

E I G E N I A B . V .

Cyber Digital Twin · Fail Fast, Fail Safe

CASE STUDY · OPEN-SOURCE INTELLIGENCE · REPRESENTATIONAL EXAMPLE

A representational LEO broadband satellite, built from open-source intelligence to show how a Cyber Digital Twin works

An illustrative example of the EIGENIA platform, built only from public information and general engineering knowledge. It is not a model of any real spacecraft. Client engagements use controlled engineering data and produce very high-fidelity models.

Example

LEO-RSAT-001, a representational satellite of the LEO broadband class

Built from

Open-source intelligence and engineering judgement only

Regimes

CRA, RED, NIS2, EU Space Act (proposed)

01

Summary

A broadband constellation is a product, a radio installation and a critical service at the same time. Each of those faces sits under a different European regime, and for the spacecraft itself the Cyber Resilience Act may not apply at all. This case study uses a representational satellite, built from open-source intelligence, to show how EIGENIA builds a product as a Cyber Digital Twin first, so that the scoping question is answered from a model rather than from assumptions.

LEO-RSAT-001 is a representational example of a LEO broadband satellite, of the general kind described in public sources: phased-array and parabolic RF payload, optical inter-satellite links, krypton electric propulsion, reaction-wheel attitude control. It is built only from open-source intelligence, with limited information, and is meant to show the method, not to describe a real spacecraft. It should not be read as high fidelity. Its geometry is procedural, its parameters are placeholders, it is not connected to any spacecraft and every behaviour shown is simulated.

REPRESENTATIONAL ONLY

This is an open-source example built to demonstrate the EIGENIA Cyber Digital Twin platform. It is not Amazon's design or any other operator's. When EIGENIA is engaged, client twins are built from the client's controlled CAD, registers, interface documents, flight software and test data, and reach a fidelity this public example cannot.

61 example register records: 52 base, 9 added and flagged	544 named meshes in the 3D model, every one keyed to a twin ID	44 typed interfaces, IF-001 to IF-044, mapped to trust zones
16 simulated mission steps from launch to passivation	9 listed deviations from the uploaded register	5,472 simulated telemetry records in the example signal schema

WHERE THE CRA MAY NOT APPLY

The CRA governs products with digital elements made available on the EU market. A satellite built and operated by the same company to deliver a service is arguably never made available to anyone. User terminals and supplied ground equipment are in scope; the spacecraft may fall to NIS2 and the proposed EU Space Act instead. Section 03 sets out each regime and its open question.

APPROACH: OPEN-SOURCE INTELLIGENCE AND ENGINEERING

Built only from publicly available statements and filings about LEO broadband satellites, plus an illustrative register and build specification written for this example. Where public information ran out, engineering judgement filled the gap, and every such value is tagged ASSUMED. Every record is tagged DOCUMENTED, DERIVED, ASSUMED or SIMULATED. Nothing here is vendor CAD or operator data.

The product

LEO-RSAT-001 is a box-shaped bus, 4.0 × 1.2 × 2.2 m, with two six-metre solar wings on drives along the orbit-normal axis. The nadir deck carries three user-link phased arrays, two gateway arrays and two gimbaled feeder dishes. Four optical terminals form the mesh. A composite-overwrapped krypton tank sits in the centre of an equipment deck, with flight computers, radios, batteries and payload electronics arranged on two decks around it.

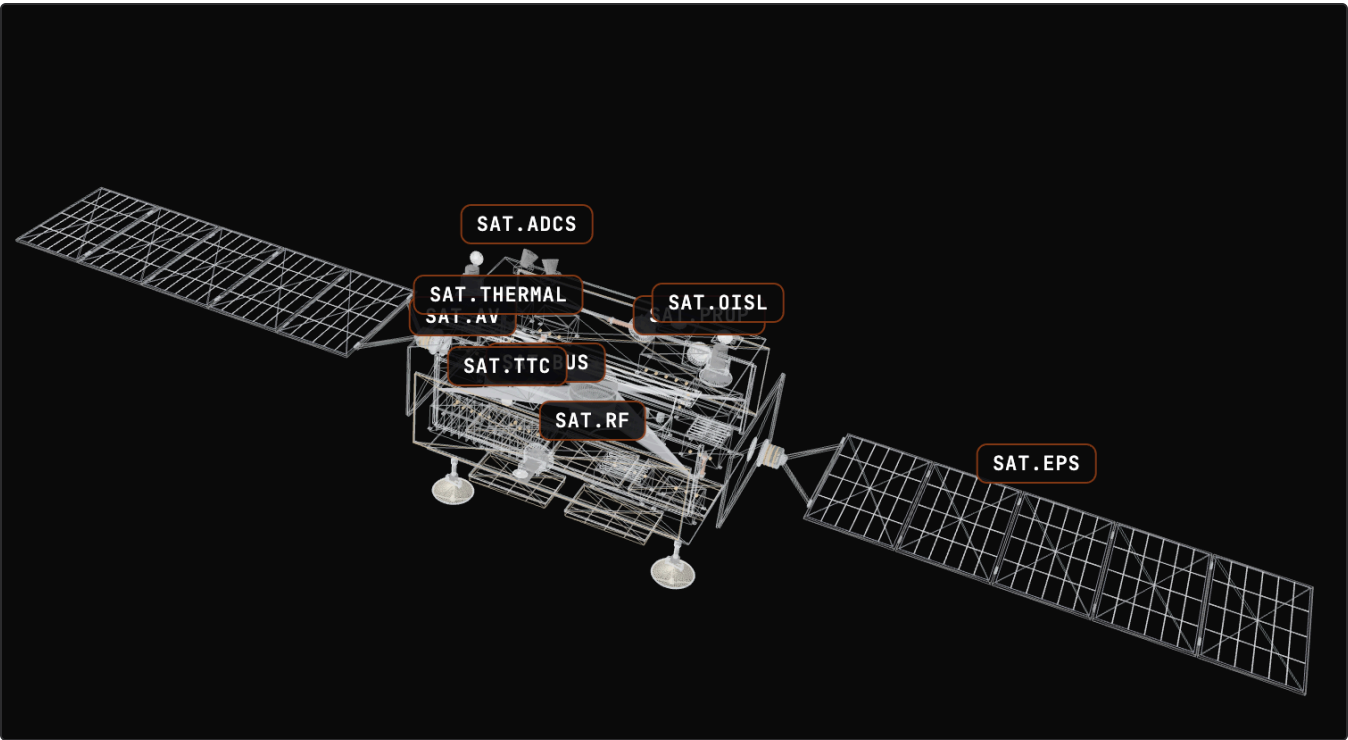


Figure 1. The representational LEO-RSAT-001 in wire render, deployed. Each tag is a subsystem twin ID from the example register (SAT.EPS, SAT.ADCS, SAT.RF and so on); clicking any part in the viewer opens its record, evidence tag and interfaces.

DOCUMENTED [4] 590 to 630 km shells More than 3,000 satellites in the initial system.	DOCUMENTED [6] Phased arrays and dishes Payload combines both antenna types.	DOCUMENTED [8] Optical mesh 100 Gbps links at nearly 1,000 km on the prototypes.	DOCUMENTED [9] Krypton propellant Loaded before dispenser integration.	DOCUMENTED [6] Reaction wheels Validated on the protoflight mission.
--	---	---	---	---

TAG	MEANING IN THIS TWIN	RECORDS
DOCUMENTED	Existence stated in a cited public source. Geometry is still assumed.	24
DERIVED	Computed from documented values or the register by a stated method.	9
ASSUMED	Register class "assumed" or "unknown", every added record, all procedural geometry.	28
SIMULATED	Every dynamic state, telemetry value and event from the SIM-A simulator.	all runtime data

03

Why this matters now

Three things changed in 2025 and 2026. RED cybersecurity requirements became mandatory for radio equipment on 1 August 2025. CRA reporting obligations started on 11 September 2026, ahead of full application on 11 December 2027. And ENISA rated the space sector as highly critical for the first time, noting that NIS2 and the CRA do not apply uniformly across it [R7]. The EU Space Act, which would add space-specific cyber duties, is still in the legislative process.

REGIME	WHAT IT COVERS HERE	APPLIES TO LEO-RSAT-001?
CRA [R1]	Products with digital elements made available on the EU market	Open. Likely not, if the operator builds and flies its own satellites. Yes for user terminals, supplied ground software and any spacecraft or subsystem sold to an EU operator.
RED + DA 2022/30 [R3]	Radio equipment placed on the market or put into service in the Union	Doubtful for a spacecraft in orbit. Clear for user terminals. Article 3(3)(d)(e)(f) requirements apply until the CRA takes over.
NIS2 [R2]	Annex I space sector: operators of ground-based infrastructure supporting space services	Yes, for the operator. Gateways, TT&C and mission control are in scope as an entity, not as a product.
EU Space Act [R4]	Proposed duties for space operators, including pre-launch threat-led testing [R6]	Proposed. The Council text of March 2026 applies it without prejudice to NIS2 [R5].
ITU RR, national licences, FCC Part 25 [R8][R9]	Spectrum coordination, market access, debris mitigation	Yes. Not cyber law, but they constrain TT&C and disposal design.
IEC 62443, ECSS, CCSDS SDLS [R10] [R11][R12]	Zones and conduits, space software assurance, link security	Voluntary. Used as the engineering basis for evidence in every regime above.

The squeeze on a constellation operator

An operator ships terminals under the CRA and RED, runs ground infrastructure under NIS2, and may soon answer to a space regulator for the satellites. Three regimes ask for the same underlying facts: what is inside, how it connects, how a vulnerability is found and fixed, and who is told. Holding those facts once, in one model, is cheaper than answering three times.

EIGENIA POSITION

We do not assume the CRA applies. Phase 1 records the scoping decision per item, with the reasoning, and the twin carries that decision so it can be revisited when the Space Act text settles.

04

The same six-phase method

PHASE	FOR LEO-RSAT-001	TWIN OUTPUT
1 Scope and classify	Decide regime per item: spacecraft, terminal, gateway, software. Classify CRA items against Annex III and IV.	Scope record per twin ID
2 Risk assessment	Threats per zone and conduit; TT&C injection, update supply chain, payload-to-bus pivot.	Threat trees keyed to IF-IDs
3 Requirements and design	Annex I Part I mapped to controls: authenticated TC, signed images, zone separation.	Requirements traceability
4 Secure development and vulnerability handling	Annex I Part II: SBOM, coordinated disclosure, in-orbit patch path within contact windows.	xBOMs, VEX, patch procedure
5 ALARP review	Residual risk argued as low as reasonably practicable, given that a satellite cannot be recalled.	Residual risk register
6 Handover to the test bench	Package, viewer, simulator and evidence delivered; go or no-go with listed gaps.	This package

Zones inside the product

ZONE	CONTAINS	CONDUIT TO
Customer traffic plane	User data through the beams	Payload processing only
Payload processing	UA1 to UA3, GA1, GA2, dishes, modem, router, O1 to O4	Spacecraft data network via ROUTER (IF-042)
Spacecraft data network	Onboard switch, PCDU, thermal	Flight control plane
Flight control plane	FC_A, FC_B, ADCS, propulsion	TT&C radio (IF-023, IF-024)
TT&C radio	TTC_A, TTC_B, TT&C antenna	Ground command system over Ka-band

DESIGN RULE

The twin is never a command path. Simulation results stop at a human-reviewed command-planning boundary, and hazard class 3 and 4 commands run on the bench only behind a physical interlock.

Inside the machine

GROUND • NIS2 ENTITY SCOPE

Mission control

Command planning, signing, flight dynamics

TT&C stations

Ka-band command and telemetry

Gateways

Feeder links to fibre and cloud edge

KA-BAND TT&C • authenticated TC frames (scheme to confirm) • IF-021, IF-022

CONDUIT

TT&C radios A and B

The only command path onto the spacecraft

Feeder and user RF, optical mesh

Customer traffic only, terminates in the payload

SPACEWIRE (reference) • onboard switch • IF-010, IF-011, IF-023, IF-024

FLIGHT CONTROL PLANE

Flight computers A and B

Mode manager, FDIR, command authentication

ADCS

4 wheels, 3 torque rods, star trackers

Propulsion

PPU, flow control, Hall thruster

CAN (reference) • PCDU, wheels, PPU, FCU • IF-012 to IF-016, IF-028, IF-029

PAYLOAD PROCESSING

Modem and channeliser

Baseband for 5 arrays and 2 dishes

Payload router

Optical mesh and control plane, IF-042 to the bus

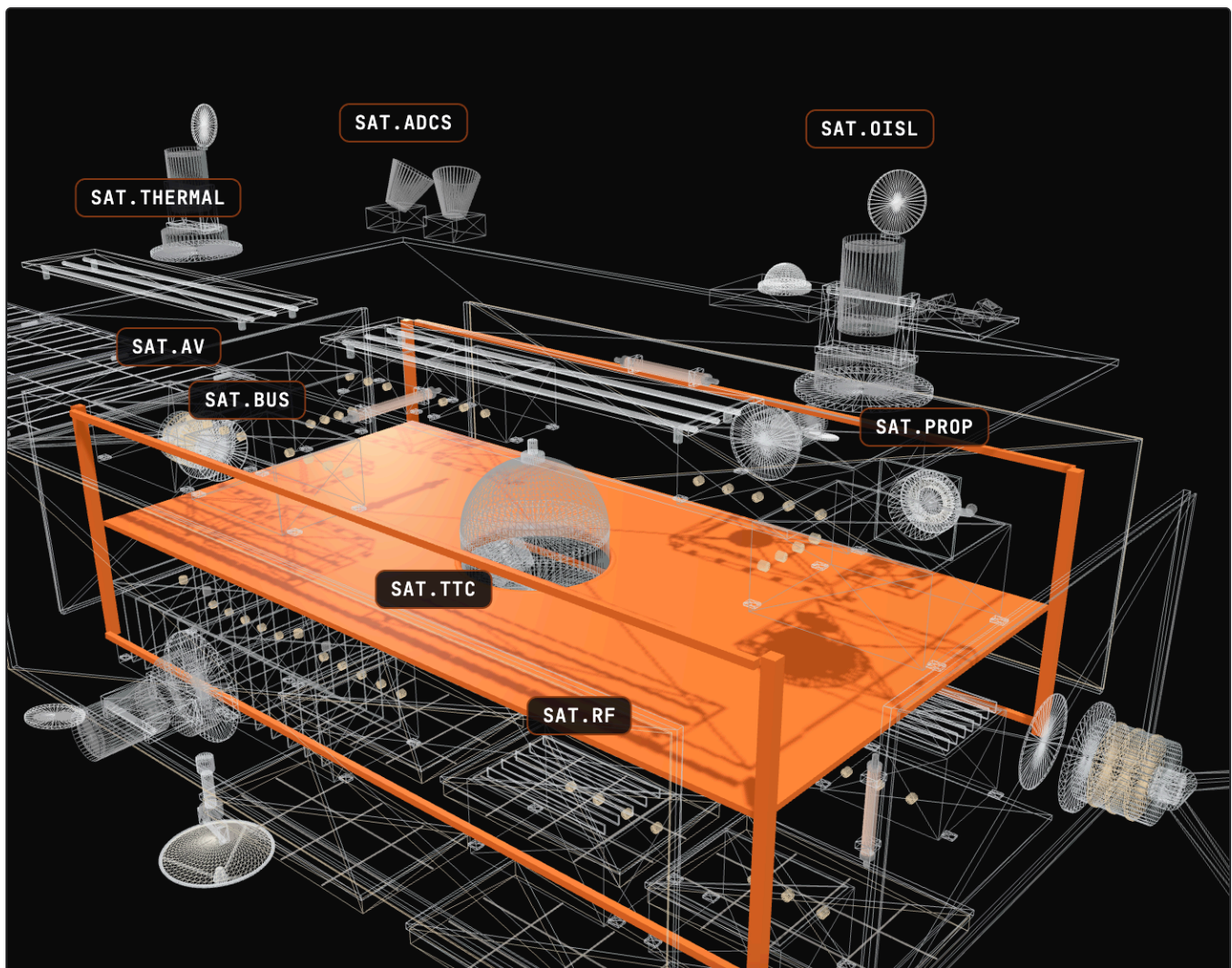


Figure 2. Bus interior, structure selected. Internal units were re-placed on two decks around the krypton tank because the register positions produced 25 volumetric clashes. The SIM-A/L1 layout has none; the change is listed as DEV-01.

Every link, typed

17 Data	10 Power	9 RF	4 Optical data	2 Krypton feed	2 Thermal
------------	-------------	---------	-------------------	-------------------	--------------

THE SINGLE COMMAND CONDUIT

Two interfaces, IF-023 and IF-024, carry every command into the flight control plane. IF-042 is the only data path from the payload to the bus. Those three links decide most of the threat model.

Eight bills of materials, one record

The build specification extends CycloneDX into eight linked BOMs. Every entry resolves to the same twin and package IDs as the 3D model.

BOM	HOLDS	STATUS IN THIS PACKAGE
HBOM	Processors, FPGAs, radios, sensors, wheels, PPU electronics	Part register ready; vendor parts unknown
SBOM	Flight applications, OS, boot software, ground adapters	Reference stack (cFS) only, not Amazon software
FBOM	Bootloaders, bitstreams, device firmware, calibration tables	Skeleton
CBOM	Algorithms, keys, certificates, trust stores, rotation	Skeleton; TC authentication scheme to confirm
MBOM	Assemblies, processes, tooling, inspection evidence	Assembly tree exported
DBOM	Telemetry schema, command definitions, retention	I/O map and signal schema exported
NBOM	Onboard and ground network nodes, paths, filtering	Interface register and zones exported
Model BOM	Simulator, equations, parameters, validity, V&V	sim.js, parameters, validation report

07

Supply chain, tier by tier

No supplier is named, because none is public for the production satellite. The twin records the tier structure and the questions each tier must answer.

TIER	ITEMS	CYBER QUESTION
0 Integrator and operator	Bus, payload integration, flight software, ground segment	Who signs flight images and holds the TC keys?
1 Subsystems	Arrays and drives, wheels, EP thruster and PPU, OISL terminals, RF payload, avionics	Which carry firmware, and can it be updated in orbit?
2 Components	Rad-tolerant processors and FPGAs, cells, Li-ion cells, krypton	Single-source items and counterfeit controls
3 Services	Launch, dispensers, ground stations, cloud edge	Which have access to the spacecraft before or after launch?

08

From vulnerability to report

If an item is in CRA scope, an actively exploited vulnerability starts the Article 14 clock. If the spacecraft sits only under NIS2, the operator reports significant incidents under Article 23 on similar deadlines. The twin holds both paths so the scoping decision selects the procedure.

The 24-hour clock

EARLY WARNING 24 h	NOTIFICATION 72 h	CRA FINAL REPORT 14 days	NIS2 FINAL REPORT 1 month
------------------------------	-----------------------------	------------------------------------	-------------------------------------

The space-specific constraint is the fix, not the report. A patch reaches the spacecraft only through a signed uplink during a ground contact. In the SIM-A run a contact lasts about eight minutes, so the procedure must plan which pass carries the image and how the satellite rolls back if a health check fails.

09

How an adversary would attack it

Command injection over TT&C IF-021 → IF-023 · TT&C radio to flight control plane - Capture a valid telecommand on the Ka-band uplink - Replay it, or forge one if authentication is weak - Command SAFE or an actuator change outside a planned pass CONTROLS - Authenticated TC frames with anti-replay counter (CCSDS SDLS) - Hazard classes with dual authorisation for class 4 - Reject, log and preserve evidence; exercised in step S09	Compromised flight software update Build and signing → ground → TT&C → FC_A, FC_B - Tamper with a dependency or the build host - Get the image signed by a legitimate pipeline - Uplink it as a routine update CONTROLS - SBOM and FBOM per image, reproducible builds - Secure boot with an on-board trust anchor - Health-checked rollback to the last approved image
---	---

A third path, from customer traffic through the payload router into the bus (IF-042), is held in the model as a zone crossing and needs the router's filtering rules before it can be scored.

10

Annex I requirements, mapped to evidence

Applies to items in CRA scope. For the spacecraft the same mapping serves as NIS2 Article 21 and Space Act evidence, which ask for the same controls.

ANNEX I	REQUIREMENT	TWIN EVIDENCE
Part I (2)(b)	Secure by default configuration	Launch configuration: TX inhibited until separation (S01, S02)
Part I (2)(d)	Protection from unauthorised access	Authenticated TC; replay rejected and logged (S09)
Part I (2)(h)	Availability of essential functions, resilience	FDIR isolates RW3 and holds attitude on three wheels (S13)
Part I (2)(j)	Limit attack surface	Two command conduits only, IF-023 and IF-024
Part I (2)(l)	Record and monitor relevant activity	TC/TM/FDIR/SEC log in the package
Part II (1)	Identify components, SBOM	Eight-BOM structure keyed to twin IDs (skeletons)
Part II (2), (8)	Remediate without delay, secure updates	In-orbit patch path with rollback (to be defined)

11

The CRA evidence pack

Digital files

FOLDER	CONTENTS
01-model	Full GLB and glTF, OBJ + MTL, nine subsystem GLBs
02-structure	Part register, part catalogue, assembly tree, materials, system map
03-kinematics	Array hinges, SADA, dish and OISL gimbals, wheel rotors
04-controller	Controller logic, 16-step sequence, I/O map, telemetry sample, TC/TM log
05-interfaces	Interface register, connections, anchors
06 to 08	Sources with citations, viewers, validation report, SHA-256 manifest (44 files)

Test bench readiness

Thirteen automated checks pass, including zero duplicate IDs, zero orphan meshes, all 44 interface endpoints resolved, zero equipment clashes, a propellant mass balance within 1 % and two identical deterministic runs.

Requirements Traceability Matrix

SCENARIO	STEP	RESULT
AT-001 Separation to sun-safe	S02 to S05	Rates 1.1 to 0.02 °/s; positive energy balance
AT-002 Eclipse traversal	S11	SOC minimum 63.5 %, above shed threshold
AT-005 Reaction wheel failure	S13	RW3 isolated, SAFE, recovered
AT-009 Invalid command signature	S09	Rejected, evidence preserved
AT-012 Historical replay	All	Identical SHA-256 over all samples

NOT YET COVERED

Gateway reroute (AT-007), payload thermal excursion (AT-008), software rollback (AT-010) and telemetry divergence (AT-011) need a network model or a bench, and are listed as gaps.

Ready for the test bench

One unified data model

Geometry, interfaces, controller sequence and telemetry share one set of IDs. A bench engineer who clicks RW3 in the viewer sees its register record, its CAN interface IF-015, its live simulated speed and the FDIR event that isolated it.

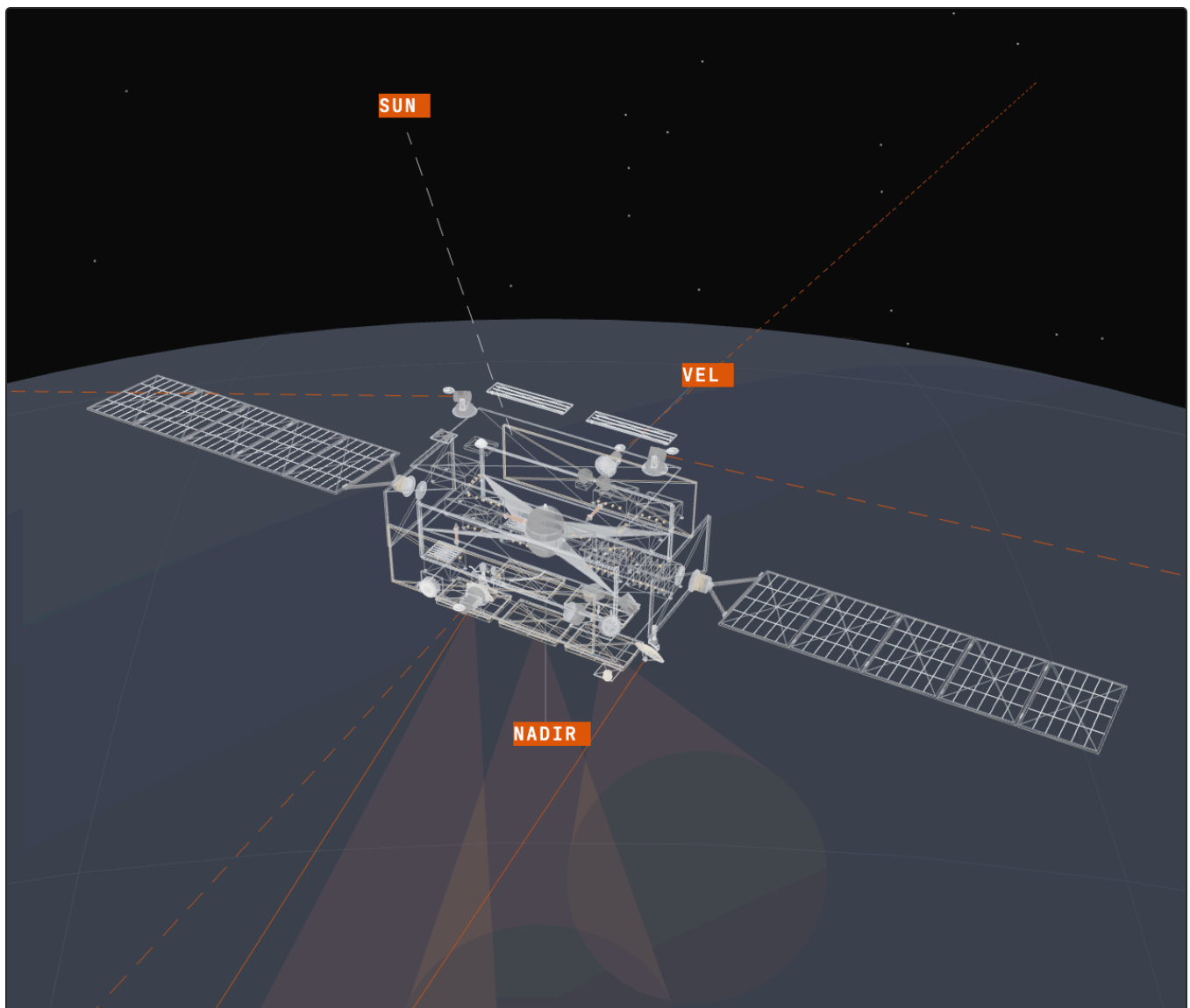


Figure 3. The animated example twin in service mode. User beams point nadir, laser links run to four peers and the sun, velocity and nadir vectors come from the orbit model. Everything shown is SIMULATED with generic reference control laws.

Q1 What is in scope? Scope record per twin ID, with regime and reasoning.	Q2 How does it connect? 44 interfaces, zones and the three critical conduits.	Q3 How does it behave? Deterministic 16-step run with fault injection.	Q4 What is missing? Gaps with owners: TC scheme, xBOM content, rollback.
--	--	---	---

Vulnerabilities, prioritised the way a bench needs them

For a spacecraft, exploitability is weighed against reachability: a flaw behind the TT&C conduit ranks above one in a payload card that customer traffic cannot address, and anything that cannot be patched in orbit ranks above anything that can.

A checklist for both assessment routes

For CRA items, Module A self-assessment or Modules B + C. For the spacecraft under NIS2 or the Space Act, the same evidence feeds the operator's risk-management and pre-launch testing record.

Pull, not push: 5S for the test bench

The bench pulls what it needs from the package by ID. Nothing is emailed as a loose spreadsheet, and the manifest proves which version was tested.

The preparedness service and the go / no-go decision

ILLUSTRATIVE DECISION FOR THE EXAMPLE

Go for a software-in-the-loop bench on the simulator and viewer. No-go for a hardware bench until the TC authentication scheme, the flight-image signing chain and the in-orbit rollback procedure are defined.

13

For bench testers: a guide

What you can expect

A model you can open in a browser, a simulator that gives the same answer every time, and records that say what is known and what is guessed.

How to use it

- **Open**
Serve 07-viewer and open the animated twin. Verify SHA256SUMS first.
- **Navigate**
Pick a part, read its twin ID, evidence tag and interfaces.
- **Exercise**
Toggle the three faults and replay. Compare the TC/TM log to sequence.json.
- **Report**
Raise findings against twin and interface IDs.

What you will not have to do

Reverse-engineer an architecture from slides, guess which items are in scope, or reconcile part names across documents.

Why use EIGENIA

The same six-phase method and the same package format for every product, from a farming robot to a satellite.

BENCH SAFETY

Hazard class 3 and 4 commands are simulation-only unless a hardware safety case and a physical interlock exist.

HONEST LIMITS

Geometry is procedural, physics parameters are scenario values, and no figure is Amazon production data.

14

The technical file, compiled

ANNEX VII ITEM	WHERE IT LIVES
General description and intended purpose	README, part register
Design, development and production	Assembly tree, kinematics, controller logic
Cybersecurity risk assessment	Zones, interface register, threat trees
Vulnerability handling, SBOM	xBOM skeletons, reporting procedure
Test reports	Validation report, checks.json
EU declaration of conformity	Only for items confirmed in CRA scope

FOR THE SPACECRAFT

If phase 1 confirms the satellite is outside the CRA, the same file is reissued as the operator's NIS2 risk-management evidence and, once adopted, the Space Act record.

15

What this gives the manufacturer

A scoping answer backed by a model, one set of IDs across geometry, interfaces and telemetry, a simulator that exercises the controls the regulators will ask about, and an explicit list of what is still unknown. The constellation operator can reuse it for every satellite in the fleet by changing the configuration, not the method.

Beyond broadband satellites

The next model is an open-source 3U CubeSat with public CAD and flight software, which will show the same method on a spacecraft whose parts are fully documented.

FROM EXAMPLE TO CLIENT TWIN

Open-source intelligence was enough to build this example; it is not enough to assess a real product. In a client engagement EIGENIA works from the client's own controlled register, CAD, interface documents, flight-software dictionaries and test data, and the twin that results is a very high-fidelity model of the actual product.

Sources

REF	SOURCE
[4]	Amazon, What is Amazon Leo (Project Kuiper)
[6]	Amazon, Kuiper protoflight mission update, Nov 2023
[8]	Amazon, Kuiper OISL test, Dec 2023
[9]	Amazon, Kuiper satellite processing facility
[R1]	Regulation (EU) 2024/2847, Cyber Resilience Act
[R2]	Directive (EU) 2022/2555, NIS2
[R3]	Delegated Regulation (EU) 2022/30 under RED
[R4]	Proposal for an EU Space Act, COM(2025) 335
[R5]	E+H, EU Space Act vs NIS2, Council compromise
[R6]	Hannes Snellman, EU Space Act and NIS2
[R7]	Covington, ENISA NIS360 2026
[R8]	ITU Radio Regulations
[R9]	47 CFR Part 25
[R10]	IEC 62443 series
[R11]	ECSS standards
[R12]	CCSDS 355.0-B Space Data Link Security

NO WARRANTY

This case study and the model it describes are a representational example built from open-source intelligence, for illustration and education only, without warranty. They make no declaration that any figure, component, configuration or finding is correct for any real product, and they are not to be relied on as a high-fidelity model. Amazon Leo and Project Kuiper are Amazon programmes; this work was produced independently from public information and implies no endorsement or assessment by Amazon. Regulatory summaries are not legal advice; applicability must be confirmed for each item.