Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing (DDM) Systems

Dominick Glavach, Julia LaSalle-DeSantis and Scott Zimmerman

Abstract This chapter will address cybersecurity threats to the Direct Digital Manufacturing (DDM) community, including potential attack scenarios and motivations. Many of these insights are the result of direct observation. As an illustrative example, we will discuss the details of a security assessment performed on an Additive Manufacturing (AM) system used for rapid prototyping and complex part production within the defense industry. Protocols and associated recommendations for incorporating security best practices during system installation and subsequent operation will also be presented.

Keywords Additive manufacturing • Direct digital manufacturing • DDM • STL • Cybersecurity

1 Introduction

Applying meaningful and assessing impactful cybersecurity controls for Direct Digital Manufacturing (DDM) is an ongoing and significant challenge for the DDM community. This issue will exponentially grow in significance as DDM technology moves into the mainstream manufacturing supply chain and more businesses and organizations take advantage of the many benefits of producing parts directly from a Computer Aided Design (CAD) drawing.

The power of DDM to enable rapid prototyping and re-design, while decreasing the investment in tooling and re-tooling, is proving to be a means of re-birth in American manufacturing and manufacturing engineering. Further, this combination

D. Glavach · J. LaSalle-DeSantis · S. Zimmerman (✉)
Concurrent Technologies Corporation, Johnstown, PA, USA
e-mail: zimmerms@ctc.com

D. Glavach
e-mail: dg@CyberSN.com

J. LaSalle-DeSantis
e-mail: lasallej@ctc.com

L. Thames and D. Schaefer (eds.), *Cybersecurity for Industry 4.0*,
Springer Series in Advanced Manufacturing, DOI 10.1007/978-3-319-50660-9_7

of benefits is especially attractive to Department of Defense applications where innovative design is required in a more and more constrained budget environment.

Based on the expectation and potential impact in revitalizing the U.S. manufacturing landscape, DDM, including Additive Manufacturing (AM) and other similarly disruptive technologies, will have a significant impact on national security. According to the National Defense University:

> The propagation of this technology has generated a host of national security considerations, which connect to broader economic and policy developments. AM can benefit the national security and defense community largely due to its economic potential. Additionally, the deployment of AM technologies in manufacturing will likely promote greater interaction between the national security community and the private sector, as businesses will be able to produce prototypes and sophisticated components more inexpensively and quickly than before (McNulty and Armes 2012).

The Economist (2014) refers to the potential for DDM to create the third industrial revolution, noting that the disruption to manufacturing will be as significant as digitization was to telecommunication, office equipment, photography and publishing. While DDM creates an incredible growth potential within manufacturing, it also comes with many of the associated cybersecurity risks that threaten other digitized industries.

Due to the potential economic and security implications of DDM, the industry is challenged to address cybersecurity risks in a timely way and develop standards, systems and processes for security before such wide scale adoption of the technology limits, or prohibits, the deployment of protection mechanisms.

While organizations like the National Institute of Standards Technology (NIST) and American Society for Testing and Materials (ASTM) are working to standardize the test products, geometries, and format of .STL files of AM, the industry would be well served to consider the lessons of rapid growth in other industries, such as power and energy, to ensure that security is a consideration right from the start.

1.1 Power and Energy a Case Study: Consequence of not Addressing Security Before a Technology Infrastructure Is at a National Level

The negative impacts of failing to include security processes and protocols at start-up can be seen within the power and energy sector. In this sector there are large deployments of programmable logic controllers (PLC) and supervisory control and data acquisition (SCADA) systems. At the time of design and deployment, these systems were not equipped with adequate security mechanisms and reliability protocols and methodologies simply did not exist.

Subsequently, in 2003, North America experienced its worst blackout to date, as 50 million people lost power in the northeastern and midwestern United States and Ontario. In some areas, power was not restored for nearly a week.

The Canada Power System Outage Task Force was formed to investigate how to prevent future blackouts and reduce the scope of those that occur. They concluded in a 2004 Final report that their single-most important recommendation is for the U. S. government to make Reliability Standards mandatory and enforceable. And so, in the Energy Policy Act of 2005 bulk electric providers were tasked to comply with the audits of a self-regulatory "electric reliability organization" called the North American Electric Reliability Council (NERC) and associated Critical Infrastructure Protection (CIP) 002-009 guidelines.

Complying with these energy and power security guidelines, after the control and data systems had become so tightly woven into the fabric of the power grid, and retrofitting security, became a much larger and more costly endeavor, than if the task of creating robust auditable security mechanisms and protocols had been tackled in the beginning. And while it's impossible to determine exactly, the costs and dangers associated with the 2003 prolonged blackout may have been mitigated if security mechanisms and reliability protocols and methodologies had been in place before the SCADA-based grid was allowed to blossom (US-Canada Power System Outage Task Force 2003).

The DDM community now stands on a similar precipice as the power and energy community did in the early 2000s. The emerging infrastructure for a technology so clearly in demand in both private and defense markets needs to define security guidelines, methodologies, and protocols before its reliability is compromised, security is breached, and a blackout-like incident occurs.

2 Defining Direct Digital Manufacturing

In a 2011 Brooking Institute web article, DDM was defined as "the fabrication of components in a seamless manner from computer design to actual part in hand. Also known as "3D printing" or "additive," "rapid," "instant," and "on-demand" manufacturing, DDM uses 3D computer-aided design files to drive the computer-controlled fabrication of parts. This next evolutionary move within manufacturing is driven by new hardware and software driven systems that use a variety of components and ingredients to build up layers of materials to create complex three-dimensional structures. These structures are designed, modeled and tested entirely within the cyber world prior to manufacturing. The Brooking Institute article details the process further:

> Unlike traditional machining methods, which involve working from a rough mold and then cutting away to achieve the desired complex shape, direct digital manufacturing creates the shape precisely and instantly, using additive fabrication. This new approach to manufacturing is a disruptive and potentially game changing technology (Schuette and Singer 2016).

With applications of the DDM technology rapidly evolving into the mainstream and defense pipeline, the importance of relevant and meaningful cybersecurity controls and reliability is also increasing. Imagine the impact to DDM pace-makers, or custom hip replacements if the supporting systems become unstable or unreliable. Imagine the impact if a nation-state actor or terrorist is able to modify the digital representation of a jet engine nozzle or if the DDM components in a counter-improvised explosive device (IED) cannot be deployed.

2.1 Installing a "New Printer"

The problems of applying rigorous cybersecurity at the onset, are compounded by the 'wild west' feeling of innovation. Opportunities to apply the DDM manufacturing technique to solve pressing problems for economic gain, are so dazzling that a slapdash security approach to incorporating DDM can occur. As an example, our involvement and interest in DDM cybersecurity began one day after a help desk call was placed asking if a technician could assist in attaching a new printer on the shop floor to the network. This task was originally assigned to a desktop technician whose principal responsibility is to perform basic break/fix activities of desktop software and hardware. Their tasking also includes installation and management of network printers and associated queues. So the technician dutifully found the appropriate Ethernet cable to attach it to the shop floor network, performed some basic configuration of the "printer" and let Dynamic Host Configuration Protocol (DHCP) do the rest.

Little did the technician and the rest of the internal information system management office know that this printer wasn't just a printer but a highly calibrated $750,000, dual-laser melting additive manufacturing system, or 3D printer. The importance, complexity and cost of the system would've been nice to know.

In this particular case, the AM equipment was delivered to the 'manufacturing' floor, unboxed and set up all without the awareness of the IT department. Once installed, the AM engineering team connected with the Enterprise Help Desk and requested "can you help connect our new printer to the network?" Unwittingly, the request was executed. Needless to say, the original equipment manufacturer (OEM) was unable to connect to the AM equipment, since it was behind the corporate firewall. Subsequent requests were submitted to the Enterprise Help Desk requesting that the OEM be given access to the equipment through the Internet for fine tuning. The printer was transferred to an open Internet connection normally provided to corporate guests. This channel is monitored, yet it has minimal shielding. It was only after subsequent investigation by the information security team that it became clear that the "printer" was in fact a metal DDM printer, not a typical office document printer. Following this discovery, the security team has moved the printer to a more secure and scrutinized subnet on the network where additional security controls and enhanced logging occur routinely and where it is still possible for the engineering team to work directly through the network with the manufacturer.

After this original connectivity was made, the materials engineers contacted the AM system manufacturers, a German owned and operated firm, and began to attempt to connect to the system over the Internet. What we later found was that this remote access to the system from the manufacturer is commonplace for the initial setup and calibration of the system, as well as for ongoing periodic access for maintenance and build troubleshooting. In this case, the printer in question could not initially be accessed directly from the Internet, as it was deep within the organizational security perimeter. So a request was made to create a hole into the company's security perimeter to allow access to the printer. This is when the security team was finally brought onboard, the threat profile and security assessment were performed, and mitigation steps taken.

To describe this phenomenon of bolting security on to a system post implementation we coined the term "the stagecoach principal." The stagecoach changed how goods got from point A to point B. It all worked well until someone noticed that there was something on the stagecoach of value and something they would want. So the robbers started to ride down from the hillside with weapons and take what they wanted. This happened because there was no active defense. So what did the stagecoach owners do? They put a marshal or person with a weapon on the stagecoach to protect it. The next time around, when the robber brought a stronger force, bringing his buddy and another horse, what does the stagecoach company do? They put a few extra horses in the rig and so the spiral continues. If they would have thought of their vulnerabilities up front the stage coaches could have avoided all of those evolutionarily mistakes.

Similarly, we continually make these types of mistakes in our push to get new technology into the mainstream market prior to developing mechanisms to update and secure them. Today is the time to think about inserting security into the digital thread, before it's too late.

3 Security Lessons from Past Industry Digitization

Digitization is as disruptive to manufacturing as it was to telecommunications, photography, and publishing. While there are many other examples, it's informative to look at the impact of digitization on security in the telecom and the previously introduced power and energy industry. Each of these industries experienced extra-ordinary fast paced growth that did or could outpace security.

3.1 Telecommunication: An Organizational and Policy Approach to Security

As privileged enablers of the digitization mega-trend, telecom companies are scrambling to find ways to monetize the infrastructure they already have in place.

The world is becoming more and more connected. Sometimes called the Internet of Things (IoT), all of our devices, more and more can communicate with each other over—with even our home thermostat connected to our watches—and the telecom industry is struggling with how to keep up with this ever increasing demand. Further, the growth of many services, like Netflix and Pandora, leverage what the telecom industry has built through 4G and 5G s, without giving much (if anything) back to sustaining the data infrastructure.

> Because many of these new services are managed in cloud-based systems, the digital environment will require a higher level of security and privacy protection than currently exists. That potentially presents yet another opportunity—it could be called a duty—for telecoms to set the benchmarks and standards for safeguarding the sensitive personal information shared by consumers, companies, and machines over these ubiquitous networks (Friedrich 2015).

As custodians of the networks, telecom carriers are charged with fighting the new threats. To address this, as well as many issues, many telecom providers are now appointing Chief Digitization Officers (CDO). CDOs for telecom networks will need to identify strategies to build features and security parameters that will ultimately end up largely shaping the future of the IoT and complementary applications. Like the power and energy sector, telecom networks are an integral part of a country's critical infrastructure and act as a backbone in enabling and linking the other critical components.

3.2 Power and Energy: A Lesson About the False Separation of Operational Technology Versus Information Technology

In some traditional security approaches, a distinction is made operational technology (OT) and information technology (IT). We have found this OT versus IT approach to be problematic, because currently the DDM "digital thread" spans both the OT and IT realms. As such, it inherits organic risks from each. For DDM, this means the lines between OT and IT, as traditionally understood, are blurring rapidly. Again, we can gain insight by looking at the lessons learned in power and energy.

Gartner, one of the world's leading information technology research and advisory company, defines **Operational Technology** (OT) as hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise. **Information Technology** (IT) is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services (Gartner 2016).

One common strategy of securing the IT side of the network from the operational side is to implement what is known as an "air gap." This air gap simply means that the networks have no direct connections between them. This approach breaks the "digital thread" as files must now be carried by hand from the design network (IT) to the manufacturing floor (OT). However, the "air gap" is rarely a successful security practice, as connections are the inevitable result of fast paced innovation and are bound to be made.

The "air gap" approach to cybersecurity has many other issues resulting in deficiencies, best illustrated in the power and energy case study. According to Sean McGurk, former Director, National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security, in a "Right Signals Blog" post:

> In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the Supervisory Control and Data Acquisition (SCADA) system or energy management system (EnMS) separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network. (Mackenzie 2016)

For DDM applications, we can leverage this finding. It seems clear that while this approach might be attractive due to its surface simplicity, the air gap no longer works. There are too many interconnected systems between the shop floor, the enterprise network and external partners. In a 2016 Cisco white paper:

> Today manufacturers need "defense-in-depth" strategies that incorporate layers of independent security controls (physical, procedural, and electronic). In an era of converged IT and OT networks, cloud computing, mobility and Internet of Things (IoT) platforms, a holistic approach to data security is required.

Further, analysts say the benefits that come from managing IT and OT convergence, alignment and integration include optimized business processes, enhanced information for better decisions, reduced costs, lower risks and shortened project timelines (Pettey and van der Meulen 2011).

4 Defining the DDM Cybersecurity Threats, Vulnerabilities, and Risk Management

The potential impacts and damages perpetrated by cyber attacks are well known to businesses and manufacturing operators. The impact can range from physical and environmental damage to intangible impacts such as brand reputation and customer trust. Economic losses can be particularly severe in industrial settings, where an attack can cause losses of millions of dollars in downtime, disrupt production schedules and, in our assessment, damage expensive machines. In the worst case, the health and/or safety of workers may also be at risk, and in the case of a DoD application, even national security.

4.1 Tenants of DDM Cybersecurity

The tenants of cybersecurity are to preserve confidentiality, integrity and availability.

- **Confidentiality** is the tenant of cybersecurity focusing on protecting information from disclosure to unauthorized parties. Confidentiality refers to the need for the secure transfer and storage of information. A DDM example of a security control to protect confidentiality would be encryption of CAD data at rest on a device or data in transit over a communication link.
- **Integrity** is the effort of maintaining and assuring accuracy and consistency of data over its entire life-cycle. Integrity is a critical objective and component within DDM. In our assessment, we saw many examples of mishandling and control of data files including CAD, ".STL", etc.
- **Availability** refers to ensuring that authorized parties are able to access information when needed. This would include the shop's need to communicate with the AM printer OEM. You may not think of availability as a cybersecurity objective but if an adversary can keep you from accessing your systems and data there is a huge competitive advantage.

As you can see in Fig. 1, the three tenants of cybersecurity are tightly integrated.

4.2 DDM Cybersecurity Threats

DDM is advancing at an exponential rate in capability, complexity and speed. As the exponential rate of change increases there is a proportional increase in cybersecurity risks. These risks can compromise the confidentiality, integrity, and integrity of DDM systems. The threats can disrupt information systems, slow operations, halt production, impact product quality, compromise intellectual property or influence company reputation. Understanding DDM cybersecurity risks and developing strategies to manage cyber risk are key factors in DDM cyber resiliency.

Integrity
Availability
Cyber Security
Confidentiality

Fig. 1 Tenants of cybersecurity

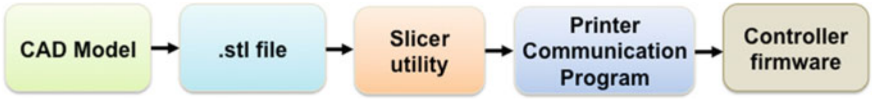


Fig. 2 Additive manufacturing digital thread

A key term used to describe the lifecycle and flow of information within the DDM process is "digital thread." The digital thread describes how the product's design and manufacturing information is authored, exchanged, and processed. A visual representation of the DDM digital thread is presented below, in Fig. 2. The process begins with the CAD 3D file that a draftsman or engineer uses to model and draw the piece. A CAD file can also be producing by scanning an object. An output of almost any mainstream CAD program is the .STL file. The .STL file communicates the details of the piece's surfaces to the hardware that will print/produce it. The slicer utility provides for the interpretation of details associated with printing (such as orientation) and allows for an opportunity to manipulate those details or 'tune' the model. The slicer utility is what cuts the 3D model into tiny digital sections that the 3D printer (firmware) can produce in the next steps of the digital thread.

There are several steps on the additive manufacturing digital thread, as shown in Fig. 2, where an attack could take place: the CAD model, the .STL file, the toolpath file, and the physical machine (controller firmware) itself. All along this digital thread there is an attack surface where the intellectual property or design can be stolen or compromised. In our assessment we saw the risks with poor configuration and data management practices and residual data left at each step on the thread.

4.3 DDM Cyber Vulnerabilities

DDM systems store data, process data with network connectivity and suffer similar cyber risks to corporate networks, laptops and mobile devices. These traditional cyber risks combined with DDM market growth presents attackers with new and potentially valuable targets. New attack opportunities include disrupting processes and facilitating theft, counterfeiting, and enabling sabotage.

Intellectual property is the most valuable target and is often under protected when in the form of an STL file.

Understanding the adversaries approach to attacking DDM systems enables stronger defense priorities and incident response strategies.

Cyber threats to manufacturing enterprises may be motivated by espionage, financial gain or other. These are digital assets so the same cyber controls that are in play to protect your home or business still apply. Things such as firewalls, intrusion detection systems and proxies should not go away.

DDM systems are complex, and so, also are attacks on DDM systems. Sophisticated and funded, competitors, partners, criminals, state actors and terrorist elements must have all the resources needed to accomplish these attacks. Let's take a look at a few of the motivations for attack.

Economic Advantage: The criminal element will get involved, any time there are goods for sale. These attackers are often not be as technically astute but they can have the capacity and resources to employee mercenary attackers as needed. This goes back to our stagecoach principal; the folks who attacked the stagecoach were not after the horses and the coach, they were after the goods, the gold and the money. There are people making significant amounts of money in this space.

Military Advantage: There are strategic and tactical military advantages to sabotaging a DDM system that entices nation state and terrorist actors. These attacks are high reward in that they may have the potential to negatively affect the operation of weapons systems on the battlefield.

Political Activism: Today we are printing products, engine parts, consumer goods and even jewelry. What could be the impact when DDM systems begin to print bio parts at scale? Printing bio parts raises ethical issues of human enhancement, population control, black market trafficking and grabs the attention of political activism (i.e. hacktivism).

DDM is advancing at an exponential rate in capability, complexity and in speed. As the exponential rate of change increases there is a proportion increase in cybersecurity risks. These risks can disrupt information systems, slow operations, halt production, impact product quality, compromise intellectual property or influence company reputation. Understanding DDM cybersecurity risks and developing strategies to manage cyber risk are key factors in DDM cyber resiliency.

4.4 DDM Risk Management Overview

Successful DDM risk management encompasses the traditional risk management processes at each component and along the entire digital thread. Managing risks along the digital thread enables the application of adequate controls to appropriately compensate for specific risk levels. Each element along the digital thread undergoes the following process.

Step 1: Identify the Risk. Identify vulnerabilities and threats with a potential for loss to availability, integrity, confidentiality. Vulnerabilities are defined as a weakness or likely deterioration in security. Threats are defined as an exploitation of a security weakness.

Step 2: Analyze the risk. Determine the likelihood and impact of each risk by developing an understanding of the risk, impact to the specific digital thread and the potential to affect the entire digital thread.

Step 3: Evaluate the Risk. Evaluate the risk by determining the risk magnitude, (the combination of likelihood and impact), technical control to minimize risk or categorized the risk as acceptable.

Step 4: Risk Controls. Risk control is the process of implementing controls or documenting acceptable risk for future evaluations

The technical advances and economic impact associated with the DDM revolution attracts an innovative and entrepreneurial audience. History shows us that new technologies have a tendency to influence a criminal opportunity via unexpected exploitation avenues. From the stagecoach to smart thermostats, security has often been an afterthought in new technology design and implementation.

In Mellissa Hathaway's paper, "Leadership and Responsibility for Cyber Security," Ms. Hathaway submits that corporate and government leadership are reactive in nature to cybersecurity needs and only act to mitigate security issues after a significant event occurs. (Hathaway 2013) She further concludes that additional legislation may be needed to incentivize corporate and government leadership to get serious about cybersecurity. Her point is further validated in the example of security and bulk energy providers described earlier in this chapter. It took a major power blackout that lasted several days for the government to create an energy security standards organization and demand bulk suppliers to comply.

The complexity and critical nature of some products being produced by DDM, ranging from fuel nozzles to human organs, render these systems obvious targets for cyber criminals, espionage actors, or digital activist groups. Regardless of motivation, gaining access to an industrial DDM system is not a trivial action and requires an intricate, but likely, attack scenario, that results in one of the following:

1. Theft (processes and property)
2. Disruption (slowing or stopping the DDM process)
3. Sabotage (inserting unforeseen time-delayed failures)

The combination of system complexity, installation methods and manner in which digital models become manufactured objects create a large attack surface. Within our assessment we focused on a few potential attack scenarios and associated risk evaluations which included:

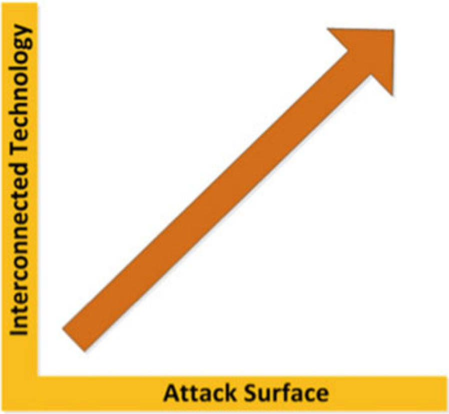
1. Model file formats
2. Data storage and transfers
3. Printer components software and firmware
4. Preproduction software
5. Engineering and production practices

We examine each of these areas in detail later in the chapter.

4.5 DDM Cyber Risks: Theft, Disruption, and Sabotage

We have bucketed what we feel are the current main risks to DDM as: Theft, Disruption and Sabotage. In addition to the new potential risks created by DDM, the traditional cyber breaches such as system compromise, unauthorized logins, viruses and ransomware are still in play. DDM systems are complex with

Fig. 3 Attack surface



potentially large attack surfaces. **Attack surface** refers to the number of things within a system that are vulnerable to attack. Your attack surface could be the STL file, printer or DDM process or model. As these systems become more obtainable to the masses, and organizations can produce goods-on-demand the system attack surface will continue to grow as seen in Fig. 3 below.

Theft—Property theft, in terms of intellectual property loss, refers to attacks that enable an adversary to reproduce physical products. Theft can be thought of in terms of process theft and license theft. Process theft is accomplished when an attacker is able to observe DDM processes in motion or recreate processes through inference by collecting data files on related but not connected systems. License theft is circumventing a right to use control to either extend beyond the intended usage time or duplicate DDM products beyond the intended quantity. License theft has a long history. As an example, not long after CD-ROMs and DVDs were used for movie distribution, someone figured out how to break the license or protection of the system and mass produce copies of the movies and then illegally distribute them.

Disruption—Disruption results in halting or delaying the DDM process through system compromise or data manipulation. For example, disruption can occur by modifying instruction sets to overheat components resulting in temporary or permanent physical damage to DDM printers.

Sabotage—Sabotage attacks impact DDM product reliability in a manner that is unnoticed by quality control processes. Sabotage includes modifications resulting in a reduction in reliability to include: slightly reducing the surface strength, slightly increasing the product size, reducing cooling speed and modifying product-infilling. Sabotage attacks on product reliability have measurable quantifiable costs including the cost to recall or the cost to remanufacture. The impact to reputation may have larger and long-term impacts.

5 Walking the DDM Digital Thread

Weaknesses and vulnerabilities within DDM systems are comparable to those within Industrial Controls Systems (ICS) elsewhere on the manufacturing shop floor. In fact, a good portion of the technical makeup of DDM systems is Programmable Logic Controllers (PLCs), which are embedded systems and actuators. This integration of ICS means that the same security vulnerabilities and weaknesses are inherited in DDM systems. According to a report produced in June of 2016 by the Department of Homeland Security Industrial Control System Computer Emergency Response Team (ICS-CERT 2016) the top six weaknesses that the team found fell into one of six categories.

1. Boundary protection
2. Least functionally
3. Authenticator management
4. Identification and authentication
5. Least privilege
6. Allocation of resources

The ICS Impact: A Case Study of Stuxnet

In August of 2011, a game changing computer worm began to get more and more press and notoriety. Little did the world understand at the time that the computer worm we now call Stuxnet would give rise to a continuously growing cyber war. Stuxnet was a 500 kilobyte computer worm that infected at least 14 industrial sites in Iran. The Stuxnet cyber kill chain operated in distinct stages; first through delivery removable media (USB Drives) and by replicating itself, targeting Microsoft Windows machines and networks, second it sought out Siemens Step7 software, which is used to program Industrial Control Systems (ICS) that operate equipment, and lastly it compromised the programmable logic controllers 11 that controlled the centrifuges. What this process delivered was the ability for the source creator to remotely monitor and spy on industrial control systems and cause the centrifuges they controlled to burst without anyone detecting the worm. This attack replicated itself globally creating many variations of the Stuxnet worm during the past few years. On the heels of the Stuxnet news, the U.S. Defense Secretary warned that the United States was vulnerable to a "cyber Pearl Harbor" that could derail trains, poison water supplies, and cripple power grids. The Secretary also noted that not only was there potential for physical damage to a system, like what was seen in Stuxnet, but also even greater potential of non-physical damage, such as stealing personal or sensitive data (Kushner 2016).

To further enforce how Stuxnet changed so much within the ICS space the FireEye report also stated "The discovery of Stuxnet in 2010 drove interest in industrial control systems (ICS) vulnerability research. FireEye iSIGHT Intelligence counted just 149 ICS vulnerability disclosures that were made between January 2000 and December 2010. Through April 2016, we have counted 1,552. We anticipate this upward trend will continue (Zhou 2016).

5.1 Data Storage and Transfers

During our team's assessment of the additive manufacturing system we observed heavy use of USB drives for data storage and transfer. This was mainly due to the fact that the systems were not networked together and the only means to move the design from the IT network to the OT network was through the use of this technology. There are many inherit risks using this type of media, including configuration management of both the physical device as well as loss or theft of the data on them.

In defense of the designer and material engineers, their first thought isn't: "How I am going to protect this data?" It is: "How am I going to get my job done?" To determine if there is a better way to accomplish this data storage and transfer we contacted the printer vendor. After a bit of discussion they provided two recommendations. The first, is a rather clunky recommendation: connect the printer to the network when printing and, when done, simply disconnect. The second, and vendor-preferred method, was that the client should use the USB drives.

This advice of just use the USB on the surface may seem like a good workaround but as seen within the spread of Stuxnet in the not too distant past, the high-profile attach was born of USBs. Both of these possible strategies are heavily dependent on training and awareness.

5.2 Stereolithography File Attack Research

As mentioned earlier the ".STL" (STereoLithography) is a file format native to CAD software created by 3D Systems. The ".STL" file type is the current defacto standard in AM. The STL file only contains the surface information of the part. At the February 2015 Direct Digital Manufacturing Cybersecurity Symposium hosted by the National Institute of Science and Technology (NIST), Christopher B. Williams Associate Professor, Virginia Tech Department of Mechanical Engineering presented research that he and his research team were able to intercept a job initialization file and decode it, allowing attackers to potentially alter printer parameters mid-print. The STL standard files are especially vulnerable to attacks that alter a design within the digital thread. The VA Tech research presented additional information on the ".STL" file and its makeup as a stored list of triangular elements (specified by the a set of x, y, and z coordinates of three vertices) in ASCII or binary format. An attack that simply edits the STL file could subtly alter the part geometry.

As a part of the research, and to further determine the potential impact of this specific attack, the VA Tech team conducted two experiments.

- **Experiment 1, a Printed Void**: The first experiment evaluated the effect of a "printed void" on the mechanical strength of a printed specimen. Several ASTM Standard D638-10 tensile test specimens with and without voids were printed via Powder Bed Fusion (a Sinterstation 2500 Plus machine) using Nylon 12 powder. Upon testing, all of the specimens containing voids fractured at the void location, while the specimens without voids failed normally. The average reduction in yield load was 14%, from 1085 N to 930 N, and the strain at failure was reduced from 10.4 to 5.8%.

- **Experiment 2, Feasibility of an Attack**: Second, a case study was performed to determine the feasibility of a cyber-attack on a simple AM system and to evaluate the ability of AM operators to detect an attack. In this experiment, upper-level and graduate engineering students were challenged to manufacture and test a tensile test specimen. Unknown to the participants, the computer used was infected with ".STL" attack software that automatically inserted voids into their files before fabrication. Upon completion of the printing, none of the participants detected the presence of the voids in their parts. Upon breaking the part, all participant teams identified that their parts failed prematurely. Two teams detected the presence of a void at the fracture location. However, both of these teams concluded that the placement was due to problems with the machine. Two teams did not notice the voids and attributed the failure to the anisotropic nature of additively manufactured parts.

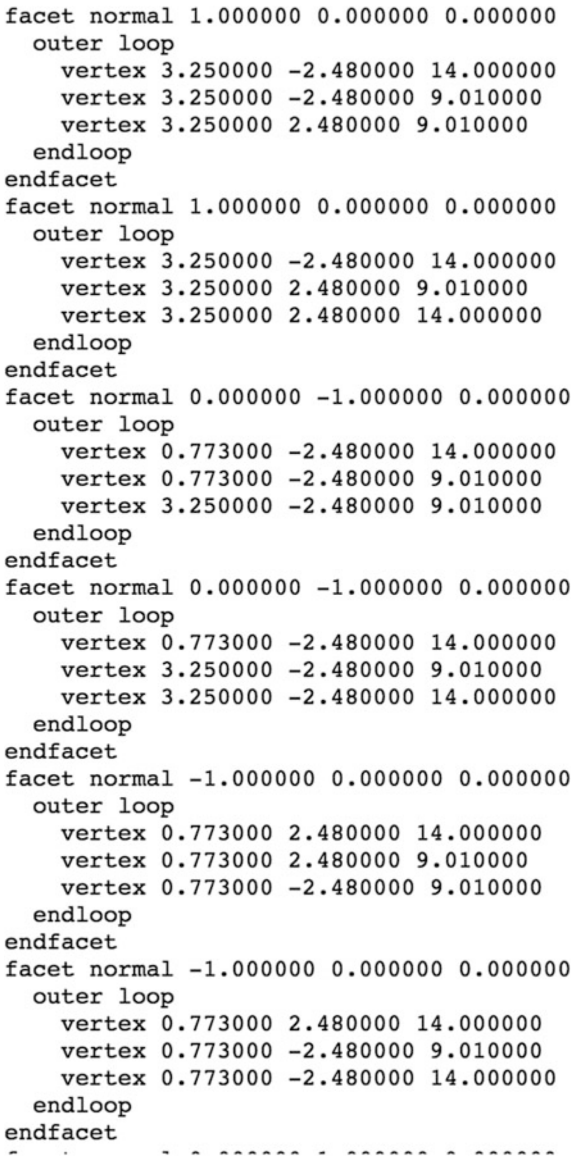
It was the VA Tech team's conclusion that attacks on STL are a viable attack avenue and the STL and other file formats should not be scrapped but that additional security protection should be put in place. These controls and mitigation steps included:

- File hashing that would allow the user to validate the authenticity of the file
- Improved checks within the quality control process
- Improved process monitoring through the development of a "side channel". This method creates a baseline operating parameter so that deviations could be detected
- Operator training (Williams 2015).

This last item, Operator Training, is probably the most impactful. It is the observation of the authors, that, in addition to the six weaknesses identified above by ICS-CERT (boundary protection; least functionally; authenticator management; identification and authentication; least privilege; and allocation of resources) we have also seen another increase in misconfiguration of settings. While the ICS-CERT team has identified the 6 weaknesses, a theme that our assessment teams sees on a regular basis is that of a lack of cybersecurity awareness training. While this is the most "low tech" of the weaknesses it pays the highest dividend in outcome (Fig. 4).

The easy access or wide adoption of a trusted file format like the ".STL" has its pros and cons. Because it is trusted, we are willing to download it and print it without much thought. These files are widely available on the Internet from various websites, both trusted and untrusted. When these files are downloaded off these unknown or potentially untrusted sites there is also no file integrity. The ".STL" files comes in two formats, binary and ascii which is human readable.

Fig. 4 Sample STL file



```
facet normal 1.000000 0.000000 0.000000
  outer loop
    vertex 3.250000 -2.480000 14.000000
    vertex 3.250000 -2.480000 9.010000
    vertex 3.250000 2.480000 9.010000
  endloop
endfacet
facet normal 1.000000 0.000000 0.000000
  outer loop
    vertex 3.250000 -2.480000 14.000000
    vertex 3.250000 2.480000 9.010000
    vertex 3.250000 2.480000 14.000000
  endloop
endfacet
facet normal 0.000000 -1.000000 0.000000
  outer loop
    vertex 0.773000 -2.480000 14.000000
    vertex 0.773000 -2.480000 9.010000
    vertex 3.250000 -2.480000 9.010000
  endloop
endfacet
facet normal 0.000000 -1.000000 0.000000
  outer loop
    vertex 0.773000 -2.480000 14.000000
    vertex 3.250000 -2.480000 9.010000
    vertex 3.250000 -2.480000 14.000000
  endloop
endfacet
facet normal -1.000000 0.000000 0.000000
  outer loop
    vertex 0.773000 2.480000 14.000000
    vertex 0.773000 2.480000 9.010000
    vertex 0.773000 -2.480000 9.010000
  endloop
endfacet
facet normal -1.000000 0.000000 0.000000
  outer loop
    vertex 0.773000 2.480000 14.000000
    vertex 0.773000 -2.480000 9.010000
    vertex 0.773000 -2.480000 14.000000
  endloop
endfacet
```

5.3 Printer Components

Generally once DDM systems are setup, calibrated and optimized, there is minimal continuous monitor and patching of the operating and control systems. A key finding during the assessment was that the operating systems on the printer, both Linux and Windows, were not even close to being up to date with patches and updates. When we spoke to the printer vendor and asked for their recommendation as to the best way to keep them up to date, they said "unplug the printer from the network when you are not using it". They clearly thought about it but a solution was simply not high on their "to do" list. Actually, in defense of the manufacturer, they did have Antivirus software on the printer. The only issue was that it kept interfering with the manufacturer and the material engineer when they were calibrating and troubleshooting, so they turned it off. It also didn't help that the version of the Antivirus software was in the German language.

In addition to operating and control systems, there are network settings within these printers that allow each subsystem to communicate. Each operating system had its own TCP/IP network stack communicating on a non-routable 10.x net.

5.4 Engineering and Production Practices

As a simple illustration of the lack of configuration management of data files, we located an Internet born ".STL" file example and emailed it directly to a material engineer's account. We crafted the email as though it looked like it came from the printer manufacturer as a tool to calibrate the printer. We named the file, printer.stl. exe and included it as an attachment on the email. Sure enough the engineer prepped and sent the ".STL" file to the printer without a second thought. This is not only a problem within the manufacturing space, we see it all the time with specially crafted email asking the recipient for an immediate response to open a Microsoft Word document and before long the system is infected or worse encrypted with ransomware.

Ransomware has become more and prevalent and if our calibration file would have included ransomware the results could be catastrophic.

As previously mentioned, USB drive or removable media use was relied on heavily by the materials engineer to transport data from CAD to a model file to ". STL" file. The revision control or configuration management was non-existent. There were uncontrolled copies of intellectual property in every location along with the residual data that could become extremely valuable to an attacker.

These printers require a lot of continued technical and maintenance support from the manufacturer, especially at initial deployment. To enable this, the German manufacturer installed remote control or remote access software on the printer that is configured to allow them to connect to the printer remotely. This could potentially create International Traffic in Arms Regulation (ITAR) issues. Not only was this software setup to allow for client controlled remote access, it also had a self starting function that enabled it whenever the printer was turned on. So without the client knowing, the manufacturer could remotely access the system at any time.

Not all remote access is bad. If done correctly, remote access for technical support can be powerful and cost effective method. However, that was not the case with the findings in our assessment. All settings were default and the communication protocols were all unencrypted. Overall remote access systems are one of the top three targets for an attacker. Leaving them set in default and wide open was a critical finding.

5.5 Assessment Methodology

AM systems can be complex, consisting of several central processing units (CPU) and PLCs, operating systems, and applications. The list includes both AM-specific components as well as applications that support the user experience, such as web-browsers and Portable Document Format (PDF) readers. The CPU/PLCs communicate via standard network protocols such as TCP/IP within the printer and then to a gateway interface for larger network access. The operating systems and applications on these controllers process design data to produce 3D components.

The assessment team utilized both our company's proprietary security assessment methodology as well as the security risk assessment provided in the NIST Draft NISTIR 8023, "Risk Management for Replication Devices" (Paulsen and Dempsey 2015).

5.6 System Assessment

Our team had the opportunity to conduct a security assessment on a newly installed AM system. The assessment methodology we used was developed by our team over a number of years and included a toolset that was mainly focused on IT systems.

The focus and priority of the materials/manufacturing/engineering staff are installation and operation, which includes connection to the internal and possibly external (OEM) network, so the relevant parts can be produced. Their concerns are usually not about how to make this system secure.

What we found was:

(1) Most applications and OS's unpatched
(2) Factory default install of AV/Host IDS (plus German language)
(3) No process for updating/patching
(4) Residual data left everywhere
(5) Poor authentication (shared/default passwords)

6 Recommendations

- Mandatory scanning (enumeration) of system prior to deploying to the network and disabling of all unneeded communications/system processes

- Review of user accounts/groups on the system including their level of privilege and accordingly adjust
- Removal of all unneeded applications installed on the system (browsers, readers, games, etc.)
- Enable host-based firewall to allow communication via secure ports to know IP addresses for manufacturer communications (disable this connectivity when not in use)
- Develop, document and train for system updates/upgrades processes

According to a 2016 Cisco report:

> To thrive in the new threatscape, manufacturers need to implement new strategies and architectures.

"Defending the edge" with firewalls and access management is as necessary as a strong OT segmentation strategy, both of which are generally lacking in ICS networks today. But this is only part of the solution in today's vulnerable industrial environments, where threats can originate both outside and inside the factory, and may be unintentionally caused by human error." (Cisco 2015)

In addition, manufacturers must also give the task of securing the shop floor to the Chief Information Security Officer and allow him to assemble a team made up of both OT and IT professionals to ensure that the flow of information from the enterprise network (design, modeling, etc.) to the shop floor (toolpath and manufacturing) is uninterrupted and secure.

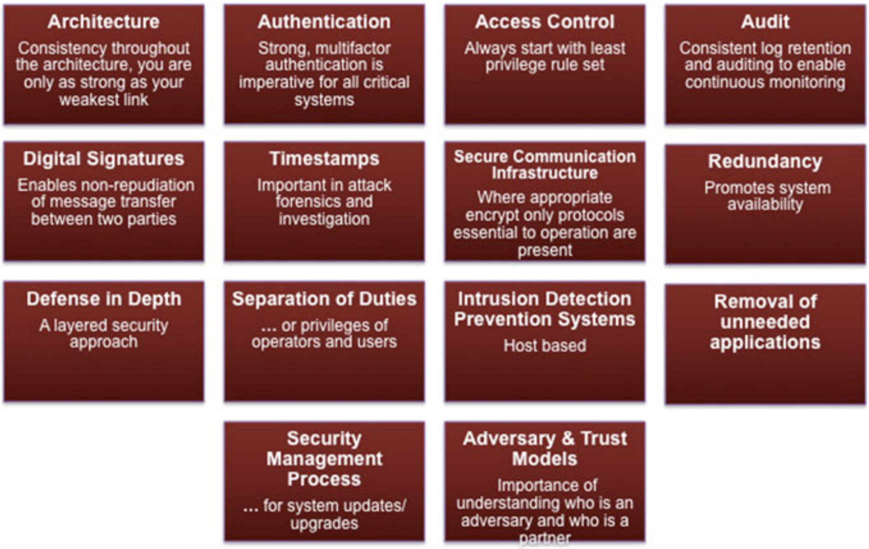
On a broader scale, the DDM community would be well-served to consistently advocate whenever possible for the implementation of security processes and standards, before a black-out incident suffered by the power and energy sector. This could come in the form of advocacy within professional groups, as well as internally promoting awareness all along the chain, from fabricators on the shop floor, to engineers. We recommend that standards, systems and processes be developed before technology is adopted broadly and when it limits or prohibits deployment of protection mechanisms.

7 Conclusion

DDM systems are an innovative and on-demand technology that represents game changing advances to supply chains, consumer goods and economic growth. In the same manner DDM systems are presenting new opportunities for innovation and creation, they are creating new cyber-attack vectors and scenarios that could present potential negative impacts to supply chains, military equipment and consumer confidence. The DDM systems are complex system of systems comprising of multiple Operating Systems, input/output peripherals, networks and process data from media types ranging from CD/DVDs, serial connections and USB thumb drives. The complexity and consistent calibration creates a hesitation from system owners to execute routine cyber hygiene (updates, strict user authentication, screen locking, inactivity timeouts and excessive service removal) activities. The lack of routine cyber hygiene maintenance creates an environment where IT or cybersecurity staffs isolate DDM systems on disconnected or “air gap” networks. The system owner’s hesitation to update and operational staff’s urge to segregate on another network compounds the cybersecurity risks, further expanding the DDM attack surface.

At a minimum for manufacturers, it is necessary to identify high-impact, quick-mitigation risks by assessing each DDM system as an individual system in the first iteration of the assessment process. Identifying high-impact, quick-mitigation risks increases cyber resiliency removing low effort opportunities to exploit vulnerabilities. Then, do a comprehensive risk assessment with planning for both mitigation and acceptance steps. It is imperative that security be an up-front consideration throughout all aspects of the equipment and process lifecycle, from design through disposal. If this is not the case and the cybersecurity staff does not develop processes and technology to mitigate risks and threats throughout, these systems will become increasingly insecure as the operational staff will find ways to circumvent implemented security controls. The following is a discussion of focus areas for DDM cybersecurity staff (Fig. 5).

Architecture—Cybersecurity consistency throughout the architecture. Identify and address high-impact quick mitigation risks and position DDM systems on networks that preserve integrity, availability, and confidentiality of data.



Architecture
Consistency throughout the architecture, you are only as strong as your weakest link

Authentication
Strong, multifactor authentication is imperative for all critical systems

Access Control
Always start with least privilege rule set

Audit
Consistent log retention and auditing to enable continuous monitoring

Digital Signatures
Enables non-repudiation of message transfer between two parties

Timestamps
Important in attack forensics and investigation

Secure Communication Infrastructure
Where appropriate encrypt only protocols essential to operation are present

Redundancy
Promotes system availability

Defense in Depth
A layered security approach

Separation of Duties
... or privileges of operators and users

Intrusion Detection Prevention Systems
Host based

Removal of unneeded applications

Security Management Process
... for system updates/ upgrades

Adversary & Trust Models
Importance of understanding who is an adversary and who is a partner

Fig. 5 Focus areas for the security team

Authentication—Strong authentication is imperative for DDM cyber resiliency. Each system across the digital thread requires authentication and integrates multi-factor authentication or account verification when remote access is used to access DDM systems.

Access Controls—Utilizing the principle of least privilege principles strengthens system integrity and enables access to information and resources necessary to accomplish tasks essential to an operator's workload.

Audit—Consistent logging of successful and unsuccessful system events enables continuous monitoring. Supplementing native logging with a centralized log-server validates log event entries and enables data retention policy compliance.

Digital Signatures—Enables non-repudiation and enables confidentiality of message transfer between two parties or systems.

Timestamps—Consistent correct time configurations on all systems in the digital thread provide critical reference points for digital forensics and breach investigation processes.

Secure Communication Infrastructure—Integrates encryption of data at rest and data in transit. Validating strong cryptographic protocols, appropriate key lengths and hashing as well as enabling Transport Layer Security (TLS) over Secure Sockets Layer (SSL) is recommended.

Redundancy—Promotes system availability. Build redundancy in systems producing products and redundancy in systems providing cybersecurity protection.

Defense in Depth—A layered security approach prevents a single failure in the security architecture to result in DDM system compromise. Defense in depth assists in security update priorities and facilitates risk acceptance.

Separation of Duties—Enables the detection of security control failures that indicate information theft and security breaches.

Intrusion Detection and Prevention systems—Complements security architectures, integrity measures and validates security controls.

Removal of Unneeded Applications—Provides cyber resilience by eliminating a potential attack surface that is not critical to successful DDM operation.

Security Management Process—A security management process allows for thorough testing of patches system updates so that the update doesn't do more harm to the system then good. It also allows for a risk/benefit analysis to be completed before patch implementation. An effective security management process comprises six subprocesses: policy, awareness, access, monitoring, compliance, and strategy.

Adversary and Trust Models—Developing and maintaining understanding adversary tactics, techniques and procedures assist in the cybersecurity priorities and risk acceptance processes. Validating partner cybersecurity controls increases DDM cyber resilience.

Weakest Link—Human error, whether accidental or intentional, can wreak havoc on DDM and bring the functionality and safety of the system to a halt. The most prevalent human threats are untrained operators causing accidental infections and disgruntled insiders.

References

Gartner (n.d.) IT Glossary. http://www.gartner.com/it-glossary. Accessed June 2016, from Gartner

Hathaway ME (2013) Leadership and responsibility for cybersecurity. Georgetown J Int Aff 71–80 (2013)

Kushner D (2016) The real story of Stuxnet, IEEE Spectrum. http://spectrum.ieee.org. Accessed June 2016

McNulty CM, Armas N (2012) Toward the printed world: additive manufacturing and implication for national security. September 2012 Institute for National Strategic Studies, National Defense University, Defense Horizons

National Cybersecurity and Communications Integration Center, ICS-CERT May-June 2016 Monitor. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Jun2016_S508C.pdf

Paulsen C, Dempsey K (2015) NIST DRAFT NISTIR 8023, Risk Management for Replication Devices, 2015. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8023.pdf

Pettey C, van der Meulen R (2011) Gartner says the worlds of IT and operational technology are converging, March 16. http://www.gartner.com. Accessed 14 June 2016, from Gartner

Sean McGurk, former Director, National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security. http://www.belden.com/blog/industrialsecurity/Goodbye-Air-Gaps-Hello-Improved-ICS-Security.cfm

Schuette L, Singer PW (2016) Direct digital manufacturing: the industrial game-changer you've never heard of. http://www.brookings.edu/research/articles/2011/10/10-digital-manufacturing-singer. Accessed July 2016

The Cisco Connected Factory: Holistic Security for the Factory of Tomorrow, Cisco Manufacturing White Paper. https://abm-website-assets.s3.amazonaws.com/manufacturing.net/s3fs-public/lead_gen_files/

The Economist (2014) A third industrial revolution. http://www.economist.com/node/2155e.2901. Accessed Nov 2014

U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

Williams CB (2015) NISTIR 8041, Proceedings of the Cybersecurity for DDM Symposium, National Institute for Science and Technology. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8041.pdf

Zhou W (2016) Overload: critical lessons from 15 years of ICS vulnerabilities report. https://www2.fireeye.com/ics-vulnerability-trend-report-2016-em.html

http://www.strategyand.pwc.com/trends/2015-telecommunications-trends, 2015 Telecommunications Trends, Bahjat El-Darwiche, Steven Hall