DRACO7RT · GROUND SYSTEMS · SECURITY · 28 OCTOBER 2026

Ground System Security and Zero Trust

How military and NASA mission operations centers are secured, what zero trust means for a MOC, and where the DRACO7RT ground stands against it

The ground segment is the way in. The one large attack on a satellite network, Viasat KA-SAT in February 2022, never touched the satellite: a misconfigured VPN appliance gave access to the management segment, and legitimate management commands wiped tens of thousands of modems. Zero trust is the answer the US government has adopted: no network location is trusted, every access is checked per session against identity, device and behaviour, and everything is logged.

Slides 2 to 10: the threat with three incidents, a reference MOC, zero trust as NIST defines it, the DoD and CISA pillars and stages, the federal and NASA direction, NASA's standards, how the Space Force does it, the frameworks for the ground segment, and positive control of the command link. Slides 11 to 18: the DRACO7RT ground as built, scored pillar by pillar, the gaps in order, the roadmap, operating practices, lessons, references and rules.

WHY THE GROUND

Three incidents: the satellite was never the weak point

Viasat KA-SAT, 24 February 2022

- Attack began about 03:02 UTC, an hour before the invasion of Ukraine
- Entry: "exploiting a misconfiguration in a VPN appliance to gain remote access to the trusted management segment"
- Lateral move into the network-management segment, then "legitimate, targeted management commands on a large number of residential modems simultaneously" that "overwrote key data in flash memory"
- Several thousand customers in Ukraine and tens of thousands across Europe offline; nearly 30,000 replacement modems shipped
- "No evidence that the KA-SAT satellite itself or its supporting satellite ground infrastructure" was compromised (Viasat, 30 March 2022)

ESA OPS-SAT, April 2023

- Thales ethical-hacking team, under ESA supervision, uploaded apparently harmless software with a vulnerability, later used it to reach the control layer, replaced a camera image and rotated the spacecraft
- Isolated from operational missions, RAM only, reverted; ESA then updated the control centre's security
- The path: valid accounts plus a deserialization flaw in the on-board management framework, i.e. the software upload and the ground trust, not the radio

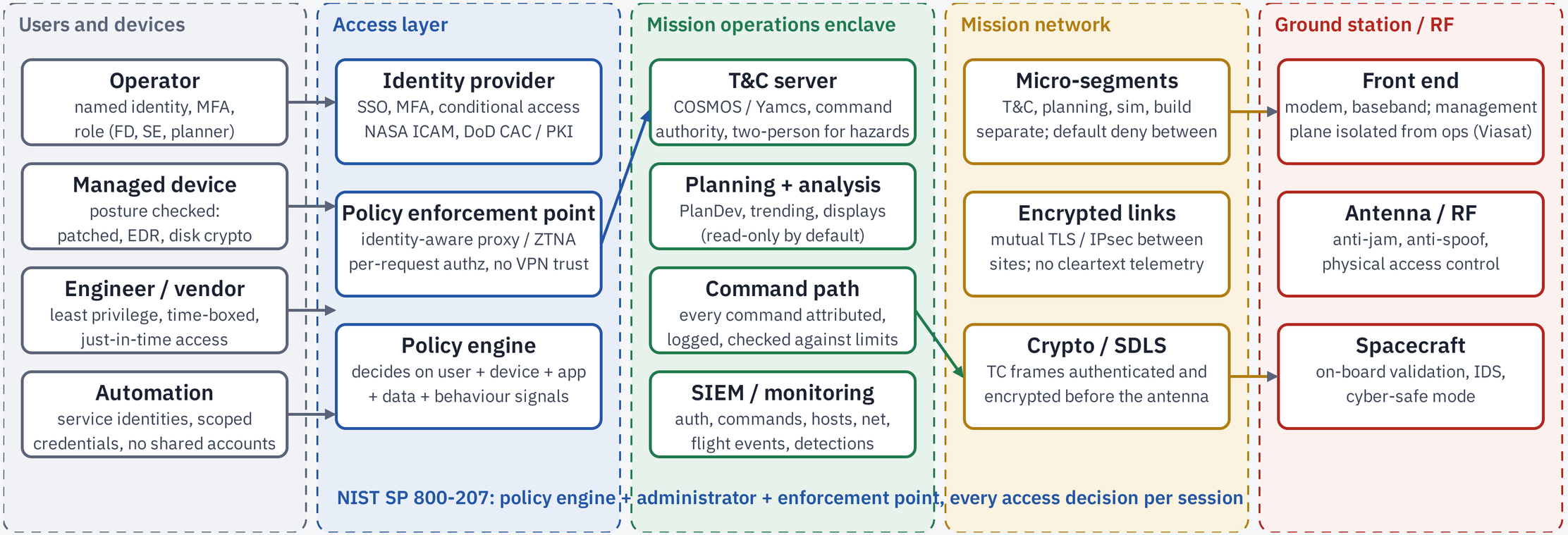
Hack-A-Sat 4, August 2023

- Space Force and AFRL ran the first capture-the-flag on an orbiting satellite, Moonlighter (3U CubeSat, Aerospace Corporation with SSC), nine challenges, seven on orbit
- Winners: mHACKeroni $50,000; Poland Can Into Space $30,000; jmp fs:[rcx] $20,000
- The point for a MOC: the government runs red teams against live ground and flight software and publishes the results

SPD-5 (4 September 2020): a space system is three segments (ground control network, space vehicle, user or mission network); plans to "retain or recover positive control of space vehicles". NIST IR 8401 (December 2022) applies the CSF to exactly this: the MOC and payload control center.

A REFERENCE MOC, ZONED

Five zones, one enforcement point per boundary, and the command path attributed end to end



A composite of NIST SP 800-207 (PE, PA, PEP), NIST IR 8401 (MOC and PCC; uplinks "typically encrypted and authenticated"; count or nonce against replay), the NASA best-practices ground principles and the Viasat lesson. Slides 11 and 12 map onto this picture.

ZERO TRUST, AS NIST DEFINES IT

NIST SP 800-207 (August 2020): per-request, least-privilege access decisions on a network assumed compromised

The seven tenets (section 2.1)

1. All data sources and computing services are resources
2. All communication is secured regardless of network location
3. Access to individual resources is granted per session
4. Access is determined by dynamic policy: client identity, application, requesting asset state, behavioural and environmental attributes
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets; "no asset is inherently trusted"
6. All authentication and authorization are dynamic and strictly enforced before access: ICAM, MFA, continual re-evaluation
7. The enterprise collects as much information as possible about assets, infrastructure and communications and uses it to improve its posture

The three components

- **Policy engine**: "the ultimate decision to grant access to a resource for a given subject", via a trust algorithm
- **Policy administrator**: establishes or shuts down the path, issues session-specific tokens
- **Policy enforcement point**: enables, monitors and terminates the connection. Engine plus administrator = the policy decision point

The three ways to build it (section 3.1)

- **Enhanced identity governance**: identity is the key input to policy
- **Micro-segmentation**: each resource or group behind its own gateway
- **Software-defined perimeters**: overlay networks; the Cloud Security Alliance SDP specification

DoD Reference Architecture v2.0 (July 2022), five tenets: assume a hostile environment, presume breach, never trust always verify, scrutinize explicitly, apply unified analytics. NIST SP 800-207A (September 2023) extends the model to service identities inside applications.

PILLARS AND MATURITY

DoD counts seven pillars and 152 activities with a deadline; CISA gives five pillars and four stages to measure against

DoD Zero Trust Strategy (21 October 2022) and Execution Roadmap v1.1 (November 2024)

- Seven pillars: **User, Device, Applications and Workloads, Data, Network and Environment, Automation and Orchestration, Visibility and Analytics**
- "There are 45 capabilities and 152 activities": 91 at **Target** level, 61 at **Advanced**
- Target level is "the minimum set … necessary to secure and protect the Department's DAAS [data, applications, assets, services] to manage risks from currently known threats"; every component must reach it **by the end of FY2027**
- Example capabilities: 1.3 Multifactor Authentication, 1.4 Privileged Access, 1.7 Least Privileged Access ("Deny User by Default Policy"), 1.8 Continuous Authentication, 5.1 Data Flow Mapping, 5.3 Macro Segmentation, 5.4 Micro Segmentation
- DoD Zero Trust Overlays v1.1 (June 2024) map NIST SP 800-53 controls to each of the 152 activities

CISA Zero Trust Maturity Model v2.0 (April 2023)

- Five pillars: **Identity, Devices, Networks, Applications and Workloads, Data**; three cross-cutting: Visibility and Analytics, Automation and Orchestration, Governance
- **Traditional**: manual lifecycles, static policies, least privilege set only at provisioning, siloed enforcement, manual response
- **Initial**: automation of attribute assignment and lifecycles begins; some changes to least privilege after provisioning
- **Advanced**: automated controls wherever applicable, cross-pillar coordination, centralized visibility and identity control
- **Optimal**: fully automated just-in-time lifecycles, dynamic least privilege, cross-pillar interoperability, continuous monitoring
- Written under Executive Order 14028 (May 2021); the Initial stage is new in v2.0

Slide 12 scores the DRACO7RT ground on the seven DoD pillars using CISA's four stages, because the DoD list separates automation and visibility, which are exactly the pillars a small lab ground can get right cheaply.

THE FEDERAL AND NASA DIRECTION

OMB set the FY2024 targets; NASA's inspector general found the mission side has not started

OMB M-22-09 (26 January 2022)

- Agencies "to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024", under EO 14028, aligned to CISA's five pillars
- **Identity**: enterprise-managed identities; "for agency staff, contractors, and partners, phishing-resistant MFA is required"
- **Devices**: "a complete inventory of every device it operates and authorizes"
- **Networks**: "encrypt all DNS requests and HTTP traffic"; break perimeters into isolated environments
- **Applications**: "treat all applications as internet-connected"; rigorous empirical testing
- **Data**: categorization and enterprise-wide logging

NASA OIG IG-25-004, Audit of NASA's Zero Trust Architecture (27 March 2025)

- "NASA has made progress implementing ZTA within its corporate environment … However, ZTA implementation for mission and JPL systems has not yet started."
- "NASA also lacks a centralized process to identify legacy IT and OT systems and does not maintain an inventory of the systems"; OCIO owned about 51.3 percent of IT assets in 2024, the rest sat with mission directorates and centers
- Four recommendations: extend the plan to the mission and JPL environment; a centralized process for legacy systems; embed OCIO experts in mission directorates; use mission directorates as pathfinders. Still open in the OIG list as of October 2026
- The OIG's own words to SMA: the "test like you fly" approach "should apply to the acquisition and implementation of new or upgraded IT and OT systems"

The policy base

- **NPR 2810.1** (effective 3 January 2022, expires 2027): security of information and information systems, explicitly including operational technology; built on the NIST Risk Management Framework (SP 800-37) and continuous monitoring (SP 800-137); every system under ongoing authorization
- **GAO-24-106624** (1 May 2024): NASA's 2023 best-practices guide is optional and not in spacecraft acquisition policy; GAO asked for a plan with dates; NASA agreed to update policy but not to a schedule

For a lab ground like DRACO7RT the relevant reading is: phishing-resistant MFA, a device inventory, encrypted traffic everywhere, applications treated as Internet-facing, and logging. Four of the five are already true here (slide 11); the device pillar is not.

NASA'S OWN STANDARDS FOR THE COMMAND LINK AND THE GROUND

NASA-STD-1006 and the Space Security Best Practices Guide say what a project must do; NPR 7150.2D says the software side

NASA-STD-1006 Space System Protection (2019, Change 1 2020; 1006A July 2022)

- **SSPR 1**: "protect the command stack with encryption that meets or exceeds ... FIPS 140 ... Level 1"
- **SSPR 2**: with an encrypted primary command link, "any backup command link shall at minimum use authentication"
- **SSPR 3**: protect the confidentiality of command-link critical program information
- **SSPR 4**: resilient to "the complete loss of, or temporary interference with, external PNT services"
- **SSPR 5, 6**: report unexplained interference; train for it
- Rationale quoted: NASA end-of-mission experiments "found that spacecraft without encryption or authentication are particularly susceptible"

Space Security Best Practices Guide, Rev B (October 2023, January 2024), ground principles

- **GR-AUTH-01**: uniquely identify and authenticate users and processes acting for them
- **GR-AUTH-03**: no "unencrypted static authenticators in applications, access scripts, configuration files"
- **GR-DEVA-01**: identify and authenticate all devices before a network connection
- **GR-INTG-01**: integrity verification of software and firmware before delivery and during operations
- **GR-MFA-01**: MFA for network access to privileged and non-privileged accounts and for local privileged access
- **GR-MON-01..04**: monitor at the external boundary and mission-critical internal boundaries; encrypted traffic stays visible to monitoring
- **GR-SOFT-01**: an explicit privilege to install software; no installation "without verification that the component has been digitally signed"
- Each principle lists its NIST SP 800-53 Rev 5 controls, the threat capability and the MITRE ATT&CK tactic it interdicts; 14 spacecraft principles alongside

NPR 7150.2D section 3.11 (March 2022)

- **SWE-154**: identify cybersecurity risks and mitigations in flight and ground software and plan them
- **SWE-156**: "perform a software cybersecurity assessment on the software components ... including risks posed by the use of COTS, GOTS, MOTS, OSS, or reused software"
- **SWE-157**: protect software with communications capabilities against unauthorized access per NASA-STD-1006
- **SWE-185**: secure coding standard verification
- DRACO7RT's classification record (Class E) marks SWE-156 "not assessed for this record": an open item

For DRACO7RT: the vehicle command link is neither encrypted nor authenticated (SSPR 1, 2); the COSMOS service password is a static authenticator in a file outside git (GR-AUTH-03 in spirit); software reaches the vehicle unsigned (GR-SOFT-01 not met); SWE-156 not done.

HOW THE MILITARY SECURES SATELLITE OPERATIONS

A deadline-driven zero trust program, dedicated cyber defense of ground systems, third-party assessment of commercial providers, and public red teams

Space Force and Space Systems Command

- **Satellite Control Network**: run by Space Delta 6; telemetry, tracking and commanding for DoD and some other satellites from seven remote tracking stations (Diego Garcia, Guam, Hawaii, New Hampshire, Oakhanger, Thule, Vandenberg) and two operations centers (Schriever, Vandenberg)
- **Digital Bloodhound** (SSC, Defensive Cyber Operations-Space): detection of cyber threats to space ground systems; FY2023 request $28.1 million, FY2024 reported $76 million. **Manticore** finds vulnerabilities, **Kraken** raises real-time defenses; Space Delta 6 uses them on protected communications, missile warning, MILSATCOM, PNT, NC3 and C2 satellite operations
- **Zero trust on the ground first**: SSC's roughly $17 million award to Xage Security (October 2023) for zero-trust access control and data protection across ground and space architectures, starting with ground stations and modems
- **IA-Pre** (Infrastructure Asset Pre-Approval, SSC Commercial SATCOM Office): providers implement NIST SP 800-53 at the **High** baseline, assessed by a third party, per asset (satellites, TT&C ground elements, integrator networks)

Advisories that came from live attacks

- **CISA/FBI AA22-076A** (17 March 2022, attributed to Russian state actors 10 May 2022): monitor SATCOM ingress and egress for traffic to "unexpected network segments" and brute-force logins; MFA; least privilege; "review trust relationships … remove unnecessary trust relationships"; "independent encryption across all communications links"; patch known exploited vulnerabilities; bring SATCOM traffic into security monitoring
- **NSA, Protecting VSAT Communications** (January 2022): encrypt before transmission, update firmware, change default credentials, isolate the management plane behind firewalls

Red teams in public

- Hack-A-Sat finals 2020 to 2023; 2023 on the orbiting Moonlighter CubeSat
- The organisers "ran actual satellite operations" during the contest: the ground segment was part of the game
- SPARTA v4.0 (DEF CON, July 2026) added "practical ground segment guidance" and revised all 90 countermeasures

The pattern: identity and segmentation on the ground first (operators, vendors and management planes live there); continuous detection on ground systems as a funded program; every outside party assessed against a fixed baseline before it touches the network.

FRAMEWORKS WRITTEN FOR THE GROUND SEGMENT

NIST IR 8401 gives the controls; SPARTA and ATT&CK give the attacker's moves to test them against

NIST IR 8401 (30 December 2022): CSF profile for satellite command and control

- Scope: "the ground segment of space operations with an emphasis on the command and control of satellite buses and payloads"; the MOC and the payload control center
- **ID.AM-1**: inventory every component, including cloud resources
- **PR.AC-5**: "establish procedures and controls to protect the integrity of ground segment networks" (segmentation)
- **PR.DS-2**: "Command uplinks are typically encrypted and authenticated. Consider measures such as a command count or nonce to protect against replay attacks or spoofing"
- **PR.DS-6**: command links with encryption or anti-replay "assure that software loads are not corrupted in transit. Digital signatures ..."
- **PR.PT-4**: "The MOC and PCC have high availability and integrity requirements"
- **DE.CM-1**: space vehicles are inaccessible and constrained, "therefore consider network monitoring as an integrated whole"
- Companions: NIST IR 8270 (introduction for commercial operators, July 2023), NIST IR 8441 (hybrid satellite networks, September 2023)

SPARTA v4.0.1 (24 August 2026)

- Space Attack Research and Tactic Analysis, the Aerospace Corporation, first released 2022
- 9 tactics, 87 techniques: Reconnaissance 9, Resource Development 5, Initial Access 13, Execution 18, Persistence 5, Defense Evasion 12, Lateral Movement 7, Exfiltration 10, Impact 8
- **90 countermeasures**, all revised for the lifecycle in v4.0; a Ground Segment Cyber Defenses section; mappers to NIST 800-53, ISO 27001, D3FEND and the NASA best-practices guide
- The flight security deck uses SPARTA's indicators of behavior as the on-board detections

MITRE ATT&CK for the ground

- Aerospace OTR-2025-00018 (October 2024, for the CCSDS security working group): a unified matrix of ATT&CK and SPARTA; ATT&CK "is highly applicable to the ground segment", SPARTA covers space and link
- The DRACO7RT cyber-scenario harness already labels every scenario with its SPARTA tactic; the ground side can be labelled the same way with ATT&CK

How to use them together: inventory and segment per IR 8401, then take each SPARTA ground technique and ATT&CK tactic that applies to COSMOS, Yamcs, PlanDev and the control service, and name the control that stops it and the log line that would show it. That table is the SWE-156 assessment.

POSITIVE CONTROL OF THE COMMAND LINK

Authenticated, encrypted, replay-proof commanding is a solved protocol problem; the work is key management and the ground-side encoder

CCSDS Space Data Link Security (SDLS)

- **CCSDS 355.0-B-2** (July 2022): a security header and trailer for the TC, TM, AOS and USLP data link protocols, "for applying data authentication and/or data confidentiality at the Data Link Layer"
- A **Security Association** per link, selected by the Security Parameter Index in every frame; it holds the algorithm, the initialization vector and the **anti-replay sequence number**; algorithms from CCSDS 352.0-B (AES-GCM in the baseline)
- **CCSDS 355.1-B-1** (February 2020), Extended Procedures: key management, security association management, monitoring and control, i.e. rekeying, starting, stopping and expiring associations, status reporting

NASA CryptoLib

- github.com/nasa/CryptoLib, v1.5.1 (23 September 2026), NASA Open Source Agreement
- "a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station"
- API: Crypto_TC_ApplySecurity on the ground, Crypto_TC_ProcessSecurity on the vehicle; TM and AOS the other way; backends WolfSSL, LibGcrypt, JPL KMC
- NOS3 integrates it (telecommand encryption with gcrypt); it is in the twin's app list, not on the DRACO7RT RTEMS vehicle
- Assurance note: heap out-of-bounds CVEs in 2025 and 2026 fixed in 1.4.3; Extended Procedures were marked work in progress before 1.3.2; pin the version (notes)

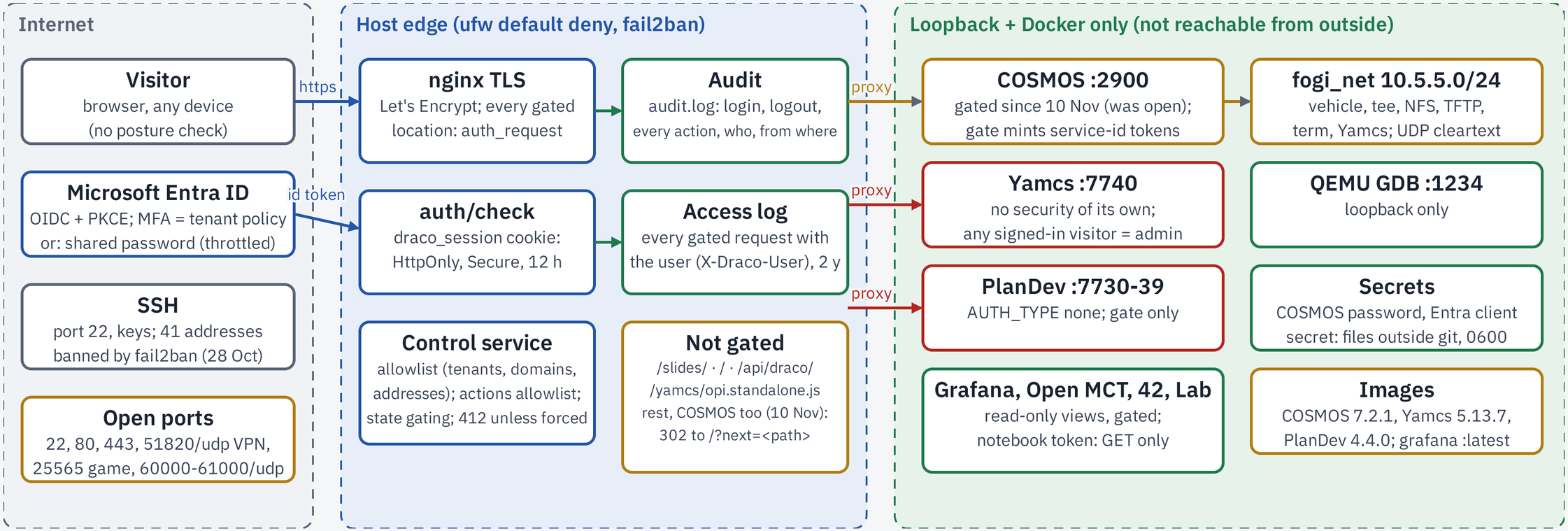
What DRACO7RT does today, and the rule that stands in

- Commands leave COSMOS or Yamcs as cleartext CCSDS over UDP with the cFE XOR checksum; the vehicle accepts any sender
- The stand-in is procedural: **one commanding station at a time** (Yamcs tc-out off by default; front door › Demo control › COMMANDING STATION shows the badge **COSMOS commanding** and holds **Switch to Yamcs** / **Switch to COSMOS**) and every front-door action audited with the user
- Attribution stops at the COSMOS door: for each sign-in the gate mints a COSMOS token from the one service password, so inside COSMOS every command is the service account
- Hazardous commands carry no mark in the dictionary yet (Tables deck, hazard list)

SPD-5 asks for "effective and validated authentication or encryption" of command, control and telemetry links; NASA-STD-1006 SSPR 1 asks for FIPS 140 encryption of the command stack. The flight security deck has the vehicle side of the same step; this deck's roadmap has the ground side.

THE DRACO7RT GROUND AS BUILT

One gate (COSMOS behind it since 10 November), one identity provider, services on the loopback; the weak points are inside



Measured 28 October 2026: ufw default deny, 41 addresses rejected by fail2ban; audit.log 341 and access.log 378 lines since 25 October. COSMOS moved behind the gate on 10 November 2026 (verified live). Sources: notes.

DRACO7RT SCORED ON THE SEVEN PILLARS

Mostly Initial on CISA's scale: the door is good, the inside trusts the door

Pillar	What exists today	Stage	Gap
User	front door card **Sign in with Microsoft** (Entra ID OIDC + PKCE, allowlist of verified addresses, tenants, domains; MFA = tenant policy) or the fallback box **Sign in with password** (shared, throttled, logged as password:<sid8>); **Sessions** signs others out; every action audited with the user	**Initial**	no role model (everyone signed in can do everything); no privileged-access tier; no per-user identity inside COSMOS, Yamcs or PlanDev
Device	nothing: any browser from any device	**Traditional**	no device inventory, no posture signal, no managed-device requirement for commanding
Applications and workloads	per-location gating (302 to /?next=...); cross-site requests refused; Demo control: one allowlisted action at a time, greyed by state (412 unless forced); notebook token GET-only, no COSMOS token; /slides/ public by design; COSMOS gated too since 10 Nov; services on loopback	**Initial**	Yamcs and PlanDev trust the gate completely (admin for all); COSMOS one service identity; no per-app authorization
Data	evidence, compliance, decks gated; secrets in files outside git with 0600; retention set (COSMOS 30 d, Yamcs 30 d, logs 2 y)	**Traditional**	no data categorization or labels; no backup and restore test of the object store, QuestDB, Yamcs archive, PlanDev DB
Network and environment	ufw default deny; fail2ban; TLS; docker bridge private, no public container port; GDB loopback	**Initial**	flat inside: one host, one bridge, cleartext UDP on fogi_net; shared host (game server, VPN); rpcbind listening; no segmentation between T&C, planning, build
Automation and orchestration	control service: allowed_actions, audited jobs, password throttle, cleanup timer, vehicle autostart, --verify (gate, token limits, public ports), selfcheck	**Initial**	no automated response to forced actions (failed password sign-ins are only throttled); no automated patching or image scanning
Visibility and analytics	audit.log + access.log with user; Yamcs events and alarms; Grafana; --verify health	**Initial**	no SIEM: nothing correlates host, auth, command and flight events; no alerting; the flight security log gaps (provenance, authorization) end here

Scoring rule: Traditional = manual and static; Initial = some automation and re-evaluation after provisioning (CISA ZTMM v2.0, slide 5). Software alone can reach Advanced on Applications, Automation and Visibility, not on Network or Device.

THE GAPS, IN ORDER OF RISK

What an attacker inside the door can do today, and what it would take to see them

#	Gap	What it allows	Fix (short)
1	**Yamcs has no authentication of its own**	any signed-in visitor opens Yamcs › **Links** (left sidebar), enables tc-out and commands (Send a command, Stacks), unattributed	Yamcs security with per-user accounts fed from the gate (X-Draco-User header auth), command privilege only for operators
2	**One identity inside COSMOS**	every command and script run is the service account; attribution stops at the door (COSMOS itself is behind the gate since 10 Nov)	COSMOS users or per-session tokens tied to the Entra identity; command history joined to audit.log by session
3	**No role model**	anyone signed in can press **LAUNCH (RTS-005)**, **Mission test (COSMOS)**, **Switch to Yamcs** in Demo control, or install tables (Workbench › 04 Deliver)	roles in microsoft.json (viewer, operator, engineer); allowed_actions checks the role; hazardous actions need operator + confirm
4	**Cleartext, unauthenticated command path**	anyone on the host or the bridge injects commands; replay is trivial	SDLS via CryptoLib (vehicle) + ground encoder in Yamcs; interim: bind CI_LAB to the tee's address and drop the rest
5	**No correlation or alerting**	brute-force, forced action, off-hours command: unread log lines	ship audit.log, access.log, nginx, sshd, Yamcs events and SpaceCOP reports to one store (Loki or an ELK) with four alerts
6	**Shared host**	a game server and a VPN endpoint on the mission host widen the attack surface and the blast radius	move them, or move DRACO7RT; at minimum separate network namespaces and users
7	**No device posture**	a compromised laptop with a valid session looks like an operator	Entra conditional access (compliant device) for the commanding role
8	**Supply chain**	grafana :latest; no SBOM; cFS snapshot patched by hand; nos3 upstream on a public remote	pin every image by digest; SBOM for the ground stack; the pre-push guard (R6)
9	**No tested restore**	object store, QuestDB, Yamcs archive, PlanDev DB: no restore drill	nightly snapshot to another host; a restore test on the calendar
✓	**Closed 10 Nov 2026**	COSMOS open to the internet (lockable password; as sim.efsi.com, none); no per-browser sign-out; no CSRF guard; notebook could command	COSMOS gated, sim.efsi.com redirects; password throttled; **Sessions** › **Sign out**; CSRF guard; token reads only

Items 1 to 3 and 5 are software only and reuse what exists (the gate already knows the user; Yamcs 5.13 has a security module; the control service already audits). Item 4 is the same step as the flight deck's roadmap step 5. Items 6 and 7 are decisions.

ROADMAP TO ADVANCED ON THE SOFTWARE PILLARS

Each step is small, reuses the gate, and leaves evidence

1 · Roles
viewer / operator / engineer in microsoft.json; allowed_actions and the tables API check the role; the page greys by role as it already greys by state. 1 day

2 · Yamcs identity
Yamcs security on, users created from the gate's identity (header or OIDC against Entra), command privilege for operators only; tc-out toggle stays a front-door action. 2 days

3 · COSMOS attribution
per-session token already minted: record session ↔ user and join COSMOS command history to audit.log; or COSMOS users per Entra identity. 1 to 3 days

4 · One log store + alerts
Loki/Promtail (or Elastic) on the host: audit, access, nginx, sshd, Yamcs events, control jobs; alerts: failed sign-ins, force=true, tc-out enabled, command outside a session. 2 days

5 · Harden the inside
CI_LAB accepts only the commanding stations' addresses (iptables on the bridge); PlanDev behind the role; rpcbind off; pin images by digest; SBOM. 1 day

6 · Backups and restore drill
nightly snapshots of the COSMOS volumes, Yamcs data, PlanDev DB to another host; one documented restore. 1 day + a drill

7 · Authenticated commanding
CryptoLib SDLS: ground encoder in Yamcs, vehicle decoder in front of CI_LAB, key management; the flight deck's step 5. Weeks

8 · Assessment and exercise
SWE-156 assessment as the IR 8401 + SPARTA + ATT&CK table; purple-team the cyber harness against this ground; host and device decisions (6, 7 on the gap list). Ongoing

After steps 1 to 6 the scorecard reads Advanced on Applications, Automation and Visibility, Initial on User and Data, Traditional on Device, Initial on Network. Steps 7 and 8 are the ones that need a decision and a budget. Nothing on this slide changes a flight app.

OPERATING PRACTICES FOR THE DRACO7RT GROUND

What the standards ask of people and procedures, and what this project already does

Access and roles

- Named identities only; the allowlist is the access list and is reviewed when someone joins or leaves (microsoft.json, outside git)
- **Least privilege by role** (roles deck): presenters view, operators command, engineers build; a role change is a file edit and an audit line
- Two-person rule for hazardous commands once the dictionary marks them (Tables deck, hazard list)
- Sessions expire in 12 hours; **Sessions** (top bar, left of **Sign out**): a Microsoft sign-in sees and signs out every browser; logged

Change control and supply chain

- Plugin upgrades by the PUT-stage recipe (run/upgrade-plugin.sh), never during a demo; version bumps in build.sh and bootstrap together
- cFS snapshot patches recorded per bug with the GDB evidence; images pinned (COSMOS 7.2.1, Yamcs 5.13.7, PlanDev 4.4.0); pin grafana too
- Secrets never in git, never on a slide; the pre-push guard against the public nos3 remote (risk R6)
- Every table and sequence change goes through the Table Workbench: **03 Check**, **04 Deliver**, dump back, audited

Monitoring, response, exercises

- Logs: audit and access with the user, 2 years; Yamcs event and alarm history 30 days; the daily cleanup job keeps retention
- **Runbook** for an incident: Demo control › **Switch to COSMOS**; **Sessions** › **Sign out all others** (Microsoft sign-in; a restart keeps them); **Fresh vehicle**; keep audit/access/console logs; investigate
- Exercise: run the cyber-scenario harness against this ground once per release; a Hack-A-Sat-style internal red team on the front door and Yamcs
- Report unexplained interference or anomalies the way NASA-STD-1006 SSPR 5 asks: to the project, in the notes, same day

The MOC is also the people: NASA's best-practices guide puts governance first (GV-RSK-01), and SPD-5 lists insider-threat training and portable-media restrictions beside the technical controls.

LESSONS APPLIED

Each incident and advisory, read against this ground

Source	Lesson	DRACO7RT today	Applies as
Viasat KA-SAT (2022)	the management plane is the attack path; a VPN appliance is a trusted network, not an identity	no VPN trust: every request is checked at nginx with the session; but the host also runs a VPN endpoint and a game server	keep per-request auth; separate the host (gap 6)
CISA AA22-076A (2022)	remove unnecessary trust relationships; monitor ingress and egress; MFA; independent encryption on every link	trust relationships inside the door are total (Yamcs, PlanDev); no egress monitoring; link to the vehicle cleartext	gaps 1, 4, 5
ESA OPS-SAT (2023)	a software upload is an attack path; verify what is loaded; detect on board	CFDP uploads to /ram unsigned; CS tables empty; no on-board IDS	flight deck steps 3, 4, 6
NSA VSAT (2022)	change default credentials; isolate management	Yamcs and PlanDev run with no credentials behind the gate; COSMOS on one service password	gaps 1, 2
NIST IR 8401 PR.DS-2	command count or nonce against replay	none on the uplink (S02 replay passes on the twin; the vehicle is the same)	flight deck step 1 and 5
NASA OIG IG-25-004	mission systems lag corporate; keep an inventory; test like you fly	the inventory is CLAUDE.md and --verify; this deck is the first zero trust pass on a mission-side system here	keep the scorecard current per release
Hack-A-Sat	red teams on live ground and flight software, in public	the cyber harness is a red team for the twin; the ground has never been attacked on purpose	roadmap step 8

The common thread: none of these needed a radio or a satellite. Identity, trust inside the perimeter, uploads and the absence of monitoring were enough.

REFERENCES

Every public fact on these slides, by document

Document	Body, date	Used for
NIST SP 800-207 Zero Trust Architecture	NIST, August 2020	definition, 7 tenets, PE/PA/PEP, 3 approaches (slide 4)
NIST SP 800-207A	NIST, September 2023	service identity inside applications (slide 4)
CISA Zero Trust Maturity Model v2.0	CISA, April 2023	5 pillars, 3 cross-cutting, 4 stages (slides 5, 12)
DoD Zero Trust Strategy; Capability Execution Roadmap v1.1; Reference Architecture v2.0; Overlays v1.1	DoD CIO, Oct 2022; Nov 2024; DISA/NSA Jul 2022; Jun 2024	7 pillars, 45/152, 91/61, FY2027, 5 DoD tenets (slides 4, 5)
OMB M-22-09	OMB, 26 January 2022	federal targets (slide 6)
IG-25-004 Audit of NASA's Zero Trust Architecture; GAO-24-106624	NASA OIG, 27 March 2025; GAO, 1 May 2024	NASA status and recommendations (slide 6)
NPR 2810.1; NPR 7150.2D section 3.11; NASA-STD-1006 (A, July 2022); Space Security Best Practices Guide Rev B	NASA, 2022; 2022; 2019/2022; Oct 2023 / Jan 2024	policy, SWE-154/156/157, SSPR 1-6, GR-* principles (slides 6, 7)
SPD-5 Cybersecurity Principles for Space Systems	White House, 4 September 2020	segments, positive control, authentication or encryption (slides 2, 10)
NIST IR 8401; NIST IR 8270; NIST IR 8441	NIST, Dec 2022; Jul 2023; Sep 2023	ground-segment CSF profile and companions (slide 9)
CCSDS 355.0-B-2 SDLS; CCSDS 355.1-B-1 SDLS-EP; nasa/CryptoLib v1.5.1	CCSDS Jul 2022; Feb 2020; NASA Sep 2026	authenticated commanding (slide 10)
Viasat KA-SAT overview; CISA/FBI AA22-076A; NSA VSAT advisory; ESA OPS-SAT demonstration; Hack-A-Sat 4	30 Mar 2022; 17 Mar 2022; Jan 2022; 4 May 2023; Aug 2023	incidents and advisories (slides 2, 8, 15)
SPARTA v4.0.1; Aerospace OTR-2025-00018	Aerospace Corporation, 24 Aug 2026; Oct 2024	attack framework, ATT&CK for the ground (slide 9)
Space Force: Digital Bloodhound, Xage award, IA-Pre, Satellite Control Network	Breaking Defense Oct 2022 / Apr 2023; DefenseScoop Oct 2023; Air & Space Forces; Space Delta 6	military practice (slide 8); trade-press figures, not primary documents

Not found, so not claimed: a published "Protect-Defend" concept for the SCN, a standalone public NASA zero trust plan, NASA-STD-1006A's exact SSPR 3 wording (quoted from 1006 Change 1). Project facts: web/control/README.md, CLAUDE.md, the host on 28 October 2026.

RULES FOR THE DRACO7RT GROUND

The zero trust tenets, written for this project

Never trust the network

- Every request to a gated path is authorized by the control service, per request; a VPN, a loopback or a Docker bridge is not an identity
- A new gated location gets the auth_request lines and the user header or it does not ship
- Services behind the gate still get their own identities (Yamcs, COSMOS, PlanDev) as the roadmap lands them
- The vehicle link is treated as hostile until SDLS is on it: one commanding station, tc-out off by default

Always verify, always record

- Named identity for every human; service identities for automation; no shared accounts on a slide, in a script or in git
- Every front-door action, every table install, every force override is an audit line with the user; keep both logs two years
- A pass needs positive evidence (a log line, a counter), never the absence of an error: the same rule as the flight side
- Report the state per release: the scorecard on slide 12 is regenerated and dated

Assume breach, limit the blast

- Roles and least privilege: a viewer cannot command; hazardous commands need an operator and a confirmation
- Prefer a refusal to a workaround: if a control blocks a demo, say so; do not disable it
- Backups exist only if a restore has been done; retention is not a backup
- The furnished tools, the hazard list and any real-mission data are controlled information and stay out of the repository (R14)

Sources for the project side: CLAUDE.md, web/control/README.md (auth model), docs/sow/risk-register.md, claude-notes/RTS-TOOL.md. Nothing in this deck is committed yet; the scorecard and the gap list are the input to the roadmap decision.