

International Journal of Production Research

ISSN: 0020-7543 (Print) 1366-588X (Online) Journal homepage: www.tandfonline.com/journals/tprs20

Streaming in metal additive manufacturing: a catalyst for secure distributed manufacturing

Moritz Kolter, Sebastian Dirks, Sven Scheres & Johannes Henrich Schleifenbaum

To cite this article: Moritz Kolter, Sebastian Dirks, Sven Scheres & Johannes Henrich Schleifenbaum (28 Feb 2025): Streaming in metal additive manufacturing: a catalyst for secure distributed manufacturing, International Journal of Production Research, DOI: 10.1080/00207543.2025.2471563

To link to this article: https://doi.org/10.1080/00207543.2025.2471563

© 2025 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.

Published online: 28 Feb 2025.

Submit your article to this journal

Article views: 864

View related articles

View Crossmark data

Citing articles: 3 View citing articles

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=tprs20

INTERNATIONAL JOURNAL OF PRODUCTION RESEARCH
https://doi.org/10.1080/00207543.2025.2471563

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

Streaming in metal additive manufacturing: a catalyst for secure distributed manufacturing

Moritz Kolter[a], Sebastian Dirks[a], Sven Scheres[b] and Johannes Henrich Schleifenbaum[a]

[a]Chair for Digital Additive Production, RWTH Aachen University, Aachen, Germany; [b]Laser Melting Innovations GmbH, Aachen, Germany

ABSTRACT

Distributed Manufacturing (DM) involves decentralised production facilities to increase flexibility, reduce costs, and enhance efficiency by bringing production closer to customers. Additive Manufacturing (AM) is a toolless production approach that promises to support DM by enabling the dispersion of production in decentralised facilities without relying on economies of scale. However, transferring manufacturing information, such as 3D models and parameters, across multiple local facilities exposes intellectual property (IP) to various threats, including manipulation and unauthorised production. To address these challenges, this work introduces a streaming protocol that securely distributes manufacturing information from the cloud to AM machines. The protocol defines a state machine that enables synchronisation between the cloud and an AM machine and a layerwise streaming sequence that protects the transmitted information. Additionally, the protocol controls how often a part can be printed. The feasibility of the protocol is demonstrated in a case study using Powder Bed Fusion of Metals as an exemplary AM technology. The case study shows that manufacturing information can be streamed parallel to the printing process while meeting hard real-time requirements. Finally, the contribution of the layerwise streaming concept to securing IP is discussed by four potential attack vectors, such as eavesdropping or data interception.

ARTICLE HISTORY
Received 22 July 2024
Accepted 18 February 2025

KEYWORDS
Additive manufacturing; powder bed fusion of metals with laser beam; AM supply chain; cybersecurity; streaming

SUSTAINABLE DEVELOPMENT GOALS
SDG 9: industry; innovation and infrastructure

1. Introduction

Additive Manufacturing (AM) has gained a lot of industrial interest over the last few years. Initially only used for prototyping, various AM technologies matured to a degree capable of producing parts that fulfil requirements for mass production (Gibson 2015). However, AM is still mainly used as a complement to traditional manufacturing because of high investment costs, high material prices, and low production rates. Nevertheless, changing business models drive the adoption of AM and shift the use of additive technologies from rapid prototyping to actual production parts (Savolainen and Collan 2020). Mass individualizations, digital warehousing, and decentralised digital supply chains are just a few examples of envisioned business models and supply chain configurations (González-Varona et al. 2020; Öberg, Shams, and Asnafi 2018; Savolainen and Collan 2020). Furthermore, current events, such as the COVID-19 pandemic (Tareq et al. 2021) and the containership 'Ever Given' blocking the Suez Canal (Lee and Wong 2021), have proven present supply chains to be vulnerable to disruptions fostering the adoption of AM to increase supply chain resilience via Distributed Manufacturing (DM) (Dwivedi, Srivastava, and Srivastava 2017; Ford and Despeisse 2016; Naghshineh and Carvalho 2022).

In conventional manufacturing, the driving rationale of economies of scale, e.g. to reduce the share of tooling costs per part, favours central production. In contrast, AM is driven by optimising the part performance or the supply chain itself (Kleer and Piller 2019). The benefits of AM lie in its toolless production approach and digital nature, e.g. allowing for individualised parts without additional tooling costs or DM without the need for multiple tools and related costs (Knofius et al. 2021). Moreover, central manufacturing often leads to lengthy and complex supply chains and, hence, to long lead times and high inventory costs. Using AM in DM, supply chains can shrink to local on-demand printing to reduce lead times and inventory costs (Sasson and Johnson 2016; Savolainen and Collan 2020). To realise local on-demand printing, the 3D model of the part to be printed needs to be digitally distributed to the decentral manufacturing facility. To minimise the transportation efforts without creating new warehouses, local facilities need to be close to the customer, which is in most cases only possible by outsourcing the manufacturing process from an

CONTACT Moritz Kolter moritz.kolter@dap.rwth-aachen.de Chair for Digital Additive Production, RWTH Aachen University, Campus-Boulevard 73, 52074 Aachen, Germany

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

© 2025 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

original equipment manufacturer (OEM) to an AM service provider. Relying on service providers is common in AM (Yampolskiy et al. 2014; Yampolskiy, Elovici, and Yung 2021) as it allows coping with uncertain and changing demands that exist for many use cases in AM, such as prototyping, spare parts, or wear parts (Achillas et al. 2015). Besides the benefits of DM using AM, it also bears cyber-security risks and loss of control of data (Sturm et al. 2017; Yampolskiy et al. 2018). There are multiple areas of vulnerability in the AM process chain, such as theft of technical data, manipulation of part quality, or the security and availability of AM equipment. Therefore, the information flow will become a critical success factor in DM but is not yet supported by adequate information and communication technology (ICT) (Naghshineh and Carvalho 2022). These ICT inadequacies resulting in legal and cyber-security issues are still barriers to adopting AM and envisaged business models relying on DM (Srai et al. 2016). A study from Yampolskiy et al. surveying 64 companies using AM reflects that finding (Yampolskiy, Elovici, and Yung 2021). Among the participating companies, 59% had no cyber-security mechanism at all, and those with AM security programmes mainly had no tailored approach. Only 4.1% of the surveyed companies had a dedicated AM security programme, even though the majority did outsource production to AM service providers and named theft of data and IP loss as critical issues. To this day, exchanging CAD Data, confidential designs, and manufacturing data relies on insecure e-mail communication. This implies that the following requirements are not yet sufficiently met:

(R1) Secure Data Transfer:

The 3D model must be secure in any data transfer and not be exposed to theft or manipulation.

(R2) Control of Production:

The owner of the 3D model – typically an OEM – shall control the number of parts being printed and permission of access to the 3D model.

To this end, a streaming protocol for laser-based AM is introduced in this paper. The protocol is designed to secure the file transfer (R1) from an OEM to an AM service provider and to preserve the OEM's control over the 3D model (R2). As a result, this work shall contribute to the demand for security and resilience in supply chains by providing ICT for DM in AM.

The remainder of the paper is structured as follows: the digital threat in AM and efforts to increase cyber-security and IP protection are discussed. Then, the streaming protocol is introduced, and its design is explained in detail. The feasibility is shown in a case study, and the implications of the streaming protocol are discussed. Lastly, a summary and an outlook on future research are given.

2. State of the art

This chapter highlights the digital threat in AM to illustrate the specific challenges for the design of the streaming protocol. Moreover, state-of-the-art cyber-security protection for AM is discussed to outline the specific research gap and potentially complementary solutions.

2.1. Digital threat in additive manufacturing

AM is a group of manufacturing technologies that produce parts by adding material layer by layer (ISO/ASTM 2021). Prior to printing, these layers are generated in a data preparation process called slicing, which involves taking the 3D model of the component and cutting it into layers of a specified height. Depending on the AM technology, the layers are subsequently processed, which may include generating an infill or setting process parameters, followed by creating a toolpath. Various data formats, as analysed in Qin et al. (2019) and Dirks, Collet, and Schleifenbaum (2022), exist to represent sliced data, which are mostly proprietary. In the additive printing process, the toolpath is then executed to manufacture the layers, which finally add up to the entire part. This process is entirely digital until the toolpath is executed during the physical printing phase (Gibson 2015).

Because of the digital nature of AM and its flexibility being a toolless manufacturing technique, the potential influence on supply chains has already been discussed from a strategic and business perspective (Kleer and Piller 2019; Öberg, Shams, and Asnafi 2018; Verboeket and Krikke 2019). DM of spare parts has been of particular interest to research as they tend to have small lot sizes and an uncertain and locally spread demand (Achillas et al. 2015; Khajavi, Holmström, and Partanen 2018; Knofius et al. 2021; Xu, Rodgers, and Guo 2021). A multitude of benefits have been encountered, such as shortened lead times through a reduction of logistical efforts (González-Varona et al. 2020) or increased customer welfare through price competition with central manufacturers (Kleer and Piller 2019). On the other side, however, Yampolskiy et al. identified multiple areas of vulnerability in the AM process chain, such as theft of technical data, manipulation of part quality, or the security and availability of AM equipment (Yampolskiy et al. 2018). They systematically analysed the literature, defined a taxonomy for attacks in AM, and identified attack targets in the AM process chain, which are discussed below.

Concerning the research goal of overcoming ITC inadequacies in DM, cyber-security risks related to file

transfer, such as theft or manipulation of the 3D model during the digital transfer to a local AM facility, are especially important. In case of theft through the service provider, the 3D model might be used to create different types of damages, such as disclosure of confidential data to competitors or loss of revenue by the production and marketing of an unauthorised entity (Yampolskiy et al. 2018). External adversaries are another cyber-security risk in the AM supply chain (Belikovetsky et al. 2017; Xu, Rodgers, and Guo 2021; Yampolskiy et al. 2014; Yampolskiy et al. 2018; Yampolskiy, Elovici, and Yung 2021). They might be interested in getting access to the IP, e.g. as part of industrial espionage. They could attack communication channels with different attack types, such as man-in-the-middle or eavesdropping (Yampolskiy et al. 2018). Besides theft, the manipulation of the 3D model is an attack target. It might cause quality issues or a wrong part, which needs to be scrapped, increasing lead time and overall production costs. Moreover, if the manipulation of the part is not detected, e.g. as a spare part in an aircraft, it might cause failure and is, therefore, a liability (Belikovetsky et al. 2017; Yampolskiy et al. 2018).

Beyond the cyber-security risk of manipulation, the transfer of the 3D model to a service provider also creates a loss of control of the production of the 3D model (Holland, Nigischer, and Stjepandic 2017; Yampolskiy et al. 2014). Despite an existing legal contract, the relationship between OEM and service provider is a question of trust. As soon as the 3D model is transferred to the service provider, the OEM loses control of how often the part is manufactured and who might get access to the 3D model. The service provider could produce and sell the part itself or illegally distribute copies of the digital model. Moreover, to take full advantage of DM, e.g. to minimise transportation costs, a widely spread customer base would require collaboration with many AM service providers, leading to a massive overhead in procurement for setting up contracts.

2.2. Cyber-security protection in additive manufacturing

Legal aspects such as IP protection (Ballardini, Flores Ituarte, and Pei 2018; Srai et al. 2016, 2020) and cyber-security risk (González-Varona et al. 2020) have been identified as barriers to adopting AM in DM. To this end, few studies have focused on providing solutions to overcome cyber-security issues and related legal aspects.

Gonzalez-Varona et al. have introduced a platform model that structures the information and economic flow for DM using AM and the transport for final party delivery (González-Varona et al. 2020). Legal aspects are covered by royalties paid to the design owners, and a secure file transfer addresses cyber-security. The transfer from the platform to the local manufacturer is done using Future Internet Ware (FIWARE), which is not specified in detail. The wording data exchange implies that the 3D model is shared, and the control is therefore assumed not to stay with the OEM.

Streaming as a remedy to secure data transfer in AM is investigated in literature (Baumann et al. 2017; Tiwari et al. 2021). Here, streaming is a mechanism by which data is sent continuously in real-time (Wu et al. 2001), e.g. if the data volume is too large to be stored or to be efficiently processed (Aggarwal 2007; Wu et al. 2001). Streaming architectures typically consist of a server that sends data and a client that receives data. The data is transferred via a continuous distribution service, primarily the Internet. A streaming protocol defines how the communication between the server and client works (Aggarwal 2007). Streaming protocols are characterised by the data format employed, the data sequence, and the synchronisation between the communicating entities.

Tiwari et al. introduced a protection mechanism against counterfeiting employing streaming. Custom anti-counterfeiting signatures are added to the 3D model before sending it to the local manufacturer (Tiwari et al. 2021). In the stream received, the manufacturer can verify the presence of a signature and, thus, the authenticity of the streaming. The signature is shared with the customer, who can check whether the file originates from a certified manufacturer. While this approach focuses on counterfeiting, it does not fully address file manipulation issues, as it only proves that the signature itself has not been manipulated. Moreover, a secure file transfer and possible attacks such as intercepting the design or eavesdropping are not solved from the design owner's perspective.

Baumann et al. introduced a streaming concept to ensure security in the AM supply chain (Baumann et al. 2017). Instead of transferring the 3D Model to the manufacturer, they stream the machine code directly to the 3D printer. Hence, the manufacturer never gains access to the 3D model, and control stays with the OEM. However, Baumann et al. also describe ways to circumvent their approach. The data streamed could be intercepted or retrieved from the memory of the 3D printer and used for unauthorised production. The approach is, thus, vulnerable to an external adversary intercepting the stream or the service provider retrieving data from the 3D printer. Despite protecting the 3D model, streaming without additional security measures does not fulfil the above-mentioned requirements for data transfer, as the number of printed parts cannot be controlled. Moreover, Baumann et al. limit their approach by considering g-code, the golden standard for only one AM technology,

i.e. material extrusion. However, g-code is not applicable to various industrially relevant AM technologies, such as powder bed fusion with laser beam of metals (PBF-LB\M) (Yampolskiy et al. 2018). This is caused by inefficient text-based storage and a lack of an information model for laser-based AM parameters, e.g. to control a laser.

In summary, different approaches have investigated the protection of digital IP and physical parts from counterfeiting along the AM process chain. However, protecting the 3D model and controlling the quantity produced when relying on an AM service provider is hardly covered or limited to material extrusion. This gap in understanding highlights the need for further research on the interface between OEMs and service providers, which offers protection for AM technologies used in DM.

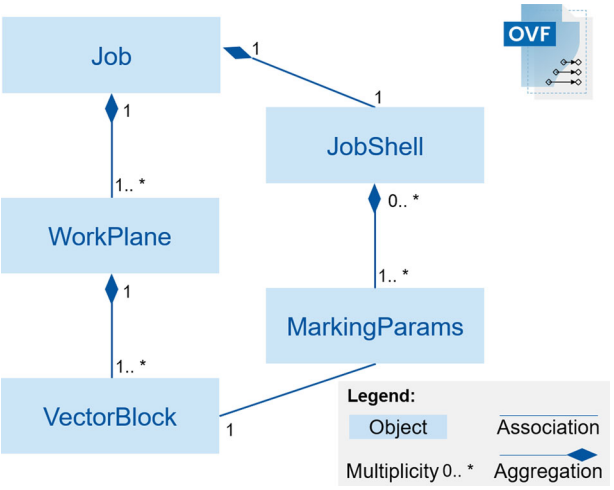


Figure 1. Class diagram of Open Vector Format (OVF) basic object model.

3. Streaming protocol

In this chapter, streaming is investigated as a potential solution to address the research gap identified in Section 2.2 and provide protection against the digital threats discussed in Section 2.1. The fundamental idea is to provide security by design for the 3D model. By streaming the sliced 2.5D data to print a part, the 3D model does not need to be shared with the service provider, and it is therefore protected. Building on the promising results of the streaming concept of Baumann et al. (2017), however, raises two unsolved research questions:

(RQ1) How can streaming be applied to more industrial-relevant AM technologies beyond material extrusion?

(RQ2) How can the streaming of AM manufacturing data be protected from circumvention to avoid unauthorized production?

Following the classical server-client architecture (Wu et al. 2001), we define a streaming protocol consisting of a state machine and a streaming sequence. The state machine synchronises the server and client and controls the communication, while the streaming sequence defines how to send the data for printing in a secure manner. Before explaining the state machine and streaming sequence in detail, we elaborate on the data format used as the foundation to ensure that both the server and client can understand and process the streamed data.

3.1. Data format

The AM printing process builds up layers sequentially; thus, the data sent to the machine to print a part is 2.5D (Bonnard, Hascoët, and Mognol 2019). For 2.5D data, there are only a few open data formats, while most AM machine manufacturers use their proprietary format (Bonnard, Hascoët, and Mognol 2019; Dirks, Collet, and Schleifenbaum 2022). The open formats, such as CLI or SLI, merely contain the vectors and the printing order, but not essential parameters, such as laser power or scanning speed. To this end, an open format containing the necessary information to print a part, the Open Vector Format (OVF), has been introduced by Dirks, Collet, and Schleifenbaum (2022). Moreover, OVF is more performant than existing data formats and well-structured. Therefore, it is suitable for streaming, as it easily allows splitting the data into single layers and transmitting large amounts of data efficiently (Dirks, Collet, and Schleifenbaum 2022). Hence, we decided to use OVF for streaming and enhance its capabilities in an open streaming protocol. Since the structure of OVF is important for the design of the streaming sequence, the most important components are described briefly.

The basic object model of OVF is depicted in Figure 1. In OVF, layers are called *work planes* and contain vectors in so-called *vector blocks*. The *vector blocks* contain the mathematical description and coordinates of the vectors to be printed, e.g. lines, curves, or circles. Each *vector block* is assigned to the corresponding *work plane* and has a key linked to the jobs *marking params* map, which defines the parameters for the printing process, e.g. laser power and scanning speed. To link the information needed for printing, the *job shell* holds global parameters, such as preheating temperature or job height, and has a map of *marking params*.

3.2. State machine

A state machine is a general approach to design and implement control structures in software systems, for

Table 1. State description and transitions of server.

State	Actions	Transition
Idle	Server is ready to stream	From *Abort* or *Streaming* if streaming or aborting is completed
Streaming	Server streams the OVF file as defined in the streaming sequence	From *Idle* to *Streaming* to start streaming, From *Waiting* or *Error* if server or machine error is resolved
Waiting	Server waits for the client, e.g. if the client is in *Error*	From *Streaming* in case of a client error
Error	Server tries to resolve the error	From *Streaming* or *Idle* in case of an internal server error
Abort	Streaming and, hence, the printing process is aborted	From *Waiting* or *Error* if an error on the server or the client side cannot be resolved

Table 2. State description and transitions of the client.

State	Actions	Transition
Idle	Client waits for the operator to be prepared for the build job	From *Error, Abort,* or *Streaming* if streaming is completed
Waiting for Job	Client ready for printing	From *Idle* after preparation
Streaming	Client request streaming of OVF file as defined in the streaming sequence	From *Waiting for Job* to *Streaming* to start streaming, From *Waiting* or *Error* if server or machine error is resolved
Waiting	Client waits for the server if the server is in *Error* state	From *Streaming,* if an error occurs on the server side
Error	Client tries to resolve the error or waits for the action of an operator (e.g. material refill)	From *Streaming* in case of an internal client error
Abort	Streaming and, hence, the printing process is aborted	From *Waiting* or *Error* if an error on the server or the client side cannot be resolved

instance, to handle faults or errors (ISO/IEC 2012). The state machine introduced here defines states for both server and client, as well as the transitions between the states. Actions and transitions of the state machine are defined in Table 1 and depicted in Figure 2 for the server and for the client in Table 2 and Figure 3, respectively. Both sides have an *Idle*, *Waiting*, *Error*, *Abort*, and *Streaming* state. The *Idle* state is the default state for the server and the client. An additional *Waiting for Job* state exists on the client side to signal that the client is ready to receive a build job. The client transitions from *Idle* to *Waiting for Job* after being set up by an operator. When a build job is available on the server and the client is in the *Waiting for Job* state, the server transitions to the *Streaming* state. The client follows by a transition into the *Streaming* state. If both server and client are in the *Streaming* state, the streaming sequence is executed (see Section 3.3). *Waiting*, *Error,* and *Abort* are states that cope with errors such as loss of connection or an internal server error. In case of an error occurrence, the respective side transitions to the *Error* state while the other side transitions to *Waiting*. Action is taken to resolve the error. Such errors could be the failure of hardware components, such as a broken laser controller or a blocked recoater. If the error is successfully resolved, both client and server change back to the *Streaming* state. Otherwise, if the error cannot be rectified, a transition from state *Error* to *Abort* is made. Subsequently, the server and the client abort the build job and return to *Idle*.

3.3. Streaming sequence

The streaming sequence has a section for initialisation, buffering, and streaming of the toolpath\vectors while printing. The streaming sequence is specified in the sequence diagram in Figure 4. The initialisation section sends general information to the machine to prepare the printing process. In OVF, such general information is stored in the job metadata of the *job shell* object, which is, therefore, sent first. The job metadata – e.g. number of work planes, part volume, and preheating temperature – allows the machine to prepare for the actual printing process. After the transmission of job metadata, a set of *work planes* that the client requests is built as a buffer. The buffer shall ensure that in case of delays in the streaming caused by network delays or temporary loss of connection, the AM machine does not need to

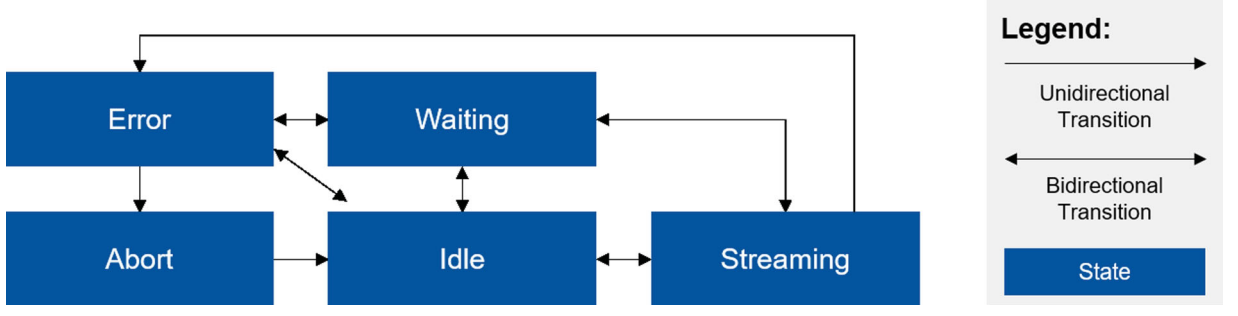


Figure 2. State machine of the server.

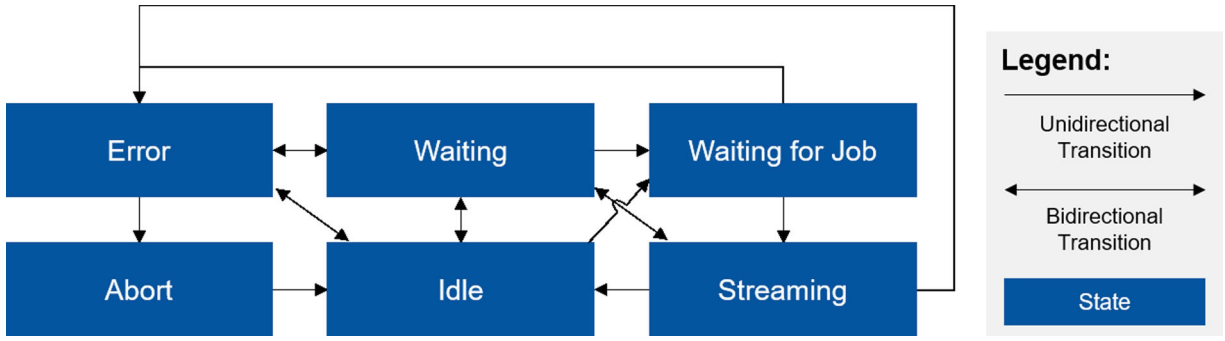


Figure 3. State machine of client.

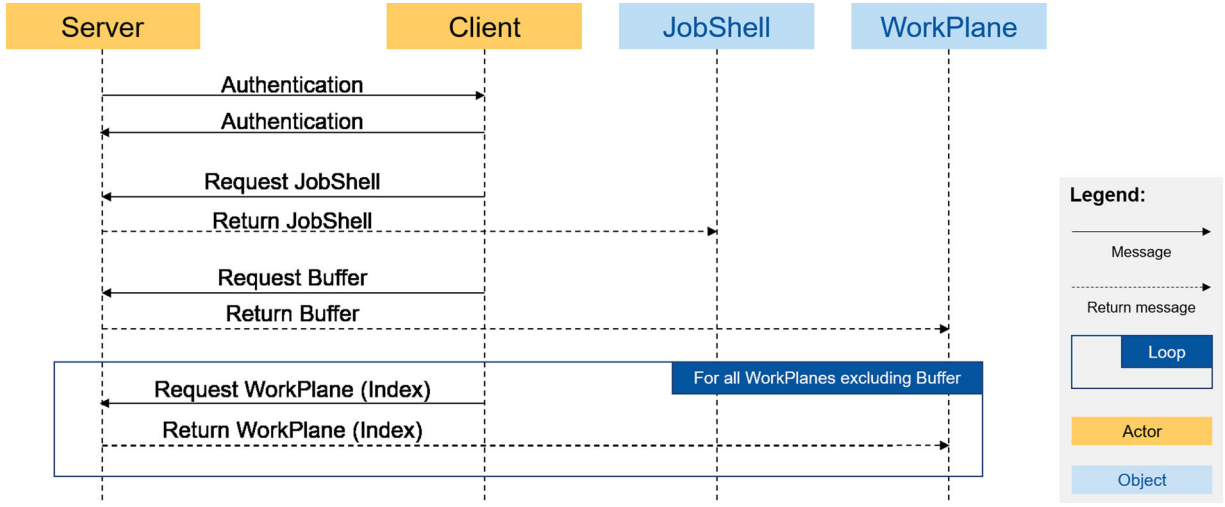


Figure 4. Sequence diagram of streaming protocol.

wait for the next layer and thus can keep printing at all times. This is important to ensure high part quality and machine productivity. The number of layers buffered is not defined in the protocol and might be set according to the expected network delay or a predefined safety margin. The buffer relaxes the real-time requirements to a soft real-time. Instead of requiring the maximum streaming time to be smaller than the layer print time, it is sufficient if the average streaming time is smaller. After receiving the buffer, the machine starts printing and requests a new layer whenever one is successfully printed. This process is repeated until all layers have been sent from the server to the client.

The rationale behind streaming 2.5D data directly to the machine is to never share the 3D model with the AM service provider that prints the part. This protects the 3D model from theft and, hence, protects the IP. Although the 2.5D data does not reveal the 3D model directly, it allows for the recreation of the physical part. Therefore, the layers streamed need to be protected as well. To protect the 2.5D data and to ensure that the part is only printed once the streaming server carries out the following measures:

- The job shell and work planes are encrypted so that only the target machine can read the streamed data, which protects against external adversaries.
- The key used for decryption is set up in a licencing system to ensure that the service provider does not make illegal copies. Beyond the key, the licence contains a counter for each work plane, which is set to one. After each access to the licence, the count is decremented so that the key can only be used once. Even if copies of the OVF objects containing the layer information are made, they cannot be read again after the printing process as the licence counter is zero.
- Work planes need to be sent in order, meaning only the subsequent layer is sent by the server as a mechanism to recognise external adversaries. Hence, the server only streams a work plane if the previous layer has been streamed immediately before.

- A work plane can only be sent once to avoid the work plane being requested and printed in parallel on another machine or from an external adversary.

4. Case study

The following case study discusses the technical feasibility of the streaming concept and the security achieved. Firstly, the technical feasibility is investigated based on a sample part. We consider the streaming feasible if the AM machine can successfully print the streamed part. On the one hand, this means that the streaming protocol provides the right data at the right time and, on the other hand, that the streaming works in real-time. Real-time can be specified as the streaming time per layer is shorter than the printing time. Secondly, to evaluate the scalability and robustness, the streaming test is carried out in one setup with a high network latency and one with a representative industrial build job. Thirdly, a threat model with four potential attack vectors is defined to assess the concept's cyber-security. The protection against those attack vectors is discussed regarding the specific implementation of the streaming sequence.

4.1. Implementation

OVF, the data format chosen for the streaming protocol, is based on Protocol Buffers (Protobuf), a cross-platform data format for the serialisation of structured data (Google LLC 2024). Therefore, we implemented the streaming protocol as Protobuf service definitions, which we published open-source (Kolter and Dirks 2023). There is a service definition that models the state machines and allows the exchange of the state of the client and server between each other as bi-directional streaming. This means that both server and client can always share their current state to trigger the other side to perform transitions between states, e.g. to start streaming or to react in case of an error. The streaming of the OVF objects is defined as a unidirectional service, as this data only needs to be transferred from the server to the client. Protobuf services can be transmitted over the internet by remote procedure calls (RPC). An RPC is a communication protocol designed for client-server interaction, enabling different platforms and systems to communicate with each other in an interoperable manner. We chose the popular gRPC as a specific RPC implementation for this case study. gRPC runs on top of standard internet protocols such as HTTP/3 and supports multiple programming languages and platforms, making it suitable for building distributed systems. The server is implemented in C# as an ASP.NET web service streaming data using gRPC following the streaming sequence and its additional security rules. The client needs to be tailored to the specific AM machine and was implemented together with the machine manufacturer Laser Melting Innovations[1] for an Alpha 140.

The security measures are implemented with the widely used ISO/IEC 9594-8, Transport Layer Security (TLS), and Advanced Encryption Standard (AES) standards. X.509 certificates specified in ISO/IEC 9594-8 are used for server and client authentication. Furthermore, the X.509 certificates are used to secure the communication channel used for streaming with TLS 1.3. The payload of the communication, specifically the OVF objects *job shell* and *work planes*, are encrypted using a library from the IT-security firm WIBU-Systems following AES-256. Beyond the functionality of encrypting using AES, the library can create secure licences containing a key and a counter, which is used to control how often the part can be printed.

4.2. Technical feasibility

A sample part was designed to test the streaming protocol's capabilities. The part was oriented and supported using the software Autodesk Netfabb Premium 2024. A rendering of the part is depicted in Figure 5. The part contains different geometrical features and requires support structures like typical parts produced by PBF-LB\M. The sample part was sliced into layers and exported as an OVF file with standard parameters for the material 1.4404. The OVF file was uploaded to the server and streamed to the Alpha 140 according to the abovementioned implementation. The buffer size was set to one as the machine and server are both located in Germany, and only minor network delays were expected.

The sample part was successfully printed using the streaming protocol in the setup mentioned above. A picture of the part produced can be seen in Figure 6, and the streaming time per layer can be seen in Figure 7. All layers were successfully streamed and printed. The different heights of the different features of the sample parts indicated that the layer information changed each layer and that the layers were printed in the correct order. The average streaming time per layer for all 516 layers was 168 ms with a minimum of 35 ms and a maximum of 983 ms. Just the recoating time, in which the material for the next layer is applied, takes about 6000 ms and is around factor six bigger than the maximum time measured. The real-time requirement of streaming faster than printing is therefore met, even without considering the laser exposure time typically taking a few minutes.

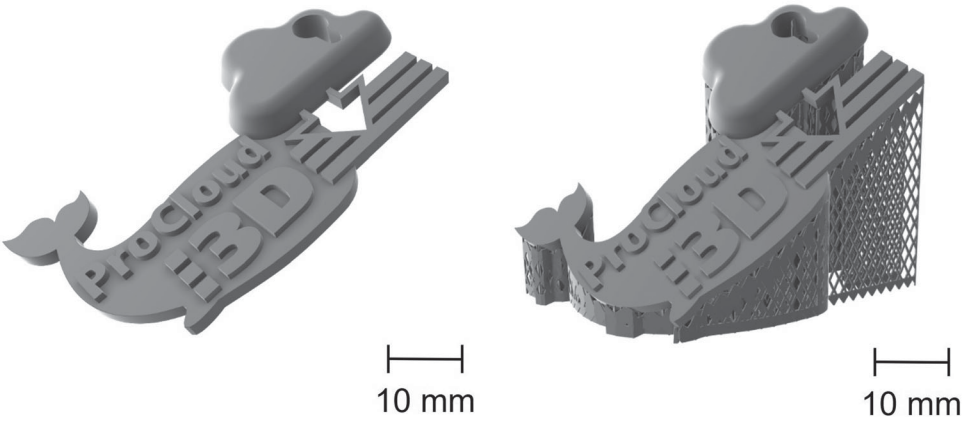


Figure 5. Rendering of sample part without support (left) and with support (right).

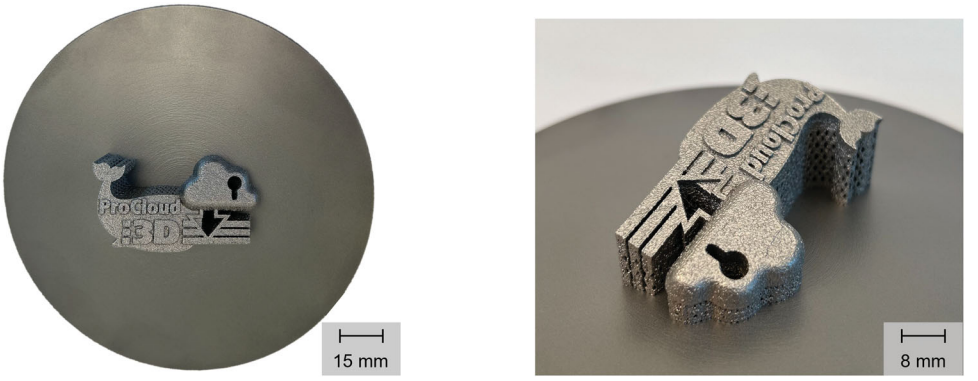


Figure 6. Printed part using the streaming protocol. (Left) Top view, (right): detail view on printed part.

4.3. Scalability and robustness

In the first test, the buffer was set to only one layer as the server and the client were both located in Germany. However, in DM, the server and the client are likely to be distanced far apart from each other. To validate the robustness of the streaming protocol, we streamed the OVF file in the aforementioned setup, but we just changed the client's location to China. Moreover, there might be other delays in the network besides the propagation delay caused by the distance of the communication points depending on the traffic and the available bandwidth. Therefore, we streamed the sample part five times, obtaining an average streaming time per layer of

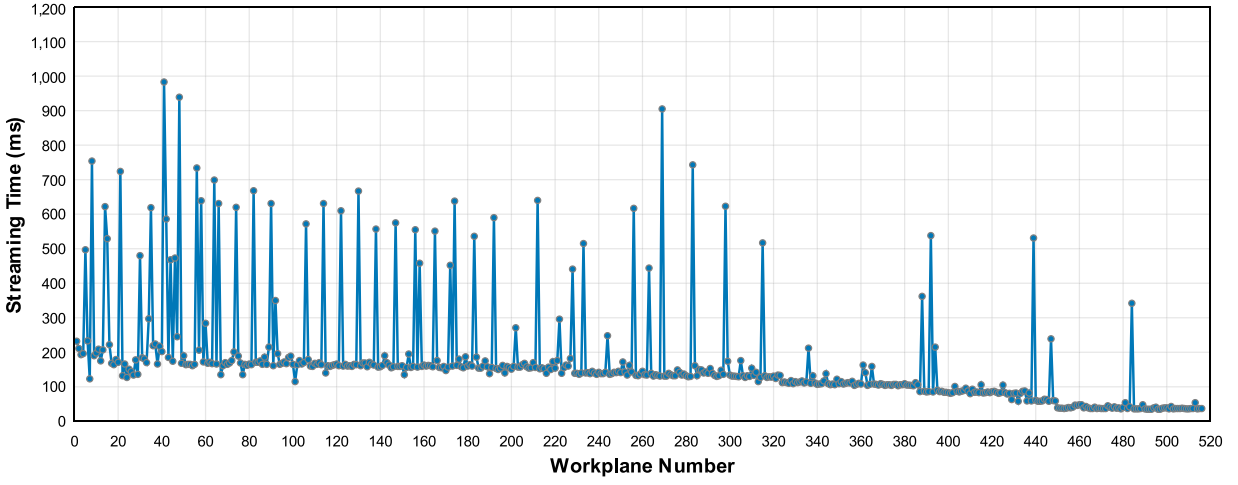


Figure 7. Streaming time per layer during printing of the sample part.

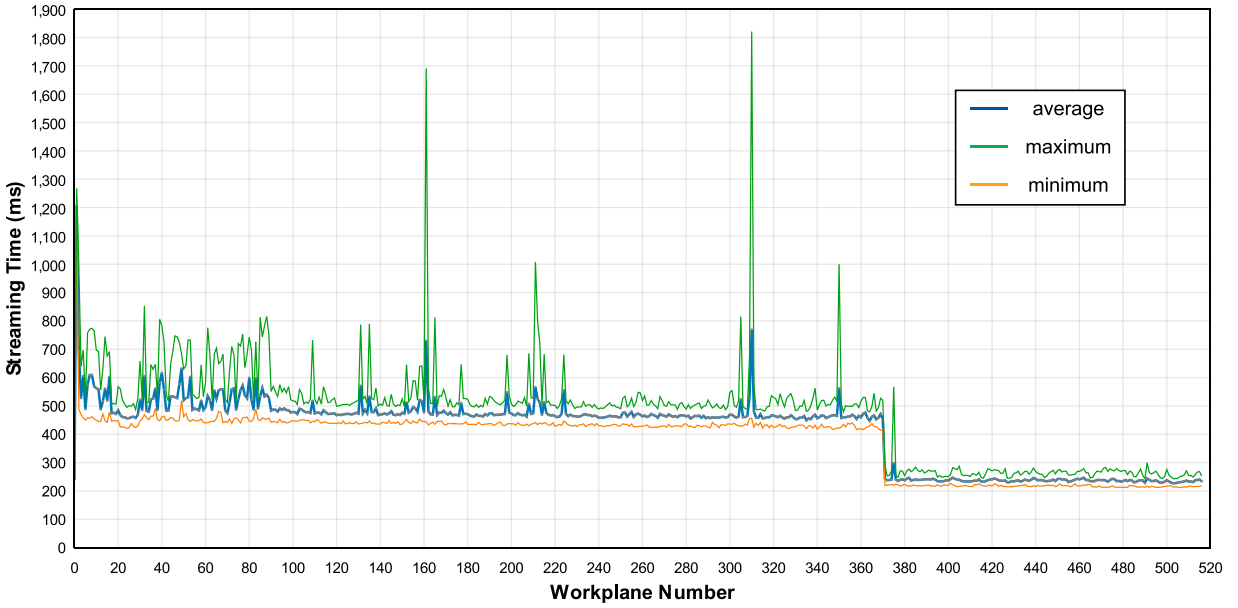


Figure 8. Streaming time in far distanced server client setup.

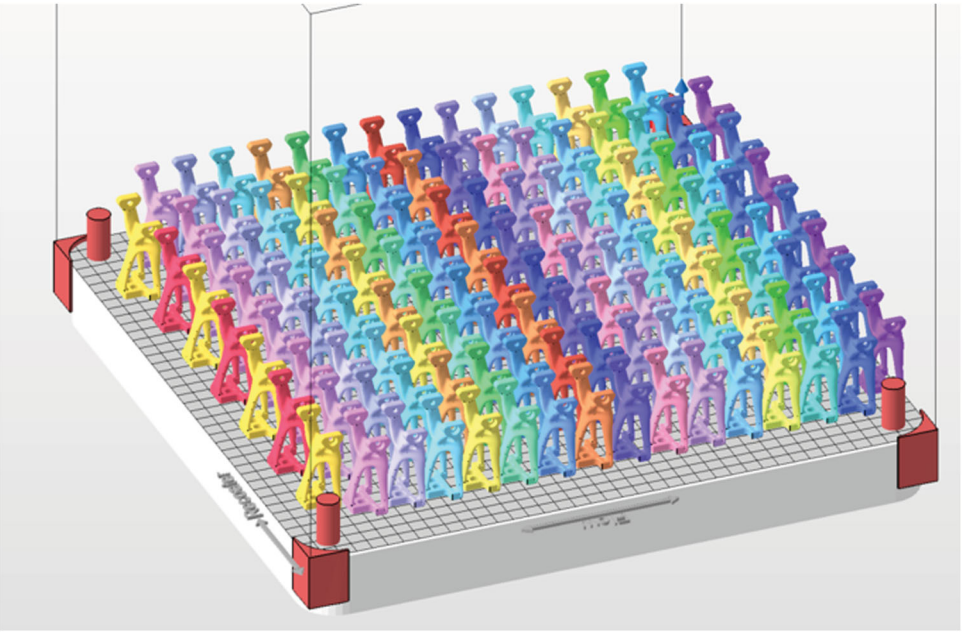


Figure 9. Densley nested build job for an EOS M290.

417 ms. Figure 8 shows the average, minimal, and maximal streaming time for each layer. A streaming time of around 200 to 500 ms can be observed for most layers, with outliers peaking up to 1821 ms. Comparing the average streaming time to the initial setup of streaming at a short distance, the network delay is around 250 ms higher. Looking deeper into the streaming times, neither the average streaming time nor outliers, e.g. caused by jitter on the network or high traffic reducing the bandwidth, are critical to meet the real-time requirement of streaming faster than printing.

AM is used to produce a wide variety of parts, and in DM, different sizes of printers will probably be used. Hence, we also investigated the scalability of the streaming protocol with another sample part in a highly packed build job nested for a widely used EOS M290. The nested build job with 127 parts can be seen in Figure 9, and the streaming time per layer for five test runs is shown in Figure 10. Obtaining an average streaming time of 199 ms and a maximum of 2302 ms also indicates that streaming is faster than the printing process. The recoating time alone of an EOS M290 is 10.000 ms, which is around four

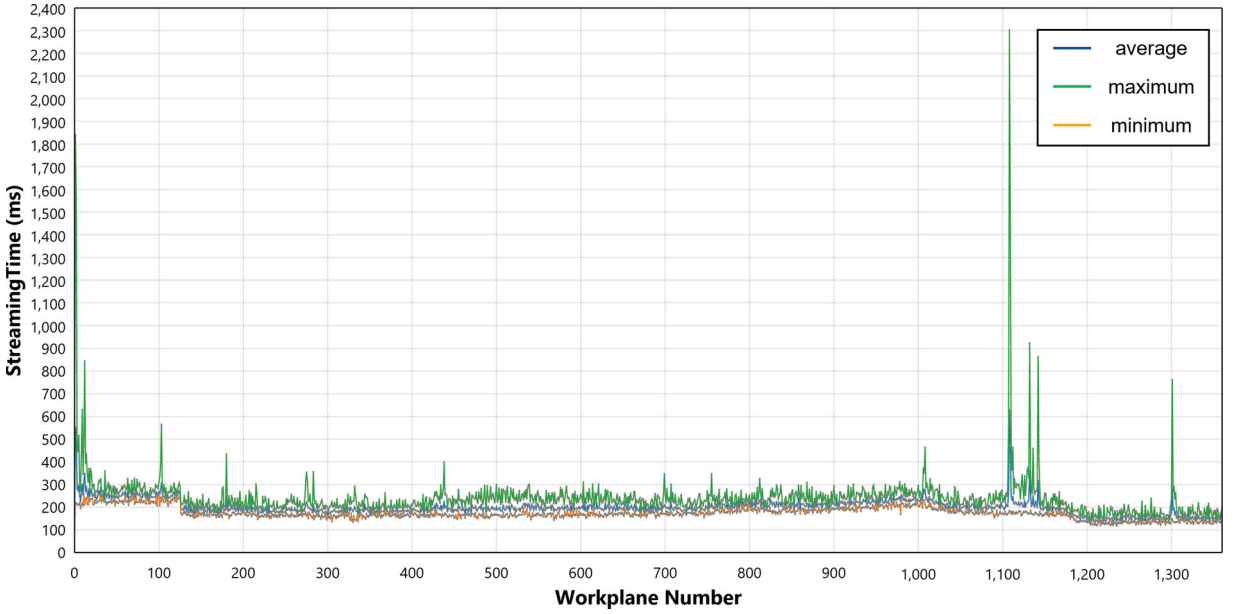


Figure 10. Streaming times for densely packed build job on an EOS M290.

times longer than the maximum streaming time in all five test runs. Consequently, real-time capability is also given for the highly packed build job.

4.4. Threat model and security

We assess four potential attack vectors (AV), as described below and depicted in Figure 11, to structure the cybersecurity analysis of the introduced approach:

(AV1) Eavesdropping: An adversary could eavesdrop on communication between server and client, for instance, using a man-in-the-middle attack.

(AV2) Interception: An adversary could reroute the communication to an unauthorised machine, fake or steal a certificate in a spoofing attack.

(AV3) Memory Dump: By dumping the memory from the machine an adversary could obtain the OVF objects.

(AV4) Software Manipulation: Manipulating the machine software to obtain data in the printing process.

The security of file transfer (R1) is addressed in the protocol's design and is considered by the selection of OVF as the data format and gRPC as the remote procedure to stream the data over the internet. The combination of Protobuf, the serialisation technology used in OVF, and gRPC allows the use of state-of-the-art authentication and encryption using X.509 certificates and TLS (Mrabet et al. 2020). This avoids eavesdropping (AV1) by encrypting the communication channel. However, attack vectors (AV2) might bypass the encryption of the communication channel, e.g. by exploiting bugs in

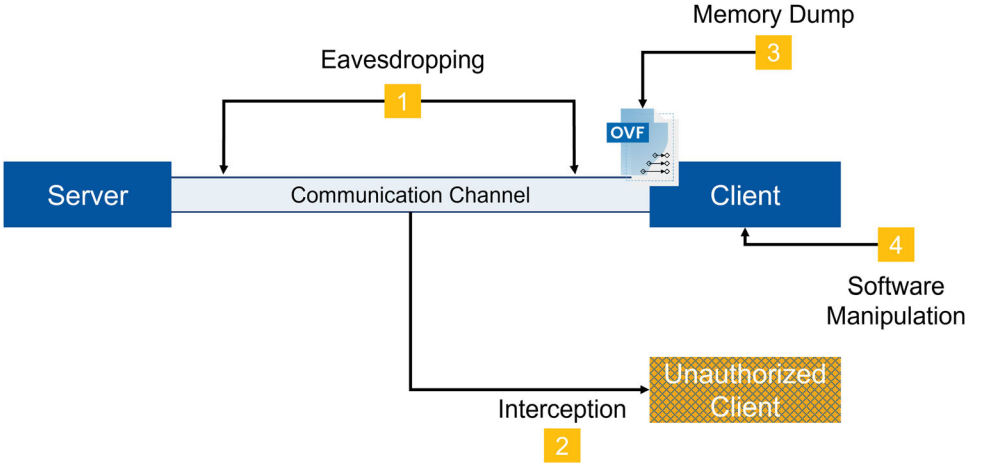


Figure 11. Potential attack vectors on the streaming approach.

the implementation or spoofing. Here comes the second encryption of the OVF itself into play. Even if the communication is intercepted, the data is protected by symmetric AES encryption.

The 3D model is never shared with the service provider as the first measure to guarantee the control of production (R2) for the OEM at all times. This is realised by streaming the parametrised toolpath directly to the AM service provider's machine in a layerwise manner. Therefore, the service provider will never gain access to the file of the 3D model and thus cannot share it with unauthorised third parties. Moreover, streaming the data layerwise and adding encryption to OVF objects in a licence system allows controlling that a part is only printed once. Even if the service provider tries to dump the memory of the machine (AV3) to obtain the OVF, it is still encrypted and hence protected. Furthermore, the counter in the licence prevents that certificate from being abused to decrypt the OVF. However, at some point in time, the machine needs to decrypt the *work plane* to print it. This opens the possibility for a new attack vector. By manipulating the machine software (AV4), a copy of the decrypted information could be made and used to create an illegal copy. This could undermine the proposed security concept. However, manipulation of the machine software is unlikely as machine software is typically encrypted. Moreover, detailed knowledge of the underlying software architecture is required to make the specific changes required for such a cyberattack.

4.5. Discussion

In the case study, the feasibility of streaming for PBF-LB\M has been demonstrated as we could successfully produce a part using the implemented streaming protocol. The dependability of the approach in terms of a stable print process without interruption is addressed by the buffer included in the protocol. The streaming test in a far distanced sever to client network setup has proven the real-time capabilities of the approach for possible DM scenarios with an OEM located in Germany and a customer in China. Looking at a minimum of 35 ms and a maximum of 2302 ms streaming time per layer, it appears that the delays are of higher influence than the streaming time caused by the package size of the stream itself. However, even without considering the entire printing time of a layer, the recoating time alone is sufficient to stream in real time. In comparison, following a g-code-based approach, as in Baumann et al. (2017), would be less performant. Figure 12 shows the data size for each layer as an OVF file and as a g-code file. In total, the data size grows from 2.96 to 25.1 gigabytes. On average, a layer's data size is 8.4 times bigger in g-code. The g-code data volume is more likely to exhaust memory resources on embedded real-time controllers of AM machines. Streaming times using a hypothetical g-code-based streaming data encoding will be greater than factor 8.4 due to additional overhead of parsing and decimal to binary conversion of the numerical data. G-code encoding thus introduces significant challenges to guarantee real-time requirements and causes additional hardware costs due to higher memory and computational requirements.

Recovery scenarios in case of errors, such as the loss of connection or an error of the machine, outline a further avenue for research. Simple network issues, such as collision on the communication channel or packet loss are handled by Transmission Control Protocol/Internet Protocol (TCP/IP), the underlying communication layer used by gRPC. However, if the control unit of the machine crashes, a recovery strategy has to be in place to resume the build process. The rule of sending each layer only once might interfere with a recovery procedure on the machine if the information in the memory is lost. This could be solved by relaxing the rule and allowing single layers to be sent twice to support the machine's recovery process.

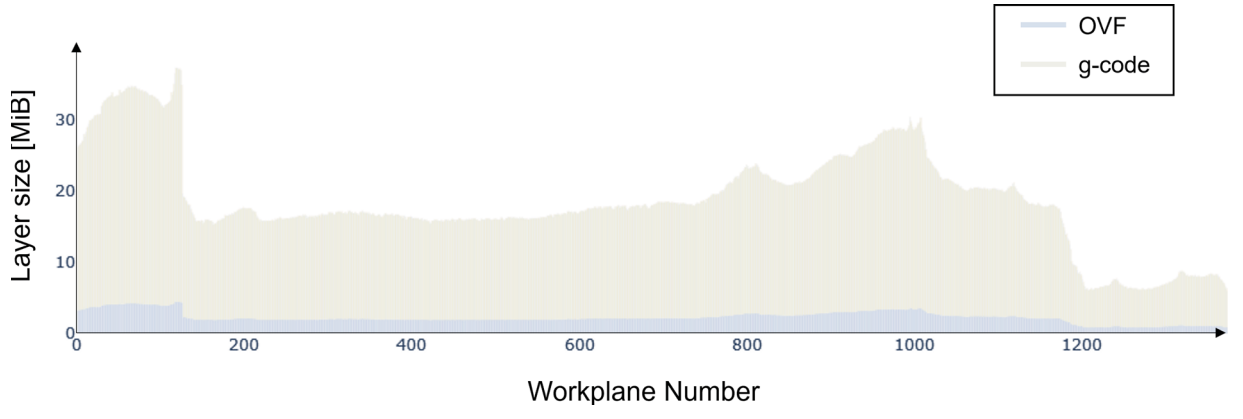


Figure 12. Data size per layer of OVF compared to g-code.

The usage of OVF as an integral part of the streaming protocol ensures its interoperability with the PBF-LB\M (and other vector-based) systems. Furthermore, the information presented in the streamed OVF objects is sufficient and ordered following the timely procedure of a PBF-LB\M printing process. OVF is built on Protobuf, a cross-platform serialisation technology that supports a multitude of different programming languages. Moreover, OVF is open-source and extendable, which also applies to gRPC to the same extent. For instance, the server could be written in Python and the client in C#, still operating on the exact same streaming protocol presented. No widely used standard exists for the representation of 2.5D manufacturing data in AM. However, OVF allows for easy adoption by various machine vendors. In regard to the research question (RQ1), OVF as data presentation and the structuring of streaming in the streaming sequence introduced demonstrate a viable application of streaming to PBF-LB\M. The feasibility of the approach to other AM technologies is not specifically tested in the case study. However, due to the similarity in the operating principle, an application to powder bed fusion with a laser beam of polymers or laser-based vat photopolymerization is likely. Despite different materials processed, all these technologies are laser-based and produce parts by joining material layerwise using vector commands across the layers. Thus, the research presented contributes to applying streaming to a wider range of AM technologies.

The case study assesses different attack vectors, showing the effectiveness of the security measures introduced. It, therefore, provides specific rules and mechanisms to address the unmet requirements for a secure data transfer in DM using AM. More specifically, sending a layer precisely once and encrypting the layer presents a solution to avoid circumvention of the streaming principle. Protecting against data interception and memory dumps is given and avoids unauthorised production. The security measures, therefore, contribute to the body of cybersecurity research in AM by answering the research question (RQ2). Compared to Baumann et al. (2017), the additional semantics of the introduced streaming protocol allow for an increase in cybersecurity. Due to the object-oriented structure of OVF, layers are clearly defined sections in the file. This enables layerwise encryption in the licence system and allows controlling the layer count and order. This way, the data is never shared in a single data transmission. Also, only single layers are decrypted at a specific moment in time. Intercepting or dumping data, even if encryption is breached, thus only results in the disclosure of a small portion of the data. The prevention of circumvention, as enhancement to the state of the art, in terms of data interception and a memory dump, thus also results in the selection of OVF as a payload in the streaming protocol.

In summary, the introduced streaming protocol is a concept that promises to overcome ICT inadequacies in DM and to enable innovative business models and resilient supply chains using AM. Typically, a service provider is involved to take over the printing process close to the point of use. This introduces the potential risk of reverse engineering, which may be accomplished using a 3D scanner, for instance. This risk is inherent to the outsourcing of production. Nevertheless, compared to obtaining access to the 3D model, it significantly increases the effort of counterfeiting and making illegal part copies, resulting in reduced appeal. To this end, combining the introduced streaming protocol with other approaches, such as Abdullah et al. (2022), Tiwari et al. (2021), might be worthwhile to increase the protection against product piracy even further. Future research could delve into adding functionalities to embed physical signatures into the printed part (Tiwari et al. 2021), for instance, to avoid the production of identical parts without a licence agreement.

The quality control in DM using AM with the introduced streaming concept itself is an aspect for further investigation because the service provider does not have information about the printed parts. Therefore, it will be hard to assess the quality beyond checking for obvious defects at the part's surface. To this end, a feedback loop from the printer back to the server similar to the approach in Abdullah et al. (2022) could be added. Data from process monitoring could be streamed back to the cloud, and the OEM could verify the quality of the printed parts. Often, the production does not stop at printing but requires post processing such as heat treatment or surface finishing. Thus, in addition to the quality after printing, the handling of post processing must be researched. It could be investigated whether streaming is practicable for other production technologies to also control post processing in DM.

5. Conclusion

The potential benefits of DM using AM, such as supply chain resilience and increased customer welfare by reduced costs, are widely known. However, the lack of adequate ITC causes cyber-security issues in DM, particularly in terms of securing data transfer and keeping control over production. This work demonstrates that streaming is a potential remedy. The case study shows that streaming manufacturing information layerwise and during the running printing process is feasible. Real-time capabilities are given for a single-part build job and for a highly packed build job with multiple parts.

Furthermore, also large distances between the server and client respectively, the service provider do not compromise the feasibility of the streaming protocol. Moreover, it shows that outsourcing in AM can work without the need to share a 3D model or process parameters with the service provider. In addition, the streaming protocol with the embedded security features also controls the number of parts being produced. This could be an important innovation to the current data flow in DM, overcoming IP security hurdles. Therefore, the work contributes to overcoming ICT inadequacies in DM. Further improvements lie in combining the presented approach with other methodologies against product piracy and in providing methods to assess quality in DM without knowledge of the printed part.

Note

1. https://www.lm-innovations.com/de-de/ (accessed 01.02. 2024).

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This research was funded by the Bundesministerium für Bildung und Forschung (Federal Ministry for Education and Research of Germany) in the Project ProCloud3D [grant number 02P18X011]. Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC-2023 Internet of Production – [grant number 390621612].

Notes on contributors



Moritz Kolter is the chief engineer for digital product and production and PhD candidate at the Chair for Digital Additive Production at RWTH Aachen University. Prior to pursuing his PhD, he received an MSc in mechanical engineering from the Technical University of Munich. Besides academia, he gained industry experience in the automotive industry working for BMW in different positions related to additive manufacturing. In his research, he uses streaming technology to solve cyber-security issues in additive manufacturing.



Sebastian Dirks is a PhD candidate at the Chair for Digital Additive Production at RWTH Aachen University. Prior to pursuing his PhD, he received a MSc in automation engineering and gained industrial experience at Bosch. In his research, he investigates how digital tools can contribute to additive manufacturing efficiencies. His publications contribute to additive manufacturing span from an open data format to advanced machine emulation concepts for cost calculation for laser-based additive manufacturing.



Sven Scheres is a software engineer at LMI – Laser Melting Innovations GmbH, also known as LMI, in Aachen. With his background in mechanical engineering and automation technology, he contributes to LMIs goal of facilitating access to affordable additive manufacturing machines. His research and development activities focus on new machine concepts and digital innovation for metal additive manufacturing.



Johannes Henrich Schleifenbaum is a full professor at RWTH Aachen University, heading the chair for Digital Additive Production since its foundation in 2016. In the realm of additive manufacturing, his research encompasses various aspects of digital manufacturing, including process optimisation, material development, and the integration of digital technologies to enhance production efficiency. With a strong background in mechanical engineering and material sciences, Prof. Schleifenbaum has significantly contributed to the advancement of additive manufacturing technologies, focusing on their industrial applications and digital transformation. He has published more than 200 papers in leading journals and conferences, sharing his insights and findings with the global scientific community.

References

Abdullah, A. M., L. Chenang, Chen Kan, and Wenmeng Tian. 2022. "Securing Cyber-Physical Additive Manufacturing Systems by in-Situ Process Authentication Using Streamline Video Analysis." *Journal of Manufacturing Systems* 62:429–440. https://doi.org/10.1016/j.jmsy.2021.12.007.

Achillas, C., D. Aidonis, E. Iakovou, M. Thymianidis, and D. Tzetzis. 2015. "A Methodological Framework for the Inclusion of Modern Additive Manufacturing into the Production Portfolio of a Focused Factory." *Journal of Manufacturing Systems* 37:328–339. https://doi.org/10.1016/j.jmsy.2014.07.014.

Aggarwal, C. C. 2007. "An Introduction to Data Streams." In *Data Streams: Models and Algorithms*, edited by C. C. Aggarwal, 1–8. Boston, MA: Springer US.

Ballardini, R. M., I. Flores Ituarte, and E. Pei. 2018. "Printing Spare Parts through Additive Manufacturing: Legal and Digital Business Challenges." *Journal of Manufacturing Technology Management* 29 (6): 958–982. https://doi.org/10.1108/JMTM-12-2017-0270.

Baumann, F. W., T. Ludwig, N. Darwin Abele, S. Hoffmann, and D. Roller. 2017. "Model-data Streaming for Additive Manufacturing Securing Intellectual Property." *Smart and Sustainable Manufacturing Systems* 1 (1): 20160011. https://doi.org/10.1520/SSMS20160011.

Belikovetsky, S., M. Yampolskiy, J. Toh, J. Gatlin, and Y. Elovici. 2017. Dr0wned – cyber-physical attack with additive manufacturing. *11th USENIX Workshop on Offensive Technologies (WOOT 17)*.

Bonnard, R., J.-Y. Hascoët, and P. Mognol. 2019. "Data Model for Additive Manufacturing Digital Thread: State of the art and Perspectives." *International Journal of Computer Integrated Manufacturing* 32 (12): 1170–1191. https://doi.org/10.1080/0951192X.2019.1690681.

Dirks, S., A. Collet, and J. H. Schleifenbaum. 2022. "Open Vector Format for Laser-Based Computer-Aided Manufacturing." In *Progress in Additive Manufacturing 2020*, edited by N. Shamsaei, and M. Seifi, 117–130. West Conshohocken, PA: ASTM International.

Dwivedi, G., S. K. Srivastava, and R. K. Srivastava. 2017. "Analysis of Barriers to Implement Additive Manufacturing Technology in the Indian Automotive Sector." *International Journal of Physical Distribution & Logistics Management* 47 (10): 972-991. https://doi.org/10.1108/IJPDLM-07-2017-0222.

Ford, S., and M. Despeisse. 2016. "Additive Manufacturing and Sustainability: An Exploratory Study of the Advantages and Challenges." *Journal of Cleaner Production* 137:1573–1587. https://doi.org/10.1016/j.jclepro.2016.04.150.

Gibson, I. 2015. *Additive Manufacturing Technologies: 3D Printing, Rapid Prototyping, and Direct Digital Manufacturing. Springer EBook Collection Engineering*. 2nd ed. New York, NY: Springer New York.

González-Varona, J. M., D. Poza, F. Acebes, F. Villafáñez, J. Pajares, and A. López-Paredes. 2020. "New Business Models for Sustainable Spare Parts Logistics: A Case Study." *Sustainability* 12 (8): 3071. https://doi.org/10.3390/su12083071.

Google LLC. 2024. Https://protobuf.Dev/ Protocol buffers documentation. Accessed January 31, 2024.

Holland, M., C. Nigischer, and J. Stjepandic. 2017. "Copyright protection in additive manufacturing with blockchain approach." In *Transdisciplinary Engineering: Proceedings of the 24th ISPE Inc. International Conference on Transdisciplinary Engineering*, July 10–14, 2017, edited by C. H. Chen. Amsterdam: IOS Press Incorporated.

ISO/ASTM. 2021. *Additive Manufacturing – General Principles – Fundamentals and Vocabulary*. 52900th ed. West Conshohocken, PA: ASTM International. Last modified 2021. https://doi.org/10.1520/F3177-21.

ISO/IEC. 2012. "Information Technology – Object Management Group Unified Modeling Language (omg uml)." Last modified 2012. https://www.iso.org/standard/52854.html.

Khajavi, S. H., J. Holmström, and J. Partanen. 2018. "Additive Manufacturing in the Spare Parts Supply Chain: Hub Configuration and Technology Maturity." *Rapid Prototyping Journal* 24 (7): 1178–1192. https://doi.org/10.1108/RPJ-03-2017-0052.

Kleer, R., and F. T. Piller. 2019. "Local Manufacturing and Structural Shifts in Competition: Market Dynamics of Additive Manufacturing." *International Journal of Production Economics* 216:23–34. https://doi.org/10.1016/j.ijpe.2019.04.019.

Knofius, N., M. C. van der Heijden, A. Sleptchenko, and W. H. M. Zijm. 2021. "Improving Effectiveness of Spare Parts Supply by Additive Manufacturing as Dual Sourcing Option." *OR Spectrum* 43 (1): 189–221. https://doi.org/10.1007/s00291-020-00608-7.

Kolter, M., and S. H. G. Dirks. 2023. *Streaming Service Definition for Open Vector Format Objects; 1.0*. RWTH Aachen University. DOI: 10.18154/RWTH-2023-01469

Lee, J. M., and E. Y. Wong. 2021. "Suez Canal Blockage: An Analysis of Legal Impact, Risks and Liabilities to the Global Supply Chain." *MATEC Web of Conferences* 339:1019. https://doi.org/10.1051/matecconf/202133901019.

Mrabet, H., S. Belguith, A. Alhomoud, and A. Jemai. 2020. "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis." *Sensors (Basel, Switzerland)* 20 (13): 3625. https://doi.org/10.3390/s20133625.

Naghshineh, B., and H. Carvalho. 2022. "The Implications of Additive Manufacturing Technology Adoption for Supply Chain Resilience: A Systematic Search and Review." *International Journal of Production Economics* 247:108387. https://doi.org/10.1016/j.ijpe.2021.108387.

Öberg, C., Tawfiq Shams, and Nader Asnafi. 2018. "Additive Manufacturing and Business Models: Current Knowledge and Missing Perspectives." *Technology Innovation Management Review* 8:15–33. https://doi.org/10.22215/timreview/1162.

Qin, Y., Q. Qi, P. J. Scott, and X. Jiang. 2019. "Status, Comparison, and Future of the Representations of Additive Manufacturing Data." *Computer-Aided Design* 111:44–64. https://doi.org/10.1016/j.cad.2019.02.004.

Sasson, A., and J. C. Johnson. 2016. "The 3D Printing Order: Variability, Supercenters and Supply Chain Reconfigurations." *International Journal of Physical Distribution & Logistics Management* 46:82–94. https://doi.org/10.1108/IJPDLM-10-2015-0257.

Savolainen, J., and M. Collan. 2020. "How Additive Manufacturing Technology Changes Business Models? – Review of Literature." *Additive Manufacturing* 32:101070. https://doi.org/10.1016/j.addma.2020.101070.

Srai, J. S., G. Graham, P. Hennelly, W. Phillips, D. Kapletia, and H. Lorentz. 2020. "Distributed Manufacturing: A New Form of Localised Production?" *International Journal of Operations & Production Management* 40 (6): 697–727. https://doi.org/10.1108/IJOPM-08-2019-0600.

Srai, J. S., M. Kumar, G. Graham, W. Phillips, J. Tooze, S. Ford, P. Beecher, B. Raj, M. Gregory, M. K. Tiwari, et al. 2016. "Distributed Manufacturing: Scope, Challenges and Opportunities." *International Journal of Production Research* 54 (23): 6917–6935. https://doi.org/10.1080/00207543.2016.1192302.

Sturm, L. D., C. B. Williams, J. A. Camelio, J. White, and R. Parker. 2017. "Cyber-physical Vulnerabilities in Additive Manufacturing Systems: A Case Study Attack on the.STL File with Human Subjects." *Journal of Manufacturing Systems* 44:154–164. https://doi.org/10.1016/j.jmsy.2017.05.007.

Tareq, M. S., Tanzilur Rahman, M. Hossain, and P. Dorrington. 2021. "Additive Manufacturing and the COVID-19 Challenges: An In-Depth Study." *Journal of Manufacturing Systems* 60:787–798. https://doi.org/10.1016/j.jmsy.2020.12.021.

Tiwari, A., E. J. Villasenor, N. Gupta, N. Reddy, R. Karri, and S. T. S. Bukkapatnam. 2021. "Protection against Counterfeiting Attacks in 3D Printing by Streaming Signature-Embedded Manufacturing Process Instructions." In *Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security*, edited by M. Yampolskiy, Y. Elovici, and M. Yung, 11–21. New York, NY: ACM.

Verboeket, V., and H. Krikke. 2019. "The Disruptive Impact of Additive Manufacturing on Supply Chains: A Literature Study, Conceptual Framework and Research Agenda."

Computers in Industry 111:91–107. https://doi.org/10.1016/j.compind.2019.07.003.

Wu, D., Y. T. Hou, W. Zhu, Y.-Q. Zhang, and J. M. Peha. 2001. "Streaming Video Over the Internet: Approaches and Directions." *IEEE Transactions on Circuits and Systems for Video Technology* 11 (3): 282–300. https://doi.org/10.1109/76.911156.

Xu, X., M. D. Rodgers, and W. G. Guo. 2021. "Hybrid Simulation Models for Spare Parts Supply Chain Considering 3D Printing Capabilities." *Journal of Manufacturing Systems* 59:272–282. https://doi.org/10.1016/j.jmsy.2021.02.018.

Yampolskiy, M., T. R. Andel, J. T. McDonald, W. B. Glisson, and A. Yasinsac. 2014. "Intellectual Property Protection in Additive Layer Manufacturing." In *Proceedings of the 4th Program Protection and Reverse Engineering Workshop*, edited by M. D. Preda, and J. T. McDonald, 1–9. New York, NY: ACM.

Yampolskiy, M., Y. Elovici, and M. Yung, eds. 2021. *Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security*. New York, NY: ACM.

Yampolskiy, M., W. E. King, J. Gatlin, S. Belikovetsky, A. Brown, A. Skjellum, and Y. Elovici. 2018. "Security of Additive Manufacturing: Attack Taxonomy and Survey." *Additive Manufacturing* 21:431–457. https://doi.org/10.1016/j.addma.2018.03.015.