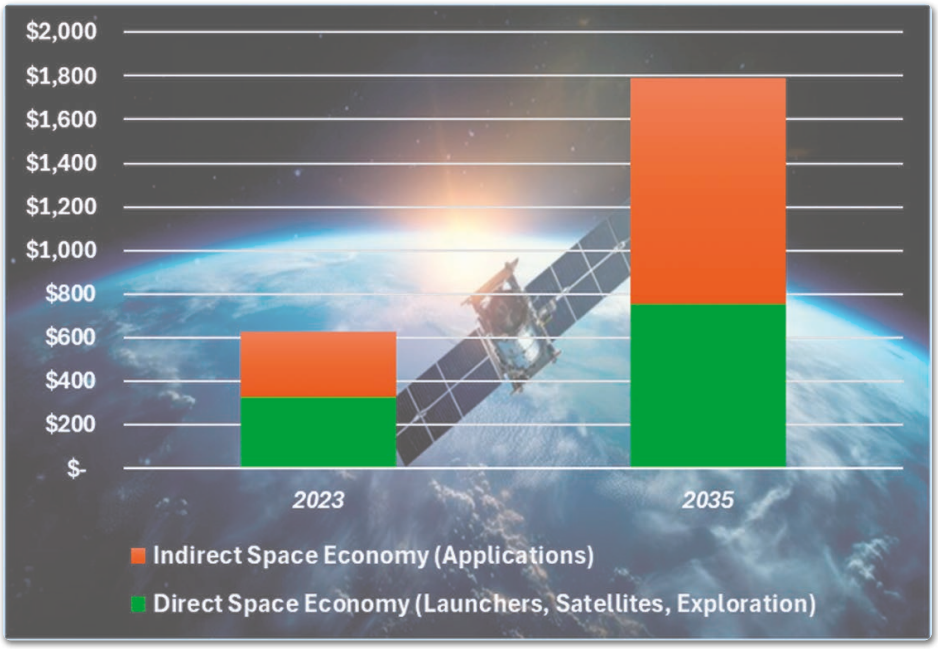
Sicherheit im Weltraum

Die nächste Herausforderung für kritische Infrastrukturen



Globale Weltraumwirtschaft
(in Mrd. US-$, Quelle: „Space: The $1.8 Trillion Opportunity for Global Economic Growth")

Weltraumsysteme spielen heute und in Zukunft eine immer wichtigere Rolle. Sie helfen uns, von Ort zu Ort zu gelangen, informieren uns über das Wetter und verbinden uns miteinander. Darüber hinaus sind sie ein zunehmend wichtiger Bestandteil unserer nationalen Sicherheitsinfrastruktur.

Größe und Umfang

der globalen Weltraumwirtschaft lassen ihre Bedeutung erahnen. Das Weltwirtschaftsforum prognostiziert, dass die Direktinvestitionen in die Weltrauminfrastruktur (Satelliten, Trägerraketen, Rover, Erkundung) von 330 Mrd. US-$ im Jahr 2023 auf 755 Mrd. US-$ im Jahr 2035 steigen werden. Im gleichen Zeitraum wird die indirekte Wirtschaft, die sich aus dem Weltraum ableitet, von 300 Mrd. US-$ auf über 1 Billion US-$ wachsen. Der Weltraum ist mittlerweile tief in unser Leben eingebunden.

Dennoch wurde der Notwendigkeit von Sicherheit im Weltraum bislang wenig Beachtung geschenkt. Cybersicherheitsmaßnahmen, die bei erdgebundenen Anwendungen üblich sind, sind im Weltraum selten. Stattdessen beruht die Sicherheit von Weltraumsystemen – seien es Satelliten, Trägerraketen oder Rover/Lander – oft auf einer Kombination aus Unauffälligkeit und großer Entfernung. Da Cybersicherheit auf der Anforderungsliste keine hohe Priorität hat, verfügen nur wenige der im Weltraum eingesetzten elektronischen Subsysteme und Mikroprozessoren über integrierte Sicherheitsfunktionen.

Doch die Risiken nehmen zu:

Die Kombination aus stetig wachsenden nationalen Sicherheitsinteressen, zunehmenden geopolitischen Spannungen und einer steigenden Abhängigkeit vom Weltraum schafft Risiken und Anreize für böswillige Aktivitäten. Die Weiterentwicklung von Open-Source-Flugsoftware bietet dabei Möglichkeiten, Sicherheitslücken zu identifizieren, die von Hackern unterschiedlichster Couleur – von Hobby-Bodenstationsbetreibern bis hin zu staatlichen Akteuren – ausgenutzt werden.

Angesichts des wachsenden Risikos steigt auch der Wille und die Notwendigkeit zu reagieren. Der Weltraum gilt heute als integraler Bestandteil der kritischen Infrastruktur eines Landes. Aufeinanderfolgende US-Regierungen haben sowohl das vitale nationale Interesse an Weltraumaktivitäten als auch die Notwendigkeit, diese Infrastruktur zu schützen, anerkannt. Im Jahr 2021 wurde im „United States Space Priorities Framework" festgestellt:

Die Vereinigten Staaten werden die Sicherheit und Widerstandsfähigkeit von Weltraumsystemen, die kritische Infrastrukturen der USA bereitstellen oder unterstützen, vor böswilligen Angriffen und Naturgefahren schützen. Insbesondere werden die Vereinigten Staaten mit der kommerziellen Raumfahrtindustrie sowie anderen nichtstaatlichen Entwicklern und Betreibern von Raumfahrtsystemen zusammenarbeiten, um die Cybersicherheit dieser Systeme zu verbessern, einen effizienten Zugang zu Frequenzen zu gewährleisten und die Widerstandsfähigkeit der Lieferketten innerhalb der gesamten nationalen Raumfahrtindustrie zu stärken.

Satelliten

sind nur eine von vielen Anwendungen für die Sicherheit der Weltrauminfrastruktur. Sie werden für ein breites Spektrum an Verteidigungs-, zivilen und kommerziellen Anwendungen eingesetzt. Da bis zum Ende dieses Jahrzehnts über 20.000 neuen Satelliten in die Umlaufbahn gebracht werden sollen, sind die Möglichkeiten für böswillige Aktivitäten und der Bedarf an Schutzmaßnahmen noch nie so groß.

Ein Satellit umfasst eine Plattform (Raumfahrzeug) und einen Nutzlastbereich.

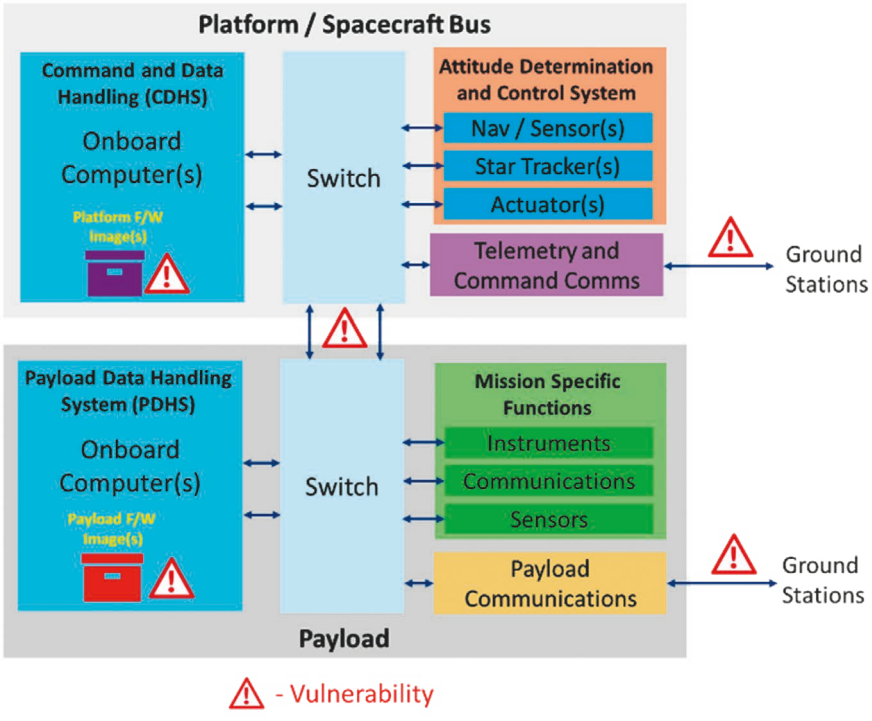
Autor:
Scott Wakelin
Senior Product Manager
Communications Business Unit
Microchip Technology, Inc.
www.microchip.com

Weltraumanwendungen

Diese verschiedenen Bereiche erfüllen unterschiedliche Funktionen, wodurch sich der Angriffsvektor und die Auswirkungen einer Sicherheitslücke unterscheiden. Der Plattform-/Raumfahrzeug-Bereich ist für den Flug und die Navigation des Satelliten selbst verantwortlich. Das Herzstück dieses Bereichs ist der Mikroprozessor (MPU), der in den Bordcomputern (OBC) innerhalb des Befehls- und Datenverarbeitungssystems (CDHS) zum Einsatz kommt. Das CDHS führt die Flugsoftware in Echtzeit aus und reagiert dabei auf Sensor- und Navigationsdaten, die vom Lagebestimmungs- und Steuerungssystem (ADCS) empfangen werden. Gleichzeitig tauscht das CDHS über das Telemetrie- und Befehlskommunikationssystem Telemetriedaten und Befehle mit Bodenstationen aus. Sicherheitslücken in diesem Bereich könnten zum vollständigen Verlust des Satelliten führen oder im schlimmsten Fall eine verheerende Kettenreaktion der Satellitenzerstörung auslösen, die als Kessler-Syndrom bezeichnet wird.

Der Nutzlastbereich

hingegen ist für die Durchführung der eigentlichen Mission des Satelliten zuständig. Beispiele sind Erdbeobachtung, Landesverteidigung, Wissenschaft, Breitbandkommunikation sowie Positionsbestimmung, Navigation und Zeitmessung (z. B. GPS). Ähnlich wie der Plattformbereich verfügt auch der Nutzlastbereich über eine Reihe von Bordcomputern im Nutzlast-Datenverarbeitungssystem (PDHS), das mit missionsspezifischen Funktionen wie Instrumenten, Kommunikationssystemen und Sensoren interagiert. Bodenstationen auf der Erde kommunizieren über das Nutzlast-Kommunikationssystem mit dem Nutzlastbereich. Zwar führen Sicherheitslücken im Nutzlastbereich möglicherweise nicht zum Verlust des Satelliten, könnten aber Informationen zur nationalen Sicherheit offenlegen, GPS-Systeme unbrauchbar machen oder die Breitbandkommunikation stören.



Beispielarchitektur eines Satelliten

Angesichts ihrer zentralen Rolle in einer Weltraumanwendung sind die verwendeten Mikroprozessoren nicht nur für das Erfüllen der Missionsziele, sondern auch für die Sicherheit des Systems entscheidend. Leistungsmerkmale wie Gesamtrechenleistung, Schnittstellen sowie Fehlertoleranz und Fehlervermeidung sind gefragt, um die Missionsziele zu erreichen. Strahlungsfestigkeit und -toleranz sind ebenfalls erforderlich, um den rauen Bedingungen im Weltraum standzuhalten, insbesondere bei missionskritischen oder bemannten Raumfahrtanwendungen, sei es in der erdnahen Umlaufbahn (LEO), auf dem Mond oder darüber hinaus.

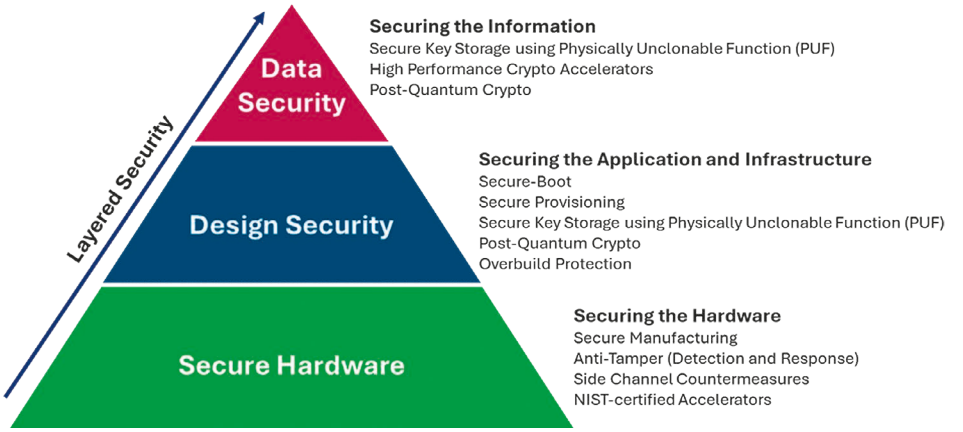
Entwickler von Raumfahrtsystemen müssen nun auch die Sicherheit berücksichtigen. Eine wirklich sichere Weltraumanwendung nutzt Mikroprozessoren in Raumfahrtqualität, die einem mehrschichtigen Sicherheitsansatz folgen.

Betrachten wir die Schichten des Sicherheitsansatzes:

Auf der untersten Ebene befindet sich die sichere Hardware. Solange die Hardware und ihre Lieferkette nicht sicher sind, kann weder der Infrastruktur noch den durch sie fließenden Informationen vertraut werden. Sichere Hardware wird durch Techniken wie sichere Fertigung, Manipulationserkennung und -abwehr, integrierte Gegenmaßnahmen gegen Seitenkanalangriffe und NIST-zertifizierte Beschleuniger erreicht.

Es folgt die Design-Sicherheit. Hier werden die Infrastruktur und das geistige Eigentum, auf denen die Weltraumanwendung basiert, gesichert. Zu den wichtigsten Mikroprozessorfunktionen in dieser Ebene gehören Secure-Boot, Secure-Provisioning und sicherer Schlüsselspeicher.

Sobald Hardware und Infrastruktur gesichert sind, können wir uns auf die Sicherung der



Mehrschichtiger Sicherheitsansatz

Informationen konzentrieren, die das System durchlaufen. In dieser Ebene müssen Mikroprozessoren in Raumfahrtqualität leistungsstarke kryptografische Beschleuniger und einen sicheren Schlüsselspeicher integrieren.

Ein in Bild 4 hervorgehobenes Leistungsmerkmal, das gerade in kritischen Infrastrukturen wie der Raumfahrt nicht übersehen werden darf, ist der dringende Bedarf an Post-Quanten-Kryptografie (PQK).

Asymmetrische Kryptografie

ist ein Grundstock jedes Systems, das auf Sicherheit setzt. In nahezu jeder terrestrischen Anwendung werden Algorithmen wie RSA und die elliptische Kurvenkryptografie (ECC) für digitale Signaturen und den Schlüsselaustausch genutzt. Angesichts herkömmlicher Schlüssellängen und der rechnerischen und mathematischen Herausforderungen bei der Faktorisierung von Primzahlen geht man davon aus, dass klassische Computer Milliarden von Jahren bräuchten, um RSA oder ECC zu knacken.

Quantencomputer

sind jedoch (noch) nicht in Sicht. Es ist möglich, wenn auch nicht wahrscheinlich, dass innerhalb der nächsten 5 bis 10 Jahre kryptografisch relevante Quantencomputer (mit ausreichend Qubits) für staatliche und andere finanzstarke Gruppen verfügbar sein werden. Die Gefahr, die von solchen Quantencomputern ausgeht, liegt in ihrer Fähigkeit, den Shor-Algorithmus zur Faktorisierung von Primzahlen auszuführen. Ein solcher Algorithmus, der auf einem Quantencomputer läuft, könnte die Zeit zum Knacken von RSA oder ECC von Milliarden von Jahren auf unter einen Tag reduzieren.

Worauf kommt es an?

Angesichts ihrer weitreichenden Nutzung in einer Vielzahl von Sicherheitsanwendungen wie Authentifizierung und Schlüsselaustausch stellt die Fähigkeit, RSA und ECC (ECDSA oder ECDH) zu knacken, eine existenzielle Bedrohung für Systeme weltweit dar.

Darüber hinaus beschränkt sich die Herausforderung nicht nur auf aktive Kommunikationsverbindungen im Moment des Geschehens. Angreifer könnten Kommunikationen „heute“ abfangen und speichern und sie „morgen“ entschlüsseln. Diese Bedrohung betrifft sowohl LEO-Konstellation für Breitbandkommunikation als auch strategische militärische Ressourcen.

Das National Institute of Standards and Technology (NIST) und die National Security Agency (NSA) haben diese Bedrohung erkannt und einen Wettbewerb ausgeschrieben, um quantensichere Public-Key-Algorithmen der nächsten Generation zu identifizieren. Im Rahmen dieses Wettbewerbs hat das NIST eine Reihe gitterbasierter PQK-Algorithmen ausgewählt, die RSA und ECC zukünftig ersetzen sollen:

- ML-KEM – Module-Lattice based Key Encapsulation Method (FIPS-203)
- ML-DSA – Module-Lattice based Digital Signature Standard (FIPS-204)

Beide sind grundlegende Voraussetzungen, um die Sicherheit unserer cyber-physischen Systeme langfristig zu gewährleisten.

Die Mikroprozessoren der Serie PIC64-HPSC

von Microchip stellen einen Durchbruch bei den Möglichkeiten eines 64-Bit-Mikroprozessors dar – auf der Erde, als auch für Weltraumanwendungen. Die MPU vereint die besten Eigenschaften handelsüblicher (COTS) Prozessoren wie Hochleistungsrechnen, Virtualisierung und KI mit der Fehlertoleranz und Strahlungsfestigkeit, die für die anspruchsvolle Umgebung des Weltraums erforderlich sind. PIC64-HPSC kombiniert Hochleistungsrechnen mit umfassenden Sicherheitsfunktionen – einschließlich vollständiger PQK-Unterstützung. Diese Funktion ist unerlässlich, um den Weltraum heute und in Zukunft zu sichern.

Mit PIC64-HPSC-MPUs lassen sich weltraumgestützte Anwendungen wie Satelliten, Trägerraketen und Rover/Lander so absichern, dass sie ihrer Rolle als wichtiger Bestandteil der kritischen Infrastruktur eines Landes gerecht werden. ◄

- **High Performance 64-bit Computing**
  - Up to 26k DMIPs
  - Virtualization
  - Artificial Intelligence
- **TSN Ethernet Integration**
  - 240G TSN Ethernet Switch
  - Comprehensive TSN Feature Set
  - Up to 20 ports with speeds from 10M to 10Gbps
- **Exceptional Fault-Tolerance**
- **Defense-Grade Security**
- **Radiation-Hardened and Radiation-Tolerant**