A New Approach to Cyberphysical Security in Industry 4.0

Andre Wegner, James Graham and Eli Ribble

Abstract This chapter presents a new paradigm that limits and protects information flows to internal and subcontracted factory floor devices to complement perimeter security as essential first steps to secure manufacturing as it embraces Industry 4.0.

Keywords Direct-to-Machine Security · PLC (Programmable Logic Controller) · Additive Manufacturing · Operator audit · Design integrity

1 Introduction

Long value chains are among the biggest security concern in manufacturing for Industry 4.0. This is the case for all manufacturing but is especially critical in the military complex. In the USA, regulations trying to manage the situation, such as DFARS 252.204-7012, utilize Information Technology (IT) paradigms that don't reflect Operation Technology's (OT) unique circumstances and focus on perimeter security. Experts in the field privately acknowledge that this kind of solution will fail and compliance requirements will soon reflect this. The absence of a security

A. Wegner (✉)
Core Digital Manufacturing Faculty for Singularity University,
Nasa Research Park, Bldg 20, Moffett Field, CA 94035, USA
e-mail: andre@authentise.com

J. Graham
True Secure SCADA, 10415 W. Hwy. 42, Goshen, KY 40026, USA
e-mail: james.graham@louisville.edu

A. Wegner · E. Ribble
Authentise Inc., 8676 S 1300 E, Sandy, UT 84094, USA
e-mail: eli@authentise.com

J. Graham
Professor Emeritus (Electrical and Computer Engineering) for the University of Louisville,
Louisville, KY 40292, USA

L. Thames and D. Schaefer (eds.), *Cybersecurity for Industry 4.0*,
Springer Series in Advanced Manufacturing, DOI 10.1007/978-3-319-50660-9_3

approach that accepts this challenge while embracing increasing digitization in manufacturing means that confidentiality, integrity, and availability of manufacturing data are at risk.

A solution to this problem should be based on consideration of the special circumstances of OT. Many different types of data are accumulated during the production of a part or product and used to verify quality, predictive maintenance and more (Ballou 1998). However, only a few of them are critical to protecting intellectual property and integrity. It is these that an OT solution should focus on:

- Bill of materials
- Design information
- Control parameters

Due to its digitally integrated nature, Additive Manufacturing (or "3D Printing") provides a fertile learning ground for this approach. The current 3D printing paradigm requires delivery of the design information and control parameters to an operator, who processes it and sends it to firmware and controller boards that operate the machinery. By contrast, the new approach presented in this chapter is to avoid giving critical data to any person or device other than the lowest level controller on the manufacturing system or systems. It generalizes an experience that is already standard in other digital industries and is becoming so in Additive Manufacturing. The solution embraces the digital manufacturing revolution delivering a connected, data-driven manufacturing process, instead of fighting it.

The next section of this chapter provides some background on computer security and explains how requirements for traditional IT cybersecurity differ from the cybersecurity requirements for Industry 4.0 manufacturing. The following section presents the secure manufacturing information architecture which addresses the security and information management for advanced digital manufacturing. The final section discusses a key component in this architecture, the manufacturing security enforcement device, and then conclusions and directions for future work in this area.

2 Background

Manufacturing cybersecurity had significant gaps even before the emergence of new manufacturing systems driven by increasingly digital devices. They highlight the security tensions as described below.

Cybersecurity and information assurance in IT systems revolve around three traditional central pillars: confidentiality, integrity and availability (CIA) (Bishop 2015). These three foundations are in tension with each other in any real IT system. For example, we can layer protections (physical and electronic) around our data and feel confident that it remains confidential and unchanged, but that is of little use if the data is not available to the person needing that data. On the other hand, making data readily available to legitimate users often means that it is also available to

individuals who can glean unauthorized information (thus violating confidentiality) or can maliciously change the data (thus destroying its integrity). The activity of engineering efficient and practical IT cybersecurity systems involves carefully balancing these three objectives to yield useable and reasonably secure results.

The requirements for cyberphysical security of advanced digital manufacturing differ in a number of ways from security of traditional IT systems. IT cybersecurity stresses layered defenses around the central core servers with less attention to peripheral devices (we usually don't care if a remote printer gets hacked). Increasing Internet of Things adoption is putting a strain to that theory (Grau 2015). In digital manufacturing, in particular, we must protect BOTH the central design computer AND the remote manufacturing equipment. Increasing threats (Brocklehurst 2014; Krebs 2012) indicate that industrial control systems are becoming the target for malicious cyber intrusions.

Within this expanded sphere of protection, needed to provide enhanced security for manufacturing and other industrial control applications, the three central CIA objectives are still paramount. Manufacturing data should be confidential in that designs represent expenditures of considerable human and computer time to create, and the creating organizations should reap the full benefit from this effort. Design data must have integrity—it must arrive at the manufacturing equipment exactly in the format and content that it had upon creation. But finally, it must also be available to be produced at any approved equipment anywhere in the world.

The challenge to maintain availability will increase as manufacturing evolves from a centralized system supported by external suppliers to a distributed system in which production occurs closer to the point of use. This is, among others, of critical concern to the defense, aviation and shipping industries, which must ensure that original spare parts reach their intended target in a short timeframe. This "Distributed Manufacturing" paradigm requires extending trust to beyond a small set of contractual suppliers, to a network of thousands of manufacturing sites able to produce the required part at any time. This stretches potential points of failure to thousands of nodes, thus challenging the existing approach of building defenses around a core even further. Instead, Distributed Manufacturing requires extensive monitoring and control-based security to function.

The ecosystem that delivers these monitoring and security features is diverse and varied. At its heart stands the concept of triangulating insight from a myriad of sources, best encapsulated in the nascent Industrial Internet of Things campaign. This brings with it several benefits based on improved collaboration (Harper 2016). Having a variety of devices, including not only the manufacturing device but other internal and external sensors capture and transmit data intensifies the pre-existing cybersecurity threat. This escalates the need for the suggested focus on securing key data points that are part of the manufacturing process.

A further manufacturing-specific security challenge is that of maintaining integrity in a multipolar development environment. The information flow in manufacturing design and production planning is not unidirectional towards the end product but instead incurs many significant iterations between design, material, and production specialists, among others. These specialists may no longer be under the

same roof or even in the same country, making it harder to protect them or their interactions. An acknowledgment of this iterative product development cycle and the distributed nature of modern experts highlights the production of the physical artifact as the weak link in a process, not as the irrelevant end of it. This, among other factors, also increases the pressure to connect previously air-gapped manufacturing devices. A lack of data flows both in and out of the machine will stunt the quest for greater efficiency, better products, and higher quality.

The increasing reliance on Computer Aided Manufacturing (CAM) is opening new attack vectors, such as attacks on the initial CAD drawings or its derivatives. Designs can be influenced in a variety of ways (scale, indents/protrusions, vertex movement) which are often subtle and difficult to discover before the part fails (Sturm 2014). This is most dramatically displayed in Additive Manufacturing devices, in which voids can be inserted into the internal geometry of the part to produce geometric failures that are silent, fully enclosed, and yield little discernable change to file size. The attack can be launched on the device firmware itself, similar to Stuxnet, or implanted in any part of the design or production process (in the STL file or the machine code). As most modern Additive Manufacturing devices have USB ports for maintenance, complex attacks may not be necessary. In a lab demonstration of this approach (by Sturm 2014), only one team of five was able to identify the attack by observing the print visually during production. In all others, there was a decrease in part strength of up to 14%. However, as others have demonstrated (Pan et al. 2017), the threat exposed most clearly in Additive Manufacturing stretches across digital manufacturing devices of all shapes and sizes (Fig. 1).

The architecture currently in use in the manufacturing environment does not address existing or emerging challenges. The design is typically entirely separated from the production environment, with manufacturing devices often air-gapped. As a result, there is no control over subcontractors in multi-step manufacturing value chains once data leaves the designer's server. Similarly, operators are also unsupervised once data is received and many issues emerge with data corruption as a result of the multi-tenanted control. The situation prevents bi-directional information flow in multi-polar development processes and is one of the key reasons why manufacturing has been relatively slow to adopt data-driven processes.

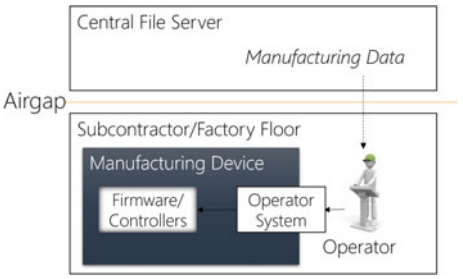

Fig. 1 Current manufacturing data flow

3 Secure Manufacturing Information Architecture

In this myriad of threats, refocusing on what represents critical information in the manufacturing process provides a starting point for better protecting the ecosystem. As discussed above, these include the bill of materials, the design file as well as control parameters. The end use for two of these, the design file and the control parameters, is the manufacturing device. Therefore, a more holistic approach to managing cyberphysical security threats in manufacturing is communicating such data directly with the relevant manufacturing device.

The fundamental problem is one of authentication and authorization: is the request to the manufacturing device authentic and is the actor requesting it authorized? For example, a technician has decided to supply a different material for a part than stated in the bill of materials. Is this request from a good actor? Is the actor authorized to make this request?

In answering these questions, we need to supply a couple of concepts. The first concept is asymmetric encryption keys. These keys come in two parts, a public half and a private half. Generally, the public half is published and used to verify or enforce that some entity possesses the private half. Keys may be held by a person, a machine, piece of software, etc. These keys can be used in encryption. If you have the public half of an entity's key, you can encrypt a message using that public half and send it to the entity. The entity can then decrypt the message with the private half (Fig. 2).

The second concept we need is that of a comptroller. A comptroller's job is to take some input data, provide a key, and store output data. The output data gets added to the end of a virtual document that becomes the record of provenance for a part that is produced. The comptroller is software that runs on a manufacturing network and authorizes each action taken on that network. A Manufacturing Security Enforcement Device (MSED) located close to or on the manufacturing device would cryptographically ensure the integrity of the transmitted data and is described in a separate section.

To illustrate the security architecture, we propose the following example: Let's suppose we want to manufacture a 10 mm cube of plastic. In a normal workflow

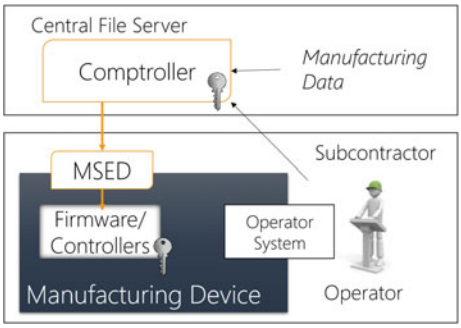

Fig. 2 Manufacturing workflow including a comptroller

today a designer would produce a CAD model of the 10 mm cube and a list of the material (PLA). These files would be provided to a technician who would use toolpath generation software to transform the cube's CAD file into a set of instructions for the printer. These instructions are then fed into the printer along with the PLA to produce the part.

There are many points of attack in this example as we described above: The CAD model could be modified, the technician could use the wrong filament, the machine could have some physical piece of hardware set outside of regular calibration or the toolpath instructions could be modified. Proper cryptographic protections can mitigate all of these attack vectors.

Let's look at this example again with a comptroller in place. At each phase, the comptroller authenticates and authorizes actions that are to be taken. First, our designer uses a CAD program to design the original cube. When the design is complete, the designer and the CAD program both supply their keys to the comptroller along with the original design. The keys confirm that the correct version of software was used and that the designer is allowed to design new models. This starts a new document for the provenance of the part identifying the designer as the root of the part. The designer then adds the bill of materials to the document indicating that this part must be printed using PLA. Later, when the technician generates the toolpath, the software tool he uses also is authenticated with the comptroller. This confirms that the technician is trained and permitted to prepare the file. The provenance document then gets a cryptographic signature with the technician's key and the toolpath generation software key. If the technician attempts any modifications of the original CAD model, the comptroller will refuse the change because the technician is not authorized to change designs, only to prepare toolpaths from the designs.

The toolpath becomes the latest part of the provenance document. The device that will manufacture the final part does not allow unencrypted toolpath bundles—all payloads must be encrypted using the device's public key and a key from the comptroller that the device has been bonded to. This means that the technician must first supply the toolpath he generates to the comptroller and indicate that he wishes to print on device X. The comptroller validates that the technician is authorized to use device X and then uses the public key for device X to produce an encrypted bundle. Device X then decrypts and validates the encrypted bundle. The bundle includes the toolpath, but it also includes the original bill of materials and CAD model since they are all linked by the same provenance document. Device X then validates that the plastic being supplied as part of the build is indeed the PLA required in the bill of materials. If the technician were to mount the wrong material, the build would not proceed. If the technician were to modify the encrypted bundle to sabotage the toolpath, the bundle would no longer cryptographically validate with device X.

During the manufacturing process device X communicates a stream of telemetry data (cryptographically signed) to the comptroller. This telemetry data is attached to the provenance document. QA processes can disqualify the build by analyzing this data and confirming that sensors are within tolerance bands. If our technician kicks

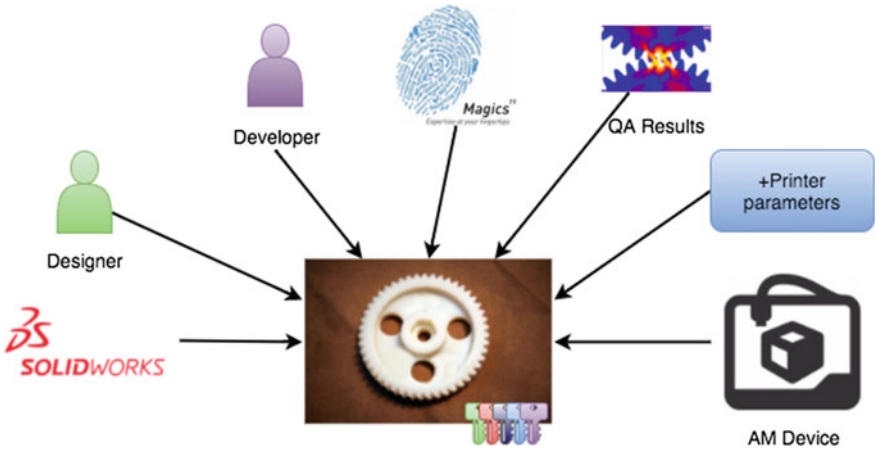

Fig. 3 Data flows managed by the comptroller

device X to sabotage the build, the comptroller can get cryptographically secure data from accelerometers that detect the kick that automatically become part of the history for the individual part (Fig. 3).

This forms the basis for a secure digital manufacturing system: A centralized authentication and authorization entity driven by asymmetric key cryptography and open standards that vendors throughout the ecosystem can implement. This includes CAD software makers, toolpath generators, static analysis, telemetry data gathering, hardware manufacturers, intrusion detection suites, and PLM. Each node in the network need only define what its inputs and outputs are, the permissions required for each action it can take, and a way to supply its key and the key of its user. This ensures a cryptographically secure chain of information about who did what with when using which tool.

Because the system relies on fine-grained, role-based controls, it works both within an organization as well as between organizations. If the comptroller is accessible across the public internet, our example above works the same way even if the original designer and the technician are on separate continents in different organizations under different legal jurisdictions. Data access and modification are based on the availability of authorized keys, not on the presence of legal contracts. Data is encrypted while in transit and only decrypted by the target software and only when it has access to the user's key. Defenses can be further hardened by using key escrow and multi-factor authentication.

From a security standpoint, it is just as important to know the origin of a part as it is to control how a part is produced. It doesn't matter if a bad actor sabotages a fuel injector nozzle as it is being built if they can more easily swap out the fuel injector nozzle for a faulty fake. Accurate part history is then the key to cyber-physical security.

For each part in the system, the comptroller maintains signed data about who took each step and which tool they used. In final part production, the comptroller stores a log of sensor data as the part is being produced. The part can be designed in such a way as to leave voids where uniquely identifying information can be added. This may include manipulations to support structures, changes to infill that respond to X-ray in particular patterns, barely-visible dots on an outer surface, or a serial number etched into the same location (Aliaga and Atallah 2009; Willis and Wilson 2013). These changes can be applied by the manufacturing device itself or as part of the toolpath generation. In either case, they represent a branching of the basic instructions that is unique for each physical part. Different industries will have different requirements and regulations around how this can and should be done, but the ultimate goal is the same: a person can take the part, look up the ID number, and request the full chain of history on the part. This prevents attacks involving supply pollution.

The chain of history can be maintained across organizations. If a prime contractor has several subs, each sub can register an organizational key with the comptroller. Each step they take in fulfilling the contract is then signed by their organization, their users, and their tools. Only data that the organization has been explicitly given access to leaves the comptroller.

In a workflow where different organizations take ownership of the produced artifacts over time, the model still works. This is a critical element as different actors expect to provide a wide range of services (Harper 2016). Each organization has their own comptroller. When an artifact, such as a CAD model, leaves one organization's control and enters another the comptroller negotiates a handle. The original comptroller notes the end of the provenance document as a handoff to a new owner. The receiving comptroller starts a new provenance document signed by the original owner indicating where the artifact came from. Tracking the history of the artifact requires communicating across organizations, but automated systems operating over the public internet makes this easy and automatable. New ledgers built on blockchain technology may be able to enforce these hand-offs should the networks become too large.

The architecture we propose here isn't without its drawbacks. Having a centralized source of authority creates a single point of failure in critical systems and a single primary target of attack for malevolent actors. There are mitigation strategies that we can employ, however.

Uptime is less of an issue than it may seem. It's simple to federate any number of comptrollers and configure them to treat one another's signature as authoritative. A single, federated data store can service the entire cluster of comptrollers if they share encryption keys, or if different clusters of comptrollers can share the underlying data. This makes it possible to take parts of the data store offline while keeping the rest available. In either storage strategy, any single comptroller can validate the provenance chain of other members of its cluster and treat them just as authoritatively, as its own history.

The far thornier issue is how to defend the comptroller as the holder of the keys. If an attacker can exfiltrate encryption keys, they can forge history. The forgery

only holds up if the attacker can then surreptitiously insert the forgery into the data store or pose as the comptroller to an external organization. If the attacker can manipulate the comptroller's data store, they could modify data access permissions or sabotage parts in any number of ways. None of this is actually more dangerous than operating without a comptroller at all. Without a comptroller, flat files are open to being manipulated at any point of transit or use, and no one would be the wiser.

Good defense-in-depth for a comptroller involves many layers. First is appropriate physical access controls and network firewalls. A comptroller can be physically secured well beyond what a shop floor would normally require as it is a data service over a LAN. That LAN should include physical intrusion detection mechanisms that can do things like limit IO when threats are encountered. Proper network gateways and firewalls can logically separate the types of data and commands that can flow through the comptroller. Air-gaps may be appropriate for certain use cases. Analysis of system logs can spot errant behavior after-the-fact. Ultimately, the comptroller should be treated with the same IT security policies that organizations employ for their file servers, domain controllers, and other sensitive data services. The added benefit is that once data leaves a file server perimeter, it is forever lost and unprotected. When data leaves the comptroller's security perimeter, it is encrypted and protected reducing the overall attack surface of the organization.

So far we've only discussed documents as single entities: a CAD model, the toolpath instructions for a particular part, the entire history of a part's creation. We can broaden this idea further when we realize that the comptroller idea is designed not to produce artifacts but to control, record, and secure operations. Operations are performed on documents—manipulations to the CAD model, constraints on the toolpath generation process, updating the Bill of Materials—but if we treat the operation as the central focus for a comptroller we open new opportunities for innovation. A CAD program that can communicate with the comptroller can begin to stream operations to the comptroller rather than just check-out and check-in documents. This not only keeps an ongoing history of the different design approaches attempted but allows the comptroller to immediately constrain the operator based on system policies and events. This becomes especially meaningful for technicians operating the manufacturing machinery. With a secure connection to the comptroller and a stream of control signals, the technician can be controlling digital manufacturing equipment in real time under the IP constraints of the design owners.

3.1 Pilot of Direct-to-Machine Security

In a commercial pilot, Authentise provided the service of securing prints to multiple online retailers of printable designs. These include toyfabb.com, cults3d.com, and others. Upon the sale of the design, Authentise's clients transmitted the design and information to Authentise's Comptroller, which then issued a link to the recipient to print. The recipient used the link first to connect their 3D printer to the Authentise

Comptroller and finalize the settings. Using those inputs, the Authentise Comptroller connected to the printer using a secure channel, prepared the machine-readable code, and sent the resulting commands into the printer. Simultaneously the print is monitored and resulting information sent to both the recipient and Authentise's client. This system is in the process of being extended to other g-code reading devices, such as CNC machines.

4 Manufacturing Security Enforcement Device

The MSED plays a key role in maintaining the end-to-end security of the secure manufacturing information architecture and is thus discussed in more detail in this section. This device sits immediately in front of the manufacturing equipment and authenticates the manufacturing instructions which come from the cloud. As the final arbitrator as to whether or not a part gets produced, this device plays a critical role in the overall secure manufacturing information architecture. Together with the other components, it assures that only information sent by an authenticated comptroller will be produced and that the message has not been altered between the cloud and the manufacturing center.

The MSED must perform near real-time decryption of the incoming data stream. As discussed previously, confidentiality of data in traditional manufacturing systems has not been a priority and most manufacturing systems data is not encrypted. The details of the part design are proprietary to the design firm and must be protected until the information is at a trusted manufacturing site. Some latency in the transfer and buffering of the incoming data stream can be supported as a few seconds of delay in the start of the manufacturing activity will not affect overall manufacturing performance.

The essential feature of the MSED is the ability to perform authentication of the design file. Was it produced by the design firm indicated in its pedigree? And was it transmitted through the cloud system without modification? A number of approaches can be used to attempt to provide this needed authentication. The best of these are cryptographically based involving computation of a unique, digital signature of the design file and the creating authority which can be verified by the MSED at the manufacturing site. Public Key Infrastructure (PKI) approaches can be used as well as Hash Method Authentication Codes (HMAC) approaches, with the latter usually requiring less computational power.

Finally, it is desirable that the MSED have a secure operating system base. Many embedded systems use real-time operating systems which are based either on Microsoft WindowsTM or LinuxTM. While these operating systems offer a large base of I/O interface drivers, networking and file systems support, and other useful software, they also contain millions of code and the unwanted byproduct of zero-day (or unknown and thus unanticipated) cyber vulnerabilities. Attacks against these unknown vulnerabilities can be devastatingly effective. Recently, alternate, smaller operating bases, designated as micro-kernels, have become available for

embedded systems use. The best of these is seL4 which has been mathematically verified to be secure (Klein et al. 2014).

Several companies currently offer products designated as industrial firewalls that offer some of the needed functionality of the MSED. These products all operate within the process control network to protect field devices such as programmable logic controllers, remote terminal units, and intelligent electronic devices by filtering incoming process network traffic.

5 Pilot of the Manufacturing Security Enforcement Device

True Secure SCADA, LLC, has recently completed a prototype MSED device utilizing the seL4 microkernel. It can be used in general industrial control applications as well as manufacturing applications. The device has been tested successfully in its laboratories for function and compatibility with industrial control devices and protocols and in currently undergoing field tests in several industrial installations. A complete overview of this device is given in (Graham 2016).

6 Conclusion

The outlined direct-to-machine communication approach can overcome the cyberphysical security challenges that arise from modern manufacturing techniques. It does so by streaming critical data directly into machines via a centralized authentication and authorization process. In particular, the solution characteristics include:

1. **Granular Authorization**: Several levels of permission for access, preview, editing, and authorizations to ensure individual users and groups only have necessary access.
2. **Monitored Operator Control**: Operator control is maintained while being monitored and restricted, if applicable.
3. **Device Support**: Due to a thin, operating client, most digital manufacturing devices can be supported, and legacy devices are easy to integrate.
4. **Distributed Responsibility**: Different sectors for manufacturing device, design owner, design transformation, and other factors spread the security risk from a single point of failure.
5. **Location Independent**: The solution can be deployed in central or hosted IT infrastructure.
6. **Data Fragments**: Only the data necessary for execution is transferred, and may be streamed for further protection.

Without such an approach, progress towards a more digitally-enhanced manufacturing environment able to improve productivity and produce higher quality and more relevant products is likely to be slow. Connecting manufacturing devices is a critical part of delivering such improvements, but without addressing legitimate security concerns, they will not progress.

In contrast to existing solutions, the direct-to-machine approach provides security in a number of meaningful ways:

1. **Integrated Security**: Direct-to-Machine Security builds on existing IT security solutions, which can be deployed to enhance the system.
2. **Layered Encryption**: Encryption in transfer with high-grade TLS and multi-layered encryption at rest with 256-bit AES. Encryption keys securely stored in separate locations.
3. **Always Up-to-Date**: Thin clients on devices mean that only central infrastructure needs updating.
4. **Minimum Sharing**: Authorized endpoints only receive minimum data required for execution.
5. **Integrity Protection**: In addition to theft, the delivery of lowest level data protects design integrity. Version, deletion, and expiration controls.
6. **Secondary Defense**: If data does leave the system it is traceable through watermarking and challenging to reverse engineer into a general design file.
7. **System Redundancy**: N + 1 or greater redundancy for all network components and system components.
8. **Threat Protection and Prevention**: Uninterruptible power and backup systems, as well as fire/flood detection and prevention, are used at storage sites.

The solution does not only enhance security and enable innovations to flourish; it creates a more responsive manufacturing environment better suited to the realities of today's shop floor. In particular, the solution:

1. **Permits Detailed Tracking**: Comptroller creates and tracks complete history of the part.
2. **Encourages Collaboration**: Security and central repository enable different firms and individuals to operate on their strengths: provide a small iteration to the design, run an engineering simulation, or complete material testing.
3. **Enables Distributed Manufacturing**: Trust in the network and ability to capture device feedback in real time allows production of parts closer to the point of use, enabling an entirely new, supply chain system.
4. **Delivers Automation**: Central processing improves automation potential as bottlenecks are identified, solutions can be more easily iterated on and deployed at scale.

Adopting a new security approach won't be easy. There are natural challenges with the approach, such as the necessity of a single point of failure. Mitigants, examples of which have already been discribed above, will need to be found in cross-industry collaboration. It is likely that these challenges will only be addressed

when the will to handle the overwhelming cyberphysical security risk in manufacturing has risen. While we have outlined that handling this problem is as much addressing a risk as it is unlocking an opportunity, the awareness of this among manufacturing executives is still low. Most likely the defense community, whose losses of manufacturing data have a cost that could go well beyond the billions of dollars in book value, will have to make this a compliance issue.

The alternative is that IT departments across the country begin to recognize manufacturing equipment as just another digital asset that needs protecting, and that the direct-to-machine approach is just a natural extension of an approach that they are already using to secure other types of data flows. What has changed is that manufacturing devices are now no longer separate from but part of that data flow. The direct-to-machine manufacturing approach is, for the first time, an approach to acknowledge that and move manufacturing into the digital century.

Acknowledgements This work is partially supported by Benjamin Collar (Siemens), Dr. Jeffrey Hieb (University of Louisville), and William Sobel (System Insights and MT Connect). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

Aliaga D, Atallah M (2009) Genuinity signatures: designing signatures for verifying 3D object genuinity. Comput Graph Forum 28(2):437–446. doi:10.1111/j.1467-8659.2009.01383.x

Ballou D, Wang R, Pazer H, Tayi G (1998) Modeling information manufacturing systems to determine information product quality. Manage Sci 44(4):462–484. doi:10.1287/mnsc.44.4.462

Bishop M (2015) Introduction to computer security. Addison-Wesley, Boston

Brocklehurst K (2014) DHS confirms US public utility's control system was hacked. The State of Security Newsletter. https://www.tripwire.com/state-of-security/incident-detection/dhs-confirms-u-s-public-utilitys-control-system-was-hacked/#. Accessed 12 Dec 2016

Grau A (2015) Can you trust your fridge? IEEE Spectrum 52(3):50–56. doi:10.1109/mspec.2015.7049440

Harper K, Gooijer T, Smiley K (2016) Composable industrial internet applications for tiered architectures. ABB Corporate Research. https://www.researchgate.net/publication/301846825_Composable_Industrial_Internet_Applications_for_Tiered_Architectures. Accessed 3 Dec 2016

Klein G, Andronick J, Elphinstone K, Murray T, Sewell T, Kolanski R et al (2014) Comprehensive formal verification of an OS microkernel. ACM Trans Comput Syst 32(1):1–70. doi:10.1145/2560537

Krebs B (2012) DHS warns of hactivist treat against industrial control systems. Krebs on Security. https://krebsonsecurity.com/2012/10/dhs-warns-of-hacktivist-threat-against-industrial-control-systems/. Accessed 3 Dec 2016

Graham J, Hieb J, Naber J. (2016) Improving cybersecurity for industrial control systems. In: 2016 IEEE 25th international symposium on industrial electronics (ISIE). doi:10.1109/isie.2016.7744960

Pan Y, White J, Schmidt D, Elhabashy A, Sturm L, Camelio J et al (2017) Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems. Int J Interact Multimedia Artif Intell 4(3):45. doi:10.9781/ijimai.2017.437

Sturm L, Williams C, Camelio J, White J, Parker R (2014) Cyber-physical vulnerabilities in additive manufacturing systems. In: Solid freeform fabrication symposium 2014. http://sffsymposium.engr.utexas.edu/sites/default/files/2014-075-Sturm.pdf. Accessed Aug 2016

Willis K, Wilson A (2013) InfraStructs. ACM Trans Graph 32(4):1. doi:10.1145/2461912.2461936