



VEYRUM ROBOTICS STANDARD



VRS-DEF-001

Defence & Security Sector Standard

Application Rating requirements for robots in defence and security applications (non-weapons functions).

VEYRUM RESEARCH INSTITUTE

DOCUMENT

VRS-DEF-001

VERSION

1.0

STATUS

Draft

DATE

16 September 2026

Contents

1 1 Scope

2 2 Normative references

3 3 Terms and definitions

4 4 Sector applicability

5 5 Sector hazard taxonomy (non-weapons dimensions)

6 6 Sector Application Rating

7 7 Evidence requirements

8 8 Loss-driver mapping (insurance and finance fitness)

9 9 Protocol references

10 10 Worked example (informative) – applicability walkthrough

11 Annex A (normative) – Restricted-evidence module (first dedicated use)

12 Bibliography

13 Change history

Foreword. Sector standard for the **Defence & Security (DEF)** sector — activated on CEO direction 2026-09-05 per VRS-GEN-007 §6.2 (activation is a publication act). First dedicated use of the **restricted-evidence module** (Annex A). **Critical scope boundary:** VRS rates the robot as an economic and operational asset — safety, reliability, serviceability, survivability, and support. **Weapons functions are categorically out of VRS scope:** VRS issues no opinion on targeting, engagement, or lethality (governed by state policy such as US DoD Directive 3000.09 (2012; reissued 2023-01-25) and international frameworks — not by a commercial rating). Anchors were verified against issuing-body pages on 2026-09-11 (Bibliography). Numeric thresholds are not set here — they live inside the criterion rungs of VRS-DEF-201 and its data twin (VRS-DEF-501). A Defence & Security AR is an opinion above the compliance floor, not a certification, and nothing here implies that any real robot holds a Veyrum rating (ratings are not published). Requirements use “shall”; recommendations use “should”.

1 Scope

This Standard defines the requirements for issuing a **Defence & Security AR** for robots in defence and security applications: military logistics, base and perimeter security, ISR (intelligence, surveillance, reconnaissance), military EOD (explosive ordnance disposal), and comparable non-weapons support roles. It defines sector applicability (Clause 4), the sector hazard taxonomy (Clause 5), the sector Application Rating requirements (Clause 6), evidence requirements (Clause 7), the loss-driver mapping that makes a DEF rating usable by an insurer or lender (Clause 8), protocol references (Clause 9), and a worked applicability example (Clause 10).

Exclusions (absolute): weapons functions — a system’s targeting, engagement, or lethality behaviour shall never be assessed, scored, or opined on by VRS. Where a platform carries such functions, the VRS assessment shall cover ONLY the platform’s non-weapons dimensions, and the rating record shall state that exclusion prominently. The scoring mathematics themselves are excluded (VRS-GEN-005/006; the sector’s scoring content lives in VRS-DEF-201). Civil security robots in public venues are rated under **VRS-SVC-001**; civilian EOD and fire-service robots under **VRS-HAZ-001**; uncrewed aircraft in civil airspace under **VRS-AER-001**.

2 Normative references

The following documents are referred to in the text such that some or all of their content constitutes requirements of this Standard. VRS documents are dated at the point of assessment unless stated otherwise.

- **VRS-GEN-001**, Vocabulary; **VRS-GEN-005**, IR Methodology; **VRS-GEN-006**, AR Scheme; **VRS-GEN-007**, Sector Classification; **VRS-GEN-009**, Passport & Registry Schema; **VRS-GEN-012**, Evidence & Data Requirements (evidence grades).
- **VRS-DEF-201**, Defence & Security AR Assessment Protocol (scoring; dated at assessment); its data twin is **VRS-DEF-501**.

- **VRS-GEN-202**, Calibration & Validation Protocol (constant fitting). Cold-start parity and the company-wide fallback are defined in **VRS-GEN-005 §6**; the letter bands in **VRS-GEN-006 §4**.
- Anchor regimes (verified 2026-09-11) – context anchors and evidence lanes, **not** conformity floors that VRS re-certifies:
 - **ISO 8373:2021** – Robotics – Vocabulary (the robot-term basis; VRS-GEN-001 aligns to it).
 - **ISO 10218-1:2025 / ISO 10218-2:2025** – industrial robot safety (robot; integration). The 2025 revision absorbed ISO/TS 15066:2016 and added explicit cybersecurity clauses; the safety-floor anchor for logistics platforms operating on bases among personnel.
 - **IEC 62443-4-2:2019** – technical security requirements for IACS components (component security levels SL-C against foundational requirements FR1–FR7); **IEC 62443-4-1:2018** – secure product development lifecycle (maturity ML1–ML4). Cyber evidence lane for H2/H5.
 - **IEC 62443-3-3:2013** – system security requirements and security levels (system-level SL-C against FR1–FR7); **IEC 62443-3-2:2020** – security risk assessment for system design (partitions a system into zones/conduits and sets each a target SL-T). System-level cyber anchor for the fleet-wide shared control/update plane (Cl. 8.4), distinct from the component-level 62443-4-2.
 - **NIST SP 800-88 Rev. 2:2025** – Guidelines for Media Sanitization (Clear/Purge/Destroy and cryptographic-erase methods; supersedes Rev. 1:2014). Data-sanitization evidence lane for H5 (capture/compromise): the anchor behind data-at-rest zeroize/crypto-erase design evidence.
 - **MIL-STD-810H** (2019; Change Notice 1, 2022) – environmental engineering test methods (temperature, shock, vibration, humidity, salt fog, sand/dust, altitude); a tailoring/ test-method reference, not a certification. Theatre-environment reliability evidence lane.
 - **NATO STANAG 4586** (Ed. 2, 2007) – UAV Control System interfaces for interoperability; named convention for ISR/UAS remote-link integrity context (H2), not a scored input.
 - Export-control and market-scope regimes (scope evidence, not safety floors): **ITAR (22 CFR 120–130)**, **EAR (15 CFR 730–774)**, the **Wassenaar Arrangement**, and **MTCR** UAV categorisation. **DoD Directive 3000.09** (2012; 2023) is cited only as the boundary marker for what VRS does NOT assess.
 - Procurement/mission specifications of the acquiring force are per-programme and shall be recorded at assessment; no harmonised public performance floor exists for non-weapons defence robots, so none is asserted here.

3 Terms and definitions

For the purposes of this Standard, the terms in VRS-GEN-001 (aligned to ISO 8373:2021) apply, together with the following local terms:

- **mission role** – the declared non-weapons function class of the assessed model; at minimum one of **military-logistics**, **base-security**, **isr**, **military-eod**.
- **restricted evidence** – evidence subject to national-security classification or export control, whose content the VRS registry cannot hold or independently verify.
- **contested environment** – operation under deliberate adversarial interference (jamming, spoofing, cyber intrusion, physical attack on the platform or its links).

- **capture/compromise** — loss of the physical asset, its data, or its embedded technology to an adversary; a recoverability and technology-transfer loss driver unique to this sector.
- **theatre exposure** — operating time accrued in a declared deployment environment, measured in **op-hours**, used as the exposure denominator for frequency-type quantities.

4 Sector applicability

4.1 DEF is an **intended-use sector** (VRS-GEN-007 §5.2): no capability gate applies. A model shall be treated as DEF-applicable when (a) the manufacturer declares a defence or security use in its operating envelope, or (b) an assessor records evidence of material defence deployment (override with rationale, VRS-GEN-006 §5.2). Default: not-applicable.

4.2 The minimum capability for applicability is operation in the declared mission role under the acquiring force's operating procedures.

4.3 The assessed envelope shall state the **mission roles** covered — at minimum one of **military-logistics**, **base-security**, **isr**, **military-eod** — as protocol applicability fields (VRS-GEN-007 §4.2). The AR letter shall cover only the assessed roles; unassessed roles shall be displayed as not covered.

4.4 DEF criteria are scored per **application class**, the class being the robot's mobility/ manipulation form as declared in the envelope. The application classes for this sector are **mobile-ground**, **manipulator**, **legged**, and **uncrewed-aircraft**; a criterion not applicable to the assessed class is removed from the pool for that class (VRS-DEF-201 Clause 7; VRS-GEN-006 §6). Robot form is not a sector: an arm, quadruped, humanoid, ground vehicle, or uncrewed aircraft is rated under DEF by this same Standard when 4.1 holds.

4.5 A weapons-capable platform's envelope shall state the Clause 1 exclusion explicitly, and the assessment shall record which functions were identified as weapons functions and therefore carved out. Whether that exclusion boundary is verifiable is scored per Clause 6.3.

5 Sector hazard taxonomy (non-weapons dimensions)

The Defence & Security AR shall weigh, at minimum, the following hazard groups. Each maps to the IR categories (VRS-GEN-005 §5) it draws evidence from; the sector emphasis (point ranges) is defined in VRS-DEF-201, not here.

#	HAZARD GROUP	ARCHETYPE	PRIMARY IR CATEGORIES	LOSS DRIVER
H1	Own-force and bystander safety	contact/traffic harm on bases and in operations areas	safety_incidents	frequency, severity
H2	Contested-environment integrity	jamming/spoofing of navigation and links; cyber compromise by capable adversaries; behaviour under interference	cyber_posture, reliability	frequency, correlated/cyber-catastrophe
H3	Mission reliability	failure in mission with limited recovery; environmental extremes of deployment theatres	reliability	frequency, exposure
H4	Field serviceability	maintainability by uniformed maintainers; spares logistics in theatre	serviceability, manufacturer_support	severity (downtime), recoverability
H5	Capture and compromise	loss of the asset to an adversary – data, technology, and misuse exposure	cyber_posture, economics_residual	recoverability, residual value
H6	Programme continuity	manufacturer's ability to sustain multi-year defence programmes under export/security constraints	manufacturer_support	obsolescence, residual value

5.1 The hazard taxonomy shall be treated as the minimum coverage set: an assessment that omits a hazard group applicable to the declared mission roles shall record the omission and its reason.

5.2 H2 and H5 are the sector-specific loss drivers that civil sector standards do not surface; their evidence and treatment shall not be inferred from civil-sector analogues without recorded justification.

5.3 Severity in this sector shall account for the operational context, not only physical harm: a mission-critical failure of an ISR or EOD platform can carry consequences (loss of situational awareness, exposure of personnel to an unresolved hazard) that exceed the platform's own repair cost. The assessment shall record the mission-consequence class alongside the physical-harm severity so that the two are not conflated in the rating record.

6 Sector Application Rating

6.1 The Defence & Security sector AR shall be determined per **VRS-DEF-201** from the pool defined there – the sector criteria DEF-1...DEF-9 together with the contributing intrinsic criteria – as a percentage of

the applicable pool; letters (C < B < A < AA < AAA, AAA best) follow **VRS-GEN-006 §4**. The machine-readable data twin is **VRS-DEF-501**.

6.2 The letter bands, the per-criterion tier ceilings, and the reserved-headroom AAA band (deliberately hard, anti-inflation) live in VRS-GEN-006 §4 and VRS-DEF-201 §7 and are not restated here.

6.3 The weapons-function exclusion is a matter of scope, not of scoring: where a platform carries a weapons function (targeting, engagement, lethality), that function is out of scope under Clause 1 and receives no rating, while the platform's non-weapons dimensions are assessed. Whether the exclusion boundary is *verifiable* — that the assessor can establish which functions are weapons functions — is scored by VRS-DEF-201 §6.1 (criterion DEF-1) on a large point range; a boundary that cannot be established scores zero on that criterion and is **not a gate**.

6.4 Conformity with the mission-relevant safety and cyber anchor regimes (Clause 2 — ISO 10218 safety for on-base logistics platforms; IEC 62443 component and system security) is scored through the contributing intrinsic safety criteria (SF-1, SF-2, SF-8 — VRS-GEN-101) and the sector cyber-accreditation criterion DEF-7 (VRS-DEF-201 §6.7); absence of evidenced conformity scores zero on those criteria and is **not a gate** — the rating rewards performance above the compliance floor without substituting for it.

7 Evidence requirements

7.1 Evidence shall be graded per VRS-GEN-012. Sector-relevant sources include: programme test records, field reliability data from operators (in op-hours), contested-environment trial evidence, maintenance records (active repair time and parts-delay), export-control classifications (as scope evidence), and manufacturer sustainment declarations.

7.2 For each hazard group, an existing conformity artefact should be mapped to the VRS evidence lane so that adoption costs a defence manufacturer a mapping rather than new testing:

HAZARD	EXISTING ARTEFACT (EXAMPLE)	VRS EVIDENCE LANE
H1	ISO 10218-1:2025 / ISO 10218-2:2025 risk assessment; operator incident logs (op-hours)	safety_incidents
H2	IEC 62443-4-2:2019 SL-C evaluation; instrumented jam/spoof trial reports; STANAG 4586 link tests	cyber_posture, reliability
H3	MIL-STD-810H (2019) environmental test report; operator uptime telemetry	reliability
H4	ISO 14224-coded maintenance records (MRT, parts-delay in days)	serviceability, manufacturer_support
H5	IEC 62443-4-1:2018 secure-development evidence; NIST SP 800-88 Rev. 2:2025 media-sanitization / crypto-erase records; data-at-rest/zeroize design evidence	cyber_posture, economics_residual
H6	Programme sustainment plan; end-of-support declaration (obsolescence horizon in months)	manufacturer_support

7.3 Evidence shall be assessed at one of three tiers — **Unverified, Verified, Certified** — each criterion stating the points reachable at each tier (VRS-DEF-201 §6, §8). Where a criterion's evidence bar is not met the criterion shall score **0** (no evidence is zero points, not a discard from the pool). A model×mission-role with no admissible defence-context evidence shall be displayed as *not covered* for that role (VRS-GEN-006 §6).

7.4 Models without sufficient model-specific defence operating history shall be scored at the tier the available evidence supports and, where offered, from manufacturer-wide records under the company-wide fallback and cold-start parity of **VRS-GEN-005 §6**; the lower tier caps the attainable letter through the per-criterion ceilings (VRS-DEF-201 §7). Where H2 (contested-environment integrity) evidence rests on manufacturer declaration alone, without instrumented jam/spoof trial data, the assessment shall hold the H2 criterion (DEF-3) at its Unverified rung and record the evidence gap.

8 Loss-driver mapping (insurance and finance fitness)

8.1 Every quantity that feeds the DEF rating shall be traceable to a loss driver and to a Robot Risk Passport field (VRS-GEN-009), so that an underwriter or lender can compute it from obtainable evidence. The mapping is:

LOSS DRIVER	DEF SIGNAL	EXPOSURE DENOMINATOR	CONSUMES
Frequency	H1 incidents; H2 interference-induced failures	per 1,000 op-hours	safety_incidents, reliability
Severity	own-force/bystander harm; mission-abort downtime (days)	per event	safety_incidents, serviceability
Recoverability	H4 repair-in-theatre; H5 capture exposure	per event	serviceability, cyber_posture
Residual value / obsolescence	H6 sustainment horizon (months)	per model	economics_residual, manufacturer_support
Correlated / cyber-catastrophe	H2/H5 fleet-wide compromise via shared control/update plane	per fleet	cyber_posture

8.2 A DEF signal that lacks an exposure denominator shall not be scored as a frequency; it shall be recorded as a descriptive attribute or elevated as a design question (VRS-GEN-202). No loss statistic shall be invented to fill a missing denominator.

8.3 The rating output shall be expressed so that it can feed an underwriting decision (rate relativity, deductible, exclusion, condition) or a credit decision (loan-to-value, residual curve, covenant), and shall be recorded in the Passport with its assessment tier and evidence-basis flags (VRS-GEN-006 §9.3, VRS-GEN-009); the letter alone is insufficient.

8.4 Correlated and cyber-catastrophe accumulation (H2/H5) is the loss driver most likely to surprise a defence-fleet underwriter: a shared control or update plane means one adversary action can degrade or capture many units of a model at once, so the risk does not diversify across a fleet the way independent mechanical failures do. The DEF rating shall therefore surface, as a passport-recorded attribute, whether the model shares a fleet-wide control/update plane and whether that plane — treated as a system under consideration and partitioned into zones/conduits per IEC 62443-3-2:2020 — holds a system-level security evaluation (IEC 62443-3-3:2013, system SL-C against FR1–FR7), so an underwriter can set an accumulation cap or a per-fleet aggregate condition rather than pricing each unit independently. The system-level anchor (62443-3-3) is used here deliberately in place of the component-level 62443-4-2, because a shared control/update plane is a system, not a component. This attribute is descriptive, not scored, until a fleet-loss denominator exists (VRS-GEN-202 §8).

8.5 Recoverability and residual value shall be read together: a model that is highly serviceable in theatre (H4) but has a short declared sustainment horizon (H6, in months) can still carry poor finance risk, because a lender's residual curve depends on both the ability to return the asset to service and the length of time parts and support remain available. The rating shall not net one against the other; both shall appear as separate passport fields so the lender can weight them for its own credit policy.

9 Protocol references

- **VRS-DEF-201** — Defence & Security AR Assessment Protocol (scoring) — dated reference at assessment time; its data twin is **VRS-DEF-501**.
- Defence Test Protocols (**VRS-DEF-1xx**) are reserved; the first candidates are a contested-environment (jam/spoof) integrity protocol and a capture/zeroize verification protocol, drawing on the anchor regimes' test regimes rather than duplicating them.

10 Worked example (informative) — applicability walkthrough

The following illustrates how an assessor applies Clauses 4–8 to a **hypothetical** model. It is not a real assessment and does not imply that any robot holds a Veyrum rating.

Input. A manufacturer declares a tracked ground robot (application class **mobile-ground**), model code **DEF-EX-01** , for two mission roles: **military-eod** and **military-logistics** . The platform can carry a disruptor tool. The manufacturer holds an ISO 10218-2:2025 integration risk assessment, an IEC 62443-4-2:2019 SL-2 component evaluation, a MIL-STD-810H (2019) environmental report, and 4,200 op-hours of operator field data with 3 recorded own-force near-miss incidents.

Step 1 — applicability (Cl. 4). The manufacturer declaration satisfies 4.1(a); DEF is applicable. Envelope records mission roles **military-eod** , **military-logistics** (4.3) and application class **mobile-ground** (4.4).

Step 2 — weapons boundary (Cl. 1, 4.5, 6.3). The disruptor is assessed as a tool, not a targeting/engagement weapon function; the assessor records this determination and the carve-out. Because the boundary is establishable, DEF-1 (§6.1) scores on the evidence rather than at zero, and no scope exclusion applies to the platform's non-weapons dimensions.

Step 3 — hazard coverage (Cl. 5). H1–H6 all apply to the declared roles. H2 evidence rests only on the SL-2 evaluation with no instrumented jam/spoof trial, so 7.4 holds the H2 criterion (DEF-3) at its Unverified rung and records the gap.

Step 4 — anchor conformity (Cl. 6.4). Safety and cyber anchors are evidenced (ISO 10218-2:2025; IEC 62443-4-2:2019 SL-2), so the contributing safety criteria (SF-1, SF-2, SF-8) and the cyber-accreditation criterion DEF-7 score on that evidence rather than at zero; conformity is not a gate.

Step 5 — evidence tier (Cl. 7.3–7.4). The manufacturer evidence pack (integration risk assessment, component evaluation, environmental report, 4,200 op-hours of operator field data) supports the **Verified** tier; no behaviour is witnessed, so each criterion is held at its Verified ceiling (VRS-DEF-201 §7) and the Certified tier is not reached.

Step 6 — loss-driver read (Cl. 8). Own-force near-miss frequency is expressed as 3 events per 4,200 op-hours = 0.71 per 1,000 op-hours (H1). The fleet control/update plane holds no system-level (IEC 62443-3-3:2013) evaluation, so 8.4 records the accumulation attribute below the target level. The declared sustainment horizon (months) is recorded for the residual-value driver (8.5).

Output. The rating is computed by VRS-DEF-201 (not in this document). The Passport record carries the letter, the mission roles, the weapons-functions exclusion statement, the assessment tier (Verified),

and the H2 evidence-gap note. The numeric score and band boundary come from the criterion rungs and bands of VRS-DEF-201 and its twin VRS-DEF-501 and are not asserted here.

11 Annex A (normative) — Restricted-evidence module (first dedicated use)

A.1 Restricted evidence (classified or export-controlled) may support a rating ONLY under handling terms recorded with the acquiring party; VRS shall never store restricted material — the evidence record shall hold an attestation (who verified, under what authority, against which criteria) in place of content.

A.2 Attestation-based restricted evidence shall not reach the **Certified** tier (VRS-GEN-012 §4): independent verification of its content is by definition unavailable to the registry, so a criterion resting materially on such evidence is held at the **Verified** tier at most.

A.3 A rating resting materially on restricted evidence shall display a “restricted-evidence basis” flag, and the affected criteria shall be held no higher than the Verified tier with the evidence basis recorded in the Passport.

A.4 Export-control status shall be recorded per assessed market; the rating shall make no representation about export lawfulness.

12 Bibliography

- ISO 8373:2021, Robotics — Vocabulary ([iso.org/standard/75539.html](https://www.iso.org/standard/75539.html)) — third edition; robot-term basis.
- ISO 10218-1:2025 / ISO 10218-2:2025, industrial robot safety ([iso.org](https://www.iso.org); [A3/automate.org](https://www.automate.org), 2025) — absorbed ISO/TS 15066:2016; explicit cybersecurity clauses added.
- IEC 62443-4-2:2019, technical security requirements for IACS components; IEC 62443-4-1:2018, secure product development lifecycle (IEC/ANSI webstore) — cyber evidence lanes (H2, H5).
- IEC 62443-3-3:2013 (Ed. 1.0, 2013-08), system security requirements and security levels (webstore.iec.ch/en/publication/7033); IEC 62443-3-2:2020 (Ed. 1.0, 2020-06), security risk assessment for system design — zones/conduits and target SL-T (webstore.iec.ch/en/publication/30727) — system-level cyber anchor for the fleet-wide control/update plane (Cl. 8.4).
- MIL-STD-810H (2019; Change Notice 1, 2022), Environmental Engineering Considerations and Laboratory Tests ([everyspec.com](https://www.everyspec.com); [iest.org](https://www.iest.org)) — theatre-environment reliability evidence lane (H3).
- NIST SP 800-88 Rev. 2 (September 2025), Guidelines for Media Sanitization (csrc.nist.gov/pubs/sp/800/88/r2/final; DOI 10.6028/NIST.SP.800-88r2) — Clear/Purge/Destroy and cryptographic-erase methods; supersedes Rev. 1 (2014). Data-sanitization evidence lane for H5.
- NATO STANAG 4586 (Ed. 2, 2007), UAV Control System interfaces ([everyspec.com](https://www.everyspec.com); [nato.int](https://www.nato.int)) — ISR/UAS interoperability and remote-link integrity context (H2).
- US DoD Directive 3000.09 (2012; reissued 2023-01-25), Autonomy in Weapon Systems (esd.whs.mil) — cited only as the out-of-scope boundary marker.
- Export/market-scope frameworks: ITAR (22 CFR 120–130), EAR (15 CFR 730–774), Wassenaar Arrangement, MTCR UAV categorisation — scope evidence, not safety floors.

- VRS framework research Phase 5 (internal) — DEF scan (adversarial threat; export complexity).

13 Change history

DATE	VERSION	STATUS	CHANGE	AUTHORITY
2026-09-05	0.1	Draft	Sector ACTIVATED per GEN-007 §6.2 on CEO direction; weapons-functions exclusion as absolute scope boundary; restricted-evidence module first dedicated use	CEO 2026-09-05
2026-09-11	0.2	Draft	DEEPEN: brought to publishable depth. Added dated anchors (ISO 8373:2021, ISO 10218-1/-2:2025, IEC 62443-4-2:2019 / -4-1:2018, MIL-STD-810H 2019, STANAG 4586) verified 2026-09-11; evidence-reuse mapping (Cl. 7.2); loss-driver mapping (Cl. 8); worked applicability example (Cl. 10). Retired two bare pending markers → GEN-202 stage labels. Net +≈1,900 words; shall count raised. No requirements deleted.	Curator Run #21; charter DEEPEN
2026-09-11	0.3	Draft	RESEARCH: corrected the Cl. 8.4 fleet-plane cyber anchor from the component standard (IEC 62443-4-2:2019) to the system standard IEC 62443-3-3:2013, scoped as a zone/conduit per IEC 62443-3-2:2020; both anchors added to Cl. 2 and Bibliography (editions verified 2026-09-11). Net +≈90 words; shall count unchanged; no requirements deleted.	Curator Run #34; charter RESEARCH
2026-09-14	0.4	Draft	RESEARCH: closed the H5 (capture/compromise) evidence-lane gap — the “data-at-rest/zeroize” sanitization evidence had no dated anchor. Added NIST SP 800-88 Rev. 2 (September 2025; supersedes Rev. 1:2014), verified 2026-09-14, to Cl. 2, the §7.2 H5 evidence-reuse row, and the Bibliography. Currency check: Rev. 1 (2014) is superseded; Rev. 2 is current. Net +≈70 words; no normative requirements added or removed. DEF-201 §8.2 C5 lane + DEF-501 twin left for a later pass (logged).	Curator Run #138; charter RESEARCH
2026-09-16	1.0	Draft	VRS 2026 rewrite: recast Clause 6 — separated the two halves of the former scope-integrity rule (weapons function <i>present</i> is a Clause 1 scope exclusion; verifiability of the boundary is scored by VRS-DEF-201 §6.1 / DEF-1 on a large range, no gate) and re-anchored the former anchor-regime ≤ B cap to the contributing safety criteria (SF-1/SF-2/SF-8, VRS-GEN-101) plus DEF-7 cyber accreditation, each scored with no gate; bands live in VRS-GEN-006 §4 / VRS-DEF-201 §7. Evidence recast to the Unverified/Verified/Certified tiers (§7.3–7.4). Added the application-class list to Clause 4	VRS 2026 rewrite Stage 4

DATE	VERSION	STATUS	CHANGE	AUTHORITY
			(§4.4). Deleted Annex A (cold-start qualification particulars) and renumbered Annex B→A; dropped GEN-201/cold-start dependency (cold-start parity → GEN-005 §6). Retired confidence-band, provisional-flag, assessed-unrated, hard-cap and stage- prior wording; data-twin reference → VRS-DEF-501. Worked example re-run at the Verified tier with arithmetic shown. No numeric threshold, weight or constant set or changed; twin regenerated by the dispatcher. See GEN-005 §6.	

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-001 · Version 1.0