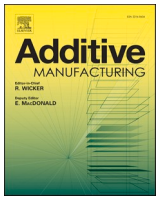
Additive Manufacturing 46 (2021) 102029

Contents lists available at ScienceDirect

Additive Manufacturing

journal homepage: www.elsevier.com/locate/addma



Research Paper

Sabotaging metal additive manufacturing: Powder delivery system manipulation and material-dependent effects

L. Graves [a], W.E. King [f], P. Carrion [b,d], S. Shao [b,d], N. Shamsaei [b,d], M. Yampolskiy [c,d,e,*]

[a] School of Computing, University of South Alabama, Mobile, AL 36688, USA
[b] Department of Mechanical Engineering, Auburn University, Auburn, AL 36849, USA
[c] Department of Computer Science and Software Engineering, Auburn University, Auburn, AL 36849, USA
[d] National Center for Additive Manufacturing Excellence (NCAME), Auburn University, Auburn, AL 36849, USA
[e] Auburn Cyber Research Center (ACRC), Auburn University, Auburn, AL 36849, USA
[f] The Barnes Global Advisors

ARTICLE INFO

Keywords:
Additive Manufacturing
Powder Bed Fusion
Security
Tampering
Sabotage
Safety

ABSTRACT

Additive Manufacturing (AM) is a direct digital manufacturing technology increasingly used to manufacture functional parts for military and civilian applications. As AM becomes more integral to national security and economic prosperity, it also becomes an attractive cyber-physical attack target. In this paper, we focus on attacks aiming to sabotage metal parts produced using *Powder Bed Fusion* (PBF), a metal AM process used to manufacture near net shaped parts for safety critical systems. Specifically, we focus on the *Powder Delivery System* (PDS), an integral PBF subsystem. In our examination, we adopt the attacker's perspective, identify possible manipulations which can be used individually or in combination to degrade part mechanical properties. We experimentally evaluate the impact of a selected manipulation on part fatigue life. Destructive testing on two different types of stainless steel specimens, 17–4PH and 316 L, confirmed effectiveness of this attack and revealed material-dependent impacts while non-destructive testing illustrated the difficulty in attack detection. Based on our analysis and experimental evaluation, we conclude that the investigated attacks have the potential to be effective against complex geometry parts such as those used in military and civilian systems while remaining undetected.

1. Introduction

Additive Manufacturing (AM) is increasingly used in both military and civilian applications due to various advantages such as reducing lead times and material waste, enabling remote spare part manufacturing, and realizing complex shape fabrication [1–3]. A well-established use of AM is the fuel injection nozzle used in the General Electric Leading Edge Aviation Propulsion (LEAP) jet engine [4]. Other examples include the Main Oxidizer Valve (MOV) body in the Space X Falcon 9 rocket and the SuperDraco Engine Chamber in their Dragon Version 2 vehicle [5]. Additionally, the U.S. Army has demonstrated a 3D printed grenade launched from a 3D printed grenade launcher [6], while the U.S. Navy has flown metal flight critical parts in naval aircraft and has an implementation plan to use AM to provide just-in-time manufacturing [7,8].

These initiatives create an environment in which national security and economic prosperity increasingly depend on the reliability of AM technology. Unfortunately, history has demonstrated that each new frontier in technology becomes the next security frontier as well. At the same time the new technology introduces new functionality, it also introduces considerations not addressed by already established security approaches. Such is the case with AM, a manufacturing technology heavily reliant on digital input files and digital control systems with minimal human intervention [9,10]. Identified AM security issues have included technical data theft, illegal part manufacturing, and cyber-physical sabotage attacks [11].

These cyber-physical attacks originate in the cyber domain, causing impacts in the physical domain through a complex causal chain of effect propagation [12,13]. The attacks can target manufactured parts, and by extension any system into which they are integrated, the AM machine, or the manufacturing environment [14]. Possible impacts of such an attack are not limited solely to physical damage but can also expose various parties along the AM workflow to financial and criminal liability [15].

* Corresponding author at: Department of Computer Science and Software Engineering, Auburn University, Auburn, AL 36849, USA.
E-mail address: mark.yampolskiy@auburn.edu (M. Yampolskiy).

https://doi.org/10.1016/j.addma.2021.102029
Received 13 December 2020; Received in revised form 16 April 2021; Accepted 30 April 2021
Available online 2 June 2021

While no attacks on real-world AM machines have been reported, several researchers have demonstrated potential attacks and possible impacts. In one case, the *dr0wned* study, Belikovetsky et al. [16] demonstrated a complete attack chain while sabotaging a drone propeller blade. The attack chain included a cyber compromise of the manufacturing environment, targeted alteration of the digital design file, and premature failure of the AM part. The sabotaged propeller came apart mid-flight resulting in the destruction of the drone and its payload. While *dr0wned* was limited to a plastic part, it demonstrates the potential for sabotaging metal parts and thus the need to investigate metal AM attacks. To date, *dr0wned* remains the only publicly-available complete sabotage attack with AM, i.e., ranging from initial compromise of an AM environment up to destruction of the system in which the sabotaged 3D-printed part was installed. Furthermore, as we will discuss in Section 2.1 and summarize in Table 1, attention to sabotage of metal AM has been lacking—despite the role that metal AM parts play in safety-critical systems.

1.2. Threat model

Through this study, we examine one of the most popular methods of metal AM used for near-net shape part manufacturing [17–19], *Powder Bed Fusion* (PBF). Specifically, we examine possible sabotage attacks facilitated through a compromised *Powder Delivery System* (PDS) which is an essential component of a PBF machine. For our threat model, we assume that the PBF machine is compromised by a common attack such as malicious firmware installation. The ability to compromise firmware even in highly secure industrial settings has been demonstrated by real world attacks such as Stuxnet [20] and provides the adversary with complete control over the cyber controlled process parameters, as has been demonstrated with desktop 3D printers [21,22]. We further assume the adversary's target is part quality degradation which is achieved by modifying the part's mechanical properties. The fatigue failure of additively manufactured metallic parts predominantly initiate from volumetric defects (such as pores and lack-of-fusion defects) under machine surface condition and from surface roughness under as-built surface condition. Therefore, to achieve the adversarial goal, the defects seeded by the sabotage need to be more severe by the typical volumetric and surface defects common in AM metallic materials. From this basis, we proceed to investigate how the goal of modified mechanical properties can be accomplished by manipulating the PDS, an essential sub-system which has yet to be studied from the security perspective.

Table 1
AM Sabotage attacks in the research literature (only publications whose end-goal is sabotage are listed).

Publication	AM Process	Outline
Xiao [21]	FDM, Plastics	Increased nozzle temperature affects a 3D printed part's form
Sturm et al. [25]	FDM, Plastics	Voids randomly inserted in the STL affect tensile strength
Yampolskiy et al. [26]	PBF, Metals	Identified PBF process parameters that can be used in sabotage
Zeltmann et al. [27]	FDM, Plastics	Substituting structural for support material affects tensile strength
Pope et al. [28]	PBF, Metals	Network communication timing can affect part quality
Belikovetsky et al. [16]	FDM, Plastics	Targeted STL modification reduces fatigue life; first complete attack
Moore et al. [22]	FDM, Plastics	Changing the filament extrusion rate affects a 3D printed part's form
Slaughter et al. [29]	PBF, Metals	Indirect sabotage via manipulated in-situ IR thermography
Ranabhat et al. [30]	SL, Composite	Optimizing sabotage to minimize the probability of detection

FDM - Fused Deposition Modeling; PBF - Powder Bed Fusion; SL - Sheet Lamination

Targeting the PDS is motivated by an assumption about adversarial goals. While the main goal is to sabotage a part's function, a typical secondary objective is for the malware to remain undetected for as long as possible to maximize the damage (as was the case with Stuxnet). While the PDS is essential for normal PBF operation, we believe it is easily overlooked and would escape scrutiny longer than more critical subsystems. Our assumption is grounded in the fact that there are literally 100 s of ways to sabotage PBF. However, there are parameters that will be under the intensive scrutiny almost immediately after defected parts are detected – such as the laser-related parameters like power density, scanning speed, or hatch distance. The PDS-related parameters are likely to be investigated only after many other possible manipulations are ruled out. Furthermore, Stuxnet demonstrated an effective strategy to prolong the time between discovery of a problem and identification of its cause: attack is not permanent but triggered by a set of conditions, and during the attack's manipulation prerecorded sensor information is replayed to the monitoring software. With this strategy, a defender is forced to rely on external measurements which only occasionally will provide indicators pointing to the true source of an attack.

The research presented in this paper targets multiple research communities, predominantly AM and Security, and requires expertise in both fields. To address this, some sections contain information that is necessary background for one community which might be considered common knowledge in the other. This paper is structured as follows. In Section 2 we discuss state of the art, addressing needs of different communities. In Section 2.1, we cover related work in AM security and AM sabotage attacks; this section provides a grounding for the wider AM community, while AM Security experts will likely be familiar with the presented research. We then provide background information on PBF in Section 2.2; this section informs Cyber-Security experts who might be not familiar with this AM process. We present our analysis identifying PDS-enabled attacks in section 3. We present an experimental evaluation of a selected attack in Section 4. We conclude this paper with a brief overview.

2. State of the art

In this section, we first present the related work on AM Security. The target audience is both AM and Cyber-Security experts which are not familiar with the research on AM sabotage. Then we provide a brief introduction into both PBF and its essential component under investigation in this paper, PDS. The target audience are Cyber-Security experts who might not be familiar with the subject; AM experts might want to skip this part of the section.

2.1. Related work

The ability to compromise AM equipment has already been demonstrated in the research literature. Moore et al. [23] analyzed popular open-source software that is used with and open-source firmware that is installed on desktop 3D printers. Based on their analysis, authors list numerous vulnerabilities that can be used to hack both. Do et al. [24] hijacked a wireless network protocol used to communicate with a desktop 3D printer, and demonstrated ability to use it for canceling a print job in progress and to submitting an entirely new job. Belikovetsky et al. [16] employed the e-mail spear phishing attack to gain a remote access to a computer used in 3D printing.

The majority of AM sabotage attacks (summarized in Table 1) have been demonstrated on fused deposition modeling (FDM), an AM process broadly used with polymers. Sturm et al. [25] randomly inserted voids in 3D object design defined in.STL file. Authors experimentally verified that this attack can degrade tensile strength of a manufactured part. Zeltmann et al. [27], using a dual extrusion desktop 3D printer, substituted parts of the 3D printed object with the support material extruded through a second nozzle. Also this attack led to the degradation

of a part's tensile strength. Belikovetsky et al. [16] tailored modifications of 3D printed propeller design to decrease a part's fatigue life. Authors also demonstrated that this atack can lead to the destruction of a system in which such part is installed (in the paper, a quadcopter UAV). Xiao [21] adjusted desktop 3D printer firmware to provide false temperature readings, while Moore et al. [22] integrated in the 3D printer firmware a factor by which the amount of extruded filament is modified. Both attacks resulted in geometrical distortions of the 3D part. Chen et al. [31] and Gupta et al. [32] proposed a category of.STL file modification that, if a part was printed with a wrong orientation, would result in geometrical distortions. Ranabhat et al. [30] presented an optimisation solution for composite material AM parts. Authors showed how the deviation from the original design can be minimized, while still achieving the stated degree of a part's performance.

Of the research addressing AM-related sabotage attacks, only a few papers have focused on metal AM. Yampolskiy et al. [26] performed an analysis to identify which manufacturing parameters could degrade part mechanical properties. Among the identified parameters, which corresponded with the critical performance parameters identified by Frazier et al. [33], were build direction, scanning strategy, scanning speed, heat source energy, and environmental conditions in the build chamber. Pope et al. [28] identified manipulations of network communication timing and of the power supply as possible means to sabotage a part during manufacture. Slaughter et al. [29] examined possible manipulations of in-situ InfraRed (IR) thermography quality control systems and demonstrated feasibility of the manipulations on a PBF machine. Ilie et al. [34] demonstrated that modifications to laser power and exposure time could be used to create predictable failure points in their work on customizing PBF part mechanical properties. While their research was focused on part design and not security, it is possible to see how these modifications could be used in attacks to induce targeted premature failure.

A framework for analyzing attacks on or with AM was devised by Yampolskiy et al. [14]. This framework is used and examined further in Section 3.1. In their analysis, Yampolskiy et al. [35] showed that, while it is possible to impose the same framework on other manufacturing technologies, there remain significant differences in AM security as opposed to Subtractive Manufacturing (SM) security. The AM versus SM security differences were further examined by Graves et al. [36] using a technology adoption security awareness cycle comprised of three perspectives —exposure, evaluation, and implementation. The authors identified differences arising from the unique AM attack targets and methods, the flexible and shifting AM workflow roles and boundaries, and the distinct AM security cost, benefit, and liability weighting. Graves et al. [36] concluded that addressing the AM security posture required specific domain expertise and that inheriting SM security was insufficient.

2.2. Background: PBF and its PDS sub-system

Powder Bed Fusion is one of the most popular metal AM methods [17–19]. In the PBF process, a thin layer of powder, usually metal or polymer, is distributed across a build plate. Once the layer has been uniformly spread, a laser or electron beam melts the powder particles to form the next layer of the additively manufactured object. The entire process is then repeated until all layers of the design file have been completed.

A variety of methods have been developed to deliver powder to and distribute it across a build plate. The powder delivery system can include but is not limited to powder cells, pistons, conveyor belts, sliders, rollers, and rakes [37,38,33,39,19]. The components of a specific PDS are machine dependent. Two common PDS configurations, the powder cell and the hopper, are depicted in Fig. 1(a) and (b), respectively. The remainder of this paper refers to powder cell and hopper configurations when discussing the PDS.

With the powder cell PDS, the fresh powder cell (left) is located adjacent to the build chamber cell (right). As the part is manufactured, the build plate is lowered a sufficient distance to accommodate the next layer while the powder cell is raised to produce the required dose to build that layer. With the hopper PDS, the powder is stored above the build chamber in a tank referred to as a "hopper." The hopper releases a predetermined dose which is then spread across the build chamber.

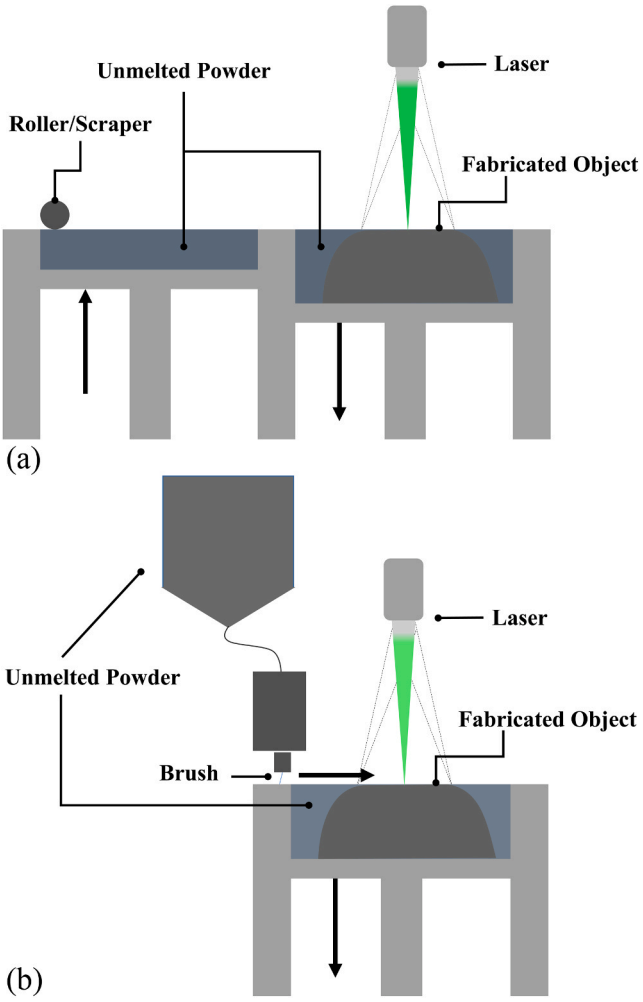


Fig. 1. Examples of powder delivery systems (PDS).

PBF requires a uniform deposition of the powder [17,18]. In the depicted powder cell configuration, a roller/scraper is employed to distribute the powder. In this PDS, the scrapper spreads the material while the roller provides compaction. The roller spins in a counter-rotating manner for consistency and evenness. In the depicted hopper configuration, the deposited dose is spread across the build chamber using a brush or scrapper. Some systems add vibration mechanisms to prevent powder agglomeration and attachment to the roller/scrapper [40,17,41,42] or brush/scrapper [43], to assist in compaction [44], and to facilitate powder fluidity [17]. The uniform deposition of the powder ensures the layer thickness is consistent, the layer surface is even, and the layer distance from the heat source is maintained.

3. Identifying PDS-enabled attacks

In this section we identify sabotage attacks that can be conducted with PDS sub-system. In Section 3.1 we first introduce an analytical approach that is taken. It is based on a framework introduced originally for the analysis of successful attack; we show how it can also be used for the preparation of attacks. The analysis starts then in Section 3.2 with

the identification of defects that can be intentionally seeded by the PDS manipulations. Then in Section 3.3 we identify *individual manipulations* of a PDS that can be conducted (i.e., changes of a single parameter while all other are fixed) and establish correlation between defects and individual manipulations. Building upon the individual manipulations that can be used as a means for sabotage attacks, in Section 3.4 we introduce a concept of *compound manipulations* – an approach that can increase attack effectiveness. We conclude our analysis in Section 3.5 by discussing ability to target parts via direct or indirect attacks.

3.1. Analytical approach

The framework we use to analyze the PDS sabotage attack was introduced by Yampolskiy et al. [11,14] and is depicted in Fig. 2. The attack analysis framework, from left to right, is composed of *attack vectors*, *attack methods*, and *targets* [11]. *Attack methods* are semantically identical manipulations that can originate from various compromisable elements in the AM process [11]. The framework uses the *attack methods* construct since various combinations of manipulations in conjunction with different compromised elements can achieve the same modification. One example of an attack method would be part geometry modification which can eventually impact fit and form or mechanical properties. Part geometry can be modified through STL file manipulations, toolpath command alterations, and changing individual actuator signals. The *attack targets* are defined as the intersection between the adversarial goals and objectives and the achievable effects that result from the attack methods [11].

Our PDS attack analysis begins with the target, traversing the framework from right to left, in a manner similar to how an adversary thinks. We start with the adversarial goal of functional part degradation. After the goal is identified, the adversary determines the achievable effects that could cause the desired part function degradation. In our scenario, the effects are those defects producible by the PDS. We examine the possible PDS induced defects in Section 3.2. Depending on the situation, the defects can lead to part degradation sufficient enough to satisfy the goal.

We explore the possible PDS manipulations which can generate defects in Sections 3.3 and 3.4. In Section 3.3, we identify *individual manipulations* where all other process parameters are fixed at their expected values and only one manipulation is applied to the build. In Section 3.4, we examine *compound manipulations*, such as intra- and inter-layer manipulations, as well as multiple type manipulations. The intra-layer manipulations can effect different parts of a single layer. The inter-layer manipulations impact adjacent layers. The multiple type manipulations can be of various types in arbitrary combinations producing unique impacts.

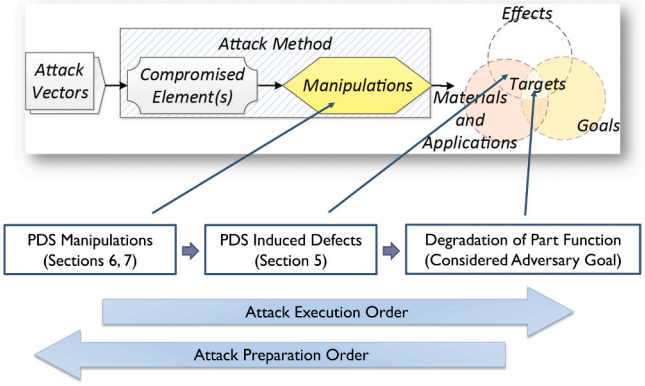


Fig. 2. Framework used in this paper for attack identification (derived from [11]). Traversing elements of this framework from left to right provides the order in which an attack is executed. To identify and prepare an attack, the framework is traversed by an adversary in the opposite direction.

Once the adversary has identified the desired manipulations, the attacker's next step would be to discern which elements to compromise and then determine which attack vectors to use. In this paper, we assume under our threat model that the AM machine is already compromised and the attacker has unfettered access and complete control of the system. Our assumptions of compromise and unfettered access and control are justified based on the AM attacks discussed or demonstrated in the security research literature [16,25,24,21,22,29,23] and investigations into security flaws and exploitation, such as a recent United States Government Accountability Office (GAO) report where testers were able to take control of and operate cyber-physical weapons systems undetected [45]. The GAO investigation identified and exploited vulnerabilities which are common in many industrial environments [46,47,45].

3.2. PDS-generated defects

In AM part manufacturing, there is a distinction between flaws and defects. Flaws are either within an acceptable threshold or can be remedied with post-processing; defects are fatal flaws which cannot be remediated [18]. The impacts described in this section can range from a flaw to a defect, based on the degree of deviation, the interaction with other process parameters, and required part-specific characteristics. All defects described below have the potential for degrading part mechanical properties.

3.2.1. Layer-related defects

Layer properties can be examined based on layer thickness, compaction, and uniformity [19,18,48,44]. Manipulation of these properties can lead to defects in a manufactured part.

3.2.1.1. Layer thickness. Layer thickness impacts not only the part geometry and feature detail but also material properties through the amount of powder available for melting and the distance between the surfaces of the current and prior layer. We distinguish between two cases of layer thickness defects, one in which the layer surface is level and one where it is angular.

In the level layer instance, the layer can be either thicker or thinner than designed (see Fig. 3a). Too thick layers experience an incomplete melting of the powder which results in delamination and produces internal porosity and rough external surfaces [18,19]. Rough external surfaces in turn serve as fracture initiation points, impacting part strength. Furthermore, the melt pool behavior will vary from that anticipated in the design as the temperature in the part will differ from expectations. Where the layer is too thick, the heat sink effect is impacted by the additional powder which interrupts the heat conductivity from the adjacent layer. An additional impact from a too thick layer would include incomplete part geometry formation.

Where the layer is too thin, the heat source will impact the prior layer, causing melting of the prior layer's unmelted powder or a re-melt of prior deposition, both of which will alter part geometry and degrade part mechanical properties [18,19]. Similarly, the layer will experience melt pool turbulence. Melt pool turbulence can result in vaporization of alloys with lower melting points and in keyholes generating voids in the part. It can also cause the molten metal to pull from the pool boundaries which in turn can lead to intra-layer delamination between the adjacent scan tracks.

In the angular layer instance (see Fig. 3b), the layer thickness rises in a gradient manner from a height h_0 to its final height h_n or decreases in a similar manner. In an extreme case, h_0 (or h_n) can be 0 which would mean that it initiates (or ends) at the surface of the prior layer. Although angular layer behavior does not appear to have been studied to our knowledge, it can be reasonably argued that the melt pool will display impacts similar to the level layer instances. In this case, the melt pool behavior is dependent on the layer thickness at the point of laser impingement. The thickness could vary from too thin to approximately

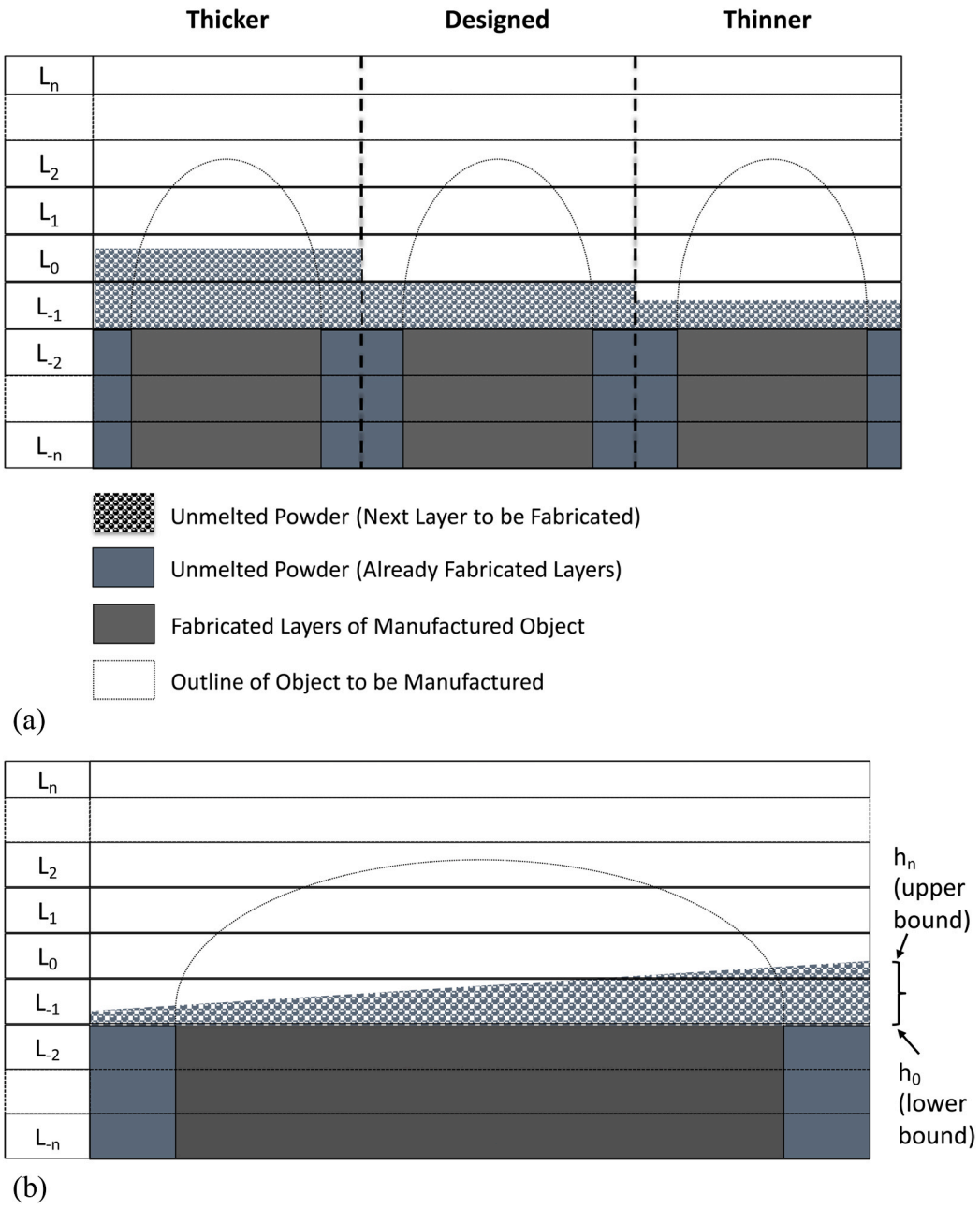


Fig. 3. *Layer-related Defects –Layer Thickness*. The deviation in layer thickness can be either uniform across the build plate or non-uniform, e.g., on a gradient. Note that the figure is simplified: As the powder is melted and its density increases, the top surface of the consolidated regions would be lower than that of surrounding powder bed.

appropriate to too thick. As the optimal build parameters anticipate a constant layer thickness, the melt pool behavior in an angled layer will not be exactly as anticipated even at the approximately appropriate point since the adjacent impingement points will be out of normal bounds.

3.2.1.2. Layer compaction. Layer compaction refers to the spacing amongst the unmelted powder particles in the bed prior to heat source application. The compactness affects the powder layer density which in turn affects the part density and properties [44,17,48,49]. Generally, a certain degree of packing density is required for part quality [19,44], with higher density associated with better mechanical properties [50]. Altered compactness which lowers the powder layer density degrades the melt pool, resulting in non- or weaker fusion and diminished part mechanical properties.

Even with very thin layers possibly minimizing compaction concerns, the physical manufacturing process leaves depressions from build fluctuations in the previous layers. These depressions, which can be quite deep, must be filled in the new layer. Compaction then remains issue, absent a perfect monolayer [51].

3.2.1.3. Layer uniformity. When the powder is atomized for use in AM, the particles are not uniform in size but rather are characterized as existing within an acceptable range. Layer uniformity refers to the distribution of these various sized particles within the powder layer. Particles exceeding the acceptable size range or anticipated distribution will breach the optimal build parameters [18,19]. Uniformity contributes to the smoothness of the powder layer surface which in turn influences melt pool characteristics and counteracts agglomeration tendencies.

3.2.2. Heat source-related defects

In PBF, the powder is melted to form the part by a heat source which can be either laser or electron beam. If the distance of the surface layer from the heat source is modified, it can alter the locus of the beam's impingement on the powder layer or the size of the beam at the point of impingement. It can also alter the exposure duration of the melted powder.

If after powder distribution, the build plate, and consequently the surface layer, is raised toward the heat source, the beam will intersect the surface higher than the optimal focal point; if it is lowered, the beam will intersect the surface below the optimal point (see Fig. 4a). Both cases will impair energy transfer, impacting the melt pool depth and quality as well as track width, possibly contributing to lack of fusion defects. Moving the build plate can also result in a larger or smaller beam exposure range (see Fig. 4b), impacting the part dimension in that layer.

3.2.3. Timing-related defects

The timing of the powder distribution process from dosing and spreading to the beginning of the next melting cycle is a component of the PBF heat transfer process. During this cycle, heat from previous build layers dissipates and also pre-heats the deposited powder in preparation for the next melting phase. This heat transfer is necessary to maintain the specified layer temperatures and temperature gradients required for a successful build.

Temperature and temperature gradient abnormalities can result in unmelted powder or lack of fusion defects. Other impacts can include overmelting, remelting, and melt pool turbulences. Altering the timing during any part of the distribution process, then, could impact the part mechanical properties.

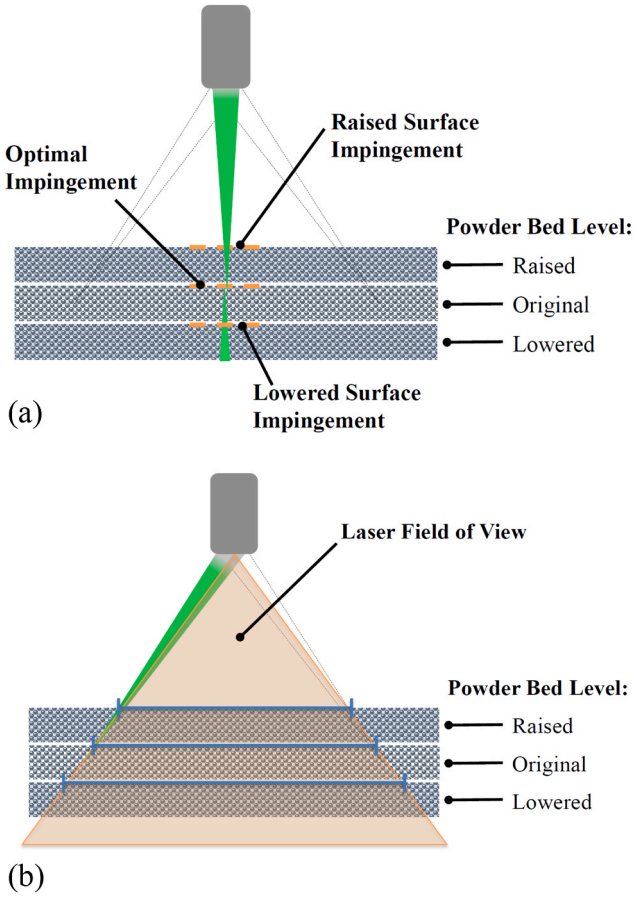


Fig. 4. Heat Source-Related Defects. The defects are introduced by modifying the distance between the heat source (the laser) and the surface of the deposited powder.

3.2.4. Kinetic-related defects

With PBF machines, there is the potential for pressure on the previous layers from shear forces and compressive stress as the powder is spread across the build chamber [17,19]. The pressure can result in compressive kinetic damage to the already completed part [17,19]. To mitigate the potential damage, rollers are counter-rotated which increases the fluidity of the powder and correspondingly decreases the pressure [17]. Additionally, there is potential for other PDS components such as a scrapper, roller, or rake to collide with the part or other machine components thereby causing kinetic damage to the part or the machine [19].

3.3. Individual manipulations

There are various malicious manipulations that can be performed on and with the PDS. The manipulations described here cause the defects described in Section 3.2, both individually and in combination. Fig. 5 summarizes the relationships. Combinations of these individual manipulations are discussed in Section 3.4.

3.3.1. Dosing

Dose is the term used to describe the amount of powder available to be spread as the next build layer. The dosing process is PBF machine dependent. As mentioned in Section 2.2, the two most common dosing mechanisms are fresh powder cells (Fig. 1a) and hoppers (Fig. 1b).

3.3.1.1. Improper powder cell dosing. Powder cell PBF machines control dosing by raising the cell chamber floor. The spreading mechanism then moves across the top of the cell chamber, pushing the powder in front of it to cover the previous layer in the build chamber. If the bed chamber floor is raised too high, the result is an amount of powder which exceeds that needed to cover the layer; the spreading mechanism will ensure that the layer thickness is appropriate, however, there will be an excessive waste of powder which is brushed away from the build chamber by the spreader. It is possible that this could have the effect of running out of powder before the build is completed. Even if powder can be added in order to finish the build, the thermal history has been affected and the delay may result in a timing-related defect.

If the bed chamber floor is not raised enough, the result is that the dose is insufficient to fully cover the entire layer. As the spreading mechanism pushes the entire batch of the powder from one side of the build chamber to another, it will result in incomplete layer coverage (see Fig. 6a), referred to as a "short feed." The effect will be a layer thickness defect where the layer becomes angled, tapering to a too thin layer.

3.3.1.2. Improper hopper dosing. Hopper PBF machines control dosing through valves. The dose quantity depends on the amount dispensed through the valve. The hopper can be stationary or traverse the build platform; which system is used is equipment manufacturer dependent [37,17,19]. In machines with a stationary hopper, the dosing behavior will have the same effect as the fresh powder cell system. In machines with a traversing hopper distribution, there is a continuous powder flow dispensing method as the spreading mechanism moves across the build chamber. In the event the valve is electro-mechanical and can be controlled through the firmware, the dose during the spreading process could be restricted or increased. If it is increased, similarly to the prior case, it will result in wasted material and the potential to exhaust the powder supply prior to build completion. If the dose is restricted, it will result in insufficient coverage (see Fig. 6b). The effect will be a layer thickness defect where the layer is too thin and where compaction and uniformity are compromised due to a lack of contact with the spreading mechanism. It is possible that there will also be a heat source-related defect from the increased distance of the thinner layer surface to the

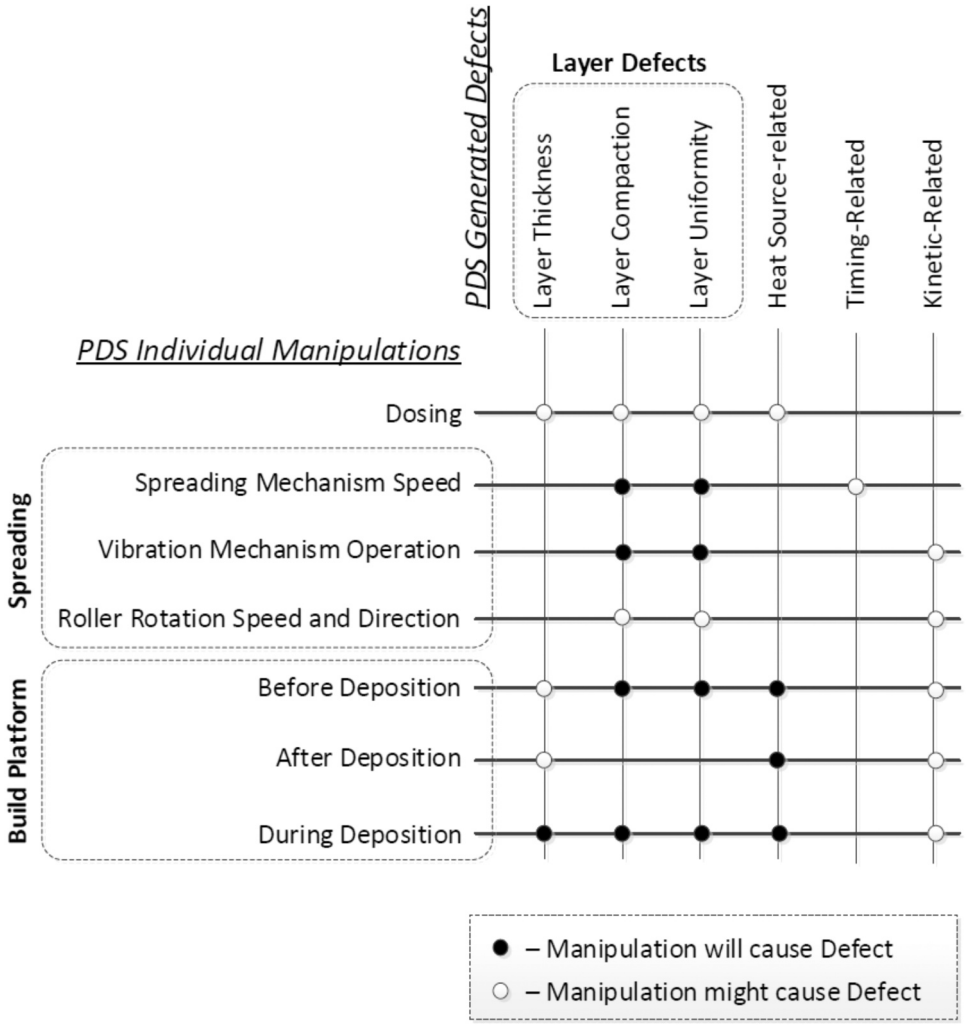


Fig. 5. Correlation between individual manipulations and generated defects.

heat source.

3.3.2. Spreading

The components of spreading mechanism are machine dependent (see Section 3.2). Machines can use rollers, scrappers, hard or soft brushes, or rakes [52,37,33,39,42], as well as combinations thereof. Some machines also incorporate vibration mechanisms to assist in compaction [44] and to facilitate powder fluidity [17].

3.3.2.1. Spreading mechanism speed. The speed with which the spreading mechanism traverses the build chamber can be controlled either via firmware or operator inputs, depending on the machine [53]. If the spreading mechanism moves too quickly it could impact packing density [53,54] and cause voids and an undulating surface [54] as well as surface roughness [55], resulting in layer defects and, possibly, timing-related defects. If it moves too slowly, it will most likely result in timing-related defects.

3.3.2.2. Vibration mechanism operation. Some researchers [40,17,56, 41,42] have investigated the use of vibration mechanisms in the PDS to improve compaction and reduce agglomeration which impacts powder layer uniformity. If the vibration mechanism is turned off, compaction will be degraded and agglomeration can occur, possibly resulting in layer uniformity defects. If the vibration mechanism is operational but the frequency or amplitude is modified outside optimal operational parameters, both under- and over-compaction might occur. Under-compaction can reduce layer density, degrading the part's mechanical properties; over-compaction can possibly produce kinetic defects, damaging the underlying part layers.

3.3.2.3. Roller rotational speed and direction. If a roller is used as part of the spreading mechanism, the roller operates in a counter-rotational direction to facilitate powder distribution and reduce metallization and compaction pressure. If the direction of the roller is reversed, uniformity, compaction, and kinetic defects can occur. If the roller rotational speed is modified, the powder spreading becomes inefficient resulting in uniformity and compaction defects.

3.3.3. Build platform

The build platform performs several functions in a PBF machine. As part of the powder distribution process, the build platform is lowered prior to the powder deposition and distribution process. Under normal conditions, the clearance defines the maximum layer thickness of the part, as excessive powder is removed by the spreading mechanism which runs on the top of the build chamber walls. However, the clearance can be either decreased or increased by raising or lowering the platform.

We distinguish between three cases, based on when the build platform modification occurs.

3.3.3.1. Before deposition. Under normal conditions, the build platform is lowered only before powder deposition. If the platform is lowered less than designed for, it will result in a thinner layer, and possibly result in

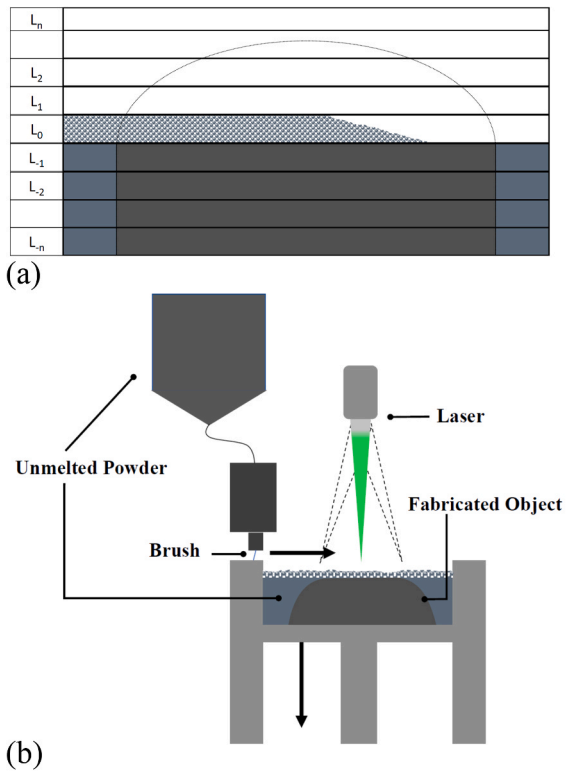


Fig. 6. Dosing Manipulations. These examples are representative of insufficient dosing.Note that the figure is simplified: As the powder is melted and its density increases, the top surface of the consolidated regions would be lower than that of surrounding powder bed.

kinetic part damage. If platform is lowered more than designed for, the result depends on the dosing mechanism. If hopper is used, this will result in compaction, uniformity, and heat-related defects. If a powder bed is used, it includes all prior described defects; plus, depending on the amount platform is lowered, it might result in a short feed similar to Fig. 6b.

3.3.3.2. After deposition. If the build platform is lowered after the powder deposition, it increases the distance between the surface of the deposited powder layer and the heat source, leading to the heat source-related defects. If the build platform is raised, it decreases this distance, also leading to heat source-related defects. In addition, tapering effects might occur at the edges of the build platform.

3.3.3.3. During deposition. If the platform is manipulated during deposition, the result depends on the dosing mechanism. If a hopper which traverses the build chamber is used and the build platform is lowered during deposition, this will result in compaction and uniformity defects both of which will increase as the variance from the designed height increases. If a hopper which traverses the build chamber is used and the build platform is raised, this will result in an angle layer with tapered edges and possible kinetic impact, depending on the degree of variance (see Fig. 7).

If a powder bed or stationary hopper is used and the build platform is lowered, the layer will start angled increasing in size, until the dose has been exhausted. After this point, there will be a tapered end, eventually leading to the exposure of the prior layer. If a powder bed or stationary hopper is used and the build platform is raised, this will lead to an angled layer with decreasing thickness along the way. In addition there will be tapered edges along the build chamber walls.

All these manipulations will result in layer and heat source-related defects. In addition, if the platform is lowered, compaction and uniformity defects will also occur. If the platform is raised, there is a possibility of kinetic defects.

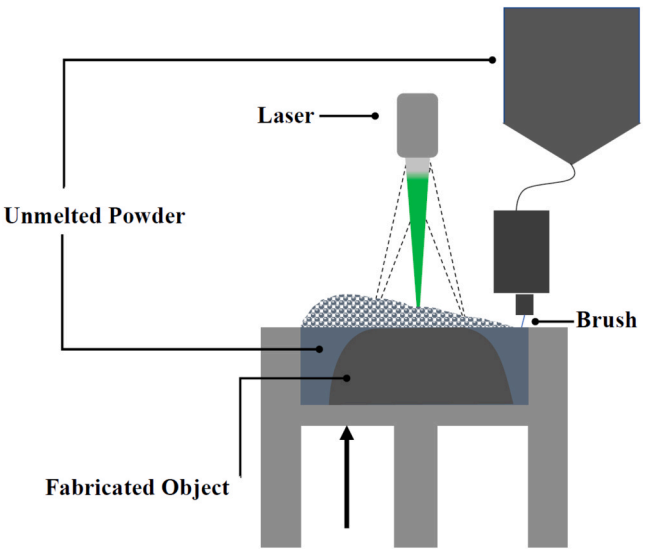


Fig. 7. *Build Platform Manipulation* –In this example, the build platform is raised during powder spreading.

3.4. Compound manipulations

While in the prior section we considered each manipulation in isolation, in this section we consider combining them. Specifically, we discuss intra-layer manipulation, inter-layer manipulations, and the combination of different types of manipulations. These are independent of each other and, as such, can result in multiple combinations with distinct impacts separate from those of the individual manipulations of which they are composed.

3.4.1. Intra-layer

The manipulation does not necessarily need to affect the entire layer of a print. Instead, it can be timed to affect a selected section of a layer. Fig. 8(a) depicts an example of the build platform manipulation which starts one-third of the way across the layer and then stops two-thirds of the way across, resulting in a distinct impact. Additionally, multiple manipulations can occur across the layer. Fig. 8(b) depicts repeated build platform manipulations, specifically raising and lowering the platform, which could produce a ripple-like effect.

3.4.2. Inter-layer

A manipulated layer can be adjacent to either as-designed or manipulated layers. If it is only adjacent to as-designed layers, the impact is identical to the individual manipulations described in Section 3.3.

When manipulated layers are adjacent to other manipulated layers, their individual impact can be combined and amplified into unique defects. For example, a single angle defect per layer for several layers would have a different impact than one layer of an angle defect. In another example, one layer height can be reduced to half the height parameter, resulting in a too thin layer thickness, with the next layer increased to one and one half times the height parameter, resulting in a too thick layer but compensating for the prior thin layer in the overall part height.

3.4.3. Multiple types

Performed manipulations are not limited to a single type described in Section 3.3. Rather, they can be combined with each other arbitrarily resulting in multiple and various unique impacts. For example,

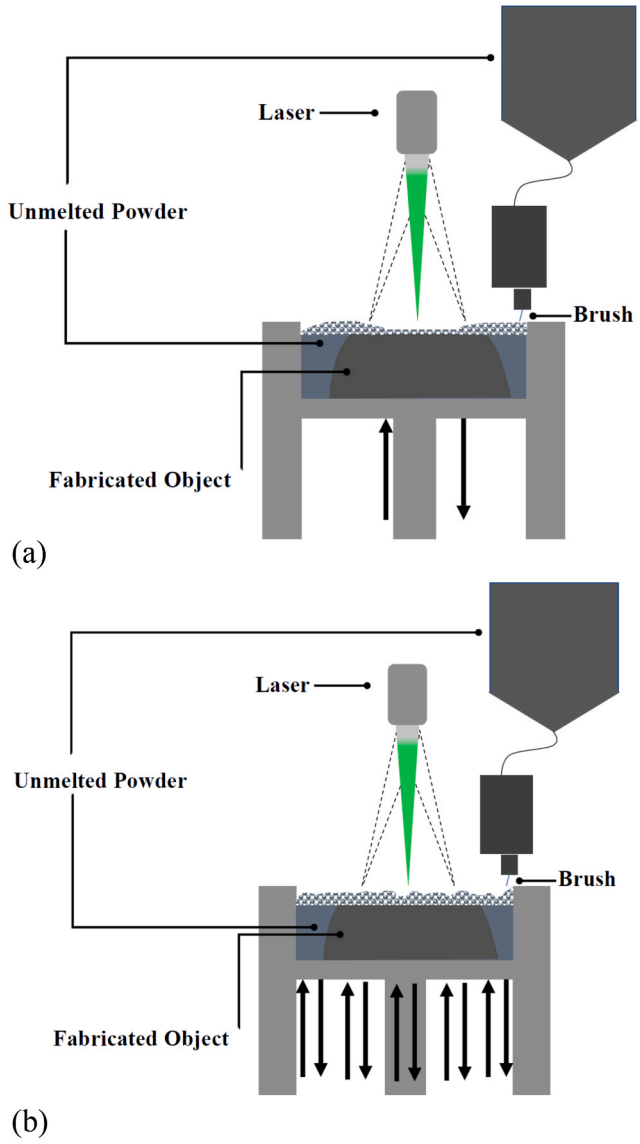


Fig. 8. Compound manipulations –intra-layer. In this example, the build platform is raised and lowered during powder spreading.

manipulation of a build platform causing a too thin layer defect combined with a roller rotation manipulation causing an over-compaction defect could result in a kinetic-related defect. Another alternative would be depositing a too thick layer and then lowering the build platform even more prior to scanning with the heat-source, resulting in a combination of layer- and heat source-related defects.

3.5. Part targeting

When the manipulations discussed in this paper are applied to an entire layer, the specific effect and degree of impact will depend on the intersection of the manipulated layer and the part. To be goal-optimized, the attack needs to be targeted. It should be designed for a specific part geometry and with knowledge of the required part functional properties. Additionally, the attacker needs to know the placement and orientation of the part on the build platform in order to identify the optimal horizontal and vertical placement of a manipulation. A targeted PDS-based attack can be either direct or indirect as described below.

3.5.1. Direct attack

A *direct attack* is where the defect is placed within the part or on its external surface. Depending on the location, the same defect can result in different outcomes. For example, an external surface defect can cause surface roughness, resulting in fatigue-initiating cracks and subsequent premature service failure. An internal defect could cause increased porosity, resulting in degraded mechanical properties such as tensile strength or ductility or in reduced fatigue life. Fig. 9(a) illustrates a targeted internal defect case. From a security perspective, direct attacks introducing part deviations are more likely to be detected by non-destructive testing.

3.5.2. Indirect attack

The adversary can launch indirect attacks by targeting unmelted powder, non-part layers, or support structures. Unmelted powder functions as part geometry support structures and as a heat sink. Any modifications to the unmelted powder regions alters thermal properties. Non-part layers are the initial and terminal layers in the build chamber which occur below and above the part. Any modifications to these layers impacts the build in ways similar to unmelted powder manipulations.

Support structures in PBF can be used as heat sinks to mitigate thermal residual stress. In a *thermal residual stress attack*, the adversary would manipulate the structures to increase the thermal residual stress, resulting in effects such as part warpage and distortion or degraded microstructure. From a security perspective, indirect attacks impacting part microstructure are likely to evade inspections since they do not affect visible layer properties of the final part. Fig. 9(b) illustrates a targeted indirect attack.

4. Experimental evaluation

The effectiveness of a sabotage attack is determined by its ability to generate the desired degree of damage and its ability to evade detection long enough for the damage to occur. In this section we empirically assess both these characteristics for a selected PDS-enabled attack applied to a metal part manufactured on Laser Beam PBF. We start in Section 4.1 by describing parts that were manufactured for the experimental evaluation. In Section 4.2 we assess the ability to detect introduced defect with Non-Destructive Testing (NDT) methods. Lastly, in Section 4.3 we use Destructive Testing (DT) to assess impact of the attack on the part's fatigue life.

4.1. Description of experiments

Two different PBF machines were used to print specimens for the experimental evaluation –an EOS M290 and a GE Additive Concept Laser M2 Series 4. The EOS M290 is a single-laser PBF machine. The GE Additive Concept Laser M2 Series 4 is a dual-laser PBF machine. The process parameters used with both machines are summarized in Table 2.

With both PBF systems, the EOS M290 and Concept Laser M2 Series 4, we used the same set of specimens. As a basis we used round fatigue specimens with uniform gage sections in accordance with ASTM E606–12 standard [57]. The design file was modified to simulate introducing a layer thickness defect. The specimens were fabricated vertically and the build began with a normal layer height. Then in the middle of the gage section, thicker layers were introduced. In case *2x*, the layer thickness was modified by a factor of 2 and in case *3x*, the layer thickness was modified by a factor of 3. Case *1x* corresponds to unmodified specimens. In the conducted experiments, the layer thickness was changed uniformly throughout the entire powder bed. Consequently, the introduced layer thickness modification impacted the entire cross-section of a specimen regardless of the specimen location on the build plate. In cases *2x* and *3x*, the section above the modification was shortened in the area next to the modified layer to prevent the added thickness from increasing the overall specimen size, creating a compensating inter-layer thickness manipulation. The geometry and dimensions of the specimens as well as the location of the defect are depicted in Fig. 10.

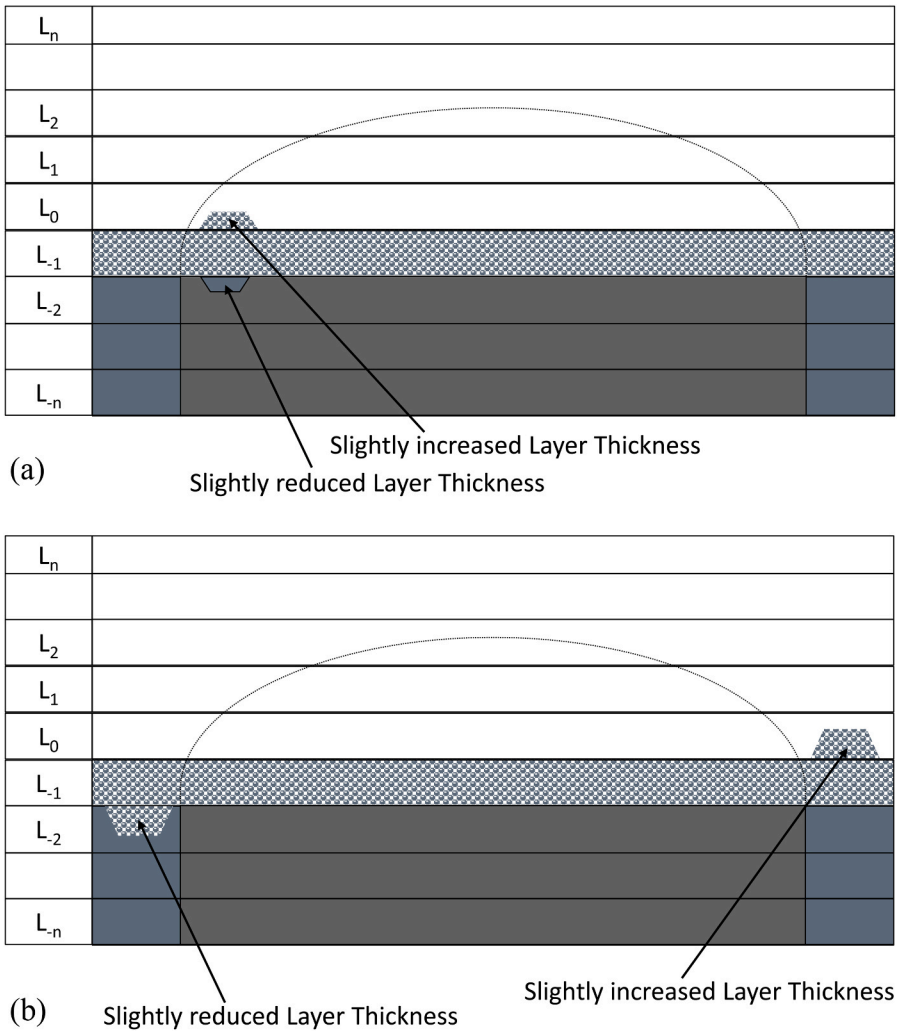


Fig. 9. Part targeting. Changes introduced by an attack can either intersect the area designated for the fabricated object (*Direct Attack*) or remain outside of it (*Indirect Attack*).Note that the figure is simplified: As the powder is melted and its density increases, the top surface of the consolidated regions would be lower than that of surrounding powder bed.

Table 2
AM systems and build process parameters.

Additive system	Material	Inert gas environment	Laser power W	Beam diameter μm	Hatch distance mm	Scanning speed mm/s	Layer thickness mm
EOS M290	17–4PH SS	Nitrogen	220	100	0.100	755.5	0.040
GE M2 S4	316 L SS	Argon	370	130	0.090	1350	0.040

Each AM machine was used to print test specimens with one of the two materials used in the study. With the EOS M290 we printed 12 specimens using Argon-atomized 17–4 pHStainless Steel (SS) powder with a 15–45 μm particle size distribution. After fabrication, the specimens were heat treated following the CA-H1025 heat treatment procedure [58,59]. With the Concept Laser M2 Series 4, we also printed 12 specimens. However, this set was made of 316 L SS with 90% of powder particles between 15.15 μm and 44.66 μm in size. We used the M2 with both lasers deployed and their optic systems configured as similarly as possible. There was no heat treatment performed on these specimens. Finally, there was no post-build surface processing performed on specimens fabricated from either material; thus, they were tested in the "as-built" surface condition.

4.2. Non-destructive testing (NDT)

To determine whether the attack could be detected non-destructively, we examined the specimens using three techniques –visual inspection, digital microscopy, and X-Ray μ CT (Computed Tomography).

4.2.1. Visual inspection

Upon print job completion, the samples were visually inspected. The modifications to the test specimens were not detectable at this stage of examination.

4.2.2. Digital microscopy

We next conducted digital microscopy using a *Keyence VHX-6000* to examine the gage section of the round fatigue specimens. Fig. 11 shows the digital microscope images for the area in which the defect was

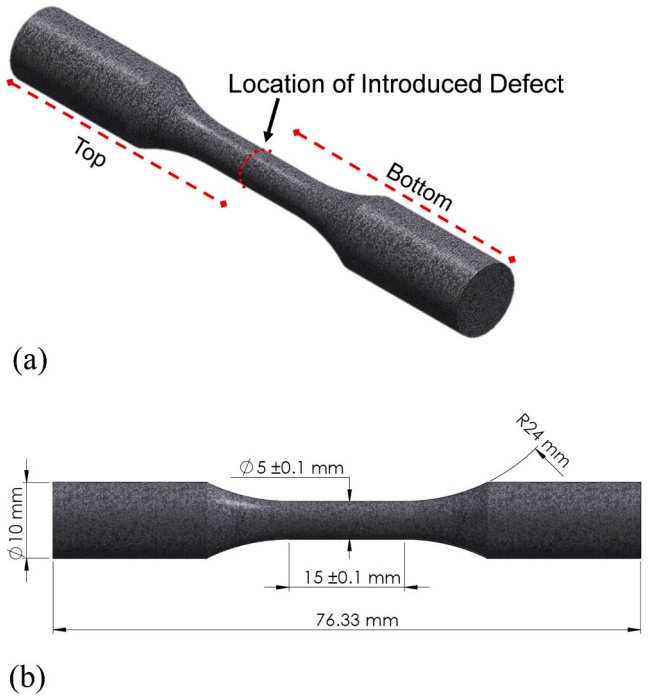


Fig. 10. Round fatigue specimens with uniform gage section used in NDT and DT.

introduced. The modified layer is in the middle of each layer. For the altered 17–4PH SS test samples, there is a subtle indication of irregularities in the layer(s) where the layer thickness has been modified (see Fig. 11c and e). However, for the altered 316 L SS specimens there is no indication that the layer thickness has been modified (demonstrated in Fig. 11d and f). This demonstrates that the ability to detect such an attack via microscopy is both limited and material dependent. Further, it should be noted that we knew the exact location of the defect introduced in a small part with a simple geometry. The probability of detecting such anomaly in a large part is low.

4.2.3. X-ray CT

We conducted NDT with a *Zeiss Xradia 620 Versa* X-ray micro-computed tomography (X-μ CT) system. The X-μ CT scans were conducted at 25 W power and 160 kV voltage. A total of 1601 projections (2 s and 18 s exposure time per projection for the 316 L and 17–4Ph, respectively) were collected per scan. The scans were focused on the area surrounding the defect location. Fig. 12 shows the reconstructed X-ray images. The imaged volume area was approximately 8FC3.0*mm* by 3.5*mm* height. The voxel size we used for the 17–4 pHSS scans was 4.3μm, while that for the 316 L SS scans was 6μm. The results presented in Fig. 12 were scaled accordingly.

The defects in the 17–4PH SS specimen are clearly visible on the CT scan (see Fig. 12a and c.) The core portion of the defect in the 316 L SS specimen is not visible to the same extent (see Fig. 12b and d). However, there are observable near-surface defects concentrated in the subject layers. This demonstrates that the detectability of this category of defect with this technology is strongly material dependent. This is because the melt pool depth at optimum processing condition is material dependent, leading to different layer overlap ratio and melt pool overlap ratios from material to material [60,61]. Thus, the severity of the Lack-of-Fusion (LoF) defects created by the modified layer thickness varies from material to material, resulting in different detectability using X-Ray CT. It should be further noted that the resolution of X-Ray CT, and therefore of ability to detect such anomalies, will be significantly reduced in larger parts.

Further discussion explaining the fatigue life results is presented in Section 4.3.2, in which we analyze and compare the fracture surfaces of specimens without defects and with x2 and x3 layer thickness defects.

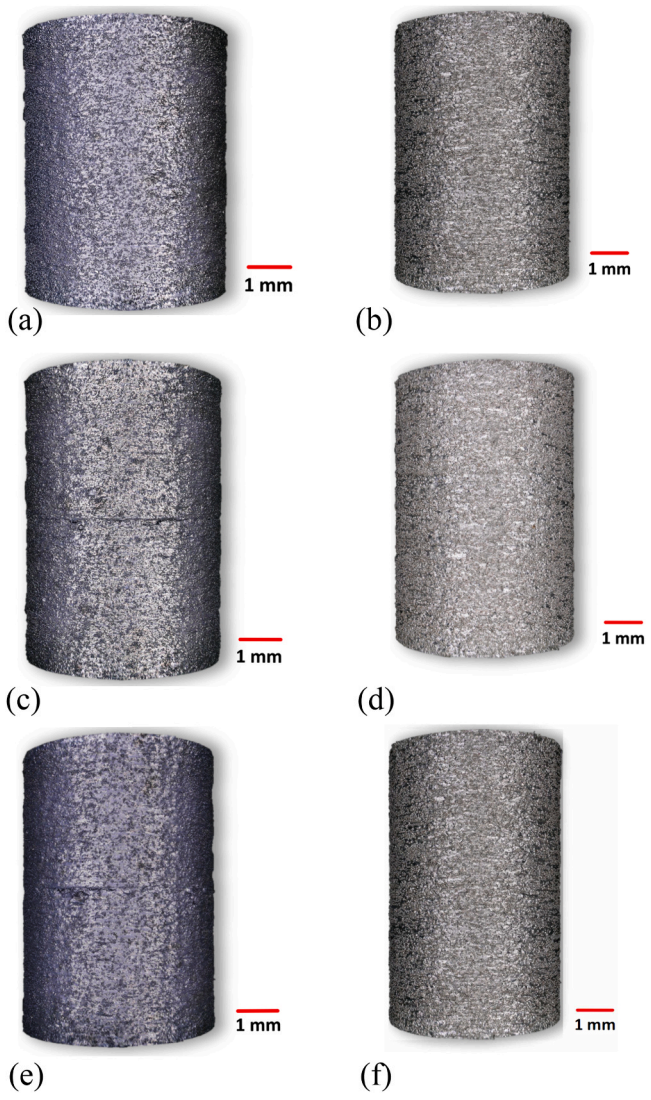


Fig. 11. Optical microscope images of the gage section. These images were obtained using the *Keyence VHX-6000* digital optical microscope.

4.3. Destructive testing (DT)

To determine the ability of the attack to successfully degrade the part's function, we examined the specimens using an servohydraulic system to measure fatigue life and a digital microscope to compare crack initiation sites.

4.3.1. Fatigue testing

We measured specimen fatigue life using an *MTS Landmark* servo-hydraulic test frame with a 100 kN load capacity. All fatigue tests were performed at room temperature using a tapered sinusoidal load waveform. Fatigue tests were conducted under fully-reversed ($R_\sigma = -1$) uniaxial force- and strain-control ($R_\epsilon = -1$) loading.[1] The frequency was

[1] R_σ is the stress ratio that is defined as $R_\sigma = \sigma_{min}/\sigma_{max}$, where σ_{min} is the minimum stress and σ_{max} is the maximum stress. R_ϵ is defined similarly with ϵ_{min} being the minimum and ϵ_{max} the maximum strain values. Similar equation and principle apply for R_ϵ, where ϵ_{min} is the minimum strain and ϵ_{max} is the maximum strain values.

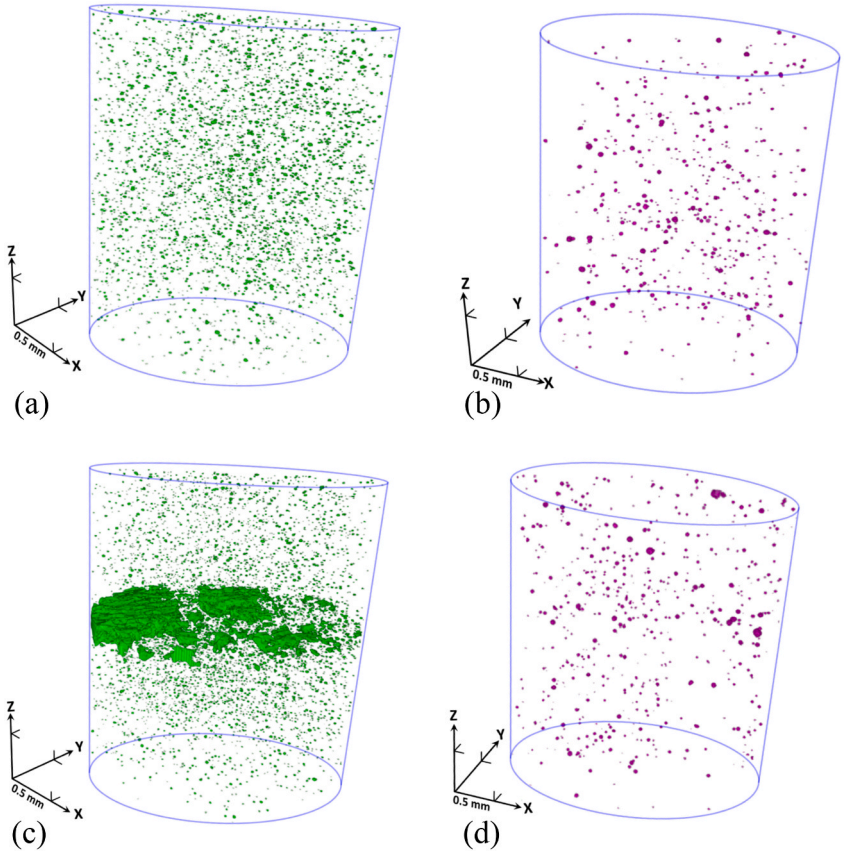


Fig. 12. Reconstructed X-Ray CT images showing internal porosity in the uniform gage section. These images were obtained using the *Zeiss Xradia 620 Versa* X-ray micro-computed tomography (X-μ CT) system.

adjusted to maintain a constant average cyclic stress/strain rate. A minimum of three specimens were tested for every condition and test parameter to ensure statistical relevancy.

The materials have different mechanical properties with the 17–4PH SS possessing higher strength and lower ductility than the 316 L SS [58, 62]. As this makes the 17–4PH SS more sensitive to defects, we adjusted the parameters to test the 17–4PH SS specimens under force-control since the cyclic stress-strain response is known to exhibit little plasticity [58]. The 316 L SS specimens were tested under strain-control since this material exhibits plastic deformation even at relative low strain amplitude values [62].

For 17–4PH SS, we selected the three stress amplitudes of 375, 350, and 325 MPa because they are close to the material's endurance limit of 293 MPa [58]. This region is of special interest as most load bearing applications are designed to not exceed the endurance limit [63] and testing near this region is known to increase the material's sensitivity to defects [63]. For the strain-controlled 316 L SS specimens, the strain amplitude results are displayed to provide better comparison. The plots are shown in Fig. 13.

The fatigue life of the 17–4PH SS specimens with defects is almost three orders of magnitude (i.e., 1000 times) shorter than the specimens without defects (see Fig. 13a), and the observed fracture initiated exclusively from the location of defect introduced by the attack. Noticeably, the 17–4PH SS specimens with 3x layer thickness defect have longer fatigue life compared to those with 2x layer thickness defect. This indicates that the attack is more detrimental to a brittle material (i.e., 17–4PH SS).

In the case of 316 L SS at 0.001 mm/mm strain amplitude, all data points are clustered together; the specimens with 3x layer thickness defect exhibit slightly shorter fatigue life than the rest of the specimens manufactured with the same laser at the same stress amplitude. For fatigue tests at 0.002 mm/mm, observed fatigue life is shorter than 75,000 reversals; the specimens without defect and those with the 2x layer thickness defects do not differ significantly in fatigue performance. However, the fatigue life of specimens with the 3x layer thickness defect was relatively shorter than the rest at both strain amplitudes.

Due to similar surface roughness conditions, the fatigue scatter of specimens with an as-built surface condition is typically minimal, even at stress/strain levels near the endurance limit. Therefore, an increased scatter in the experimental results is indicative of the sabotage effects. These factors need to be considered by an attacker.

In addition to the test parameters and fracture conditions, we recorded the location at which the fracture occurred. In the case of specimens without defect, the fracture could occur in any part of the gage section. In the case of specimens with introduced defects, however, the fracture location was almost exclusively in the middle part where defect was introduced. The implication, from a security perspective, is that an adversary can alter the fracture point location, ensuring that it is both effective and difficult to inspect and/or detect.

4.3.2. *Fractography*

After specimen failure, we examined the fracture surface using the *Keyence VHX-6000* digital microscope. We conducted the analysis on specimens of all three defect-types, manufactured with both types of materials. The goal of the analysis was to find distinct features and crack initiation sites that would be characteristic of the defect caused by the increased layer thickness.

Fig. 14 shows selected analyzed specimens. In the case of the defect-free 17–4PH SS specimen, due to the as-built surface condition, the fracture surface is smooth with multiple, well-defined crack initiation sites originating around the circumference of the specimen (denoted by the shaded blue area). The fracture surface with the defects, however,

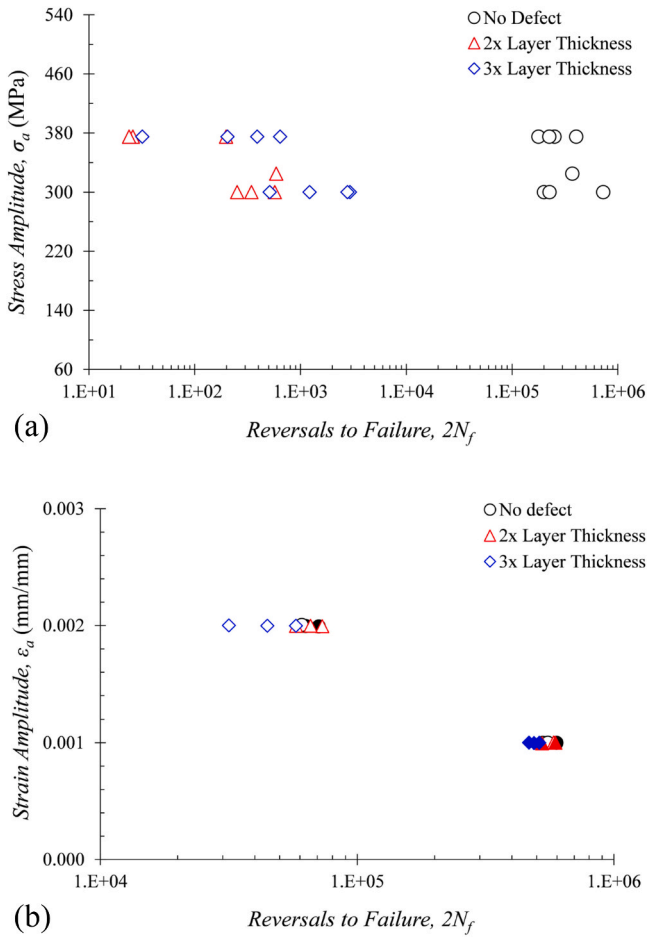


Fig. 13. Fatigue Test Results.

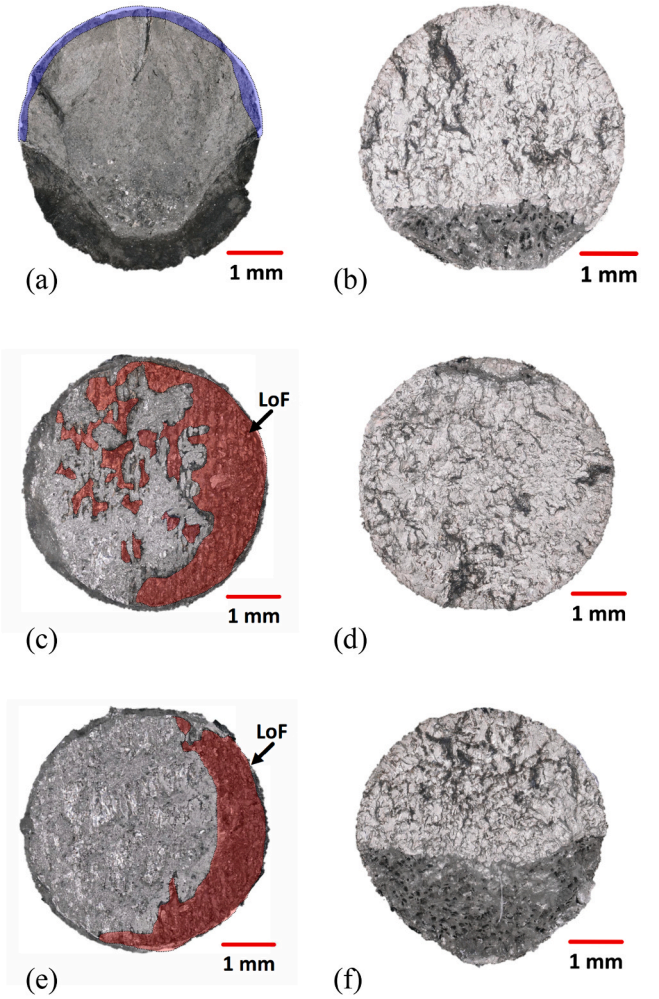


Fig. 14. Fractography (17–4PH SS Specimens Tested at 375 MPa; 316 L Specimens Tested at 0.002 mm/mm strain amplitude). These images were obtained using the *Keyence VHX-6000* digital optical microscope.

presents a brittle-type fracture indicating that the lack-of-fusion was the main reason for shorter fatigue life span. Furthermore, when comparing fractography of specimens with two different defect levels (see Fig. 14c and e), we observed that the lack-of-fusion area (darker gray) of the specimen with 2x layer thickness defect is considerably larger than is the case with the specimen with 3x layer thickness defect. As a result, the load bearing area of the specimen in Fig. 14(c) is smaller. This can explain why the specimen with the smaller defect unexpectedly exhibited a shorter fatigue life than the specimen with the larger defect. The mechanisms leading to this development require additional investigation.

In the case of the 316 L SS specimens, there are no substantial differences for the defect-free and 3x layer thickness defect specimens due to the specimens not fully fracturing, even after the test was deemed complete (50% load drop). Subsequently, the specimens were pulled apart with a monotonic load. The resulting final fracture areas are depicted by the darker gray in Fig. 14(b) and (f). In contrast, the 2x specimen continued running until final fracture occurred and the fatigue life was adjusted to the same failure criteria as the rest of the experiments (see Fig. 14d). After further investigation, we observed that the specimen with the 3x layer thickness defect presents more internal cracks rather than lack-of-fusion defects which leads to a more rugged surface.

5. Conclusion

In this paper we focused on a largely neglected security threat in Additive Manufacturing (AM) – the sabotage of metal 3D-printed functional parts. As the role of AM in supporting national security and economic prosperity expands, correspondingly so does its visibility as a cyber-physical attack target. In examining a potential attack avenue, this paper focused on *Powder Bed Fusion*, a metal AM process used to manufacture parts for safety critical systems, and its *Powder Delivery System*, an integral component of PBF machines.

We first analyzed a possible PDS attack from the attacker's perspective. We identified the target as degradation of part function which would be accomplished by compromising the part mechanical properties through the introduction of PDS-induced defects. We then identified manipulations capable of producing said defects which could be used individually or in combination for sabotage attacks.

Once we had identified various, potential manipulations, we experimentally evaluated the impact of a compound, intra-layer layer thickness manipulation on defect creation and amplification as well as the impact of two, distinct individual layer thickness manipulations on mechanical properties as measured by fatigue life. The results were first evaluated using non-destructive testing (NDT). The visual inspections, digital microscopy, and X-Ray CT indicated that while some defects could be detected with NDT, the level of detection was material dependent and would be more challenging when used against actual parts with complex geometry as opposed to our geometrically simplistic test specimens.

In the destructive testing (DT) phase, our experimental evaluation used fatigue testing to measure the induced defect impact on the specimen mechanical properties. The DT with a servohydraulic test system

documented material dependent premature failure of the test specimens, with the 17–4PH specimen notably experiencing a three orders of magnitude difference. The fractography confirmed the correlation of the failures with the induced defects. The DT results combined with the NDT results indicate that successful attacks, which accomplish the goal of damaging a part while avoiding detection, will be material and part geometry dependent.

In summary, this paper demonstrates the possibility of sabotaging metal AM parts via manipulations of the PDS sub-system of a PBF machine. We proposed an approach where attackers can "work backwards" from their intended goal and targeted sub-system to first identify *Individual Manipulations* of this sub-system, assessing their effectiveness in causing defects and avoiding detection. They can then construct *Compound Manipulations* capable of both amplifying malicious effects and reducing the probability of detection. This approach is applicable to other sub-systems and other AM processes as well. We verified experimentally that our selected attack can indeed degrade a part's fatigue life while avoiding detection by the non-destructive testing (NDT). During experimental evaluation we discovered that the attack's degrading effect and detectability by NDT are material-dependent—factors that should be considered by both attackers and defenders.

We want to emphasize that, while some of the discussed defects also occur in non-sabotaged AM, there is a fundamental difference between "naturally occurring" and "sabotaged" process flaws that lead to build part defects. Natural causes, such as imperfections in the manufacturing process, tend to be present in the entire build, with the process parameters exhibiting bounded stochastic fluctuations. In the case of sabotage, the deviations can be carefully planned and introduced in a strictly localized manner, ensuring that the part's function is degraded and the probability of detection is minimized.

Based on our research, we conclude that sabotage attacks on a PBF machine through the PDS are both feasible and effective. Given the use of metal PBF parts in safety-critical systems and the anticipated growth of the AM industry, it is apparent that AM security requires immediate attention from experts with the unique combination of cyber-security and AM specific domain expertise.

CRediT authorship contribution statement

L. Graves: Conceptualization, Methodology, Investigation, Writing - original draft, Visualization. **W.E. King:** Methodology, Validation. **P. Carrion:** Investigation, Visualization, Data Curation. **S. Shao:** Investigation, Supervision. **N. Shamsaei:** Methodology, Resources, Supervision, Project administration. **M. Yampolskiy:** Conceptualization, Methodology, Investigation, Writing - original draft, Writing - review & editing, Visualization, Supervision, Project administration.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was funded in part by the U.S. Department of the Navy, Office of Naval Research under Grant N00014-18-1-2488, and in part by the U.S. Department of Commerce, National Institute of Standards and Technology under Grant NIST-70NANB19H170.

The authors would like to acknowledge Mr. Richard McIlwain, a former student of Dr. Yampolskiy, for his initial work investigating powder delivery systems.

The authors would like to express special gratitude to Dr. Ibo Matthews and Mr. Gabe Guss from Lawrence Livermore National Laboratory who manufactured some of the specimens for the experimental evaluation and provided valuable comments to the preprint of this manuscript.

References

[1] N. Shamsaei, A. Yadollahi, L. Bian, S.M. Thompson, An overview of direct laser deposition for additive manufacturing; Part II: mechanical behavior, process parameter optimization and control, Addit. Manuf. 8 (2015) 12–35.
[2] A. Yadollahi, N. Shamsaei, Additive manufacturing of fatigue resistant materials: challenges and opportunities, Int. J. Fatigue 98 (2017) 14–31.
[3] M. Seifi, M. Gorelik, J. Waller, N. Hrabe, N. Shamsaei, S. Daniewicz, J. J. Lewandowski, Progress towards metal additive manufacturing standardization to support qualification and certification, JOM 69 (2017) 439–455.
[4] T. Kellner, How 3D Printing Will Change Manufacturing, 2017.
[5] H. Post, SpaceX Launches 3D-Printed Part to Space, Creates Printed Engine Chamber, 2014.
[6] S. Burns, J. Zunino, Rambo's Premiere, 2017.
[7] J. Burrow, P. Cullom, M. Dana, Department of the Navy (DON) Additive Manufacturing (AM) Implementation Plan V2.0 (2017), 2017.
[8] J. Kasprzak, A. Lass, C. Miller, Development, test, and evaluation of additively manufactured flight critical aircraft components, AHS Int. Forum 73 (2017).
[9] C. Paulsen, Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium, Technical Report, 2015.
[10] America Makes ASTM Center of Excellence, ASTM AM Data Management and Schema Workshop - Strategic Guide: Findings and Path Forward, Technical Report, 2019.
[11] M. Yampolskiy, W.E. King, J. Gatlin, S. Belikovetsky, A. Brown, A. Skjellum, Y. Elovici, Security of additive manufacturing: attack taxonomy and survey, Addit. Manuf. 21 (2018) 431–457.
[12] M. Yampolskiy, P. Horvath, X.D. Koutsoukos, Y. Xue, J. Sztipanovits, Taxonomy for description of cross-domain attacks on CPS, in: Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems 2013 ACM, New York, NY, USA , pp.135–142.
[13] M. Yampolskiy, P. Horváth, X.D. Koutsoukos, Y. Xue, J. Sztipanovits, A language for describing attacks on cyber-physical systems, Int. J. Crit. Infrastruct. Prot. 8 (2015) 40–52.
[14] M. Yampolskiy, A. Skjellum, M. Kretzschmar, R.A. Overfelt, K.R. Sloan, A. Yasinsac, Using 3D printers as weapons, Int. J. Crit. Infrastruct. Prot. 14 (2016) 58–71.
[15] L. Graves, M. Yampolskiy, W. King, S. Belikovetsky, Y. Elovici, Liability exposure when 3d-printed parts fall from the sky, in: Proceedings of the Critical Infrastructure Protection XII: 12th IFIP WG 11.10 International Conference, ICCIP 2018, Arlington, VA, USA, March 12–14, 2018, Revised Selected Papers, Springer, pp. 221–246.
[16] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin, Y. Elovici, dr0wned – cyber-physical attack with additive manufacturing, in: 11th USENIX Workshop on Offensive Technologies (WOOT 17), USENIX Association, Vancouver, BC, 2017, p. 16.
[17] I. Gibson, D.W. Rosen, B. Stucker, Additive Manufacturing Technologies, second ed., Springer, New York City, 2015.
[18] J.O. Milewski, Additive manufacturing of metals, Springe Ser. Mater. Sci. 258 (2017) 1–339.
[19] L. Yang, K. Hsu, B. Baughman, D. Godfrey, F. Medina, M. Menon, S. Wiener, Additive Manufacturing of Metals: The Technology, Materials, Design and Production, Springer, 2017.
[20] N. Falliere, L.O. Murchu, E. Chien, W32. stuxnet dossier White Pap. Symantec Corp., Secur. Response 5 2011 6.
[21] Xiao Zi Hang (Claud Xiao), Security Attack to 3d Printing, 2013. Keynote at XCon2013.
[22] S.B. Moore, W.B. Glisson, M. Yampolskiy, Implications of malicious 3d printer firmware, in: Proceedings of the 50th Hawaii International Conference on System Sciences 2017 IEEE, 6089 6098.
[23] S. Moore, P. Armstrong, T. McDonald, M. Yampolskiy, Vulnerability analysis of desktop 3d printer software. Resilience Week (RWS), 2016, IEEE, 2016, pp. 46–51.
[24] Q. Do, B. Martini, K.-K. R. Choo, A data exfiltration and remote exploitation attack on consumer 3d printers, IEEE Trans. Inf. Forensics Secur. 11 (2016) 2174–2186.
[25] L. Sturm, C. Williams, J. Camelio, J. White, R. Parker, Cyber-physical vunerabilities in additive manufacturing systems, Context 7 (2014) 8.
[26] M. Yampolskiy, L. Schutzle, U. Vaidya, A. Yasinsac, Security challenges of additive manufacturing with metals and alloys. Critical Infrastructure Protection IX, Springer, 2015, pp. 169–183.
[27] S.E. Zeltmann, N. Gupta, N.G. Tsoutsos, M. Maniatakos, J. Rajendran, R. Karri, Manufacturing and security challenges in 3d printing, JOM 68 (2016) 1872–1881.
[28] G. Pope, M. Yampolskiy, A Hazard Analysis Technique for Additive Manufacturing, in: Better Software East Conference, p. 17.
[29] A. Slaughter, M. Yampolskiy, M. Matthews, W.E. King, G. Guss, Y. Elovici, How to ensure bad quality in metal additive manufacturing: In-situ infrared thermography from the security perspective, in: Proceedings of the 12th International Conference on Availability, Reliability and Security, ACM, New York, NY, USA, 2017, pp. 78: 1–78:10.
[30] B. Ranabhat, J. Clements, J. Gatlin, K.-T. Hsiao, M. Yampolskiy, Optimal sabotage attack on composite material parts, Int. J. Crit. Infrastruct. Prot. 26 (2019), 100301.
[31] F. Chen, G. Mac, N. Gupta, Security features embedded in computer aided design (cad) solid models for additive manufacturing, Mater. Des. 128 (2017) 182–194.

[32] N., Gupta, F., Chen, N.G., Tsoutsos, M., Maniatakos, Obfuscade: Obfuscating additive manufacturing cad models against counterfeiting, in: Proceedings of the 54th Annual Design Automation Conference 2017, pp. 1–6.
[33] W.E. Frazier, Metal additive manufacturing: a review, J. Mater. Eng. Perform. 23 (2014) 1917–1928.
[34] A. Ilie, H. Ali, K. Mumtaz, In-built customised mechanical failure of 316l components fabricated using selective laser melting, Technologies 5 (2017) 9.
[35] M. Yampolskiy, W. King, G. Pope, S. Belikovetsky, Y. Elovici, Evaluation of additive and subtractive manufacturing from the security perspective, in: Proceedings of the International Conference on Critical Infrastructure Protection, Springer, pp. 23–44.
[36] L.M.G. Graves, J. Lubell, W. King, M. Yampolskiy, Characteristic aspects of additive manufacturing security from security awareness perspectives, IEEE Access (2019) 1.
[37] J. Dawes, R. Bowerman, R. Trepleton, Introduction to the additive manufacturing powder metallurgy supply chain, Johns. Matthey Technol. Rev. 59 (2015) 243–256.
[38] I. Ederer, A. Hartman, Method and device for conveying particulate material during the layer-wise production of patterns, 2014. US Patent 8,727,672.
[39] W.J. Sames, F. List, S. Pannala, R.R. Dehoff, S.S. Babu, The metallurgy and processing science of metal additive manufacturing, Int. Mater. Rev. 61 (2016) 315–360.
[40] C.M. Gaylo, I.J. Imiolek, Method for Dispensing Of Powders, 1999. US Patent 5,934,343.
[41] N. Roy, M. Cullinan, μ -SLS of Metals: Design of the powder spreader, powder bed actuators and optics for the system, in: Proceedings of the 26th Annual International Solid Freeform Fabrication Symposium-An Additive Manufacturing Conference 2015 University of Texas at Austin, Austin, TX 134 155.
[42] M. Vaezi, S. Chianrabutra, B. Mellor, S. Yang, Multiple material additive manufacturing–part 1: a review: this review paper covers a decade of research on multiple material additive manufacturing technologies which can produce complex geometry parts with different materials, Virtual Phys. Prototyp. 8 (2013) 19–50.
[43] Y.-C. Hagedorn, Manual for SLM research equipment: AconityLab, Technical Report, Fraunhofer-Institute for Laser Technology (ITL), Aachen, Germany, 2015.
[44] A. Budding, T.H. Vaneker, New strategies for powder compaction in powder-based rapid prototyping techniques, Procedia CIRP 6 (2013) 527–532.
[45] U.S. Government Accountability Office, Weapon systems cybersecurity: DOD just beginning to grapple with scale of vulnerabilities, Technical Report, U.S. Government Accountability Office, Washington, D.C., 2018.
[46] Department of Homeland Security/Industrial Control Systems Cyber Emergency Response Team, ICS-CERT: Overview of cyber vulnerabilities, 2018.
[47] GE Oil & Gas, Top 10 cyber vulnerabilities for control systems, Technical Report, GE Oil & Gas, 2016.
[48] Y. Shanjani, E. Toyserkani, Material spreading and compaction in powder-based solid freeform fabrication methods: mathematical modeling, in: Proceedings of the 19th Annual International Solid Freeform Fabrication Symposium, SFF, volume 2008, pp. 399–410.
[49] A. Zocca, C.M. Gomes, T. Mühler, J. Günster, Powder-bed stabilization for powder-based additive manufacturing, Adv. Mech. Eng. 6 (2014), 491581.
[50] C.K. Chua, K.F. Leong, 3D Printing and Additive Manufacturing: Principles and Applications (with Companion Media Pack) of Rapid Prototyping, fourth ed., World Scientific Publishing Company,, 2014.
[51] P.J. DePond, G. Guss, S. Ly, N.P. Calta, D. Deane, S. Khairallah, M.J. Matthews, In situ measurements of layer roughness during laser powder bed fusion additive manufacturing using low coherence scanning interferometry, Mater. Des. 154 (2018) 347–359.
[52] R.C. Crean, Benchmarking DoD Use of Additive Manufacturing and Quantifying Costs, Technical Report, Air Force Institute of Technology Wright-Patterson AFB United States, 2017.
[53] T.G. Spears, S.A. Gold, In-process sensing in selective laser melting (slm) additive manufacturing, Integr. Mater. Manuf. Innov. 5 (2016) 2.
[54] E.J. Parteli, T. Pöschel, Particle-based simulation of powder application in additive manufacturing, Powder Technol. 288 (2016) 96–102.
[55] S. Haeri, Y. Wang, O. Ghita, J. Sun, Discrete element simulation and experimental study of powder spreading process in additive manufacturing, Powder Technol. 306 (2017) 45–54.
[56] D. Nasato, T. Pöschel, E. Parteli, Effect of vibrations applied to the transport roller in the quality of the powder bed during additive manufacturing, in: Proceedings of the International Conference on Additive Technologies, Nürnberg, Germany, pp. 29–30.
[57] A. E606/E606M-12, Standard test method for strain-controlled fatigue testing, 2012.
[58] P. Nezhadfar, R. Shrestha, N. Phan, N. Shamsaei, Fatigue behavior of additively manufactured 17-4 pHstainless steel: synergistic effects of surface roughness and heat treatment, Int. J. Fatigue 124 (2019) 188–204.
[59] Sheet, Strip, Astm a693–16, standard specification for precipitation-hardening stainless and heat-resisting steel plate, 2016.
[60] A. du Plessis, I. Yadroitsava, I. Yadroitsev, Effects of defects on mechanical properties in metal additive manufacturing: a review focusing on x-ray tomography insights, Mater. Des. 187 (2020), 108385.
[61] N. MSFC-STD, et al., Specification for control and qualification of laser powder bed fusion metallurgical processes (2017).
[62] R. Shrestha, J. Simsiriwong, N. Shamsaei, Fatigue behavior of additive manufactured 316l stainless steel parts: effects of layer orientation and surface roughness, Addit. Manuf. 28 (2019) 23–38.
[63] R.I. Stephens, A. Fatemi, R.R. Stephens, H.O. Fuchs, Metal Fatigue in Engineering, John Wiley & Sons,, 2000.