

FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

MODULE WORKBOOK · STUDENT EDITION

Module 05

Adversary Management

The method behind the week-final resilience measures, and every measure it produced,
each protecting the one element its threat names.

COPYRIGHT AND LEGAL NOTICES

© 2026 D2 Team CORP, a 501(c)(3) nonprofit. All rights reserved.

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. Redistribution outside the cohort and those bodies is not authorized.

Verbatim sources. Every taxonomy definition in this document is the published METEORSTORM taxonomy text, quoted exactly. Definitions are never abbreviated, paraphrased, or reworded in this publication.

Trademarks. ethicallyHackingspace (eHs)® is a brand of D2 Team CORP, not a separate legal entity. 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 05 Adversary Management, module workbook, student edition
EDITION	Student edition · revised 2026-09-24
CONTACT	www.d2teamcorp.org

STUDENT EDITION

The teaching chapters and the complete worked deliverable. Your instructor holds the instructor edition, which adds the session plan and the marking guidance.

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, in five working days. 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 mandates chose it. Executive Order 14144 puts the command and control of an operational platform first, and the NIS2 Directive places a duty of care and a reporting clock on the ground operator. The fleet is already flying, so the first pass ran on the part that would end the mission if an adversary took it. 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. Every one of those is a recorded decision taken at the enumeration meeting, 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 procedure 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.

CONTENTS

- 01 CH 1 The Day in One Page
- 02 CH 2 What Both Departments Bring to the Table
- 03 CH 3 The AN-RES Method, and the Twin
- 04 CH 4 The Catalogue, Complete
- 05 CH 5 The Week in Hand
- 06 CH 6 Tag and Share

PART I

Orientation

What the day produces, and what each department brings to the table before any of it can be written.

CH 1 The Day in One Page

CH 2 What Both Departments Bring to the Table

CH 1 THE DAY IN ONE PAGE

Four days in, the platform has a decomposition, a threat catalogue, an attack-path map, and a detection portfolio with playbooks. Today both operating departments hold the pen together, because resilience needs operating procedures and architectural change at the same time, and neither department can commit the other.

IN THE CLASSROOM

This module runs as slides, then a classroom of three parts. Have this workbook, the question set and the day's meeting minutes open. The classroom does this, in this order:

THE WORKBOOK	Chapter 3, Sequencing, and Chapter 5, The Week in One Table. From the week table, count how many of the four threats and four paths name each element. Name the one that recurs most. Say which of the four NIST SP 800-160 Volume 2 goals, anticipate, withstand, recover or adapt, a measure on it would serve.
THE QUESTION SET	Questions 1, 4 and 12 are worked and marked in the classroom, each answer given with its reason. The rest are yours.
LESSONS LEARNED FROM THE MINUTES	Open the Day 5 minutes at the decision register and read Item 01, What a resilience measure has to name; Item 03, Measure 01, dual-control commanding, and the cost of it; Item 05, Measure 03, and closing the gap the week has been carrying. The rule, the objection and the decision are taken from the record, not from the slide.

Why resilience comes last. Not because it matters least, but because it needs the accumulated set to be useful. Only after Functions 02, 03, and 04 can you see which platform elements keep recurring: the elements that appear in the most threats, the most paths, and the most detections are where the adversary keeps having to go. Those are the elements worth spending money on. Run Function 05 first and you harden by intuition; run it last and you harden by evidence.

What you build. Four AN-RES elements: 2 Ground, 1 Link, 1 Space. Every one names one platform element it protects (TRE), the path or threat it counters, its resiliency goal, and the department that owns it. Every one also records where the protected element sits in its life and the cadence the measure actually holds at, because two of these four cannot be installed on the element they protect today. Chapter 4 prints the whole deliverable.

The chain, closed. One chain is one number carried across the week, and Day 5 is where the chain closes. Day 2 anchored AN:THR:Threat:00 to SVC:CP:Control Plane:09, the ground command-acceptance service. Day 3 walked AN:ATT:Attack Path:00 to that same element, Day 4 watched it with AN:DET:Detection Signature:00, and today AN:RES:Resilience Measure:00 hardens it. Threat,

path, signature and measure all carry ordinal 00 and all name that one element. Every entry in chapter 4 works the same way.

The Owner field. This is the first day where a deliverable names who carries it. A measure that is an operating procedure belongs to Satellite Operations. A measure that is an architectural change belongs to Satellite Design and Engineering. Most belong to both, and the split is written out, because a measure owned by everyone is owned by no one.

What the week ends with. A working decomposition, an anchored threat set, an attack-path set, a signature and playbook set, and a resilience-measure set, all against the same reference platform and all in the same five-field language. Chapter 5 shows the five sets as one artifact and walks a single ordinal through all of them.

CH 2 WHAT BOTH DEPARTMENTS BRING TO THE TABLE

"Both operating departments at the meeting, because resilience needs operating procedures and architectural change."

DEEP DIVE DECK, SLIDE 4 · DAY-5 SATELLITE OPERATIONS AND SATELLITE DESIGN AND ENGINEERING WORKING SESSION

Every previous day had one department holding the pen: the SOC on Day 2, Satellite Design and Engineering on Day 3, the SOC again on Day 4. Day 5 is the only session with two, and the reason is structural rather than ceremonial. A resilience measure almost always has two halves: something must be built, and something must be done differently every day thereafter. Dual-control commanding is a workflow in the commanding software and a discipline on the operations floor. Frequency agility is a waveform capability and a band-switching procedure. Commit only one half and the measure does not hold.

THE OWNER FIELD, AND WHY IT EXISTS

OWNER VALUE	WHAT IT MEANS	EXAMPLE FROM THIS CATALOGUE
Satellite Design and Engineering	The measure is an architectural change: something is built, signed, or re-designed.	Measure 03, measured-boot architecture and signing pipeline
Satellite Operations	The measure is an operating procedure: something is done differently on every pass.	No sole-owned SatOps measure in this set; the discipline halves sit inside the Both entries
Both, with the split named	Two halves, each committed by its department, written out so neither can assume the other.	Measures 00, 01, and 02

The rule the meeting settled on. A measure recorded as Both must name the split. "Both" on its own is a measure nobody owns; "Satellite Design and Engineering builds the segmentation and dual-approval workflow, Satellite Operations holds the maintenance-window and peer-review discipline" is a measure two people can be held to.

PART II

The method and the catalogue

The process for producing one entry correctly, then the complete catalogue this day produced, entry by entry.

CH 3 The AN-RES Method, and the Twin

CH 4 The Catalogue, Complete

CH 3 THE AN-RES METHOD, AND THE TWIN

“Six steps, fixed order. A measure with no target and no objective is decoration, not resilience.”

DEEP DIVE DECK, SLIDES 7, 8, AND 9 · AN-RES ENUMERATION PROCESS · DIGITAL TWIN (BOTH SLIDES)

Inputs. The week’s attack-path and threat sets against the telecommand path, and a working session with Satellite Operations and Satellite Design and Engineering, building the continuity, backup, and supply-chain measures NIS2 requires and the failover EO 14144 expects for command and control.

Output. One AN-RES element per measure, each anchored via TRE to the one platform element it protects.

The constraint. Every element carries exactly one TRE element and names its resiliency goal. A measure with no target and no goal is decoration, not resilience. The TRE may name an element in **any** structural layer, PCE included: what is fixed is that it holds one element, at the lowest layer the source resolves, and that it is the element the AN-THR this measure counters already names as its TOE. Every element also declares the lifecycle of the element it protects and the cadence the measure holds at, because a measure that cannot be installed is not a control in force.

THE SIX STEPS, FIXED ORDER

1. **Enumerate the LAYER.** LAYER = **AN**, fixed. A resilience measure is a decision about the platform, not a part of it.
2. **Identify the resiliency goal.** One of Anticipate, Withstand, Recover, or Adapt, per NIST SP 800-160 Volume 2. SOURCE takes exactly two values, **observable** or **synthetic**, declared at the gate and stamped on the entry. Measures are enumerated **prospectively**, before they are exercised, which is what makes completeness auditable: a reviewer walks the attack paths and checks that each has a corresponding measure or a consciously accepted residual risk.
3. **Set the TAG to RES.** A Resilience-Measure element within the Analytic Layer.
4. **Assign an ORDINAL.** Two digits from 00, one per distinct measure, taken from the running register that also tracks work outside this scope. Each measure keeps the ordinal of the chain it closes, so this week's four are 00, 01, 02, 03. An ordinal is issued once and never renumbered, which is why a scoped set is legitimately non-consecutive as the register fills.
5. **Enumerate the TRE.** Target of Resilience Enhancement: **one** enumerated platform element the measure protects, and it is the same element the **AN-THR** this measure counters names as its TOE. AN-RES uses TRE, not TOE or TDM: the element made more resilient, not the element exploited or the element scanned. One element, never a list, and never a "primary" among several. The wider chain the protection reaches is written in the description. Then run the **lifecycle test** on that element, below, because where it sits in its life decides whether the measure can be installed on it at all.
6. **Write the DESCRIPTION.** The measure, the resiliency goal it serves, the AN-ATT or AN-THR elements it counters, and the source citation: internal engineering, control-framework guidance, a peer-shared pattern, or a post-incident lesson. Record the **cadence** the measure actually holds at, and where that cadence is not in force, the compensating control or the residual risk that stands in its place.

Repeat for the next measure. When every enumerated path carries a measure or a recorded residual risk, the AN-RES enumeration is current.

Why one element and not a list. A field holding two elements cannot say which one the entry is about. Two later readers act on that field: an auditor asks whether the path is countered, and an engineer asks what to change. Give them two elements and they answer different questions from the same record. The reach is real and it belongs in the description, where it can be read as reach rather than mistaken for a second target.

CHOOSING AMONG THE FOUR GOALS

The four cyber-resiliency goals come from NIST SP 800-160 Volume 2, and every AN-RES serves exactly one of them. Choose by what the measure changes about the attack, not by how important it feels:

GOAL	TEST	IN THIS CATALOGUE
Anticipate	It removes the opportunity before the adversary acts.	Measures 00 and 03
Withstand	The mission continues while the attack is under way.	Measures 01 and 02
Recover	It restores a known-good state afterwards.	Carried by the Day-4 playbooks rather than by a measure in this set
Adapt	It changes the platform so the same path does not work twice.	Not in this set; the honest reading of a four-measure catalogue

The same measure can be argued into two goals, and that argument is worth having at the meeting, because the goal determines how the measure is later reviewed for effectiveness. An Anticipate measure is reviewed by asking whether the opportunity is still closed; a Withstand measure by asking whether the mission still runs under load. Record the goal you can defend, and record why.

WHERE THE ELEMENT SITS IN ITS LIFE, AND WHAT THE MEASURE CAN THEREFORE BE

The TRE says what a measure protects. It does not say what you are allowed to change. Those are two different questions, and the second one has a test of its own, because a measure protects an element but cannot always be installed *on* that element. Firmware in orbit is fixed for its service life. A waveform lives in a radio that is already flying. A ground service can be rebuilt this quarter. Same catalogue, three different kinds of measure, and until you say which is which they all read the same on the page.

The lifecycle test. Ask where the protected element sits in its life. The answer decides what the measure can be.

LIFECYCLE	THE PROTECTED ELEMENT	SO THE MEASURE IS
reachable	Changeable now.	Applied to the element directly.
through	Fixed in itself, but reachable through something you do control.	A compensating control on the path to it.
fixed	Fixed for its service life.	A requirement for the next build . It cannot be installed on what is flying.

The cadence. The lifecycle is a fact about the element. The cadence is a statement about the organization: what it actually holds today, which is the thing an auditor, a regulator, and the next operator on shift all want to know.

CADENCE	WHAT THE ORGANIZATION HOLDS TODAY
in-force	Installed, or installable this quarter.
phased	Part is installable now, part belongs to the next build.
next-build	Cannot be installed on the flying platform at all.

The rule that keeps the catalogue honest. Anything not in force must name a **compensating control** or a recorded **residual risk**. Coverage you cannot install is not coverage. A compensating control names the element it is applied to. A residual risk names its owner and what closes it. Where the cadence is in force, both fields are empty, and that emptiness is a statement rather than an omission.

What a compensating control is, and what it is not. It is not a weaker version of the measure and it is not a promise to build one. It is a control you can install today, placed on something you do control, chosen because the adversary has to cross it to reach the element you cannot change. It buys distance, not trust. Saying so plainly is the point: a compensating control written as though it hardened the protected element re-creates exactly the false reading the lifecycle test exists to prevent.

Worked case: measure 03, where the catalogue read as covered and nothing was installed

AN:RES:Resilience Measure:03 specifies supply-chain provenance verification **at integration**, and its TRE is AST:FW:Firmware:01, the on-board computer boot firmware. That vehicle is in orbit. Integration happened before launch. The measure cannot be installed on the element it protects: the lifecycle is **fixed** and the cadence is **next-build**.

The second half is worse. The paired signature AN:DET:Detection Signature:03 cannot fire either, because Function 03 recorded its required source as a **Gap**. So against the one threat that reaches the flight computer, Kestrel holds nothing today: no control on the element, and no visibility of it. Before these fields existed, this entry read on the page exactly like measures 00 and 01, which are installed. That is the failure the cadence field exists to prevent. A catalogue that reads as covered where nothing is installed is worse than one that admits the gap, because it stops anyone looking.

The compensating control, recorded on the entry. Measured boot cannot be installed on AST:FW:Firmware:01 in orbit, so the flight firmware is protected from the ground instead: dual approval on every image entering the patch deployment pipeline AST:SW:Software:03, provenance verification before staging, and a hold on any push outside a window on SVC:CP:Control Plane:02. This does not make the flight firmware trustworthy; it makes it harder to reach. That sentence is part of the record, not a caveat on it: harden what the adversary must cross, and say what you have not fixed.

The residual risk, recorded with its owner. The flying vehicle carries no boot-time attestation and its signature AN:DET:Detection Signature:03 cannot fire. A tampered image that reaches the on-

board computer is undetected on orbit. Owner: Satellite Design and Engineering, closed by measured boot on the next build.

Nothing else about the entry moves: same ordinal, same TRE, same goal, same owner. What changes is that a reader can now tell a measure that is running from a measure waiting on a spacecraft nobody has built yet.

Worked case: measure 02, one record with two lifecycles

AN:RES:Resilience Measure:02 bundles two things. The pre-arranged backup band and the automatic switching threshold are configuration and procedure, and Satellite Operations can adopt them now. The frequency-agile spread-spectrum waveform is not: the entry itself assigns it to Satellite Design and Engineering, and it lives in the radio of a spacecraft that is already flying. One record, two lifecycles, which is why the lifecycle reads **through** and the cadence reads **phased**.

The compensating control. The pre-arranged backup band and the automatic switching threshold are installable now on SVC:HY:Hybrid:02, and carry the measure until the agile waveform flies. Satellite Operations owns the procedure.

The residual risk. Until a frequency-agile spread-spectrum waveform flies, the link can be denied faster than a band switch can be authorized. Owner: Satellite Design and Engineering, for the next spacecraft.

Why this is one record and not two. The chain requires exactly one measure per ordinal: threat, path, signature and measure all carry 02 and all name AST:SI:Signal:00. Splitting the measure into an operations entry and an engineering entry would put two measures on one ordinal and break the property the whole week rests on. The two lifecycles are expressed where they belong, in the cadence, the compensating control and the residual risk, so a reader sees one measure and can still tell which half is running.

And the two that need neither field. Measures 00 and 01 protect elements that are reachable now, a ground control-plane service and the operator console software, so their lifecycle is **reachable**, their cadence is **in-force**, and they carry no compensating control and no residual risk. Read the four entries together and the catalogue says out loud what it holds: two measures running, one running in part, one waiting for the next build.

THE DIGITAL TWIN

A digital twin is a high-fidelity virtual replica of the operational system, pairing flight software, simulated subsystems, and an RF-environment model so a candidate measure runs end to end in simulation. Every AN-RES measure changes how the platform behaves under stress, so the twin is where measures are validated, adversary scenarios rehearsed, and trade-offs quantified before a measure is accepted into the design. It also collapses the engineering loop: on the twin a change is designed, developed, and validated in hours rather than days, and defects are caught where they are cheapest to fix.

The deck argues for the twin across two slides but never shows a twin result. Here is what one looks like for measure 02, so the argument becomes a method you can run.

Twin run · validating AN:RES:Resilience Measure:02, frequency-agile link

Question: does automatic band-switching keep the command link usable under the jamming profile of AN:ATT:Attack Path:02, and what does it cost?

Scenario: replay the chain-02 profile against the twin: sustained noise injection across the primary uplink band, timed to an overhead pass, run twice, once with the agility waveform enabled and once without.

Without the measure: noise floor crosses the threshold, the link degrades then loses lock, and the command window is lost for the remainder of the pass. Commanding waits for the next contact.

With the measure: the switch fires at threshold and commanding continues on the backup band for the remainder of the pass, at reduced throughput.

The cost, quantified: the agility waveform consumes additional power and the backup band carries lower throughput, so downlink margin and duty cycle both fall while the measure is active. That is the trade-off curve, and it is why this is an engineering decision rather than an obvious yes.

The abuse case, also run: an adversary who learns the threshold could deliberately trip it to herd the platform onto the weaker band at will. The threshold logic is exercised against exactly that abuse on the twin before it flies.

Rejection criterion: if the measure cannot hold the command link through the simulated attack, or if the duty-cycle cost breaks the mission profile, it is rejected on the evidence rather than on argument.

Every measure in chapter 4 carries the twin question it would be validated by, so this pattern generalizes rather than sitting as a single example.

WHY THIS IS A REPEATABLE PROCESS

The 2025 CNSS update requires a hardware root of trust for secure reboot, and the DHS model lets operators share Indicators of Behavior to warn their peers. Compliance is not one-and-done: under FISMA and the NIST Risk Management Framework (SP 800-37 Rev. 2), a subset of security controls must be assessed at least annually. That is why resilience is a repeatable, cross-organizational process rather than a one-time fix, and why the resilience set is explicitly a living artifact: as the architecture, the attack-path set, and the adversary evolve, the set evolves with them. (Source: Air and Space Forces Magazine, 19 November 2025.)

CH 4 THE CATALOGUE, COMPLETE

“Every measure names the one platform element it protects, the threat or attack path it counters, the resiliency goal, and the department that owns it.”

DEEP DIVE DECK, SLIDES 12 THROUGH 15 · RESILIENCE MEASURES: GROUND, LINK, SPACE ·
WEEK-FINAL ENUMERATED RESILIENCE MEASURES

How to read each entry. The first row is the anchor: the one element the TRE names, inherited from the AN-THR this measure counters. Everything under it is the record a department acts on. The lifecycle and cadence rows answer the question chapter 3 taught, whether the measure can be installed on the element it protects and what the organization holds today, and where the cadence is not in force the next two rows carry the compensating control and the residual risk. The reach paragraph after each table lists the further elements the protection touches, printed so the difference between the anchor and the reach is visible, which the deck cannot show at a glance. The twin question is what the measure would be validated by before it is accepted.

GROUND · 2 AN-RES

AN:RES:Resilience Measure:00 · Zero-trust segmentation of the device management plane

Air-gap or strict zero-trust segmentation of the device management plane from external networks; hardware-rooted attestation on any management-plane access; dual-approval workflow on firmware pushes with enforced maintenance windows.

FIELD	VALUE
TRE (anchor)	SVC:CP:Control Plane:09
What that is	The ground command-acceptance service. The one element this measure protects, taken from AN:THR:Threat:00 . Day 3 walked to it and Day 4 watches it.
Counters	AN:ATT:Attack Path:00 · AN:THR:Threat:00
Goal	Anticipate: it removes the high-impact path entirely by raising the barrier to management-plane access
Owner	Both. Satellite Design and Engineering owns the segmentation and dual-approval rebuild; Satellite Operations owns the maintenance-window discipline.
Lifecycle	reachable . The ground command-acceptance service can be changed now, so the measure is applied to the element itself.
Cadence	in-force . Installed, or installable this quarter.
Compensating control	None, and none needed. The cadence is in force, so nothing is standing in for this measure.
Residual risk	None recorded. Nothing about this measure is deferred.
Source	Viasat, CISA, and SentinelLabs KA-SAT post-incident guidance (2022); NIST SP 800-207 (Zero Trust Architecture)
Twin question	Does an operator still complete a legitimate emergency firmware push inside the dual-approval workflow within the pass window, and what does the added latency cost?

AN-RES ANCHORS · 1 OF 4 ENTRIES · AFTER AN:RES:RESILIENCE MEASURE:00

AN-RES anchors · TRE, Target of Resilience Enhancement

Layer 5 has no parent. Each entry names exactly one platform element through its TRE field.



One measure, one anchor. The measure sits in Layer 5 and names one platform element through its TRE field. What the segmentation additionally shields is in the reach paragraph below, not in this figure, because the reach is description and the anchor is the target.

Why this looks like Monday's figure. It is the same figure with a different tag. That is the point of the chain: AN:RES:Resilience Measure:00 names the element AN:THR:Threat:00 named, so the box on the right has not moved all week.

Reach behind the anchor. Segmenting the management plane also shields the ground crypto service (SVC:CP:Control Plane:08), the patch deployment software (AST:SW:Software:03) and the patch binary store (AST:DA:Data:02), because the route to all three ran through the management plane. None of those is a second TRE. They are what the anchor buys, and they belong in this paragraph so a reader can tell protection from target.

FIELD NOTE Both ground measures need both departments, and a measure owned by everyone is owned by no one. Ruling: Owner is recorded as Both, with the split named. Satellite Design and Engineering builds the segmentation and the dual-control workflow; Satellite Operations holds the maintenance-window and peer-review discipline. First win: every ground measure now has a signature under it, so nothing waits on an unnamed owner.

AN:RES:Resilience Measure:01 · Dual-control commanding for high-impact actions

A second operator must approve before transmission; per-operator behavior baselines and pre-pass briefings make out-of-pattern actions stand out.

FIELD	VALUE
TRE (anchor)	AST:SW:Software:04
What that is	The operator console software. The one element this measure protects, taken from AN:THR:Threat:01 . Day 3 walked to it and Day 4 watches it.
Counters	AN:ATT:Attack Path:01 · AN:THR:Threat:01
Goal	Withstand: a single insider cannot act alone on high-impact sequences
Owner	Both. Satellite Design and Engineering owns the dual-control workflow in the commanding software; Satellite Operations owns the operational discipline of peer review.
Lifecycle	reachable . The operator console software can be changed now, so the approval gate is built into the element itself.
Cadence	in-force . Installed, or installable this quarter.
Compensating control	None, and none needed. The cadence is in force.
Residual risk	None recorded. Nothing about this measure is deferred.
Source	NIST SP 800-53 SC-3 and AC-6 (separation of duties, least privilege); NIST SP 800-160 v2 withstand-goal guidance
Twin question	Under a time-critical anomaly, does dual control delay a legitimate recovery command past the point of safety? If it does, the measure needs a defined break-glass path, itself audited.

AN-RES ANCHORS · 2 OF 4 ENTRIES · AFTER AN:RES:RESILIENCE MEASURE:01



The second measure anchors to an asset, so it draws in the asset colour. Two measures, two structural layers, and in both cases the anchor was inherited rather than chosen.

What you do not choose. The anchor is not an authoring decision on Day 5. It was fixed on Day 2. If you find yourself picking a different element, either the measure counters a different threat than you think, or the threat was anchored wrong, and that is a Day 2 defect to raise rather than a Day 5 workaround.

Reach behind the anchor. Dual control also constrains the console workstation (AST:HW:Hardware:04), console operations (SVC:CP:Control Plane:13) and the ground command-acceptance service (SVC:CP:Control Plane:09), since the approval gate sits between the operator and all three. The TRE still names one element: the console software, where the gate is built.

Note the feedback loop. This measure is also what turns Day 4's Signature 01 from Partial to something stronger: the peer-review tag stream that the signature depends on is produced by the dual-control workflow this measure builds. Function 05 is not only defending against the adversary, it is closing the dependencies Function 04 had to declare.

LINK · 1 AN-RES

AN:RES:Resilience Measure:02 · Frequency-agile spread-spectrum link with backup band

Frequency-agile and spread-spectrum link operation with a pre-arranged backup band; the band switch fires automatically when the noise floor exceeds threshold.

FIELD	VALUE
TRE (anchor)	AST:SI:Signal:00
What that is	The uplink and downlink waveforms. The one element this measure protects, taken from AN:THR:Threat:02. Day 3 walked to it and Day 4 watches it.
Counters	AN:ATT:Attack Path:02 · AN:THR:Threat:02
Goal	Withstand: communications continue under sustained interference
Owner	Both. Satellite Design and Engineering owns the frequency-agile waveform implementation; Satellite Operations owns the band-switching procedure.
Lifecycle	through. The waveforms live in a radio that is already flying, so the measure reaches them through the band plan and the switching procedure the ground does control.
Cadence	phased. The backup band is adoptable now; the frequency-agile waveform belongs to the next build.
Compensating control	The pre-arranged backup band and the automatic switching threshold are installable now on SVC:HY:Hybrid:02, and carry the measure until the agile waveform flies. Satellite Operations owns the procedure.
Residual risk	Until a frequency-agile spread-spectrum waveform flies, the link can be denied faster than a band switch can be authorized. Owner: Satellite Design and Engineering, for the next spacecraft.
Source	ITU interference-mitigation guidance; SPARTA SPACE-T1429 mitigation patterns
Twin question	The worked run in chapter 3: does the link hold under the chain-02 jamming profile, at what duty-cycle and downlink cost, and can an adversary herd the platform by tripping the threshold?

AN-RES ANCHORS · 3 OF 4 ENTRIES · AFTER AN:RES:RESILIENCE MEASURE:02

AN-RES anchors · TRE, Target of Resilience Enhancement

Layer 5 has no parent. Each entry names exactly one platform element through its TRE field.



The link measure joins. Its anchor is a signal asset, which is a reminder that the target layer follows the source rather than the segment: any structural layer may be named, PCE included, at the lowest layer the source resolves.

The measure is written before it is exercised. Nothing on this platform has yet run the agility waveform under a real jamming campaign. The measure is enumerated anyway, which is what makes coverage auditable: a reviewer walks the four paths and asks whether each carries a measure or an accepted residual risk, not whether each has already been tested.

Reach behind the anchor. Band agility also protects the link access control authority (**SVC:CP:Control Plane:05**), the FEC and ECC service (**SVC:HY:Hybrid:01**) and tracking (**SVC:HY:Hybrid:02**), all of which degrade with the waveform. The TRE names the waveform because that is the element the threat named.

FIELD NOTE Satellite Operations wanted the band switch automatic, at machine speed; Satellite Design and Engineering warned that an adversary who learns the threshold could herd the platform onto the backup band at will. Ruling: the switch stays automatic, and the threshold logic is exercised on the digital twin against exactly that abuse before it flies. First win: the jamming response is rehearsed in simulation rather than argued in a meeting.

SPACE · 1 AN-RES

AN:RES:Resilience Measure:03 · Measured-boot firmware and supply-chain attestation

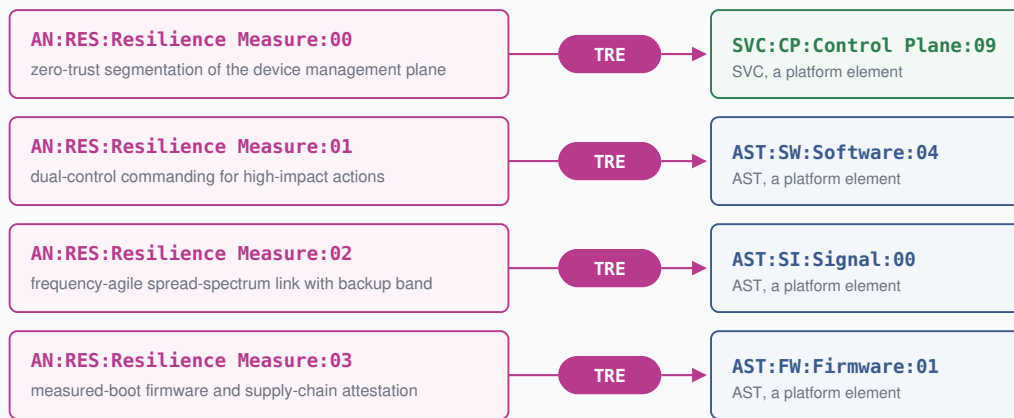
Measured-boot firmware attestation with signed-vendor manifest; supply-chain provenance verification at update; quarantine of any component whose hash does not match the signed expected value.

FIELD	VALUE
TRE (anchor)	AST:FW:Firmware:01
What that is	The on-board computer boot firmware. The one element this measure protects, taken from AN:THR:Threat:03 . Day 3 walked to it and Day 4 recorded the boot-attestation gap on it.
Counters	AN:ATT:Attack Path:03 · AN:THR:Threat:03
Goal	Anticipate: tampered firmware never reaches an operational role
Owner	Satellite Design and Engineering, sole owner of the measured-boot architecture, the signing pipeline, and the supply-chain verification process.
Lifecycle	fixed . The on-board computer boot firmware is fixed for its service life, and attestation specified at integration cannot be applied to a vehicle that has already launched.
Cadence	next-build . Nothing in this measure can be installed on the flying platform.
Compensating control	Measured boot cannot be installed on AST:FW:Firmware:01 in orbit, so the flight firmware is protected from the ground instead: dual approval on every image entering the patch deployment pipeline AST:SW:Software:03 , provenance verification before staging, and a hold on any push outside a window on SVC:CP:Control Plane:02 . This does not make the flight firmware trustworthy; it makes it harder to reach.
Residual risk	The flying vehicle carries no boot-time attestation and its signature AN:DET:Detection Signature:03 cannot fire. A tampered image that reaches the on-board computer is undetected on orbit. Owner: Satellite Design and Engineering, closed by measured boot on the next build.
Source	NIST SP 800-193 (Platform Firmware Resilience); SLSA supply-chain guidance
Twin question	Does attestation reject a tampered image without also rejecting a legitimate emergency patch, and what is the recovery path if a valid image fails verification on orbit?

AN-RES ANCHORS · 4 OF 4 ENTRIES · THE COMPLETE DAY-5 RESILIENCE ANCHOR MAP

AN-RES anchors · TRE, Target of Resilience Enhancement

Layer 5 has no parent. Each entry names exactly one platform element through its TRE field.



Each AN-RES entry with its one TRE target, the enumerated platform element from its catalogue entry, in the layer colours of the structural ETEN reference.

Four measures, four anchors, and the same four elements Day 2 produced. This figure and the Module 02, 03 and 04 figures are identical on the right-hand side, which is what a working chain looks like at the end of a week.

What the chain bought. Four elements were named once on Monday and carried through four functions without a single cross-reference table. An auditor holding ordinal 03 holds the threat, the route, the signature and the measure, and can ask the only question that matters: is this exposure countered, or is the residual risk accepted on the record?

Reach behind the anchor. Measured boot and manifest verification also protect the telecommand service (SVC:CP:Control Plane:04), the electrical power service (SVC:CP:Control Plane:02) and the repeater firmware (AST:FW:Firmware:02), because a tampered load reaching any of them is rejected by the same attestation. The TRE names the on-board computer boot firmware because that is the element the threat named.

FIELD NOTE This measure was argued twice before Day 5: Day 3 enumerated the boot-attestation hook as a gap with an owner, and Day 4 recorded coverage as conditional on it. Ruling: Satellite Design and Engineering signs as sole owner of the measured-boot architecture, the signing pipeline, and the supply-chain verification. Second ruling, once the cadence was written down: the measure is **NEXT-BUILD**, so the entry carries the ground-side compensating control and the residual risk rather than reading as covered. First win: the moment attestation flies, Day 4's conditional signature turns Full without another meeting, and the residual risk closes with it.

PART III

Putting it to work

Who reads what you wrote, and how it leaves the room as machine-readable intelligence rather than a document a partner has to re-key.

CH 5 The Week in Hand

CH 6 Tag and Share

CH 5 THE WEEK IN HAND

“End of week. You now hold a working decomposition, an anchored threat set, an attack-path set, a signature and playbook set, and a resilience-measure set against the same reference platform.”

DEEP DIVE DECK, SLIDE 22 · DAY 5 COMPLETE / COURSE COMPLETE

THE FIVE SETS

DAY	FUNCTION	SET	SIZE	ANCHOR FIELD
1	F01 Concept of Operations	The CONOPS decomposition	44 elements (4 PCE, 4 SEG, 15 SVC, 21 AST)	PARENT
2	F02 Contextualized Threat Modeling	AN-THR threat catalogue	4 (Ground 2, Link 1, Space 1)	TOE
3	F03 Converged Detection Engineering	AN-ATT attack paths	4, with 12 waypoint hooks	TOE, one element, the same one the threat names
4	F04 Incident Response Preparation	AN-DET signatures plus playbooks	4 + 4	TDM, that same element
5	F05 Adversary Management	AN-RES resilience measures	4	TRE, that same element

Read the last column downward. From Function 02 onward the anchor field changes name and the element does not: TOE, TOE, TDM, TRE, all naming one thing. That is the chain, and it is why an ordinal is enough to hold a whole chain.

ONE ORDINAL, ALL FIVE FUNCTIONS

The course claims that a single identifier chain runs through every function. Here it is for ordinal 01, in full:

FUNCTION	ELEMENT	WHAT IT ADDED	OWNER
F01	AST:SW:Software:04	The operator console software exists, is named once, and sits under console operations, the Ground segment, and the Terrestrial environment.	SatOps and SD&E jointly, as the CONOPS
F02	AN:THR:Threat:01	An adversary with stolen or coerced command authority would target it. TOE names that one element.	Security Operations
F03	AN:ATT:Attack Path:01	The route to it: console hardware, then the console software itself, then console operations. What a defensive cyber operator must hold to see it is carried on the path itself, as required data sources; this path needs no signal source. TOE names that same element.	SD&E with the SOC
F04	AN:DET:Detection Signature:01 + PB-01	A rule that fires on out-of-pattern command authority, and the playbook that contains, recovers, and reports when it does. TDM names that same element.	Security Operations
F05	AN:RES:Resilience Measure:01	Dual control, so a single compromised operator cannot execute the high-impact action at all. TRE names that same element.	Both operating departments

One element, four target fields. The element never changes across that table. What changes is the question being asked about it: F02 asks what an adversary wants with it, F03 asks how they reach it, F04 asks what would be visible, F05 asks what to change. Four questions, four field names, one *AST:SW:Software:04*. If any row named a different element, the chain would be broken and the reader would need a cross-reference table to reassemble it.

What each function added that the previous one could not. F01 gave the element a name every department uses. F02 said an adversary wants it. F03 said how they would reach it and where that reaching is visible. F04 made the visibility fire and gave the response an owner and a clock. F05 removed the opportunity, or narrowed it, so the earlier layers have less work to do. Remove any one link and the chain breaks: a threat with no element is intelligence, a path with no threat is speculation, a signature with no path watches nothing in particular, and a measure with no accumulated evidence is a guess about where to spend.

WHAT RECURS, AND WHAT TO PROTECT NEXT

Read the accumulated set for repetition. **SVC:CP:Control Plane:09**, the ground command-authorization service, appears in two threats, two attack paths, two detection signatures, and two resilience measures: it is the single most recurrent element of the week. That recurrence is the adversary-management answer. Elements that keep appearing are where the adversary keeps having to go, so they are where hardening buys the most, and they are also where a single failure costs the most. The next measure this platform needs is not chosen by which threat is scariest, it is chosen by counting.

YOUR ROLE ACROSS THE WEEK

Adversary management is the fifth and final function where a Full Spectrum professional drives change, and you do not have to be the resilience engineer or the operator to lead it. Resilience needs both operating procedures and architectural change, and Satellite Operations and Satellite Design and Engineering can sometimes be provided by separate organizations from each other and from Security Operations. Your job is to build the cross-functional team and get them to commit measures together. Across the week, these five functions have been your deliberate points of insertion: each one is where you reach across organizational lines and transform how those departments defend the platform together.

CH 6 TAG AND SHARE

TAG meteorstorm:AN="AN-RES"

A peer operator receives the measure, the one element it protects, what it counters, its resiliency goal, and its owner split. If the measure was validated on a twin, the twin run travels with it: a reproducible, vendor-neutral artifact that ports across Space ISAC members and forms the empirical basis for shared resilience rather than shared opinion. That is the strongest thing this week produces for the community, because a peer can rerun the scenario on their own twin and compare.

Module 05 Adversary Management Workbook · Full Spectrum Space Cybersecurity Professional

4 AN-RES · Ground 2 + Link 1 + Space 1 · per NIST SP 800-160 v2