

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: 29 November 2026

L. Melegassi  
Catellix  
28 May 2026

The MVPS Adversarial-Audit Methodology: A Reproducible  
Discipline for Measurement-Security Internet-Drafts  
draft-melegassi-irtf-mvps-methodology-00

## Abstract

The Multi-Vantage Path Snapshot (MVPS) family of Internet-Drafts is built on a single discipline rather than a single algorithm. This document records that discipline as a set of nine machine-checkable meta-invariants (M-1..M-9): every claim is classified as a Theorem, a Design, or a Conjecture; every Theorem traces to a closed basis of twelve imported results (I1..I12); every Conjecture carries a four-field falsification protocol; every draft ships a proof/validator/receipt trio; and an adversarial-audit ledger of eight rounds and forty-four findings is kept, each finding either defended or reclassified.

The contribution is offered to the research community as a template that other measurement-security efforts MAY adopt, independent of MVPS's specific mathematics. This document defines no protocol, introduces no wire format, and requests no IANA action. Its claims are themselves validated: `scripts/validate_methodology_discipline.py` returns exit 0 over the eleven discipline checks and writes `evidence/methodology_discipline_receipt.json`.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 29 November 2026.

## Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this

document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
1.1. Why a Methodology Draft . . . . .	3
1.2. Scope and Non-Goals . . . . .	3
2. Terminology . . . . .	4
3. The Three-Class Claim Taxonomy . . . . .	4
4. The Closed Import Basis (I1..I12) . . . . .	5
5. The Nine Meta-Invariants (M-1..M-9) . . . . .	6
6. The Adversarial-Audit Ledger . . . . .	7
7. The Proof/Validator/Receipt Trio . . . . .	8
8. Numerical Receipt . . . . .	9
9. Applicability Beyond MVPS . . . . .	9
10. Security Considerations . . . . .	10
11. IANA Considerations . . . . .	10
12. References . . . . .	10
12.1. Normative References . . . . .	10
12.2. Informative References . . . . .	11
Appendix A. Invariant-to-Check Map (Normative) . . . . .	11
Author's Address . . . . .	12

## 1. Introduction

The MVPS family comprises many Internet-Drafts that share neither a single detector nor a single deployment profile. What they share is a discipline: a fixed set of rules for what may be claimed, on what basis, and with what evidence. This document records that discipline so that it can be reviewed, reused, and -- like every MVPS claim -- falsified.

The discipline was not designed in advance. It emerged from eight rounds of adversarial audit (labelled K, G, H, W, S, B, L, N) that found forty-four defects across versions 1.0 through 3.0 and the first new-draft candidates. Version 4.0 defends or reclassifies all forty-four. The rules below are the engineering invariants that survived that process.

### 1.1. Why a Methodology Draft

Measurement-security work fails review for predictable reasons: unstated scope, conjecture presented as theorem, thresholds asserted without calibration, and results that cannot be reproduced. Each of the nine meta-invariants in Section 5 targets one such failure mode and replaces it with a check that returns a deterministic verdict.

This is a research contribution in the IRTF sense: not a protocol, but a reproducible method. It is documented here so reviewers of any single MVPS draft can see the frame the draft was built in, and so other efforts can adopt the same frame.

### 1.2. Scope and Non-Goals

This document:

- o records the claim taxonomy, the import basis, the meta-invariants, and the audit ledger;
- o ships a validator that checks the eleven discipline conditions and emits a numerical receipt.

This document does NOT:

- o prove any MVPS detection theorem (those live in their own proof companions);
- o assert optimality of any MVPS construction (MVPS is positioned at maturity step 3 of 5; see Section 5, M-9);
- o define any wire format, code point, or protocol behavior.

## 2. Terminology

Claim: any assertion uttered in the name of MVPS.

Claim class: exactly one of Theorem [T], Design [D], or Conjecture [C].

Imported theorem: one of the twelve external results I1..I12 on which MVPS is permitted to stand (Section 4).

Trace: a finite chain of substitutions from a Theorem to one or more imported theorems.

Falsification protocol: the four-tuple (observable, data source, statistical test plus significance level, current blocker) attached to every Conjecture.

Trio: the (proof companion, validator, numerical receipt) triple that backs a submittable draft.

The key words "MUST", "MUST NOT", "SHOULD", and "MAY" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals.

## 3. The Three-Class Claim Taxonomy

Every claim MUST belong to exactly one class:

[T] Theorem. Proved from the imported results I1..I12 plus the MVPS axioms. A Theorem MUST name its trace (Section 4).

[D] Design. An explicit architectural choice. A Design is not falsifiable but MUST be stated, not assumed.

[C] Conjecture. An empirical claim that MUST be accompanied by the four-field falsification protocol.

A label outside these three (for example, unqualified marketing language such as "unbreakable" or "detects all zero-days") MUST be rejected. The cardinal error of the framework is inflation: stating a Conjecture as a Theorem. Invariant M-4 is the negative control against that error.

## 4. The Closed Import Basis (I1..I12)

MVPS stands on a closed set of twelve published results. No Theorem may depend on anything outside this basis:

I1	Lin 1991	-- Jensen-Shannon divergence bounds
I2	Mardia-Kent-Bibby	-- $D^2 \sim \chi^2$ (Gaussian, known Sigma)
I3	Anderson / Hotelling	-- $T^2$ distribution
I4	Glivenko-Cantelli	-- empirical CDF convergence
I5	Wald 1947	-- SPRT optimality

I6	Dempster 1958	-- Mahalanobis geometry
I7	Cramer-Rao	-- estimation lower bounds
I8	McShane-Whitney	-- distribution-free bounds
I9	Bernstein	-- sub-exponential concentration
I10	Liggett	-- coupling / monotone systems
I11	Wilson 1927	-- binomial confidence intervals
I12	Minsker / Cohen	-- geometric-median max-bias

A claim that cannot reduce, by a finite chain, to one or more of I1..I12 is not a theorem; it is an opinion.

## 5. The Nine Meta-Invariants (M-1..M-9)

- M-1 EXHAUSTIVE CLASSIFICATION. Every claim maps to exactly one of {Theorem, Design, Conjecture}; any other label is rejected.
- M-2 IMPORT COMPLETENESS. The import registry is exactly I1..I12, each named to a published result.
- M-3 THEOREM TRACEABILITY. Every Theorem names a trace into I1..I12.
- M-4 NO INFLATION. A claim with no valid trace MUST NOT be admitted as a Theorem.
- M-5 LEDGER COMPLETENESS. The audit ledger covers eight rounds and forty-four findings (35 + 3 + 6), each defended or reclassified.
- M-6 FALSIFIABILITY. Every Conjecture carries the four-field falsification protocol.
- M-7 TRIO PRESENCE. Every draft declaring a validator has that validator on disk; the receipt corpus is commensurate with the validator corpus.
- M-8 COMPANION PRESENCE. The methodology's companion documents are present (the Ten Commandments, the methodology proof, the v4.0 catalogue, the foundations registry).
- M-9 HONEST MATURITY. The ladder Exist -> Prove -> Calibrate -> Harden -> Optimize is declared; MVPS is positioned at step 3 (Calibrate). Optimality language MUST NOT be used until a step-5 dominance proof exists.

Each invariant maps to one or more validator checks; the map is normative and appears in Appendix A.

## 6. The Adversarial-Audit Ledger

The ledger records every audit finding and its disposition. A finding is "defended" when v4.0 implements the corrected mathematics, or "reclassified" when the claim is demoted from Theorem to Design or Conjecture.

Rounds	Series	Findings	Disposition
K,G,H,W,S,B	v1.0-v3.0 (six rounds)	35	all defended
L	cross-draft reconcile	3	L_DL; L_LT; demote R-NVD
N	two new-draft rounds	6	L_ORB.*; L_ZD.*

TOTAL		44	44/44 pass	
+-----+	+-----+	+-----+	+-----+	+-----+

The master validator scripts/validate\_v4\_against\_all\_attacks.py records, per finding, the original attack and the v4.0 mechanism that defends it, and returns 44/44.

### 7. The Proof/Validator/Receipt Trio

A draft is submittable only when it ships a trio:

- o a proof companion (the closed-form mathematics, with each claim classified per Section 3);
- o a validator (a script that checks the proof's numerical and structural claims and returns exit 0);
- o a numerical receipt (a JSON artifact emitted by the validator, carrying platform metadata and a self-hash for reproducibility).

Invariant M-7 checks that every draft declaring a validator has that validator present, and that the receipt corpus is commensurate with the validator corpus. The trio is what makes a claim reproducible by a third party with no access to the authors.

### 8. Numerical Receipt

The methodology is subjected to its own discipline. The validator scripts/validate\_methodology\_discipline.py evaluates eleven checks covering M-1..M-9 and writes evidence/methodology\_discipline\_receipt.json. At time of writing all eleven checks PASS:

M-CLASS-1, M-TRACE-1, M-TRACE-2, M-NOINFLATE-1, M-AUDIT-1,  
M-AUDIT-2, M-FALSIFY-1, M-TRIO-1, M-TRIO-2, M-DOC-1, M-PROGRESS-1.

The receipt records the claim classes, the I1..I12 registry, the eight audit-round labels, the forty-four finding total, the maturity ladder, the count of draft validators discovered, and a SHA-256 of its own canonicalized body for tamper-evidence. The receipt is in turn bound by the MVPS Proof Envelope [I-D.melegassi-ippm-mvps-proof-envelope].

### 9. Applicability Beyond MVPS

The discipline is independent of MVPS's detector. Any measurement-security effort MAY adopt:

- o a fixed claim taxonomy with a machine-checked partition,
- o a closed, named import basis with mandatory traceability,
- o an adversarial-audit ledger with defend-or-reclassify dispositions,
- o a falsification-protocol requirement for every empirical claim,
- o a proof/validator/receipt trio regenerable in continuous integration.

These five elements are the transferable contribution.

## 10. Security Considerations

This document defines no protocol and therefore introduces no new attack surface. Its security relevance is indirect but real: the discipline is what prevents a measurement-security framework from making unfalsifiable detection claims that operators might rely on. The "no inflation" invariant (M-4) and the falsification requirement (M-6) are the load-bearing controls; without them a framework can silently overstate what it detects.

The numerical receipt carries a SHA-256 of its canonicalized body and is bound by the MVPS Proof Envelope [I-D.melegassi-ippm-mvps-proof-envelope], so a reader can detect post-hoc tampering with the recorded verdicts.

## 11. IANA Considerations

This document has no IANA actions.

## 12. References

### 12.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017.

### 12.2. Informative References

- [I-D.melegassi-ippm-mvps-proof-envelope] Melegassi, L., "MVPS Proof Envelope: Tamper-Evident Binding of Proofs, Validators, and Receipts", draft-melegassi-ippm-mvps-proof-envelope-00, May 2026.
- [I-D.melegassi-ippm-mvps-latency-reconciliation] Melegassi, L., "MVPS Detection-Latency Reconciliation", draft-melegassi-ippm-mvps-latency-reconciliation-00, May 2026.
- [MVPS-V4] Melegassi, L., "MVPS Mathematical Existence Proof v4.0", May 2026.
- [TEN-CMDS] Melegassi, L., "The Ten Commandments of MVPS", May 2026.

## Appendix A. Invariant-to-Check Map (Normative)

The validator scripts/validate\_methodology\_discipline.py implements the following map. A draft conforms to this methodology iff all listed checks return PASS.

M-1	EXHAUSTIVE CLASSIFICATION	-> M-CLASS-1
M-2	IMPORT COMPLETENESS	-> M-TRACE-1
M-3	THEOREM TRACEABILITY	-> M-TRACE-2
M-4	NO INFLATION	-> M-NOINFLATE-1
M-5	LEDGER COMPLETENESS	-> M-AUDIT-1, M-AUDIT-2
M-6	FALSIFIABILITY	-> M-FALSIFY-1
M-7	TRIO PRESENCE	-> M-TRIO-1, M-TRIO-2
M-8	COMPANION PRESENCE	-> M-DOC-1
M-9	HONEST MATURITY	-> M-PROGRESS-1

Eleven checks, nine invariants. The receipt records the verdict of each check and a self-hash of its canonicalized body.

Author's Address

Leonardo Melegassi  
Catellix  
Brazil  
Email: [melegassi@catellix.com](mailto:melegassi@catellix.com)