pas en tête des exigences, peu de sous-systèmes électroniques et de microprocesseurs utilisés dans l'espace intègrent des fonctionnalités de sécurité.



Figure 2 : Applications spatiales

Pourtant, le risque s'accroît. La combinaison de l'augmentation des enjeux de sécurité nationale, des tensions géopolitiques croissantes et de la dépendance accrue à l'espace crée à la fois des risques et des incitations à des activités malveillantes. De plus, l'émergence de logiciels de vol open source expose des failles de sécurité pouvant être exploitées par des hackers de tous niveaux, allant des opérateurs amateurs de stations au sol aux acteurs étatiques.

Face à ces risques croissants, la volonté et la nécessité de réagir s'intensifient. L'espace est désormais considéré comme une composante essentielle des infrastructures critiques d'un pays. Les administrations américaines successives ont reconnu à la fois l'intérêt national vital des activités spatiales et la nécessité de protéger cette infrastructure. En 2021, le **United States Space Priorities Framework** a souligné :

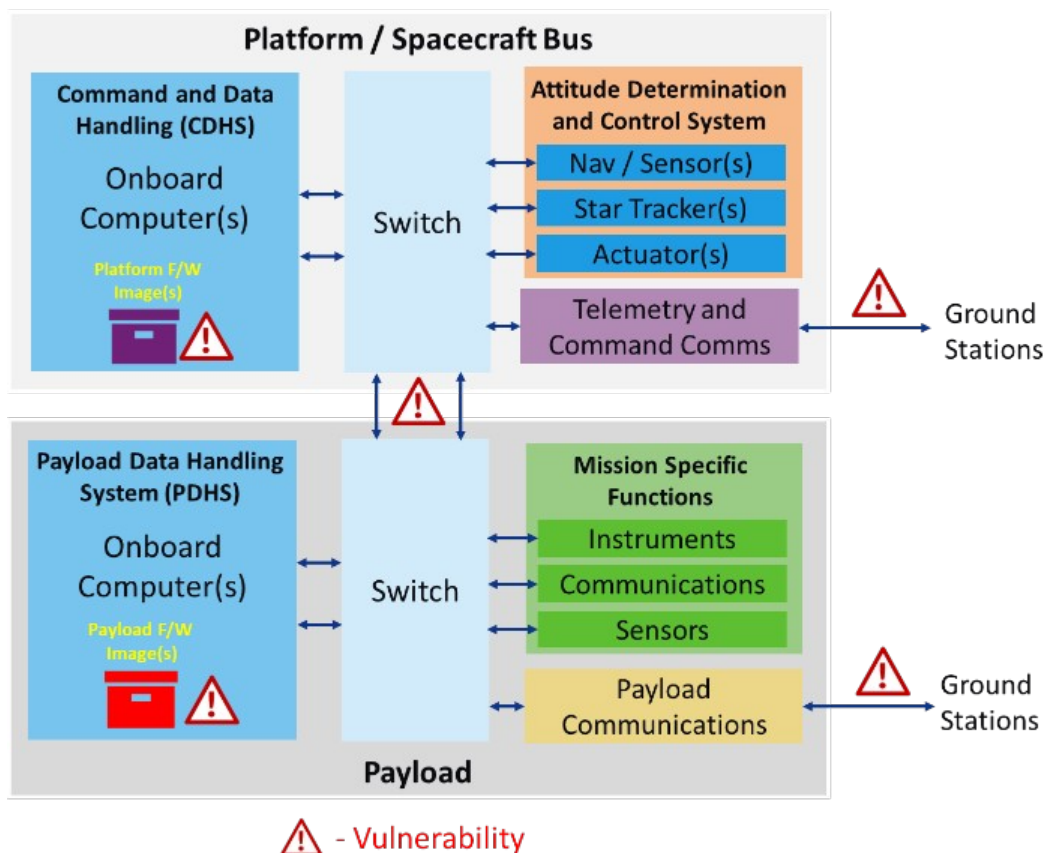
Les satellites sont l'une des nombreuses applications de sécurité dans l'infrastructure spatiale.

Les satellites sont utilisés pour une large gamme d'applications militaires, civiles et commerciales. Avec **plus de 20 000 nouveaux satellites prévus d'ici la fin de la décennie**, les opportunités d'activités malveillantes et le besoin de protection n'ont jamais été aussi élevés.

Un satellite typique comprend une plateforme ou un bus spatial ainsi qu'une section de charge utile. Ces différentes sections remplissent des fonctions distinctes, ce qui signifie que la surface d'attaque et l'impact d'une faille de sécurité varient. La **plateforme** ou **bus spatial** est responsable du vol et de la navigation du satellite. Au cœur de cette section se trouve le **microprocesseur (MPU)** utilisé dans les **ordinateurs de bord (OBC)** du **système de commande et de gestion des données (CDHS)**.

Le **CDHS** exécute les logiciels de vol en temps réel et en réponse aux données des capteurs et de navigation reçues du **système de détermination et de contrôle d'attitude (ADCS)**. Simultanément, le CDHS échange des **télémetries et des commandes avec les stations au sol via le système de télécommande et de communication**. Une faille de sécurité dans cette section pourrait entraîner **la perte totale du satellite** ou, dans le pire des cas, provoquer une **réaction en chaîne destructrice connue sous le nom de syndrome de Kessler**.

Figure 2 Example Architecture for a Satellite



D'un autre côté, la section **Charge utile** est responsable de la mission spécifique du satellite. Parmi les missions possibles, on trouve l'**observation de la Terre**, la **défense nationale**, la **recherche scientifique**, les **communications haut débit** et la **navigation et synchronisation temporelle** (comme le GPS).

Tout comme la section **Plateforme**, la section **Charge utile** intègre un ensemble d'ordinateurs de bord au sein du **système de gestion des données de charge utile (PDHS)**, qui interagit avec les fonctions spécifiques à la mission, telles que les instruments, les communications et les capteurs. Les **stations terrestres** communiquent avec cette section via le **système de communication de la charge utile**.

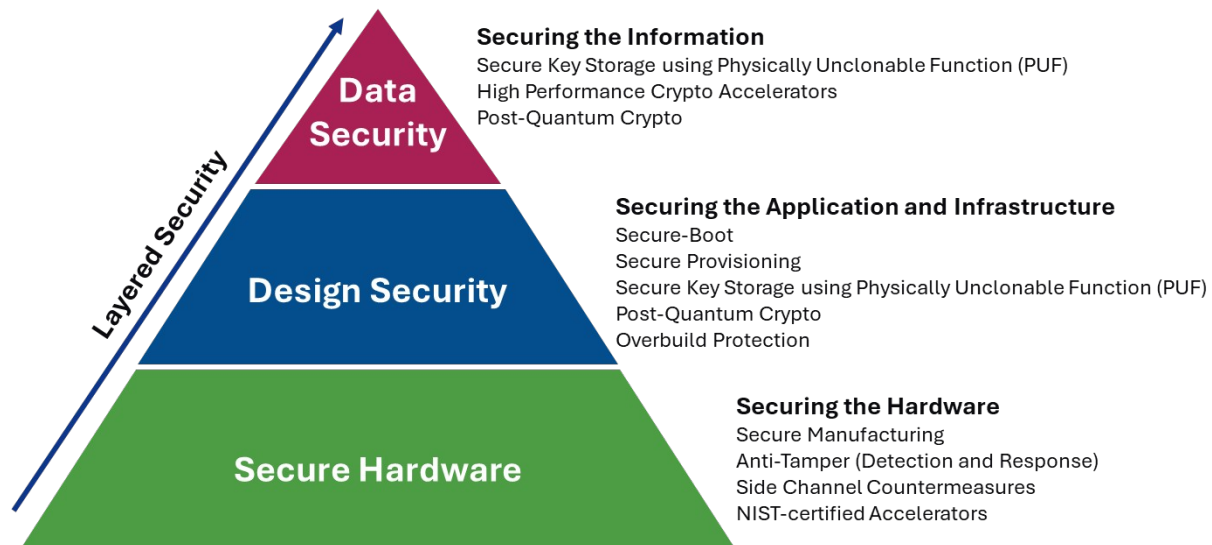
Bien que les failles de sécurité dans cette section ne conduisent pas nécessairement à la perte du satellite, elles pourraient exposer des **informations sensibles de sécurité nationale**, rendre les **systèmes GPS inopérants** ou **perturber les communications haut débit**.

Compte tenu de leur rôle central dans une application spatiale, les **microprocesseurs** utilisés sont essentiels non seulement pour remplir les objectifs de mission, mais aussi pour assurer la **sécurité du système**. Ils doivent intégrer des fonctionnalités telles que des **performances de calcul élevées**, des **interfaces adaptées**, ainsi qu'une **tolérance et une prévention des pannes** pour répondre aux exigences de la mission. De plus, une **protection contre les radiations** est indis-

pensable pour résister à l'environnement spatial extrême, en particulier pour les applications critiques ou les vols habités, qu'ils se déroulent en **orbite terrestre basse (LEO)**, sur la **Lune** ou au-delà.

Les développeurs de systèmes spatiaux doivent désormais prendre en compte la **sécurité**. Une application spatiale véritablement sécurisée s'appuiera sur des **microprocesseurs de qualité spatiale**, suivant une **approche en couches** pour garantir la protection du système.

Figure 3 Approche de la sécurité par tranche



À la couche la plus basse se trouve le **matériel sécurisé**. Si le **matériel** et sa **chaîne d'approvisionnement** ne sont pas sécurisés, ni l'infrastructure ni les informations qui y transitent ne peuvent être considérées comme fiables. La sécurisation du matériel repose sur des techniques telles que la **fabrication sécurisée**, la **détection et la réponse aux tentatives de falsification**, l'**intégration de contre-mesures contre les attaques par canaux auxiliaires**, et bien sûr, l'utilisation d'**accélérateurs certifiés par le NIST**.

Vient ensuite la **sécurité de conception**. À ce niveau, l'**infrastructure** et la **propriété intellectuelle** sur lesquelles repose l'application spatiale sont sécurisées. Parmi les fonctionnalités clés des microprocesseurs à cette couche, on retrouve le **démarrage sécurisé (secure-boot)**, l'**approvisionnement sécurisé (secure-provisioning)** et le **stockage sécurisé des clés cryptographiques**.

Enfin, une fois que le matériel et l'infrastructure sont sécurisés, l'attention peut se porter sur la **sécurisation des informations transitant dans le système**. À cette couche, les microprocesseurs de qualité spatiale doivent intégrer des **accélérateurs cryptographiques haute performance** ainsi qu'un **stockage sécurisé des clés**.

Une capacité clé mentionnée dans la **Figure 2**, qui ne doit pas être négligée – en particulier pour les infrastructures critiques comme l’espace – est le **besoin urgent et croissant de la cryptographie post-quantique**.



La **cryptographie asymétrique** est un **pilier fondamental** de tout système de sécurité. Dans presque toutes les applications terrestres, des **algorithmes** tels que **RSA** et **Elliptic Curve Cryptography (ECC)** sont largement utilisés pour les **signatures numériques** et les **échanges de clés**. Étant donné la **taille traditionnelle des clés** et les défis **mathématiques et computationnels** liés au **factoring des nombres premiers**, on estime généralement que les **ordinateurs classiques** mettraient **des milliards d’années** à casser les algorithmes **RSA ou ECC**.

Cependant, **les ordinateurs quantiques se profilent à l’horizon**. Il est possible, voire probable, que dans les **5 à 10 prochaines années**, des **ordinateurs quantiques suffisamment puissants** (avec un nombre de **qubits** suffisant) deviennent accessibles aux **États et autres groupes disposant de ressources financières importantes**.

Le **danger** que représentent ces ordinateurs quantiques réside dans leur capacité à exécuter **l’algorithme de Shor**, qui permet de **factoriser un nombre premier**. Cet algorithme, exécuté sur un **ordinateur quantique**, pourrait réduire le temps nécessaire pour **casser RSA ou ECC** de **milliards d’années à moins d’une journée**.

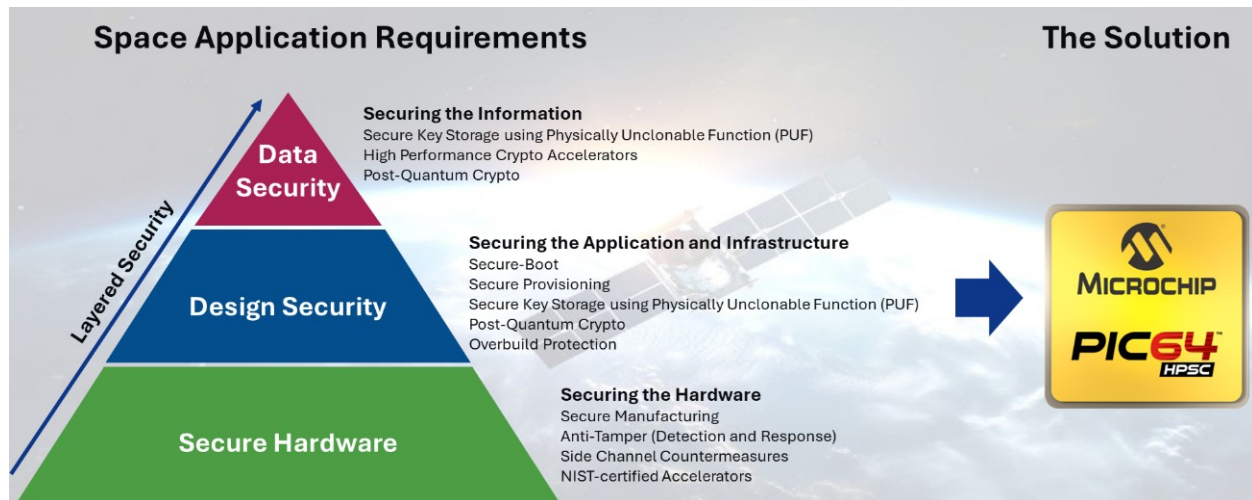
Étant donné l’utilisation massive de **RSA** et **ECC (ECDSA ou ECDH)** dans de nombreuses **applications de sécurité** (authentification, échange de clés, etc.), leur vulnérabilité constitue une **menace existentielle** pour les systèmes du monde entier.

De plus, le problème ne concerne pas seulement les **communications en temps réel**. Des **agents malveillants** pourraient **intercepter et stocker** des communications **aujourd’hui** afin de les **décrypter demain** grâce à des **ordinateurs quantiques**. Cette menace concerne aussi bien les **constellations en orbite basse (LEO) dédiées aux communications haut débit** que les **actifs militaires stratégiques**.

Le **National Institute of Standards and Technology (NIST)** et la **National Security Agency (NSA)** ont reconnu cette menace et ont lancé une **compétition** pour identifier les **algorithmes cryptographiques de nouvelle génération résistants aux attaques quantiques**. À l’issue de cette compétition, le **NIST** a sélectionné un ensemble d’**algorithmes basés sur les réseaux euclidiens modulaires** pour remplacer progressivement **RSA et ECC** :

- **ML-KEM – Méthode d’encapsulation de clé basée sur les réseaux euclidiens modulaires (FIPS-203)**
- **ML-DSA – Standard de signature numérique basé sur les réseaux euclidiens modulaires (FIPS-204)**

Les algorithmes **ML-KEM** et **ML-DSA** sont des **éléments fondamentaux** pour garantir la **sécurité et la pérennité** de nos **systèmes cyber-physiques** à long terme.



La famille de microprocesseurs **PIC64-HPSC** de **Microchip** représente une avancée révolutionnaire en matière de capacités offertes par un **microprocesseur 64 bits** – aussi bien sur Terre que pour les applications spatiales.

Ce dispositif associe les **meilleures fonctionnalités** des **processeurs commerciaux standards (COTS)**, telles que le **calcul haute performance**, la **virtualisation** et l'**intelligence artificielle (IA)**, avec la **tolérance aux pannes** et le **durcissement aux radiations** indispensables pour survivre dans l'environnement spatial exigeant.

Les **MPUs PIC64-HPSC** combinent une **puissance de calcul élevée** avec un **ensemble complet de fonctionnalités de sécurité**, y compris une **prise en charge complète de la cryptographie post-quantique** – une capacité essentielle pour sécuriser l'espace, aujourd'hui et à l'avenir.

Grâce aux **MPUs PIC64-HPSC**, les applications spatiales telles que **les satellites, les lanceurs et les rovers/atterrisseurs** peuvent être sécurisées conformément à leur rôle de **composantes clés des infrastructures critiques nationales**.