



VEYRUM ROBOTICS STANDARD



VRS-DEF-110

Defence & Security — Demonstration Protocol

The Defence & Security sector's witnessed steps for a Certified rating — configuration inspection confirming no weapons function, own-force and bystander protection at speed and load, positioning-denied and link-loss behaviour, field maintainability by unit-level maintainers, zeroisation and tamper response, update and access controls — run in the same session as the intrinsic protocol.

VEYRUM RESEARCH INSTITUTE

DOCUMENT

VRS-DEF-110

VERSION

1.0.0

STATUS

Draft

DATE

16 September 2026

Contents

1 Introduction

2 1 Scope

3 2 Normative references

4 3 Terms and definitions

5 4 Relationship to the intrinsic protocol

6 5 The declared envelope

7 6 The steps

7.1 6.1 Part 1 – Scope integrity

7.2 6.2 Part 2 – Own-force and bystander protection at speed and load

7.3 6.3 Part 3 – Contested-environment integrity

7.4 6.4 Part 4 – Environmental qualification present at the site

7.5 6.5 Part 5 – Field maintainability by unit-level maintainers

7.6 6.6 Part 6 – Capture and compromise resilience

7.7 6.7 Part 7 – Cyber accreditation practice

8 7 Worked example (informative)

9 Annex A (normative) – Criterion coverage

10 Bibliography

11 Change history

Foreword. This Test Protocol is new in the VRS 2026 edition and is the Defence & Security sector’s extension of VRS-GEN-203, the intrinsic demonstration protocol. The sector’s scope is fixed by VRS-DEF-001: the rated configurations are unarmed platforms — logistics and reconnaissance vehicles, explosive-ordnance and CBRN robots, perimeter-security platforms, maritime-security surface vessels — and the first step of this Protocol is the inspection that confirms it, on camera, against the manufacturer’s attestation. What follows is largely what the Field & Outdoor and Hazardous & Emergency protocols witness, in the conditions this sector adds: the operating area contains own-force personnel and base traffic; positioning and links are denied, jammed or spoofed rather than merely lost; the maintainer is a soldier with an organic tool kit and a card, not a technician with a workshop; and a captured or abandoned platform must give up nothing. Every denial or spoofing input is the manufacturer’s own, applied lawfully in a shielded enclosure or on the range route. The Protocol carries only what the intrinsic steps do not already witness; accreditation, export status and the incident record are documentary. Steps run between Parts E and F of VRS-GEN-203, in the same session, on the same feed, into the same export. Standards carry no step identifiers; every step here names the VRS-DEF-201 subclause that requires it. As a protocol it is versioned vX.Y.Z (VRS-GEN-004 §5.4). Requirements use “shall”.

1 Introduction

The Defence & Security anchor set is the military environmental-test standard family, the national and coalition cyber-accreditation regimes, the functional-safety standards the platforms inherit from their civil counterparts, and — for the explosive-ordnance and CBRN class — the same response-robot test methods the Hazardous & Emergency sector uses. Much of it is documentary by nature: accreditation is granted, export status is declared, the incident record is what public and declassified sources show. The Certified tier adds a witnessed session on a stock, unarmed unit, run by an observer who did not build it.

The steps concentrate on the conditions that distinguish the sector. Own-force protection is witnessed with human-sized and prone targets at speed and load, and with base-traffic behaviour at a marked crossing and gate. Contested-environment integrity is witnessed by denying and — where the manufacturer can do so lawfully in a shielded enclosure — spoofing positioning, and by degrading then cutting the link. Maintainability is witnessed as a unit-level maintainer would experience it: organic tools, a card, the field. And compromise resilience is witnessed end to end: zeroise, remote disable, tamper, and a removed storage module that reads as nothing. No hazard is introduced; the environmental step uses only a condition present at the site.

2 1 Scope

This Protocol specifies the Defence & Security demonstration steps by which the criteria of VRS-DEF-201 Clause 6 are demonstrated at the Certified tier, for every application class of VRS-DEF-201 §7.3 (ground UGV (logistics/ISR) · EOD/CBRN · base/perimeter security · maritime security USV). It applies to every Certified Defence & Security assessment, by every Certified route of VRS-GEN-003 §6.9.

It specifies: how this Protocol relates to VRS-GEN-203 (Clause 4); the envelope the manufacturer declares before the session (Clause 5); the steps (Clause 6); and a worked example (Clause 7). Annex A maps every VRS-DEF-201 criterion to its intrinsic steps, its sector steps, or neither.

It does not: repeat any session requirement, step, marking rule or record rule of VRS-GEN-203, all of which apply unchanged; define any criterion, point, ceiling or ladder (VRS-DEF-201); or define the Defence & Security information pack (VRS-GEN-013). The assessed configuration carries no weapons function (VRS-DEF-001); the first step confirms it. No person is in the operating area as a detection target; human-sized and prone test targets stand in. Every positioning-denial, spoofing or link-interference input is the manufacturer's own, applied lawfully within a shielded enclosure or on the range route.

3 Normative references

- **VRS-GEN-203**, Demonstration Protocol – Intrinsic – session requirements (Clause 4), step rules (Clause 5), marks and scores (Clause 7), Session Record (Clause 8), all of which apply to this Protocol.
- **VRS-DEF-201**, Defence & Security – AR Assessment Protocol – the criteria whose Certified rows this Protocol serves; application classes (§7.3).
- **VRS-DEF-001**, Defence & Security Sector Standard – the declared envelope and class fields.
- ◦ **VRS-GEN-101**, Safety – the intrinsic safety criteria the Defence & Security pool contributes to.
- ◦ **VRS-GEN-103**, Serviceability & Support – the intrinsic module-swap and fault-recovery steps that serve parts of VRS-DEF-201 §6.5.
- ◦ **VRS-GEN-105**, Cyber Posture – the intrinsic steps that witness parts of VRS-DEF-201 §6.6 and §6.7.
- ◦ **VRS-FLD-110** and **VRS-HAZ-110** – the sibling sector protocols whose physical steps this Protocol parallels for the same platform types.
- **VRS-GEN-003**, Governance Charter and Independence – Certified routes and route parity (§6.9).

4 Terms and definitions

Terms defined in VRS-GEN-001 and VRS-GEN-203 apply. In addition:

3.1 assessed configuration – the unarmed platform configuration recorded for the rating, with its payload interfaces, mounts and software build, as attested by the manufacturer under VRS-DEF-001.

3.2 own-force personnel – people in the vehicle's operating area who are part of the operating unit; represented in this Protocol by human-sized and prone test targets.

3.3 base traffic – vehicles, crossings and gates on a marked base-road layout, represented by vehicle-sized targets and floor marks.

3.4 positioning denial – removal of satellite positioning by the manufacturer's own means (shielding, receiver disable, test mode).

3.5 spoofing — a false positioning input staged by the manufacturer, applied only where lawful and only within a shielded enclosure or on the range route.

3.6 organic tool kit — the declared tools carried by or issued to the operating unit for unit-level maintenance.

3.7 maintainer card — the declared unit-level maintenance instruction the maintainer works from.

3.8 zeroisation — the declared command that erases keys, mission data and maps and places the platform in its disabled state.

3.9 tamper trigger — a declared physical event (enclosure opened, storage removed, switch actuated) that produces the declared tamper response.

5 4 Relationship to the intrinsic protocol

4.1 This Protocol shall be run only as part of a session under VRS-GEN-203. Every requirement of VRS-GEN-203 Clause 4 applies to every step here without repetition or exception.

4.2 Position in the session. The steps of Clause 6 shall run after VRS-GEN-203 Part E and before VRS-GEN-203 Part F, so that one continuous recording and one export cover both protocols. The endurance sample opened in VRS-GEN-203 Part C continues to run through this Protocol.

4.3 Step identifiers. Steps shall carry identifiers of the form DEF-110.nn ; they are Session Record step identifiers under the same rules as VRS-GEN-203 §5.1 and shall never be reused.

4.4 Required by. Every step shall name the VRS-DEF-201 subclause(s) whose Certified row it serves. VRS-DEF-201 carries no reference back to this Protocol.

4.5 Classes and declared subjects. Each step lists the application classes it applies to. A step whose class is not in the assessed envelope shall not be run. A step whose subject the manufacturer has not declared shall be marked *not declared* and has no effect on any score (VRS-GEN-203 §3.10). DEF-110.01 and Parts 2, 3 and 6 shall be run for every Defence & Security assessment; Part 4 only where a declared condition is present at the site.

4.6 Bound. The sum of step bounds for one class shall not exceed 120 min. Marks, failure, declined steps, continuation sessions and the Session Record follow VRS-GEN-203 Clauses 5, 7 and 8.

4.7 Criteria witnessed by intrinsic steps. Where a sector criterion's Certified row is already witnessed by intrinsic steps, Annex A names them and the criterion is scored from those marks together with any sector steps listed. VRS-DEF-201 §6.1 (scope integrity) is witnessed directly by DEF-110.01; a configuration found to carry a weapons function or provision for one shall end the session and the assessment shall not proceed at any tier for that configuration (VRS-DEF-001).

4.8 Scope integrity. Where DEF-110.01 finds a weapons function, a fire-control interface or a provision for one without hardware change, the observer shall close the session, mark every remaining step *not run*, and record the finding; the configuration is outside the scope of VRS-DEF-001 and shall not be rated.

4.9 Lawful inputs and people. Every positioning-denial, spoofing or radio-interference input shall be the manufacturer's own, applied within a shielded enclosure or on the range route under the site's authorisation, and shall not radiate beyond it. No person shall be in the operating area as a detection

target or in the vehicle's path during motion; targets stand in (VRS-GEN-203 §4.8). A step so performed shall be marked *not achieved* and the ground recorded.

4.10 Classification. Nothing in the session shall require the disclosure of classified or export-controlled information; where a declared function cannot be shown for that reason, the step shall be marked *declined* with the ground recorded and the criterion scored accordingly, and the manufacturer may substitute a Verified-evidence statement under VRS-GEN-012.

4.11 Admissibility of a mark. A step's mark shall be inadmissible, and the step shall be marked *not achieved*, where the dimension, mass, speed, force or condition it depends on was not shown on camera, or where the configuration demonstrated differs from the assessed one. The observer shall record the ground.

6 5 The declared envelope

5.1 Before the session the manufacturer shall have declared, in the information pack and per assessed application class: the application class and the configuration record with the attestation reference; maximum speed (m/s), payload (kg), worst surface and stopping distance (m); the human-sized and prone target profiles (mm); the base-road layout with following distance (m) and gate standoff (m); the positioning-denial and (where lawful) spoofing means and the declared safe degradation with its stop distance (m); the link-degraded threshold and the loss fail-safe with its distance and time (m, s); any site condition offered for Part 4; the field-replaceable modules, organic tool kit, maintainer card and field-repair, pack-swap and fault-recovery times (min); the zeroisation and remote-disable commands, the re-provisioning means and the encryption state; the tamper triggers and responses; and the update mechanism, roles and authentication token.

5.2 Every apparatus in Clause 6 shall be sized from those declarations and no other source (VRS-GEN-203 §4.7). A parameter not declared makes the steps that depend on it *not declared* (4.5); a manufacturer that declares a smaller envelope demonstrates a smaller envelope and is scored against it under VRS-DEF-201.

5.3 The declared envelope shall match the one recorded for the rating (VRS-DEF-001, VRS-GEN-009); a step demonstrated at a value other than the declared one shall be inadmissible (4.11).

7 6 The steps

Columns: **ID** — Session Record step identifier · **Step** — outcome to witness · **Classes** — application classes the step applies to (4.5) · **Witness** — means (VRS-GEN-203 §3.13) · **Apparatus** — manufacturer-supplied, at declared value · **Bound** — minutes · **Required by** — VRS-DEF-201 subclause(s) served.

7.1 6.1 Part 1 — Scope integrity

The step that fixes the sector's scope: an unarmed configuration, confirmed on camera against the attestation before any other sector step runs (4.8).

ID	STEP	CLASSES	WITNESS	APPARATUS	BOUND	REQUIRED BY
DEF-110.01	Configuration inspection – no weapons function. The assessed unit is inspected on camera against the manufacturer’s configuration record: every payload interface, mount and connector is shown and identified; no weapons function, fire-control interface or provision for one without hardware change is present; the software build shown on the console matches the attested non-weaponised build; the demonstrator reads the attestation reference on camera. The identity and stock-standard declarations of the intrinsic open are re-confirmed for this configuration.	all	CAM+FEED	Manufacturer’s configuration record and attestation	10 min	Required by VRS-DEF-201 §6.1

7.2 6.2 Part 2 — Own-force and bystander protection at speed and load

The operating area contains own-force personnel and base traffic. Targets stand in for both.

ID	STEP	CLASSES	WITNESS	APPARATUS	BOUND	REQUIRED BY
DEF-110.02	Personnel target entering the operating area at speed and load. Laden to the declared payload, at the declared maximum speed on the declared worst surface, a human-sized test target of the declared profile enters the protective zone from the side; the vehicle stops before contact within marks set at the declared stopping distance; repeated with the target stationary and prone in the path; the feed shows the stop and its trigger.	all	CAM+FEED+APP	Human-sized and prone targets at declared dimensions on a line or trolley; worst-surface sample; marks; declared load	12 min	Required by VRS-DEF-201 §6.2
DEF-110.03	Base-traffic and convoy behaviour. On a marked base-road layout the	ground UGV (logistics/ISR) · EOD/CBRN · base/perimeter security	CAM+FEED+APP	Marked crossing and gate; vehicle-sized lead target on a	10 min	Required by VRS-DEF-201 §6.2

ID	STEP	CLASSES	WITNESS	APPARATUS	BOUND	REQUIRED BY
	vehicle yields at a marked crossing to a vehicle-sized target, holds the declared following distance behind a lead target at the declared speed, and stops for a barrier or gate at the declared standoff; the feed shows each state.			trolley or towed		

7.3 6.3 Part 3 — Contested-environment integrity

Positioning is denied and, where lawful, spoofed; the link is degraded and cut. Every input is the manufacturer’s own, inside a shielded enclosure or on the range (4.9).

ID	STEP	CLASSES	WITNESS	APPARATUS	BOUND	REQUIRED BY
DEF-110.04	Positioning denied and spoofed. With satellite positioning denied by the manufacturer's own means (shielding, receiver disable or declared test mode) and, where the manufacturer can stage it lawfully within a shielded enclosure or on the range route, a spoofed positioning input applied, the vehicle detects the condition, flags it on the console and enters its declared safe degradation (dead-reckon to a stop within the declared distance, hold, return by inertial or visual navigation); the boundary is not crossed.	all	CAM+FEED+APP	Manufacturer's denial and (where lawful) spoofing means in a shielded enclosure; boundary and distance marks	12 min	Required by VRS-DEF-201 §6.3
DEF-110.05	Link interference and loss. The command link is degraded and then cut by the manufacturer's own means	all	CAM+FEED+APP	Means of degrading and cutting the link; marks	8 min	Required by VRS-DEF-201 §6.3

ID	STEP	CLASSES	WITNESS	APPARATUS	BOUND	REQUIRED BY
	(attenuation, shielded enclosure, inhibit); the vehicle warns at the declared degraded threshold and on loss performs its declared fail-safe (stop, hold, return to the last link point) within the declared distance and time; link state and behaviour are shown when the link is restored.					

7.4 6.4 Part 4 — Environmental qualification present at the site

Conditional. Only a condition already present at the site.

ID	STEP	CLASSES	WITNESS	APPARATUS	BOUND	REQUIRED BY
DEF-110.06	Declared theatre condition present at the site. Where a declared condition (temperature, sand or dust, immersion or spray, vibration on a declared rough track) is present at the site and can be shown safely, the vehicle performs a representative task in it; the condition reading and the vehicle’s state are shown on the feed.	all	CAM+FEED	The site condition; the manufacturer’s meter where applicable	10 min	Required by VRS-DEF-201 §6.4 — Conditional — recorded as not present otherwise

7.5 6.5 Part 5 — Field maintainability by unit-level maintainers

A soldier with an organic tool kit and a card, in the field — not a technician in a workshop.

ID	STEP	CLASSES	WITNESS	APPARATUS	BOUND	REQUIRED BY
DEF-110.07	Module swap with organic tools. One declared field-replaceable module is replaced by the demonstrator, acting as a unit-level maintainer with the declared organic tool kit and the maintainer card or manual only, in field conditions (outdoors or in the declared field environment); time from video against the declared field-repair time; the vehicle returns to service and the swap is logged.	all	CAM+FEED	Spare module; declared organic tool kit; maintainer card	15 min	Required by VRS-DEF-201 §6.5
DEF-110.08	Energy-pack swap and fault recovery by the maintainer. The energy pack is swapped by the same maintainer per the card, timed; a fault is induced by the manufacturer's procedure and the maintainer diagnoses it from the console or fault indicator and clears it per the card; time from video against the declared times.	all	CAM+FEED	Spare pack; maintainer card	10 min	Required by VRS-DEF-201 §6.5

7.6 6.6 Part 6 — Capture and compromise resilience

A captured or abandoned platform gives up nothing: zeroise, remote disable, tamper, and a storage module that reads as nothing.

ID	STEP	CLASSES	WITNESS	APPARATUS	BOUND	REQUIRED BY
DEF-110.09	Zeroisation and remote disable. The declared zeroisation command is issued from the console (or the declared local control); the console shows keys, mission data and maps erased and the vehicle in its declared disabled state; a declared remote-disable command is shown to stop and lock the vehicle; the events appear in the security log; the vehicle is restored by the declared re-provisioning and its data-at-rest encryption state is shown.	all	FEED	Manufacturer's console and re-provisioning means	10 min	Required by VRS-DEF-201 §6.6
DEF-110.10	Tamper response and data-at-rest protection. A declared tamper trigger (enclosure opened, storage module removed, declared tamper switch) is actuated; the console shows the tamper event, the	all	CAM+FEED+APP	Manufacturer's reader for the storage module	8 min	Required by VRS-DEF-201 §6.6

ID	STEP	CLASSES	WITNESS	APPARATUS	BOUND	REQUIRED BY
	declared response (alert, lock, zeroise) and the encrypted state of removable storage; a removed storage module read on the manufacturer's reader shows no plaintext mission data.					

7.7 6.7 Part 7 — Cyber accreditation practice

Extends the intrinsic update and authentication steps with the accreditation-regime controls: hardware token, audit trail spanning the session.

ID	STEP	CLASSES	WITNESS	APPARATUS	BOUND	REQUIRED BY
DEF-110.11	Signed update, access controls and audit under accreditation controls. A signed update is applied through the declared mechanism with verification shown and an unsigned package refused where one can be staged; operator and maintainer roles require the declared authentication (including any declared hardware token) and default credentials are refused; the security log shows the update, logins and the zeroisation events of Part 6 with timestamps.	all	FEED	Update package(s); declared authentication token	10 min	Required by VRS-DEF-201 §6.7

6.8 Timing budget. All 11 steps sum to 115 min. Per class, with every applicable step declared: ground UGV (logistics/ISR) 115 min · EOD/CBRN 115 min · base/perimeter security 115 min · maritime security

USV 105 min. Every class is within the 120 min bound of 4.6.

8 7 Worked example (informative)

A manufacturer of a hypothetical tracked logistics carrier (class: ground UGV) declares: an attested cargo-only configuration with two standard payload rails and no fire-control interface; 3 m/s maximum speed at 400 kg on gravel with a 2.5 m stopping distance; targets of 1 700 × 500 mm and 300 × 1 700 mm; a 10 m following distance and a 3 m gate standoff; positioning denial by shrouding and a lawful spoof injection through the receiver's test port inside a shielded tent, with dead-reckon-to-stop within 8 m; a link-degraded warning at the declared margin and hold on loss within 2 m; heat present at the range as a site condition; a drive-module swap in 25 min and a pack swap in 5 min with the organic kit and card; zeroisation from the console with a 3 min re-provisioning, remote disable, a lid-switch tamper trigger and encrypted removable storage; and updates through the maintainer console with a hardware token.

After VRS-GEN-203 Part E the sector steps run from 12:40 on the range. DEF-110.01: rails, mounts and connectors identified; no fire-control interface; build matches the attested non-weaponised build; attestation reference read (achieved). DEF-110.02: laden at 3 m/s, the 1 700 mm target from the side, stop at 2.2 m; prone target, stop (achieved). DEF-110.03: yields at the crossing to the towed vehicle target, holds 10–11 m behind the lead, stops 3.1 m from the gate (achieved). DEF-110.04: shrouded, flags loss, dead-reckons to a stop in 6 m; in the tent the spoof injection is flagged as inconsistent and the vehicle holds (achieved). DEF-110.05: link attenuated, warning at the margin; cut, hold within 1 m (achieved). DEF-110.06: 38 °C ambient shown on the vehicle's sensor, task performed (achieved). DEF-110.07: drive module swapped on the gravel with the organic kit and card in 21 min, logged (achieved). DEF-110.08: pack swapped in 4 min; sensor fault induced, diagnosed from the indicator and cleared per the card in 3 min (achieved). DEF-110.09: zeroise — keys, mission data and maps erased, vehicle disabled; remote disable stops and locks; re-provisioned in 3 min; encryption state shown (achieved). DEF-110.10: lid opened, tamper alert and lock; storage module removed and read on the reader — ciphertext only (achieved). DEF-110.11: signed update applied with the token, unsigned refused, default credentials refused, log shows the session's events (achieved). Sector time 105 min; VRS-GEN-203 Part F follows.

The reviewer scores VRS-DEF-201 §6.1 from DEF-110.01 with GEN-203.02 and GEN-203.05; §6.2 from DEF-110.02 and DEF-110.03 with GEN-203.09 and GEN-203.12; §6.3 from DEF-110.04 and DEF-110.05 with GEN-203.13 and GEN-203.15; §6.4 from DEF-110.06 with GEN-203.39; §6.5 from DEF-110.07 and DEF-110.08 with the intrinsic serviceability steps; §6.6 from DEF-110.09 and DEF-110.10 with GEN-203.32 and GEN-203.37; §6.7 from DEF-110.11 with GEN-203.33 and GEN-203.38; §6.8 and §6.9 from the pack. No number in this example is a requirement; every apparatus value came from the manufacturer's own declaration.

9 Annex A (normative) — Criterion coverage

Every criterion of VRS-DEF-201 Clause 6 appears once with the intrinsic steps (VRS-GEN-203) and the sector steps (this Protocol) that witness it, or the statement that it has none.

CRITERION	SUBCLAUSE	WITNESSED BY
DEF-1 Scope integrity — weapons-function exclusion verified	VRS-DEF-201 §6.1	intrinsic GEN-203.02, GEN-203.05; sector DEF-110.01
DEF-2 Own-force and bystander protection at speed and load	VRS-DEF-201 §6.2	intrinsic GEN-203.09, GEN-203.12; sector DEF-110.02, DEF-110.03
DEF-3 Contested-environment integrity	VRS-DEF-201 §6.3	intrinsic GEN-203.13, GEN-203.15; sector DEF-110.04, DEF-110.05
DEF-4 Environmental qualification	VRS-DEF-201 §6.4	intrinsic GEN-203.39; sector DEF-110.06
DEF-5 Field maintainability by uniformed maintainers	VRS-DEF-201 §6.5	intrinsic GEN-203.28, GEN-203.29, GEN-203.30; sector DEF-110.07, DEF-110.08
DEF-6 Capture and compromise resilience	VRS-DEF-201 §6.6	intrinsic GEN-203.32, GEN-203.37; sector DEF-110.09, DEF-110.10
DEF-7 Cyber accreditation and vulnerability handling	VRS-DEF-201 §6.7	intrinsic GEN-203.33, GEN-203.38; sector DEF-110.11
DEF-8 Programme continuity and export/security constraints	VRS-DEF-201 §6.8	no step — scored at the Certified tier from the Verified evidence
DEF-9 Mission incident record	VRS-DEF-201 §6.9	no step — scored at the Certified tier from the Verified evidence

10 Bibliography

- MIL-STD-810H (2019, with Change 1 2022), *Environmental Engineering Considerations and Laboratory Tests*.
- MIL-STD-461G (2015), *Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment*.
- NATO AEP-4818 (2021), *Allied Engineering Publication — Unmanned Ground Vehicle interoperability*.
- NATO STANAG 4586 Ed. 4 (2017), *Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability*.
- ISO 3691-4:2023, *Industrial trucks — Safety requirements and verification — Part 4: Driverless industrial trucks and their systems*.
- ISO 13849-1:2023, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*.
- IEC 62443-4-2:2019, *Security for industrial automation and control systems — Part 4-2: Technical security requirements for IACS components*.

- NIST FIPS 140-3 (2019), *Security Requirements for Cryptographic Modules* (zeroisation and tamper response).
- ASTM E2521-16, *Standard Terminology for Evaluating Response Robot Capabilities*.
- DNV-ST-0342 (2023), *Craft – Unmanned surface vessels*.

11

Change history

DATE	VERSION	STATUS	CHANGE	AUTHORITY
2026-09-16	1.0.0 (draft)	Draft	Created for the VRS 2026 edition (rewrite Batch D; sector demonstration protocol). 11 steps in 7 Parts extending VRS-GEN-203 for the Defence & Security criteria of VRS-DEF-201: configuration inspection confirming no weapons function (a finding ends the session – 4.8), personnel targets at speed and load, base-traffic behaviour, positioning denied and lawfully spoofed in a shielded enclosure, link degraded and cut, conditional site condition, module and pack swap by a unit-level maintainer with organic tools, zeroisation and remote disable, tamper response and encrypted storage read as nothing, signed update and token authentication with audit. Classified functions may be declined with the ground recorded (4.10). Annex A covers all 9 criteria.	Rewrite instructions §6 (VRS-XXX-110); sector traceability matrix (DEF derived demonstration steps); CEO ruling 2026-09-15 that standards carry no catalogue identifiers

About Veyrum Research Institute

Veyrum Research Institute is the research arm of Veyrum – the independent intelligence and trust layer for the robotics industry (research, ratings and registry, advisory, data, and specialist insurance & finance introductions).

Disclaimer

The opinions in this document are independent and current as of the date of publication, based on information believed reliable; they are not guarantees or warranties of safety, fitness, or compliance, and are not engineering, legal, or financial advice. This document may be revised. © 2026 Veyrum.

Contact: hello@veyrum.com · VRS-DEF-110 · Version 1.0.0