MIPractice – Attack Surface/Hardening Precision Addon Specification

Epistemic attack-surface analysis for MIPractice case outputs

Version: 1.0 · Status: Optional addon (default off)
Spec basis: `MIPractice_addon_AH_precision.yaml`
Relation: Secondary overlay for `MIPractice_case_v2.0`
Author: T. Zöller · Language: EN · Governance-aligned

---

1. Purpose and scope

The **AH Precision Addon** (Attack Surface/Hardening) is an *optional epistemic overlay* for MIPractice case analyses. Its sole purpose is to evaluate the **analysis itself** for precision risks, overreach, ambiguity and misuse potential.

- It does **not** analyse persons.
- It does **not** analyse enactments.
- It does **not** modify A-, M-, IA- or D-results.
- It analyses the **language, scope and inference structure** of an existing analysis.

> **Core idea**
> The AH addon treats an analysis as an artefact with its own *attack surface*. It makes visible where an otherwise valid MIPractice analysis may become vulnerable to misinterpretation, moral drift, reification or instrumental misuse.

2. Conceptual position within MIPractice

The AH Precision Addon is **not a model extension**. It is a **meta-analytic discipline layer**.

MIPractice core model
- Reads enactments, roles and structures
- Produces A–C–R–P–D profiles
- Evaluates asymmetry via IA-box
- Documents trajectories and practice conclusions

AH Precision addon
- Reads wording, scope and inference
- Flags epistemic risk points
- Suggests hardening actions
- Protects reversibility and dignity of interpretation

A MIPractice analysis remains **fully valid** without the addon. The addon only adds *precision transparency*.

3. Activation and integration

3.1 Default state

The AH Precision Addon is **default off**. It may only be used *after* a complete MIPractice analysis exists.

3.2 Integration points

- `case.addons.ah_precision`

- `uniform_report.addons.ah_precision`

Integration rules:

- additive only (no overwrite)
- no mutation of scores or IA labels
- removable without loss of analytical validity

4. Core concepts

4.1 Attack surface

The **attack surface** of an analysis is the set of points where its interpretation may be distorted, misused or overextended.

4.2 Attack point (AP)

An **attack point** marks a concrete risk location in the analysis, such as:

- scope drift (overgeneralisation)
- moral loading (normative phrasing)
- trigger ambiguity
- evidence gaps
- reification risk

4.3 Hardening action

A **hardening action** is a suggested modification that increases epistemic robustness without changing the substantive finding.

5. Output contract

When the addon is active, the following outputs are required:

Field	Description
precision_score	Approximate epistemic robustness (band or qualitative)
attack_points[]	Structured list of identified attack points
hardening_actions[]	Linked mitigation or clarification suggestions
confidence_and_risk_shifts	Observed stability shifts in C / IA / D-risk
addon_note	Mandatory disclaimer clarifying addon scope

6. Guardrails for the AH addon

- AH findings are never judgments of persons or actions.
- AH may not be used standalone.
- AH may not reinterpret A/M/IA scores.
- AH must preserve reversibility of all readings.
- AH may not be used for ranking, sanctioning or shaming.

> **Meta-guardrail**
> If the AH addon itself becomes a source of authority, moralisation or closure, its use constitutes an epistemic violation within MIPractice logic.

7. Relationship to dignity

The AH Precision Addon does not assess dignity. Its function is **preventive**:

- to reduce dignity-risk by avoiding overreach,
- to keep interpretations contextual and reversible,
- to prevent analytic language from turning into implicit verdicts.

In this sense, AH acts as an epistemic analogue to D_0-guardrails — protecting persons by disciplining analysis.

8. Intended use and misuse

Intended use:

- research transparency
- AI governance and auditing
- high-stakes organisational analysis
- publication-ready MIPractice cases

Not intended for:

- case evaluation without core analysis
- grading or scoring persons
- weaponised critique of analysts
- automated decision enforcement

9. Closing note

The AH Precision Addon formalises a simple principle:

> The more powerful an analysis becomes, the more disciplined its language must be.

Used correctly, the addon does not weaken MIPractice analyses — it makes them safer, clearer and more defensible.