Synspective

GMO CYBER SECURITY IERAE

CYSAT 2026

Beyond General Space Cybersecurity

Toward a Risk Management Framework Specialized for SAR Satellite Service Providers

Yusuke Koide, Synspective Inc.
Kosuke Ito (*), Shinichi Kan, Yoshihiko Nagoya and Hiroko Ogane, GMO Cybersecurity by Ierae, Inc.

(*) Presenter

Who we are

Yusuke Koide
Leads space-system cybersecurity at the METI guidelines committee for space-system cybersecurity and ISAC.

Kosuke Ito, PhD
Leads product security governance initiatives, including IoT security standards, PSIRT, Secure SDLC, and certifications.

Shinichi Kan
Product security specialist focusing on IoT and automotive systems. Now extending to Space cyber domain.

Yoshihiko Nagoya
Experienced in threat modeling and security training instructor in a cybersecurity private company.

Hiroko Ogane
Experienced in threat modeling and security training instructor in a cybersecurity private company.

Today's presenter

Background / Objective

BACKGROUND

Issues / Challenges:

- Existing space-cybersecurity discussion is high-level and generic.
- Little of it is directly useful when designing a small SAR satellite product.
- Threat analysis must work under Small Sat constraints - limited SWaP-C, short development cycles, mass production for constellations.
- Industry needs a method that designers can actually run - and trust the prioritisation it produces.

OBJECTIVE

How should existing threat-modelling and risk-analysis frameworks be combined for a small SAR satellite system?

Find a method that delivers good results within the time and cost constraints that a Small Sat programme can afford.

"Reasonable enough, fast enough, defensible."

Methodology

A four-step pipeline. Steps 1 and 2 focused on scope and asset work. In step 3, we studied multiple known frameworks in parallel to compare their respective outputs.

01 Scope definition

Identify use-case categories and abstract the system into data flows. Define the analysis boundary.

02 Asset analysis

Catalogue protected information assets. Score each by C / I / A. Map damage scenarios to derive Impact Level (IL).

03 Threat analysis

Trial multiple classifications **(STRIDE / SPARTA / ENISA)**. Derive Threat Level (TL) and Risk Level (RL) per threat scenario.

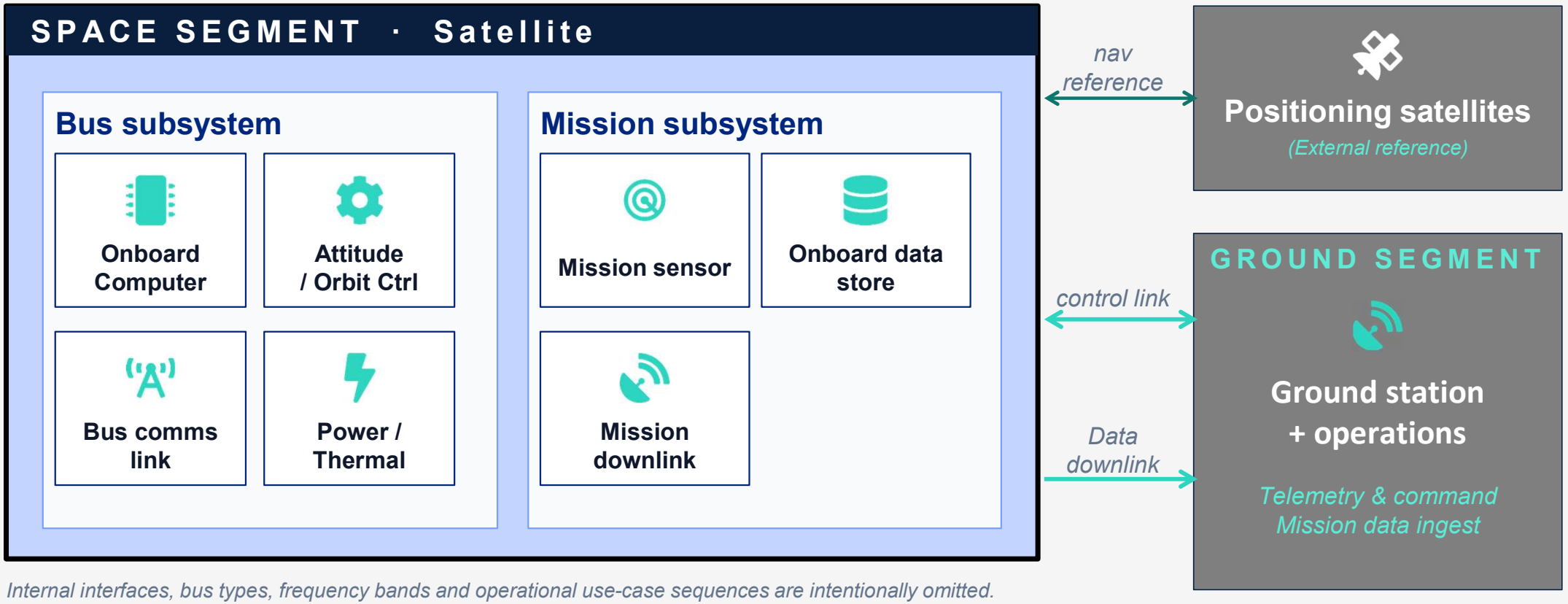
04 Method evaluation

Compare frameworks on coverage, intuitiveness and effort. Recommend a working method for Small Sat programmes.

Iterate - each pass refines scope, assets and threat detail.

Step 1 - Defining the Target System and Research Scope

We generalised our analysis to a small Earth Observation satellite system – including but not limited to SAR – with a focus on the Onboard Computer. The following overview diagram abstracts internal interfaces.



Internal interfaces, bus types, frequency bands and operational use-case sequences are intentionally omitted.

Step 2 - Asset Analysis

Information assets (A through I) were identified in scope. Asset value (used CIA scoring) ties to a damage-scenario list : collision, satellite loss, customer-data exposure, mission failure, etc.

ID	Information asset	Asset value	Primary impact if compromised
A	**Cryptographic keys**	H	Security controls disabled → satellite loss
B	**Area of Interest (customer information)**	H	Customer data exposure
C	**Raw mission observation data**	H	Customer data exposure / delivered data tampered
D	**Satellite firmware**	H	Security controls disabled → Mission-impacting outcome
E	**Housekeeping data**	M	Operational degradation
F	**Power/attitude control command**	M	Satellite loss (power/attitude)
G	**Orbit-control command**	H	Mission-impacting outcome / regulatory event
H	**Mission-tasking command**	M	Mission-impacting outcome
I	**Beacon-stop command**	M	Mission-impacting outcome

This assumes the use of a typical Earth observation small satellite.
H = High, M = Medium, L = Low. Highlighted cells indicate the dimensions where compromise drives the largest business or safety impact.

METHOD COMPARISON

Step 3 - Threat Analysis across Three Frameworks in Parallel

To find a method that suits Small Sat constraints, we ran the same threat-scenario set through three taxonomies. Risk scoring follows the **SPARTA 5×5 matrix** (Impact × Likelihood, scores 1–25, calibrated against NIST SP 800-30).

STRIDE

Microsoft (general IT)

Categories

Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege.

Fitness for Small Sat

Familiar to SW teams, but several space-specific threats (supply chain, physical, legacy infra) do not map cleanly.

SPARTA

Aerospace Corporation (space)

Categories

Access Control, Integrity, Availability, Mission Assurance, Confidentiality, Supply Chain, Defensive Cyber Operations.

Fitness for Small Sat

Built for space. Categories like Mission Assurance and Supply Chain align with what actually hurts a Small Sat operator.

ENISA

ENISA Space Threat Landscape

Categories

Nefarious activity, Eavesdropping /Hijacking, Physical attack, Unintentional damage, Failure/malfunction, Legacy infrastructure.

Fitness for Small Sat

Broad coverage including non-malicious causes; analysts found classification intuitive in our trials.

WHAT WE ANALYSED

Threat Scenarios in Scope

Threat scenarios were derived from the guidance by METI (Ministry of Economy, Trade and Industry of Japan), studying the past incidents and the IoT/OT experiences of the expert group. Grouped here by attack mode - attack-surface mapping is intentionally generalised.

Communications & cryptography

- Intentional jamming of the control link
- Spoofing of legitimate communications
- Cryptographic-key compromise → spoofing, leakage or denial of service
- Replay attack → eavesdropping or malicious command injection

Software & onboard execution

- Malware infection of the onboard OS
- Exploitation of software vulnerabilities onboard
- Malware embedded in onboard software
- Receipt of a patch with malicious code injected upstream

Network access & ground segment

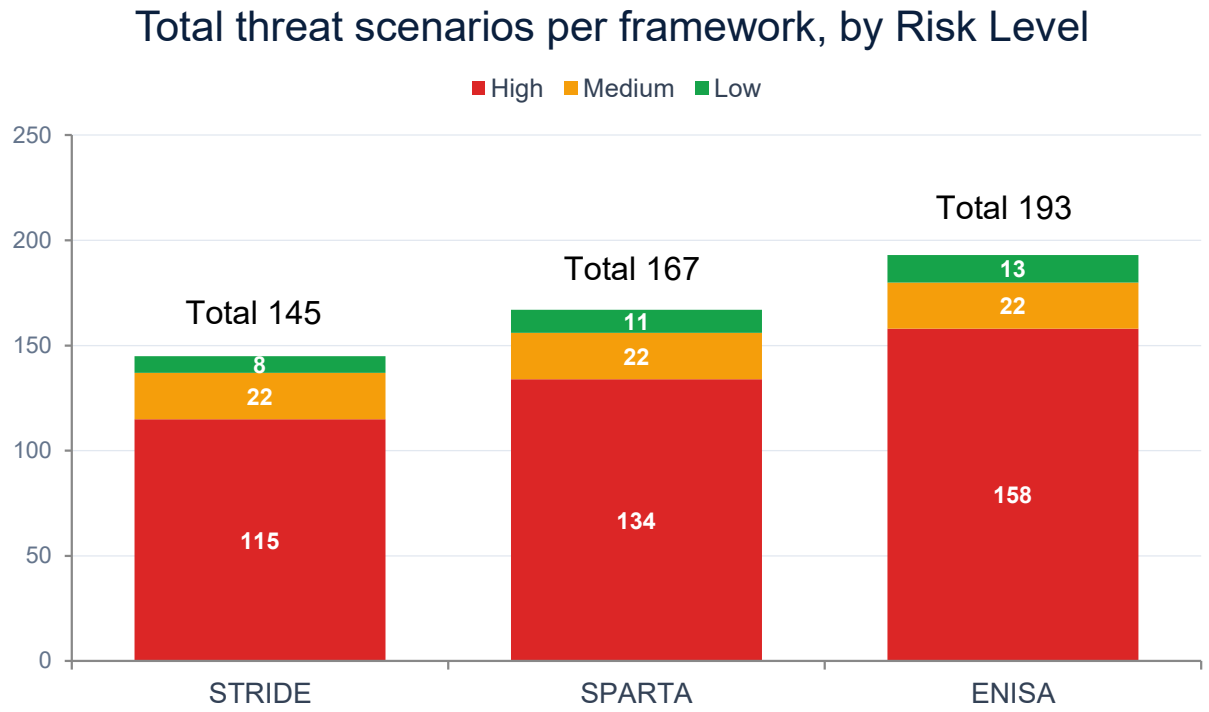
- Network intrusion via vulnerable security protocol
- Network intrusion via misconfiguration
- Unauthorised commands originating from the ground segment
- Compromise of the internal onboard bus / data-bus injection

Hardware, supply chain & physical

- Acceptance of tampered onboard hardware (constellation-level supply-chain risk)
- Resource-exhaustion attack against satellite interfaces
- Intentional damage to a sensor subsystem
- Abuse of hardware-level command paths

Results - Threat Scenarios Generated by Each Framework

The risk distribution was generally consistent, even though the total number of scenario lines generated by each method differed due to the different granularity of the categories for the same scope and assets.



This assumes the use of a typical Earth observation small satellite.

By the total numbers

Framework	Total	High	Med	Low
STRIDE	145	115	22	8
SPARTA	167	134	22	11
ENISA	193	158	22	13

Observation

SPARTA best matched the operators' intuitive understanding. **STRIDE** was the most concise, but it misses some paths specific to Small Sat. **ENISA** generates the most rows because it splits unintentional and legacy-infrastructure causes.

Critical Finding 1 - The Max Risk Level Assets

Several information assets have reached the highest risk level (Impact Level 5 x Threat Level 5).

We analysed the asset risk levels for a typical Earth observation small satellite on a scale of 1 to 25.

RL **25** of 25

Archetype 1 · Assets sitting at the system trust foundation

Assets in a layer that, if compromised, can bypass legitimate monitoring and defence mechanisms. Detection and recovery are operationally very difficult, so impact magnitude and irreversibility are large.

Delayed detection, hard recovery, fleet-wide propagation potential.

RL **25** of 25

Archetype 2 · Control elements tied to physical-safety / regulatory events

Control category where misbehaviour or malicious action surfaces as physical damage or regulatory breach. Must be treated as a safety / compliance event, not as a service incident.

Physical damage, regulatory burden, impact on operating licence.

RL **25** of 25

Archetype 3 · Assets where path multiplicity drives residual risk

Individual CIA scoring is mid-tier, but the number of associated threat scenarios and the multiplicity of reachable paths drive residual risk to the top in combination.

Impact spreads across many surfaces; full mitigation coverage is hard.

RL **25** of 25

Archetype 4 · Compliance-obligation control elements

Assets directly tied to a strict regulatory obligation. Availability and integrity are themselves part of the legal duty - routinely under-represented by CIA-only scoring.

Loss of operating authority; impact on the operating prerequisites of the business.

Critical Finding 2 - Gap between Hypothesis and Result

The SPARTA matrix top-tier results did not match with our hypothesis prior to the study . The gap itself is one of the most useful findings of this work.

Prior hypothesis

We expected the highest-confidentiality information assets to top the risk matrix:

- **Cryptographic keys**
  → Core of authentication and encryption; leakage maximises impact.
- **Area of Interest (customer information)**
  → Sensitive customer data itself; leakage causes immediate business impact.
- **Raw mission observation data**
  → Core delivered value; tampering or leakage is high-impact.

Confidentiality-led thinking

GAP ⟷

Actual result (High Risk Level Assets)

What actually reached the top tier was a different class of asset:

- **Assets at the system trust foundation / boundary**
- **Control elements that produce physical-safety / regulatory events**
- **Assets where path multiplicity drives residual risk (CIA mid-tier)**
- **Control elements tied to a regulatory obligation**

Integrity / Availability / Regulation dominate

What the gap shows: Confidentiality ≠ Risk. For Small Sat operators, the decisive factors were route redundancy, regulatory necessity, and the ripple effect on the entire system.

FINDINGS

What We Learned

SPARTA / ENISA fit the analyst's intuition better than STRIDE for Small Sat work.

STRIDE lacks a natural framework for situating space-specific concerns (supply chain, mission assurance, legacy infrastructure, and unintentional damage). During this study, analysts achieved faster and more consistent threat classification using SPARTA and ENISA.

Confidentiality intuition did not predict the highest-risk assets.

Initial assumption was that the high-confidentiality assets (cryptographic keys, Area of Interest, and raw observation data) would become the primary risks. However, the items that reached the maximum risk level (RL=25) were triggered by integrity, availability, and regulatory risks. It has become clear that relying only on the standard CIA assessment can lead to a systematic undervaluation of these critical areas.

SPARTA / ENISA still leave room to optimise the threat-scenario set.

While SPARTA / ENISA are highly compatible, current scenarios were fixed for comparison. Our next iteration will refine these into an actionable toolkit by consolidating overlaps and adding unique satellite cases for design team integration.

Future Work - Extending the Method for more

Today's analysis only covers a single SAT configuration. We like to extend our study for more comprehensive system-level, encompassing multiple small Earth observation satellites, relay satellites, and ground systems—such as a satellite constellation..

Threat-scenario optimisation

NOW Scenario set fixed for cross-method comparability.

NEXT Consolidate duplicates, refine granularity, add satellite-specific cases — sharpen the SPARTA / ENISA set into a form design teams can act on.

METHOD REFINEMENT

AI-assisted threat analysis

NOW Manual analysis by joint analysts; effort scales with scope.

NEXT Explore AI assistance for scenario generation, asset–threat mapping and risk review — to widen coverage and cut iteration cost.

TOOLING & SCALE

Inter-satellite relay

NOW Direct space-to-ground link, single hop.

NEXT Third-party relay satellites in constellation use - an extra trust boundary; end-to-end protection required across an unowned segment.

TRUST BOUNDARY

Ground segment topology

NOW Dedicated, operator-owned ground station.

NEXT Shared / Ground-Station-as-a-Service - multi-tenant separation, and the supply chain widens to include the GSaaS provider.

SHARED INFRA

Dev / build environment

NOW Threat analysis scoped to the satellite product itself.

NEXT Bring CI/CD and OSS dependencies into scope - build tooling, signing keys and the dependency tree become attack surfaces; upstream compromise reaches the flight asset directly.

UPSTREAM SUPPLY-CHAIN

The unifying view

Attack surface extends beyond the satellite itself, across the full development and operations ecosystem. Future work updates the threat analysis along each axis above and pairs it with HILS-class verification, so results plug directly into design decisions.

Contact us and Practical Output

Yusuke Koide
<yukoi@synspective.com>

Kosuke Ito, PhD
<kosuke.ito@gmo-cybersecurity.com>

Threat analysis template
(please contact us)

Synspective

GMO CYBER SECURITY IERAE