

Dual-Use and Security Evidence in Additive Manufacturing Applied to Photopolymer Processes: Scope Boundaries, Controls, and Evidence Gaps

Lifecycle assurance and responsible innovation

Juan Seguro

3Dresyns by Resyner Technologies S.L.

© 2026 Juan Seguro. All Rights Reserved.

Correspondence: info@3Dresyns.com · www.3Dresyns.com

ER-490 · Engineering Review · Version 0.1 · 12 October 2026

Abstract

The evidence available to this review is additive-manufacturing-general, not photopolymer-specific. One source is an AM security taxonomy and survey, and the other is a 2026 analysis of additive manufacturing of conventional military equipment and its implications for arms control and security [1,2]. Photopolymer processing is therefore a scope boundary for this review, not a claim that the controlled evidence has demonstrated photopolymer-specific threats, capabilities or controls. The article identifies governance questions that a photopolymer implementation would have to answer while deliberately excluding operational attack detail, diversion routes and control-circumvention procedures. Responsible disclosure is not established by the controlled evidence and remains an unevidenced requirement if later incorporated. A benign configuration-discrepancy exercise and a recovery assessment make defensive controls testable without introducing attack instructions.

Keywords: dual-use risk · additive manufacturing · photopolymer processes · security · access controls · evidence gaps · responsible disclosure

1. Scope and ownership

ER-490 uses AM-general security and dual-use evidence to define questions that may become relevant when advanced photopolymer processes are deployed. It does not report a photopolymer-specific threat assessment and does not claim that the evidence has already been applied or validated for photopolymer processes.

2. Evidence base

Source [1] is a survey and taxonomy of security in additive manufacturing and is used here at publisher-abstract depth [1]. Source [2] addresses additive manufacturing of conventional military equipment, arms control and security and is used here at full-text depth [2]. Both are AM-general. Neither is presented as direct evidence of a photopolymer-specific capability, access pathway, threat or control effectiveness.

3. Scope boundary for photopolymer processes

Photopolymer manufacturing can involve digital design files, networked equipment, process settings and distributed production records, but the existence of those features does not by itself establish a specific security risk. This article therefore uses photopolymer processing only to define the implementation boundary within which AM-general security questions would need to be tested.

4. Capability and access questions

A defensible assessment should identify what manufacturing capability is being considered, who is authorised to access it, what digital and physical assets are in scope, and what evidence would demonstrate misuse or control failure. The controlled sources motivate these question classes at AM level [1,2]; they do not answer them for photopolymer systems.

5. Controls

Security controls should be evaluated against a defined asset and failure condition. Examples of control categories can include access governance, provenance, configuration control and release authority, but this review does not prescribe a particular security architecture and does not claim effectiveness for any photopolymer implementation.

6. Dual-use boundary

Dual-use analysis asks whether a legitimate manufacturing capability could also support an unintended or controlled use. Source [2] provides AM-level security and arms-control context [2]. ER-490 does not translate that context into a statement that a specific photopolymer process or material has military utility.

7. Evidence gaps

The controlled source set does not establish photopolymer-specific capability, access, threat or control findings. It also does not establish a responsible-disclosure procedure for photopolymer manufacturing. Those remain evidence gaps rather than missing details to be supplied by analogy.

8. No operational attack or circumvention detail

This article intentionally excludes instructions for attacking AM systems, diverting controlled output, bypassing access controls, defeating monitoring or evading safeguards. The engineering object is qualification of governance and evidence boundaries, not operational enablement.

9. Minimum qualification record

A future photopolymer-specific security assessment should identify the system boundary, protected assets, authorised roles, capability under review, access model, control objective, evidence collected, test or incident state, decision rule and residual uncertainty. Claims should remain at the level demonstrated by that record.

10. Responsible disclosure remains unevidenced

Responsible disclosure may be relevant when a security weakness is discovered, but neither controlled source establishes a photopolymer-specific disclosure procedure in the evidence available here. No procedure is asserted. If later included, its source and governance basis should be explicit.

11. A defensive assurance case for manufacturing configuration

The proposed security assessment identifies the assets needed to reproduce the intended manufacturing state: approved design, material identity, build configuration, equipment configuration, process records and acceptance evidence. For each asset it asks what loss of confidentiality, integrity or availability would mean for the particular workflow. The consequence should be tied to the asset and decision rather than assigned from a generic AM threat label.

A hypothetical configuration discrepancy illustrates the defensive question. A receiving operator finds that the build configuration differs from the approved revision. The response should preserve the discrepancy, identify affected work and route disposition through the defined authority. A valid digital signature on one file would not establish that the physical material, equipment and all associated files match that configuration. The assurance case therefore needs a chain of checks whose scope is explicit.

The exercise described here does not require creating or distributing an attack. It can use a controlled test record or a benign mismatch in a non-production environment to assess whether the system detects, contains and documents an inconsistency.

12. Assess recovery as well as prevention

A proposed recovery exercise would begin from a declared loss of access to a required manufacturing record and test whether the organisation can restore an authorised state with its evidence intact. Restoring a file is only one observation. The assessment should also determine whether the restored revision is correct, whether affected production can be identified and whether the authority to resume work is documented.

Metrics need a defined starting event and completion condition. Time to retrieve a backup, time to verify the configuration and time to resume authorised production are different intervals. Combining them into one favourable number can hide the unresolved activity. Likewise, a successful demonstration on one record type does not establish recovery capability for every asset.

A threat assessment should be updated when the workflow changes, including new external interfaces or changes in who can authorise configuration. The aim is to preserve a defensible manufacturing state under the assessed conditions. Dual-use and security concerns remain subject to their own context; this framework does not infer malicious intent from a technical deviation or provide operational instructions for compromising a manufacturing system.

Supplementary critical engineering analysis: Threat model and scope control: Dual-use concerns differ between design-file theft, unauthorized reproduction, tampering with process parameters and disclosure of sensitive manufacturing data. A security review must define the protected asset, credible actor, access route, observable indicator and consequence before prescribing countermeasures. General additive-manufacturing cyber-risk literature offers candidate methods, but specific claims concerning a photopolymer machine require evidence of its architecture and exposure paths.

Integrity verification without overclaiming: Version-controlled build files, access logs and independently retained acceptance data improve accountability. However, a hash proves digital-file consistency rather than dimensional accuracy, chemical identity or functional safety of a cured part. Security controls should therefore connect to manufacturing validation, and their effectiveness should be evaluated with permitted test cases. No detailed attack procedure or exploit path is needed for this engineering governance review.

Critical evidence synthesis: Dual-use governance: distinguish threat models from proven attacks: Additive-manufacturing security literature spans theft of design files, unauthorised modification of process settings, manipulation of traceability records and misuse of manufacturing capabilities. These mechanisms do not share the same evidence base or mitigation strategy. A credible technical review maps each threat to an actor capability, vulnerable interface, potential consequence and observable detection mechanism, while separating demonstrated attack outcomes from plausible scenarios. The existence of a theoretical pathway is not itself evidence of successful exploitation of photopolymer equipment.

For photopolymer processes, proposed controls should be tested against process-specific failure modes, not imported unchanged from metal AM. File hashes may detect post-approval design changes but do not establish correctness of exposure settings or absence of physical tampering. Access controls, signed build recipes, independent material qualification and part acceptance testing address different layers. Validation should report residual risk and false alarm behaviour rather than implying that any single digital safeguard assures the properties of the manufactured part.

Threat-model boundaries and validation of controls: A dual-use review must separate the technical capabilities of vat photopolymerisation from speculation about intended harmful use. A useful threat model defines assets, credible adversarial actions, attack surfaces and observable consequences. For engineering quality, plausible targets include malicious build-file modification, unauthorized parameter changes, compromised material certificates and removal of inspection records.

A cryptographic checksum establishes whether two files are identical, but cannot prove that a file's content is clinically, legally or technically acceptable. Authenticity requires trusted key management and traceable approvals; process correctness further requires machine and part-level evidence. Security controls must not be reported as qualification evidence for resin performance.

Controls should be tested against defined failure injections: altered slice data, swapped resin lot, modified exposure settings, falsified acceptance record and lost network access. For each case specify detection time, permitted fallback, record preservation and recovery responsibility. Restricting digital access without securing local machine configuration leaves a separate untested path.

The literature base supporting generalized AM security claims should be separated from evidence demonstrated on photopolymer equipment. Controls proposed in this article are bounded risk-management measures; no claim of measured attack frequency or guaranteed prevention follows from the framework alone.

13. Limitations

The evidence is AM-general. Source [1] is limited here to publisher-abstract depth. Photopolymer appears in the article as a bounded implementation context, not as a claim that threats or controls have been demonstrated for a specific resin, printer or workflow.

Separating threats, vulnerabilities and demonstrated impact: A general additive-manufacturing security taxonomy identifies possible attack surfaces, not evidence that a particular photopolymer machine has been compromised. Threat modeling should distinguish an adversary's objective, access, manipulated artifact and possible consequence. Altering an exposure map, changing a build orientation or substituting a material lot have different detection opportunities and need not produce the same observable defect. A security claim must specify which scenario has been tested and which remains hypothetical.

A robust validation design combines digital integrity tests with physical part acceptance checks. A verified slice file does not ensure that measured irradiance, resin condition and post-processing matched the intended process. Conversely, a mechanically passing specimen cannot prove that confidential design information was protected. Tests should address both information integrity and material-state integrity, preserving a clear distinction between general dual-use concern, process-specific vulnerability and experimentally demonstrated harm.

14. Conclusions

AM security and dual-use literature provides a basis for defining capability, access, control and governance questions [1,2]. It does not establish photopolymer-specific findings. ER-490 therefore keeps the photopolymer domain as a scope boundary, names the missing evidence explicitly and excludes operational attack or control-circumvention detail.

References

1. Yampolskiy M, King WE, Gatlin J, Belikovetsky S, Brown A, Skjellum A, Elovici Y. Security of additive manufacturing: Attack taxonomy and survey. *Additive Manufacturing*. 2018;21:431-457. <https://doi.org/10.1016/j.addma.2018.03.015>.
2. Grand-Clement S, Reinertsen SS. Additive Manufacturing of Conventional Military Equipment: Implications for Arms Control and Security. UNIDIR Science and Technology Watchtower. 2026. 40 pp. <https://doi.org/10.37559/CWP/26/ERC/06>.

Competing interests

The author is Founder, CEO and CTO of 3Dresyns by Resyner Technologies S.L. The company develops and supplies photoresins and related process materials. No proprietary formulation, manufacturing sequence, process window or comparative product recommendation is disclosed.

Data availability

No new experimental dataset was generated.

Copyright

© 2026 Juan Segurola. All Rights Reserved.