

A multi-layer cyber-physical 3D printing security framework for the aerospace and defense industry

Grzegorz Budzik^{1*} , Andrzej Paszkiewicz² , Lucjan Śniezek³,
Mirosław Surowaniec^{1,4} , Kamil Burczy^{5,6} , Dariusz Rączka² 

¹ Department of Machine Design, Faculty of Mechanical Engineering and Aeronautics, Rzeszow University of Technology, Al. Powstańców Warszawy 12, 35-029 Rzeszów, Poland

² Department of Complex Systems, Faculty of Electrical and Computer Engineering, Rzeszow University of Technology, Al. Powstańców Warszawy 12, 35-029 Rzeszów, Poland

³ Institute of Robots & Machine Design, Faculty of Mechanical Engineering, Military University of Technology, ul. Gen. S. Kaliskiego 2, 00-908 Warsaw, Poland

⁴ Huta Stalowa Wola S.A., ul. Gen. Tadeusza Kasprzyckiego 8, 37-450 Stalowa Wola, Poland

⁵ Doctoral School of the Rzeszow University of Technology, Al. Powstańców Warszawy 12, 35-029 Rzeszów, Poland

⁶ Polskie Zakłady Lotnicze Sp. z o.o., ul. Wojska Polskiego 3, 39-300 Mielec, Poland

* Corresponding author's e-mail: gbudzik@prz.edu.pl

ABSTRACT

Additive manufacturing technologies rely on extensive digital data processing, beginning with 3D-CAD model development and continuing through data preparation, process planning, manufacturing execution, and post-processing operations. As additive manufacturing systems become increasingly adopted in aerospace, space, defense, and other critical industrial sectors, ensuring the security of both digital and physical assets becomes a significant challenge. This paper presents a multi-layer cyber-physical security framework for additive manufacturing environments. The proposed approach distinguishes three complementary security layers: the 3D geometric data processing layer, the technological process data layer, and the physical process layer. For each layer, critical assets, potential cybersecurity threats, and recommended protection mechanisms are identified and analyzed. Particular attention is devoted to the protection of engineering data, process parameters, machine configurations, simulation results, and manufacturing infrastructure, as these elements directly influence the quality, reliability, and operational safety of manufactured components. The paper further extends the analysis by introducing a multi-level physical protection model dedicated to additive manufacturing facilities and evaluating the proposed security measures using the Confidentiality–Integrity–Availability (CIA) model. The results demonstrate that effective protection of additive manufacturing environments requires the integration of organizational, physical, and cyber-physical security mechanisms across the entire production lifecycle. The proposed framework may support the development of secure additive manufacturing environments for aerospace, space, defense, and other industries producing high-value or safety-critical components.

Keywords: additive manufacturing, cybersecurity, cyber-physical systems, 3D printing, CIA model, multi-layer analysis, information security, aerospace industry, defense industry.

INTRODUCTION

For many years, 3D printing supported production processes at the concept stage or during the early development of geometric prototypes.

Rapid prototyping devices based on additive processes most often constituted separate laboratory units with limited physical access and limited access to manufacturing-cycle data. Due to the limited access to the laboratory infrastructure

used, the security systems applied were not significantly expanded. Currently, the development of additive technologies and their increasingly broad application in the defense, aerospace, and space industries require a new approach to production security, associated with a multi-layer perspective on modeling, prototyping, and production processes [1]. Because additive manufacturing requires the numerical preparation and processing of process data, particular attention should be paid to a number of aspects related to ensuring the security of numerical data, which may sometimes constitute classified information. Additive manufacturing is no longer limited to developing a 3D model and printing it using an additive machine. Many stages associated with the technological process can be distinguished in the preparation of the data required to carry out printing: positioning in the 3D printer workspace, division into working cross-sections (layers), determination of the layer manufacturing structure, and generation of support structures. All of these technological factors are directly responsible for the properties of products, including their mechanical strength, which in the case of aerospace, space, or defense applications is an important production issue and, in many cases, is subject to standardization [2]. Technological data belong to information subject to strict access control. Some of this information may be included in the description of process-file data, some constitutes technological information, and some may relate to information used exclusively by the 3D printer operator [3]. In the case of additive technologies, it should be remembered that post-process activities are performed after each such operation, and these activities form an important part of the technological process. These operations affect the geometric accuracy of manufactured elements and their mechanical properties, also when, for example, thermo-chemical treatment or coatings are applied. Data of this type do not have to follow the additively manufactured product, which may constitute a semi-finished product or a component [4]. In this case, information protection may take place at both the numerical and physical levels.

3D printing also requires an appropriate approach to pre-process operations, which include, among others, preparation of the equipment and materials, the material storage process, and material delivery. These factors ultimately affect product quality and should be protected appropriately [5].

Another important factor in 3D printing-based production is quality control, based on geometric measurements, among other things. Information regarding product accuracy is critical in every industry and is a component of the Industry 4.0/5.0 framework. [6].

RELATED WORK

The processing of process data during additive manufacturing constitutes an extremely important sequence of operations that transform input data into useful output information used to carry out 3D printing. This issue has been known and developed from the beginning of the implementation of additive techniques as an alternative to conventional manufacturing [7]. Several areas related to additive manufacturing can be distinguished here, in particular those concerning 3D-CAD solid modeling and the software used for this purpose [8, 9]. Important issues in this case also include software-based data processing and the data formats used in 3D printing processes, which define how a three-dimensional model is obtained, including, among others, creation of the previously mentioned 3D-CAD models, reverse engineering, surface or volumetric 3D scanning, computed tomography, and artificial intelligence [10, 11]. In each of these cases, different methods of data processing can be used, adapted to the intended use of the model and its accuracy as the basis for the manufacturing process. These cases require not only data processing, but also secure transfer of data between individual workstations, for example a tomograph, a data-processing station, and a 3D printer.

The first data transfer solutions were based on direct data transfer from the computer on which the model was prepared to the printer's computer. From a data transfer perspective, these solutions are safe and continue to be used. 3D printing stations do not have to operate within a single laboratory location; therefore, network transfers may be used, and access to data should be based on an appropriate and secure organizational structure. Such a structure is used by aerospace and defense companies, which effectively limit the possibility of an external cyberattack on the network and also protect it against physical interference, for example by preventing mass-storage devices from being connected to USB ports of devices belonging to the company structure.

The issue of data security for additively manufactured products has recently acquired a new dimension. Considerations regarding general aspects of cybersecurity in additive manufacturing are appearing in the literature [12]. This can apply to both a general approach, encompassing many aspects of data processing, and studies on specific approaches to selected process stages, such as the possibility of cyberattacks targeting additive manufacturing [13, 14]. An important issue is the approach to the process from the point of view of legal conditions in various areas of application, for example the manufacturing of critical-infrastructure components. It is necessary to mention the use of artificial intelligence algorithms in the process of generating data for 3D printing and the risks relating both to legal conditions concerning ownership rights to the model and to the place where these data are processed and stored, the methods of making them available, and the data sources on which AI algorithms operate [15]. Many 3D printing systems operate in a network environment; therefore, the issue of developing an appropriate hierarchy of access to data and devices, as well as appropriate security protocols, is particularly important in the context of cybersecurity [16, 17].

Taking into account the analysis of the current state of the art, this article proposes a new multi-layered approach to security in additive manufacturing, encompassing the comprehensive area of

data processing and the physical area, which is crucial for production safety, particularly in the defense and aerospace industries.

PROPOSED SOLUTION

System model

The analysis of the additive process and the associated pre-process and post-process operations, as well as the physical aspects of manufacturing processes based on 3D printing, made it possible to develop a multi-layer model for security analysis and protection systems for 3D printing as a cyber-physical production system. In this article, in order to illustrate certain stages of the additive process, a model of a drone support frame was developed, which may serve as a representative example of a model used both in aerospace technologies and in defense applications.

The model distinguishes three main layers of data processing and protection: the first layer, involving the preparation and processing of geometric data of the three-dimensional model (3D data processing - 3DDP); the second layer, involving technological data directly related to the additive process (technological processing data - TPD); and the third, physical layer, which may include pre-process, process, and post-process operations, finishing, and quality control, and is

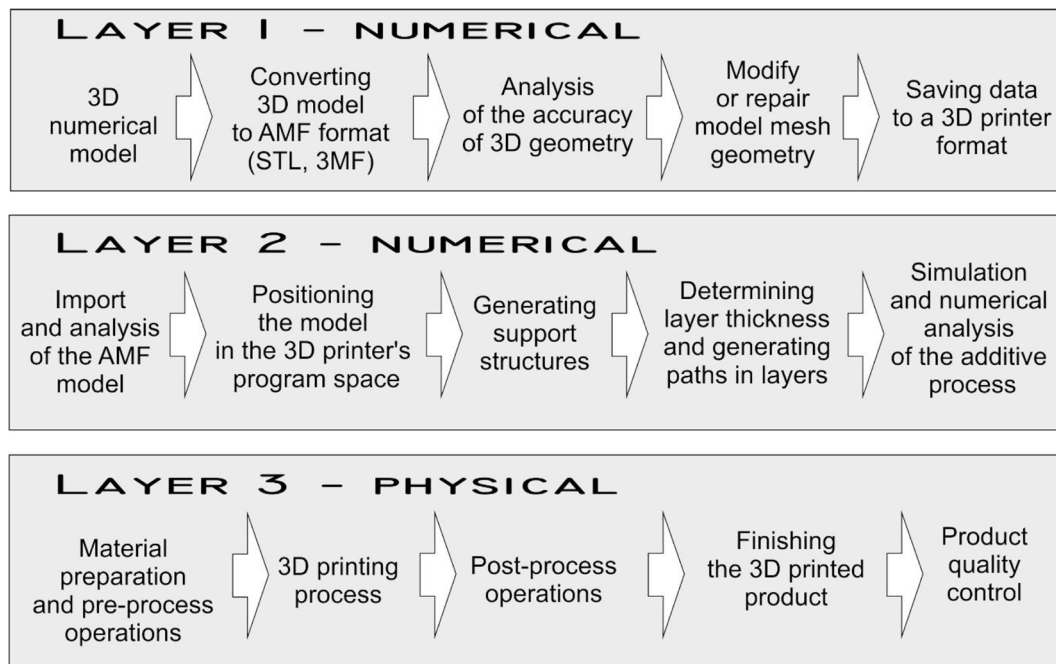


Figure 1. Multi-layered model of 3D printing process

based on physical access control to room zones and products manufactured by 3D printing (physical data of processes - PDP). The concept of the multi-layered model is illustrated in Figure 1.

LAYER ONE

The first layer, involving the preparation and processing of three-dimensional geometry data, refers to the standard 3D-CAD modeling processes based on software that is usually general-purpose and widely used in the technical sector. In this case, the software itself is usually not a protected asset related to a given product, because it is widely available commercially on the market. Exceptions may include calculation procedures or procedures for creating models specific to the aerospace, space, or defense industries that are specially dedicated to this software. In such cases, software or calculation macros must be subject to appropriate procedures protecting them against external unauthorized interference.

In this layer, five components can generally be distinguished: development of a 3D numerical model using 3D-CAD systems or 3D digitization; conversion of the developed model to STL format; analysis of the representation accuracy of the 3D model; modification or repair of the geometry (the STL model mesh); and saving to a format dedicated to the 3D printer. The individual stages or components of this layer may be modified and may occur in different configurations depending on the form of data preparation. When new

geometry is created, 3D modeling is a creative process carried out using 3D-CAD software. This can be followed using the example of a 3D-CAD model of a drone support structure intended to be manufactured by 3D printing. In the process of object modeling, various sequences leading to the creation of the model can be used and recorded in the structure tree (specification) of a given program (Figure 2). In 3D-CAD modeling programs, the structure tree is a very important element both in creating the original model and in introducing modifications resulting from technological changes or product modernization.

It should be remembered that the structure tree can be edited only by the same program and in the same version, or possibly in a higher version. The individual sequences should be treated as important technological data that should be protected. 3D-CAD software allows data to be saved in universal formats such as STEP, IGS, STL, or AMF; however, formats of this type describe only the solid geometry and do not allow the model-creation structure to be edited. The conversion process is responsible for the accuracy with which the geometry is represented relative to the nominal 3D-CAD model; for this reason, it should be treated as important technological data that should be protected. After conversion from a 3D-CAD model or from digitization, an STL file may contain defects or shape errors (Figure 3a) and may require repair. This requires the use of appropriate software sequences in order to generate a model with accurate geometry (Figure 3b), which may be covered by a cybersecurity procedure.

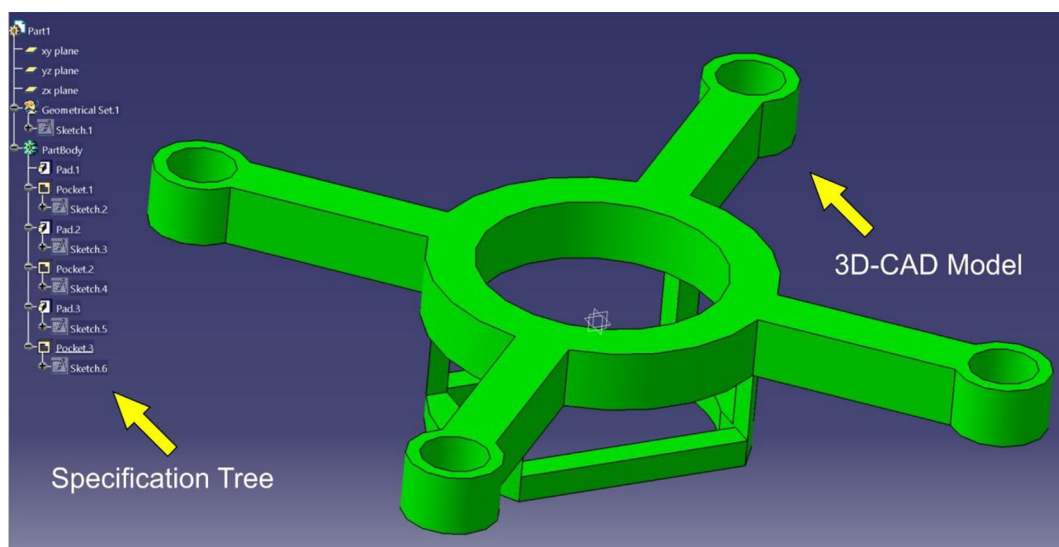


Figure 2. 3D-CAD model of the drone support structure

The last stage in the first layer is optional and may also be performed at the beginning of the second layer, depending on the specific nature of the additive manufacturing process. This stage cannot be assigned unambiguously to a given layer, because it depends on the 3D-CAD modeling software used, the software for converting files to STL format, the software controlling the 3D printer, and the type of data transfer to a specific printer. When network communication is used between computers for modeling and data processing and the 3D printer, appropriate network security procedures must be applied.

From the cybersecurity perspective, the first layer of preparation and processing of three-dimensional geometry data includes a number of digital assets that constitute an important element of an enterprise's intellectual property. The most important protected resources include 3D-CAD models, model structure trees, modeling procedures, calculation macros, design procedures, data exchange files (STEP, IGS, STL, AMF), geometry repair algorithms, and data obtained in the 3D digitization process. Information recorded in the model structure tree is of particular importance because it contains the complete history of geometry creation and design knowledge that makes it possible to reconstruct the process of designing the product. In the case of components intended for the aerospace, space, or defense industries, these data may represent much greater value than the final geometric model itself. In the analyzed layer, threats related to the loss of data confidentiality, integrity, and availability may occur. Loss of confidentiality may include theft of CAD models, takeover of AMF or STL files, copying of design

documentation, and acquisition of design procedures by unauthorized persons. The takeover of complete design data that makes it possible to reconstruct the product geometry and the applied design solutions is particularly dangerous.

The second group of threats is the violation of data integrity. This may include modification of the model geometry, changes to conversion parameters between data formats, manipulation of the model structure tree, or the introduction of difficult-to-detect design changes. Even minor modifications of geometry can lead to a significant deterioration of the product's functional properties. For example, changing the thickness of a selected structural rib of a drone support frame by approximately 0.2 mm may not be noticed during standard visual inspection, but it may result in reduced structural strength and a shortened service life. Another important threat is the loss of availability of design data, which may result from deletion of design files, encryption of CAD repositories by ransomware, or failure of the IT infrastructure used to store design documentation. Loss of access to current versions of models may lead to production downtime and the need to recreate part of the design work.

In order to reduce the risk of the described threats, appropriate protection mechanisms must be implemented. The most important include multi-level access control to design data, encryption of repositories storing models, the use of digital signatures enabling verification of file authenticity, versioning of design documentation, and archiving of successive model versions. In addition, it is recommended to maintain a register of changes introduced in CAD files, perform

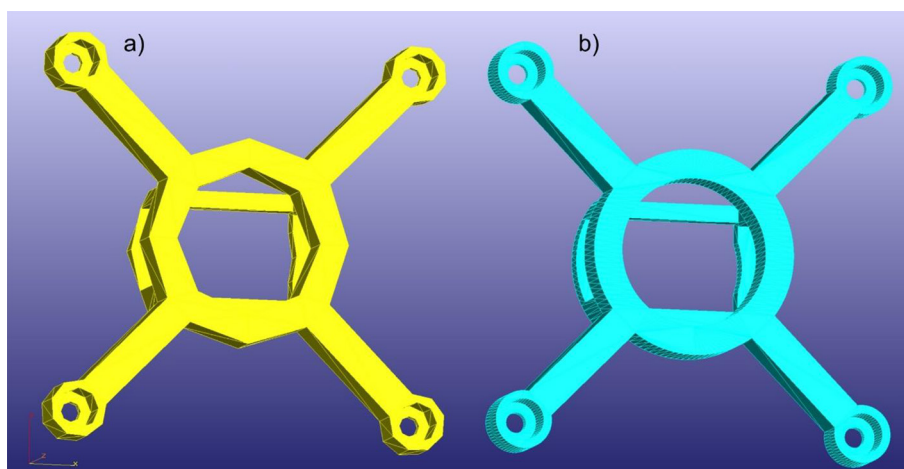


Figure 3. STL model of the drone support structure: a) with insufficient geometry representation accuracy, b) model after correction of representation accuracy

regular backups, and monitor access to design resources. The application of these mechanisms makes it possible to reduce the risk of unauthorized interference with design data and increases the level of protection of the intellectual property of an enterprise using additive technologies.

LAYER TWO

The second layer of numerical data processing is closely related to preparing data directly for 3D printing and for the 3D printer. The process can be carried out using software in various configurations, i.e. 3D printer libraries used by 3D-CAD software manufacturers, standalone programs for processing and converting 3D-CAD files to AMF format, or software dedicated to 3D printers. Each of these options may be available online

or offline. It should be added that some 3D printer manufacturers require users' data concerning manufactured models to pass through their servers over the network. From the point of view of data security, the use of this type of 3D printer and software entails a significant risk of data interception and unauthorized use (Figure 5). Due to the requirements for manufacturing products for the aerospace or defense industry, such a situation is not acceptable. In the second layer, the position of the model relative to the coordinate system of the additive machine is determined. These are important parameters that determine the mechanical properties of products, as well as dimensional and shape accuracy and the time of the manufacturing process. Figure 4 shows STL models of the drone support frame in different orientations relative to the printing plane: Figure 4a - supported on the structure fastening the power supply and control

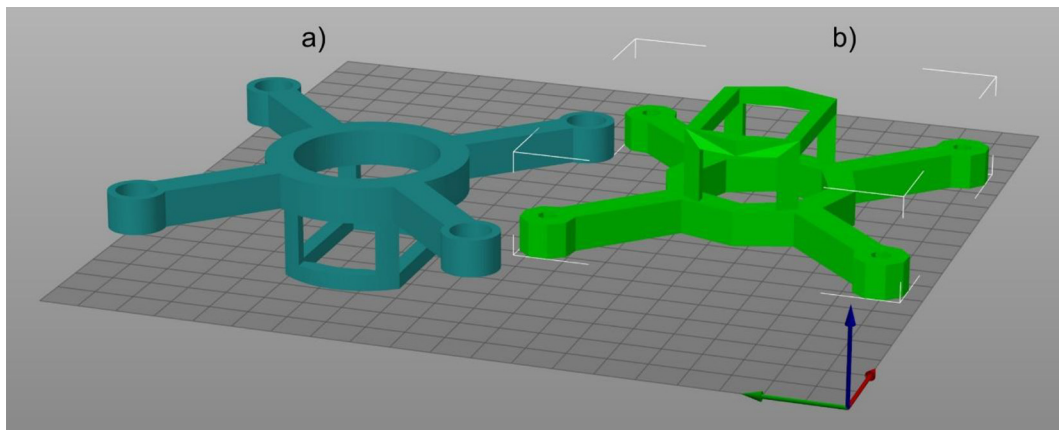


Figure 4. STL models of the drone support frame on the software build platform of a 3D printer: a) mounting structure positioned on the platform, b) motor arms positioned on the working plane

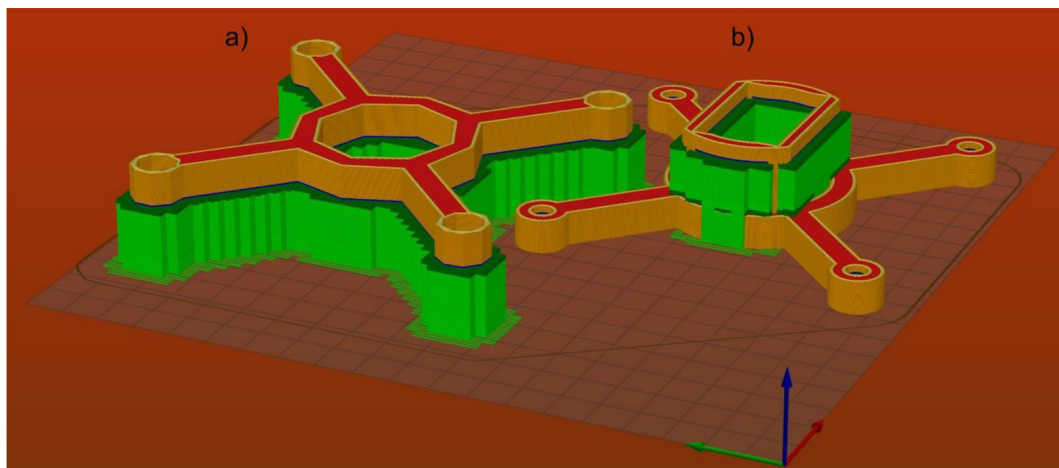


Figure 5. STL models of the drone support frame on the software build platform of a 3D printer with support structures: a) mounting structure positioned on the platform, b) motor arms positioned on the working plane

system; Figure 4b - supported on the motor-mounting arms. The same applies to process data for individual cross-sections, for example the arrangement of material paths for the MEX method or the path of the scanning laser beam in the PBF process.

In the final stage of the second layer, a numerical simulation of the process can be carried out, making it possible to detect potential process defects before the final 3D print is launched. The process can be traced cross-section by cross-section in order to detect possible discontinuities in the internal structure. Figure 6 shows a view of layer 171 for the models on the build platform. As in the previous stages, numerical data are generated and require special protection; reference should be made to the last two layers of the process, namely the cyber-physical configuration of 3D printing.

Depending on the number of options available in the programs controlling the printing process, it is possible, among other things, to change the working cross-section thickness (model layer), infill style, support type, and 3D print cross-section (layer) thickness. All of these parameters constitute important technological data that directly affect the strength of the model, printing time, and material consumption. The selection of these parameters often requires extensive experience on the part of the 3D printer operator and sometimes requires simulation studies and strength tests; therefore, these data are important from the point of view of their security.

The second layer covers the preparation of technological data directly related to the execution of the 3D printing process. In this layer, parameters are defined that determine how the product is made, its mechanical properties, dimensional and shape accuracy, and manufacturing time. From the cybersecurity perspective, it is one of the most important elements of the additive process, because it contains the technological knowledge of the enterprise, which often has greater value than the geometry of the model itself. The most important protected assets include data concerning the orientation of the model on the build platform, configuration of support structures, process parameters, paths of motion of the head or laser beam, files controlling the printer, results of numerical simulations, and device configuration. These data have a direct impact on the quality, strength, and reliability of the manufactured component.

The main threats in this layer include loss of confidentiality of technological data, unauthorized modification of process parameters, and interception of data during their transmission between the process-preparation workstation and the 3D printer. Changes to model orientation, process parameters, scanning strategy, or support configuration are particularly dangerous, because they may lead to deterioration of the mechanical properties of the product without visible changes in its external geometry. An additional threat is the

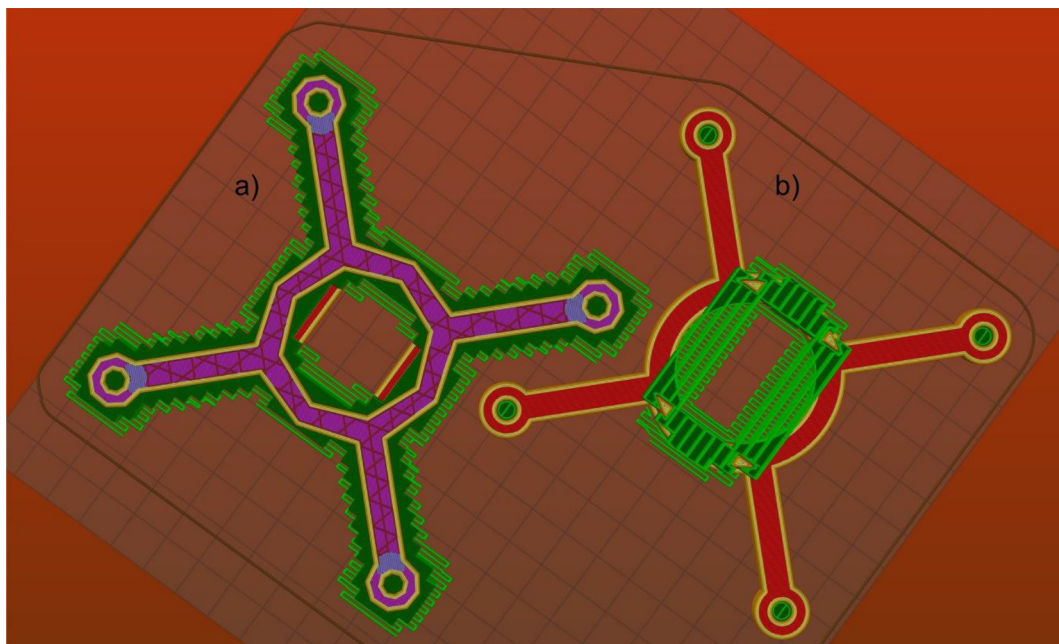


Figure 6. View of layer 171 of the models during 3D print simulation: a) mounting structure positioned on the platform, b) motor arms positioned on the working plane

loss of data availability caused by failures of IT systems or malicious software. In order to reduce risk, it is recommended to apply access control to technological data, transmission encryption, segmentation of the production network, digital signatures for process files, and registration of all changes to technological parameters. An important element of protection is also ensuring Process Integrity, understood as maintaining the immutability of key production parameters from the moment the process is prepared until the product has been manufactured.

LAYER THREE

The third, physical layer is related to the preparation of material (raw material), pre-process and process operations, and the 3D printing process itself. It additionally includes finishing and quality control and, if applicable, preparation for shipment. It is based on physical access control to room zones and products manufactured by 3D printing. An additively produced 3D model may be a finished product or a semi-finished product for further processing. For this reason, it must be transported to subsequent technological workstations or to a warehouse. Depending on internal or external logistics, products should be protected both against damage and against the possibility of visual or physical interference by unauthorized persons. For this reason, companies manufacturing licensed or aerospace products have implemented appropriate access-control procedures for persons within the enterprise as well as persons from outside the company. From the cybersecurity perspective, this layer constitutes a combination of physical, organizational, and cyber-physical safeguards whose purpose is to protect the production infrastructure, technological data, and manufactured components against access by unauthorized persons. The most important protected assets include 3D printers, workstations, network infrastructure, input materials, semi-finished products and finished products, as well as technological documentation and quality-control results. Components intended for the aerospace, space, and defense industries are subject to particular protection, because their loss, copying, or modification may lead to the disclosure of confidential information or may threaten operational safety.

The main threats include unauthorized access to production zones, photographing or copying technological information, theft of components and materials, manipulation of 3D printer settings, and interference with the enterprise's ICT infrastructure. Actions by persons who have legitimate access to enterprise resources but may lead to unauthorized acquisition or disclosure of production data also remain a significant threat.

In order to reduce risk, multi-layer protection mechanisms are used, including access control to facilities and production zones, CCTV monitoring, user identification using RFID cards, registration of activity in protected zones, and archiving of access logs. Physical safeguards are complemented by cybersecurity solutions such as segmentation of the production network, management of user permissions, monitoring of system activity, and protection of IT and OT infrastructure against unauthorized interference. Building security awareness among employees and regularly improving procedures for protecting information and production resources also remain important elements.

Within the third layer of safeguards, a procedure for visits by external persons to an aerospace company is presented (Table 1).

The individual security levels, in accordance with the adopted procedure, are intended to comprehensively protect production information against access by unauthorized persons. Security procedures are continually developed; it is also necessary to build information awareness among enterprise employees and security personnel.

The presented protection levels perform different security functions related to protecting the resources of the additive manufacturing environment. In order to determine the impact of individual safeguards on the protection of information and technological resources, an additional analysis was carried out using the classical CIA model (Confidentiality, Integrity, Availability). This model is one of the fundamental paradigms of cybersecurity and makes it possible to assess the extent to which individual protection levels support the preservation of confidentiality, integrity, and availability of information and resources used in the additive manufacturing process. The results of the analysis are presented in Table 2.

The analysis presented in Table 2 indicates that the individual protection levels support the implementation of the basic security attributes defined in the CIA model (Confidentiality, Integrity,

Table 1. Multi-level security model for visitor access to an aerospace additive manufacturing facility

Security level	Protected assets	Potential threats	Potential effects	Protection mechanisms
Level 1: Perimeter protection	Enterprise infrastructure, buildings, warehouses, production zones	Intrusion by unauthorized persons, reconnaissance of the facility, infrastructure sabotage, theft of property	Loss of information confidentiality, infrastructure damage, disruption of the production process	Plant fencing CCTV monitoring vehicle entry control security post ban on photography and filming
Level 2: Visitor registration	Organizational data, information on production processes, enterprise personnel	Impersonation of authorized persons, unauthorized entry to the facility, acquisition of information about the enterprise	Breach of organizational security, acquisition of information about technological processes	Identity verification, declaration of the purpose of the visit, authorization of the meeting, issuance of a temporary pass, signing of the regulations
Level 3: Access to a protected zone	Technological documentation, production workstations, industrial equipment	Unauthorized access to critical zones, observation of production processes, acquisition of technological information	Disclosure of confidential information, loss of intellectual property, possibility of preparing sabotage activities	Entry only with an escort, RFID access-point control, restricted access to selected zones, monitoring of visitor movement
Level 4: Additive manufacturing zone	3D printers, process data, input materials, semi-finished products, finished products	Theft of technological data, copying of process parameters, manipulation of printer settings, material substitution, sabotage of the production process	Deterioration of product quality, loss of technological advantage, manufacture of components that do not meet safety requirements	Restricted access to 3D printers, secured workstations, monitoring of the production process, registration of user activity
Level 5: Zone exit procedure	Production data, documentation, components, and materials	Removal of documentation, copying of data, unauthorized removal of components or materials	Information leakage, loss of intellectual property, violation of security procedures	Return of the pass, exit control, confirmation of visit completion, archiving of access logs

Table 2. Multi-level physical and cyber-physical protection model for an additive manufacturing environment, illustrated by an aerospace company

Security level	Confidentiality	Integrity	Availability	Justification
Level 1: Perimeter protection	Y	Y	Y	Limits unauthorized access to infrastructure and reduces the risk of physical damage to production resources.
Level 2: Visitor registration	Y	N	N	Ensures identification and authorization of persons gaining access to the facility.
Level 3: Access to a protected zone	Y	Y	N	Limits the possibility of obtaining information and interfering with the production environment.
Level 4: Additive manufacturing zone	Y	Y	Y	Protects technological data, equipment, and the continuity of the production process.
Level 5: Zone exit procedure	Y	Y	N	Limits the risk of taking information, documentation, and components outside the protected area.

Note: Y – the attribute is satisfied at the corresponding security level, N – the attribute is not considered at the corresponding security level.

Availability). The CIA assessment was performed qualitatively based on the primary security objective addressed by each protection level. An attribute was marked as “Y” when the corresponding security level directly supports the protection of confidentiality, integrity, or availability through its implemented safeguards. An attribute was marked as “N” when the corresponding security level has no direct or significant impact on the given security objective. The safeguards related to perimeter protection and the additive manufacturing zone have the greatest impact on maintaining all three

attributes, as they are responsible both for protecting information and technological resources and for ensuring continuity of the production process. The remaining protection levels focus mainly on ensuring the confidentiality and integrity of data and on reducing the risk of unauthorized access to infrastructure, technical documentation, and manufactured components. The obtained results confirm that effective protection of an additive manufacturing environment requires the use of complementary organizational, physical, and cyber-physical safeguards.

CONCLUSIONS

The analysis conducted showed that additive manufacturing systems used in the aerospace, space, and defense industries should be treated as complex cyber-physical environments requiring a comprehensive approach to security. Unlike conventional manufacturing technologies, additive manufacturing is based on intensive digital data processing carried out at many stages of product preparation, process planning, and production execution. As a result, both geometric data and technological data become key assets requiring protection against unauthorized access, modification, and loss.

The main result of the conducted research is the development of a multi-layer cyber-physical security model dedicated to additive manufacturing environments. The proposed approach includes three complementary security layers: the layer of preparation and processing of 3D geometric data, the layer of technological process data, and the physical layer of the production process. For each layer, key assets subject to protection, potential cybersecurity threats, and protective mechanisms were identified. The developed model enables a systematic analysis of vulnerabilities and security requirements throughout the digital chain of the additive manufacturing process.

The considerations also indicate that cybersecurity in additive manufacturing cannot be limited solely to the protection of geometric models. Technological process parameters, device configurations, simulation results, post-process procedures, and physical access to the production infrastructure may directly affect the quality, reliability, and operational safety of manufactured components. This is particularly important in aerospace and defense applications, where even minor modifications of process parameters may lead to deterioration of the mechanical properties of the product or limitation of its operational capabilities.

An additional result of the work is the extension of the physical protection model to include an analysis of protected assets, potential threats, the effects of their occurrence, and the corresponding protection mechanisms. This analysis is complemented by an assessment of the proposed security levels using the CIA model (Confidentiality, Integrity, Availability). The obtained results confirm that effective protection of an additive manufacturing environment requires the integration of organizational, physical, and cyber-physical

safeguards implemented at all stages of the production process.

Further research may focus on developing quantitative risk-assessment methods for additive manufacturing environments, integrating cybersecurity monitoring mechanisms with additive manufacturing devices, and using artificial intelligence methods to detect anomalies and protect technological data in cyber-physical production systems.

REFERENCES

1. Wohlers report 2022: 3D printing and additive manufacturing global state of the industry, Wohlers Associates, Fort Collins (Colo.), <https:// Wohlers Associates.com/>
2. ISO/ASTM 52900:2021 Additive manufacturing — General principles — Fundamentals and vocabulary, ISO/TC 261 Additive manufacturing.
3. Bong Kim D., Witherell P., Lipman R., and C. Feng S. Streamlining the additive manufacturing digital spectrum: A systems approach, *Addit. Manuf.*, 2015; 5: 20–30. <http://dx.doi.org/10.1016/j.addma.2014.10.004>
4. Kowalska N., Szczygiel P., Skrzyniarz M., Błasiak S. Effect of shells number and machining on selected properties of 3D-printed PLA samples, *POLIMERY* 2024; 69(3): 186–190.
5. Gibbons D.W., Ko H. Configuration Control for Additive Manufacturing, in *Proceedings of the 32nd Annual International Solid Freeform Fabrication Symposium*, Austin, Texas, 2021; 269–282. <http://dx.doi.org/10.26153/tsw/17554>
6. Wieczorowski, M., Kurkiewicz, A., Bigerelle, M., Pereira, A., Królczyk, G., Berkman, F., Gapinski, B., Determinants and Challenges of Metrology 5.0. In: Hryb, M., Zhou, J., Wieczorowski, M., Dostatni, E., Moncarz, P.D. (eds) *Advances in Manufacturing V. Manufacturing 2026. Lecture Notes in Mechanical Engineering*. Springer, Cham.
7. Loibl A., Manoharan T., and Nagarajah A. Procedure for the transfer of standards into machine-actionability, *Journal of Advanced Mechanical Design, Systems, and Manufacturing*, 2020; 14(2).
8. Paszkiewicz A., Budzik G., Przytuła M., Rączka D., Madera M., Kądziołka T., Application of cyber-physical systems for additive manufacturing of polymer products, *POLIMERY*, 2024; 69: 11–12, 651–656.
9. Um J., Park J., and Stroud I.A. Squashed-slice algorithm based on STEP-NC for multi-material and multi-directional additive processes, *Applied Sciences*, 2021; 11(18): 8292.
10. Woźniak J., Paszkiewicz A., Budzik G., Przeszlowski Ł., Kiełbicki M., Zimon D., Development of additive

- technologies in the light of the Industry 4.0 and Industry 5.0 conception in accordance with the IOE idea, *International Journal for Quality Research*, 2024; 18(2): 643–658.
11. Budzik G., Przeszlowski Ł., Paszkiewicz A., Lis T., Rączka D., Stępień-Załucka B., Gierula D., Burczy K., Surowaniec M., Strength of drone structural elements generated using artificial intelligence algorithms and manufactured from polymer materials using the MEX method, *POLIMERY*, 2026; 71(2): 103–108.
 12. Graves L. M. G., Lubell J., King W., and Yampolskiy M., Characteristic aspects of additive manufacturing security from security awareness perspectives, *IEEE Access*, 2019; 7: 103833–103853. <https://doi.org/10.1109/ACCESS.2019.2931738>
 13. Belikovetsky S., Yampolskiy M., Toh J., Gatlin J., and Elovici Y., Drowned – Cyber-Physical Attack with Additive Manufacturing, 11th USENIX Workshop on Offensive Technologies (WOOT 17), USENIX Association, 2017; 16, <https://www.usenix.org/conference/woot17/workshop-program/presentation/belikovetsky>
 14. Yampolskiy M., King W.E., Gatlin J., Belikovetsky S., Brown A., Skjellum A., and Elovici Y., Security of additive manufacturing: Attack taxonomy and survey, *Additive Manufacturing*, 2018; 21: 431–457.
 15. Budzik G., Przeszlowski Ł., Oleksy M., Załucki M., Modelling three-dimensional numerical objects using software based on AI algorithms - creative and intellectual rights, in: *Technological and Legal Aspects of AI in the City*, University of Rzeszów, Instituto Iberoamericano de Estudios Jurídicos (eds.) Fábio da Silva Veiga, Beata Stępień-Załucka, 2025; 12–23.
 16. Smaragdakis G., Matta I., Bestavros A. SEP: A stable election protocol for clustered heterogeneous wireless sensor networks. In: *Proc. 2nd Int. Workshop Sensor Actor Netw. Protocols Appl. (SANPA)*. Boston, MA, USA; 2004.
 17. Budzik G., Przytuła M., Paszkiewicz A., Cygnar M., Przeszlowski Ł., Dziubek T. Possibilities of automating the additive manufacturing process of material extrusion – MEX, *Technical Journal* 2024; 18(3): 480–485.