

Cybersecurity of Digital Manufacturing Recipes and Equipment: Access, Integrity, Provenance and Recovery

Protecting the digital-to-physical chain in additive manufacturing without compromising equipment safety or availability

Juan Segurola

3Dresyns by Resynr Technologies S.L.

© 2026 Juan Segurola. All Rights Reserved.

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

ER-350 · Engineering Review · Version 0.5 · 28 September 2026

Abstract

Digital files and recipes can alter physical geometry, exposure, supports and post-processing. A defensible security architecture identifies design files, build files, machine parameters, material recipes, calibration data, user credentials and production records, then assigns owners and required protections. Printers, cure chambers and material-handling systems may have long service lives, vendor dependencies and safety/availability constraints. Hashes, signatures, controlled repositories and versioned recipes can help show that the executed digital object matches the approved one. Design approval, recipe editing, machine operation, maintenance and cybersecurity administration are different privileges. Qualification therefore depends on preserving the measured state, configuration and exception history needed to distinguish these mechanisms in production rather than relying on nominal recipe identity alone.

Keywords: cybersecurity; additive manufacturing; digital manufacturing; recipe integrity; operational technology; provenance; recovery

1. Significance and scope

Digital files and recipes can alter physical geometry, exposure, supports and post-processing. The engineering question is how access control, integrity protection, provenance and recovery should secure the digital-to-physical manufacturing chain without undermining the availability and safe operation of production equipment. The review focuses on evidence that supports repeatable manufacturing decisions and excludes proprietary recipes, supplier-specific settings and undocumented operator heuristics.

1.1 Corpus boundary

ER-350 owns cybersecurity controls for digital manufacturing recipes, additive equipment and connected production assets. It does not own general corporate information security or the electronic batch-record semantics covered by ER-349.

2. Additive manufacturing creates cyber-physical consequences

Digital files and recipes can alter physical geometry, exposure, supports and post-processing. Cybersecurity therefore has to protect confidentiality, integrity and availability while recognising that an integrity failure can become a product-quality failure. NIST has specifically highlighted additive manufacturing data and direct digital manufacturing as security targets [1-3].

3. Asset and data classification comes first

A defensible security architecture identifies design files, build files, machine parameters, material recipes, calibration data, user credentials and production records, then assigns owners and required protections. Treating every file identically obscures the assets whose alteration would have the greatest physical consequence [1,2].

4. OT security differs from office IT

Printers, cure chambers and material-handling systems may have long service lives, vendor dependencies and safety/availability constraints. NIST SP 800-82 emphasises risk-based safeguards tailored to operational technology rather than indiscriminate deployment of controls that could disrupt production [4].

5. Integrity and provenance need independent evidence

Hashes, signatures, controlled repositories and versioned recipes can help show that the executed digital object matches the approved one. However, provenance must include the transformation chain from design through slicing and machine execution; protecting only the original CAD file leaves downstream manipulation exposed [1-3].

6. Access control should follow manufacturing roles

Design approval, recipe editing, machine operation, maintenance and cybersecurity administration are different privileges. Shared accounts erase attribution and should be avoided where the equipment supports individual identity. Emergency access should be exceptional, logged and reviewed [2,4,5].

7. Recovery is part of security

Backups are useful only if configurations, recipes and machine states can be restored in a controlled way. Recovery testing should include known-good software/firmware, recipe repositories, certificates or keys where used, and verification that restored equipment returns to a qualified manufacturing state [4,5].

8. Qualification architecture

A manufacturing-security baseline should combine governance, asset inventory, access control, integrity monitoring, network segmentation, secure update practice, event logging, backup and incident response. Controls should be selected against the specific digital-to-physical risk rather than applied as a generic checklist [1-5].

Table 1. Qualification matrix for cybersecurity of digital manufacturing recipes and equipment.

Asset	Primary risk	Control emphasis
Design/build files	Theft or malicious alteration	Access, integrity, provenance
Recipes	Unauthorised parameter change	Version control and approval
Printer/controller	Compromise or unsafe command	OT segmentation and hardening
Production records	Tampering or loss	Integrity, backup, retention
Credentials/keys	Privilege abuse	Identity and lifecycle control

9. Interpretation matrix

For manufacturing cybersecurity, a recipe or equipment anomaly may arise from unauthorised modification, integrity loss, configuration drift, credential misuse or an incomplete recovery. Diagnosis should correlate hashes, access logs, approved baselines and recovery records to establish where the digital-to-physical chain diverged.

Table 2. Diagnostic interpretation matrix for manufacturing cybersecurity.

Security event	Manufacturing question	Recovery evidence
File hash mismatch	Was approved geometry altered?	Known-good signed/versioned source
Unexpected parameter change	Who changed recipe and when?	Audit and access logs
Controller compromise	Can machine be trusted?	Reimage/requalify procedure
Backup restore	Is production state valid?	Post-recovery qualification check

10. Limitations and evidence gaps

Cybersecurity evidence for additive-manufacturing systems is dominated by general OT guidance and threat analyses rather than long-term incident datasets for photopolymer production. Equipment lifecycles, proprietary controllers and disconnected subsystems can constrain the controls that are technically deployable. This review therefore defines security objectives and evidence needs, not a universal control set or quantified residual-risk threshold.

11. Conclusions

Cybersecurity of digital manufacturing should protect the integrity and provenance of the digital-to-physical chain while preserving safe equipment operation. Access control, change traceability, asset classification and recoverability are complementary controls rather than substitutes. Qualification should demonstrate that unauthorised or corrupted recipe states can be detected, contained and recovered without losing manufacturing evidence.

References

1. Milaat F, Lubell J. Layered Security Guidance for Data Asset Management in Additive Manufacturing. *Journal of Computing and Information Science in Engineering*. 2023. doi:10.1115/1.4064128.
2. Paulsen C. Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium. NISTIR 8041. National Institute of Standards and Technology, 2015. doi:10.6028/NIST.IR.8041.
3. Pascoe C, Quinn S, Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. National Institute of Standards and Technology, 2024. doi:10.6028/NIST.CSWP.29.
4. Stouffer K, Pease M, Tang C, Zimmerman T, Pillitteri V, Lightman S, Hahn A, Saravia S, Sherule A, Thompson M. Guide to Operational Technology (OT) Security. NIST SP 800-82 Rev. 3. National Institute of Standards and Technology, 2023. doi:10.6028/NIST.SP.800-82r3.
5. ISO/ASTM 52920:2023. Additive manufacturing - Qualification principles - Requirements for industrial additive manufacturing processes and production sites. ISO, Geneva, 2023.

Competing interests

The author is Founder, CEO and CTO of 3Dresyns by Resyner Technologies S.L. No comparative product recommendation is made.

Data availability

No new experimental dataset was generated for this review.