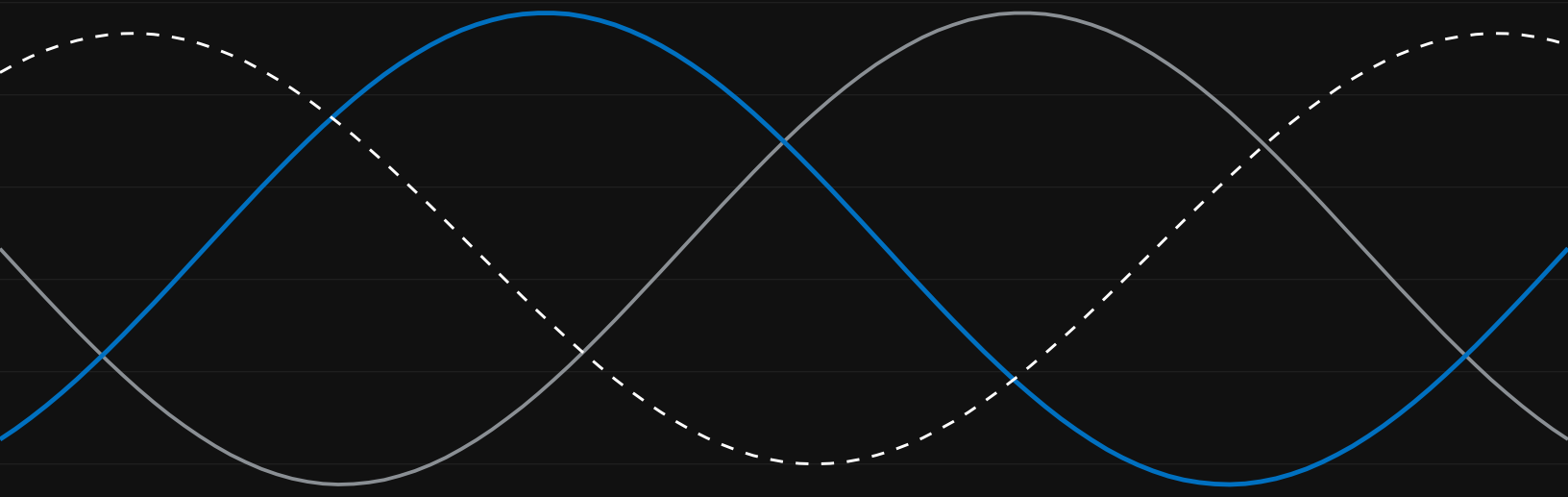
Module 01 · Workbook · Student edition

Concept of Operations

The method behind the Day-1 decomposition, taught once, and the complete telecommand deliverable it produced, element by element.



ethicallyHackingspace (eHs)®
TLP:AMBER

Copyright and legal notices

© 2026 ethicallyHackingspace (eHs)®. All rights reserved.

> **Printing.** To save toner, print from page 2. The cover is a dark full-page plate and carries nothing the pages after it do not.

TLP:AMBER. Limited disclosure. Recipients may share this document only within their own organization and its clients, on a need-to-know basis, and only to the extent necessary to act on the information.

This document is part of the Full Spectrum Space Cybersecurity Professional program. It is provided to enrolled learners and to the credentialing bodies it is submitted to. Sharing beyond what that marking permits, and any resale, is not authorized.

Verbatim sources. Every taxonomy definition quoted in this document is the published METEORSTORM taxonomy text, quoted exactly and never abbreviated, paraphrased or reworded. Where the course explains an element in its own words, the explanation is not presented as the definition. One typographical error in the published file, a doubled period, is corrected.

Trademarks. ethicallyHackingspace (eHs)® is the copyright holder of this publication; D2 Team CORP is its publisher. Other names appearing in this document are the property of their respective owners and are used for identification only.

No warranty. This publication is provided for education. It is not legal, regulatory, or engineering advice for any specific system.

Publisher	D2 Team CORP, a 501(c)(3) nonprofit
Program	Full Spectrum Space Cybersecurity Professional
Document	Module 01 Concept of Operations, module workbook, student edition
Edition	Student edition · revised 2026-11-19
Contact	www.d2teamcorp.org

Student edition

The teaching chapters and the complete worked deliverable.

What this document is and how to use it

What it is. The Module 01 workbook for Concept of Operations, METEORSTORM Function 01: the method, taught once, and the complete worked result for Kestrel Orbital, the fictional satellite operator this course uses as its example.

How to use it. Read it beside the Module 01 lesson, then keep it as your reference for the method. The contents list every chapter and section with its page. The scope of the worked result is stated on the page after the contents.

What goes with it. The Module 01 question set is a separate download; the answers to its questions are printed in it.

How to use this workbook

The Module 01 lesson on the course site runs in the order below. This workbook is the reference for every step. The lettered parts are worked on the lesson page, not in this workbook.

Story film	Master Decomposition at Kestrel Orbital
Video 1	One component, three answers
Video 2	Naming one element
Video 3	Every element names its parent
Part A	Build identifiers and check four records
Video 4	Forty-four elements, built top down
Part B	Place parents in the register
Video 5	One element, the Day 1 rulings, and MISP
Part C	Write one element
Check	Check your understanding

Use this at work. Blank record sheets, for your own use, are in the METEORSTORM desk pack on the course downloads page.

© 2026 ethicallyHackingspace (eHs)®

Contents

CH 1 The Day in One Page 7

Kestrel Orbital, the company 7

CH 2 One Data Model for Three Departments 9

The taxonomy: the published taxonomic elements 9

The ontology: the relationships 10

CH 3 The Four Layers 11

3.1 · PCE, where the platform operates 12

3.2 · SEG, how the platform is distributed 13

3.3 · SVC, what the platform delivers 14

3.4 · AST, what the platform is built from 14

CH 4 How Elements Are Named 16

The TEN, four hyphenated fields 16

The ETEN, five colon-delimited fields 17

One complete worked ETEN 17

CH 5 The ETEN Process, Once, Then the Deltas 19

The SEG delta 20

The SVC delta 21

The AST delta 21

CH 6 The Telecommand Decomposition, Complete 24

6.1 · PCE, 4 elements 25

6.2 · SEG, 4 elements 27

6.3 · SVC, 15 elements 30

6.4 · AST, 21 elements 35

CH 7 Deploying the Taxonomy in the SOC 43

The machine tag 43

The three deployment steps 43

One tagged event, read 44

The first adoption step 45

© 2026 ethicallyHackingspace (eHs)®

CH 8 **Use This at Work** 46

Ten things to do at your work center 46

Desk pack sheets for Function 01 47

Where the method is in this workbook 48

What you will be able to do

We will be looking at systems decomposition so you can decompose an operational space platform top down into named, parented elements in a published nomenclature, and defend the scope boundary of that decomposition.

O1	State why three departments need one description of the telecommand path
O2	Name the four structural layers and the root every element resolves to
O3	Write one ETEN in five fields, with the parent it names
O4	State the Day 1 scope ruling and the owner of each ruling
O5	Read a MISP event tagged with the meteorstorm taxonomy

The detail behind those objectives:

KNOWLEDGE

K1	The four structural layers, Primary Capability Environment, Segment, Service and Asset, and what each one records.
K2	The two identifier nomenclatures: the type nomenclature, hyphenated and without an ordinal, and the enumerated nomenclature, colon delimited with an ordinal.
K3	The parent chain and the no-orphan rule: walking upward from any element always reaches an environment.
K4	Ordinal assignment: counted per tag, two digits from 00, issued once and never renumbered, with gaps retained as canon.
K5	The eight-step enumeration process and which step is the gate that stops a wrong-layer entry.

SKILLS

S1	Write a well-formed five-field identifier for one enumerated element.
S2	Assign a correct ordinal against a running inventory, including where gaps exist.
S3	Link a child to its parent and verify the chain terminates at an environment.
S4	Apply the scope rule to admit or exclude a candidate element, and justify the ruling.
S5	Detect a malformed identifier and name the rule it violates.

ABILITIES

A1	Decompose an unfamiliar platform path top down, unprompted, producing an inventory another department can use.
A2	Defend a scope boundary to a department that wanted it drawn elsewhere.

TASKS

T1	Produce a complete, parented concept of operations for a telecommand path.
T2	State what the pass covers, what it excludes, and why.
T3	Hand the enumeration to threat modeling as an inventory that threats can anchor to.

© 2026 ethicallyHackingspace (eHs)®

Scope and standing of this work · read before judging the enumeration

What this is. Kestrel Orbital's first application of the METEORSTORM framework, produced by three departments who had never used it before. It is a deliberately scoped first pass over the telecommand path: the command-and-control chain from the operator console to execution on orbit.

Why that scope, and not more. The three mandates chose it. Executive Order 14144 sets the command-and-control protections required of civil space systems, which Kestrel Orbital adopts as binding by company directive, the NIS2 Directive places a duty of care and a reporting clock on the ground operator, and the Space ISAC exchange carries what the other two produce. The fleet is already flying, so the first pass ran on the telecommand path, the elements that would end the mission if an adversary took them. Enumerating everything else first would have been thorough and useless.

What it is not, stated plainly. It is not an exhaustive model of the platform and does not claim to be. Elements off the telecommand path are not enumerated. Some assets group several physical units where those units share an owner, a build and a patch path. Gaps in the ordinal sequence mark elements the register tracks outside this scope. Within the path the service and asset layers are a first pass, and a second pass would find more. Every one of those is a decision recorded when the enumeration was made, not an oversight discovered later.

How it grows. Ordinals are issued once and never renumbered, so everything enumerated here keeps its identifier as the register expands. The same eight-step enumeration procedure from Module 01 runs on the next scope, and the one after that. A first pass that names its boundary can be extended. One that hides its boundary has to be rebuilt.

The standard we hold ourselves to. A scope choice is stated openly. A defect is fixed, never narrated. If you find an element misnamed, a parent wrong, or a count that does not add up, that is a defect and we want to hear about it. If you find something outside the telecommand path missing, that is the scope, it was chosen deliberately, and it is on the roadmap. The two are not the same criticism, and this work is built so you can tell them apart.

© 2026 ethicallyHackingspace (eHs)®

Part I **Orientation**

Why three departments describing one platform three different ways is the problem you were hired to solve, and what one shared description buys.

CH 1 The Day in One Page

You are building SCOR, the department that evolves the three departments, Security Operations, Satellite Operations, and Satellite Design & Engineering, toward Resilient Cyber Operations by applying the five METEORSTORM functions in order. Today's function supplies what the three have never had: one centralized taxonomy, ontology, and enumeration process for the platform, so context and enrichment are recorded against the same elements. You do not need to be the expert in each department; your job is to build the team and run the functions.

Kestrel Orbital, the company

Kestrel Orbital is a fictional operator, invented for this course. Every identifier, count and record in it comes from the Day-1 inventory.

Fact	Kestrel Orbital
The fleet	Geostationary, a continuous link at a fixed look angle, and medium Earth orbit, contacted in a single-station window
The sites	Mission operations in Reston, Virginia. The northern ground station in Kiruna, Sweden
Three departments	Security Operations Center. Satellite Operations Center. Satellite Design and Engineering
Three people	Maya Reyes, analyst lead. Theo Lindgren, senior controller. Dana Whitfield, systems engineer
Your job	Stand up SCOR, Space Cybersecurity Operations and Resilience

Key points

- SCOR applies the five METEORSTORM functions in order; today's function supplies one taxonomy, ontology and enumeration process for the platform.
- Three mandates set the scope, and the telecommand path comes first because the mandates land on it.
- Today's deliverable is a 44-element CONOPS of the telecommand path, every PARENT link populated below the root, no orphans.

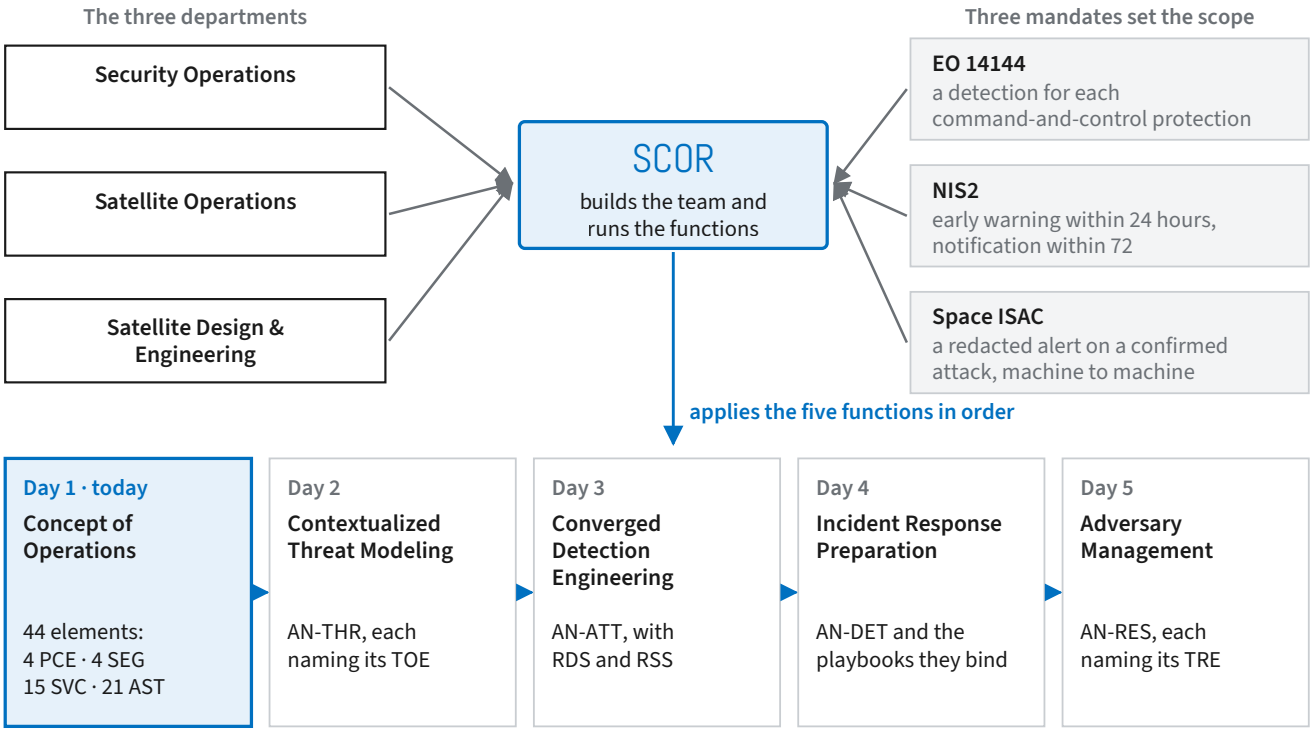
Three mandates set the scope, one duty per line:

- **EO 14144:** SCOR writes a detection for each command-and-control protection Executive Order 14144 requires.

© 2026 ethicallyHackingspace (eHs)®

- **NIS2:** SCOR executes the incident-sharing thresholds the directive sets: early warning within 24 hours, incident notification within 72.
- **Space ISAC:** SCOR shares a redacted alert on a confirmed command-and-control attack, machine to machine.

Figure 1 The day in one page: three departments and three mandates, one team, five functions in order



Read it as today's output as the input to every day after it: each later analytic element names one of today's elements.

Why telecommand first. Because the mandates land on it. Executive Order 14144, Sec. 3(c) as amended by Executive Order 14306, sets the protections required for the command and control of civil space systems, and Kestrel Orbital adopts them as binding by company directive KO-EXEC-2026-014: encrypt the commands, protect their integrity, authenticate the source, and reject unauthorized commands. The NIS2 Directive puts the ground-based infrastructure that carries it under mandatory cybersecurity risk-management and reporting duties. The path that keeps the satellite under control is the path you must be able to show is protected, so that is where your decomposition starts.

Today, Day 1. Today you decompose the telecommand path, the path that keeps the satellite under control, across the four layers from start to finish. You will leave with a first pass of the path enumerated as ETENs under one taxonomy and one parent chain, so a finding one department records resolves to the same element for the other two. The model you use today already covers the environments Kestrel Orbital's business plan drives toward, maritime, aerial, and deep space, so nothing you name now needs renaming when those markets arrive.

What you build. A 44-element CONOPS of the telecommand path, run end to end: 4 PCE, 4 SEG, 15 SVC, 21 AST, every PARENT link populated below the root, no orphans. Chapter 6 prints the whole deliverable.

© 2026 ethicallyHackingspace (eHs)®

The week ahead. Day 2 is Function 02, Contextualized Threat Modeling: each threat is enumerated as an analytic element, AN-THR, that names one of today's elements in its Target of Exploitation (TOE) field. Day 3 is Function 03, Converged Detection Engineering: attack paths (AN-ATT) against the same elements, with the required data sources (RDS) and required signal sources (RSS) a defensive cyber operator must hold to see each step. Day 4 is Function 04, Incident Response Preparation: detection signatures (AN-DET) and the playbooks they bind, written against the NIS2 reporting clocks. Day 5 is Function 05, Adversary Management: resilience measures (AN-RES), each naming the element it protects in its Target of Resilience Enhancement (TRE) field. Module 02 consumes exactly what you finish today: a threat whose TOE cannot name an element in this CONOPS is excluded on the record until the CONOPS enumerates that element.

CH 2 One Data Model for Three Departments

> "The three departments have no centralized taxonomy, ontology, or enumeration process, so a finding one department records is not normalized for the other two."

Reading notes, before anything else. Identifiers ahead use two nomenclatures: hyphens for a taxonomic element (TEN), and colons plus a two-digit ordinal for an enumerated element (ETEN). Chapter 4 prints the full lesson on both.

The silo problem. Ask the three departments about the same component and you get three answers, because there is no centralized taxonomy. A finding recorded against one department's naming has to be re-keyed before the next department can act on it, and every re-keying loses precision and time. METEORSTORM gives all three departments one data model, a taxonomy and an ontology, and an enumeration process to populate it. Every component of the platform in scope is recorded as exactly one enumerated element, in one of four layers: **PCE**, **SEG**, **SVC**, **AST**.

Key points

- Without one taxonomy, a finding recorded in one department's naming is re-keyed before the next can act, losing precision and time.
- The taxonomy names every element; the ontology places it in the parent chain.
- One name, three uses, no translation.

What each department gets back. Security Operations writes detections that target an exact element. Satellite Operations uses the same names on console to know what is degraded. Satellite Design & Engineering routes patches against the same data model. One name, three uses, no translation.

The taxonomy: the published taxonomic elements

Every element takes its TAG and LABEL from the published taxonomy, so cyber, space operations, engineering, vendors, peer operators, and Space ISAC members record the same element under the same TEN. The published taxonomic elements per layer:

- **PCE · 5 elements**: TE Terrestrial, AQ Aquatic, AE Aerial, OR Orbital, DS Deep Space.

© 2026 ethicallyHackingspace (eHs)®

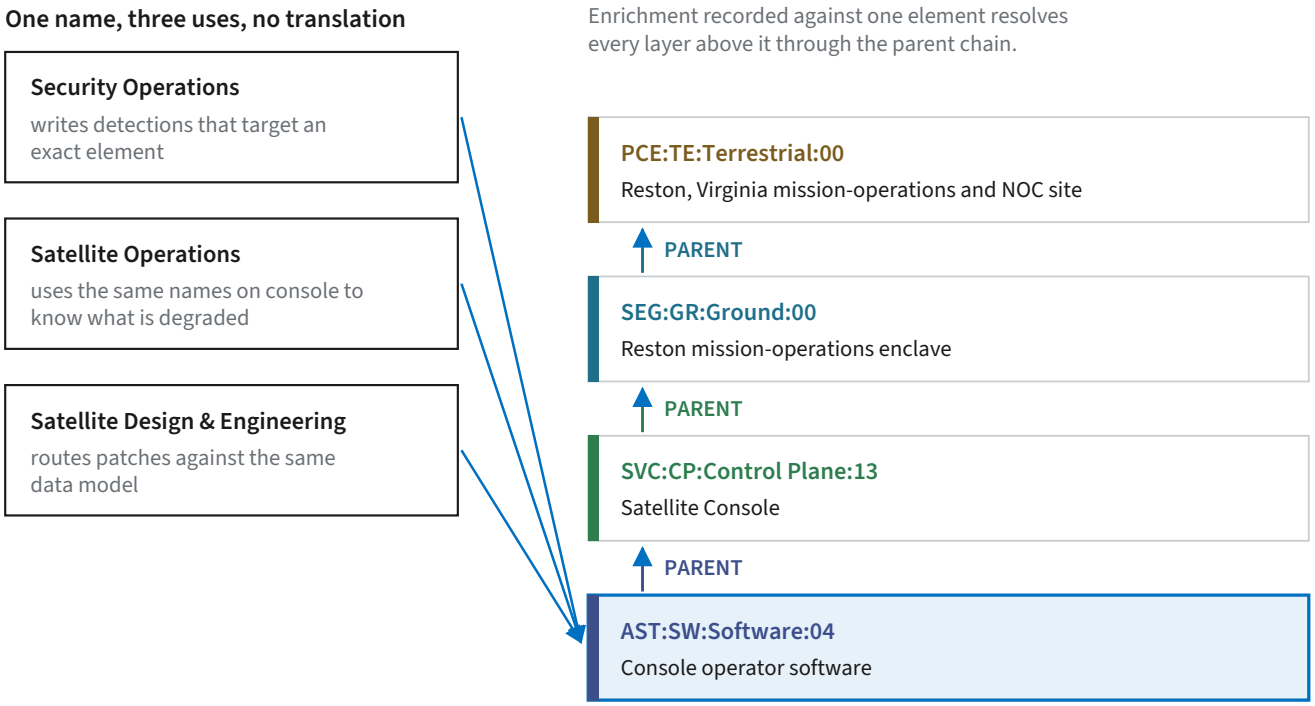
- **SEG · 10 elements**: LA Launch, LI Link, GR Ground, US User, AQ Aquatic, LO Low Altitude, HI High Altitude, NE Near Space, SP Space, DE Deep Space.
- **SVC · 3 elements**: CP Control Plane, DP Data Plane, HY Hybrid.
- **AST · 6 elements**: HW Hardware, FW Firmware, SW Software, DA Data, SI Signal, HY Hybrid.

The ontology: the relationships

Every element below the root names its parent in its PARENT field, and those parent links form one strict chain, the parent chain: Asset to Service to Segment to Environment. Every enumerated element resolves to a **PCE**; an element below the root with no PARENT is not a valid ETEN.

- A **SEG** element names one or more **PCE** elements in PARENT.
- A **SVC** element names one or more **SEG** elements in PARENT.
- An **AST** element names every **SVC** element it carries in PARENT, at least one.

Figure 2 One element, three departments: the same name, resolved through the parent chain



Read it as the element at the bottom as the one record all three departments touch, and the chain above it as the context every one of them inherits.

Why both. Named by the taxonomy, placed by the ontology, every element carries its full context. Enrichment is recorded against one element and resolves every layer above it through the parent chain in a single query, the same chain all three departments read from their own end.

© 2026 ethicallyHackingspace (eHs)®

Part II **The method**

The four layers, the rules for naming an element, and the enumeration process. Taught once here, applied unchanged in Modules 02 to 05.

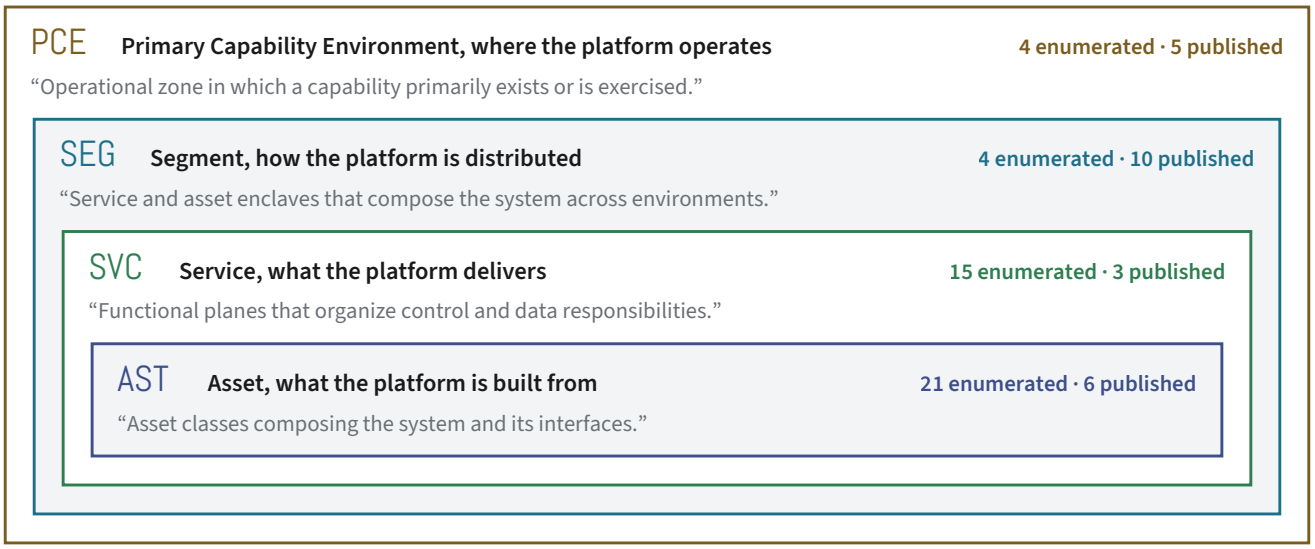
CH 3 The Four Layers

Four sub-chapters, one per structural layer, in decomposition order. Each opens with the layer's verbatim definition, then carries the per-element depth: every taxonomic element in the layer, its full TEN, and, for the taxonomic elements this scenario does not enumerate, why they are out of scope. The figure below carries the four layers; 3.1 lists the five published environments.

Key points

- Four structural layers in decomposition order: PCE, SEG, SVC, AST.
- A taxonomic element is enumerated only when the platform operates in it.
- Every child names its parent, so every element resolves to the environment it operates in.

Figure 3 The four layers, nested: each with its role, its published definition and its counts



Every child names its parent: AST to SVC to SEG to PCE. Counts: enumerated on the telecommand path; published in the taxonomy.

Read it as the published count as the taxonomy and the enumerated count as this platform: a few tags can produce many instances, which is why SVC and AST enumerate more elements than they publish.

© 2026 ethicallyHackingspace (eHs)®

3.1 · PCE, where the platform operates

> **PCE** · Primary Capability Environment · layer definition, verbatim: *"Operational zone in which a capability primarily exists or is exercised."*

Layer 1, the root of the parent chain. Every other layer resolves to a PCE element through the parent chain, so every element beneath inherits the PCE context. PCE is also the layer that deconflicts nature from adversary. When a symptom appears, operations often cannot tell an environmental effect (space weather, atmospheric drag, radiation) from a cyber-physical adversary action, and naming the environment keeps a natural anomaly from being chased as an attack and an attack from being written off as weather.

Element	Full TEN (verbatim)	Depth	Scope today
PCE-TE	**PCE-TE-Terrestrial-Surface-based operational zones on planetary bodies.**	The land surface of a planet: the ground the platform is built and operated on. Two of these sites are in scope today.	**In scope**: the Reston and Kiruna sites.
PCE-AQ	**PCE-AQ-Aquatic-Water-based operational zones, including but not limited to Earth's maritime domains.**	On or under water: sea-surface and subsurface operating areas.	Out of scope: the platform does not operate there today; enumerated when Kestrel operates in the maritime environment.
PCE-AE	**PCE-AE-Aerial-Atmospheric operational zones spanning lower, upper, and near-space regions.**	Inside the atmosphere: the lower, upper, and near-space air a platform can fly in.	Out of scope: no Kestrel capability operates in the atmosphere on the telecommand path.
PCE-OR	**PCE-OR-Orbital-Operational zones within planetary or satellite orbits.**	In orbit around a body: where the satellite itself flies.	**In scope**: the GEO and MEO regimes.
PCE-DS	**PCE-DS-Deep Space-Operational zones beyond planetary orbital regimes.**	Beyond planetary orbits: interplanetary and deep-space distances.	Out of scope: the fleet flies no deep-space mission; enumerated when it does.

The scope rule that governs the column above: a taxonomic element is enumerated only when the platform operates in it. The out-of-scope taxonomic elements complete the taxonomy so you can read any platform, and Step 01 of the ETEN Process (chapter 5) is what keeps them out of this CONOPS.

How the three departments use PCE. Security Operations inherits PCE context on every alert without re-deriving it. Satellite Operations reads PCE to know which regulatory regime and response posture applies. Satellite Design & Engineering reads it because the same hardware behaves differently on the ground than on orbit.

© 2026 ethicallyHackingspace (eHs)®

3.2 · SEG, how the platform is distributed

> SEG · Segment · layer definition, verbatim: *"Service and asset enclaves that compose the system across environments."*

Layer 2, anchored to PCE. Adversaries do not attack "the satellite"; they pick an enclave to operate against, like the link, a ground enclave, or the spacecraft enclave on orbit. SEG records those enclaves so you can describe what you are actually defending. The SEG boundary is the line your defensive cyber operators hold. Tiebreak for the recurring trap: PCE and SEG share several tag names; zone means PCE, group of services and assets means SEG.

Element	Full TEN (verbatim)	Scope today
SEG-LA	SEG-LA-Launch-Surface-based services and assets for primary launch operations.	Out of scope: the platform is operational on orbit, and the launch enclave is not on the telecommand path.
SEG-LI	SEG-LI-Link-Services and assets enabling platform communications across signal paths.	**In scope**: one link enclave carries telecommand up and telemetry down.
SEG-GR	SEG-GR-Ground-Surface-based services and assets for primary platform operations, serving as the primary locus of control plane activity.	**In scope**: two ground enclaves, Reston and Kiruna, hold command authority and the radio.
SEG-US	SEG-US-User-Services and assets for primary end-user operations.	Out of scope: SEG-US is a taxonomic element in the data model and out of scope for this platform, so it is not enumerated.
SEG-AQ	SEG-AQ-Aquatic-Water-based services and assets for primary platform operations, not limited to Earth's maritime domains.	Out of scope: its PARENT would be an environment the platform does not operate in.
SEG-LO	SEG-LO-Low Altitude-Aerial services and assets in the lower atmosphere.	Out of scope: its PARENT would be an environment the platform does not operate in.
SEG-HI	SEG-HI-High Altitude-Aerial services and assets above the lower atmosphere but below near space.	Out of scope: its PARENT would be an environment the platform does not operate in.
SEG-NE	SEG-NE-Near Space-Aerial services and assets above high altitude and below orbital regions.	Out of scope: its PARENT would be an environment the platform does not operate in.
SEG-SP	SEG-SP-Space-Services and assets operating in planetary or satellite orbits.	**In scope**: the spacecraft enclave on orbit.
SEG-DE	SEG-DE-Deep Space-Services and assets operating beyond planetary orbital regimes.	Out of scope: its PARENT would be an environment the platform does not operate in.

How the three departments use SEG. Security Operations scopes threat hunts to a SEG ("anything on the Link"). Satellite Operations holds the segmentation boundary. Satellite Design & Engineering owns the architecture decisions that put each asset inside the right enclave.

© 2026 ethicallyHackingspace (eHs)®

3.3 · SVC, what the platform delivers

> SVC · Service · layer definition, verbatim: *"Functional planes that organize control and data responsibilities."*

Layer 3, anchored to SEG. Two enclaves tagged identically can still do completely different jobs. SVC records the function an enclave delivers, so you can say what is actually at risk when something happens. Services that span more than one segment set DISTRIBUTED to Y and list every participating SEG in PARENT.

Element	Full TEN (verbatim)	Depth	Scope today
SVC-CP	SVC-CP-Control Plane-Services for managing and orchestrating platform control functions.	The functional plane that commands the platform.	**In scope**: 10 instances.
SVC-DP	SVC-DP-Data Plane-Services for managing and orchestrating mission product functions.	The functional plane that moves mission product.	**In scope**: 1 instance.
SVC-HY	SVC-HY-Hybrid-Services integrating both control and data plane functionalities.	Services that do both, like Command and Data Handling.	**In scope**: 4 instances.

All three SVC taxonomic elements are enumerated on the telecommand path; scope at this layer is applied per enumerated element. Only the services that authorize, protect, carry, or execute commands on the path are enumerated.

How the three departments use SVC. Security Operations writes a detection rule against a service when the behavior belongs to the function, so the rule fires against the function, not the specific device, and survives hardware refreshes. Satellite Operations writes the continuity plan at SVC ("telecommand authentication is offline, fall back to…"). Satellite Design & Engineering owns the SVC interface contract that every AST must implement.

3.4 · AST, what the platform is built from

> AST · Asset · layer definition, verbatim: *"Asset classes composing the system and its interfaces."*

Layer 4, anchored to SVC. Enrichment that names a service or a segment cannot be acted on by the people who actually patch, monitor, replace, or quarantine. Satellite Design & Engineering does not patch "the control plane"; they patch a specific firmware image on a specific device at a specific site. AST is the layer patches are applied to, and the layer where

© 2026 ethicallyHackingspace (eHs)®

your three departments converge. A detection names the one element it observes, in whichever layer that element sits: a service when the behavior belongs to the function (3.3), an asset when it belongs to one concrete element. Of the four detection signatures written in Module 04, one names a service, **SVC:CP:Control Plane:09**, and three name assets.

Element	Full TEN (verbatim)	Scope today
AST-HW	AST-HW-Hardware-Physical components supporting platform operations.	**In scope**: 7 instances.
AST-FW	AST-FW-Firmware-Embedded control code governing hardware functions.	**In scope**: 2 instances.
AST-SW	AST-SW-Software-Applications and logic executing operational tasks.	**In scope**: 6 instances.
AST-DA	AST-DA-Data-Information generated, processed, or consumed by the platform.	**In scope**: 4 instances.
AST-SI	AST-SI-Signal-Communication channels and transmission frequencies.	**In scope**: 2 instances.
AST-HY	AST-HY-Hybrid-Composite elements combining multiple asset types.	Taught, no instance today: no composite element on the telecommand path needed asset-level resolution as a unit; AST-HY is enumerated only when a composite is the right resolution.

How the three departments use AST. Security Operations names a specific AST instance when a finding belongs to one concrete element. Satellite Operations logs incidents at AST resolution. Satellite Design & Engineering owns the asset inventory, the patch pipeline, and the vulnerability management work at this layer. An AST element that carries several services names each of them in PARENT. The optional SUBSYSTEM tag is different: it groups several assets into one physical group, such as the spacecraft bus group chapter 6.4 recommends. The Day 1 inventory does not record a SUBSYSTEM value yet. Units inside one asset, like the sensors in **AST:HW:Hardware:00**, need no tag: they are already one element.

© 2026 ethicallyHackingspace (eHs)®

CH 4 How Elements Are Named

> "An ETEN is written **LAYER:TAG:LABEL:ORDINAL:Description**."

Two nomenclatures, one lesson. The TEN names a type and is read from the published taxonomy; the ETEN names one real instance on your platform and is what you produce. Reading the data model means reading TENs; applying it means writing ETENs.

Key points

- A TEN names a type and is read from the published taxonomy; an ETEN names one real instance on your platform and is what you produce.
- The ETEN copies Layer, Tag and Label from the TEN and adds the Ordinal and the Description.
- One identifier carries exactly one description, everywhere it appears.

The TEN, four hyphenated fields

A TEN is written **LAYER-TAG-LABEL-Definition**. It names a taxonomic element, not one enumerated element, and carries the framework's canonical Definition for that category. That Definition reads the same on every platform. Every TEN is published in the taxonomy: you look it up and never invent it. Four worked walkthroughs, one per layer:

Full TEN	Layer	Tag	Label	In practice
PCE-OR-Orbital-Operational zones within planetary or satellite orbits.	**PCE** · root layer; the environment the platform operates in	**OR** · selected from the published taxonomy; never invented	Orbital · the label of the published TEN for that tag	Class-level talk about orbital environments: "Every PCE-OR instance needs a conjunction-risk feed."
SEG-SP-Space-Services and assets operating in planetary or satellite orbits.	**SEG** · a self-contained enclave with one operational role	**SP** · selected from the published taxonomy; never invented	Space · the label of the published TEN for that tag	On the space segment: "**SEG-SP** assets share the orbital safety boundary."
SVC-CP-Control Plane-Services for managing and orchestrating platform control functions.	**SVC** · the function an enclave delivers	**CP** · selected from the published taxonomy; never invented	Control Plane · the label of the published TEN for that tag	"Every **SVC-CP** service is in scope for command-link integrity."
AST-SW-Software-Applications and logic executing operational tasks.	**AST** · the concrete element that implements a service	**SW** · selected from the published taxonomy; never invented	Software · the label of the published TEN for that tag	"**AST-SW** elements must enter SBOM tracking."

© 2026 ethicallyHackingspace (eHs)®

In every row the fourth field, the Definition, is framework canon and is the same on every platform.

The ETEN, five colon-delimited fields

An ETEN is written **LAYER:TAG:LABEL:ORDINAL:Description**. LAYER, TAG, and LABEL come straight from the published TEN. You add the two-digit ORDINAL that tells instances apart and the per-instance Description that scopes this exact item. All five fields are required on every enumerated element. Field by field:

- **LAYER.** The structural layer the element belongs to: **PCE**, **SEG**, **SVC**, or **AST**. Field 1 of 5.
- **TAG.** The two-letter code that names the element within the layer (for example **TE** for Terrestrial, **GR** for Ground, **CP** for Control Plane, **HW** for Hardware, **SW** for Software). Always picked from the published list, never invented. Field 2 of 5.
- **LABEL.** The plain-English name that goes with the two-letter code, for example Terrestrial for **TE**, Ground for **GR**, Software for **SW**. Field 3 of 5.
- **ORDINAL.** A two-digit number, starting at **00**, that tells multiple instances of the same element apart. The first ground segment is **SEG:GR:Ground:00**, the second is **SEG:GR:Ground:01**, and so on. Ordinals are scoped to the (LAYER, TAG) pair, continue across segments rather than restarting, and are never re-used. Field 4 of 5.
- **DESCRIPTION.** A short, free-text note about this specific instance: what it is, where it is, what role it plays, and anything later work will need to know. The description is what turns a TAG and LABEL into one specific enumerated element on your platform. Field 5 of 5.

One complete worked ETEN

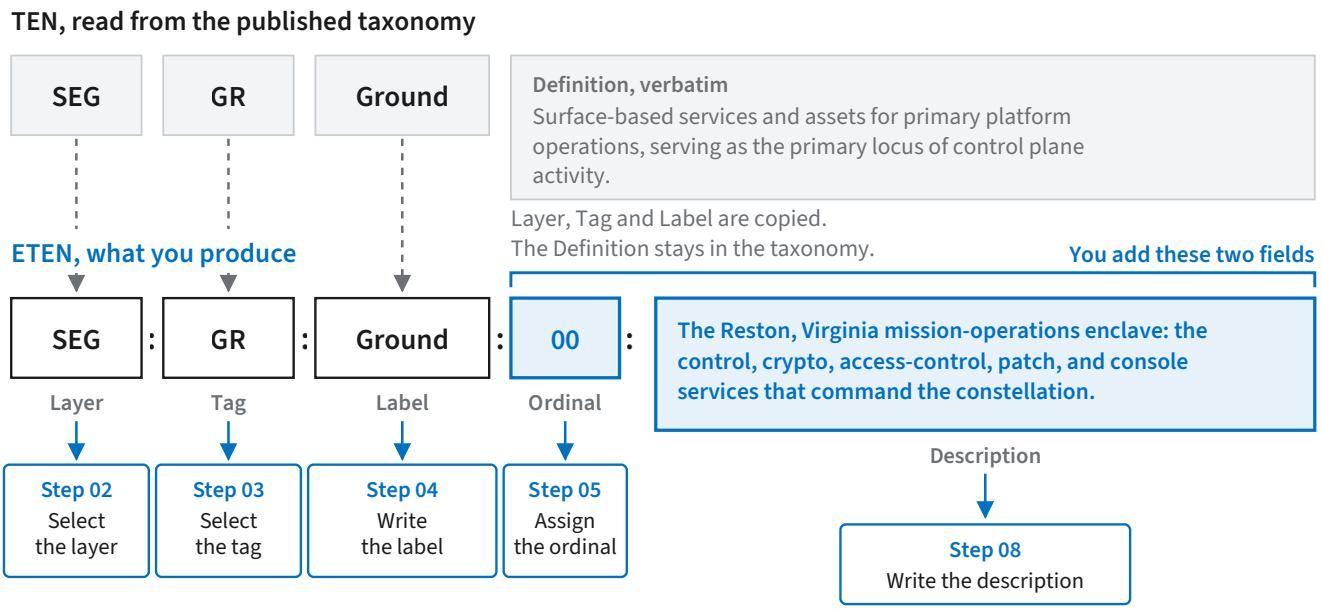
Kestrel Orbital's Reston mission-operations ground segment, written out as a five-field enumerated element:

Field	Value
LAYER	**SEG**
TAG	**GR**
LABEL	Ground
ORDINAL	**00**
DESCRIPTION	The Reston, Virginia mission-operations enclave: the control, crypto, access-control, patch, and console services that command the constellation.

Read together: **SEG:GR:Ground:00:The Reston, Virginia mission-operations enclave: the control, crypto, access-control, patch, and console services that command the constellation.** Its PARENT names the environment it operates in, **PCE:TE:Terrestrial:00**, the Reston site, which was enumerated first: every parent is enumerated before the child that names it.

© 2026 ethicallyHackingspace (eHs)®

Figure 4 Anatomy of an ETEN: two fields added to the TEN, each field set by one step



Step 06 · Link the parent

PARENT PCE:TE:Terrestrial:00, the Reston site, enumerated first: every parent is enumerated before the child that names it. The parent governs the record but does not print inside the five fields.

Read it as the TEN supplying three fields and you supplying two. The parent is linked at Step 06 and governs the record without printing inside the five fields.

The canonical-description rule. One identifier carries exactly one description, everywhere it appears: workbook, detection, ticket, diagram. **PCE:OR:Orbital:00** is the geostationary regime, and its one description is: “The geostationary orbit regime (~35,786 km) part of the fleet flies in, fixing its coverage geometry, contact windows, and radiation exposure.” A teaching example that needs a different description uses a different ordinal or a platform outside the deliverable. The description is a required, scoping field of the record, so two descriptions on one identifier would be two different records wearing the same name.

© 2026 ethicallyHackingspace (eHs)®

CH 5 The ETEN Process, Once, Then the Deltas

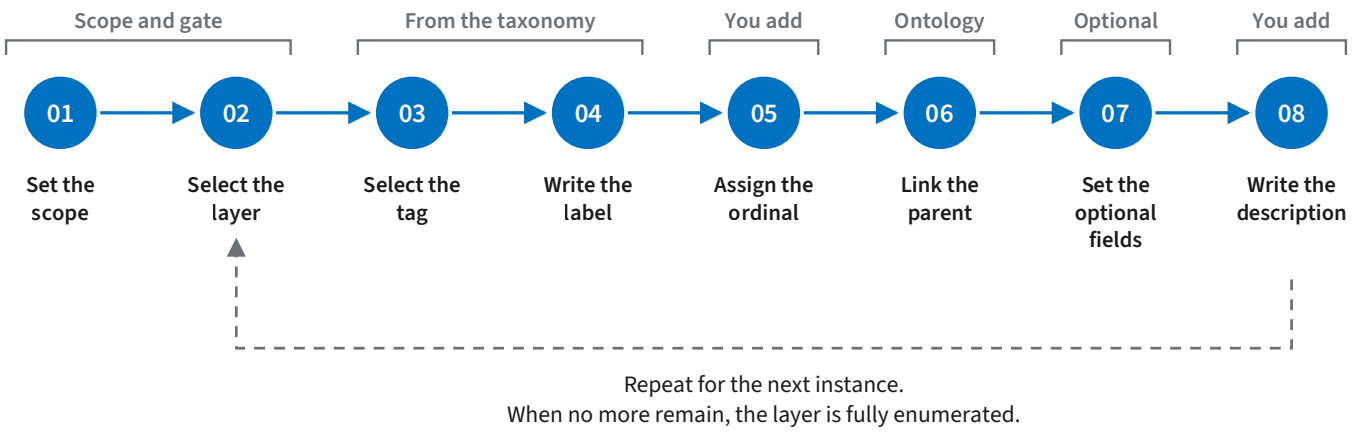
> "Eight steps, fixed order. The frame repeats for each layer; only the input, the parent rule, and the scope change."

The normative ETEN Process is printed once below, in full, as it is applied at the PCE layer, the first walk. After it come the three per-layer deltas, side by side, so the one thing each layer changes reads as the headline instead of being buried in identical framing.

Key points

- Eight steps, fixed order, at every layer.
- From layer to layer only the gate, the tags in scope, the parent rule and the optional field change.
- Every parent is enumerated before the child that names it.

Figure 5 The ETEN Process: eight steps in fixed order, repeated for every instance



The normative ETEN Process · eight steps, fixed order · applied at the PCE layer

1. **Set the SCOPE.** From the resilience objective and the requirements that drive the decomposition: the command-and-control mission the three mandates hold Kestrel Orbital to, Executive Order 14144, the NIS2 Directive and the Space ISAC alert on a confirmed command-and-control attack, giving the Day-1 CONOPS its scope, the telecommand path. An element outside the scope is not enumerated.
2. **Select the LAYER.** Working top down, the first structural layer is PCE. The gate is the layer definition, verbatim: *"Operational zone in which a capability primarily exists or is exercised."* You are naming a WHERE, a zone, not a thing in it. Zone means PCE; a group of services and assets means SEG. An element that fails the gate is reclassified, not forced through.

© 2026 ethicallyHackingspace (eHs)®

3. **Select the TAG.** From the taxonomy for this layer: **TE**, **AQ**, **AE**, **OR**, **DS**. Never invent one. On the telecommand path the Step 01 scope admits **TE** and **OR**.
4. **Write the LABEL.** The third field of the published TEN for the selected tag: Terrestrial (TE), Aquatic (AQ), Aerial (AE), Orbital (OR), or Deep Space (DS).
5. **Assign the ORDINAL.** Two digits from **00**, counted per TAG. Two terrestrial sites become **PCE:TE:Terrestrial:00** and **PCE:TE:Terrestrial:01**; the two orbital regimes become **PCE:OR:Orbital:00** and **PCE:OR:Orbital:01**.
6. **Link the PARENT.** PCE is the root of the ontology: it takes no PARENT. Every SEG enumerated next names one or more of these environments, so parents exist before children.
7. **Set the OPTIONAL FIELDS.** None at this layer. DISTRIBUTED belongs to services, SUBSYSTEM to assets; TARGET and SOURCE belong to the analytic elements of Functions 02 through 05.
8. **Write the DESCRIPTION.** One plain sentence for this exact instance, written at its own layer: the operational zone, its location, role, and jurisdiction. The Step 02 gate applies again here; a zone described as the things inside it is non-compliant.

Repeat for the next instance. When no more remain, the layer is fully enumerated.

The same eight steps, in the same fixed order, run at every layer. What follows is everything that actually changes.

The SEG delta

The delta. Segments add the first PARENT links: every element names at least one PCE above it; three SEG tags in scope.

Whose input. The environments are already enumerated. With the Security Operations Center, the two build-and-operate departments scoped the enclaves on the telecommand path: three SEG tags, Space and Link (the command path from uplink to execution on orbit) and Ground (the ground-based infrastructure NIS2 binds); SEG-US, the customer edge, is a taxonomic element that is out of scope for this platform, so it is not enumerated. **Output.** One ETEN of the form **SEG:TAG:LABEL:ORDINAL:Description** per enclave. **Constraints.** Every SEG element names at least one PCE in PARENT at Step 06; existing segment diagrams were imported and tagged rather than redrawn. **Review.** Confirm each SEG element names its PCE elements in PARENT before presenting.

Step	What changes at SEG
02 Gate	The layer definition, verbatim: *"Service and asset enclaves that compose the system across environments."* You are naming an ENCLAVE, a grouping of services and assets, not the zone it sits in and not the hardware inside it.
03 Tag	Ten published tags; the Step 01 scope admits **SP**, **LI**, and **GR**.
05 Ordinal	The Reston and Kiruna ground enclaves become **SEG:GR:Ground:00** and **SEG:GR:Ground:01**.
06 Parent	One or more PCE ETENs already enumerated. **SEG:GR:Ground:00** names its terrestrial site, **PCE:TE:Terrestrial:00**; **SEG:SP:Space:00** spans both regimes and names **PCE:OR:Orbital:00, PCE:OR:Orbital:01**.

© 2026 ethicallyHackingspace (eHs)®

Step	What changes at SEG
07 Optional	None at this layer.
08 Description	The enclave of services and assets, its role, the site or regime it occupies, redundancy posture, and the interfaces it exposes. An enclave described as the hardware inside it is non-compliant.

The SVC delta

The delta. Services can span segments: one element, DISTRIBUTED Y, every participating SEG in PARENT.

Whose input. The segments are already enumerated. Satellite Operations named the services it runs and Satellite Design & Engineering the services it built: on the telecommand path, the fifteen services that authorize, encrypt, carry, and execute commands, including the cryptography and Access Control and Authentication (ACA) services the mandates' duties land on. **Output.** One ETEN of the form **SVC:TAG:LABEL:ORDINAL:Description** per service. **Constraints.** Cross-segment services list every participating SEG in PARENT at Step 06, set **DISTRIBUTED** to Y at Step 07, and stay one service element, not duplicates. **Review.** Confirm the function each service delivers before presenting; naming the function, not the device, is what lets the Security Operations Center write detections that survive a hardware refresh.

Step	What changes at SVC
02 Gate	The layer definition, verbatim: *"Functional planes that organize control and data responsibilities."* You are naming a functional RESPONSIBILITY, what the platform does, not what it is built from.
03 Tag	Three published tags: **CP**, **DP**, **HY**, matching the responsibility the service carries.
05 Ordinal	Counted per TAG across the whole layer, continuing across segments: **SVC:CP:Control Plane:00** and **SVC:DP:Data Plane:00** coexist; a second control-plane service is **SVC:CP:Control Plane:01**.
06 Parent	One or more SEG ETENs. A cross-segment service lists every participating segment and stays one element, not duplicates.
07 Optional	**DISTRIBUTED**: Y when PARENT lists two or more segments, N when the service runs on a single segment.
08 Description	The functional responsibility, beginning "The service that …". A service described as the device it runs on is non-compliant.

The AST delta

The delta. Assets take one or more SVC parents each, and an asset splits and takes the next ordinal wherever owner, build or patch path diverges.

Whose input. The services are already enumerated. Satellite Design & Engineering supplied the concrete assets from its inventory lists: on the telecommand path, the twenty-one hardware, software, firmware, data, and signal assets that implement the command-path services, ACA software and credentials among them. **Output.** One ETEN of the form **AST:TAG:LABEL:ORDINAL:Description** per element. **Constraints.** Every AST element names at least one SVC in PARENT at Step 06, never zero, and every service a shared asset actually carries; physical units that share an owner, a build and a patch path are one element, and where any of those diverge the element splits and takes the next ordinal, so a finding resolves to

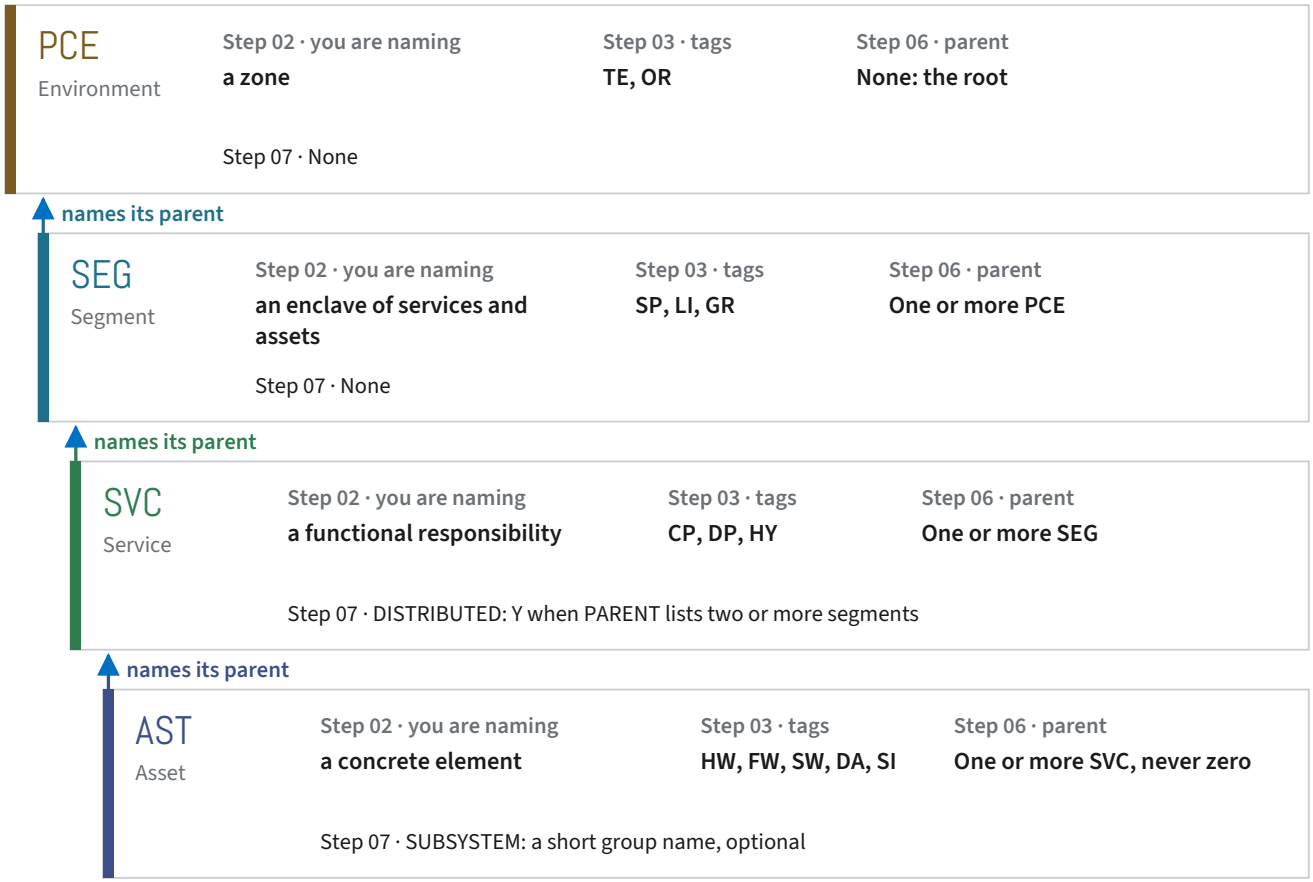
© 2026 ethicallyHackingspace (eHs)®

exactly one element. **Review.** Confirm each AST element names its SVC elements in PARENT before presenting; this is the resolution at which a patch lands and a detection that names one concrete element fires, and where all three departments converge.

Step	What changes at AST
02 Gate	The layer definition, verbatim: *"Asset classes composing the system and its interfaces."* You are naming a CONCRETE ELEMENT, a real component the platform is built from.
03 Tag	Six published tags: **HW**, **FW**, **SW**, **DA**, **SI**, **HY**, matching the category of the concrete element.
05 Ordinal	A distinct ordinal for every asset element. Physical units that share an owner, a build and a patch path are one element; where any of those diverge, the element splits and takes the next ordinal.
06 Parent	One or more SVC ETENs, never zero: every service the asset carries (for example, **AST:SW:Software:00** names **SVC:CP:Control Plane:00**). An asset that carries several services names each one; the element total is unchanged, because it counts records, not parent links.
07 Optional	**SUBSYSTEM**, optional: a short free-text group name reused verbatim on every asset in one coherent group (an antenna plus its controller plus its tracking software). Otherwise leave blank.
08 Description	One plain sentence beginning with the element class: "The physical …", "The embedded …", "The flight software …", "The stored …", "The transmitted …". Include make, model, or version where applicable.

© 2026 ethicallyHackingspace (eHs)®

Figure 6 What changes at each layer: the parent chain the process builds



Read it as a ladder: each layer names its parent in the layer above, so the chain from any asset reaches the environment it operates in.

In every walk, at every layer, the constants are the same: eight steps in fixed order, tags read from the published taxonomy and never invented, the Step 02 gate applied twice (once selecting the layer, again writing the description), and the loop line: repeat for the next instance until none remain.

© 2026 ethicallyHackingspace (eHs)®

Part III **The deliverable**

The complete telecommand decomposition, element by element, and what changes in the Security Operations Center once the taxonomy is deployed.

CH 6 The Telecommand Decomposition, Complete

> "The deliverable. Four PCE elements, four SEG elements, fifteen SVC elements, and twenty-one AST elements: forty-four ETENs in canonical syntax, every PARENT field populated below the root, one taxonomy and one parent chain all three departments record against, ready to present and carry into Day 2."

Every element of the Day-1 CONOPS, layer by layer, with its identifier, canonical description, parent, and source reference. This chapter is the full catalog. The full ETEN of any row is its identifier joined to its description: **LAYER:TAG:LABEL:ORDINAL:Description**.

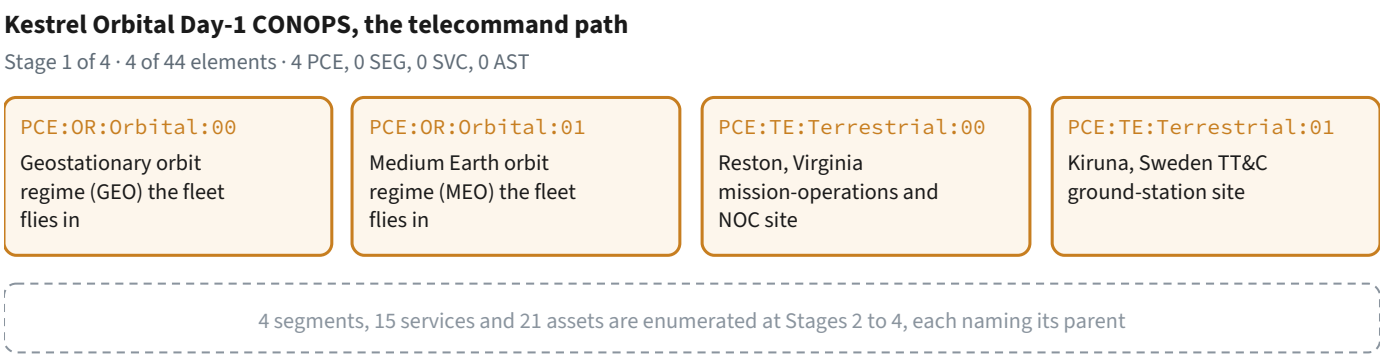
PCE	SEG	SVC	AST
4	4	15	21
Environments	Segments	Services	Assets

Acronyms in the tables. ADCS, Attitude Determination and Control System. ACA, Access Control and Authentication. C&DH, Command and Data Handling. EPS, Electrical Power System. TCS, Thermal Control System. OBC, On-Board Computer. OBDH, On-Board Data Handling. HSM, Hardware Security Module. FEC, Forward Error Correction. ECC, Error-Correcting Code. FDIR, Fault Detection, Isolation, and Recovery. TT&C, Telemetry, Tracking, and Command. T2, Tracking and Telemetry. NOC, Network Operations Center. RF, Radio Frequency. GEO, Geostationary Earth Orbit. MEO, Medium Earth Orbit.

© 2026 ethicallyHackingspace (eHs)®

6.1 · PCE, 4 elements

Figure 7 Stage 1 of 4 · 4 of 44 elements · environments only



PCE is the root layer: these four elements name no parent.

Four environments, and nothing under them yet. The dashed line counts what Stages 2 to 4 add; those elements exist on the platform and are not enumerated yet.

Why only four environments. Kestrel operates in these four places today. This pass enumerates the telecommand path, so it enumerates the environments that path crosses and no others. The taxonomy still carries Aquatic, Aerial and Deep Space, and they take ordinals the day the business flies there. Enumerating an environment the platform does not use would be padding, and padding is what makes a model impossible to maintain.

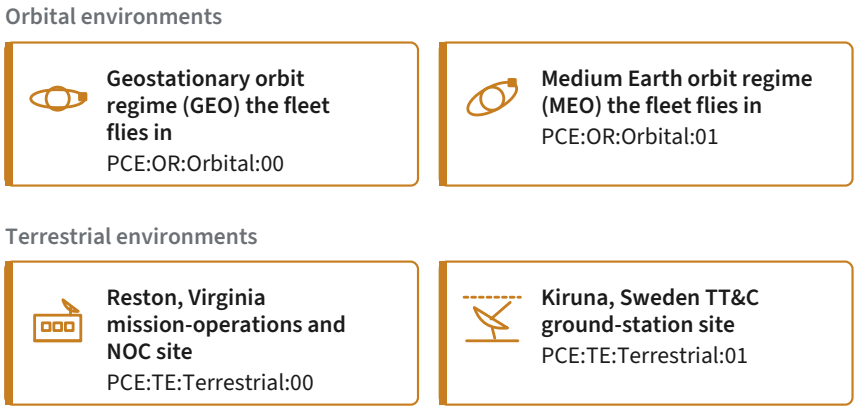
SCOR convenes the departments that own where the platform lives: Satellite Operations, which flies the constellation, and Satellite Design & Engineering, which built it, with the Security Operations Center sitting in. The room finds two distinct terrestrial sites and two orbital regimes, so Terrestrial takes two ordinals and Orbital takes two. PCE is the only layer with no parent: these four elements are the roots every other element in the CONOPS resolves to through the parent chain.

Identifier	Element	Canonical description	Parent	Reference
PCE:OR:Orbital:00	Geostationary orbit regime (GEO) the fleet flies in	The geostationary orbit regime (~35,786 km) part of the fleet flies in, fixing its coverage geometry, contact windows, and radiation exposure.	none (root)	METEORSTORM taxonomy (MISP, v2); NIST IR 8270
PCE:OR:Orbital:01	Medium Earth orbit regime (MEO) the fleet flies in	The medium Earth orbit regime, where part of the fleet flies at ~8,000 km, with its own orbital periods, contact windows, and radiation environment.	none (root)	METEORSTORM taxonomy (MISP, v2); NIST IR 8270

© 2026 ethicallyHackingspace (eHs)®

Identifier	Element	Canonical description	Parent	Reference
PCE:TE:Terrestrial:00	Reston, Virginia mission-operations and NOC site	The Reston, Virginia land site: the terrestrial zone of primary mission operations and the network operations center.	none (root)	METEORSTORM taxonomy (MISP, v2); NIST IR 8401
PCE:TE:Terrestrial:01	Kiruna, Sweden TT&C ground-station site	The Kiruna, Sweden land site (67.9°N): the terrestrial zone of the polar TT&C ground station that carries the command path into the link.	none (root)	METEORSTORM taxonomy (MISP, v2); NIST IR 8401

Figure 8 The four environments as icons: the roots of the parent chain



Root elements: a PCE takes no parent.

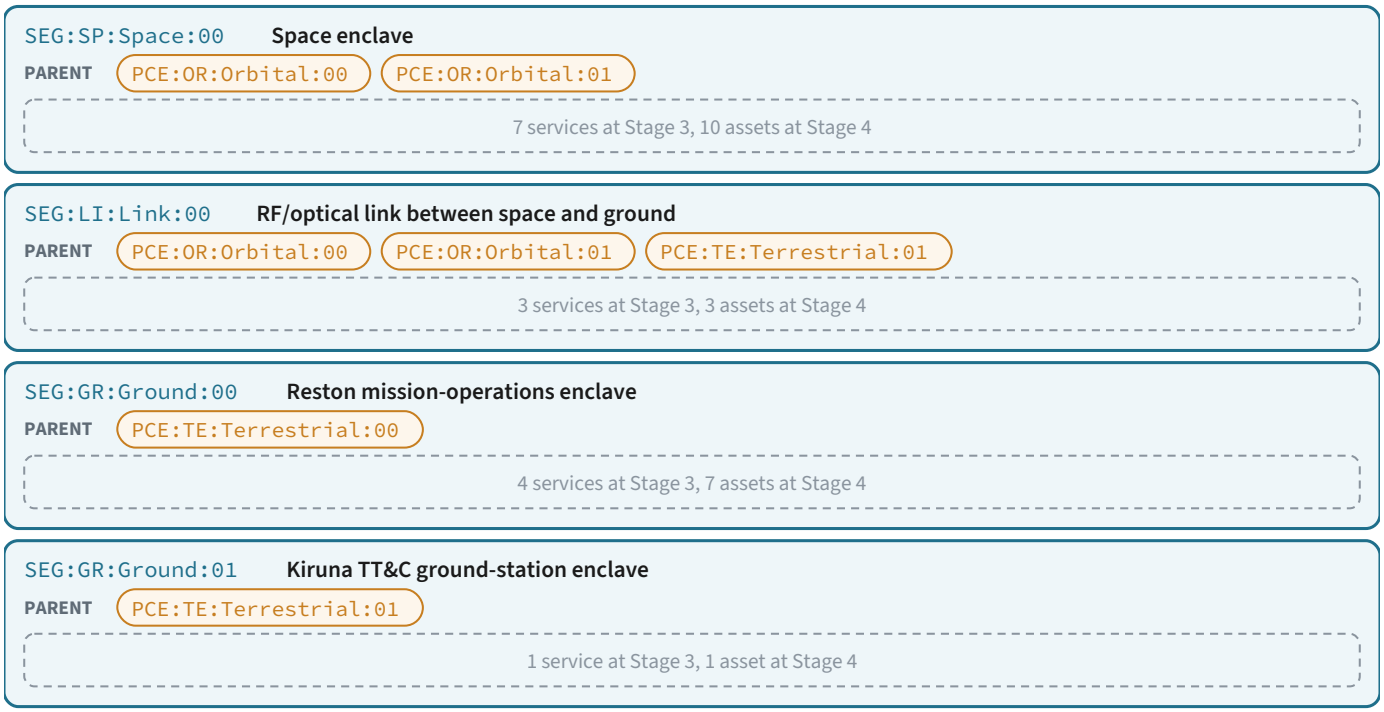
Field note

Satellite Operations wanted one orbital entry; Satellite Design & Engineering needed per-regime enrichment, because a GEO spacecraft and a MEO spacecraft do not share space weather. Ruling: one PCE per regime, two ordinals. First win: radiation and conjunction context is now recorded against the correct regime instead of averaged across the fleet.

© 2026 ethicallyHackingspace (eHs)®

6.2 · SEG, 4 elements

Figure 9 Stage 2 of 4 · 8 of 44 elements · environments and segments



Each band is one segment; its PARENT pills are the environments it names.

Four SEG elements name the environments in PARENT. Each band is one segment, and its PARENT pills are the environments it names. The Link segment names three, both orbital regimes and Kiruna, because the radio link runs from the Kiruna antenna to the fleet in both regimes.

Why four segments and not more. A real operator has segments this pass does not touch: user terminals, a corporate estate, a launch chain. They are out because the command path does not run through them, not because they are safe. SEG-US, the User segment, is in the taxonomy and deliberately unenumerated here, which is the honest way to record a boundary.

The room traces the actual command flow: an operator originates a command at a console, mission operations authorizes it on the Ground, the Link carries it as an RF or optical signal, and the spacecraft executes it in Space. Four enclaves are enumerated on the path; SEG-US, the customer edge, is a taxonomic element that is out of scope for this platform, and

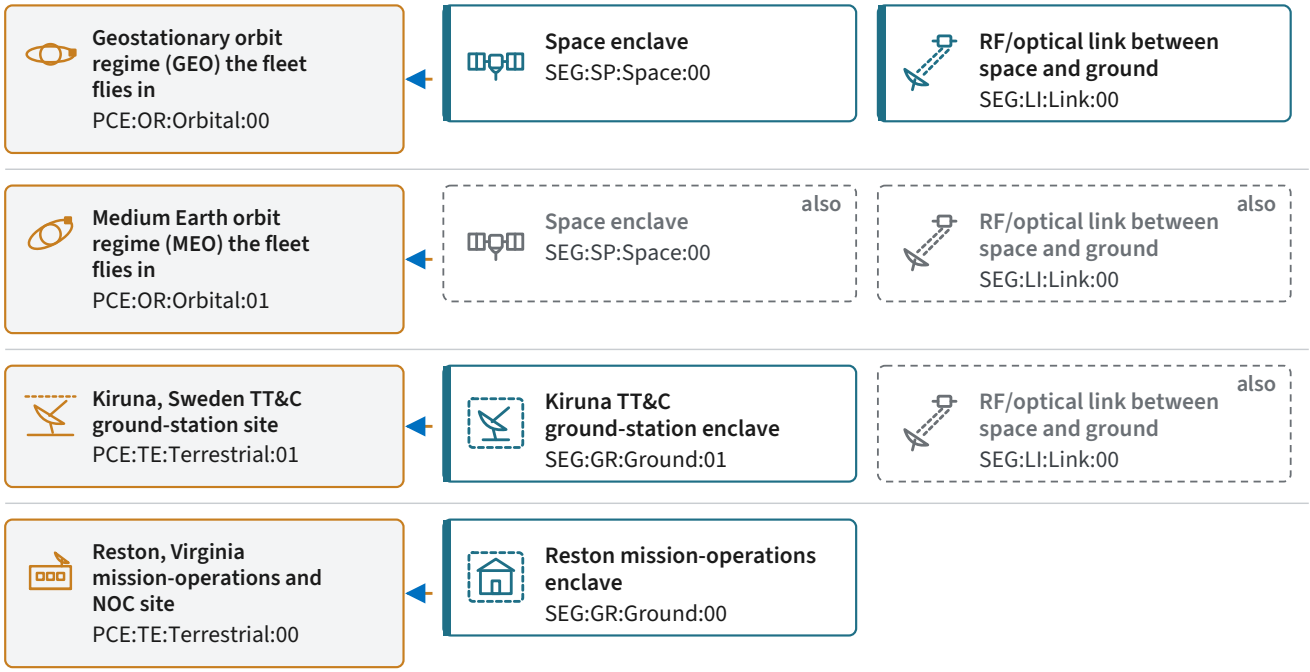
© 2026 ethicallyHackingspace (eHs)®

Launch and the physical regimes AQ, LO, HI, NE, and DE drop out at Step 01. Two hops of that flow have no element on this pass: the transport between the Reston and Kiruna sites, and the receipt of the uplink on board. Both are held outside this first pass, like the services and assets behind the ordinal gaps.

Identifier	Element	Canonical description	Parent	Reference
SEG:SP:Space:00	Space enclave	The on-orbit enclave: the flight services and their assets operating on the constellation spacecraft, beyond physical reach.	PCE:OR:Orbital:00, PCE:OR:Orbital:01	NIST IR 8270
SEG:LI:Link:00	RF/optical link between space and ground	The link enclave: the services and assets carrying telecommand up and telemetry and mission data down across the RF and optical signal path between space and ground.	PCE:OR:Orbital:00, PCE:OR:Orbital:01, PCE:TE:Terrestrial:01	NIST IR 8270; CCSDS 232.0-B
SEG:GR:Ground:00	Reston mission-operations enclave	The Reston, Virginia mission-operations enclave: the control, crypto, access-control, patch, and console services that command the constellation.	PCE:TE:Terrestrial:00	NIST IR 8270; NIST IR 8401
SEG:GR:Ground:01	Kiruna TT&C ground-station enclave	The Kiruna, Sweden polar TT&C ground-station enclave: the ground terminal service and its antenna and RF front end that radiate the command path into the link.	PCE:TE:Terrestrial:01	ESA/SSC Esrange-Kiruna documentation; NIST IR 8401

© 2026 ethicallyHackingspace (eHs)®

Figure 10 The four segments as icons, each beside the environments it names in PARENT



Arrows point to the parent named in PARENT. A dashed card marked “also” is an element drawn in full under its first parent.

Field note

Two orbital environments, one Space segment: the fleet flies as one commanded constellation, and splitting every flight service per regime would have doubled the inventory before any enrichment required it. Plan of record: track the SDA (space domain awareness) to measure what is MEO-specific versus GEO-specific, then build the longer-term plan to coordinate enumerating the entire platform.

The **User** segment (taxonomic element **SEG-US-User**) remains part of the METEORSTORM data model but is **out of scope for this platform**, so it is not enumerated in the Kestrel CONOPS. Example ETEN syntax, for reference only: **SEG:US:User:00**.

© 2026 ethicallyHackingspace (eHs)®

6.3 · SVC, 15 elements

Figure 11 Stage 3 of 4 · 23 of 44 elements · services added

Kestrel Orbital Day-1 CONOPS, the telecommand path

Stage 3 of 4 · 23 of 44 elements · 4 PCE, 4 SEG, 15 SVC, 0 AST

SEG:SP:Space:00 Space enclave

PARENT PCE:OR:Orbital:00 PCE:OR:Orbital:01

- **ADCS** — SVC:CP:Control Plane:00 — 3 assets at Stage 4
- **C&DH** — SVC:HY:Hybrid:00 — 3 assets at Stage 4
- **Comms** — SVC:DP:Data Plane:00 — 1 asset at Stage 4
- **Crypto (Space)** — SVC:CP:Control Plane:01 — 1 asset at Stage 4
- **EPS** — SVC:CP:Control Plane:02 — 1 asset at Stage 4
- **TCS** — SVC:CP:Control Plane:04 — 1 asset at Stage 4
- **Attack Detection / Recovery** — SVC:CP:Control Plane:06 — 2 assets at Stage 4

SEG:LI:Link:00 RF/optical link between space and ground

PARENT PCE:OR:Orbital:00 PCE:OR:Orbital:01 PCE:TE:Terrestrial:01

- **ACA (Link)** — SVC:CP:Control Plane:05 — 1 asset at Stage 4
- **Error Handling (FEC/ECC)** — SVC:HY:Hybrid:01 — 1 asset at Stage 4
- **T2 (Tracking & Telemetry)** — SVC:HY:Hybrid:02 — 1 asset at Stage 4

SEG:GR:Ground:00 Reston mission-operations enclave

PARENT PCE:TE:Terrestrial:00

- **Crypto (Ground)** — SVC:CP:Control Plane:08 — 1 asset at Stage 4
- **ACA (Ground)** — SVC:CP:Control Plane:09 — 2 assets at Stage 4
- **Patch Updates** — SVC:CP:Control Plane:12 — 2 assets at Stage 4
- **Satellite Console** — SVC:CP:Control Plane:13 — 2 assets at Stage 4

SEG:GR:Ground:01 Kiruna TT&C ground-station enclave

PARENT PCE:TE:Terrestrial:01

- **Ground Terminal (antenna / RF)** — SVC:HY:Hybrid:03 — 1 asset at Stage 4

Each band is one segment; its PARENT pills are the environments it names.

© 2026 ethicallyHackingspace (eHs)®

Fifteen SVC elements, each naming its segment in PARENT. The count on each service is the assets that name it in PARENT at Stage 4. **AST:HW:Hardware:06** names three services and is counted under each, so the per-service counts add up to more than the segment's assets; the Stage 4 figure marks it with an asterisk.

Why fifteen services. Three departments in one room, working a fixed time box, resolved the command path to fifteen services. A second pass would find more, and would split some of these where a distinct owner or a distinct patch path appears. Fifteen is the count this scoped pass resolved; the ordinal gaps record the services held outside this scope.

Satellite Operations named the services it runs and Satellite Design & Engineering the services it built. Ordinals continue across segments inside each tag, so no ordinal repeats anywhere in the layer: Space holds Control Plane 00, 01, 02, 04 and 06, Data Plane 00 and Hybrid 00; the Link holds Control Plane 05 and Hybrid 01 and 02; the Ground holds Control Plane 08, 09, 12 and 13 and Hybrid 03. Control Plane 03, 07, 10 and 11 are services the register tracks outside this scope. All fifteen run inside a single segment, so DISTRIBUTED is N for each.

SEG:SP:Space:00

Space segment services, 7

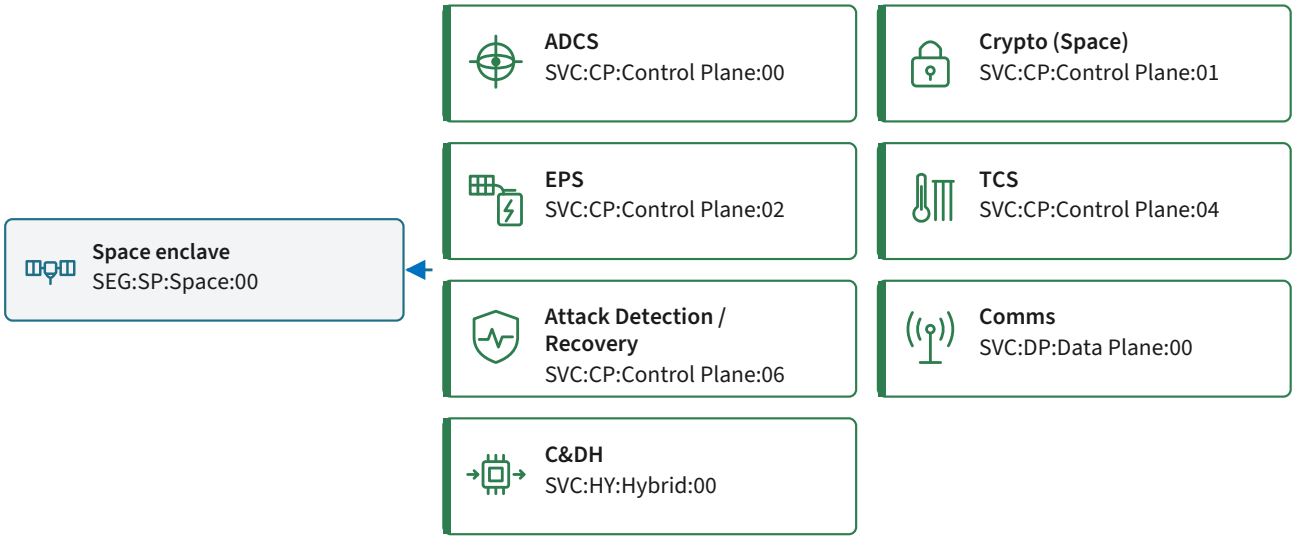
The space segment's job for telecommand: keep the vehicle alive on orbit, accept commands, execute and route them, detect hostile manipulation on board, and return telemetry to the ground. Five control-plane (ADCS, space crypto, EPS, thermal, attack detection and recovery), one data-plane (comms) and one hybrid (C&DH). The data-plane service is enumerated on this pass because it carries telemetry to the ground; the payload chain is not enumerated here.

Identifier	Service	Canonical description	Parent	Reference
SVC:CP:Control Plane:00	ADCS	The service that determines and controls spacecraft orientation (ADCS).	SEG:SP:Space:00	NASA/ESA ADCS
SVC:CP:Control Plane:01	Crypto (Space)	The service that encrypts and authenticates on board, including telecommand authentication (Crypto, space).	SEG:SP:Space:00	NIST SP 800-57; Falco et al. 2024
SVC:CP:Control Plane:02	EPS	The service that generates, stores, and distributes electrical power (EPS).	SEG:SP:Space:00	NASA SST (Power)
SVC:CP:Control Plane:04	TCS	The service that holds every component within its temperature limits (TCS).	SEG:SP:Space:00	NASA SST (Thermal)
SVC:CP:Control Plane:06	Attack Detection / Recovery	The service that detects hostile command or state manipulation on board and recovers from it.	SEG:SP:Space:00	NIST IR 8270; Falco et al. 2024

© 2026 ethicallyHackingspace (eHs)®

Identifier	Service	Canonical description	Parent	Reference
SVC:DP:Data Plane:00	Comms	The service that carries telemetry to the ground (Comms).	SEG:SP:Space:00	CCSDS 132.0-B; NIST IR 8270
SVC:HY:Hybrid:00	C&DH	The service that executes commands and moves data across the vehicle, on both the control and data planes (C&DH).	SEG:SP:Space:00	ESA OBDH

Figure 12 The Space segment's services as icons, beside the segment they name



Arrows point to the parent named in PARENT.

Field note

One C&DH, one EPS, one ADCS entry serves both fleets by the scoping decision. Ordinals count per TAG and survive re-parenting, so if SDA tracking later justifies a per-regime split, every identifier keeps its name; only PARENT fields change. Win: Security Operations and Engineering stopped keeping two names for the same flight function.

© 2026 ethicallyHackingspace (eHs)®

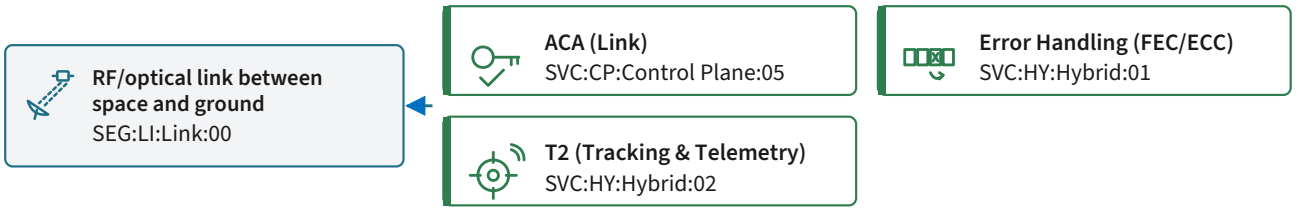
SEG:LI:Link:00

Link segment services, 3

The link segment's job for telecommand: authenticate inbound commands, correct bit errors, and run tracking and telemetry.

Identifier	Service	Canonical description	Parent	Reference
SVC:CP:Control Plane:05	ACA (Link)	The service that authenticates command sources and enforces command acceptance on the uplink (ACA, link).	SEG:LI:Link:00	Falco et al. 2024; NIST SP 800-57
SVC:HY:Hybrid:01	Error Handling (FEC/ECC)	The service that detects or corrects bit errors on the link (FEC/ECC error handling).	SEG:LI:Link:00	CCSDS 231.0-B
SVC:HY:Hybrid:02	T2 (Tracking & Telemetry)	The service that tracks the vehicle and returns telemetry across the control loop and the data path (T2).	SEG:LI:Link:00	CCSDS TT&C

Figure 13 The Link segment's services as icons, beside the segment they name



Arrows point to the parent named in PARENT.

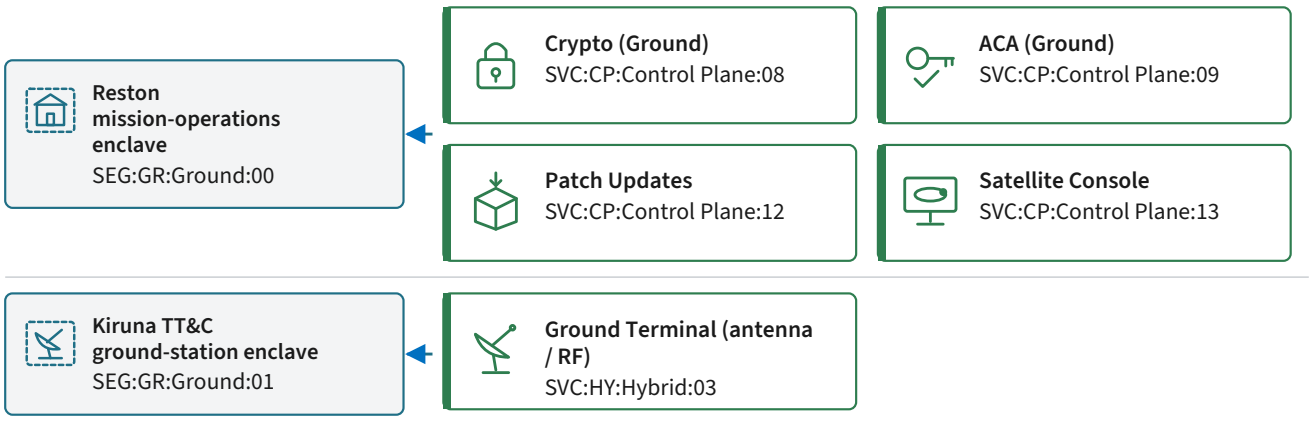
SEG:GR:Ground:00 · SEG:GR:Ground:01

Ground segment services, 5 (4 Reston + 1 Kiruna)

The ground segment's job for telecommand: command protection, command authorization, patch delivery, and the operator console at Reston, and the RF ground terminal at Kiruna. Four control-plane services hold command authority at Reston; the Kiruna enclave holds the radio.

Identifier	Service	Canonical description	Parent	Reference
SVC:CP:Control Plane:08	Crypto (Ground)	The service that protects commands before uplink and data after downlink (Crypto, ground).	SEG:GR:Ground:00	NIST SP 800-57
SVC:CP:Control Plane:09	ACA (Ground)	The service that decides who may command and which commands are released to the link (ACA, ground).	SEG:GR:Ground:00	Falco et al. 2024; NIST SP 800-57
SVC:CP:Control Plane:12	Patch Updates	The service that delivers and installs software and firmware updates under control (Patch Updates).	SEG:GR:Ground:00	NIST SP 800-40
SVC:CP:Control Plane:13	Satellite Console	The service that gives operators the mission-ops console: telemetry monitoring and command issue.	SEG:GR:Ground:00	NIST IR 8401
SVC:HY:Hybrid:03	Ground Terminal (antenna / RF)	The service that transmits the command uplink and receives the downlink at the Kiruna ground station (RF ground terminal).	SEG:GR:Ground:01	NIST IR 8401; CCSDS TT&C

Figure 14 The Ground segments' services as icons, beside the segment each names



Arrows point to the parent named in PARENT.

Field note

Four control-plane services hold command authority at Reston; the Kiruna enclave holds the radio. The PARENT step made the meeting state on the record which enclave actually radiates, a question that had lived in hallway knowledge until it had an identifier to be recorded against. Win: failover and jurisdiction analysis now cite enclaves, not buildings. Ground ACA (**SVC:CP:Control Plane:09**) is a separate element from ACA on the link (**SVC:CP:Control Plane:05**) even though the two share a role, because each is authored and runs on its own segment.

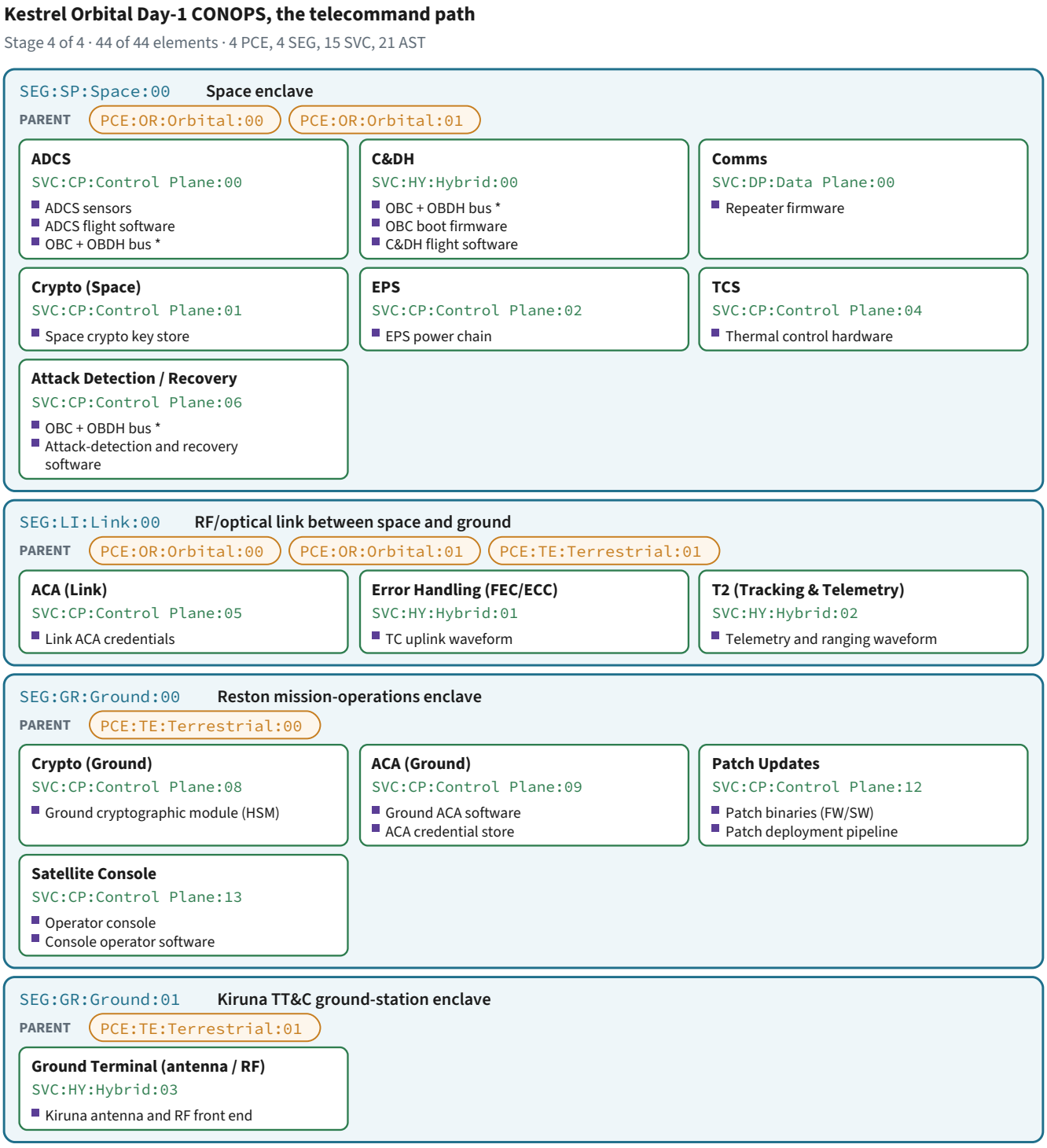
6.4 · AST, 21 elements

Satellite Design & Engineering supplied the concrete assets from its inventory lists and console inventories. Every asset names every service it carries in PARENT, at least one; ordinals continue per tag across the whole platform, so a finding resolves to exactly one element: Hardware holds 00, 01, 03, 04, 05, 06 and 08, Software 00 and 02 to 06, Firmware 01 and 02, Data 00 to 03, and Signal 00 and 01. Hardware 02 and 07, Software 01 and Firmware 00 are assets the register tracks outside this scope, so the next free Hardware ordinal is 09. This is the resolution at which a patch lands and a detection that names one concrete element fires.

What this is, and what it is not. This is a complete, parented decomposition *of the telecommand path*, not a complete model of Kestrel Orbital. It is a first pass on one platform under a real time constraint. Some assets group several physical units where those units share an owner, a build and a patch path; where any of those diverge, the element splits and takes the next ordinal. The gaps in the ordinal sequence are elements the register still tracks outside this scope, and the transport between the Reston and Kiruna sites and the receipt of the uplink on board have no element yet. Say all of this out loud when you present it: a decomposition presented as finished invites a reviewer to find the missing thing, while one presented as a scoped first pass invites them to fund the next one.

© 2026 ethicallyHackingspace (eHs)®

Figure 15 Stage 4 of 4 · 44 of 44 elements · complete



Each band is one segment; its PARENT pills are the environments it names. * an asset that names more than one service is listed under each.

Twenty-one AST elements close every branch. Every enumerated element now resolves to a PCE through the parent chain.

© 2026 ethicallyHackingspace (eHs)®

SEG:SP:Space:00

Space segment assets, 10

Four Hardware, three Software, two Firmware, and one Data asset implement the seven flight services. The OBC boot code and the repeater's operating code live in non-volatile memory on a separate signing and uplink path, so they are Firmware, not Software.

Identifier	Asset	Canonical description	Parent	Reference
AST:FW:Firmware:01	OBC boot firmware	The embedded OBC boot firmware, the root of trust that runs first at power-on.	SVC:HY:Hybrid:00	NIST SP 800-193
AST:FW:Firmware:02	Repeater firmware	The embedded repeater firmware that governs receive, process, and retransmit on the link.	SVC:DP:Data Plane:00	NIST SP 800-193; CCSDS 232.0-B
AST:HW:Hardware:00	ADCS sensors	The physical attitude sensors: star trackers, sun sensors, gyros, magnetometers.	SVC:CP:Control Plane:00	NASA/ESA ADCS
AST:HW:Hardware:01	EPS power chain	The physical power chain: solar arrays, batteries, power distribution.	SVC:CP:Control Plane:02	NASA SST (Power)
AST:HW:Hardware:03	Thermal control hardware	The physical thermal hardware: heaters, radiators, coatings, insulation.	SVC:CP:Control Plane:04	NASA SST (Thermal)
AST:HW:Hardware:06	OBC + OBDH bus	The physical on-board computer and OBDH bus on each constellation spacecraft.	SVC:HY:Hybrid:00 + SVC:CP:Control Plane:00 + SVC:CP:Control Plane:06	ESA OBDH
AST:SW:Software:00	ADCS flight software	The flight software that runs the ADCS control algorithms.	SVC:CP:Control Plane:00	NASA cFS
AST:SW:Software:05	Attack-detection and recovery software	The flight software that detects hostile command or state manipulation in flight and recovers.	SVC:CP:Control Plane:06	NIST IR 8270; Falco et al. 2024

© 2026 ethicallyHackingspace (eHs)®

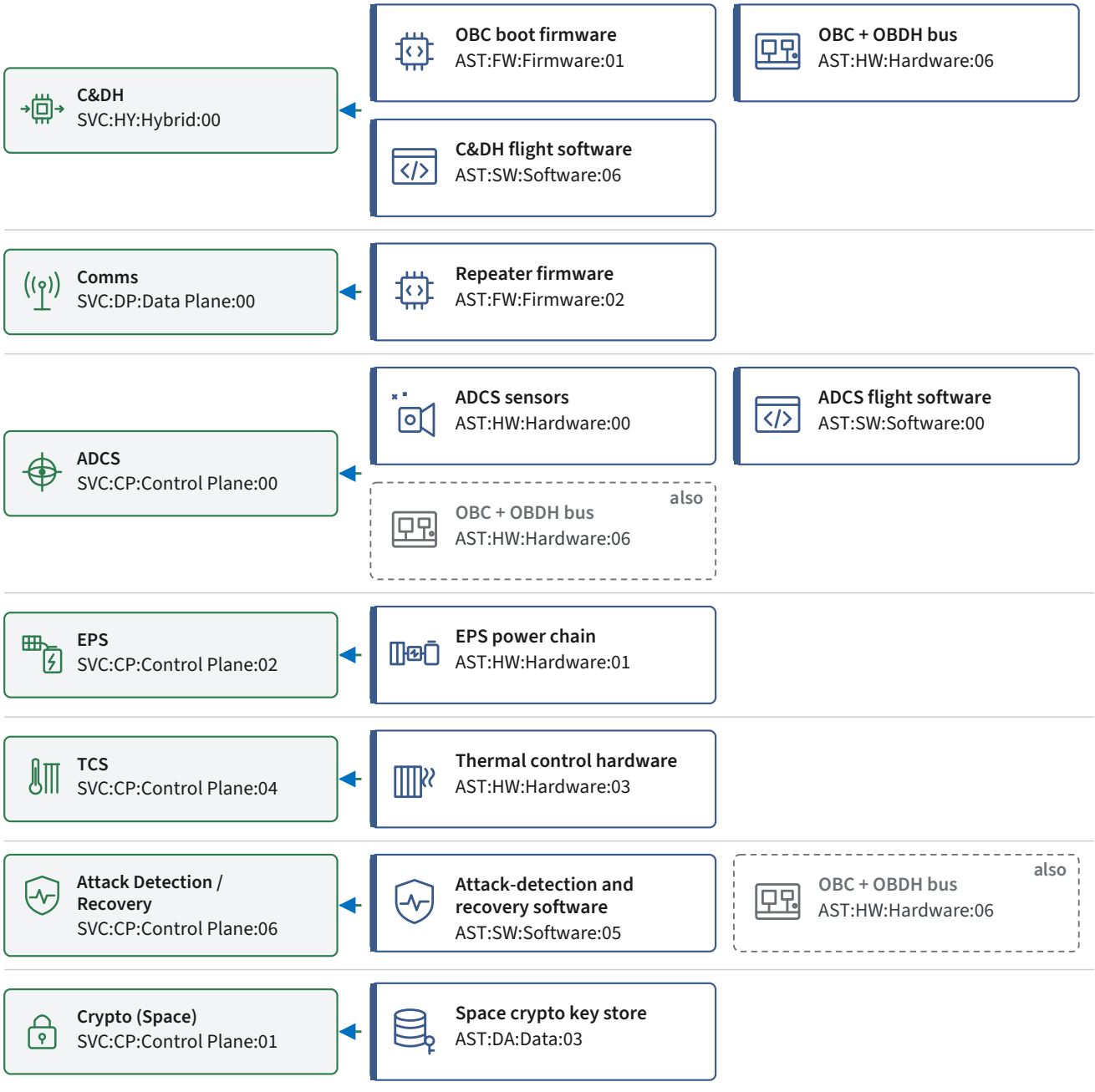
Identifier	Asset	Canonical description	Parent	Reference
AST:SW:Software:06	C&DH flight software	The flight software that executes commands and runs FDIR for C&DH.	SVC:HY:Hybrid:00	NASA cFS; ESA OBDH
AST:DA:Data:03	Space crypto key store	The stored flight keys and certificates the space cryptographic service encrypts and authenticates with.	SVC:CP:Control Plane:01	CCSDS 355.0-B (SDLS); CCSDS 357.0-B; NIST SP 800-57

Field note

A recommended SUBSYSTEM grouping, not yet recorded in the Day 1 inventory: a Bus group would gather the shared spacecraft bus so the inventory can be queried by physical subsystem regardless of which service each asset names in PARENT: the group gathers the on-board computer and data bus (**AST:HW:Hardware:06**), the C&DH flight software (**AST:SW:Software:06**), and the boot firmware (**AST:FW:Firmware:01**). One flight key store and one boot-firmware entry cover both fleets. Win: which binary on which spacecraft became one identifier instead of a meeting.

© 2026 ethicallyHackingspace (eHs)®

Figure 16 The space assets as icons, beside the service each names



Arrows point to the parent named in PARENT. A dashed card marked “also” is an element drawn in full under its first parent.

© 2026 ethicallyHackingspace (eHs)®

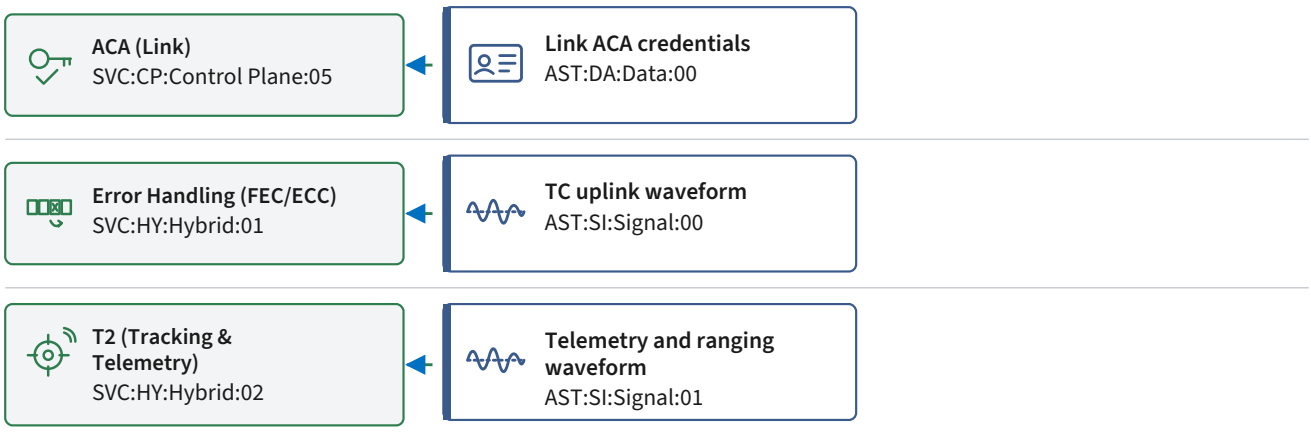
SEG:LI:Link:00

Link segment assets, 3

The stored credentials and the two waveforms. No asset here forms a physical subsystem group.

Identifier	Asset	Canonical description	Parent	Reference
AST:DA:Data:00	Link ACA credentials	The stored link ACA credentials the access-control service checks.	SVC:CP:Control Plane:05	NIST SP 800-57
AST:SI:Signal:00	TC uplink waveform	The transmitted telecommand uplink waveform that carries commands from ground to spacecraft.	SVC:HY:Hybrid:01	CCSDS 231.0-B; CCSDS 232.0-B
AST:SI:Signal:01	Telemetry and ranging waveform	The transmitted telemetry and ranging waveform: the modulated downlink signal, its framing, coding, and ranging tones.	SVC:HY:Hybrid:02	CCSDS 132.0-B (TM Space Data Link); CCSDS TT&C

Figure 17 The link assets as icons, beside the service each names



Arrows point to the parent named in PARENT.

© 2026 ethicallyHackingspace (eHs)®

SEG:GR:Ground:00 · SEG:GR:Ground:01

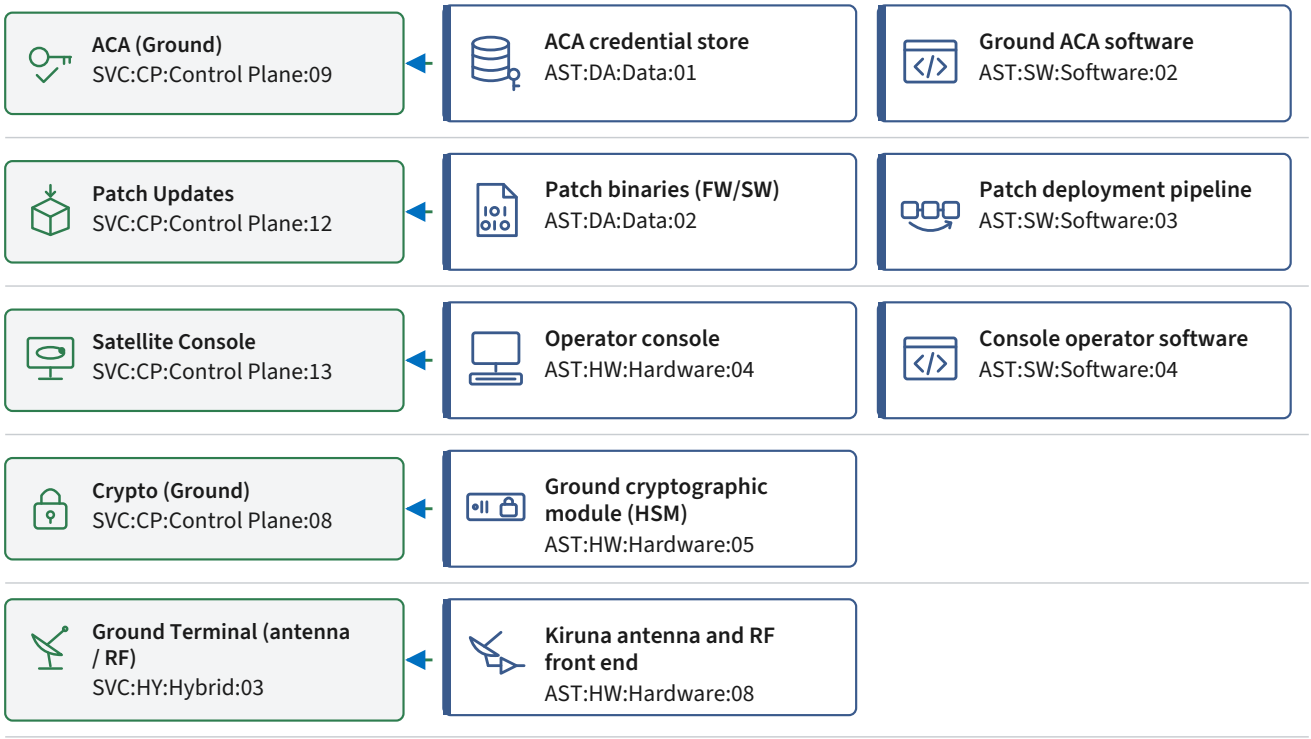
Ground segment assets, 8 (7 Reston + 1 Kiruna)

Three Software, two Data, and three Hardware assets: seven at Reston and the antenna and RF front end at Kiruna, each naming in PARENT the ground service it implements.

Identifier	Asset	Canonical description	Parent	Reference
AST:DA:Data:01	ACA credential store	The stored ACA credentials the ground authentication service relies on.	SVC:CP:Control Plane:09	NIST SP 800-57
AST:DA:Data:02	Patch binaries (FW/SW)	The stored patch binaries, firmware and software, staged for deployment.	SVC:CP:Control Plane:12	NIST SP 800-40; NIST SP 800-193
AST:SW:Software:02	Ground ACA software	The ground software that enforces command acceptance before release to the link (ACA).	SVC:CP:Control Plane:09	Falco et al. 2024; NIST SP 800-57
AST:SW:Software:03	Patch deployment pipeline	The software pipeline that builds, signs, distributes, and installs patches.	SVC:CP:Control Plane:12	NIST SP 800-40
AST:HW:Hardware:04	Operator console	The physical operator workstation from which telemetry is monitored and commands are issued.	SVC:CP:Control Plane:13	NIST IR 8401
AST:SW:Software:04	Console operator software	The software C2 application on the operator console, the ground command-and-control suite.	SVC:CP:Control Plane:13	NIST IR 8401
AST:HW:Hardware:05	Ground cryptographic module (HSM)	The physical ground cryptographic module (HSM) that stores ground keys and performs encryption, decryption, signing, and verification.	SVC:CP:Control Plane:08	CCSDS 355.0-B (SDLS); NIST SP 800-57
AST:HW:Hardware:08	Kiruna antenna and RF front end	The physical Kiruna antenna, feed, and low-noise / high-power RF front end.	SVC:HY:Hybrid:03	NIST IR 8401; CCSDS TT&C

© 2026 ethicallyHackingspace (eHs)®

Figure 18 The ground assets as icons, beside the service each names



Arrows point to the parent named in PARENT.

Field note

Two coherent groups are recommended for the SUBSYSTEM tag, not yet recorded in the Day 1 inventory: the patch pipeline plus the binaries it stages as a Patch Deployment subsystem, and the operator workstation plus the console application it runs as an Operator Console subsystem. In this pass every service names one segment, and every asset names the services it physically carries: one each, except **AST:HW:Hardware:06**, the on-board computer and OBDH bus, which names three; the Space and Link segments each name more than one environment. Win: all three departments now cite the same 44 identifiers, and nothing on the telecommand path is recorded twice under two namings.

Assets are the leaf layer of the CONOPS. Each names in PARENT the service it implements, and each of those services resolves through its SEG to a PCE, so every asset closes a branch of the parent chain from PCE to asset. With all 44 elements enumerated, the CONOPS is complete and ready for Function 02, where each AN-THR element names one of these elements in its TOE.

© 2026 ethicallyHackingspace (eHs)®

CH 7 Deploying the Taxonomy in the SOC

> "That single data model is the Concept of Operations the next four METEORSTORM functions build on, and it deploys today into the Security Operations Center's MISP-based Threat Intel Platform."

The same model this module enumerated is published as the **meteorstorm** namespace in the public MISP (Malware Information Sharing Platform) taxonomies repository, live and open source. Your organization adopts it with no re-architecture: tag the threat intel, alerts, and events you already produce, and the structural context travels with every finding to each department and every Space ISAC partner.

Key points

- The model is published as the meteorstorm namespace in the public MISP taxonomies repository.
- Three steps deploy it: retrieve, enable, apply.
- A tagged event carries its structural context to every department and every Space ISAC partner running the same namespace.

The machine tag

A machine tag is a triple: **namespace:predicate="value"**. Two worked examples:

- **meteorstorm:SEG="SEG-GR"** · a finding on the Ground segment.
- **meteorstorm:AST="AST-FW"** · a firmware asset.

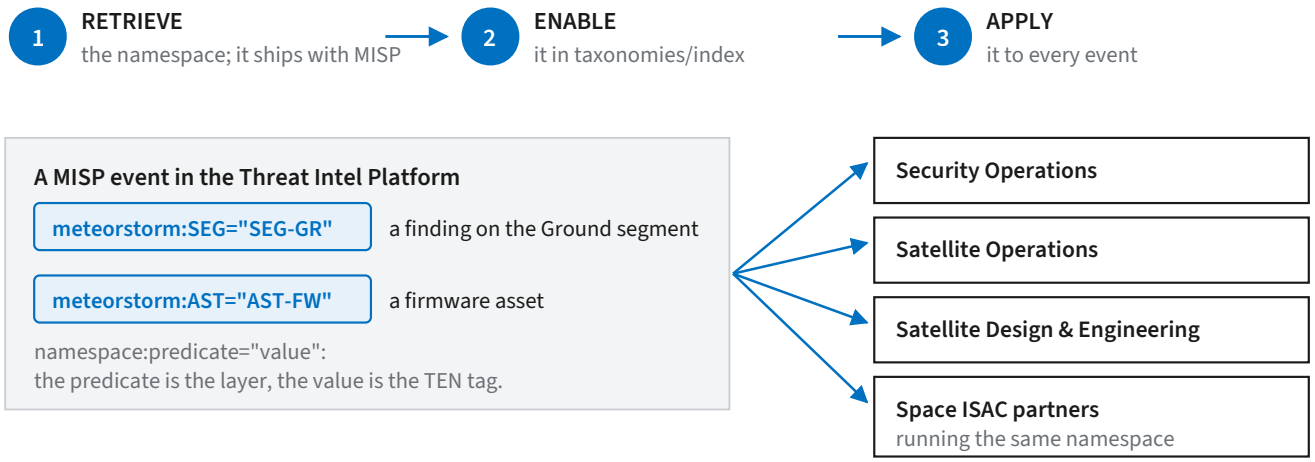
The predicate is the layer, the value is the TEN tag, so a tagged event carries its structural context in machine-readable form. The finding itself cites the exact instance by its ETEN, and the parent chain above that element is resolved from the ETEN, so it is never restated.

The three deployment steps

1. **RETRIEVE** the namespace; it ships with MISP.
2. **ENABLE** it in **taxonomies/index**.
3. **APPLY** it to every event.

© 2026 ethicallyHackingspace (eHs)®

Figure 19 Deploying the taxonomy: three steps, then every tagged event travels with its context



The structural context travels with every finding, read without translation.

One tagged event, read

MISP event 27 in the Security Operations Center's Threat Intel Platform shows the two working together. Five layer tags classify the event, and five attributes carry the records: each attribute value is an ETEN, and each attribute comment carries that element's parent, which is the ontology written down.

The five tags on the event: **meteorstorm:PCE="PCE-TE"**, **meteorstorm:SEG="SEG-GR"**, **meteorstorm:SVC="SVC-CP"**, **meteorstorm:AST="AST-SW"**, **meteorstorm:AST="AST-DA"**.

Type	Value	Comment, as recorded on the event
text	**AST:SW:Software:02**	Ground ACA software: enforces command acceptance before release to the link. PARENT: SVC:CP:Control Plane:09
text	**AST:DA:Data:01**	ACA credential store the ground authentication service relies on. PARENT: SVC:CP:Control Plane:09
text	**PCE:TE:Terrestrial:00**	Reston, Virginia mission-operations and NOC site. PARENT: none, root element
text	**SEG:GR:Ground:00**	Reston mission-operations enclave. PARENT: PCE:TE:Terrestrial:00
text	**SVC:CP:Control Plane:09**	ACA (Ground): decides who may command and which commands are released to the link. PARENT: SEG:GR:Ground:00. DISTRIBUTED: N

Read a tag as the type, identical in every organization, and an attribute as one real element on this platform, with its parent in the comment.

In the MISP taxonomy file each value also carries an expanded name, for example Terrestrial Environment for **PCE-TE**. The LABEL in a TEN and an ETEN is the short form, Terrestrial.

© 2026 ethicallyHackingspace (eHs)®

The first adoption step

Deploying the taxonomy into the Security Operations Center's MISP-based Threat Intel Platform is the first adoption step a team can take with nothing new procured. Satellite Design & Engineering builds the same taxonomy into the next platform when it leaves the drawing board, and all three departments use it together in the four functions that follow, Modules 02 to 05.

What deployment closes the loop on: information sharing with Space ISAC is a company mandate, and this taxonomy is what makes it work machine to machine. A confirmed command-and-control attack becomes a redacted, tagged event whose structural context any partner running the same namespace reads without translation.

© 2026 ethicallyHackingspace (eHs)®

CH 8 Use This at Work

This workbook teaches Function 01 on Kestrel Orbital. To run it on your own platform, work from the **METEORSTORM desk pack**, a separate course download. Its sheets are blank framework templates. They are for your own use and are not returned to the course.

Ten things to do at your work center

Function 01 gives the departments that share a platform one centralized taxonomy, ontology and enumeration process, so context and enrichment are recorded against the same elements.

Each of these can be done with what is already on your desk, in the order given. They are for your own use and are not returned to the course. The sheets named are in the METEORSTORM desk pack.

01 **Set the scope before you name anything.** Write the resilience objective and the requirements that drive the decomposition. An element outside the scope is not enumerated.
What you gain: the decomposition is scoped to the mission objective instead of exhaustive by default, and what is out is stated with its reason.
Chapter 5, Step 01 · desk pack sheet 03, Function 01 Concept of Operations: method card

02 **Apply the layer gate before you name an element.** Work top down, PCE, SEG, SVC, AST, and check each element against the layer's published definition. Zone means PCE; a group of services and assets means SEG. An element that fails the gate is reclassified, not forced through.
What you gain: with the environment named as a zone, a natural anomaly is not chased as an attack and an attack is not written off as weather.
Chapter 3, Sections 3.1 to 3.4 · Chapter 5, Step 02 · desk pack sheet 03, Function 01 Concept of Operations: method card

03 **Read the tag and the label from the published taxonomy.** Take both from the list for that layer. Never invent one.
What you gain: the tag is the type, identical in every organization, so a partner running the same namespace reads it without translation.
Chapter 5, Steps 03 and 04 · desk pack sheet 01, Quick reference: the four structural layers

04 **Assign the ordinal, and split where ownership diverges.** Two digits from 00, counted per tag. Physical units that share an owner, a build and a patch path are one element; where any of those diverge, the element splits and takes the next ordinal.
What you gain: a finding resolves to exactly one element, at the resolution where a patch lands.
Chapter 5, Step 05 and the AST delta · desk pack sheet 04, Function 01: element record sheet

05 **Link every parent before you move down a layer.** A segment names one or more environments, a service names one or more segments, and an asset names every service it carries, at least one. An element below the root with no PARENT is not a valid ETEN.
What you gain: enrichment recorded against one element resolves every layer above it through the parent chain in a single query.
Chapter 2, The ontology: the relationships · Chapter 5, Step 06 · desk pack sheet 04, Function 01: element record sheet

© 2026 ethicallyHackingspace (eHs)®

06 **Name each service by its function, not its device.** A service that spans segments stays one element: set DISTRIBUTED to Y and list every participating segment in PARENT.
What you gain: a detection rule written against the service fires on the function and survives a hardware refresh.
Section 3.3 · Chapter 5, The SVC delta · desk pack sheet 04, Function 01: element record sheet

07 **Write one description, at the element's own layer.** One plain sentence for this exact instance, with the gate applied a second time. One identifier carries exactly one description, everywhere it appears.
What you gain: a finding recorded against the identifier is not re-keyed before the next department can act on it, so no precision or time is lost.
Chapter 4, The canonical-description rule · Chapter 5, Step 08 · desk pack sheet 04, Function 01: element record sheet

08 **Check the register before you present it.** Confirm that each segment names its environments, each service states the function it delivers, and each asset names its services.
What you gain: a deviation from baseline on a named element raises a question every department can read, and the attacker loses stealth.
Chapter 5, the Review sentence of each delta · desk pack sheet 05, Function 01: element register and enumeration checklist

09 **Tag one event you already produce.** Retrieve the meteorstorm namespace, which ships with MISP, enable it, and apply it to the event.
What you gain: the structural context travels with the finding to each department and to every partner running the same namespace, with nothing new procured.
Chapter 7, The three deployment steps

10 **Cite the exact element in one finding.** Write the element's ETEN in the finding. The parent chain above it is resolved from the ETEN, so it is never restated.
What you gain: the detection targets an exact element, the console shows what is degraded, and the patch is routed against the same data model.
Chapter 2, What each department gets back · Chapter 7, The machine tag

Desk pack sheets for Function 01

Sheet	Use it to
01 Quick reference: the four structural layers	Read the four structural layers, the published tags and labels, and the TEN and ETEN syntax without opening this workbook.
03 Function 01 Concept of Operations: method card	Run the eight steps in order, with the gate that applies at each layer.
04 Function 01: element record sheet	Write one enumerated element per record, in field order, with its PARENT.
05 Function 01: element register and enumeration checklist	Hold one row per element, and check an enumeration before you present it.

© 2026 ethicallyHackingspace (eHs)®

Where the method is in this workbook

You need	Chapter and heading
The published tags and labels, by layer	Chapter 2, The taxonomy: the published taxonomic elements. Chapter 3 prints each full TEN.
The gate for each layer	Chapter 3, the definition under each of 3.1 to 3.4. Chapter 5, Step 02 and the 02 Gate row of each delta table.
The five fields of an ETEN	Chapter 4, The ETEN, five colon-delimited fields, and One complete worked ETEN.
The eight steps	Chapter 5, The normative ETEN Process.
The rules	Chapter 2, The ontology: the relationships (the parent rules). Chapter 4, The canonical-description rule. Chapter 5, the Constraints and Review sentences of each delta, with DISTRIBUTED for services and SUBSYSTEM for assets.
A complete worked model	Chapter 6, all 44 elements with identifier, description, parent and reference.
The machine tag and the three deployment steps	Chapter 7.

© 2026 ethicallyHackingspace (eHs)®