INVITED PAPER

A Survey of Cybersecurity of Digital Manufacturing

This article presents and discusses the cybersecurity risks in the emerging digital manufacturing (DM) context, assesses the impact on manufacturing, and identifies viable approaches to secure DM.

By Priyanka Mahesh, Akash Tiwari, Chenglu Jin, Panganamala R. Kumar, *Life Fellow IEEE*, A. L. Narasimha Reddy, *Fellow IEEE*, Satish T. S. Bukkapatanam, Nikhil Gupta, *Associate Member IEEE*, and Ramesh Karri, *Fellow IEEE*

ABSTRACT | The Industry 4.0 concept promotes a digital manufacturing (DM) paradigm that can enhance quality and productivity, which reduces inventory and the lead time for delivering custom, batch-of-one products based on achieving convergence of additive, subtractive, and hybrid manufacturing machines, automation and robotic systems, sensors, computing, and communication networks, artificial intelligence, and big data. A DM system consists of embedded electronics, sensors, actuators, control software, and interconnectivity to enable the machines and the components within them to exchange data with other machines, components therein, the plant operators, the inventory managers, and customers. This article presents the cybersecurity risks in the emerging DM context, assesses the impact on manufacturing, and identifies approaches to secure DM.

KEYWORDS | Digital manufacturing (DM).

Manuscript received May 10, 2020; revised August 21, 2020; accepted October 11, 2020. Date of publication November 3, 2020; date of current version March 23, 2021. The work of Priyanka Mahesh, Chenglu Jin, Nikhil Gupta, and Ramesh Karri was supported in part by the National Science Foundation Cyber-Physicaln Systems under Grant CMMI-1932264 and in part by NSF under Grant DGE-1931724. The work of Chenglu Jin was also supported in part by the NYU Center for Cybersecurity and in part by the NYU Center for Urban Science and Progress. The work of Panganamala R. Kumar was supported in part by the NSF Science & Technology Center under Grant CCF-0939370, in part by NSF under Grant CCF-1934904, in part by the U.S. Army Research Office under Contract W911NF-18-10331, in part by the U.S. Army Research Laboratory under Cooperative Agreement Number W911NF-19-2-0243 and Contract W911NF-19-2-0033, in part by the U.S. Office of Naval Research (ONR) under Contract N00014-18-1-2048, and in part by the Department of Energy under Contract DE-EE0009031. The work of A. L. Narasimha Reddy was supported by the Qatar National Research Foundation under Grant 9-069-1-018. The work of Satish T. S. Bukkapatanam was supported in part by the National Science Foundation under Grant CMMI-1432914 and Grant S&AS INT-1849085 and in part by the Texas A&M University's X-Grants Program. The work of Nikhil Gupta and Ramesh Karri was supported in part by the NYU Center for Cybersecurity. The work of Ramesh Karri was supported in part by the NYU-AD Center for Cybersecurity. *(Corresponding author: Chenglu Jin.)*

Priyanka Mahesh is with the Division of Programs in Business, New York University, Brooklyn, NY 11201 USA (e-mail: pm2929@nyu.edu).

Akash Tiwari and **Satish T. S. Bukkapatanam** are with the Department of Industrial and Systems Engineering, Texas A&M University, College Station, TX 77843 USA (e-mail: akash.tiwari@tamu.edu; satish@tamu.edu).

Chenglu Jin is with the Center of Urban Science and Progress and Center of Cybersecurity, New York University, Brooklyn, NY 11201 USA (e-mail: chenglu.jin@nyu.edu).

Panganamala R. Kumar and **A. L. Narasimha Reddy** are with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843 USA (e-mail: prk@tamu.edu; reddy@tamu.edu).

Nikhil Gupta is with the Department of Mechanical and Aerospace Engineering, New York University, Brooklyn, NY 11201 USA (e-mail: ngupta@nyu.edu).

Ramesh Karri is with the Department of Electrical and Computer Engineering, New York University, Brooklyn, NY 11201 USA (e-mail: rkarri@nyu.edu).

Digital Object Identifier 10.1109/JPROC.2020.3032074

I. INTRODUCTION

Digitalization of manufacturing aided by advances in sensors, artificial intelligence, robotics, and networking technology is revolutionizing the traditional manufacturing industry by rethinking manufacturing as a service. Concurrently, there is a shift in demand from high-volume manufacturing to batches-of-one, custom manufacturing of products [1]. While the large manufacturing enterprises can reallocate resources and transform themselves to seize these opportunities, the medium-scale enterprises (MSEs) and small-scale enterprises with limited resources need to become federated and proactively deal with digitalization. Many MSEs essentially consist of general-purpose machines that give them the flexibility to execute a variety of process plans and workflows to create one-off products with complex shapes, textures, properties, and functionalities. One way the MSEs can stay relevant in the next-generation digital manufacturing (DM) environment is to become fully interconnected with other MSEs by using the digital thread and becoming part of a larger, cybermanufacturing business network [2]. This allows the MSEs to make their resources visible to the market and continue to receive work orders.[1] Digitization will also enhance compliance with the larger industry and customers in terms of

[1]MSEs serve as suppliers to OEMs and other parts of the manufacturing supply networks.

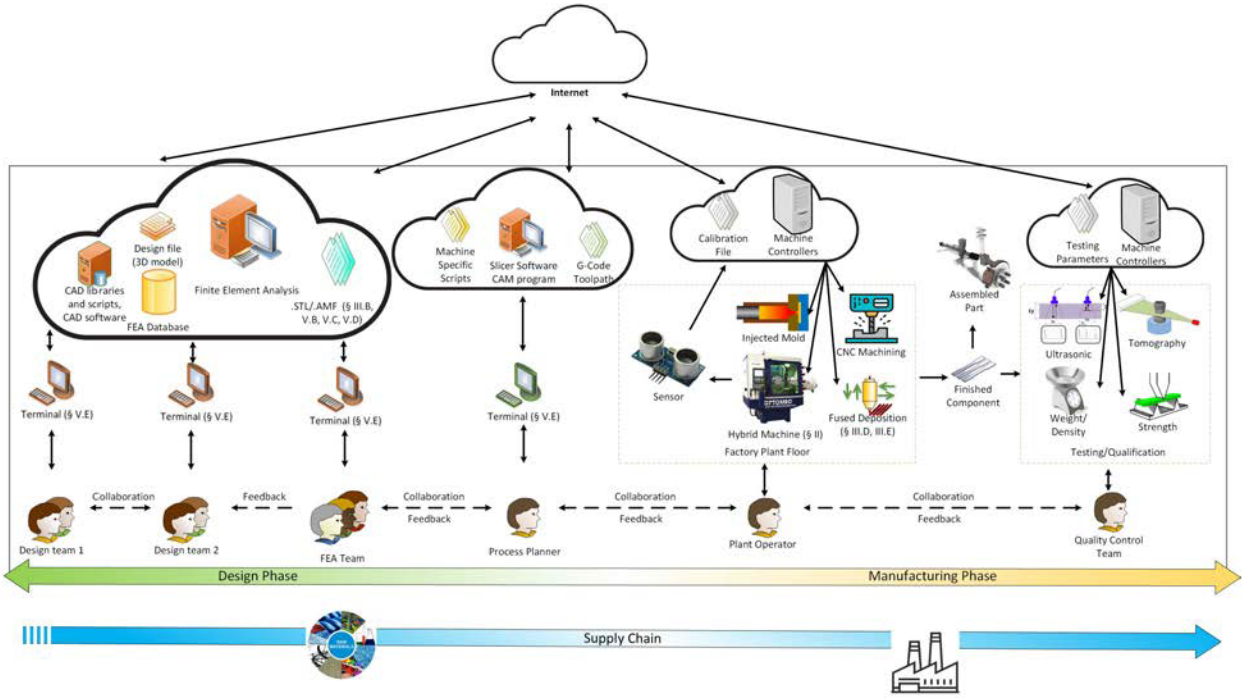

Fig. 1. ***Representative process workflow in DM systems. The workflow is broadly divided into design and manufacturing phases. The design teams, finite-element analyst (FEA) teams, and process planners come up with designs and manufacturing processes. The plant operators operate DM machines, and the finished components are tested by quality control teams using various testing methods. In future DM systems, the workflow, including design and manufacturing phases, will run in clouds since they provide flexibility, reliability, and connectivity. Also, this new paradigm of DM systems comes with security concerns that we will address in this article. In this figure, we explicitly point to (sub)sections in this article where the topic is addressed.***

technology standards and practices and access resources and services available through the interconnected digital supply chain network (DSN).

In the emerging DM, timeliness of information is important for lean production, as well as quality and productivity assurance. Digitization creates communication channels across vendors and OEMs, on the one hand, and between the various machines and processes inside an MSE, on the other hand. DM requires the integration of cyber (computing and communications) resources with the physical resources in the manufacturing process and supply chain. Continuous streaming of data from sensors at various locations in the manufacturing plant (e.g., individual machines and the network of machines) informs the data-driven decision-making that guides design modifications, calibrates manufacturing methods, and programs the robot tasks and paths that they navigate the manufacturing floor. Securing such a distributed and connected cyber–physical system against cyberattacks requires developing novel approaches that are tailored to the threats faced by such systems. The cyberattacks can range from sabotage of product quality and intellectual property theft to ransomware. The attack surface, threat vectors, and solutions need to be analyzed to enable a secure, resilient, and scalable next-generation DM.

Traditionally, manufacturing plants have been siloed and naturally create air gaps making them secure [3]. On the one hand, DM exploits the information from various sensors and devices to streamline the process and material flow. On the other hand, the distributed and collaborative nature of DM exposes it to risks that come with the connectivity required to implement DM. A typical DM process workflow is illustrated in Fig. 1. A large part of the process before the actual manufacturing step is completely digital and relies on computational resources and computer networks for design, simulation, and programming the controllers of the manufacturing machines. The DM system may consist of additive, subtractive, and hybrid manufacturing (HM) machines. This process flow requires connectivity throughout the process chain. However, connectivity poses a security risk that needs to be addressed by traditional and novel cybersecurity solutions that apply to various steps of the process flow. This article presents the hybrid machine (HM) tool as an archetype for DM, analyzes the cybersecurity risks, develops an attack taxonomy, and proposes novel solutions for the DM cyber–physical system.

This article is organized as follows. Section II presents an HM cell, a building block of DM, and uses it to discuss vulnerabilities. A taxonomy of threats for DM and attack case studies are discussed in Section III.

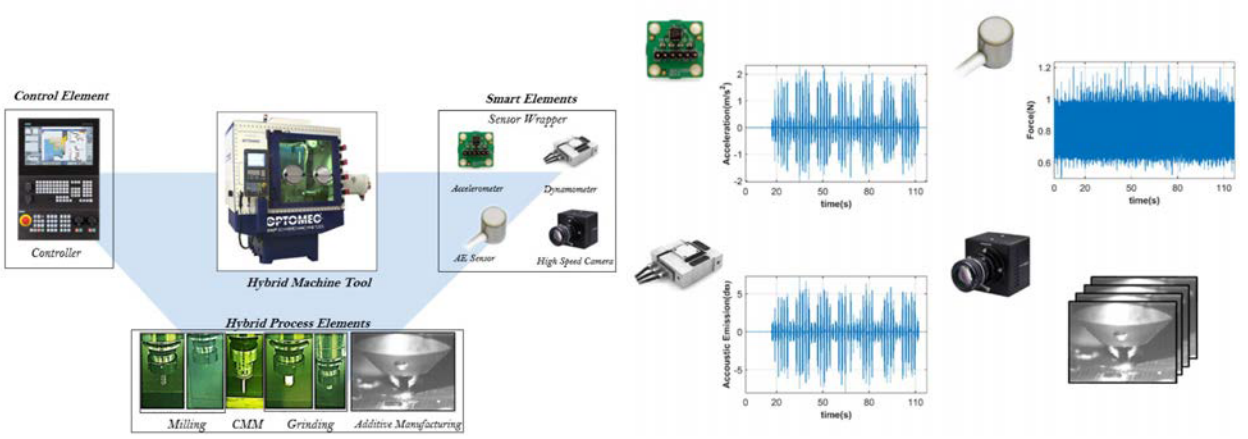

Fig. 2. *(a) Texas A&M University's Smart HM Tool with its constituent elements. (b) Data streams collected from the sensor wrapper of the smart element [11].*

A survey of existing taxonomies in DM systems is presented in Section IV. Section V demonstrates how novel manufacturing-unique defenses can mitigate the attacks. Section VI discusses lessons learned from state of the art in DM security and research challenges.

II. HYBRID MACHINE TOOL: A DM BASIC BLOCK

HM tools are excellent archetypes of a DM building block. They make a case to explain how traditional manufacturing is transforming into DM. This resulting transformation, however, creates additional attack vectors for DM. The case of an HM tool, therefore, allows identifying, analyzing, and addressing the vulnerabilities from these attack vectors before the widespread adoption of DM.

The most common configurations of HM tools combine additive and subtractive manufacturing processes on the same platform [4] so that process chains spread across multiple machines (possibly located at different enterprises) can be carried out within a single machine. This is especially beneficial for the fabrication of custom components, as it results in reduced setup times, material costs, and error in handling. HMs have been increasingly considered in the industry for remanufacturing and repair of high-value components and in manufacturing parts that require complex process chains. Pipe casings for offshore oil extraction have several features (e.g., fins and spiral coatings) on the surface critical. The use of an HM for such a part was proved to reduce the material cost by ~97.2% in addition to the tooling cost [5]. An HM can customize implants by milling the implant–abutment interface followed by printing the abutment custom-designed for a patient [6], create novel injection molds with improved cooling performance over traditional fabrication methods [7], and enable surface patching in the mold and die repair [8] and turbine blade repair [9].

More pertinently, HM tools are, oftentimes, integrated with the state-of-the-art digital information technology (IT) systems (e.g., software and data warehouse) and operational technology (OT) systems (e.g., sensors and communication channels) to work in tandem to produce the desired part [10]. Integration of digital technologies provides the connectivity and computational infrastructure for enabling HM tools to be part of a DM network. Connectivity includes the feedback loops within the machines based on the machine state and feedback loops based on the observations of the process from an observer external to the machine. It also refers to the communication channels among the manufacturing resources within the manufacturing cell. The computational infrastructure supports data collection, storage, analysis, and decision-making elements of manufacturing. While connectivity and computational infrastructure improve the utilization of the manufacturing resources, they can be attack vectors for internal and external adversaries.

Due to the use of IT/OT technologies in these HM tools, much of the threats these systems face are similar to those of the conventional IT/OT technologies. However, the sabotaging effect of these threats poses direct safety and productivity challenges to the manufacturing enterprise. For example, traditional cybersecurity attacks on legacy systems that are connected to IT/OT technologies in the recent past have resulted in machine downtime, idle time, and reduced reliability of the system, causing massive monetary losses to the enterprise.

Vulnerable nodes in the supporting infrastructures must be identified and secured to realize the economic and efficiency benefits of DM. In the following, we describe key components of our use-case HM and the possible vulnerabilities in the context of DM. The discussion on the identified vulnerabilities of the HM serves as a motivation for the development of taxonomy and the solutions to the vulnerabilities for DM in the rest of this article.

A. Transforming an HM as Part of a DM Ecosystem

Fig. 2(a) illustrates an HM located at Texas A&M University. It consists of three key elements: the hybrid process

element, the controller, and the smart element [11]. The hybrid process elements include the milling tools, the coordinate measuring touch probe, grinding tools, and the laser-engineered net-shaping process that employs a directed energy deposition printing head. These tools support consecutively running the additive and subtractive manufacturing operations within a process cycle. The control element allows the user to interface with the hybrid process element and the execution of process cycles. It acts as an internal observer that gathers the internal state of the machine (e.g., position, feed rate, laser power, and spindle speed) and sends actuation signals based on the instructions specified by the operator. The smart elements include sensors with supporting hardware. Hardware and software that enable data acquisition from the sensors are termed the sensor wrapper [12], [13]. The sensor wrapper implementation is composed of high-resolution sensors (accelerometers, acoustic emission sensors, dynamometers, and a high-speed camera), data acquisition system, signal conditioning elements, such as filters and amplifiers, and human–machine interface. The sensor signals allow the process states to be estimated during a process cycle for feedback control [14], as well as for providing observations from the perspective of an external observer (e.g., the operator) [15]. The three elements of the HM work in harmony to enable refined control over the process. Such harmony is possible due to the coordination among process hardware and Internet-of-Things (IoT) devices in the computing and the communication channels.

The very capabilities of an HM tool that allows fabrication of parts with complex geometries and functionalities (as it combines multiple manufacturing processes into a single platform), as noted earlier, create complexities in the process cycles and allow for faults to creep into the process. While process faults are inevitable for any complex system, one needs to execute corrective measures to mitigate the effects of these faults. Monitoring the process as an external observer is, therefore, essential in operating the HM tool. The hybrid elements can allow the operator to take corrective actions when a fault is observed. For example, a defect created in the part during the additive manufacturing cycle can be undone by executing a subtractive cycle over the layer with the defect before resuming the additive cycle. Taking corrective measures after a fault occurs leads to loss in manufacturing lead time and physical resources. The smart elements can intervene to save time and resources by informing the operator about an imminent fault. This is possible by using the information that the sensor wrapper collects. Fig. 2(b) illustrates the time-synchronized data stream for an additive manufacturing cycle collected over 120 s. The data stream for the force signals is densely packed; therefore, an adjacent plot represents the force plot for a 0.05-s window. The information generated from the sensor wrapper is voluminous. The data streams from acoustic emission, the accelerometer, and the force transducers over a 120-s period generate 89.5, 44.7, and 8.92 MB of data, respectively. The high-speed camera generates 110-GB streaming image data over the 120-s period.

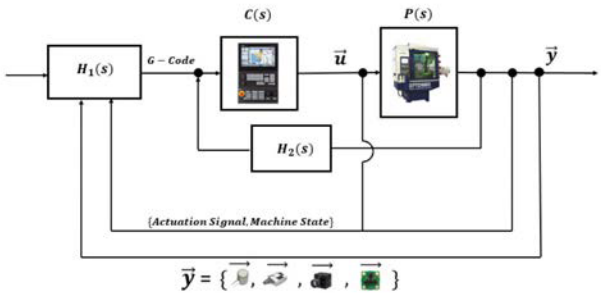

Fig. 3. *Closed-loop control block diagram of the HM tool.*

The controller (internal observer) observes and controls the HM tool based on the machine state. The external observer, however, observes the process and takes corrective measures. This establishes two feedback loops. The controller sends actuation signals to the HM tool based on instructions within the G-code (subject to change based on the external observations of the process) that is sent by the operator. The G-code file contains high-level instructions meant to be executed on the HM. The operator may observe the information stream and take corrective measures by sending new instructions when the information stream resembles the nascent stages of an imminent fault, thereby overcoming the fault altogether. This is illustrated in Fig. 3 as a closed-loop controller.

The refined control over the process is, thus, achieved by a feedback control that is based on both the information on the machine state and the information about the process. The feedback control entails collecting, processing, and analyzing voluminous information to derive inferences about the process in real time. This requires computing on large amounts of information in a timely manner and may resort to AI methods to process the information. This makes the need for computing infrastructure apparent. Factors influencing the computing infrastructure include the environment where computing happens, the latency of the computation, the type of data, and the amount of data.

In online quality control where the corrective and prognostic measures are to be taken, information from the sensor is processed in real time to infer about the state of the process, and therefore, data storage and computing resources must be in the vicinity of the process to avoid latency. Another situation for online quality control is where the latency of the calculation is not an issue, but there are no computational resources on the shop floor. Then, the computational services offered by cloud platforms are leveraged. For offline quality control, where a defect in the part is identified later, the investigator may use data collected during the process to identify process faults—missed by online quality control—that may have led to a defect.

Thus, the computing infrastructure is dictated by the requirements of the manufacturing cell. Data storage,

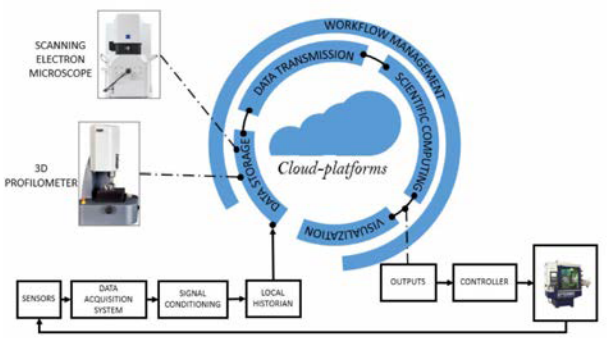

Fig. 4. *Cloud computing platform for an HM cell.*

computations, and transmission of the calculations to the destination are essential to establish the closed-loop control. Since manufacturing shop floors may be limited in their capacity to cater to such requirements efficiently, cloud computing infrastructure could be economical and efficient. Cloud computing infrastructure is mature and reliable for application in the HM cells. Cloud service providers (e.g., Amazon Web Services and Rackspace) have integrated the elements of storage, computation, and communication. Amazon provides storage services (the Elastic Block Store) and hosts well-known software (R, MATLAB, and Mathematica) as virtual machines (VMs). All computations can be visualized on the cloud VMs with software, such as Tableau. The workflow in the cloud can be orchestrated by scientific workflow software such as Kepler.

Fig. 4 illustrates the cloud as central to online and offline quality control for the HM cells. Signals collected by the sensors from the plant are stored in a local historian and uploaded to the cloud for storage. From this point, scientific workflow management software handles the flow of data. The computing VM is activated to receive and analyze the data and calculate new control outputs that are downloaded onto the controller, closing the loop. For offline quality control, scanning electron microscopes, and 3-D profilometers in the HM cell inspect the part. These instruments download process-related data streams from the cloud and identify the anomalies in the process to explain defects in the part.

B. Vulnerabilities in an HM Tool

Although the HM tool is only one of the multiple resources of a DM process workflow, this critical resource has multiple vulnerable nodes. Cardenas *et al.* [16] identified possible attacks on the cyber–physical system and discussed theoretical formulation for the attacks to be addressed and the requirements of a secure cyber–physical system using extant theory in controls, information security, and network security. The issues identified in [16] were, however, generalized for a cyber–physical system. Likewise, specific to securing a DM system, Fig. 5 identifies eight vulnerable nodes in the closed-loop control diagram, as shown in Fig. 3.

1) The first class of vulnerabilities can be used to manipulate the instructions sent to the controller/plant. The adversary can intervene at nodes 1 and 2. At node 1, the adversary modifies the instruction (typically a G-code) sent by the operator. The adversary may intervene at node 2 and tamper with the actuation signal sent to the plant.
2) The second class of vulnerabilities is the replay attack. At node 4, since the actuation signal is monitored, the replay attack can trick the external observer into thinking that the instructions are executed as per specifications.
3) The third class of vulnerabilities arises due to the feedback loops. The internal observer (controller) and the external observer use the machine state and process information to send new instructions. The adversary may intervene at nodes 3, 5, and 6 to relay false information on the machine state and process resulting in erroneous feedback control. This sabotages the process of online quality control.
4) The last class of vulnerabilities is identified at nodes 7 and 8. Node 7 corresponds to the side-channel attacks leading to IP theft. Node 8 represents indirect sabotage of the system in place due to counterfeit production.

In Fig. 5, the block $H_2(s)$ within the innermost feedback loop is a transfer function block that estimates the machine state (e.g., spindle speed, bed and tool position, and laser power) based on the measurements from built-in sensors, such as optical scales and other motion trackers. The controller is continually tracking the error between the reference signal (generated from the interpretation of the instructions in the G-code) and the feedback signal of the estimated machine state from the HM tool. The reference signal specifies what the machine state should be at any given point in time as per the instructions in the G-code. The controller sends actuation signals ($\vec{u}$) to the HM tool that nullifies this error, thus bringing the machine state to the reference state. Injection attacks performed at node 2 include false actuation signals that drive the machine to

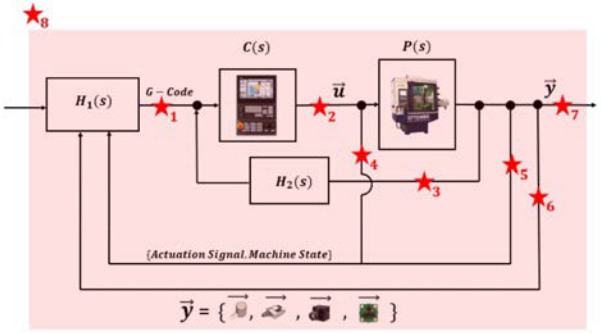

Fig. 5. *Vulnerable nodes in an HM tool. The vulnerable nodes are identified by a red star, indexed by a subscript.*

undesirable states resulting in process faults. In the case of a man-in-the-middle attack (replay attack) carried out at node 3, the transfer function block receives incorrect observations (contrary to the actual observations made by the optical scales within the machine), leading to a trail of miscalculations of the estimate of the machine state, error, and, therefore, the actuation signal itself, therefore again resulting in the machine being driven to undesirable states and, thus, eventually faults in the process.

The block $H_1(s)$ in the outer feedback loop estimates the state of the process based on information from a sensor wrapper [17] and generates new instruction sets as required. Typically, the transfer functions tend to be nonlinear operators to fuse information on the nonlinear and nonstationary dynamics underlying the measured signals to detect changes for corrective actions [18] or anticipate anomalies for prognostication and anticipatory control [19]. The state of the process is defined in terms of the thermomechanical state variables that capture the process that determines the transformation of the geometry, morphology, and the microstructure of the part as it is being realized, as well as the health of the machine and its components. Information derived from the sensor wrapper may include thermal history, acoustic emission, and vibrations. The new set of instructions generated based on the estimated process state includes reduction of laser power for the DED process if the desired melt-pool geometry, thermal history, and/or microstructure are not realized, remanufacturing of layers due to part distortions, and stopping the machine for preventive maintenance due to tool wear. Information on thermal history can be used to predict part deformation during additive manufacturing cycles [20]. Vibration data in a grinding process can predict surface quality [17]. Acoustic emission signals can be used to predict the cutting conditions for orthogonal cutting experiments [21]. Such applications of the sensory information from the process allow for the generation of prognosis-based instructions to the controllers.

The outer feedback loop tracks the process and serves the purpose of minimizing the process deviation and averting any process anomaly. Attacks on the outer feedback loop have a direct consequence on the inner feedback loop since instructions generated by the outer feedback loop are direct inputs to the inner feedback loop. Man-in-the-middle attacks carried out at node 4, 5, or 6 yield incorrect process state estimations and, therefore, wrong prognosis, leading to the generation of incorrect instructions to the controller. Injection attacks at node 1 serve the effect of controllers in the inner feedback loop tracking reference signals generated from the adversary's instructions, obviating the efforts of the prognosis-based instructions from the external feedback loop.

Side-channel attacks at node 7 involve adversaries monitoring the footprint generated by the process. These footprints, for example, can be captured using a microphone that collects the acoustic sounds produced by the machine when in operation [22] or by tapping into the sensor data and other signals in the outer feedback loop. Adversaries that track these footprints from unmonitored channels could reverse-engineer the product and create counterfeits that could find their way into the supply chain of critical components. Although the effect of a counterfeited product is not as pronounced in the manufacturing of low-volume, high-value customizable parts as is the case where these HMs are put to use, the existence of such threats cannot be overlooked. Counterfeit products do not qualify the strict quality standards causing devastation in critical applications. They also sabotage brand reputation. Counterfeiting practices threaten the entire HM tool that is meticulously put in place with its feedback loops to ensure strict part quality and highlighted as node 8.

The aforementioned vulnerabilities identified in Fig. 5 for the HM tool have been independently exploited in other DM systems such as FDM 3-D printers. Various attacks have been devised to exploit the vulnerability of, and sabotage, such systems. Attacks that resemble the exploitation of the vulnerabilities at the nodes in Fig. 5 include: Belikovetsky *et al.* [23] demonstrated the modification of G-code (node 1) that resulted in undetectable (node 3) malicious printing sequences being executed; Moore *et al.* [24] developed malicious firmware that modifies original actuation commands to change the 3-D printing parameters (node 2,3) that go unnoticed; and attacks at nodes 4–6 resemble the attacks at node 3; however, they differ in the purpose to which the feedback is put to use. These feedbacks are established for more advanced purposes of sending corrective G-code based on a real-time process state and sensor data. Attacks at these nodes, although similar to those at node 3, still remain to be demonstrated. Chhetri *et al.* [25] demonstrated an acoustic emanation-based side-channel attack, leading to counterfeit by reverse engineering and, therefore, IP issues (nodes 7 and 8). Other similar attacks are presented in the context of the developed taxonomy and discussed as case studies later in Section III.

Vulnerabilities outside of the specified schema in Fig. 5 include those that are innate to any software and data management systems used to interface with the operational technologies, as well as those occurring across a wider supply chain [26] that employs DM and the process chains enabled by them. Examples include ransomware outbreaks at TSMC (WannaCry) [27] in 2018 and Norsk Hyrdo (LockerGoga) [28] in 2019, forcing the companies either to halt operations or switch to the manual operation costing an estimated $180M and $71M, respectively.

III. DIGITAL MANUFACTURING: TAXONOMY OF THREATS

Cyber-enablement and interconnectivity of DSNs introduce threats including financial theft and theft of IP. Some of the threats are unique to DM including digitally printing dangerous or illegal components, stealing competitor IP (e.g., the design files), modifying them, and manufacturing counterfeits or substandard components, and deny service

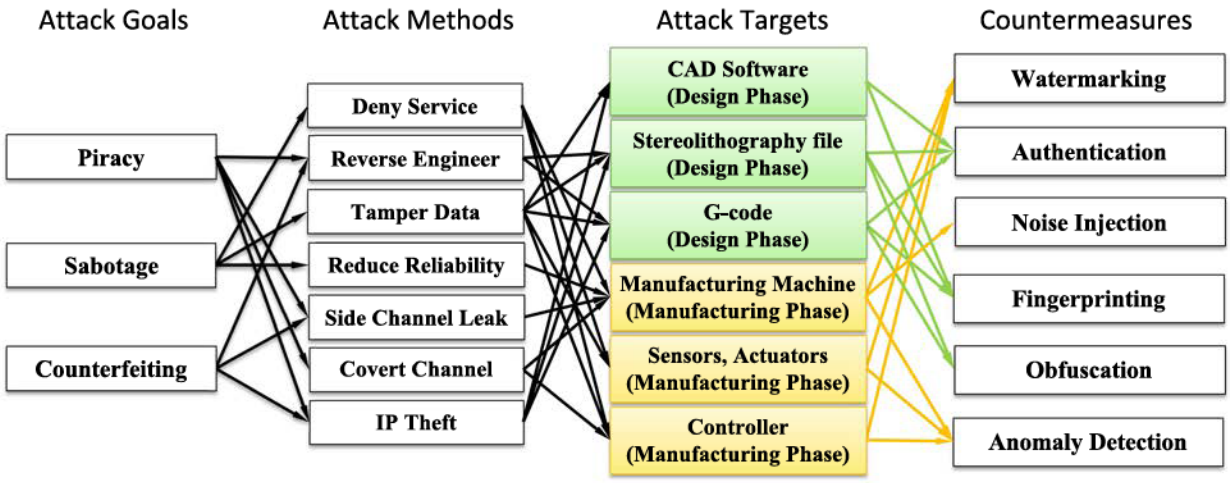

Fig. 6. *Threat taxonomy and corresponding security measures. The left column (first) shows the goals of attackers, the second to the left column describes possible attacks, the third column shows the targets of attackers, and the last (right) column shows countermeasures. The arrows from the first column to the second column show how an attacker can achieve different goals using various attacks, and the arrows from the second column to the third column show how each attack can be applied to each target. Finally, the arrows from the third column to the fourth column show how each component in DM systems can be protected by countermeasures.*

by taking manufacturing plants or critical parts of the manufacturing plants (e.g., printers) offline. The attackers may have different motivations, including: 1) nation-state actors; 2) organized criminals; 3) politically, socially, or ideologically motivated hacktivists; 4) hackers with financial gain or sabotage intent; 5) competitors; and 6) malicious insiders. The motivation of the attacker, resources available, and the damage caused in each category can be different and should be a part of the threat analysis.

A. Taxonomy of Threats

Fig. 6 shows a taxonomy of attacks, attack goals, methods, targets, and the countermeasures. Attackers can choose their attack method based on their goals and targets.

Attack goals: These can be grouped into three classes.

1) **Piracy** refers to illegally copying or fabricating a design that violates the copyright of the original design.
2) **Sabotage** entails introducing defects in the product, damaging machines, or interfering with the processes to cause delay or damage.
3) **Counterfeiting** attacks are defined as illegal attempts to imitate authentic products.

Attack methods: These can be characterized into seven categories.

1) **Denial-of-service (DoS)** attacks prevent access to the manufacturing systems.
2) **Reverse engineering:** Given a file or physical product as the output of a design/manufacturing stage in the supply chain, reconstruct files in a previous step.
3) **Data tampering** refers to the tampering of data read/written, stored, and sent/received by the manufacturing system.
4) **Reliability degradation** refers to a reduction in production yield, on-time performance of systems, and an unpredictable decrease in the service life of the part.
5) **Side-channel leakage** refers to reconstructing the product design and manufacturing conditions side-channel information measured during the manufacturing (e.g., acoustic, thermal, electromagnetic, and vibration).
6) **Covert channel** attacks are when an insider intentionally sends secret information to the outside receiver while remaining detected or noticed by others.
7) **IP theft** directly stealing digital proprietary information (e.g., design files) from the computers or machines in manufacturing systems. Often, such information can be used for developing competing products.

Attack targets: Based on the supply chain of DM system presented in Fig. 1, we first largely classify the targets into design phase targets (marked in green in Fig. 6) and manufacturing phase targets (yellow in Fig. 6). We identify three targets in each phase as explained in the following.

1) **CAD software** is widely used to facilitate product design by a single designer or by a collaborative design team. It can be targeted by an attacker in a data tampering attack such that the CAD software will not generate the correct files as expected.
2) **Stereolithography** also known as STL file format is a widely used generic format that describes the surface

geometry of a 3-D object by a tessellation scheme. The file resolution can change product quality.

3) **G-code** is the numerical control programming language. G-code files define the processing parameters, such as tool path, nozzle temperature, laser power, and material type. It stores crucial design information, and so, its integrity and confidentiality are critical.
4) **Manufacturing machines** are the physical machines that manufacture the products in the physical world.
5) **Sensors and actuators**: In a manufacturing control feedback loop, sensors and actuators are responsible for measuring and driving the physical process, respectively.
6) **Controllers** in a feedback loop carry out the decision-making process to control the behavior of the machines, and the G-code files define the controller behavior.

Countermeasures are of six categories.

1) **Watermarking** is a security technique that embeds inseparable and hidden information in signals/files such that owners of the original signals/files can use the hidden information to prove their ownership or the authenticity of the signals/files.
2) **Authentication** helps identify if they are interacting with the authentic copy of a file/message/identity.
3) **Noise injection** refers to the countermeasures that inject noise signals in its side-channel information leakage, so an attacker will not be able to retrieve meaningful secret information from side-channel information measurement.
4) **Fingerprinting** exploits the intrinsic characteristics of designs/machines/processes as a method to uniquely identify designs or products produced by a design file or a manufacturing machine.
5) **Obfuscation** of design files prevents designs from being understood and, thus, reverse-engineered by malicious attackers. Obfuscation introduces difficulties for an attacker to reverse-engineer a given product.
6) **Anomaly detection** can be applied to multiple layers. For example, it can be used on the controller of a manufacturing system to detect whether there are any suspicious sensor readings in the system. It can also be applied to the manufacturing machine itself to detect whether there is anything different from expected behaviors, for example, by monitoring the side-channel information leakage of the machines. Anomaly detection can also be applied to the network layer to intercept the packages in the network. It can also be applied to the products, and the products will be checked against the specification, especially a few security-critical properties will be checked explicitly.

The taxonomy presented in Fig. 6 can be used to develop defenses for various attack scenarios. For example, to prevent an attacker from tampering with the design files (e.g., STL files), a defender can embed identification codes in the design to authenticate the product. If the design is tampered with or reverse-engineered, the embedded code will be impacted and will not match with the correct one.

According to this taxonomy, we classify recent related works in Table 1. We first classify the articles based on whether they focus on attacks or defenses or both. Then, the threat models that they consider are identified. In the case that this article is a survey that covers a variety of threat models, we will leave the threat model field blank. Finally, we categorize all articles based on the attack methods that they presented or based on the defenses. Not surprisingly, most of the articles are focused on defenses. However, in order to develop a defense, the threat model that it targets overwhelmingly indicates that sabotage is the main attack goal, and the attacks are launched either to tamper with the files or for IP theft. IP theft is a major concern in DM because the design of hardware parts remains the same for many years, even decades. Revision to the designs that have been in place for so long due to design theft becomes an expensive and taxing exercise. A related issue in manufacturing is that a legitimately obtained part can be reverse-engineered and then used for unauthorized or counterfeit production leading to IP theft. The deterrence in such cases lies in the production method that cannot be easily copied or decoded. Although DoS attacks are the major concern in the financial and technology sectors, they are not the major concern in the manufacturing sector. This is because, in many large manufacturing enterprises, the manufacturing machines are maintained on a separate, protected internal network, which is then securely connected to the Internet for software or firmware updates only under supervision when the production activity is not taking place. A growing concern is the manufacturing-unique side channels (e.g., acoustics) and related attacks aided by machine learning to uncover patterns in data obtained from the multiple sensing sources, such as acoustic, thermal, power meter, and security camera sensors.

The threats listed in our taxonomy apply to all manufacturing machines, including the HMs. Attackers can sabotage the products by tampering with the control signals or instructions (e.g., the G-Code) from the operators. Attackers can steal design secrets from side-channel leaks. To explain the attacks and potential impact of the attacks on various aspects of the DM process chain, we present five case studies shown as red rows in Table 1.

B. Case Study 1: Drowned Attack on AM

Informed by the taxonomy of Fig. 6, the goal of this attack was sabotage. The attack was conducted to reduce the reliability of the part, and the attack target was design files. This attack on a 3-D printer deliberately introduced defects into the part during printing [23]. The controller PC connected to the 3-D printer was compromised by exploiting an unpatched vulnerability in WinRAR. The

Table 1 Categorization of DM Security Studies. "DoS," "Rev. Engg.," "Tamper," "Unreliable," and "Cov. Channel" Stand for "Denial of Service" "Reverse Engineering," "Tampering Data," "Reduce Reliability," and "Covert Channel," Respectively. Red Rows Are Attack Case Studies in Section III. Blue Rows Are Defense Case Studies in Section V

			Attack Goals			Attacks						
Papers	Attacks	Defenses	Piracy	Sabotage	Counterfeit	DoS	Rev. Engg.	Tamper	Unreliable	Sidechannel	Cov.channel	IP Theft
Gupta *et al.* [26]		✓		✓				✓				✓
Strurm *et al.* [29]				✓	✓			✓				
Ranabhat *et al.* [30]	✓			✓				✓	✓			
Belikovetsky *et al.* [23]	✓			✓	✓		✓				✓	
Yampolskiy *et al.* [31]		✓		✓					✓			
Wu *et al.* [32]		✓		✓				✓		✓		✓
Chhetri *et al.* [33]		✓		✓				✓	✓	✓		
Desmit *et al.* [34]	✓		✓					✓	✓			✓
Chen *et al.* [35]		✓		✓	✓							✓
Elhabashya *et al.* [36]		✓		✓				✓		✓		✓
Moore *et al.* [24]	✓			✓		✓		✓	✓			
Bracho *et al.* [37]		✓								✓	✓	✓
Graves *et al.* [38]	✓		✓	✓								✓
Yampolskiy *et al.* [39]		✓	✓				✓	✓		✓		✓
Chhetri *et al.* [40]		✓					✓	✓		✓		✓
Belikovetsky *et al.* [41]		✓	✓	✓				✓		✓		
Chhetri *et al.* [42]		✓					✓			✓		✓
Baumann *et al.* [43]		✓					✓	✓				✓
Wu *et al.* [44]	✓			✓		✓		✓				✓
Gupta *et al.* [45]	✓	✓		✓	✓			✓				✓
Moore *et al.* [46]	✓		✓	✓						✓		✓
Tsoutsos *et al.* [47]		✓					✓	✓				
Belikovetsky *et al.* [48]	✓			✓			✓	✓	✓	✓		✓
Zarreh *et al.* [49]		✓		✓		✓		✓	✓			✓
Miller *et al.* [50]		✓					✓			✓	✓	✓
Chaduvula *et al.* [51]		✓		✓	✓			✓				
Raban *et al.* [52]	✓	✓			✓			✓			✓	✓
Chen *et al.* [53]		✓			✓		✓					
Yu *et al.* [54]		✓		✓						✓		
Hoffman *et al.* [55]		✓						✓	✓			✓
Abdulhameed *et al.* [56]		✓		✓				✓				
Padmanabhan *et al.* [57]		✓							✓			✓
Prinsloo *et al.* [58]		✓		✓		✓		✓		✓	✓	
Chhetri *et al.* [59]	✓	✓								✓		
Calzado *et al.* [60]		✓					✓					
Yampolskiy *et al.* [61]	✓			✓				✓				
Ivanova *et al.* [62]					✓			✓				
Bridges *et al.* [63]		✓					✓	✓		✓		✓
Holland *et al.* [64]		✓										✓
Chhetri *et al.* [65]	✓		✓							✓		✓
Wei *et al.* [66]		✓			✓		✓					
Wu *et al.* [67]		✓		✓				✓				
Vincent *et al.* [68]		✓		✓		✓			✓	✓		✓
Riel *et al.* [69]		✓				✓				✓	✓	
Ren *et al.* [70]		✓				✓		✓			✓	
He *et al.* [71]		✓		✓		✓					✓	✓
Wu *et al.* [72]	✓	✓		✓			✓	✓	✓			
Fey *et al.* [73]		✓		✓					✓			✓
Elhabashy *et al.* [74]		✓		✓				✓				
Slaughter *et al.* [75]	✓	✓		✓				✓		✓		
Satchidanandan *et al.* [76]		✓		✓				✓				
Satchidanandan *et al.* [77]		✓		✓				✓				
Woollaston [78]	✓			✓		✓						
Satchidanandan *et al.* [79]		✓		✓				✓				
Behera *et al.* [80]		✓		✓				✓				
Wu *et al.* [81]		✓		✓				✓				
Yanamandra *et al.* [82]	✓		✓		✓							✓
Do *et al.* [83]	✓		✓	✓				✓				✓
Gao *et al.* [84]		✓	✓		✓							✓
Chhetri *et al.* [85]		✓	✓							✓		
Chhetri *et al.* [25]	✓		✓							✓		
Chen *et al.* [86]		✓			✓		✓	✓				
Song *et al.* [87]		✓			✓		✓					✓
Song *et al.* [88]	✓		✓		✓					✓		
Al Faruque *et al.* [89]	✓		✓		✓					✓		

Fig. 7. *(a) Two 3-D printed propellers. One is defective. (b) CAD model of the design. (c) Design is compromised at the joints causing in-service failure [23].*

attack decreased the fatigue life of a quadcopter propeller causing a midflight failure by manipulating the part geometry [an example shown in Fig. 7(b)]. The attack was executed in three stages: the attacker compromises the controller PC, developed a counterfeit design similar to the original design, and replaced the original design file on the victim's PC with the counterfeit design file with the manipulations shown in Fig. 7(c). A reverse shell backdoor was installed on the PC, which was used to submit jobs to the 3-D printer. This allowed the malicious software to take over the 3-D printer and execute commands by the hacker. According to our taxonomy, a variety of defenses can be applied to this scenario. Although the attacker exploited a software vulnerability, the sabotage was detected by rigorously testing the part.

C. Case Study 2: Cyberattack on Honda Auto Plant

Honda' Tokyo-based automotive production plant was forced to go offline by the self-propagating malware, WannaCry, impacting the production of about 1000 vehicles [78]. The WannaCry malware infected hundreds of thousands of computers worldwide by exploiting vulnerabilities in unpatched legacy systems [90]. The plant was shut down for 48 h to recover operations and data, as both the Industrial Control Systems (ICS) and IT networks were impacted [78]. As shown in Fig. 8, the ransomware got deployed in the plant computer network using a backdoor in an older unpatched version of the windows OS and then infected all systems in the network. According to our taxonomy in Fig. 6, the attacker, in this case, launched a DoS attack on the automotive plant by infecting and tampering with their controller computers in the control network.

D. Case Study 3: Additive Manufacturing Firmware Attack

Attackers may target the firmware of a 3-D printer. If the firmware is compromised, attackers can sabotage the system by either modifying the control or deny the service of the machines. The attacker's strategy is to exploit the firmware in order to selectively affect the integrity of printed artifacts; this approach is particularly effective in case random sample testing is applied after the artifact is printed, as it increases the chance of bypassing detection. Furthermore, any intervention to the printer firmware (especially at the bootloader level) can make the attack persistent.

There are different tactics an attacker can employ to infect the printer firmware. Most 3-D printers and HM platforms support Internet connectivity to allow remote management or troubleshooting from the manufacturer, as part of a service-level agreement with the end-users. In this case, attackers can exploit vulnerabilities in the network services running on the printer and eventually escalate their privileges on the printer. This privilege escalation can be exploited to update the printer with infected firmware in case the signed firmware updates are not

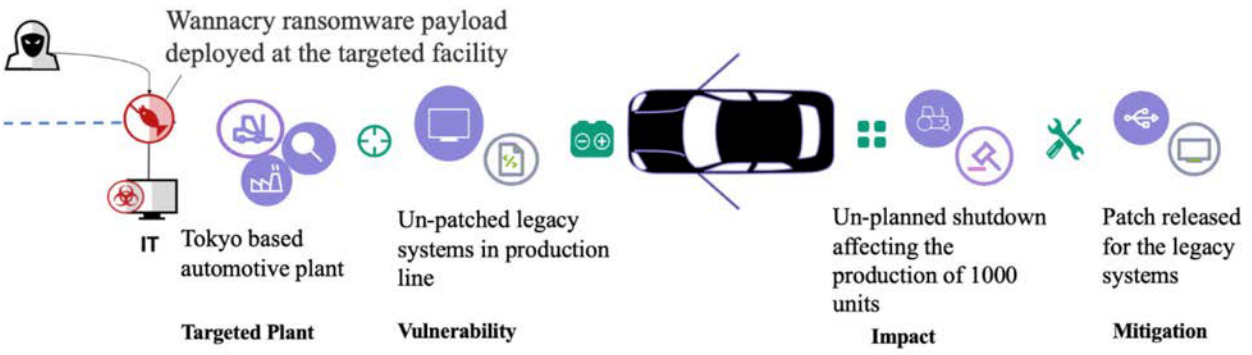

Fig. 8. *WannaCry cyberattack on the Honda automotive plant computer network [78].*

Table 2 Survey and Taxonomy of Taxonomies. The Green, Yellow, and Gray Columns Represent Computer Security, Electronic Manufacturing System Security, and Mechanical Manufacturing System Security, Respectively

	Papers ⟶	[91]	[92]	[93]	[94]	[95]	[31]	[96]	[45]	[97]	[98]	[99]	[74]	[100]	Ours
	Timeline ⟶	1994	2010	2014	2014	2014	2016	2016	2017	2017	2017	2018	2019	2020	2020
Attacks	Sabotage (Product)	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
	Sabotage (Machine)						✓			✓	✓	✓	✓		✓
	Sabotage (Environment)						✓				✓	✓			
	Information Leakage	✓	✓	✓	✓				✓	✓	✓	✓		✓	✓
	Piracy			✓		✓			✓	✓	✓	✓			✓
	Counterfeit			✓		✓			✓			✓			✓
Countermeasures	Obfuscation			✓	✓			✓							✓
	Watermarking			✓											✓
	Authentication			✓											✓
	Noise Injection			✓											✓
	Post-Deployment Monitoring				✓			✓							
	Anomaly Detection				✓			✓							✓
	Split Manufacturing			✓				✓							
	Fingerprinting			✓											✓
Metrics	Attempts to find secret			✓											
	# of Collisions			✓											
	Amount of Info. Leakage			✓											
	Detection Probability			✓											
	False Positive Rate			✓											

supported. Another attack vector that may be exploited is the input file parser within the printer. In cases where the firmware processes tool path input files (e.g., G-code files), any input sanity vulnerability may allow memory corruption and execution flow hijacking. In this case, attackers can inject malicious routines through input files or reuse existing code within the firmware memory space.

As soon as an attacker has infected the printer firmware, they can easily control the actuators of the printer (e.g., print head motors, extruder valves, or laser operation). By controlling these actuators in a judicious fashion, attackers can inject physical property attacks [24]. Furthermore, attackers can also perform a DoS attack on the printer so that legitimate users can no longer use the 3-D print service.

E. Case Study 4: Dissolvable Support Material

This attack is applicable to multihead/multimaterial printers, where support material can be printed in addition to the build material. Typically, the support material is dissolvable, and as soon as the part is printed, it is submerged into an oxidizer (e.g., acid) to separate it from the build material [45]. The attack consists of maliciously replacing build material in the interior details of the 3-D part with support material. Then, as soon as the print is complete and the solvent removes all support material, it would also carve hollow spaces within the part, where the original build material was replaced. The effect of this attack is to reduce the structural integrity of the part since the internal structure will no longer be solid. According to our taxonomy in Fig. 6, this attack can be classified either as sabotage on DM machine or the design files set up for multimaterial printing in order to reduce the reliability of the products.

IV. SURVEY AND TAXONOMY OF TAXONOMIES IN DIGITAL (MANUFACTURING) SYSTEMS

Many relevant cybersecurity taxonomies have been proposed in the past, for example, in the area of general cybersecurity [91], electronic manufacturing (supply chain) security [92]–[96], [100], and mechanical manufacturing system security [31], [45], [74], [98], [99]. In this section, we will go through the history and present a comprehensive study of security taxonomies for manufacturing systems. A comparison is shown in Table 2.

A taxonomy of malicious computer software was introduced in [91]. In the early days of cybersecurity research, the main goals of cyberattacks were to either take over the control of a computer or steal secret information from a computer system. They are still the main focuses of security research nowadays. However, with the introduction of cyber–physical systems, the scope of attacks has been significantly extended.

In 2010, the threat landscape is extended to the underlying hardware of a computer system, and Karri *et al.* [92] proposed a taxonomy of hardware Trojans in ICs. The taxonomy shows how a chip can be maliciously designed or fabricated to jeopardize the security of the whole computer system.

Rostami *et al.* [93] presented a taxonomy covering a much broader scope of hardware supply chain security. The taxonomy includes a variety of attacks, including sabotaging the integrated circuits (ICs) and computer systems, stealing information, IC design piracy, and IC counterfeiting. In addition to attacks, it also discusses countermeasures and security metrics. Most importantly, in their taxonomy, the connections between countermeasures and corresponding attacks are presented clearly. This provides a comprehensive overview of the field, which greatly facilitates the readers in understanding how to

defend against certain attacks. Our taxonomy follows the structure presented in [93] as a comprehensive overview of the field of cybersecurity of DM systems.

In 2014, Bhunia *et al.* [94] extended the taxonomy of hardware Trojans in electronics manufacturing and added a classification scheme for countermeasures of hardware Trojans. The general categories of countermeasures include runtime monitoring, anomaly detection, and design for trust techniques.

Also, in 2014, Ghosh *et al.* [95] extended the scope of IC manufacturing security to printed circuit board (PCB) manufacturing security. They proposed an attack taxonomy that includes malicious modification during manufacturing, piracy, and product counterfeiting issues.

In 2016, Yampolskiy *et al.* [31] analyzed the possibility of turning an additive manufacturing system into a weapon, which can cause physical damages, injuries or death, and environmental contamination. In this analysis, a taxonomy was proposed to analyze the kind of elements that can be compromised in the system and how an attacker can manipulate other elements in the system through the compromised element. One aspect not often discussed in other related surveys is maliciously tampered source materials that can introduce potential hazards or risks to the system. Also, since the focus of this article was to study the feasibility of weaponizing additive manufacturing systems, secret information leakage was not covered by the taxonomy at all [31].

Xiao *et al.* [96] compiled a decade of research on the topic of hardware Trojans. They proposed a comprehensive taxonomy of countermeasures of hardware Trojans to categorize countermeasures. The three main categories of hardware Trojan countermeasures are anomaly detection, split manufacturing, and design for trust.

Gupta *et al.* [45] presented a taxonomy summarizing the potential attacks and risks of additive manufacturing systems. In their taxonomy, they classified attacks on additive manufacturing based on the step (when), means (how), outcome (what), intent (why), and abstraction (where) of the attacks.

Pan *et al.* [97] presented two taxonomies: one is the threat taxonomy for manufacturing systems and the other is for quality control systems. Interestingly, the threat taxonomy for manufacturing systems is constructed as a chain for attack development, starting from possible vulnerabilities, and then vulnerabilities can be exploited by attack vectors to achieve attack goals on the target. Also, the goals are defined as abstract security properties, including confidentiality, integrity, and availability. Thus, it may not be well connected with readers who do not have a cybersecurity background.

Wu and Moon [98] introduced a taxonomy of cross-domain attacks on cybermanufacturing systems. Similar to other taxonomies, the taxonomy in [98] consists of four dimensions: attack vectors, attack impacts, attack methods, and attack consequences. Remarkably, the authors highlighted the domains of different attacks, either in the cyber or physical domain.

Yampolskiy *et al.* [99] proposed a detailed taxonomy for the security threats in additive manufacturing systems. It first classified all the security threats based on the attackers' goals into two categories: theft of technical data and sabotage. Then, the attack targets and attack methods for these two attack goals are presented in two taxonomies separately. The taxonomies classified the attack targets and methods in very fine-grained details, and the descriptions are specific to additive manufacturing. This significantly helps readers understand the whole taxonomy, but it also limits its applicability to other manufacturing systems. The proposed taxonomy is at a more general level than that in [99]; we hope that this taxonomy applies to a wider range of manufacturing systems.

Elhabashy *et al.* [74] proposed an attack taxonomy of production systems. Their taxonomy and ours have the same structure, that is, we all classify the security threats on manufacturing/production systems based on attack goals/objectives, attack methods, and attack targets/locations. Since Elhabashy *et al.* [74] analyzed the systems from a quality control perspective, they only considered security threats, which will lead to low-quality/altered products. Comparing with the one in [74], our taxonomy in Fig. 6 has broader coverage in terms of the attack goals/objectives, that is, we include security threats (counterfeiting and piracy) that can potentially steal sensitive information from manufacturing systems. Consequently, more attack methods are included in our taxonomy, for example, reverse engineering and side-channel leaks.In [100], a detailed taxonomy of Trojan attacks on PCB was presented. The primary purpose of Trojans in PCBs is either function tampering or information leakage from the PCBs.

Our taxonomy is developed based on a seminal work that introduced a taxonomy of hardware security threats [93]. Similar to other related attack taxonomy on (additive) manufacturing systems mentioned earlier, we also identify attack goals, methods, and targets as important dimensions to categorize and understand attacks on DM systems. In addition, we introduce countermeasures in the taxonomy following the approach used in [93] so that one can use our taxonomy to quickly identify possible countermeasures for an attack of concern to him/her. We highlight the connections between adjacent dimensions to help readers build a knowledge graph of cybersecurity of DM systems. From Table 2, we also notice that our taxonomy does not include post-deployment monitoring and split manufacturing as countermeasures because, to the best of our knowledge, there are no existing works that take these two approaches to protect DM systems. However, these may also present new directions for developing novel countermeasures for DM systems.

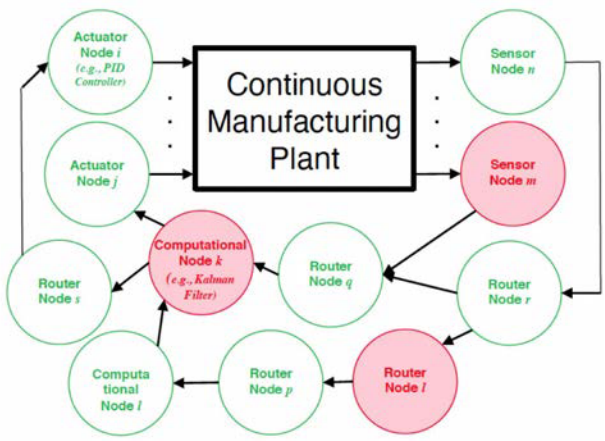

Fig. 9. *Manufacturing plant with some subverted nodes.*

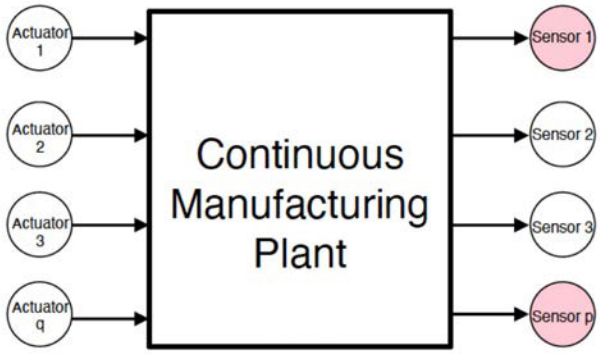

Fig. 10. *Abstraction of a manufacturing plant with compromised sensors.*

V. DIGITAL MANUFACTURING: CYBER–PHYSICAL COUNTERMEASURES

This section presents five case studies (marked in blue in Table 1) of manufacturing-unique defenses spanning watermarking of controllers used in a range of manufacturing settings, design obfuscation, part identification and provenance checking using embedded codes, authentication of designs in the signal-processing domain, and an epidemiological approach to manufacturing IoT device security by leveraging their diversity.

A. Securing Manufacturing Controllers via Dynamic Watermarks

As outlined in the foregoing, the sensors, actuators, and control laws play a critical role in DM systems pertinent to both discrete manufacturing and continuous process industry. Discrete manufacturing is concerned with the manufacture or assembly of discrete units. In process industries, the production processes are continuous, and batches are indistinguishable [101]. In either case, the production process often depends on maintaining the compositions, temperatures, feed rates, pressures, the levels of tanks, flow rates, and so on. The regulation of all the required variables is done through a feedback control loop that senses the relevant output variables and calculates what actuation commands to apply.

The measurements made by the sensors typically travel over a communication network. The measurements may also be processed at nodes in the network either for fusing information or for performing computations to support the control law. The problem of cybersecurity arises since sensor measurements or other information traveling over the communication network may be intercepted en route and altered. It is also possible that, in distributed control systems, the sensors may be compromised to report false measurements. Therefore, for securing the manufacturing processes, it is critical to address the security of the overall distributed control system. Fig. 9 depicts a manufacturing plant with some compromised nodes in the feedback loops.

One can unify all the cases via a simple abstraction where just sensors are compromised, as indicated in Fig. 10. Wherever the corruption of the measurements may have taken place, one can just suppose that the sensor has been compromised.

The resulting threat model is shown in Fig. 11. One or more sensors/communication/computational nodes in the DM cyber–physical system may be compromised, as indicated in Fig. 9. A compromised sensor node can report any false data at any time, as shown in Fig. 11. We do not restrict the range of false-data attacks. With this abstraction in hand, it is possible to develop an active defense based on the idea of "dynamic watermarking" [76], [77], [79]. The basic idea is illustrated in Fig. 12. Consider the problem of verifying if a sensor is being truthful in reporting its plant output measurements. The actuation nodes superimpose a small secret random "excitation signal" onto their nominal actuation command.

This secret excitation can be regarded as a form of "watermarking" in the signal domain for the dynamical (control) system and, hence, the name dynamic watermarking. This excitation applied into the plant manifests itself in a transformed way in the outputs of the plant—it is indelible just like a watermark on a sheet of paper. The manner in which it is transformed depends on the

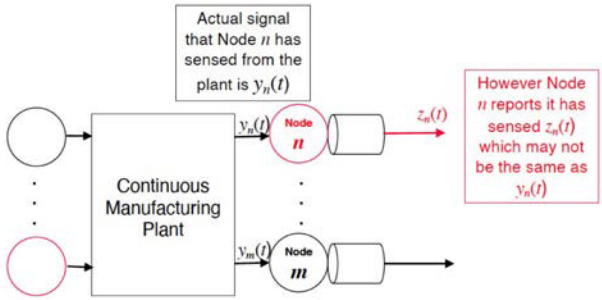

Fig. 11. *Malicious behavior of sensor nodes.*

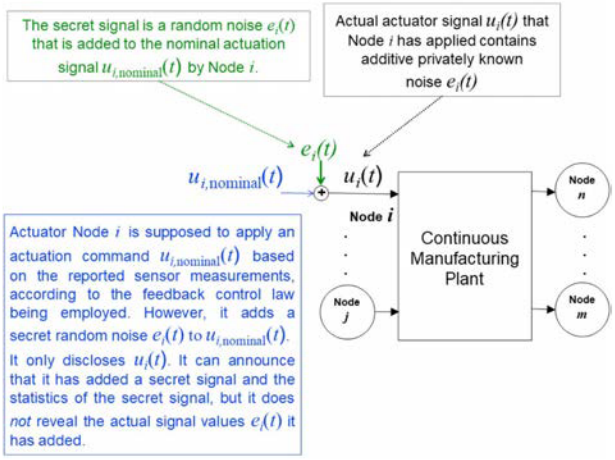

Fig. 12. ***Dynamic watermarking: the actuator node i adds a secret noise $e_i(t)$, "watermark," to the nominal control input $u_{i,nominal}(t)$ that it is expected to apply given the reported sensor measurements. It can disclose that it is adding a secret noise and it can disclose the statistics of the watermark, but it does not reveal the actual value of the random signal $e_i(t)$.***

dynamics of the pathway from the actuator to the particular output. In model-based control, design engineers have a good model of this pathway. If a sensor reports measurements that do not contain the transformed watermark, then the actuator can deduce that the sensor measurements have been compromised somewhere. One can conclude that an attack is happening and act appropriately.

The tests to determine whether the sensor measurements contain the appropriate watermark are statistical in nature. They rely on the fact that noise is normally present in the sensor measurements and that the attacker cannot separate this ambient noise from the superimposed private excitation applied by the actuator. The statistical tests that can be conducted in various scenarios are described in [79], [102]. To illustrate the core of the idea, consider the following example.

Example: Consider a fully observed linear, scalar Gaussian-controlled dynamical system described by the following equation:

$$x[t+1] = ax[t] + bu[t] + w[t]$$

where $x[t]$ is the state of the system and $u[t]$ is the control input at time t. $w[t] \sim \mathcal{N}(0, \sigma_w^2)$ is i.i.d. noise with a Gaussian distribution. We suppose that a, b, σ_w^2 are known to the control system designer. Let $z[t]$ be the measurement reported by the sensor. A truthful sensor reports $z[t] \equiv x[t]$, but a malicious sensor reports $z[t] \not\equiv x[t]$. We assume that an arbitrary history-dependent feedback control policy g is in place so that the control policy-specified input is $u_{\text{nominal}}[t] = g_t(z^t)$, where $z^t := (z[1], z[2], \ldots, z[t])$ denotes the reported measurements up to time t. This results in a closed-loop system, $x[t+1] = ax[t] + bu_{\text{nominal}}[t] + w[t]$. Suppose that the actuator superimposes a Gaussian noise unknown to the sensor on its control input: $u[t] = u_{\text{nominal}}[t] + e[t]$, where $e[t] \sim \mathcal{N}(0, \sigma_e^2)$ is a "dynamic watermark." The true state, therefore, satisfies

$$x[t+1] - ax[t] - bu_{\text{nominal}}[t] \sim N(0, \sigma_w^2) \tag{1}$$

and

$$x[t+1] - ax[t] \sim N(0, b^2\sigma_e^2 + \sigma_w^2). \tag{2}$$

The intuition behind dynamic watermarking is that by superimposing the private excitation that is unknown to the sensor, the actuator forces the sensor to report measurements that are correlated with $\{e[t]\}$, lest it be exposed. In particular, for this scalar system, the following two "attack detector tests" can be done by the actuator to detect if the sensor is malicious.

Attack detector test 1: Actuator checks if the reported sequence of measurements $\{z[t]\}$ satisfies

$$\lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} (z[t+1] - az[t] - bu_{\text{nominal}}[t] - be[t])^2 = \sigma_w^2.$$

Attack detector test 2: Actuator checks if the reported sequence of measurements $\{z[t]\}$ satisfies

$$\lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} (z[t+1] - az[t] - bu_{\text{nominal}}[t])^2 = b^2\sigma_e^2 + \sigma_w^2.$$

If the sensor is honest and reports truthful measurements $z[t] \equiv x[t]$, it passes both tests. If either test fails, the actuator can declare the presence of a malicious sensor in the system.

The more difficult question is: if the signal $z[t]$ passes both tests 1 and 2, then what guarantees can we provide on the DM CPS? Rather strong guarantees can be provided if the signal passes both tests. Let $v[t+1] := z[t+1] - az[t] - bu_{\text{nominal}}[t] - be[t] - w[t]$. It has the interpretation as the additive distortion sequence introduced by the malicious sensors to the process noise present in the system. If $z[t] \equiv x[t]$, then $v[t] \equiv 0$.

Theorem 1 [79]: Suppose that the reported sequence of measurements passes the two tests. $\lim_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} v^2[t] = 0$. That is, $\{v[t]\}$ is a zero power signal.

It states that if the malicious sensors wish to remain undetected by passing the above two tests employed by the actuators, then the only attack that they can launch is to distort the process noise in the system by adding a zero power signal to it. This, in turn, allows dynamic watermarking to provide powerful guarantees on the overall closed-loop performance of the DM Plant even under attack. Suppose, for example, that $|a| < 1$,

and a closed-loop linear control law has been designed to maintain stability, $u_{\text{nominal}}[t] = fx[t]$ with $|a + bf| < 1$ and with the control gain g chosen to yield good quadratic regulator performance.

Theorem 2 [79]: The malicious sensor cannot compromise the mean-square performance if it is to remain undetected through the above-mentioned two tests: $\lim_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} x^2[t] = (\sigma_w^2 + B^2\sigma_e^2)/(1 - |a + bf|^2)$.

System metrics, such as the quadratic regulation cost, cannot be degraded by the malicious sensors, no matter what attack strategy they employ, without being detected.

Dynamic watermarking is only designed to detect an attack. What is to be done after an attack is detected depends on the context. In some plants, one may be able to switch to manual control. In others, one may be able to replace the sensor or reboot the system. Dynamic watermarking is an active defense in which the actuators inject secret excitation in order to monitor the system and detect any adversarial presence. This idea was introduced in [103] to detect replay attacks and extended in [104] to detect other attacks. The articles [79], [102], [105] develop detectors that provably detect arbitrary attacks that introduce nonzero power distortion. Dynamic watermarking is a general methodology that can apply in a variety of contexts. It has been implemented in a laboratory process control system [106]. Similarly, a laboratory demonstration showing the efficacy of dynamic watermarking in an automation transportation testbed [107] was followed by an implementation on a real autonomous vehicle driven in autonomous mode. It holds the potential to be deployed as a general-purpose detection strategy in DM and continuous manufacturing plants and in IoT and manufacturing systems with sensors and actuators.

B. Security of Design Files: Obfuscating Designs

A major concern in the DM is the security and authenticity of CAD files. These files provide incredible capabilities and information to the designers. For example, some design software programs save the entire workflow as a feature tree that the designers can use to conveniently recall a previous design step by a single click. Such capabilities are security risks because these files reveal not only the design but also the design process. Hence, embedding security in the design files may compromise some of the functionalities [108].

Recent studies have shown the possibility of embedding a layer of security in the form of design features. These features can be developed with design elements, such as overlapping surfaces, curvatures, and scaling functions. A part 3-D printed from the design file containing such security features will appear to be different than the onscreen representation of the geometry unless the security key is applied. An example of such a secure CAD file is shown in Fig. 13, where a stolen CAD file will print

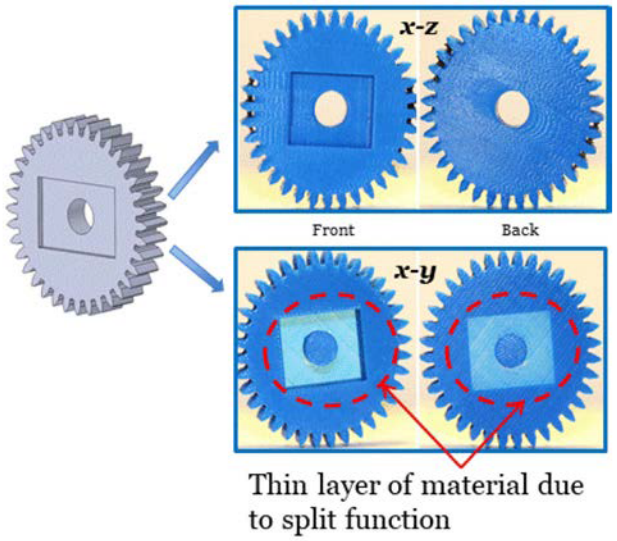

Fig. 13. *Same CAD model of a gear shows different physical geometries when it is sliced and printed on the 3-D printer build plate in the x–z and x–y orientations due to the security features embedded in it.*

with a different gear geometry if the file is not sliced and printed in the prescribed orientation. A combination of slicing orientation, slicing resolution, printer resolution, and other manufacture-time processing parameters can be used for designing such security features.

C. Securing Manufactured Parts by Embedding Codes

Parts manufactured by subtractive or formative manufacturing rely on surface markings for identification or authentication. Serial number, bar code, QR codes, and identifications are stamped or embossed on the parts. Additive manufacturing presents a unique possibility of encoding information in part during manufacturing because the part is printed layer by layer. Either conventional or bespoke identification marks can be encoded in the product. These internal markings can be read by imaging methods, such as tomography, radiography, and ultrasonic imaging. We have demonstrated embedding a QR code inside the part [108]. The method of embedding the internal identification codes depends on the AM technology. For example, sintering temperature can be changed locally to generate a feature that provides a different signature when the product is subjected to tomography. Methods such as selective laser sintering have a resolution of only a few micrometers, so an individual feature of such size is not a concern in terms of the mechanical properties of the part. The method demonstrated slices a larger QR code into hundreds of pixel-sized parts. These parts are spatially distributed in a large number of slices of the part after the slicing operation. Each part is below the critical size to compromise the mechanical properties. Slicing the code

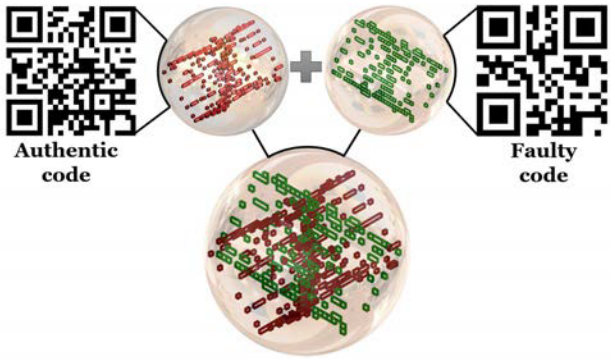

Fig. 14. *Two QR codes are sliced into 300 parts each and embedded as interpenetrating codes. The correct slicing will retain only the authentic code. Incorrect slicing will retain points that will not produce any scannable code.*

into hundreds of parts makes it difficult to find the unique direction from which it becomes a scannable code. Such obfuscations can be designed to work in a number of ways. For instance, the sliced codes can be oriented such that the code is present in the CAD/STL files, but slicing will remove it and produce a solid part without a trace of the code [53].

Reverse-engineered and reconstructed CAD files will not have the code. Hence, the parts manufactured from these files will also not have the codes. Furthermore, the parts printed from stolen CAD files will have the code and will allow identifying the unauthorized counterfeit. In another embodiment, two interpenetrating codes can be designed such that slicing at certain angles will remove one code with the remaining code used for identification, as shown in Fig. 14 [108]. This scheme will result in reverse-engineered CAD files that do not resemble the original ones.

D. IP Protection by Fingerprinting in Acoustic Domain

CAD files are inputs for 3-D printers in AM. These files are not designed just for visualization of the part design but also to manufacture the part. This places limits on encryption and compression methods that can be applied to such files. Any algorithm that causes a loss of information is not useful for such an application; only lossless methods are required.

Behera *et al.* [80] propose a novel encryption method where a lossless algorithm converts the CAD files to the frequency-domain audio files. The frequency-domain files are saved as spectrograms and used to generate fingerprints of the design in the form of (time, frequency) pairs for the amplitude peaks. These fingerprints can be used as an alternate modality for file authentication in the manufacturing process chain.

Fig. 15 shows a CAD model of a wheel hub, which is transformed into a frequency-domain spectrogram. The red dots in the spectrogram mark the fingerprints identified for the model. The number of fingerprints depends on a designer-specified threshold or automatically determined based on the security level. If the spectrogram is saved or the threshold level is low enough, the spectrogram can be converted back to the CAD model without any distortion or loss of geometry. Such spectrograms are sensitive to change in the design file. Even changing a dimension to the limit of resolution of the CAD file will create detectable perturbations in the fingerprints.

E. Securing Manufacturing IoT Networks by Device Population Diversity

The manufacturing industry is adopting IoT devices at 40% annual growth rates for enhanced asset management and increased productivity [109]. The proliferation of IoT and other noncompute devices is increasing the diversity of devices connected to the network in the next-generation manufacturing system [110]. The number and diversity of IoT devices are expected to grow over time as sensors and controllers are deployed widely [111]–[117].

Due to the increasing diversity in IoT devices, their ease in connecting to networks, weak default password configurations, and general lack of ability to automatic upgrade of firmware, they are easy targets for cyberattacks [118]–[122]. While efforts to deal with the vulnerability of a particular equipment or a unit in a manufacturing system have been reasonably addressed, assuring cybersecurity in the presence of a diverse "population mix" of IoT sensors and other noncompute devices deployed in the next-generation manufacturing plants or across the enterprise has not received much attention.

As a proxy to studying the device population mix in a real-world manufacturing enterprise, we carried out a measurement campaign of types of devices on a large-scale campus network [117]. We carried out a census of devices connected to the campus network and classified them based on their function. The results are shown in Fig. 16(a). The devices connected to the network included desktops, laptops, mobile phones, VOIP phones, printers, TV displays, AV equipment, science appliances, and building automation gear, among others. While the importance of keeping the computing equipment patched and up-to-date has for obvious reasons been recognized for

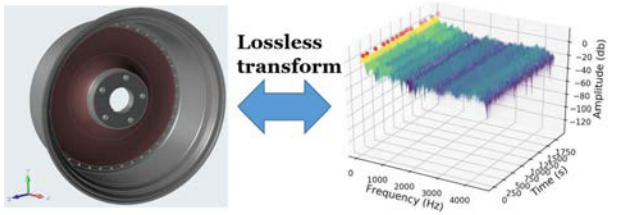

Fig. 15. *Lossless transformation of a wheel hub solid model from a CAD format to a frequency-domain spectrogram.*

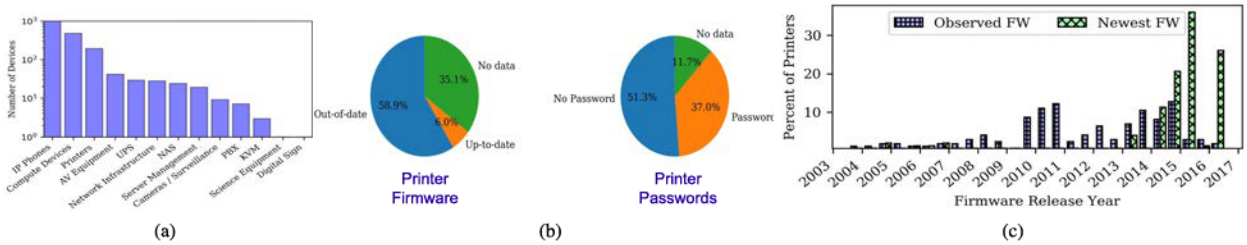

Fig. 16. *(a) Diversity in device population on a network. (b) Printers with no passwords. (c) Status of firmware updates on printers.*

quite some time, only recently, the security of noncompute IoT devices is receiving attention [123]. Our study showed that over 71% of devices on the campus network are noncompute. Among these, ∼59% of the printers on the network had out-of-date firmware [see Fig. 16(b)] and over half of the printers had no password. In a manufacturing plant, the percentage and diversity of noncompute devices are expected to be higher.

Current network security approaches and tools are device-agnostic and ignore the diversity of the networked IoT devices. However, not all the devices are created equal, and not all the devices are updated and maintained at the same level of network hygiene. In the campus network that we studied, while the computers are managed, patched, and secured by the IT team, the printers are maintained by graduate students, the VOIP phones are managed by the communications department, and the building automation devices are maintained by the facilities department. This leads to inconsistencies in the hygiene and health across devices. We advocate enhancing security tools to consider the diversity of the device populations. As shown in Fig. 1, the device population mix in a typical manufacturing floor network will look considerably different from the design network.

Public health experts and epidemiologists consider population diversity and the differing impact of diseases on different groups in keeping the population healthy. Similarly, we advocate network security policies and mechanisms tailored to the population of devices in the manufacturing network. This has benefits over the state-of-the-art device-agnostic approaches.

The dynamics of the device population has a significant impact on virus/attack epidemics in the network. For example, the Mirai attack targeted particular type of devices, and the networks with these devices had more compromises. Knowing the local device population allows one to mine the national vulnerability database (NVD) [124], [125] to study vulnerabilities specific to the network. The NVD is a repository of known vulnerabilities characterized by anticipated criticality. We can construct device-population-specific attack vulnerability profiles. Besides the NVD database, one could use internal information to augment the network monitoring tools. For example, a programmable logic controller (PLC) controlling a boiler may need to be more carefully monitored and protected compared to a printer on the network. If additional information about the devices is available, this can be factored into allocation decisions on monitoring devices. Data from our study on campus devices revealed that the firmware in printers is not upgraded as frequently as in other devices [see Fig. 16(c)]. While this knowledge is beneficial in deploying IT resources for updating/patching the device firmware to reduce the number of unpatched vulnerabilities, until that time these devices[2] are upgraded, extra resources may be needed to monitor them.

It is important to study the vulnerabilities of the network device population and take steps to protect local device populations. Following are at least three ways.

1) Based on the number of local devices and the known vulnerabilities on these devices, network monitoring tools and resources can be optimally apportioned to maximize their effectiveness in detecting and containing the attacks. At the time of connection, the level of provided network service can be tailored to the known security vulnerabilities of the device requesting network service. The levels of service could include complete DoS, limited access through security perimeters, requiring security patches, or upgrades before providing full access to the network. These approaches apply to one device at a time at the time of connecting to the network.
2) Isolate similarly vulnerable devices on a virtual LAN (VLAN) to provide suitable security for these devices. For example, the Windows 8 devices for which no new security patches will be available could be isolated in a separate VLAN and protect them with a security device that carefully monitors Windows 8-specific attacks. Similarly, IoT devices in a critical infrastructure could be put on a separate VLAN that only trusted users can access. Even if they are not perfect, such population-specific isolation and protections will improve security.
3) Given the device population, network monitoring tools can aggregate anomalies based on device types to find patterns of attacks on specific types of devices. More information can be gleaned by aggregation based on the device type. Observed anomalies can be checked against vulnerabilities in the NVD database to find attack vectors.

[2]For example, devices with older firmware or vulnerabilities from CERT database.

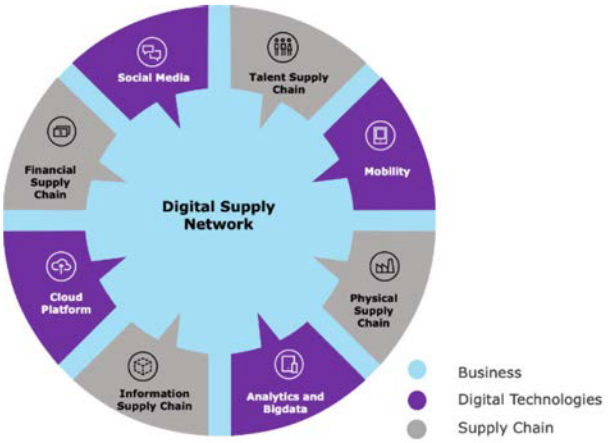

Fig. 17. *Emerging DSN.*

VI. CONCLUSION

Adoption of DM requires companies to migrate to a DSN, as shown in Fig. 17. The figure shows how a classical linear manufacturing supply chain collapses into a set of dynamic networks due to digitalization. DSNs enabled by networking within and across organizations are integral to the DM. While the integration of social media may be a counterintuitive component in the DSN, companies are adopting social media platforms to report service outages and system malfunctions and for customer support. As shown in our study, the elements of the DM process chain open up large attack surfaces and introduce many vulnerabilities making them susceptible to traditional cyberattacks and attacks that impact the physical DM and quality of manufactured products. Digitalization of the entire DM supply chain while making the production and movement of goods efficient increases the attack surface and introduces new attack vectors.

Not all participants in a manufacturing supply chain may have the same level of resources to implement the most advanced defenses. The weakest links in a supply chain, besides compromising their own assets, may compromise the assets of all participants in the supply chain. This is especially true for the MSEs, with limited resources, who nevertheless have to embrace the adoption of digitalization and DM. When the MSEs employ the digital thread while setting up the DM workflow and use the DSN to establish connectivity within their enterprise and across enterprises in the supply chain, they have to tackle the threats on multiple levels. The challenge for these MSEs is, therefore, to be judicious in using the limited resources to address these threats. The MSEs must prioritize which cybersecurity issues to address as they transition to a DM workflow.

While this study focused on cybersecurity of manufacturing-unique elements of a DSN, other elements in the DSN, such as the information, financial, and business networks, are also important. Some of them can be secured using well-known information security approaches, such as encrypting data and authenticating the communications. Side-channel attacks and reverse engineering of products are threats that extend beyond the DM network and impact a company significantly. Reverse engineering of a product can lead to revenue loss, where the CAD models may be generated by skillful designers based on an actual part acquired from the OEM without any disruption or breaches to the connected supply chain. These additional risks need to be addressed when securing DM. Most DM IoT technology components lack sufficient device activity logging capability. Insecure network protocols are typically used to connect DM components to the Internet. Various methods can be used to assess the security posture of a manufactured product. Traditional systems have typically either been designed without security in mind or with the explicit presumption that the system is isolated and so not subject to cyberattacks [3]. The new generation of manufacturing sectors resulting from the adoption of the DM process workflow and migration to the DSN needs a special focus on securing the complex systems that are integrated within the control network in the manufacturing plant. Hence, security controls should be designed from the inception of software development to hardware configuration in the control network. ■

Acknowledgment

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the National Science Foundation, Army Research Office, Army Research Lab, the Office of Naval Research (ONR), the Department of Energy, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

REFERENCES

[1] R. Y. Zhong, X. Xu, E. Klotz, and S. T. Newman, "Intelligent manufacturing in the context of industry 4.0: A review," *Engineering*, vol. 3, no. 5, pp. 616–630, Oct. 2017.

[2] A. S. Iquebal *et al.*, "Towards realizing cybermanufacturing kiosks: Quality assurance challenges and opportunities," *Procedia Manuf.*, vol. 26, pp. 1296–1306, 2018.

[3] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *J. Manuf. Syst.*, vol. 47, pp. 93–106, Apr. 2018.

[4] M. Praniewicz, T. Kurfess, and C. Saldana, "Adaptive geometry transformation and repair for hybrid manufacturing," *Procedia Manufacturing*, vol. 26, pp. 228–236, Jan. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2351978918307017

[5] T. Yamazaki, "Development of a hybrid multi-tasking machine tool: Integration of additive manufacturing technology with CNC machining," *Procedia CIRP*, vol. 42, pp. 81–86, Jan. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2212827116004777

[6] D. Alter. (2018). *3D Hybrid Printing and Implant-Supported Prosthetics*. Accessed: May 2020. [Online]. Available: https://www.aegisdentalnetwork.com/idt/2018/06/3d-hybrid-printing-and-implant-supported-prosthetics

[7] M. Soshi, J. Ring, C. Young, Y. Oda, and M. Mori, "Innovative grid molding and cooling using an additive and subtractive hybrid CNC machine tool," *CIRP Ann.*, vol. 66, no. 1, pp. 401–404, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0007850617300938

[8] L. Ren, A. P. Padathu, J. Ruan, T. Sparks, and F. W. Liou, "Three dimensional die repair using a

hybrid manufacturing system," in *Proc. 17th Solid Freeform Fabr. Symp.*, Austin, TX, USA, 2006, pp. 14–16.

[9] P. Zelinski. (2017). *3D Hybrid Printing and Implant-Supported Prosthetics*. Accessed: May 2020. [Online]. Available: https://www.shorturl.at/

[10] (2019). *The SHM Platform*. Accessed: Aug. 2020. [Online]. Available: https://smtamu.wixsite.com/about/smart-manufacturing-at-texas-a-m

[11] B. Botcha, A. S. Iquebal, and S. T. Bukkapatnam, "Smart manufacturing multiplex," *Manuf. Lett.*, vol. 25, pp. 102–106, Aug. 2020.

[12] B. Botcha *et al.*, "Implementing the transformation of discrete part manufacturing systems into smart manufacturing platforms," in *Proc. ASME 13th Int. Manuf. Sci. Eng. Conf.*, 2018, pp. 1–9.

[13] A. S. Iquebal, B. Botcha, and S. Bukkapatnam, "Towards rapid, *in situ* characterization for materials-on-demand manufacturing," *Manuf. Lett.*, vol. 23, pp. 29–33, Jan. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2213846319300951

[14] P. Rao, S. Bukkapatnam, O. Beyca, Z. Kong, and R. Komanduri, "Real-time identification of incipient surface morphology variations in ultraprecision machining process," *J. Manuf. Sci. Eng.*, vol. 136, no. 2, pp. 021008-1–021008-11, Apr. 2014.

[15] R. Palanna, S. Bukkapatnam, and F. S. Settles, "Model-based tampering for improved process performance—An application to grinding of shafts," *J. Manuf. Process.*, vol. 5, no. 1, pp. 24–32, 2003.

[16] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2008, pp. 495–500.

[17] B. Botcha, V. Rajagopal, R. B. N, and S. T. Bukkapatnam, "Process-machine interactions and a multi-sensor fusion approach to predict surface roughness in cylindrical plunge grinding process," *Procedia Manuf.*, vol. 26, pp. 700–711, Jan. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2351978918307510

[18] A. S. Iquebal and S. Bukkapatnam, "Change detection and prognostics for transient real-world processes using streaming data," in *Recent Advances in Optimization and Modeling of Contemporary Problems—INFORMS*. 2018, pp. 279–315.

[19] C. Cheng *et al.*, "Time series forecasting for nonlinear and non-stationary processes: A review and comparative study," *IIE Trans.*, vol. 47, no. 10, pp. 1053–1071, Oct. 2015.

[20] M. R. Yavari, K. D. Cole, and P. Rao, "Thermal modeling in metal additive manufacturing using graph theory," *J. Manuf. Sci. Eng.*, vol. 141, no. 7, Jul. 2019, Art. no. 071007, doi: 10.1115/1.4043648.

[21] Z. Wang *et al.*, "Acoustic emission characterization of natural fiber reinforced plastic composite machining using a random forest machine learning model," *J. Manuf. Sci. Eng.*, vol. 142, no. 3, Mar. 2020, Art. no. 031003, doi: 10.1115/1.4045945.

[22] M. A. Al Faruque, S. R. Chhetri, A. Canedo, and J. Wan, "Acoustic side-channel attacks on additive manufacturing systems," in *Proc. ACM/IEEE 7th Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Apr. 2016, pp. 1–10.

[23] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin, and Y. Elovici, "dr0wned–cyber-physical attack with additive manufacturing," in *Proc. 11th USENIX Workshop Offensive Technol. (WOOT)*, 2017.

[24] S. B. Moore, W. B. Glisson, and M. Yampolskiy, "Implications of malicious 3D printer firmware," in *Proc. 50th Hawaii Int. Conf. Syst. Sci. (HICSS)*, T. Bui, Ed., Hilton Waikoloa Village, HI, USA, Jan. 2017, 2017, pp. 1–10. [Online]. Available: http://hdl.handle.net/10125/41899

[25] S. R. Chhetri, A. Canedo, and M. A. A. Faruque, "Confidentiality breach through acoustic side-channel in cyber-physical additive manufacturing systems," *ACM Trans. Cyber-Phys. Syst.*, vol. 2, no. 1, pp. 1–25, Feb. 2018.

[26] N. Gupta, A. Tiwari, S. T. Bukkapatnam, and R. Karri, "Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks," *IEEE Access*, vol. 8, pp. 47322–47333, 2020.

[27] J. Kirk. (2018). *Wannacry Outbreak Hits Chipmaker, Could Cost $170 Million*. Accessed: Aug. 2020. [Online]. Available: https://www.bankinfosecurity.com/chipmaker-tsmc-wannacry-attack-could-cost-us170-million-a-11285

[28] B. Briggs. *Hackers Hit Norsk Hydro With Ransomware. The Company Responded With Transparency*. Accessed: Aug. 2020. [Online]. Available: https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

[29] L. D. Sturm, C. B. Williams, J. A. Camelio, J. White, and R. Parker, "Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the. STL file with human subjects," *J. Manuf. Syst.*, vol. 44, pp. 154–164, Jul. 2017.

[30] B. Ranabhat, J. Clements, J. Gatlin, K.-T. Hsiao, and M. Yampolskiy, "Optimal sabotage attack on composite material parts," *Int. J. Crit. Infrastruct. Protection*, vol. 26, Sep. 2019, Art. no. 100301.

[31] M. Yampolskiy, A. Skjellum, M. Kretzschmar, R. A. Overfelt, K. R. Sloan, and A. Yasinsac, "Using 3D printers as weapons," *Int. J. Crit. Infrastruct. Protection*, vol. 14, pp. 58–71, Sep. 2016.

[32] M. Wu, Z. Song, and Y. B. Moon, "Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods," *J. Intell. Manuf.*, vol. 30, no. 3, pp. 1111–1123, Mar. 2019.

[33] S. R. Chhetri, A. Canedo, and M. A. Al Faruque, "KCAD: Kinetic cyber-attack detection method for cyber-physical additive manufacturing systems," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*. Nov. 2016, pp. 1–8.

[34] Z. DeSmit, A. E. Elhabashy, L. J. Wells, and J. A. Camelio, "Cyber-physical vulnerability assessment in manufacturing systems," *Procedia Manuf.*, vol. 5, pp. 1060–1074, 2016.

[35] F. Chen, G. Mac, and N. Gupta, "Security features embedded in computer aided design (CAD) solid models for additive manufacturing," *Mater. Des.*, vol. 128, pp. 182–194, Aug. 2017.

[36] A. E. Elhabashya, L. J. Wellsb, and J. A. Camelioc, "Cyber-physical security research efforts in manufacturing—A literature," *Procedia Manuf.*, vol. 34, pp. 921–931, Jun. 2019.

[37] A. Bracho, C. Saygin, H. Wan, Y. Lee, and A. Zarreh, "A simulation-based platform for assessing the impact of cyber-threats on smart manufacturing systems," *Procedia Manuf.*, vol. 26, pp. 1116–1127, Jan. 2018.

[38] L. M. Graves, J. Lubell, W. King, and M. Yampolskiy, "Characteristic aspects of additive manufacturing security from security awareness perspectives," *IEEE Access*, vol. 7, pp. 103833–103853, 2019.

[39] M. Yampolskiy, T. R. Andel, J. T. McDonald, W. B. Glisson, and A. Yasinsac, "Intellectual property protection in additive layer manufacturing: Requirements for secure outsourcing," in *Proc. 4th Program Protection Reverse Eng. Workshop*, 2014, pp. 1–9.

[40] S. R. Chhetri, N. Rashid, S. Faezi, and M. A. Al Faruque, "Security trends and advances in manufacturing systems in the era of industry 4.0," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2017, pp. 1039–1046.

[41] S. Belikovetsky, Y. Solewicz, M. Yampolskiy, J. Toh, and Y. Elovici, "Detecting cyber-physical attacks in additive manufacturing using digital audio signing," 2017, *arXiv:1705.06454*. [Online]. Available: http://arxiv.org/abs/1705.06454

[42] S. R. Chhetri and M. A. Al Faruque, "Side channels of cyber-physical systems: Case study in additive manufacturing," *IEEE Des. Test. Comput.*, vol. 34, no. 4, pp. 18–25, Aug. 2017.

[43] F. W. Baumann and D. Roller, "Additive manufacturing, cloud-based 3D printing and associated services–overview," *J. Manuf. Mater. Process.*, vol. 1, no. 2, p. 15, 2017.

[44] D. Wu *et al.*, "Cybersecurity for digital manufacturing," *J. Manuf. Syst.*, vol. 48, pp. 3–12, Jul. 2018.

[45] N. Gupta, F. Chen, N. G. Tsoutsos, and M. Maniatakos, "Obfuscade: Obfuscating additive manufacturing cad models against counterfeiting," in *Proc. 54th Annu. Design Autom. Conf.*, 2017, pp. 1–6.

[46] S. B. Moore, J. Gatlin, S. Belikovetsky, M. Yampolskiy, W. E. King, and Y. Elovici, "Power consumption-based detection of sabotage attacks in additive manufacturing," 2017, *arXiv:1709.01822*. [Online]. Available: http://arxiv.org/abs/1709.01822

[47] N. G. Tsoutsos, H. Gamil, and M. Maniatakos, "Secure 3D printing: Reconstructing and validating solid geometries using toolpath reverse engineering," in *Proc. 3rd ACM Workshop Cyber-Phys. Syst. Secur.*, 2017, pp. 15–20.

[48] S. Belikovetsky, Y. A. Solewicz, M. Yampolskiy, J. Toh, and Y. Elovici, "Digital audio signature for 3D printing integrity," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1127–1141, May 2019.

[49] A. Zarreh, C. Saygin, H. Wan, Y. Lee, A. Bracho, and L. Nie, "Cybersecurity analysis of smart manufacturing system using game theory approach and quantal response equilibrium," *Procedia Manuf.*, vol. 17, pp. 1001–1008, Jan. 2018.

[50] D. B. Miller, W. B. Glisson, M. Yampolskiy, and K.-K.-R. Choo, "Identifying 3D printer residual data via open-source documentation," *Comput. Secur.*, vol. 75, pp. 10–23, Jun. 2018.

[51] S. C. Chaduvula, A. Dachowicz, M. J. Atallah, and J. H. Panchal, "Security in cyber-enabled design and manufacturing: A survey," *J. Comput. Inf. Sci. Eng.*, vol. 18, no. 4, pp. 040802-1–040802-15, Dec. 2018.

[52] Y. Raban and A. Hauptman, "Foresight of cyber security threat drivers and affecting technologies," *Foresight*, 2018.

[53] F. Chen, Y. Luo, N. G. Tsoutsos, M. Maniatakos, K. Shahin, and N. Gupta, "Embedding tracking codes in additive manufactured parts for product authentication," *Adv. Eng. Mater.*, vol. 21, no. 4, Apr. 2019, Art. no. 1800495.

[54] S.-Y. Yu, A. V. Malawade, S. R. Chhetri, and M. A. Al Faruque, "Sabotage attack detection for additive manufacturing systems," *IEEE Access*, vol. 8, pp. 27218–27231, 2020.

[55] W. Hoffman and T. A. Volpe, "Internet of nuclear things: Managing the proliferation risks of 3-D printing technology," *Bull. At. Scientists*, vol. 74, no. 2, pp. 102–113, Mar. 2018.

[56] O. Abdulhameed, A. Al-Ahmari, W. Ameen, and S. H. Mian, "Additive manufacturing: Challenges, trends, and applications," *Adv. Mech. Eng.*, vol. 11, no. 2, 2019, Art. no. 1687814018822880.

[57] A. Padmanabhan and J. Zhang, "Cybersecurity risks and mitigation strategies in additive manufacturing," *Prog. Additive Manuf.*, vol. 3, nos. 1–2, pp. 87–93, Jun. 2018.

[58] J. Prinsloo, S. Sinha, and B. von Solms, "A review of industry 4.0 manufacturing process security risks," *Appl. Sci.*, vol. 9, no. 23, p. 5105, Nov. 2019.

[59] S. R. Chhetri, A. Barua, S. Faezi, F. Regazzoni, A. Canedo, and M. A. Al Faruque, "Tool of spies: Leaking your ip by altering the 3D printer compiler," *IEEE Trans. Dependable Secure Comput.*, early access, Jun. 20, 2019, doi: 10.1109/TDSC.2019.2923215.

[60] M. Jiménez, L. Romero, I. A. Domínguez, M. D. M. Espinosa, and M. Domínguez, "Additive manufacturing technologies: An overview about 3D printing methods and future prospects," *Complexity*, vol. 2019, pp. 1–30, Feb. 2019.

[61] M. Yampolskiy, L. Schutzle, U. Vaidya, and A. Yasinsac, "Security challenges of additive manufacturing with metals and alloys," in *Proc. Int. Conf. Crit. Infrastruct. Protection*. Cham, Switzerland: Springer, 2015, pp. 169–183.

[62] O. Ivanova, A. Elliott, T. Campbell, and C. B. Williams, "Unclonable security features for

additive manufacturing," *Additive Manuf.*, vols. 1–4, pp. 24–31, Oct. 2014.
[63] S. M. Bridges, K. Keiser, N. Sissom, and S. J. Graves, "Cyber security for additive manufacturing," in *Proc. 10th Annu. Cyber Inf. Secur. Res. Conf.*, 2015, pp. 1–3.
[64] M. Holland, C. Nigischer, and J. Stjepandic, "Copyright protection in additive manufacturing with blockchain approach," *Transdisciplinary Eng. A, Paradigm Shift*, vol. 5, pp. 914–921, Jul. 2017.
[65] S. R. Chhetri, S. Faezi, A. Canedo, and M. A. Al Faruque, "Poster abstract: Thermal side-channel forensics in additive manufacturing systems," in *Proc. ACM/IEEE 7th Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Vienna, Austria, Apr. 2016, pp. 11–14.
[66] C. Wei, Z. Sun, Y. Huang, and L. Li, "Embedding anti-counterfeiting features in metallic components via multiple material additive manufacturing," *Additive Manuf.*, vol. 24, pp. 1–12, Dec. 2018.
[67] M. Wu *et al.*, "Detecting attacks in cybermanufacturing systems: Additive manufacturing example," in *Proc. MATEC Web Conf.*, vol. 108, 2017, p. 06005.
[68] H. Vincent, L. Wells, P. Tarazaga, and J. Camelio, "Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems," *Procedia Manuf.*, vol. 1, pp. 77–85, Jun. 2015.
[69] A. Riel, C. Kreiner, G. Macher, and R. Messnarz, "Integrated design for tackling safety and security challenges of smart products and digital manufacturing," *CIRP Ann.*, vol. 66, no. 1, pp. 177–180, 2017.
[70] A. Ren, D. Wu, W. Zhang, J. Terpenny, and P. Liu, "Cyber security in smart manufacturing: Survey and challenges," in *Proc. IIE Annu. Conf.*, 2017, pp. 716–721.
[71] H. He *et al.*, "The security challenges in the iot enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence," in *Proc. IEEE Congr. Evol. Comput. (CEC)*, Jul. 2016, pp. 1015–1021.
[72] M. Wu *et al.*, "Establishment of intrusion detection testbed for CyberManufacturing systems," *Procedia Manuf.*, vol. 26, pp. 1053–1064, 2018.
[73] M. Fey, *3D Printing and International Security: Risks and Challenges of an Emerging Technology*, vol. 144. Frankfurt, Germany: DEU, 2017.
[74] A. E. Elhabashy, L. J. Wells, J. A. Camelio, and W. H. Woodall, "A cyber-physical attack taxonomy for production systems: A quality control perspective," *J. Intell. Manuf.*, vol. 30, no. 6, pp. 2489–2504, Aug. 2019.
[75] A. Slaughter, M. Yampolskiy, M. Matthews, W. E. King, G. Guss, and Y. Elovici, "How to ensure bad quality in metal additive manufacturing: In-situ infrared thermography from the security perspective," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, 2017, pp. 1–10.
[76] B. Satchidanandan and P. R. Kumar, "Secure control of networked cyber-physical systems," in *Proc. IEEE 55th Conf. Decis. Control (CDC)*, Dec. 2016, pp. 283–289.
[77] B. Satchidanandan and P. Kumar, "Control systems under attack: The securable and unsecurable subspaces of a linear stochastic system," in *Emerging Applications of Control and Systems Theory*. New York, NY, USA: Springer, 2018, pp. 217–228.
[78] V. Woollaston. (2017). *Wannacry is Back! Virus Hits Australian Traffic Cameras and Shuts Down a Honda Plant in Japan*. Accessed: May 2020. [Online]. Available: https://www.wired.co.uk/article/nhs-cyberattack-ransomware-security
[79] B. Satchidanandan and P. R. Kumar, "Dynamic watermarking: Active defense of networked cyber–physical systems," *Proc. IEEE*, vol. 105, no. 2, pp. 219–240, Feb. 2017.
[80] R. K. Behera, S. Sivaprakasam, L. N. Jagannathan, and N. Gupta, "System and method for security and management of computer-aided designs," U.S. Patent 16 657 048, Oct. 18, 2019.
[81] M. Wu and Y. B. Moon, "Alert correlation for detecting cyber-manufacturing attacks and intrusions," *J. Comput. Inf. Sci. Eng.*, vol. 20, no. 1, pp. 011004-1–011004-12, Feb. 2020.
[82] K. Yanamandra, G. L. Chen, X. Xu, G. Mac, and N. Gupta, "Reverse engineering of additive manufactured composite part by toolpath reconstruction using imaging and machine learning," *Composites Sci. Technol.*, vol. 198, Sep. 2020, Art. no. 108318.
[83] Q. Do, B. Martini, and K.-K.-R. Choo, "A data exfiltration and remote exploitation attack on consumer 3D printers," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 10, pp. 2174–2186, Oct. 2016.
[84] Y. Gao, B. Li, W. Wang, W. Xu, C. Zhou, and Z. Jin, "Watching and safeguarding your 3D printer: Online process monitoring against cyber-physical attacks," in *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 2, no. 3, pp. 1–27, 2018.
[85] S. R. Chhetri, S. Faezi, and M. A. Al Faruque, "Information leakage-aware computer-aided cyber-physical manufacturing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2333–2344, Sep. 2018.
[86] F. Chen, J. H. Yu, and N. Gupta, "Obfuscation of embedded codes in additive manufactured components for product authentication," *Adv. Eng. Mater.*, vol. 21, no. 8, Aug. 2019, Art. no. 1900146.
[87] C. Song, Z. Li, W. Xu, C. Zhou, Z. Jin, and K. Ren, "My smartphone recognizes genuine QR codes! practical unclonable qr code via 3D printing," in *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 2, no. 2, 2018, pp. 1–20.
[88] C. Song, F. Lin, Z. Ba, K. Ren, C. Zhou, and W. Xu, "My smartphone knows what you print: Exploring smartphone-based side-channel attacks against 3D printers," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 895–907.
[89] M. A. Al Faruque, S. R. Chhetri, A. Canedo, and J. Wan, "Forensics of thermal side-channel in additive manufacturing systems," Dept. Elect. Eng. Comput. Sci., Univ. California, Irvine, CA, USA, Tech. Rep. 16-01, 2016.
[90] Kaspersky. *What is Wannacry Ransomware?* Accessed: May 2020. [Online]. Available: https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry
[91] C. E. Landwehr, A. R. Bull, J. P. McDermott, and W. S. Choi, "A taxonomy of computer program security flaws," *ACM Comput. Surv.*, vol. 26, no. 3, pp. 211–254, Sep. 1994, doi: 10.1145/185403.185412.
[92] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, "Trustworthy hardware: Identifying and classifying hardware trojans," *Computer*, vol. 43, no. 10, pp. 39–46, Oct. 2010.
[93] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proc. IEEE*, vol. 102, no. 8, pp. 1283–1295, Aug. 2014.
[94] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware trojan attacks: Threat analysis and countermeasures," *Proc. IEEE*, vol. 102, no. 8, pp. 1229–1247, Aug. 2014.
[95] S. Ghosh, A. Basak, and S. Bhunia, "How secure are printed circuit boards against trojan attacks?" *IEEE Des. Test*, vol. 32, no. 2, pp. 7–16, Apr. 2015.
[96] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "Hardware Trojans: Lessons learned after one decade of research," *ACM Trans. Design Autom. Electron. Syst.*, vol. 22, no. 1, pp. 1–23, Dec. 2016.
[97] Y. Pan *et al.*, "Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems," *Int. J. Interact. Multimedia Artif. Intell.*, vol. 4, no. 3, p. 45, 2017.
[98] M. Wu and Y. B. Moon, "Taxonomy of cross-domain attacks on CyberManufacturing system," *Procedia Comput. Sci.*, vol. 114, pp. 367–374, 2017.
[99] M. Yampolskiy *et al.*, "Security of additive manufacturing: Attack taxonomy and survey," *Additive Manuf.*, vol. 21, pp. 431–457, May 2018.
[100] T. Hoque, S. Yang, A. Bhattacharyay, J. Cruz, and S. Bhunia, "An automated framework for board-level trojan benchmarking," 2020, *arXiv:2003.12632*. [Online]. Available: http://arxiv.org/abs/2003.12632
[101] T. Boissonneault. *Institute of Industrial & Systems Engineers: Process Industries Division*. Accessed: May 2020. [Online]. Available: https://www.iise.org/details.aspx?id=887
[102] B. Satchidanandan and P. R. Kumar, "On minimal tests of sensor veracity for dynamic watermarking-based defense of cyber-physical systems," in *Proc. 9th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2017, pp. 23–30.
[103] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2009, pp. 911–918.
[104] S. Weerakkody, Y. Mo, and B. Sinopoli, "Detecting integrity attacks on control systems using robust physical watermarking," in *Proc. 53rd IEEE Conf. Decis. Control*, Dec. 2014, pp. 3757–3764.
[105] B. Satchidanandan and P. R. Kumar, "Secure control of networked cyber-physical systems," in *Proc. IEEE 55th Conf. Decis. Control (CDC)*, Dec. 2016, pp. 283–289.
[106] J. Kim, W.-H. Ko, and P. R. Kumar, "Cyber-security with dynamic watermarking for process control systems," in *Proc. AIChE Annu. Meeting*, 2019. [Online]. Available: https://www.aiche.org/conferences/aiche-annual-meeting/2019/proceeding/paper/452a-cyber-security-dynamic-watermarking-process-control-systems
[107] W.-H. Ko, B. Satchidanandan, and P. R. Kumar, "Theory and implementation of dynamic watermarking for cybersecurity of advanced transportation systems," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2016, pp. 416–420.
[108] F. Chen, G. Mac, and N. Gupta, "Security features embedded in computer aided design (CAD) solid models for additive manufacturing," *Mater. Des.*, vol. 128, pp. 182–194, Aug. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0264127517304355
[109] S. T. S. Bukkapatnam, K. Afrin, D. Dave, and S. R. T. Kumara, "Machine learning and AI for long-term fault prognosis in complex manufacturing systems," *CIRP Ann.*, vol. 68, no. 1, pp. 459–462, 2019.
[110] H. Yang, S. Kumara, S. T. Bukkapatnam, and F. Tsung, "The Internet of Things for smart manufacturing: A review," *IISE Trans.*, vol. 51, no. 11, pp. 1190–1216, 2019.
[111] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, "Secure Internet of Things (IoT)-based smart-world critical infrastructures: Survey, case study and research opportunities," *IEEE Access*, vol. 7, pp. 79523–79544, Jul. 2019.
[112] A. O. Akmandor, H. Yin, and N. K. Jha, "Smart, secure, yet energy-efficient, Internet-of-Things sensors," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 4, no. 4, pp. 914–930, Oct. 2018.
[113] D. Kumar *et al.*, "All things considered: An analysis of IoT devices on home networks," *USENIX Secur. Symp.*, 2019, pp. 1169–1185.
[114] A. Sivanathan *et al.*, "Characterizing and classifying IoT traffic in smart cities and campuses," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2017, pp. 559–564.
[115] Z. Zheng and A. L. N. Reddy, "Safeguarding building automation networks: The-driven anomaly detector based on traffic analysis," in *Proc. IEEE ICCCN*, Jul. 2017, pp. 559–564.
[116] Z. Zheng, S. Jin, R. Bettati, and A. L. N. Reddy, "Securing cyber-physical systems with adaptive commensurate response," in *Proc. IEEE CNS Conf.*, Oct. 2017, pp. 1–9.
[117] Z. Zheng, A. Webb, A. L. N. Reddy, and R. Bettati, "IoTAegis: A scalable framework to secure the Internet of Things," in *Proc. IEEE ICCCN*, Jul. 2018, pp. 1–9.
[118] E. Fernandes, A. Rahmati, K. Eykholt, and A. Prakash, "Internet of Things security research:

A rehash of old ideas or new intellectual challenges?" in *Proc. IEEE Secur. Privacy*, Aug. 2017, pp. 79–84.
[119] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the Internet of Things: Security and privacy issues," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 34–42, Mar./Apr. 2017.
[120] H. Ghadeer, "Cybersecurity issues in Internet of Things and countermeasures," in *Proc. IEEE Int. Conf. Ind. Internet (ICII)*, Oct. 2018, pp. 195–201.
[121] F. Dang *et al.*, "Understanding fileless attacks on linux-based IoT devices with honeycloud," in *Proc. ACM MobiSys*, 2019, pp. 482–493.
[122] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically evaluating security and privacy forconsumer IoT devices," in *Proc. ACM IoT S&P*, 2017, pp. 1–6.
[123] P. Ducklin. (2016). *Mirai 'Internet of Things' Malware From Krebs DDoS Attack Goes Open Source*. Accessed: May 2020. [Online]. Available: https://nakedsecurity.sophos.com/2016/10/05/mirai-internet-of-things-malware-from-krebs-ddos-attack-goes-open-source/
[124] CERT. (2020). *Vulnerability Notes Database*. [Online]. Available: https://www.kb.cert.org/vuls/
[125] NIST. (2020). *National Vulnerability Database*. [Online]. Available: https://nvd.nist.gov/

ABOUT THE AUTHORS

Priyanka Mahesh received the B.Tech. degree in computer science from SRM University, Chennai, India, in 2016. She is currently working toward the master's degree at New York University, Brooklyn, NY, USA.

She has worked in the consulting industry in the field of cybersecurity on projects related to telematics and industrial control systems (ICS) security. Her research is focused on addressing security concerns in cyber–physical systems, embedded systems, and ICS in order to build trustworthy Internet-of-Things (IoT) systems.

Akash Tiwari received the B.Tech. degree in industrial and systems engineering from IIT Kharagpur, Kharagpur, India, in 2019. He is currently working toward the Ph.D. degree at the Department of Industrial and Systems Engineering, Texas A&M University, College Station, TX, USA.

He was a Summer Intern with Royal Enfield Motors Factory, Chennai, India, in 2017. In 2018, he was a Summer Research Intern with the Durham University Business School, Durham, U.K.

Chenglu Jin received the Ph.D. degree from the Electrical and Computer Engineering Department, University of Connecticut, Storrs, CT, USA, in 2019.

He was a Research Assistant Professor with the Center for Cybersecurity and the Center for Urban Science and Progress, New York University (NYU), Brooklyn, NY, USA. He joined the Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands, as a tenure-track researcher. His research interests are cyber–physical system security, hardware security, and applied cryptography.

Panganamala R. Kumar (Life Fellow, IEEE) received the B.Tech. degree in electronics engineering from IIT Madras, Chennai, India, in 1973, and the D.Sc. degree in systems science and mathematics from Washington University in St. Louis, St. Louis, MO, USA, in 1977.

He was a Faculty Member with the University of Maryland at Baltimore County, Baltimore, MD, USA, from 1977 to 1984, and the University of Illinois at Urbana–Champaign, Champaign, IL, USA, from 1985 to 2011. He was the Leader of the Guest Chair Professor Group on Wireless Communication and Networking, Tsinghua University, Beijing, China. He is currently an Honorary Professor with IIT Hyderabad, Hyderabad, India. He is also with Texas A&M University, College Station, TX, USA. His research interests include cyber–physical systems, cybersecurity, privacy, wireless networks, renewable energy, smart grid, autonomous vehicles, and unmanned air vehicle systems.

Prof. Kumar is a member of the U.S. National Academy of Engineering, The World Academy of Sciences, and the Indian National Academy of Engineering. He is also a Fellow of the Association for Computing Machinery (ACM). He was awarded the Doctor Honoris Causa by ETH Zurich. He was a recipient of the IEEE Field Award for Control Systems, the Donald P. Eckman Award of the American Automatic Control Council (AACC), the Fred W. Ellersick Prize of the IEEE Communications Society, the Outstanding Contribution Award of ACM SIGMOBILE, the INFOCOM Achievement Award, and the SIGMOBILE Test-of-Time Paper Award. He was a recipient of the Distinguished Alumnus Award from IIT Madras, the Alumni Achievement Award from the Washington University in St. Louis, and the Daniel Drucker Eminent Faculty Award from the College of Engineering, University of Illinois at Urbana–Champaign.

A. L. Narasimha Reddy (Fellow, IEEE) was a Research Staff Member with IBM Almaden Research Center, San Jose, CA, USA, from 1990 to 1995. He is currently a J. W. Runyon Professor with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX, USA, where he is also the Associate Dean for Research of the Texas A&M Engineering Program and the Assistant Director of Strategic Initiatives & Centers of the Texas A&M Engineering Experiment Station. He holds five patents. His research interests are in computer networks, storage systems, and computer architecture.

Dr. Reddy was awarded a Technical Accomplishment Award while he was at IBM. He received the NSF Career Award in 1996. His honors include an Outstanding Professor Award by the IEEE Student Branch at Texas A&M from 1997 to 1998, the Outstanding Faculty Award by the Department of Electrical and Computer Engineering from 2003 to 2004, the Distinguished Achievement Award for teaching from the Former Students Association of Texas A&M University, and a citation "for one of the most influential papers from the 1st Association for Computing Machinery (ACM) Multimedia Conference."

Satish T. S. Bukkapatanam received the M.S. and Ph.D. degrees in industrial and manufacturing engineering from Pennsylvania State University, State College, PA, USA, in 1994 and 1997, respectively.

He is currently the Rockwell International Professor with the Department of Industrial and Systems Engineering, Texas A&M University, College Station, TX, USA, where he has been selected as the Fulbright-Tocqueville Distinguished Chair and is also the Director of the Texas A&M Engineering Experimentation Station (TEES) Institute for Manufacturing Systems. His research in smart manufacturing addresses the harnessing of high-resolution nonlinear dynamic information, especially from wireless microelectromechanical systems (MEMS) sensors, to improve the monitoring and prognostics, mainly of ultraprecision and nanomanufacturing processes and machines, and wearable sensors for cardiorespiratory processes. His research has led to over 160 articles in journals and conference proceedings.

Dr. Bukkapatanam is a Fellow of the Institute for Industrial and Systems Engineers (IISE) and the Society of Manufacturing Engineers (SME).

Nikhil Gupta (Associate Member, IEEE) is currently a Professor of mechanical and aerospace engineering with New York University, Brooklyn, NY, USA, where he is also with the NYU Center for Cybersecurity. His research is focused on developing methods to secure computer-aided design files against theft of intellectual property and unauthorized production of parts. His group is also using machine learning methods for reverse engineering of parts and mechanical property characterization. He is the author of over 195 journal articles and book chapters on composite materials, materials characterization methods, and additive manufacturing security.

Ramesh Karri (Fellow, IEEE) received the B.E. degree in electronics and communication engineering (ECE) from Andhra University, Visakhapatnam, India, in 1985, and the Ph.D. degree in computer science and engineering from the University of California at San Diego, San Diego, CA, USA, in 1993.

He is currently a Professor of electrical and computer engineering with New York University, Brooklyn, NY, USA, where he also codirects the NYU Center for Cyber Security. He cofounded the Trust-Hub and organizes the Embedded Systems Challenge, the annual red team blue team event. He has published over 275 articles in leading journals and conference proceedings. His research and education activities in hardware cybersecurity include trustworthy integrated circuits, processors, and cyber–physical systems; security-aware computer-aided design, test, verification, validation, and reliability; nanomeets security; hardware security competitions, benchmarks, and metrics; biochip security; and additive manufacturing security.

Dr. Karri is a Fellow of the IEEE for his contributions to and leadership in trustworthy hardware. His work in trustworthy hardware received the Best Paper Award Nominations at the IEEE International Conference on Computer Design (ICCD) 2015 and the IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS) 2015, and the Best Paper Awards at the Association for Computing Machinery (ACM) *Transactions on Design Automation of Electronic Systems* (TODAES) 2017, the International Testing Conference (ITC) 2014, the ACM Conference on Computer and Communications Security (CCS) 2013, DFTS 2013, VLSI Design 2012, the ACM Student Research Competition at the Design Automation Conference (DAC) 2012, the International Conference on Computer-Aided Design (ICCAD) 2013, DAC 2014, ACM Grand Finals 2013, the Kaspersky Challenge, and the Embedded Security Challenge. He received the Humboldt Fellowship and the National Science Foundation CAREER Award. He has been serving as an Associate Editor of IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, *ACM Journal of Emerging Computing Technologies*, *ACM TODAES* (since 2014), IEEE ACCESS, IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, IEEE DESIGN AND TEST (since 2015), and IEEE EMBEDDED SYSTEMS LETTERS (since 2016). He is also the Editor-in-Chief of *ACM Journal on Emerging Technologies in Computing*. He has served as an IEEE Computer Society Distinguished Visitor from 2013 to 2015. He has served on the Executive Committee of the IEEE/ACM DAC and led the Security@DAC Initiative from 2014 to 2017. He has given keynotes, talks, and tutorials on hardware security and trust.