NISTIR 8041

Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium

Celia Paulsen

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8041

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8041

Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium

Celia Paulsen
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8041

April 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

National Institute of Standards and Technology Internal Report 8041
143 pages (April 2015)

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8041

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: csddm@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

Direct Digital Manufacturing (DDM) involves fabricating physical objects from a data file using computer-controlled processes with little to no human intervention. It includes Additive Manufacturing (AM), 3D printing, and rapid prototyping. The technology is advancing rapidly and has the potential to significantly change traditional manufacturing and supply chain industries, including for information and communication technologies (ICT).

On February 3, 2015, the National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) Computer Security Division hosted a one-day symposium to explore cybersecurity needed for DDM, to include ensuring the protection of intellectual property and the integrity of printers, elements being printed, and design data. Speakers and attendees from industry, academia, and government discussed the state of the industry, cybersecurity risks and solutions, and implications for Information and Communications Technology (ICT) supply chain risk management.

Keywords

3D Printing; Additive Manufacturing; Cyber Physical Systems; Cybersecurity; Direct Digital Manufacturing; Industrial Control Systems; Information Security

Acknowledgements

The NIST Information Technology Laboratory would like to acknowledge Kevin Jurrens, Richard Ricker, Kim Schaffer, and Bill Newhouse of NIST for their contributions in putting together this symposium. NIST would also like to acknowledge each of the presenters for their participation.

Executive Summary

Information Technology has increasingly been incorporated into every segment of the economy. In manufacturing, the basic technology of Direct Digital Manufacturing (DDM) been around for dozens of years. This involves the creation of a physical object from a digital design using computer-controlled processes with little to no human intervention. With the popularization and advancement of Additive Manufacturing (AM) and 3D printing, it is becoming much more common. These technologies have the potential to significantly change traditional manufacturing and supply chain industries, including information and communications technologies (ICT).

On February 3rd, 2015, the NIST Information Technology Laboratory (ITL) Computer Security Division hosted a one-day symposium to explore the cybersecurity aspects of DDM. There were approximately 50 attendees from government, industry, and academia representing a broad array of DDM practitioners, cybersecurity professionals, researchers, and manufacturing innovation organizations.

During the symposium, speakers and attendees discussed DDM cybersecurity risks, challenges, solutions, and implications for ICT supply chain risk management. Although the presenters were all from diverse backgrounds representing a variety of viewpoints, each had similar arguments:

- Cybersecurity risks to DDM are very real;
- Cybersecurity threats have the potential to disrupt the manufacturing revolution;
- There is real opportunity to improve the security of the manufacturing supply chain, and
- The time to build cybersecurity in to the DDM process is now.

During discussions and the concluding working session, participants generally agreed that the biggest challenge to building cybersecurity into DDM is culture. Organizations – especially small businesses - may not recognize that AM or 3D printing devices have any cybersecurity risks and may be unwilling to compromise efficiency for security. Other key areas discussed included cost-effective technological capabilities, technical standards, and general guidance. While several existing technical standards were identified, most were not specific to cybersecurity in DDM. Attendees noted that technical and standards-based solutions for DDM are limited and do not address the rapid, changeable, and distributed manufacturing environment of the future. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*[1], and the NIST Framework for Improving Critical Infrastructure Cybersecurity[2] were identified as potential starting points for developing risk management guidance for DDM.

.

Table of Contents

List of Appendices

1 Overview

Direct Digital Manufacturing (DDM) involves fabricating physical objects from a data file using computer-controlled processes with little to no human intervention. Traditionally, these technologies have not been widely adopted, but with the popularization of Additive Manufacturing (AM) and 3D printing, they are becoming increasingly common. These technologies are advancing rapidly and have the potential to significantly change traditional manufacturing and supply chain industries, including for information and communication technologies (ICT).

On February 3, 2015, the National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) Computer Security Division hosted a one-day symposium to explore the cybersecurity aspects of DDM, to include ensuring the protection of intellectual property and the integrity of printers, elements being printed, and design data.

There were approximately 50 attendees from government, industry, and academia representing a broad array of DDM practitioners, cybersecurity professionals, researchers, and manufacturing innovation organizations. During the symposium, speakers and attendees discussed cybersecurity risks, challenges, solutions, and implications for Information and Communications Technology (ICT) supply chain risk management.

The agenda contained an invited talk, four presentations, and a panel discussion that exemplified diverse perspectives. A concluding working session captured the viewpoints of the attendees in several key areas. In addition, attendees provided inputs on the risks, challenges, existing solutions, and potential/theoretical solutions for cybersecurity in DDM. Responses focused around culture / humans, threats to the integrity of design, technological capabilities – especially around quality control and event detection, and guidance specific to cybersecurity in DDM.

The remainder of this publication is structured as follows:

- Section 2 contains a summary of each presentation, and speaker submitted abstracts and presentations where applicable. Presentations are included in the order they were given during the symposium.
- Section 3 contains an analysis of attendee perceptions based on completed attendee handouts / response sheets and the concluding working session.
- Section 4 presents conclusions, including possible future steps and recommendations.
- Appendix A contains data from completed handouts / response sheets.
- Appendix B contains data collected during the concluding working session
- Appendix C contains biographies of the presenters as contained in the agenda.
- Appendix D lists acronyms used throughout the document.

2 Abstracts and Presentations

This section contains a brief summary of each presentation along with the abstracts speakers submitted, when applicable, and any slides used. Presentations in this section are listed in the order they were given during the symposium.

Welcome

James St. Pierre
Deputy Director of the Information Technology Laboratory (ITL), NIST

Key Points:

- NIST's mission is to promote "U.S. innovation and industrial competitiveness."
- Safeguarding the "digital threads" of the manufacturing process is critical to promoting innovation and industrial competitiveness.
- The core principles of NIST's ITL efforts include collaboration, openness, and transparency.
- We welcome the opportunity to collaborate to identify risks, challenges, gaps and opportunities as we look to "build security in" to the direct digital manufacturing processes and discuss ways forward.

Invited Talk

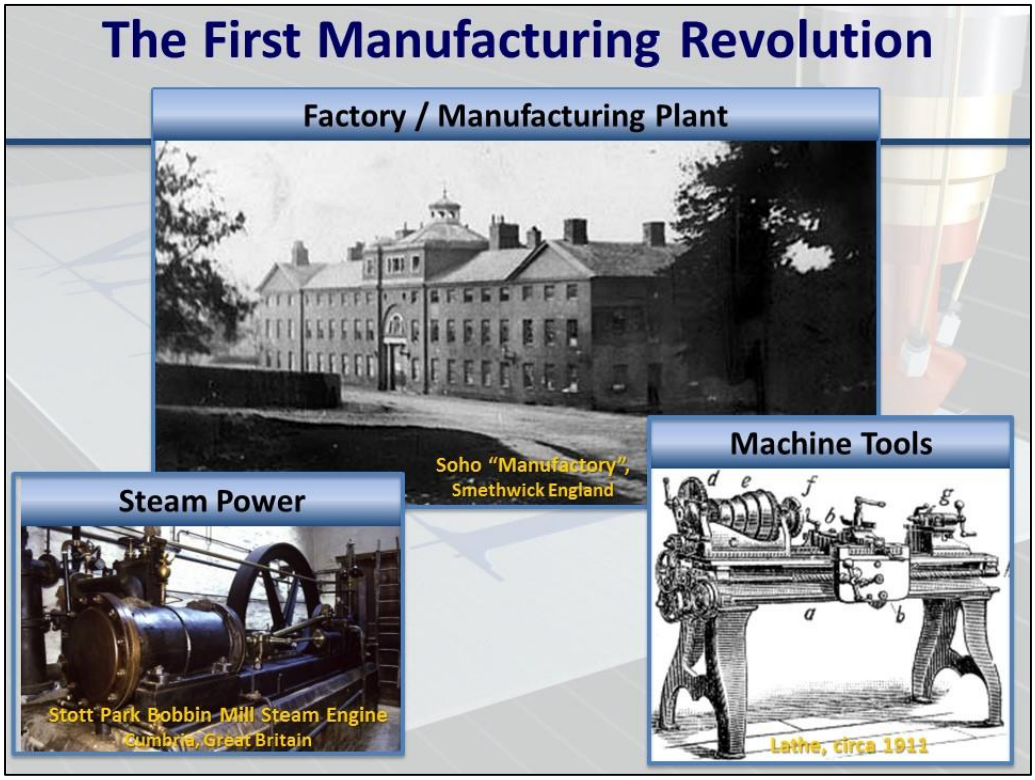
Michael F. Molnar
Director, NIST Advanced Manufacturing Program Office
Director, Advanced Manufacturing National Program Office (AMNPO)

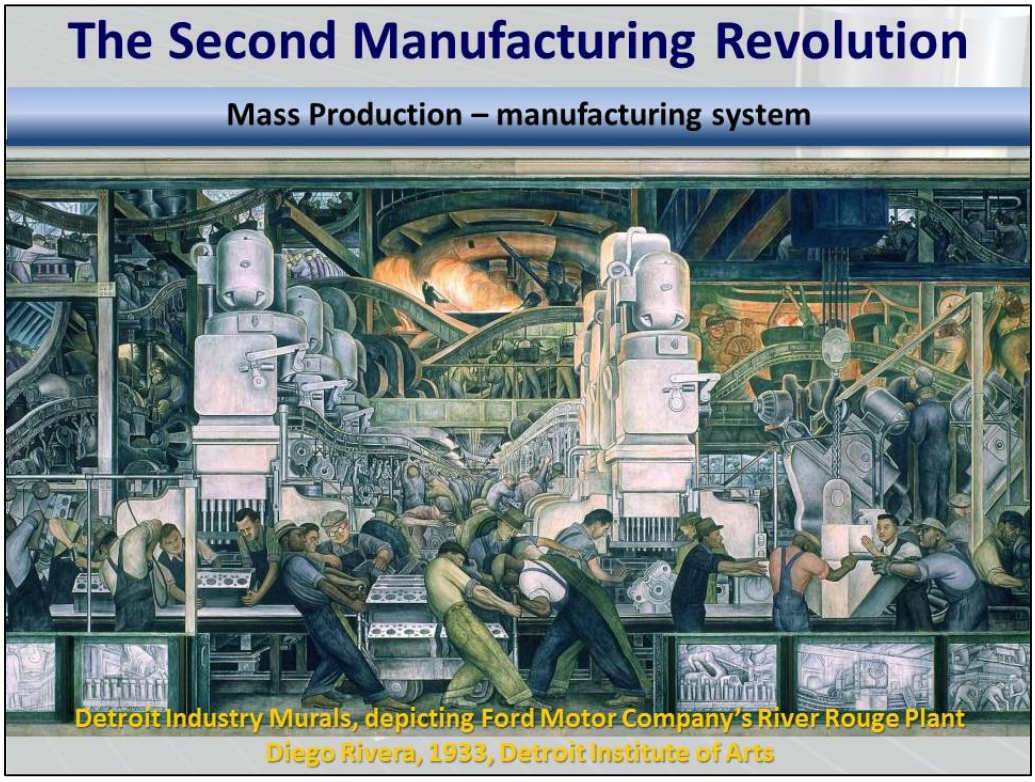
Key Points:

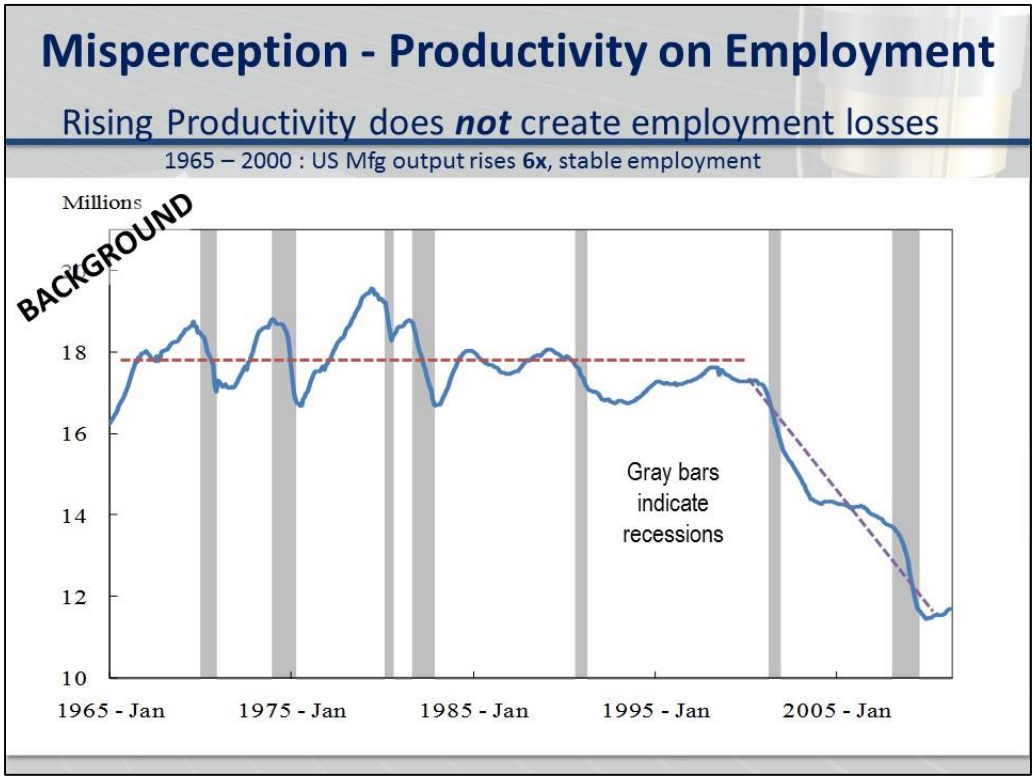
- The first two manufacturing revolutions were about bringing capabilities together. The third and current manufacturing revolution is about new capabilities – creating things we never could have before.
- Misconceptions about manufacturing include that it is "dirty and declining," meaning it may not be an attractive job field.
- Manufacturing plays a central role in the U.S. economic base.
- In 2013, the National Network of Manufacturing Innovation (NNMI) was created with bi-partisan support to advance the US's manufacturing capabilities.
- The Revitalize American Manufacturing Innovation (RAMI) Act of 2014 (H.R. 2996/S. 1468) calls for open-topic proposals for creating additional NNMI institutes. Currently 8 are planned with a goal of 45 total.

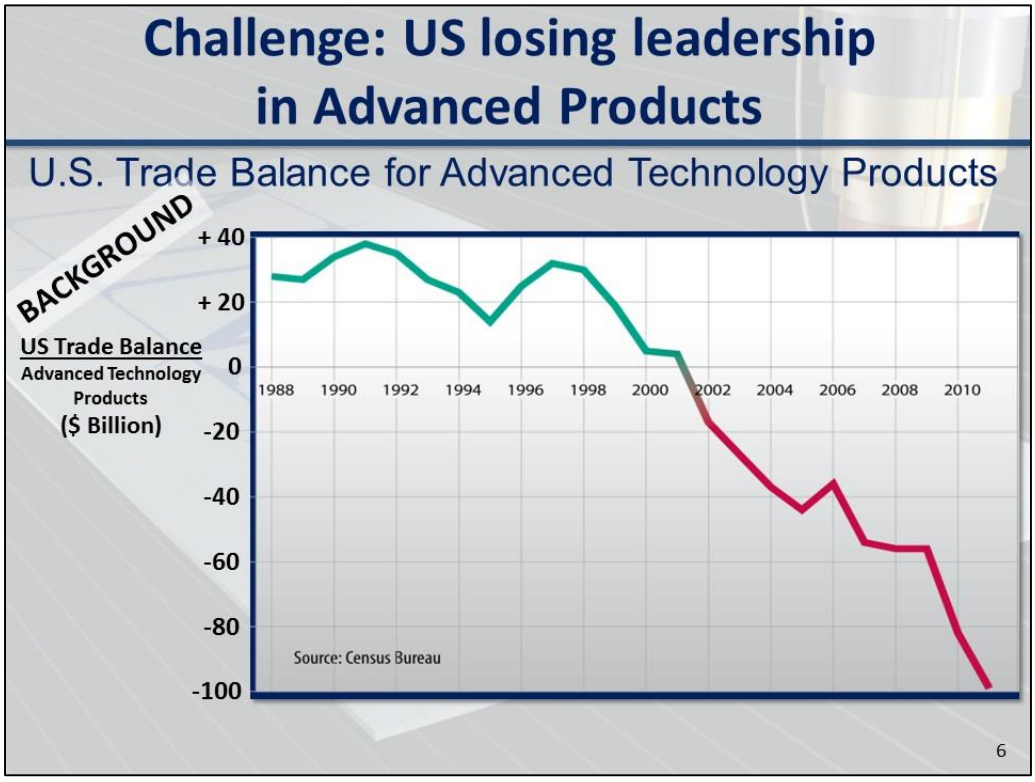
- Ed Morris was invited to speak about the first pilot NNMI institute - America Makes. He spoke about how they examined cyber implications and how advanced manufacturing would not exist without the digital component.
- Dean Bartles was invited to speak about the second pilot NNMI institute – the Digital Manufacturing and Design Innovation Institute (DMDII) in Chicago, Illinois. The DMDII focuses on digital design solutions and that cybersecurity ranked among the top five concerns of manufacturing leaders. DMDII Project Call 15-01 is specifically focused on cybersecurity and closes March 20, 2015.
- With digital manufacturing, the U.S. is regaining its focus on manufacturing and raising a new generation of *makers*.

Presentation:

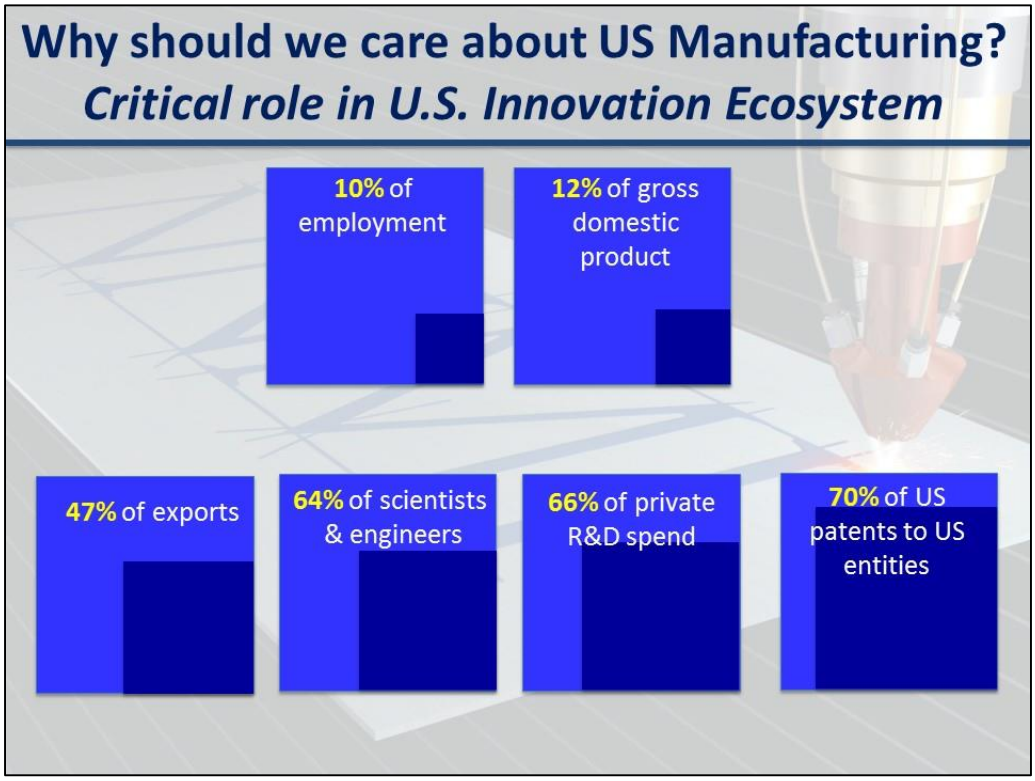

The First Manufacturing Revolution
Factory / Manufacturing Plant
Soho "Manufactory", Smethwick England
Steam Power
Stott Park Bobbin Mill Steam Engine Cumbria, Great Britain
Machine Tools
Lathe, circa 1911


The Second Manufacturing Revolution
Mass Production – manufacturing system
Detroit Industry Murals, depicting Ford Motor Company's River Rouge Plant
Diego Rivera, 1933, Detroit Institute of Arts


Misperception - Productivity on Employment
Rising Productivity does *not* create employment losses
1965 – 2000 : US Mfg output rises 6x, stable employment
Millions
BACKGROUND
18
16
14
12
10
Gray bars indicate recessions
1965 - Jan
1975 - Jan
1985 - Jan
1995 - Jan
2005 - Jan


Challenge: US losing leadership in Advanced Products
U.S. Trade Balance for Advanced Technology Products
BACKGROUND
US Trade Balance
Advanced Technology Products
($ Billion)
+ 40
+ 20
0
-20
-40
-60
-80
-100
1988
1990
1992
1994
1996
1998
2000
2002
2004
2006
2008
2010
Source: Census Bureau
6


Products invented here, now made elsewhere - not driven by labor cost
BACKGROUND
LITHIUM ION BATTERY
7


Why should we care about US Manufacturing?
Critical role in U.S. Innovation Ecosystem
10% of employment
12% of gross domestic product
47% of exports
64% of scientists & engineers
66% of private R&D spend
70% of US patents to US entities

Agenda

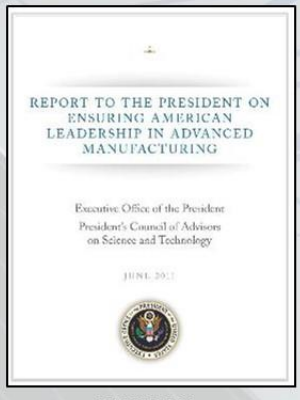
U.S. Manufacturing Yesterday
Historical View and Challenge

U.S. Manufacturing Today
Creating NNMI

U.S. Manufacturing Tomorrow
A Digital Manufacturing Renaissance requiring Cybersecurity

PCAST: The independent basis of NNMI

President's Council of Advisors on Science and Technology



PCAST 2011
Recommends Advanced Manufacturing Initiative as national innovation policy

PCAST 2012
Recommends Manufacturing Innovation Institutes to address key market failure

PCAST 2014
Recommends strong, collaborative network of Manufacturing Innovation Institutes

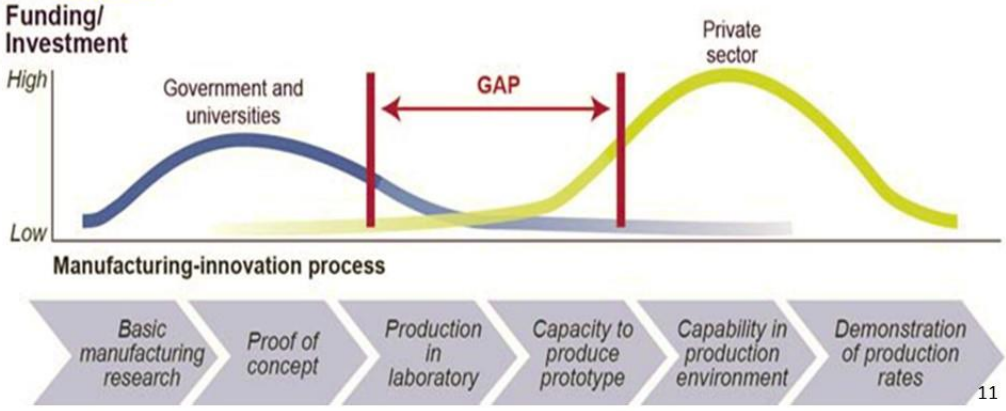
10

The "Scale-up" Gap or Missing Middle

Basic R&D

Common terms
The "valley of death"
The "missing Bell Labs"
The "industrial commons"

Commercialization



11

The President's Vision – 45 Institutes

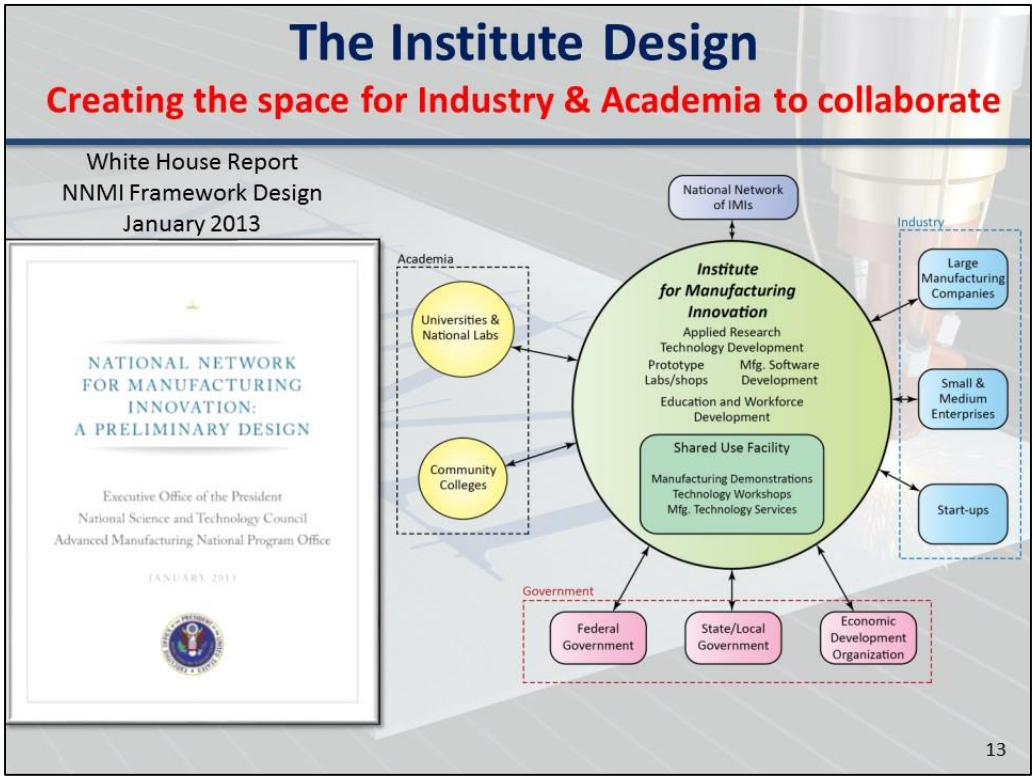
AP Photo/Susan Walsh

"In my State of the Union Address, I asked Congress to build on a successful pilot program and create 15 manufacturing innovation institutes that connect businesses, universities, and federal agencies to turn communities left behind by global competition into global centers of high-tech jobs.

"Today, I'm asking Congress to build on the bipartisan support for this idea and triple that number to 45 – creating a network of these hubs and guaranteeing that the next revolution in manufacturing is 'Made in America.'"

- July 30, 2013

12


The Institute Design
Creating the space for Industry & Academia to collaborate
White House Report
NNMI Framework Design
January 2013
NATIONAL NETWORK FOR MANUFACTURING INNOVATION: A PRELIMINARY DESIGN
Executive Office of the President
National Science and Technology Council
Advanced Manufacturing National Program Office
JANUARY 2013
National Network of IMIs
Academia
Universities & National Labs
Community Colleges
Institute for Manufacturing Innovation
Applied Research
Technology Development
Prototype Labs/shops
Mfg. Software Development
Education and Workforce Development
Shared Use Facility
Manufacturing Demonstrations
Technology Workshops
Mfg. Technology Services
Industry
Large Manufacturing Companies
Small & Medium Enterprises
Start-ups
Government
Federal Government
State/Local Government
Economic Development Organization
13


NNMI Authorized: Revitalize American Manufacturing & Innovation Act
118 bipartisan RAMI Bill Sponsors
Rep. Tom Reed
R NY-23
Rep. Joe Kennedy
D MA-4
Sen. Sherrod Brown
D Ohio
Sen. Roy Blunt
R Missouri
U.S. HOUSE OF REPRESENTATIVES
UNITED STATES SENATE
SEAL OF THE PRESIDENT OF THE UNITED STATES
September 15, 2014 – Passed House
100 Cosponsors (51D, 49R)
December 11, 2014 – Passed Senate with 2015 Appropriations
18 Cosponsors (10D, 7R, 1I)
December 16, 2014 – Signed By President Obama
Bipartisan Momentum Supporting NNMI Passage
14

RAMI and NIST

Call to Action: RAMI calls upon the U.S. Secretary of Commerce and NIST to **establish**:

1. **The "Network for Manufacturing Innovation Program"** *(Network function)* - to convene and support a network of Institutes
2. **New "Centers for Manufacturing Innovation"** *(Institutes)* - using an open topic, open competition process
3. **The National Program Office** at NIST - to oversee and carry out the program *(coordination, network support, and reporting)*

15

Establish/Convene the Network: *Network Current Status*

Full Network Goal: 45 regional hubs

New Institutes Planned for FY16:

Open topic competition – *addressing "white space" between mission agency topics*

Selected topic competitions supporting Agency mission – *using agency authorities and budgets*

16

Agenda

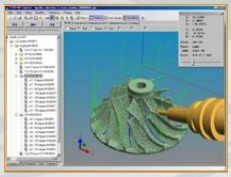
U.S. Manufacturing Yesterday
Historical View and Challenge

U.S. Manufacturing Today
Creating NNMI

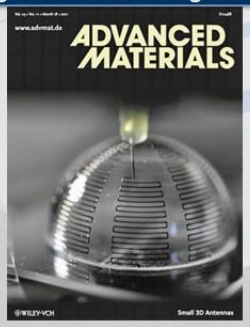
U.S. Manufacturing Tomorrow
A Digital Manufacturing Renaissance requiring Cybersecurity

The Third Manufacturing Revolution

Digital Mfg – smart, adaptive, optimized, distributed

Example Digital Manufacturing Technology – "Additive Manufacturing"

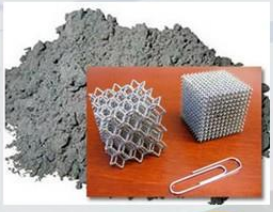


The First Pilot Manufacturing Innovation Institute

Additive Manufacturing/3D Printing – Youngstown OH

Prime Awardee: National Center for Defense Manufacturing and Machining

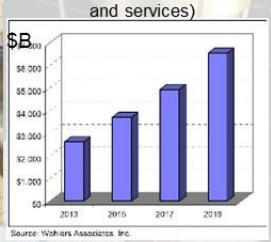
- Initial $30M federal investment matched by $40M industry, state/local
- Strong leveraging of equipment, existing resources
- Strong business development
- Tiered membership-based model, low cost to small business and nonprofits



- **Now at $50M federal, $60M co-invested**
- **OVER 100 Participating partners!**

Why Additive Manufacturing?
High Potential for Transformative Impact

Projected AM Sales (products and services)



"20% of output of 3D printers is now final products, rather than prototypes. By 2020 it may be 50%." – *The Economist (2011)*

Government agency investments and interest

Consumer Product Market

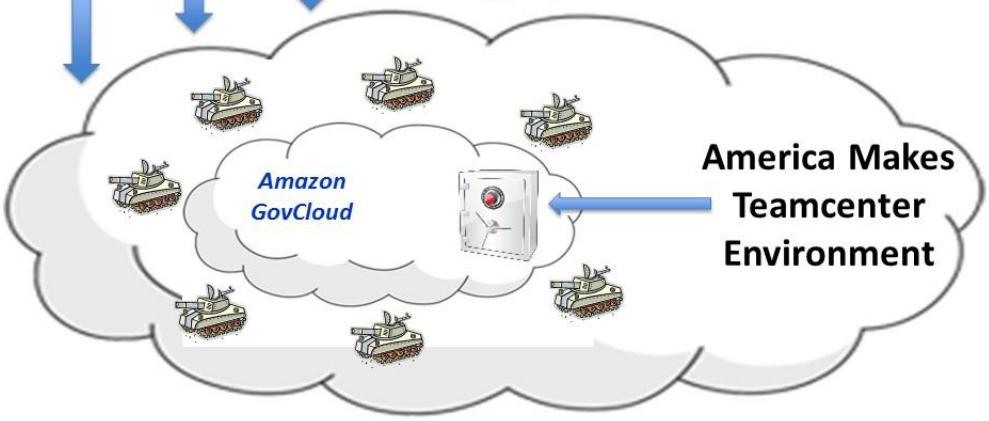
America Makes

America Makes – National Additive Manufacturing Innovation Institute: Cybersecurity Actions

- *"Cyber Security Awareness"* Presentation to all Members at Spring 2014 Program Management Review by Victoria Yan Pillitteri, Advisor for Information System Security, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology
- Reinforced the cybersecurity defenses on our America Makes website after successfully defeating a brute force foreign-based cyber attack in August 2014
- Host periodic FBI Cybersecurity Briefs to America Makes management team
- Deployed Siemens Teamcenter for America Makes PLM data management, hosted by Amazon in "GovCloud"
- Rigorous Password access protocols in place

America Makes

- Our site is hosted by Amazon in "GovCloud"
- GovCloud is ITAR Compliant and provides America Makes additional levels of security for securing project data and deliverables



NCDMM has passed security audits conducted by Siemens & Amazon

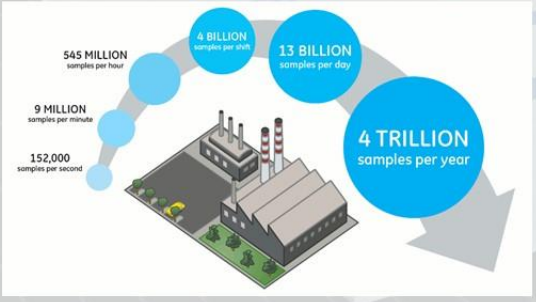
2nd Pilot Institute:
Digital Manufacturing & Design Innovation

$70M public investment, ~$240M match

Lead: UI Labs

Hub location: Chicago, Illinois

- **41 Companies**
- **23 Universities and Labs**
- **9 Other Organizations**



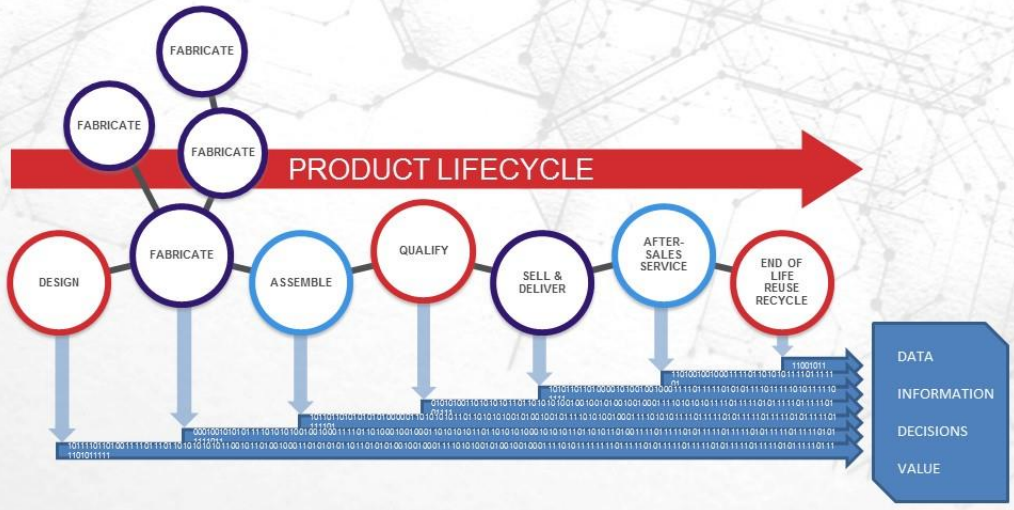
***Mission**: Establish a state-of-the-art proving ground that links IT tools, standards, models, sensors, controls, practices and skills, and transition these tools to the U.S. design & manufacturing base for full-scale application*

Over 3:1 Industry Cost Share

23

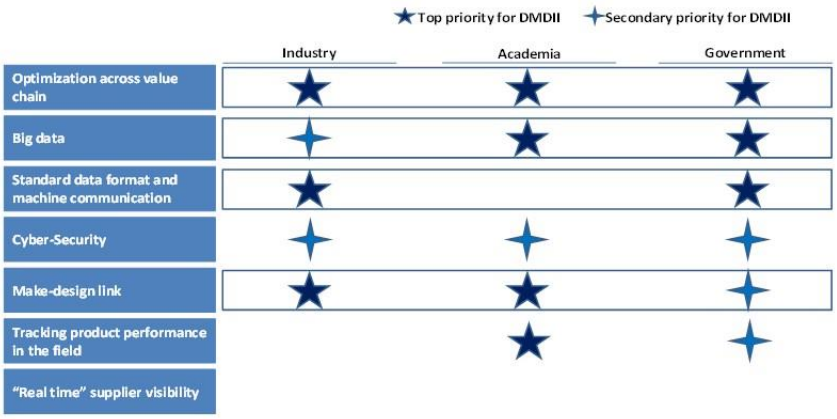
WHAT IS DIGITAL MANUFACTURING?

DIGITAL LAB FOR MANUFACTURING



Data is gathered and available for optimization of process and product at every point in the cycle, is aggregated for used in the DIGITAL MANUFACTURING COMMONS

Manufacturing cyber security ranks among the top five priorities for manufacturing leaders



In building the DMDII Technology Roadmap, DMDII surveyed 170 manufacturing leaders from industry, academia, and government.

DMDII
a UI LABS Collaboration
Cyber Security Approved for Public Release February 9, 2015

DMDII Strategic Investment Plan for Intelligent Machines

Four key DMDII investment areas for 2015 and beyond.

IM1: Communications Standards for Intelligent Machines
Provide a framework and standards for communication for Intelligent Machines, including: legacy and modern production machines, robotic devices, manufacturing cells, and other smart manufacturing systems.

IM2: Cyber Security for Intelligent Machines
Demonstrate technologies that de-risk the networking of production equipment within the smart factory.

IM3: Operating System for Cyber Physical Manufacturing
Technologies for horizontal and vertical resource management from the lowest hardware to the highest enterprise level. Includes real time streaming of machine tool data, and remote operation of production equipment.

IM4: Intelligent Machining Toolkit
Use real-time analytics and machine learning to optimize the smart factory.

DMDII
a UI LABS Collaboration
Cyber Security Approved for Public Release February 9, 2015

DMDII Project Call 15-01: Factory Infrastructure Cybersecurity Assessment

Key Challenge: Protecting the operational systems of a manufacturing enterprise presents a different set of challenges from protecting enterprise IT systems and networks.

- The project objectives are to:
  - Identify minimum capabilities that satisfy DFARS requirements (252.204-7012) for incorporating information security measures in a typical industry setting
  - Estimation of the costs to reach and maintain those DFARS-compliant capabilities
  - Development and test of a vulnerability assessment tool

White Papers are Due March 20
DMDII will fund 3 projects at a total of $1.2M
More information at: http://dmdii.uilabs.org

DMDII Cyber Security | Approved for Public Release | a UI LABS Collaboration | February 9, 2015

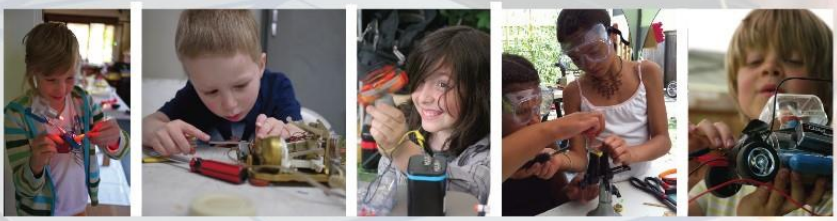
Opportunities from Digital Manufacturing

Democratization of tools needed to Design and Make

Shared access to non-profit and commercial makerspaces.

Future Digital Manufacturers

Inspiration *to* Innovation *to* Making



Thank you

For questions or comments, please contact the

Advanced Manufacturing National Program Office

amnpo@nist.gov

www.manufacturing.gov

301-975-2830

Unless otherwise labeled, images are courtesy of The White House, the National Institute of Standards and Technology, and Shutterstock

Presentation 1: *An Analysis of Cyber Physical Vulnerabilities in Additive Manufacturing*

Christopher B. Williams
Associate Professor, Virginia Tech Department of Mechanical Engineering

Key Discussion Points:

- Current research in Cyber Physical Systems is focused on Supervisory Control and Data Acquisition (SCADA) systems, but Additive Manufacturing is different.
- Researchers were able to intercept a job initialization file and decode it, allowing attackers to potentially alter printer parameters mid-print. The STL (or newer AMF) standard files are especially vulnerable to attacks which alter a design.
- The presenters described an experiment run on students at Virginia Tech. Seven groups of students were given an "extra credit" assignment to design a standard dog bone, print it, and test it. An exploit was easily developed which inserted a void in the STL file. Students failed to recognize any anomalies prior to printing and testing. No students correctly diagnosed the anomalies as a cybersecurity problem.
- Recommendations include improved quality control processes, hashing, improved process monitoring, and operator training.
- Some attendees commented that other forms of manufacturing have similar vulnerabilities.
- Cybersecurity solutions should be built under the assumption that manufacturers are not cybersecurity experts.

An Analysis of Cyber-Physical Vulnerabilities in Additive Manufacturing

Logan Sturm[1], Christopher B. Williams[1], Jaime A. Camelio[2], Jules White[3], Robert Parker[4]
[1]Department of Mechanical Engineering, [2]Department of Industrial & Systems Engineering, [3]Department of Computer Science
[1,2]Virginia Tech, [3]Vanderbilt University, [4]VT-ARC
[1,2,4]Blacksburg, VA, USA

Keywords—Additive Manufacturing; 3D Printing; Cyber/Physical security

EXTENDED ABSTRACT

While the "digital thread" of advanced manufacturing technologies enables a more efficient design process, it also presents opportunities for cyber-attacks to impact the physical word. A cyber-attack on manufacturing systems could cause injury to plant workers and damage to the machine itself. More insidiously, an attack could be designed to cause a process to produce faulty parts that might find their way into end-user products. With the rise in both the number of cyber-physical systems connected to networks and in malicious cyber-attacks, there is a clear need for research to understand the vulnerabilities of cyber-physical systems. While methods exist for detecting cyber-attacks on computer systems, no such research has been done on detecting an attack from the physical parts created by the attack.

In this work, the authors scope their research solely on Additive Manufacturing (AM; also referred to as "3D Printing") technologies. The AM process chain has unique vulnerabilities that warrant a detailed investigation due to their ability to fabricate parts in a layer-wise fashion. Because of the potential damage from a cyber-physical attack, there is a need to look at AM systems to determine what vulnerabilities exist and how to prevent and mitigate the threat of cyber-attacks.

The digital nature of the AM process chain provides an opportunity for a cyber-attack to cross into the physical world. There are four main steps on the process chain where an attack could take place: the CAD model, the .STL file, the toolpath file, and the physical machine itself. While the authors will discuss attack vectors at each of these steps within the process chain, their focus will be on vulnerabilities within the .STL file as it is the one vulnerability that does not require specific modification for an individual AM machine. As STL file creation occurs at the beginning of the process chain and the file format is standardized across every AM machine, a focused attack could have severe implications across an AM production line regardless of the machine type or manufacturer.

The current defacto standard in AM, the STL file only contains the surface information of the part. This information is stored as a 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. STL file edits/attacks could take the form of (i) part scaling, (ii) surface indents or protrusions, (iii) vertex movement, and (iv) insertion of internal voids within the part. While most of these vectors affect the surface of the part geometry – and thus could possibly detected using standard quality control dimensional measurements – the void attack is completely enclosed inside the model. Because of this, such an attack would be undetectable by dimensional measurements and may be difficult or impossible to find visually. The use of supporting material in many processes also renders the void undetectable by weighing, since the void is filled with a structurally deficient, but equivalently dense material.

To ascertain the potential impact of this specific attack, two experiments were performed. First the authors 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 on 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 1085N to 930N, and the strain at failure was reduced from 10.4% to 5.8%.

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.

Based on the results of this study, it appears that a real threat from cyber-physical attacks exists and that further research needs to be done on how to mitigate such attacks. The inclusion of software checks, hashing, process monitoring, and worker training are proposed as methods of reducing these threats. Future work includes the development of physical hashing techniques and of improved side channel process monitoring and control.

Presentation:

VirginiaTech
Invent the Future

An Analysis of Cyber-Physical Vulnerabilities in Additive Manufacturing

DREAMS
Design, Research, and Education for Additive Manufacturing Systems
http://www.dreams.me.vt.edu/

Christopher B. Williams

Associate Professor
Director, DREAMS Lab
Associate Director, MII
Virginia Tech
Department of Mechanical Engineering

VirginiaTech
Invent the Future

The DREAMS Lab at Virginia Tech

DREAMS
Design, Research, and Education for Additive Manufacturing Systems
http://www.me.vt.edu/dreams

Vision:

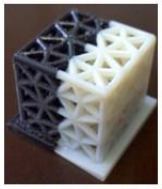
To advance the science, state of the art, and pedagogy of AM, and thereby lead the transition of today's layered fabrication techniques into viable platforms for the realization of end-use products.

VirginiaTech
Invent the Future

VirginiaTech Invent the Future

DREAMS Lab: Research Foci

- **Design for Additive Manufacturing**
  - DfAM decision support methodologies
  - Cellular material topology design & optimization



Multi-Material Optimization

- **Process and Materials Research**
  - 3D Printing of novel photopolymers
  - 3D Printing of metals and ceramics
  - 3D Printing with nanocomposites
  - Embedded electrical and actuation systems

Material Jetting of 0.5wt% Quantum Dots

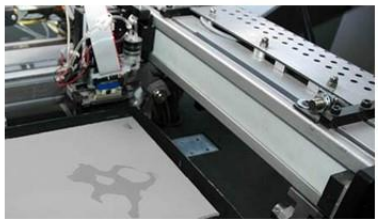
- **Education**
  - K-12 STEM Outreach
  - Undergraduate and graduate courses
  - Continuing education

Metal Oxide 3D Printing

VirginiaTech Invent the Future

DREAMS Lab: Facilities

Extrusion



Metal/Ceramic Binder Jetting

Multi-Material Jetting

Polymer Powder Bed Fusion

Foundry Sand Binder Jetting

Mask Projection Vat Photopolymerization

VirginiaTech
Invent the Future

VT Research Center in Arlington

The Virginia Tech Research Center in Arlington (VTRCA) opened in June 2011 and is 144,000 GSF.

The College of Engineering has 19,000 GSF and ICTAS is occupies an additional 7,000 GSF.

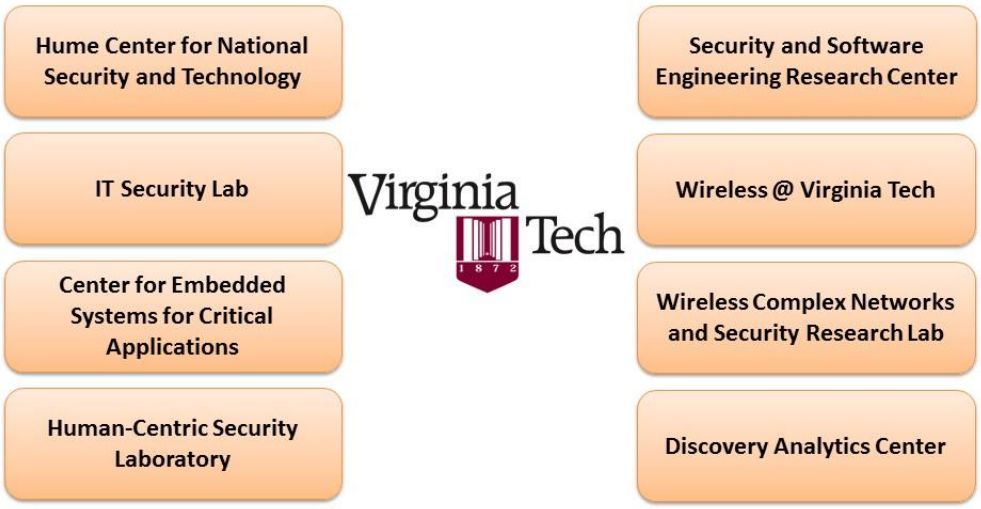
VT Cybersecurity-Focused Research Centers

Hume Center for National Security and Technology	• Communication and Computation Challenges as related to the USG, including critical infrastructure, cyber defense, and cellular/wifi communications challenges • Provides opportunities for students to work directly on USG programs
Security and Software Engineering Research Center	• NSF Industry/University Cooperative Research Center • Consortium where companies can invest in seed research in the domain of software/cyber security
IT Security Lab	• Operated by the University IT Security Office • Teaching hospital for enterprise network security
Wireless @ Virginia Tech	• Core focus on wireless research and education • Programs in secure mobility, secure spectrum access
Center for Embedded Systems for Critical Applications	• Applied formal methods for embedded systems security • Software malicious intent characterization, software synthesis, supply chain security
Complex Networks and Security Research Lab	• Security in networking with emphasis on wireless • Cryptographic approach to cloud information security
Human-Centric Security Laboratory	• Leveraging human behaviors in cyber security research • Emphasis on program analysis of mobile apps
Discovery Analytics Center	• Machine learning approaches to anomaly detection • Visual analytics programs geared toward improving cyber analyst workflow

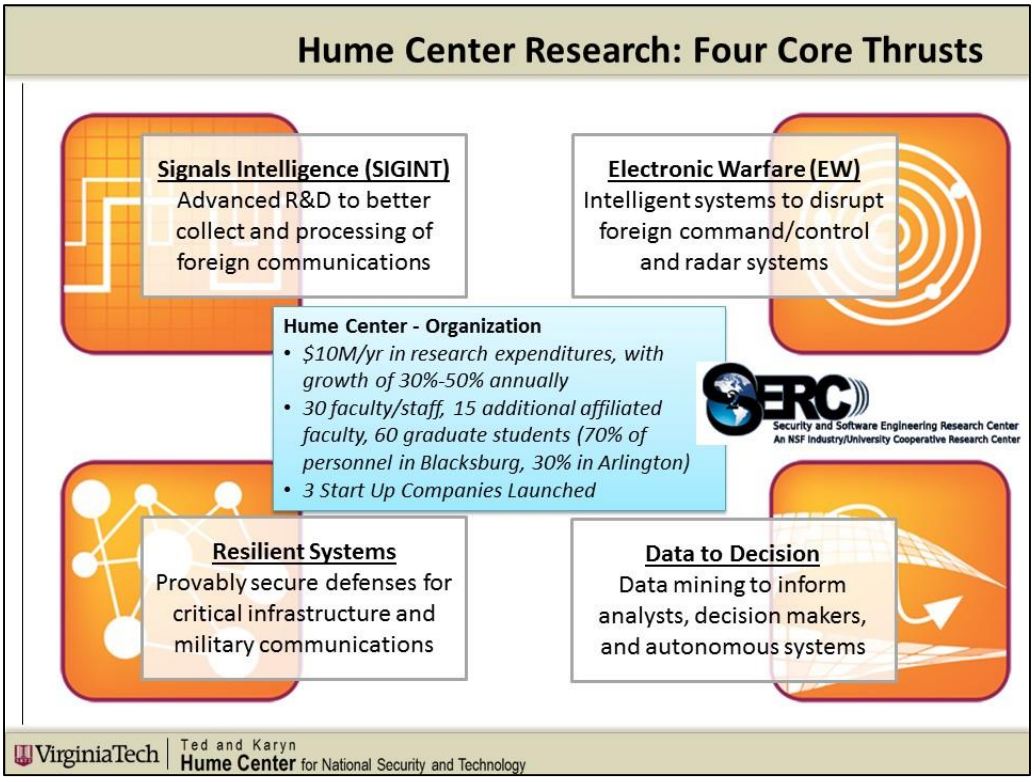
7

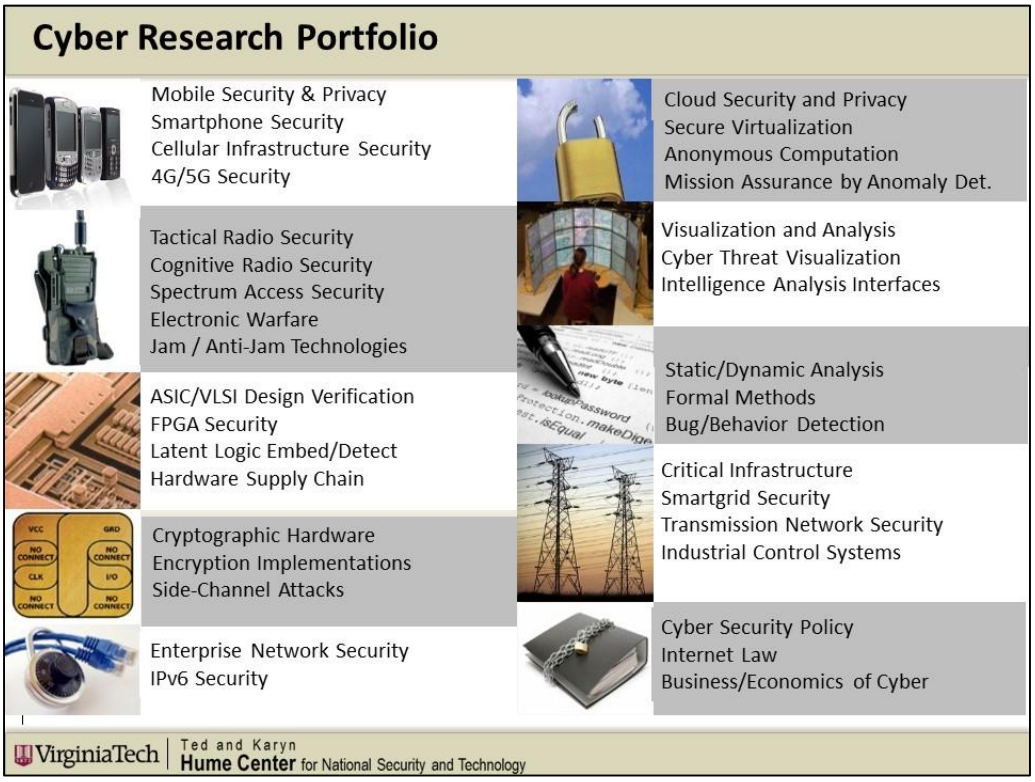
VirginiaTech | Ted and Karyn Hume Center for National Security and Technology

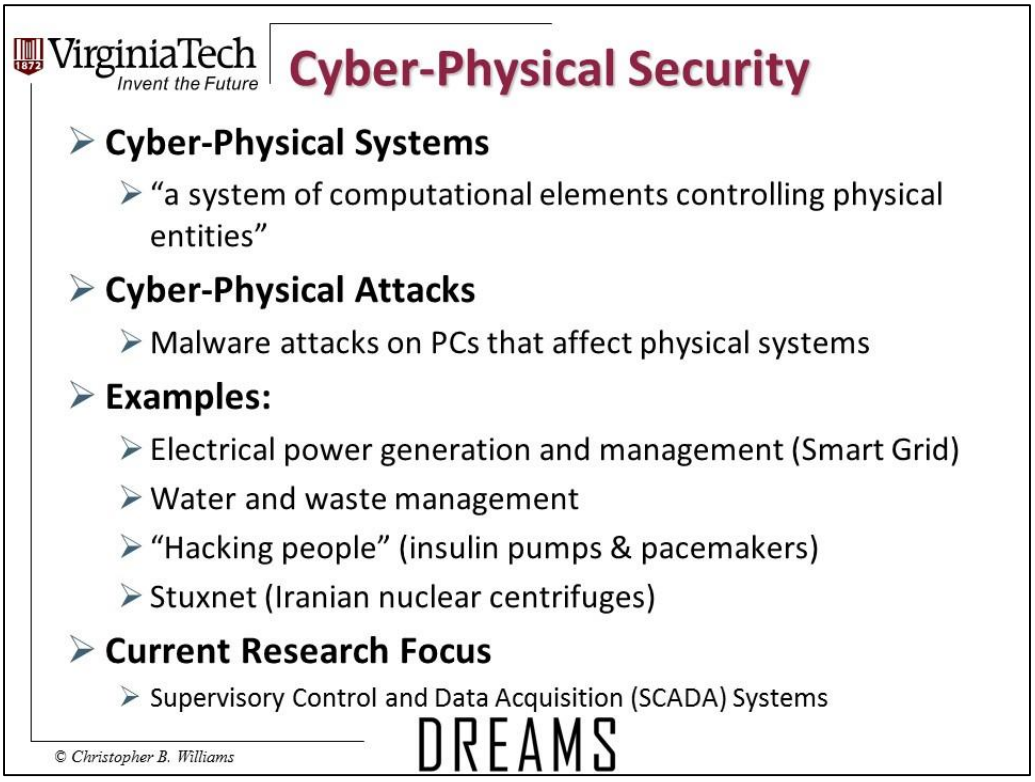
VT Cybersecurity-Focused Research Centers



VirginiaTech | Ted and Karyn Hume Center for National Security and Technology

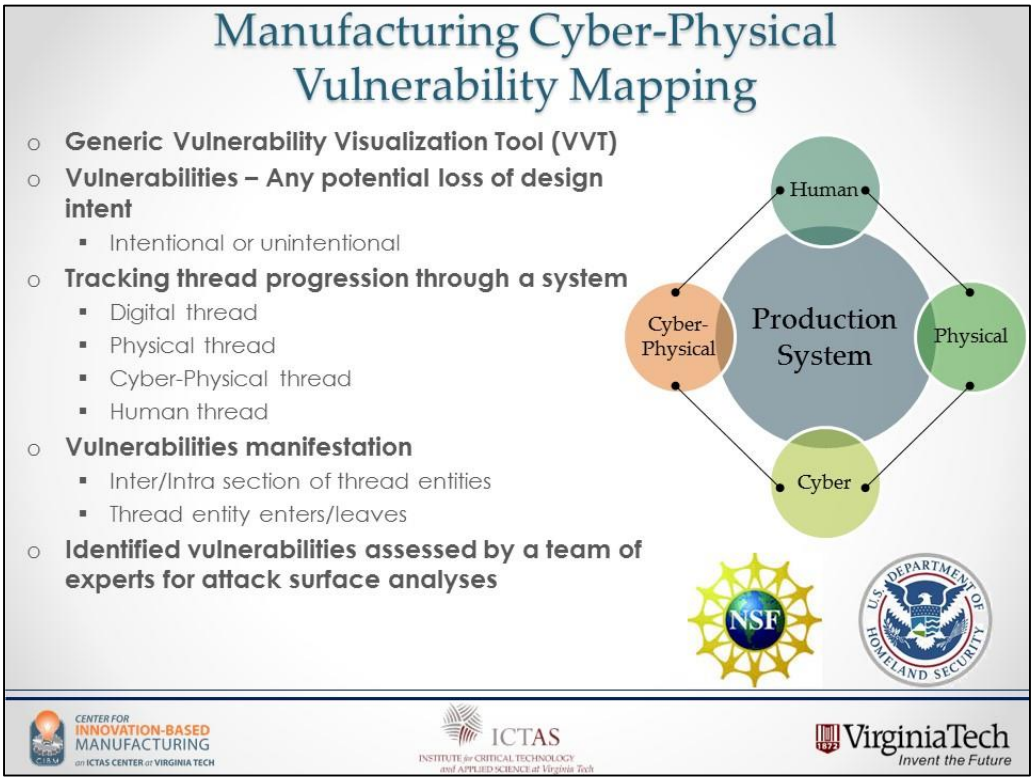

Hume Center Research: Four Core Thrusts
Signals Intelligence (SIGINT)
Advanced R&D to better collect and processing of foreign communications
Electronic Warfare (EW)
Intelligent systems to disrupt foreign command/control and radar systems
Hume Center - Organization
• $10M/yr in research expenditures, with growth of 30%-50% annually
• 30 faculty/staff, 15 additional affiliated faculty, 60 graduate students (70% of personnel in Blacksburg, 30% in Arlington)
• 3 Start Up Companies Launched
SERC
Security and Software Engineering Research Center
An NSF Industry/University Cooperative Research Center
Resilient Systems
Provably secure defenses for critical infrastructure and military communications
Data to Decision
Data mining to inform analysts, decision makers, and autonomous systems
VirginiaTech | Ted and Karyn Hume Center for National Security and Technology


Cyber Research Portfolio
Mobile Security & Privacy
Smartphone Security
Cellular Infrastructure Security
4G/5G Security
Tactical Radio Security
Cognitive Radio Security
Spectrum Access Security
Electronic Warfare
Jam / Anti-Jam Technologies
ASIC/VLSI Design Verification
FPGA Security
Latent Logic Embed/Detect
Hardware Supply Chain
Cryptographic Hardware
Encryption Implementations
Side-Channel Attacks
Enterprise Network Security
IPv6 Security
Cloud Security and Privacy
Secure Virtualization
Anonymous Computation
Mission Assurance by Anomaly Det.
Visualization and Analysis
Cyber Threat Visualization
Intelligence Analysis Interfaces
Static/Dynamic Analysis
Formal Methods
Bug/Behavior Detection
Critical Infrastructure
Smartgrid Security
Transmission Network Security
Industrial Control Systems
Cyber Security Policy
Internet Law
Business/Economics of Cyber
VirginiaTech | Ted and Karyn Hume Center for National Security and Technology


VirginiaTech
Invent the Future
Cyber-Physical Security
Cyber-Physical Systems
"a system of computational elements controlling physical entities"
Cyber-Physical Attacks
Malware attacks on PCs that affect physical systems
Examples:
Electrical power generation and management (Smart Grid)
Water and waste management
"Hacking people" (insulin pumps & pacemakers)
Stuxnet (Iranian nuclear centrifuges)
Current Research Focus
Supervisory Control and Data Acquisition (SCADA) Systems
© Christopher B. Williams
DREAMS


VirginiaTech
Invent the Future
Cyber-Physical Security
Opportunity
"Research in computer security has focused traditionally on the protection of information. Researchers have not considered how attacks affect the physical world." [Cardenas et al, 2009]
Current Research Focus
Supervisory Control and Data Acquisition (SCADA) Systems
However, is this enough to protect our Manufacturing Infrastructure?
© Christopher B. Williams
DREAMS
Cardenas et al., 2009, "Challenges for Securing Cyber Physical Systems." Workshop on Future Directions in Cyber-Physical Systems Security, DHS.


VirginiaTech
Invent the Future
Manufacturing Cyber-Physical Security Team
Virginia Tech
Dr. Chris Williams & Logan Sturm
DREAMS Lab
Dr. Jaime Camelio & Dr. Lee Wells
Center for Innovation-based Manufacturing
VT-ARC
Robert Parker
Vanderbilt University
Dr. Jules White
DREAMS
Design, Research, and Education for Additive Manufacturing Systems
CENTER FOR INNOVATION-BASED MANUFACTURING
an ICTAS CENTER at VIRGINIA TECH
VT-ARC
VANDERBILT
© Christopher B. Williams


Manufacturing Cyber-Physical Vulnerability Mapping
Generic Vulnerability Visualization Tool (VVT)
Vulnerabilities – Any potential loss of design intent
Intentional or unintentional
Tracking thread progression through a system
Digital thread
Physical thread
Cyber-Physical thread
Human thread
Vulnerabilities manifestation
Inter/Intra section of thread entities
Thread entity enters/leaves
Identified vulnerabilities assessed by a team of experts for attack surface analyses
Human
Cyber-Physical
Production System
Physical
Cyber
NSF
CENTER FOR INNOVATION-BASED MANUFACTURING an ICTAS CENTER at VIRGINIA TECH
ICTAS
INSTITUTE for CRITICAL TECHNOLOGY and APPLIED SCIENCE at Virginia Tech
VirginiaTech
Invent the Future

VirginiaTech
Invent the Future

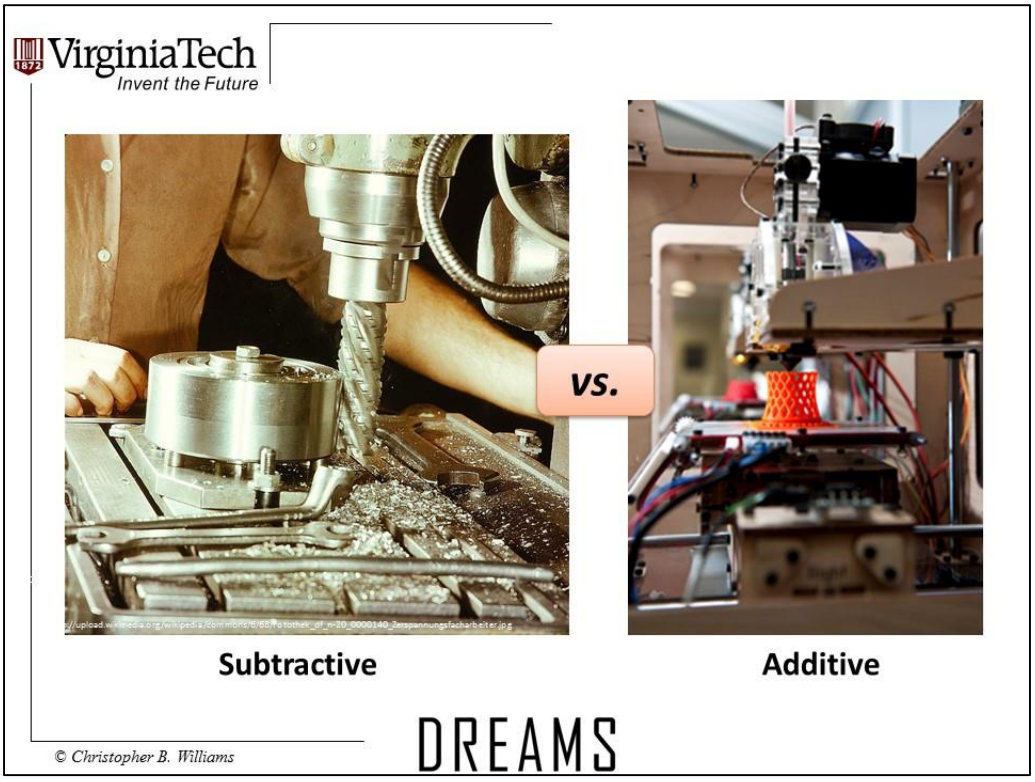
What are the Cyber-Physical vulnerabilities in Additive Manufacturing?

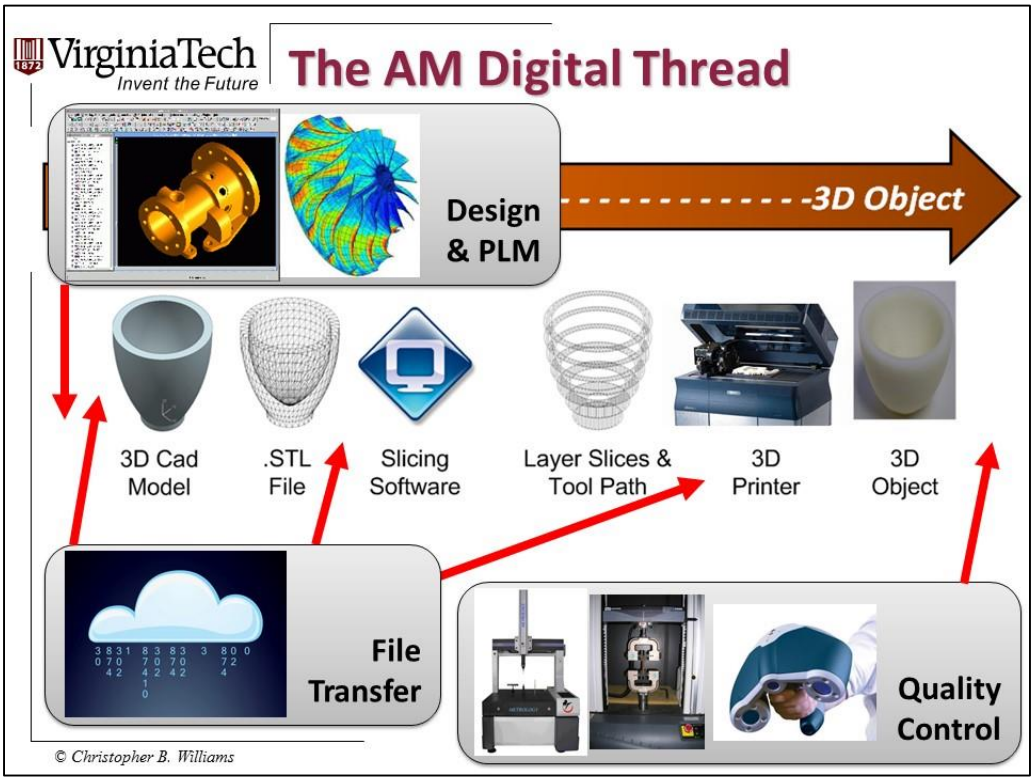
DREAMS

VirginiaTech
Invent the Future

Additive Manufacturing

DREAMS

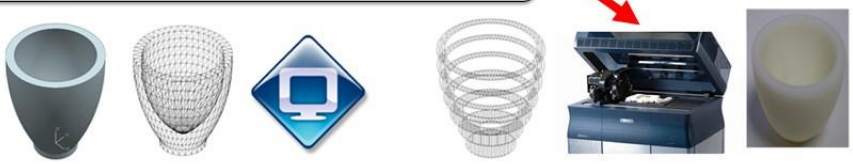

VirginiaTech
Invent the Future
vs.
Subtractive
Additive
DREAMS
© Christopher B. Williams


VirginiaTech
Invent the Future
The AM Digital Thread
Design & PLM
3D Object
3D Cad Model
.STL File
Slicing Software
Layer Slices & Tool Path
3D Printer
3D Object
File Transfer
Quality Control
© Christopher B. Williams

VirginiaTech Invent the Future

The AM Digital Thread

- Replace / modify firmware
- Machine tampering / modification



3D Cad Model | .STL File | Slicing Software | Layer Slices & Tool Path | 3D Printer | 3D Object

Digital Thread | Vulnerabilities | STL Attack | Case Study | Summary

VirginiaTech Invent the Future

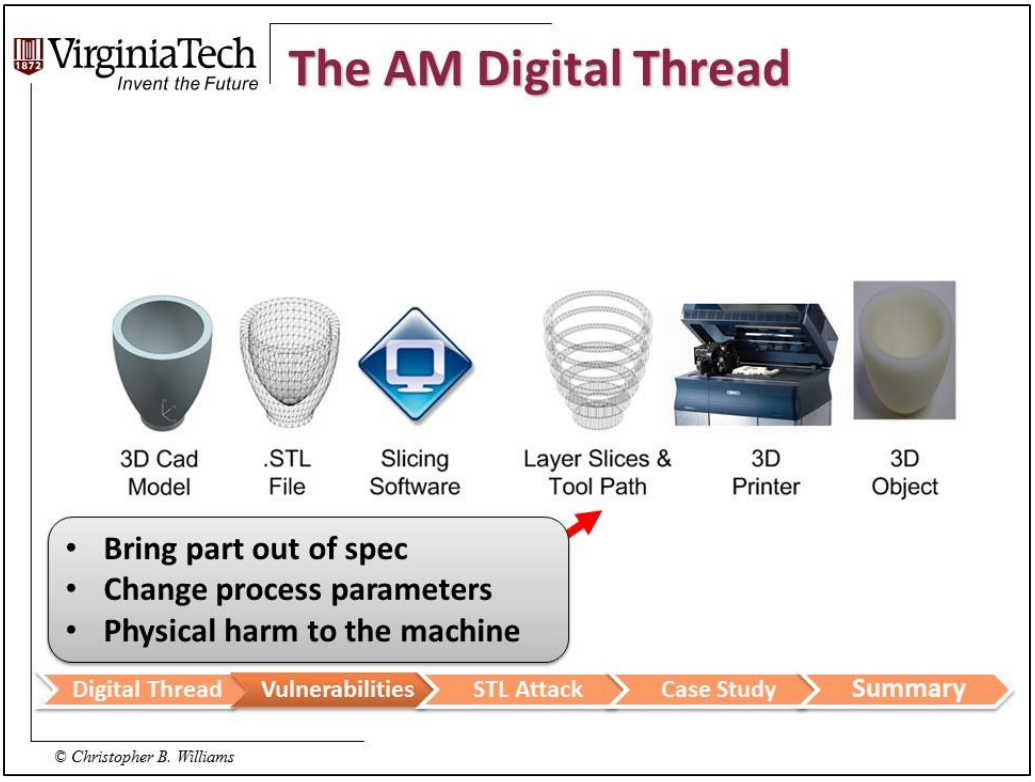
Demo: Machine Attack

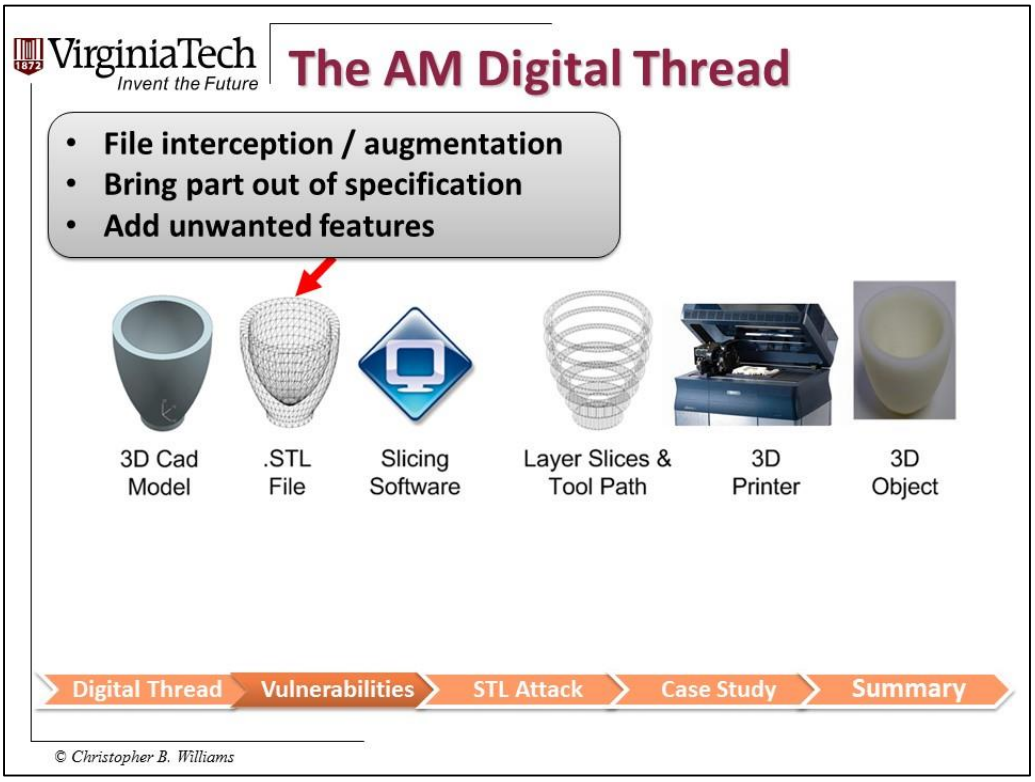
- Machine initialization file sent over intranet before print job
- Common cyber forensics software (packet sniffing) was able to intercept this file and decode it
- Attacker could alter vital printer parameters in mid-print
  - Turn off cooling fans
  - Turn off support material

```
1  ActivationOverShoot=0
2  ActiveMarginInPercent=10
3  ActiveTanks=1,3,2
4  AdvanceFireTest=0
5  AdvanceFire_1200DPI=9
6  AllowEmulationDelay=0
7  AmbientFanControlByPass=1
8  AmbientLog=1
9  AmbientTemperatureByPass=0
10 AmbientTemperatureFanControl=383
11 AtLeastDelayTimeBetweenLayers=0
12 AutoPrintCurrentZLocation=0
```

Digital Thread | Vulnerabilities | STL Attack | Case Study | Summary

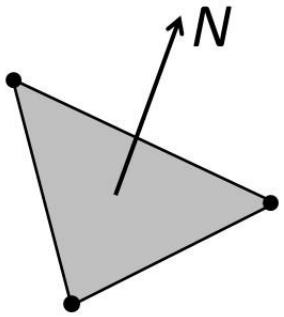
DREAMS


VirginiaTech
Invent the Future
The AM Digital Thread
3D Cad Model
.STL File
Slicing Software
Layer Slices & Tool Path
3D Printer
3D Object
• Bring part out of spec
• Change process parameters
• Physical harm to the machine
Digital Thread
Vulnerabilities
STL Attack
Case Study
Summary
© Christopher B. Williams


VirginiaTech
Invent the Future
The AM Digital Thread
• File interception / augmentation
• Bring part out of specification
• Add unwanted features
3D Cad Model
.STL File
Slicing Software
Layer Slices & Tool Path
3D Printer
3D Object
Digital Thread
Vulnerabilities
STL Attack
Case Study
Summary
© Christopher B. Williams

STL Overview

```
solid AME
  facet normal 0.0000000e+00 0.0000000e+00 -1.0000000e+
    outer loop
      vertex 2.7577722e+00 2.4375000e+00 0.0000000e+00
      vertex 2.6187184e+00 2.6187184e+00 0.0000000e+00
      vertex 2.6941842e+00 2.5326663e+00 0.0000000e+00
    endloop
  endfacet
  facet normal 0.0000000e+00 0.0000000e+00 -1.0000000e+
    outer loop
      vertex 2.8451851e+00 2.2264667e+00 0.0000000e+00
      vertex 2.7577722e+00 2.4375000e+00 0.0000000e+00
      vertex 2.8083946e+00 2.3348480e+00 0.0000000e+00
    endloop
  endfacet
  facet normal 0.0000000e+00 0.0000000e+00 -1.0000000e+
    outer loop
      vertex 2.8750000e+00 2.0000000e+00 0.0000000e+00
      vertex 2.8451851e+00 2.2264667e+00 0.0000000e+00
      vertex 2.8675143e+00 2.1142104e+00 0.0000000e+00
    endloop
  endfacet
  facet normal 0.0000000e+00 0.0000000e+00 -1.0000000e+
    outer loop
      vertex 2.8451851e+00 1.7735333e+00 0.0000000e+00
      vertex 2.8750000e+00 2.0000000e+00 0.0000000e+00
      vertex 2.8675143e+00 1.8857896e+00 0.0000000e+00
    endloop
  endfacet
```



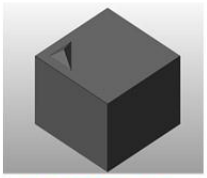
1 triangular facet
Normal vector
3 vertices

Digital Thread | Vulnerabilities | STL Attack | Case Study | Summary

DREAMS

STL Attack: Exterior Attacks

- **Increase/decrease part scale**
  - Part can be brought out of specification
- **Surface dimples / protrusions**
  - Bumps or voids added to the part surface
- **Moved vertices**
  - Part features can be altered by moving vertices


Add protrusion


Move vertex inward


Move vertex outward

Digital Thread | Vulnerabilities | STL Attack | Case Stud

DREAMS

VirginiaTech Invent the Future

STL Attack: Internal Voids

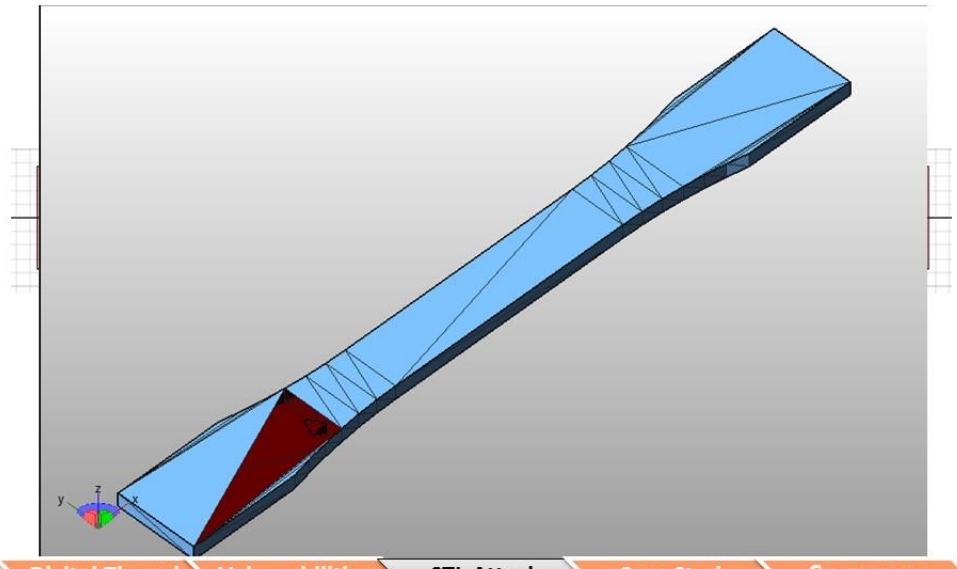
- Affect internal structure without affecting external structure
- Internal Voids
  - Append STL file with additional triangles
  - Tetrahedron defined by 4 triangles
    - Minimal increase in file size
  - Invert normals to define void space
- "Printed" voids serve as crack propagation sites in part application

Digital Thread | Vulnerabilities | STL Attack | Case Study | Summary

DREAMS

VirginiaTech Invent the Future

STL Attack: Void Placement

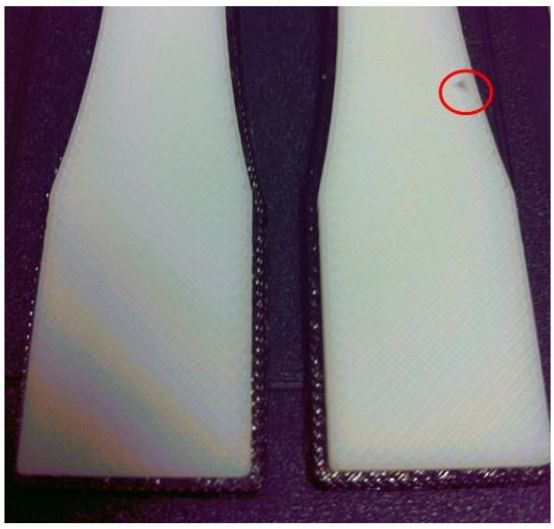


Digital Thread | Vulnerabilities | STL Attack | Case Study | Summary

DREAMS

VirginiaTech Invent the Future

STL Attack: Void Placement



Digital Thread | Vulnerabilities | STL Attack | Case Study | Summary

DREAMS

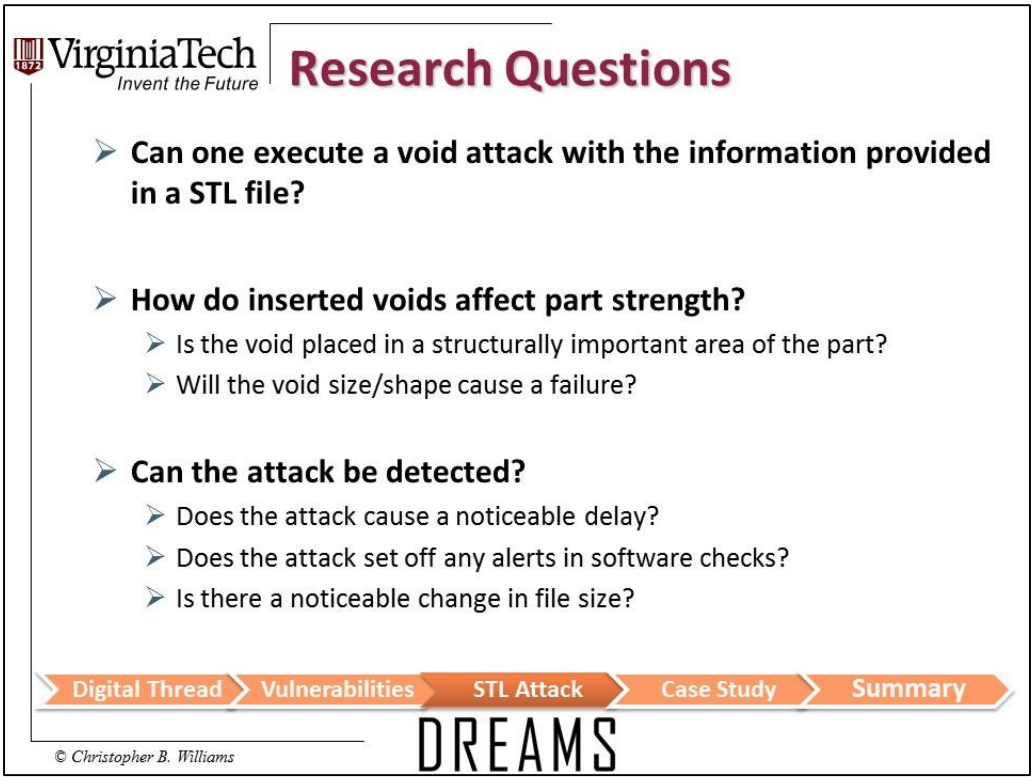
VirginiaTech Invent the Future

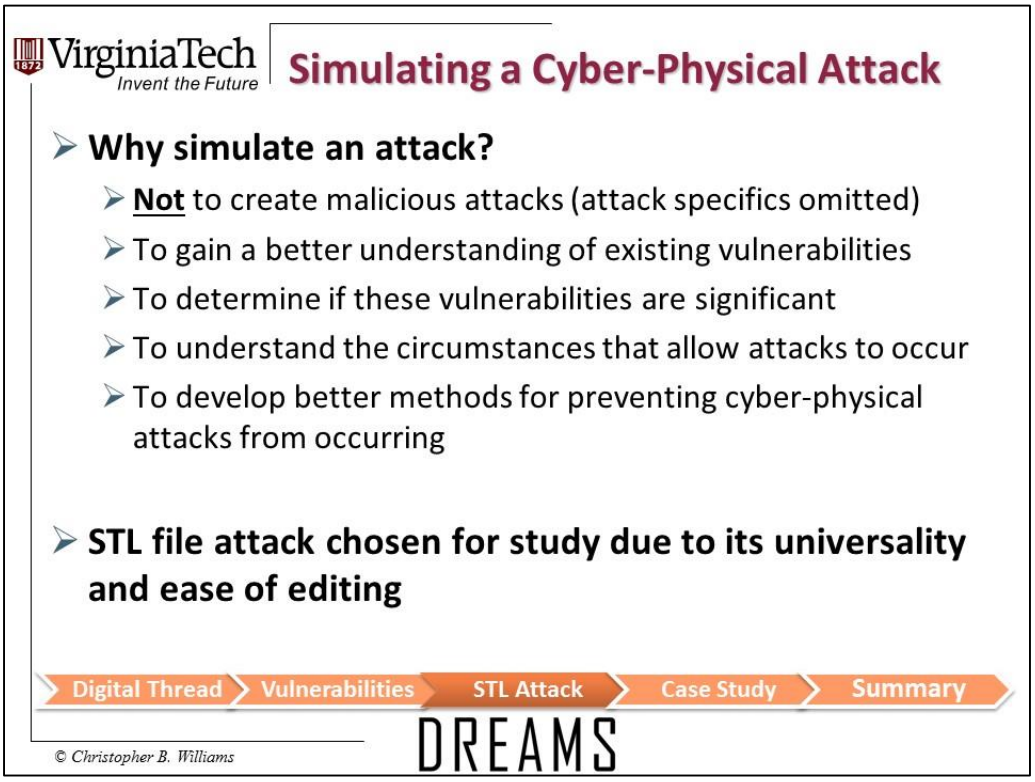
STL Attack: How to Detect?

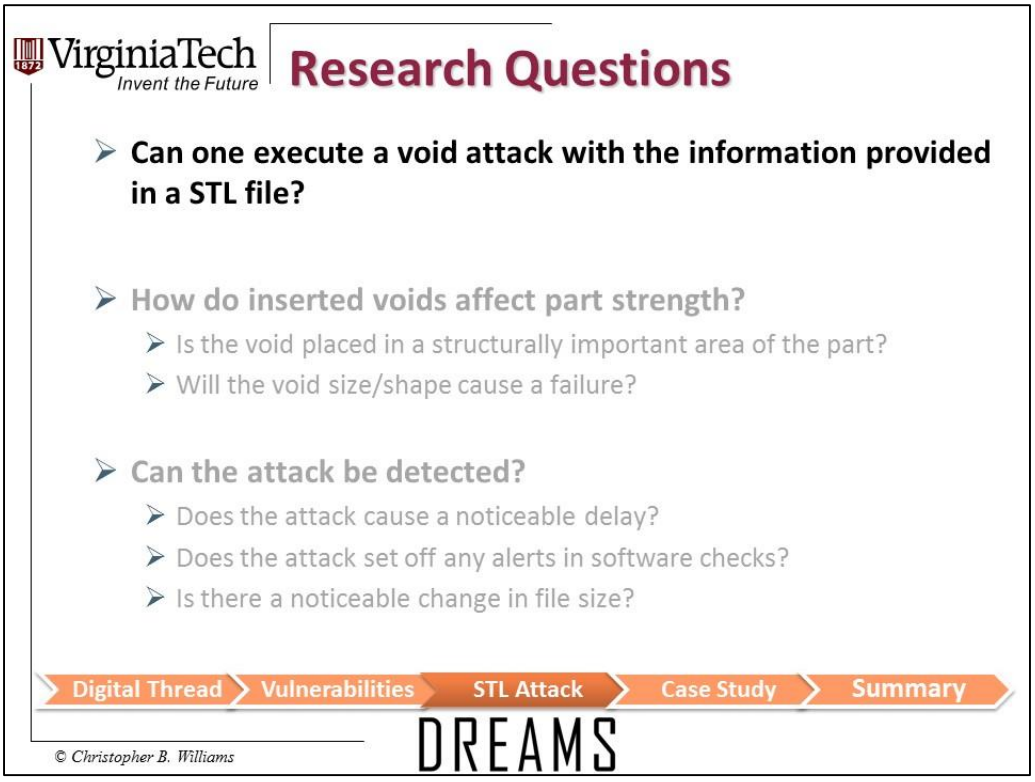
- External surface is untouched
- Mass difference is undetectable
- In-situ monitoring is validated against STL file
- Human visual inspection of every layer?
- CT scan of each completed part?

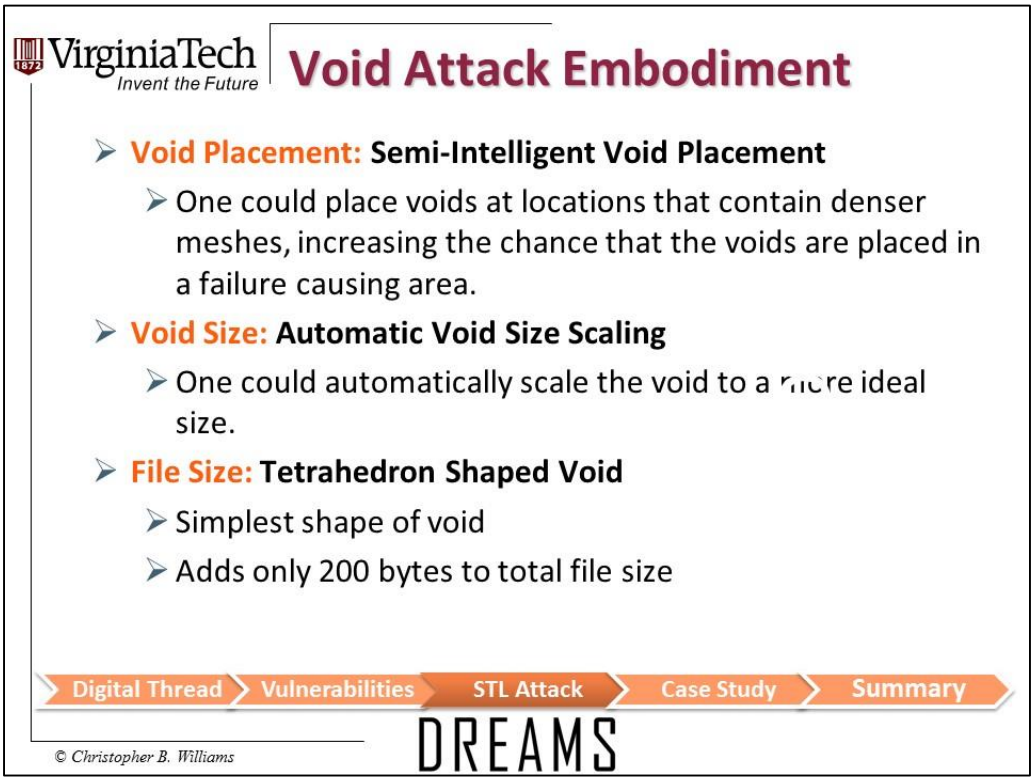
Digital Thread | Vulnerabilities | STL Attack | Case Study | Summary

DREAMS


VirginiaTech
Invent the Future
Research Questions
Can one execute a void attack with the information provided in a STL file?
How do inserted voids affect part strength?
Is the void placed in a structurally important area of the part?
Will the void size/shape cause a failure?
Can the attack be detected?
Does the attack cause a noticeable delay?
Does the attack set off any alerts in software checks?
Is there a noticeable change in file size?
Digital Thread
Vulnerabilities
STL Attack
Case Study
Summary
© Christopher B. Williams
DREAMS


VirginiaTech
Invent the Future
Simulating a Cyber-Physical Attack
Why simulate an attack?
Not to create malicious attacks (attack specifics omitted)
To gain a better understanding of existing vulnerabilities
To determine if these vulnerabilities are significant
To understand the circumstances that allow attacks to occur
To develop better methods for preventing cyber-physical attacks from occurring
STL file attack chosen for study due to its universality and ease of editing
Digital Thread
Vulnerabilities
STL Attack
Case Study
Summary
© Christopher B. Williams
DREAMS


VirginiaTech
Invent the Future
Research Questions
Can one execute a void attack with the information provided in a STL file?
How do inserted voids affect part strength?
Is the void placed in a structurally important area of the part?
Will the void size/shape cause a failure?
Can the attack be detected?
Does the attack cause a noticeable delay?
Does the attack set off any alerts in software checks?
Is there a noticeable change in file size?
Digital Thread
Vulnerabilities
STL Attack
Case Study
Summary
© Christopher B. Williams
DREAMS


VirginiaTech
Invent the Future
Void Attack Embodiment
Void Placement: Semi-Intelligent Void Placement
One could place voids at locations that contain denser meshes, increasing the chance that the voids are placed in a failure causing area.
Void Size: Automatic Void Size Scaling
One could automatically scale the void to a more ideal size.
File Size: Tetrahedron Shaped Void
Simplest shape of void
Adds only 200 bytes to total file size
Digital Thread
Vulnerabilities
STL Attack
Case Study
Summary
© Christopher B. Williams
DREAMS

VirginiaTech Invent the Future

Research Questions

- Can one execute a void attack with the information provided in a STL file?
- **How do inserted voids affect part strength?**
  - Is the void placed in a structurally important area of the part?
  - Will the void size/shape cause a failure?
- Can the attack be detected?
  - Does the attack cause a noticeable delay?
  - Does the attack set off any alerts in software checks?
  - Is there a noticeable change in file size?

Digital Thread | Vulnerabilities | STL Attack | Case Study | Summary

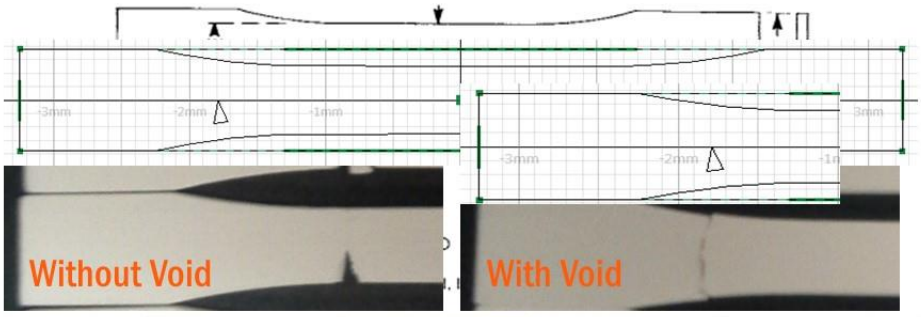
DREAMS

VirginiaTech Invent the Future

Effects on Part Strength

- **Void attack performed on ASTM Standard D638-10 tensile test specimen**
  - Single void automatically placed by software

ASTM D638 – 10



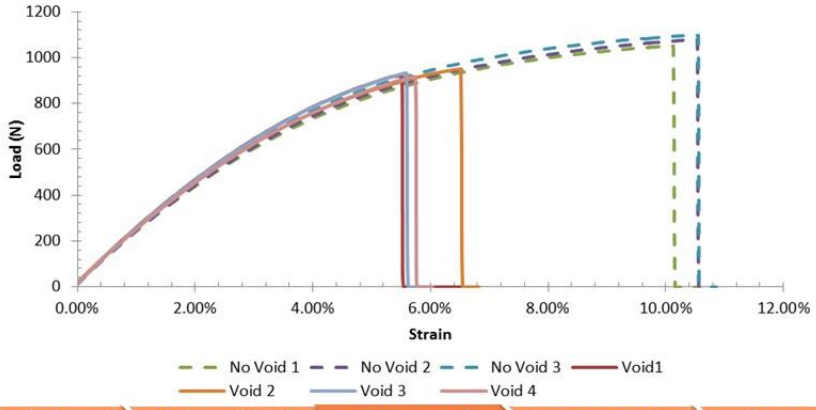
Digital Thread | Vulnerabilities | STL Attack | Case Study | Summary

DREAMS

VirginiaTech Invent the Future

Effects on Part Strength

- **Voids had a measurable reduction on part strength**
  - Average reduction in yield load from 1085N to 930N (14%)
  - Average strain at failure reduced from 10.4% to 5.8%



Digital Thread | Vulnerabilities | STL Attack | Case Study | Summary

DREAMS

VirginiaTech Invent the Future

Research Questions

- Can one execute a void attack with the information provided in a STL file?
- How do inserted voids affect part strength?
  - Is the void placed in a structurally important area of the part?
  - Will the void size/shape cause a failure?
- **Can the attack be detected?**
  - Does the attack cause a noticeable delay?
  - Does the attack set off any alerts in software checks?
  - Is there a noticeable change in file size?

Digital Thread | Vulnerabilities | STL Attack | Case Study | Summary

DREAMS

VirginiaTech Invent the Future

Human Subjects Testing

Goal:

- **Evaluate potential threat of a cyber attack via attack simulation on students**

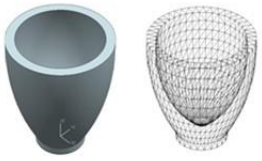
Digital Thread | Vulnerabilities | STL Attack | Case Study | Summary

DREAMS

VirginiaTech Invent the Future

Human Subjects Testing

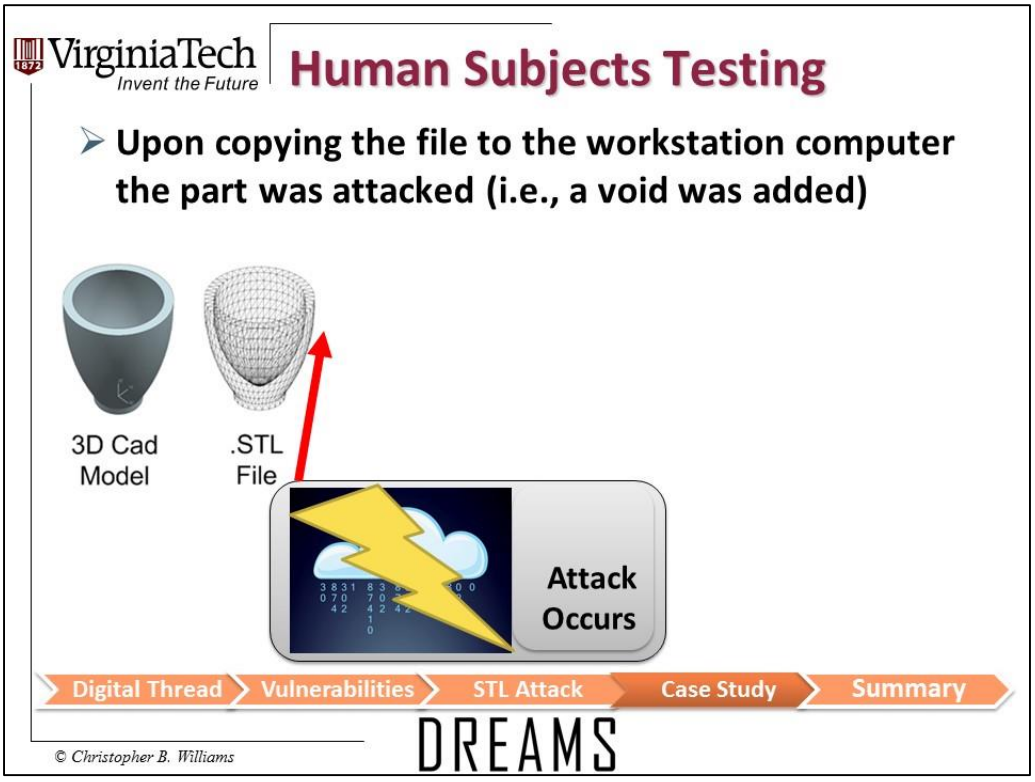
- **Students asked to model an ASTM standard tensile test specimen and bring the .STL to print**

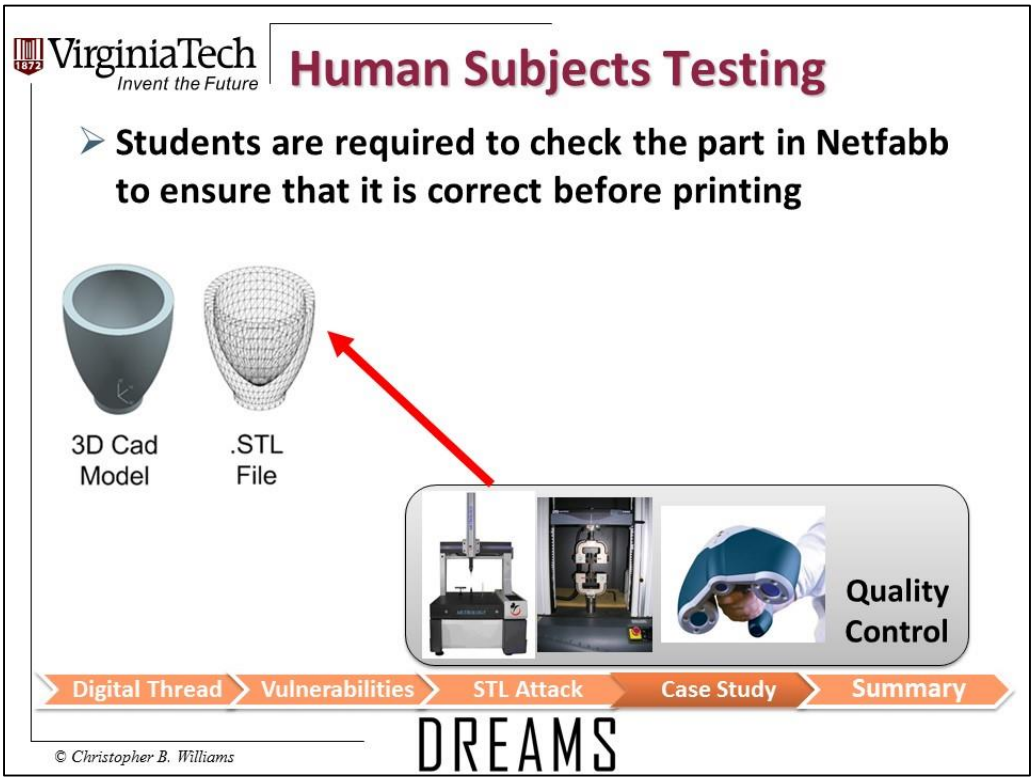


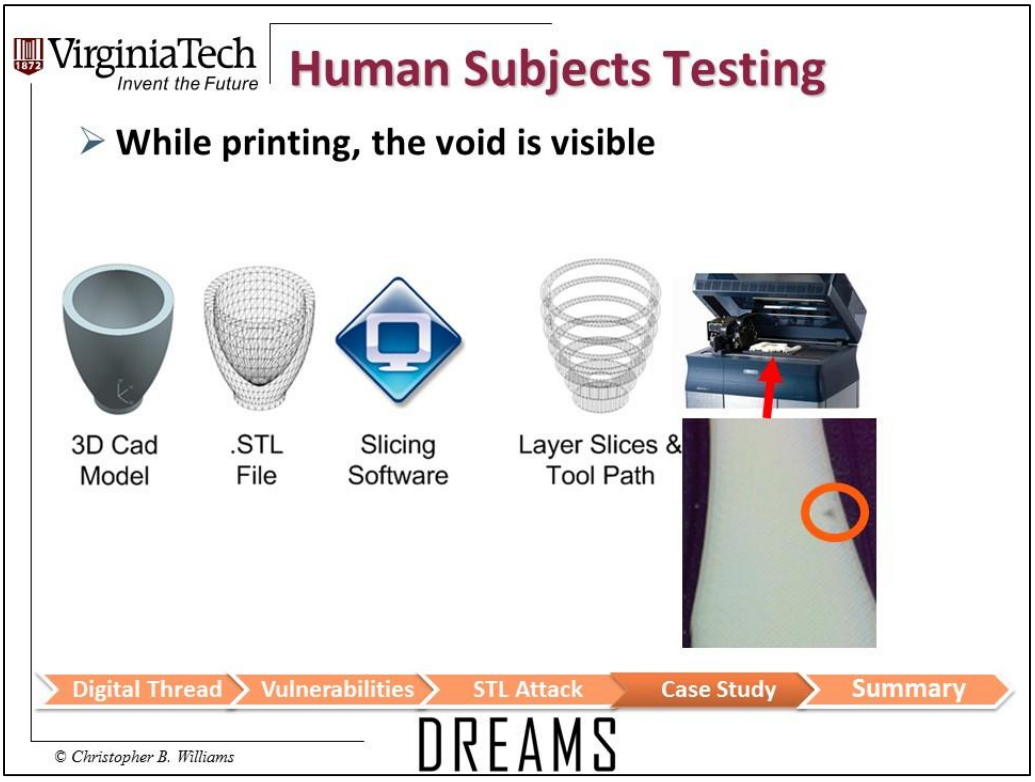
3D Cad Model .STL File

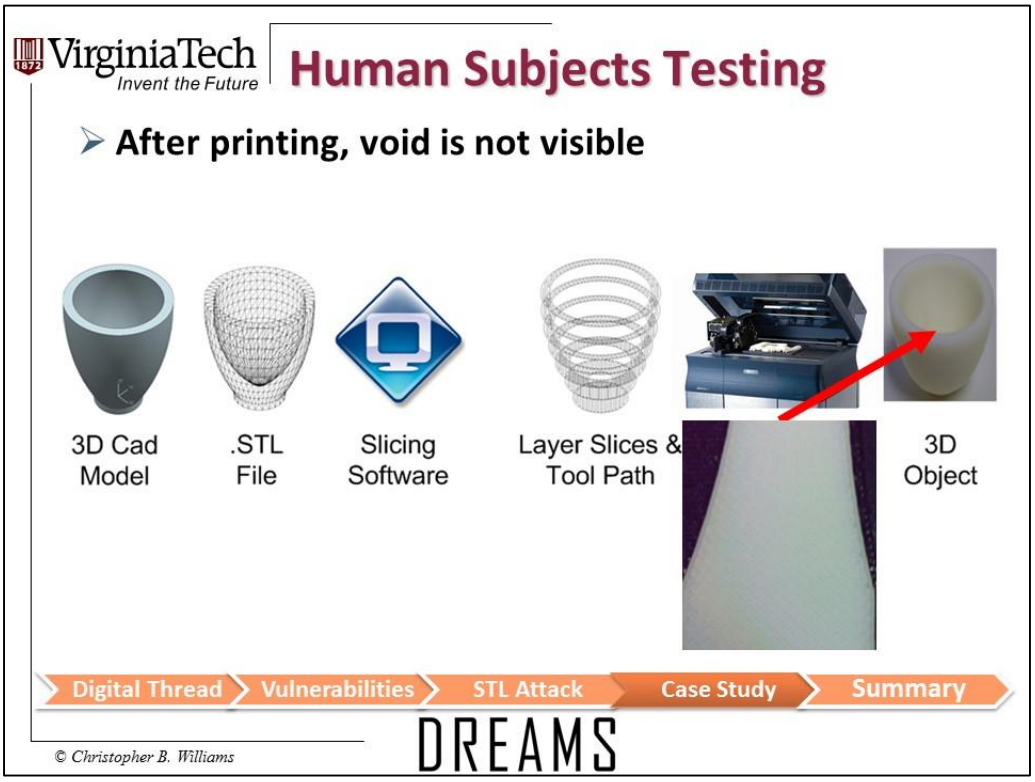
Digital Thread | Vulnerabilities | STL Attack | Case Study | Summary

DREAMS


VirginiaTech
Invent the Future
Human Subjects Testing
Upon copying the file to the workstation computer the part was attacked (i.e., a void was added)
3D Cad Model
.STL File
Attack Occurs
Digital Thread
Vulnerabilities
STL Attack
Case Study
Summary
© Christopher B. Williams
DREAMS


VirginiaTech
Invent the Future
Human Subjects Testing
Students are required to check the part in Netfabb to ensure that it is correct before printing
3D Cad Model
.STL File
Quality Control
Digital Thread
Vulnerabilities
STL Attack
Case Study
Summary
© Christopher B. Williams
DREAMS


VirginiaTech
Invent the Future
Human Subjects Testing
While printing, the void is visible
3D Cad Model
.STL File
Slicing Software
Layer Slices & Tool Path
Digital Thread
Vulnerabilities
STL Attack
Case Study
Summary
© Christopher B. Williams
DREAMS


VirginiaTech
Invent the Future
Human Subjects Testing
After printing, void is not visible
3D Cad Model
.STL File
Slicing Software
Layer Slices & Tool Path
3D Object
Digital Thread
Vulnerabilities
STL Attack
Case Study
Summary
© Christopher B. Williams
DREAMS

Human Subjects Testing

- Final part was measured and inspected before being broken on a tensile test machine

Digital Thread > Vulnerabilities > STL Attack > Case Study > Summary

DREAMS

Human Subjects Testing

- 4 groups participated (18 students)
- None of the groups detected the void before printing. (Netfabb check)
- 2 groups stayed while the parts were built
  - 1 group noticed signs of the voids during the build
- None of the groups indicated seeing the voids after the part was printed (before testing)
- All groups identified the part failed prematurely

Digital Thread > Vulnerabilities > STL Attack > Case Study > Summary

DREAMS

VirginiaTech Invent the Future

Human Subjects Testing

- 2 of the groups detected the void after testing
  - Explanations were tied to printer error

Digital Thread | Vulnerabilities | STL Attack | Case Study | Summary

DREAMS

VirginiaTech Invent the Future

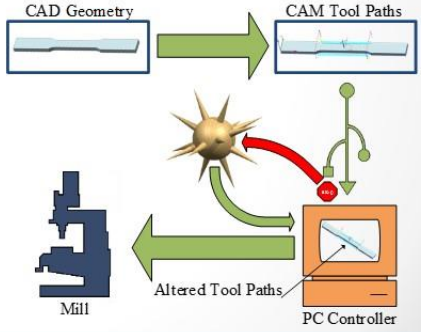
Prevention: STL Void Detection

- Determine the number of shells in a file
  - Files with only one shell cannot contain a simple void
- Determine shell size
  - Shells with a small number of faces are likely to be nonfunctional parts
- Identify inverted shells
  - Void normals will all be facing inwards
- How to detect small features that are not separate shells?

DREAMS

Attack Demonstration
Subtractive Processes – Machining

- **Goals**
  - Demonstrate Attack Feasibility
  - Understand Diagnostic Procedure of Unaware Engineers/Operators
- **Engineering Students Tasked to:**
  1) Create an ASTM Compliant Tensile Test Specimen using CAD
  2) Generate Tool Paths to Machine the Specimen using CAM
  3) Transfer the Tool Paths to a PC Controlled Mill
  4) Machine the Specimen
- **Malicious Software**
  - Located on PC Controller
  - Detects File Transfers
  - Replaces Tool Paths Files
- **Outcome**
  - Incorrect Part Manufactured
  - 19% Reduction in Performance

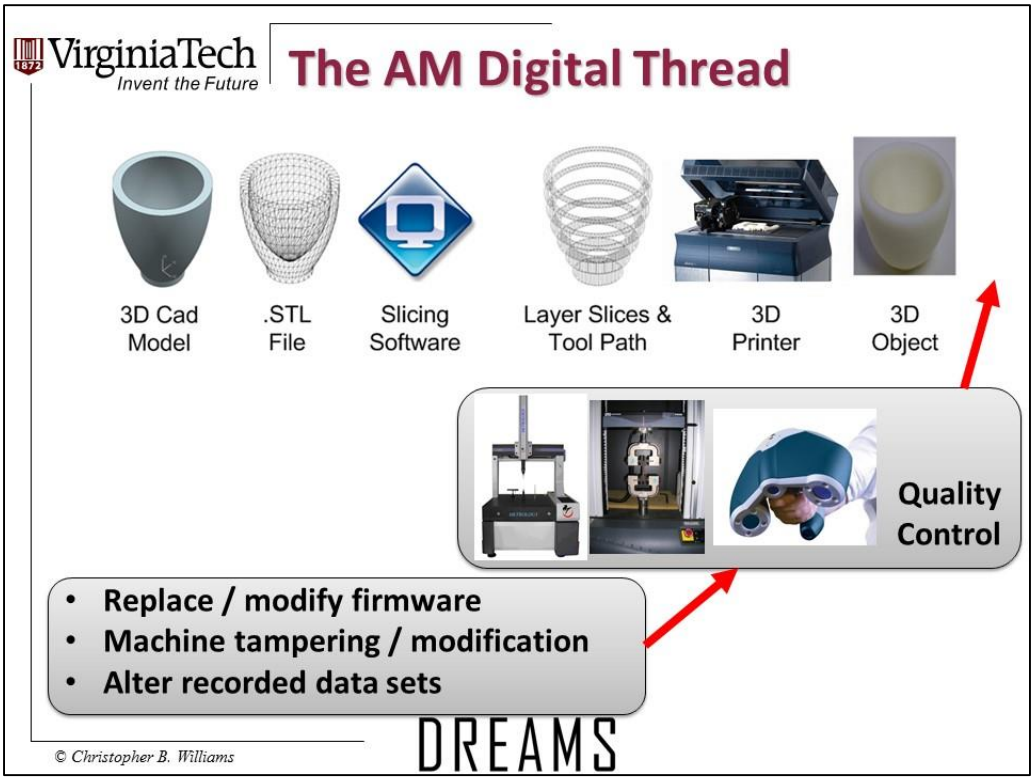


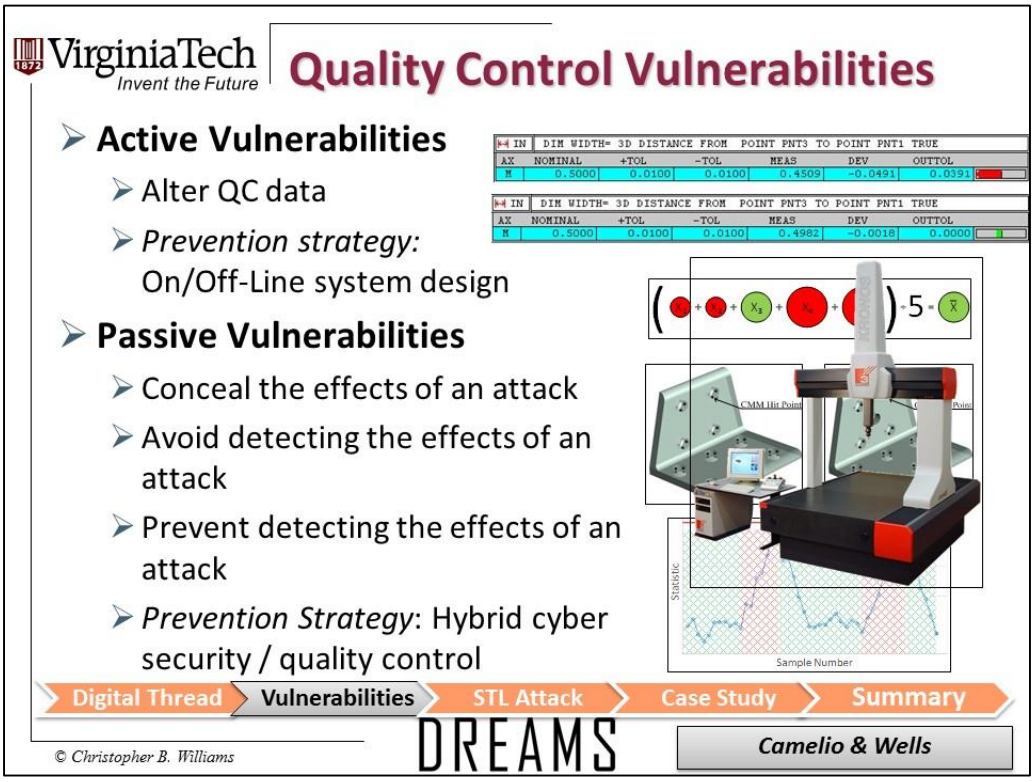
CENTER FOR INNOVATION-BASED MANUFACTURING an ICTAS CENTER at VIRGINIA TECH
ICTAS INSTITUTE for CRITICAL TECHNOLOGY and APPLIED SCIENCE at Virginia Tech
VirginiaTech Invent the Future

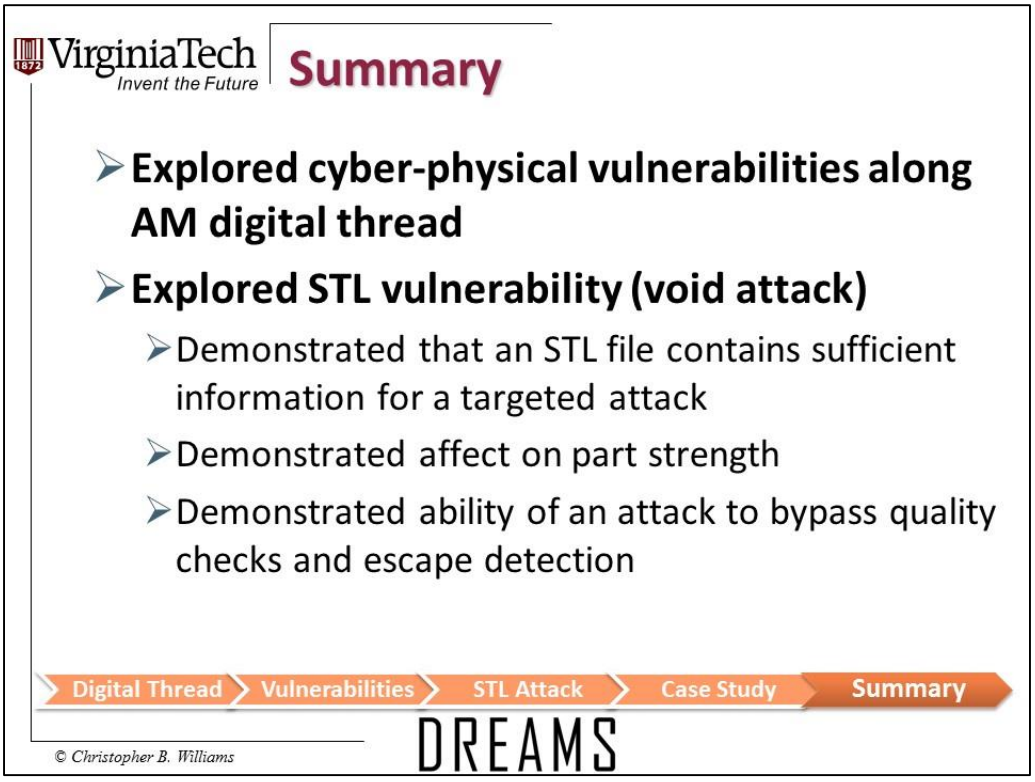
Demonstration Results

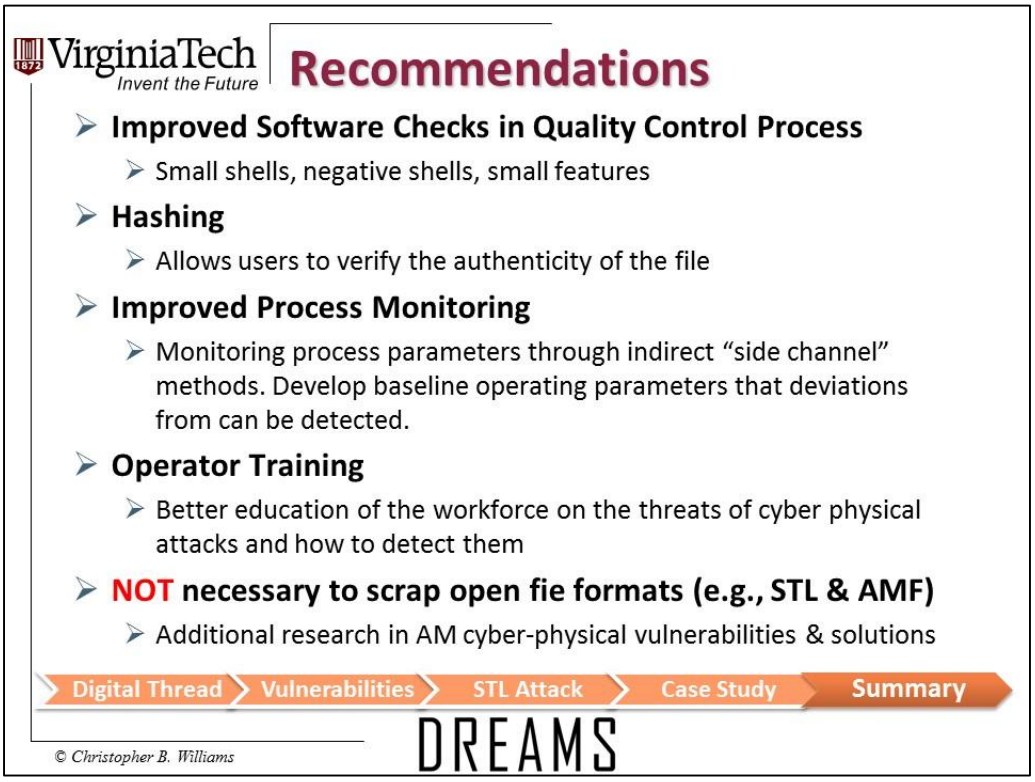
- **7 Groups attacked (3-4 students each)**
- **No group detected the attack**
- **First 3 groups did not measure the part**
  - Part "Looked Correct"
- **Last 4 groups measured the part, identified as incorrect**
- **Diagnostic strategies**
  - Step-by-step: each step of the process was checked for errors
    - Incorrect file was identified
  - Step-by-step (reverse): each step (in reverse) was checked for errors
    - No problem was identified
  - Ordered: steps were checked for errors from most likely to least likely
    - No problem was identified
- **Correct diagnosis was never made**

CENTER FOR INNOVATION-BASED MANUFACTURING an ICTAS CENTER at VIRGINIA TECH
ICTAS INSTITUTE for CRITICAL TECHNOLOGY and APPLIED SCIENCE at Virginia Tech
VirginiaTech Invent the Future


VirginiaTech
Invent the Future
The AM Digital Thread
3D Cad Model
.STL File
Slicing Software
Layer Slices & Tool Path
3D Printer
3D Object
Quality Control
• Replace / modify firmware
• Machine tampering / modification
• Alter recorded data sets
© Christopher B. Williams
DREAMS


VirginiaTech
Invent the Future
Quality Control Vulnerabilities
Active Vulnerabilities
Alter QC data
Prevention strategy: On/Off-Line system design
Passive Vulnerabilities
Conceal the effects of an attack
Avoid detecting the effects of an attack
Prevent detecting the effects of an attack
Prevention Strategy: Hybrid cyber security / quality control
Digital Thread
Vulnerabilities
STL Attack
Case Study
Summary
Camelio & Wells
© Christopher B. Williams
DREAMS


VirginiaTech
Invent the Future
Summary
Explored cyber-physical vulnerabilities along AM digital thread
Explored STL vulnerability (void attack)
Demonstrated that an STL file contains sufficient information for a targeted attack
Demonstrated affect on part strength
Demonstrated ability of an attack to bypass quality checks and escape detection
Digital Thread
Vulnerabilities
STL Attack
Case Study
Summary
© Christopher B. Williams
DREAMS


VirginiaTech
Invent the Future
Recommendations
Improved Software Checks in Quality Control Process
Small shells, negative shells, small features
Hashing
Allows users to verify the authenticity of the file
Improved Process Monitoring
Monitoring process parameters through indirect "side channel" methods. Develop baseline operating parameters that deviations from can be detected.
Operator Training
Better education of the workforce on the threats of cyber physical attacks and how to detect them
NOT necessary to scrap open fie formats (e.g., STL & AMF)
Additional research in AM cyber-physical vulnerabilities & solutions
Digital Thread
Vulnerabilities
STL Attack
Case Study
Summary
© Christopher B. Williams
DREAMS

VirginiaTech
Invent the Future

An Analysis of Cyber-Physical Vulnerabilities in Additive Manufacturing

Thank you.

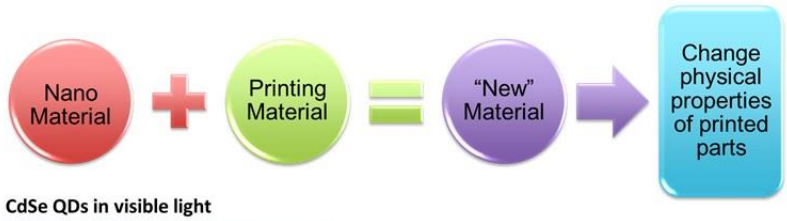
DREAMS
Design, Research, and Education for Additive Manufacturing Systems
http://www.dreams.me.vt.edu/

Christopher B. Williams
Associate Professor
Director, DREAMS Lab
Associate Director, MII
Virginia Tech
Department of Mechanical Engineering

DREAMS

VirginiaTech
Invent the Future

Process: AM Nanocomposites

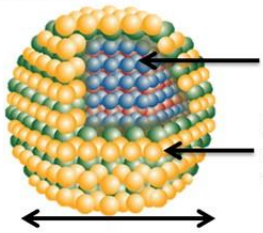


CdSe QDs in visible light

CdSe QDs in UV light (365 nm)

Increase in QDs size

Quantum Dot

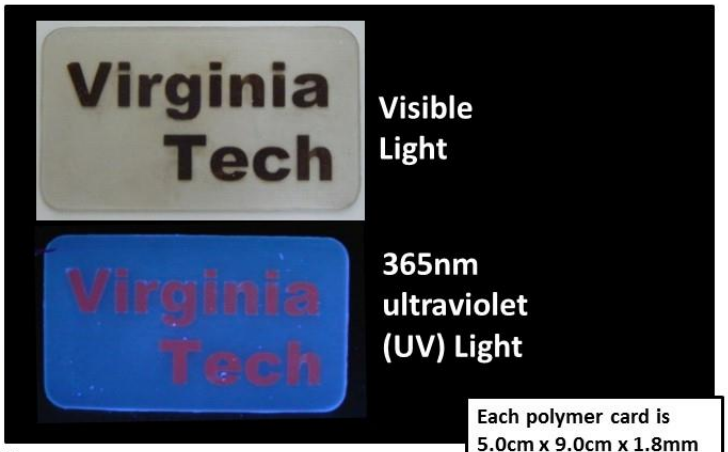


http://www.photonics.com/Article.aspx?AID=29421

In collaboration with Tom Campbell & VT LENS Lab
http://www.ictas.vt.edu/lens/index.html

VirginiaTech Invent the Future

Process: AM Nanocomposites



Each polymer card is 5.0cm x 9.0cm x 1.8mm

Embedded QD lettering:

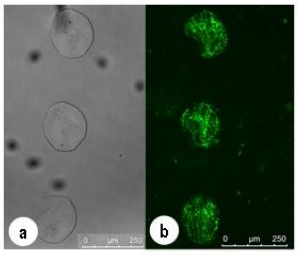
- Each letter is 700µm thick
- Made from a quantum dot nanocomposite resin (2.0% CdSe).
- Fabricated via Stratasys (Objet) PolyJet 3D Printing

DREAMS

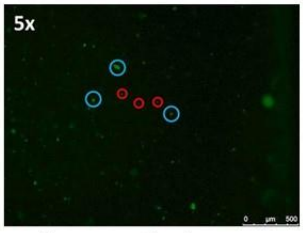
VirginiaTech Invent the Future

Process: AM Nanocomposites

- Selective jetting of QD nanoink enables "watermarking" of 3D Printed goods
- Printed mark is a physical feature – not a 'sticker'
- Printed mark is a material property – it cannot be replicated via 3D Scanning
- Stochastic arrangement of nanoparticles in droplet create unique identifier that cannot be replicated



Images of jetted QD Nanoink in (a) visible and (b) UV light



Fluorescent microscope images of QD nanoparticles in 3D Printed part.

DREAMS


VirginiaTech
Invent the Future
Relevant Publications
Elliott, Ivanova, Williams, Campbell (2013), "Inkjet Printing of Quantum Dots in Photopolymer for use in Additive Manufacturing of Nanocomposites," Advanced Engineering Materials, in press.
Ivanova, Williams, Campbell (2013), "Additive Manufacturing (AM) and Nanotechnology: Promises and Challenges," Rapid Prototyping Journal, Volume 19, Issue 5.
Elliott, Ivanova, Williams, Campbell (2012), "An Investigation of the Effects of Quantum Dot Nanoparticles on Photopolymer Resin for use in Polyjet Direct 3D Printing," International Solid Freeform Fabrication Symposium, Austin, TX.
© Christopher B. Williams
DREAMS

Presentation 2: *Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing Systems*

Scott Zimmerman, CISSP-ISSEP
Principal IT Advisor, Concurrent Technologies Corporation (CTC)

Dominick Glavach, CISSP, GCIH
Principle Fellow, Information Systems Security Engineer, CTC

Key Discussion Points:

- Digitization of manufacturing increases the risks for theft, disruption, and sabotage. There are vulnerabilities in preproduction software, data storage and data transfers, the StereoLythography (STL) file format, printer components, and engineering / production practices.
- The presenters discussed their experience with obtaining a 3D printer and the cybersecurity challenges experienced when setting it up.
- Many AM machines contain old firmware, cannot be patched easily, and have poor authentication processes. It was commented that this is not unusual for manufacturing systems.
- The AM process is also complex, variable / changeable, and tends to leave a lot of residual data in various places, making cybersecurity without interfering with functionality a challenge.
- There is a significant opportunity to be proactive rather than reactive regarding cybersecurity due to the nature of the technology and the state of the industry. The authors presented several recommendations for cybersecurity controls and highlighted the value of traditional cybersecurity controls such as firewalls.
- Participants stressed the need for focusing on people – a recent attack was described that began with a phishing scam. One participant commented that manufacturers and users are not security aware, yet DDM supports minimal digital knowledge - any security solution needs to be simple and usable.

Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing Sytems

Scott Zimmerman, CISSP-ISEP
Concurrent Technologies Corporation
Johnstown, PA USA
zimmerms@ctc.com

Dom Glavach, CISSP
Concurrent Technologies Corporation
Johnstown, PA USA
dg@ctc.com

Abstract – Applying meaningful and assessing impactful cybersecurity controls are ongoing and significant challenges for the Direct Digital Manufacturing (DDM) Community. These issues will be significant as the technology moves into the mainstream manufacturing supply chain. This presentation will, therefore, address cybersecurity threats to DDM, including insight into potential attack scenarios and motivations, gained through direct observations. 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, cybersecurity, direct digital manufacturing, programmable logic controllers

1 INTRODUCTION

Based on the expectation and potential impact in revitalizing the U.S. and global manufacturing landscape, Direct Digital Manufacturing (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…. 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." [1] While supply chain implications and benefits are numerous, cybersecurity remains a significant challenge.

The Economist (April 2012) refers to the potential for DDM to create the third industrial revolution[2], noting that the disruption to manufacturing will be as significant as digitization was to telecommunication, office equipment, photography and publishing. While digitization creates an incredible growth potential within manufacturing, it also comes with many of the associated cybersecurity risks that impact 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. The negative impacts of failure to include security protocols at start-up can be seen within the power and energy sector, which has 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 to contend with the threats of the connected world in the current environment. Now these systems are so tightly woven into the fabric of the power grid, retrofitting security is a much larger task than if it had been tackled in the beginning.

[2] CHARACTERIZING THE THREAT

The technical advances and economic impact associated with the DDM revolution attracts an innovative and entrepreneurial audience. History illustrates 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. Hathaway states that corporate and government leadership are reactive in nature to cybersecurity needs and only act to mitigate security issues after a significant event occurs. She further concludes that additional legislation may be needed to incentivize corporate and government leadership to get serious about cybersecurity.[3]

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, resulting 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. The proposed presentation explores possible attack scenarios and associated risk evaluations in the areas of:

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

[3] SECURITY ASSESSMENT RESULTS

System Installation

With the opportunity to conduct a security assessment on a newly installed AM system, we have identified risks at the inception; it begins with internal coordination and communications between enterprise Information Technology (IT) and shop floor personnel. In general, the focus and priority of the materials/manufacturing/engineering staff are installation and operation, which includes connection to the internal and possibly an external network, so the relevant parts can be produced. Their initial concerns are not about how to make this system secure.

In the particular case under consideration, 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 OEM 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 system, not a typical office document printer. Following this discovery, the security team has moved the printer to a secure and scrutinized subnet on the network. Now, additional security controls and enhanced logging occur routinely and yet where it is still possible for the engineering team to work directly through the network with the manufacturer.

Assessment Methodology

AM systems can be complex, consisting of several central processing units (CPU) and PLCs, operating systems, and applications (including both AM-specific ones as well as applications that support the user experience, such as web-browser 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.

We deployed both the corporate security assessment methodology as well as the security risk assessment provided in the NIST DRAFT NISTIR 8023, Risk Management for Replication Devices. We will present and discuss specific scan results and findings. In addition, we will propose a series of security protocols as best practices for any DDM system implementation. We list a selection of possible solutions below and we will expand on the requirements for success in this presentation.

Recommendations

- Mandatory scanning (enumeration) of system prior to deploying to the network and disable all unneeded communications/system processes,
- Review of user accounts/groups on the system including their level of privilege and adjust accordingly,
- 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)
- Processes developed for system updates/upgrades

Conclusion

High-end AM printers are expensive, highly calibrated machines, increasingly complex, and generally not 'plug-and-play' systems. With respect to the system discussed in this presentation, there has been a great deal of ongoing support from the OEM in order to optimize printer operational performance. This type of support requires remote connectivity to the system. When the manufacturer is a foreign entity, this situation compounds security challenges and complicates protocols due to the need to comply with International Traffic in Arms (ITAR) regulations that may prohibit collaborations. At a minimum, many security assessment protocols and mitigation procedures implemented typically for enterprise business systems should be applied or adapted for implementation and operation of DDM systems.

REFERENCES

C.M. McNulty, N. Armas, "Toward the Printed World: Additive Manufacturing and Implication for National Security," September 2012 Institute for National Strategic Studies, National Defense University, Defense Horizons

The Economist, "A third industrial revolution". Accessed November 2014, http://www.economist.com/node/21552901

M.E. Hathaway, "Leadership and Responsibility for Cybersecurity", Georgetown Journal of International Affairs, pages 71-80, March 2013.

f

Presentation:

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

NIST Cybersecurity for
Direct Digital Manufacturing Symposium
February 3, 2015

Scott Zimmerman, CISSP-ISSEP
Principal Technical Advisor
sdz@ctc.com
(814) 410-7710

Dom Glavach, CISSP
Principal Information Security Engineer
dg@ctc.com
(814) 421-5555

Concurrent Technologies Corporation

1

Agenda

- Introductions
- Defining the threat
- Attack scenarios
- Assessment
- Recommendations
- Conclusion

Concurrent Technologies Corporation

Approved for Public Release 2

Concurrent Technologies Corporation (CTC) Summary

- Established in 1987
- An independent, nonprofit, R&D organization
- Staff of approximately 1,000 dedicated professionals
- Approximately 40 locations

CTC has been a thought leader in providing cybersecurity solutions for over fifteen years. We deliver holistic solutions based on experience in protection, detection, and reaction measures as well as network engineering, management, modeling, and assessment activities. We provide both offensive and defensive capabilities. CTC's expertise in cybersecurity can be successfully applied to support cyber analysis, improve situational awareness, increase operational performance, assure compliance with security policies, and address emerging technical challenges.

CTC Concurrent Technologies Corporation

Approved for Public Release 3

Cybersecurity

- Objectives of cybersecurity are to preserve:
  - Confidentiality - protecting information from disclosure to unauthorized parties
  - Integrity - maintaining and assuring accuracy and consistency of data over its entire life-cycle
  - Availability - ensuring that authorized parties are able to access information when needed
- Measurement of cybersecurity
  - Risk – potential for loss
  - Threat – exploitation of a vulnerability
  - Vulnerability – weakness in security
- Risk cannot be eliminated yet it can be managed and reduced
- DDM market presents new opportunities and attack vectors for those who wish to harm national security and for the criminal element
- Timely to build in and not bolt on security later

CTC Concurrent Technologies Corporation

Approved for Public Release 4

DDM Cybersecurity

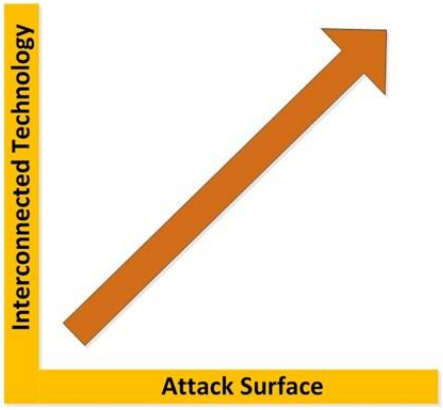
- Digitization is as disruptive to manufacturing as it was to telecommunications, photography, publishing and other digitized industries
- No air gap now between enterprise information systems and shop floor
- Definite increase in attacks from information systems to critical infrastructure and cyber-physical systems
- Presents an opportunity to be proactive rather than reactive
  - Develop standards, systems and processes before technology is adopted broadly when it limits or prohibits deployment of protection mechanisms
- From stagecoach to smart thermostats, security is often an afterthought in new technology design and implementation.

CTC Concurrent Technologies Corporation

Approved for Public Release 5

DDM Cyber Risks

- Theft
  - Property, Process, License
- Disruption
  - Process, Production, Equipment
- Sabotage
  - Products, Reputation



CTC Concurrent Technologies Corporation

Approved for Public Release 6

DDM Cyber Threats

- Who will attack?
  - Sophisticated and funded, competitors, partners, criminals, state actors and terrorist elements
- Why attack?
  - Economic advantage
  - Military strategic and tactical advantages
  - Political statements

Additive Manufacturing Digital Thread

DDM Cyber Vulnerabilities

- Preproduction software
- Data storage and data transfers
- Model file formats
- Printer components
- Engineering and production practices

Preproduction Software

- AutoCAD
  - 5 Common Vulnerabilities and Exposures (CVE)
  - 2 enable unauthorized program execution
  - 3 enable unauthorized access
- Trimble SketchUp
  - 4 CVEs
  - 2 enable unauthorized program execution
  - 2 enable software disruptions (overflows)

Data Storage and Transfers

- USB
  - Uncontrolled media
  - Historically known as an exploitation avenue
  - Residual data
  - Configuration management
- Network
  - Enables automated attacks
  - Increases complexity
  - Multiparty access and access controls

Model File Formats

STL files (STereoLithography)

- "Trusted" standard in the industry
- Binary and plaintext formats
- Lack file integrity checks

Printer Components

Highly calibrated system with

- Operating Systems
  - Microsoft Windows and Linux
  - Internet Explorer
- Camera software
- Firmware
- Control software
- Self contained network

Engineering and Production Practices

- Internet born STL examples
  - Calibrate your printer.stl.exe
- Revision control
  - N copies of intellectual property in X locations
- Residual data
  - Everywhere
- Support and maintenance
  - Remote access and remote control

DDM Case Study

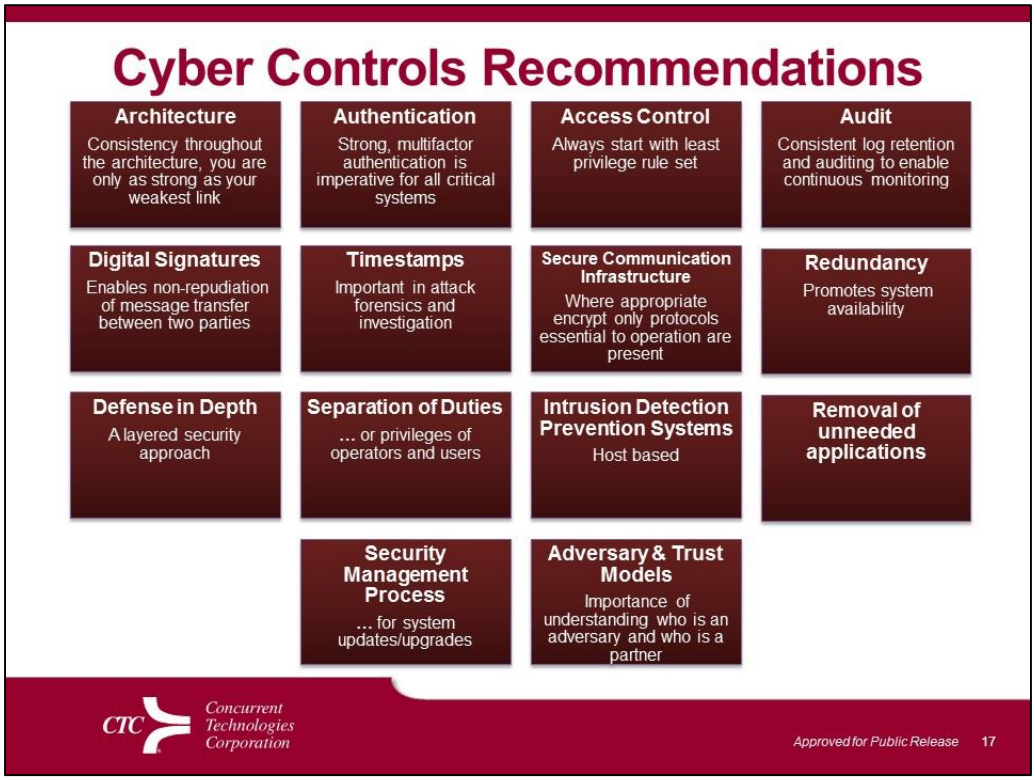
"Hey, can you install this new printer we just received?"

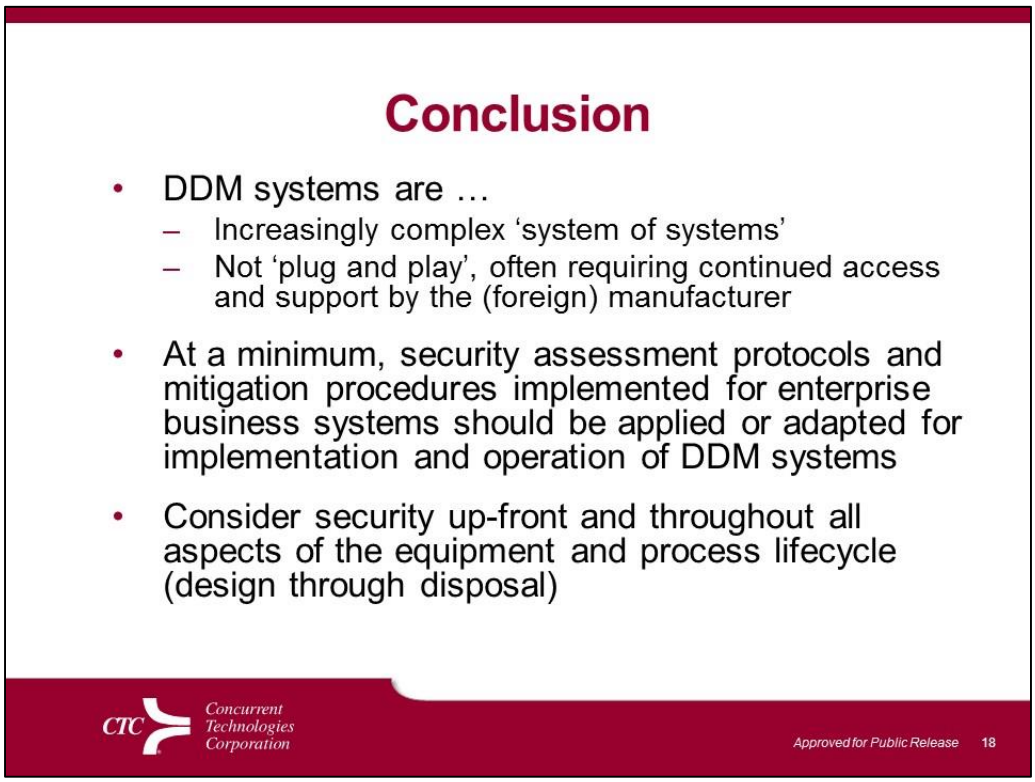
- AM system for rapid prototyping

Selective Laser Melting (SLM) Machine, SLM Solutions

DDM Cyber Assessment

- Assessment methodologies
  - CTC proprietary assessment methodology
  - NIST DRAFT NISTIR 8023, Risk Management for Replication Devices
- Results
  - Most applications and OS's unpatched
  - Factory default install of AV/Host IDS
  - No process for updating/patching
  - Residual data left everywhere
  - Poor authentication (shared/default passwords)


Cyber Controls Recommendations
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
CTC Concurrent Technologies Corporation
Approved for Public Release 17


Conclusion
DDM systems are …
Increasingly complex 'system of systems'
Not 'plug and play', often requiring continued access and support by the (foreign) manufacturer
At a minimum, security assessment protocols and mitigation procedures implemented for enterprise business systems should be applied or adapted for implementation and operation of DDM systems
Consider security up-front and throughout all aspects of the equipment and process lifecycle (design through disposal)
CTC Concurrent Technologies Corporation
Approved for Public Release 18


NOTICE
SAFETY GLASSES REQUIRED IN THIS AREA
CAUTION
FORKLIFT TRAF
KEEP CLEAR
CTC
Concurrent Technologies Corporation
1-800-CTC-4392
www.ctc.com
CTC
Concurrent Technologies Corporation
19

Presentation 3: *Cybersecurity for Advanced Manufacturing – Securing the Digital Thread*

Dr. Michael F. McGrath
National Defense Industrial Association (NDIA) Manufacturing Division

Key Discussion Points:

- The intersection between cyber/cybersecurity and manufacturing is critical.
- The presenter described three concerns expressed by manufacturers: theft, alteration, and disruption. These closely mirror the traditional Confidentiality, Integrity, and Availability (CIA) security objectives..
- IT solutions don't always fit the manufacturing world. Manufacturers often have a mix of old and new equipment. The new can be secured, but securing the old is much more difficult, and the old has to work with the new.
- Culture change is necessary. Some participants indicated the industry has to change – vendors will say anything to sell a product; manufacturing CEOs place productivity over security, and CISOs don't have much say regarding the manufacturing operations.
- Requirements are beginning to be seen – e.g. Defense Acquisition Regulations System (DFARS) clause which requires flow down of responsibility to sub-suppliers.
- Some companies may be especially vulnerable as they may not recognize a risk. Interconnected supply chains with a lot of data sharing may be especially vulnerable if they use small company suppliers who don't recognize cybersecurity risks in manufacturing.
- Manufacturing presents a unique set of problems combining cyber plus Industrial Control System (ICS) vulnerabilities. Existing cybersecurity controls may not be sufficient in a DDM environment. The problem is not unique to AM, but AM presents a significant opportunity to build security in.
- An NDIA working group regarding cybersecurity in manufacturing is currently being formed.

Cybersecurity for Advance Manufacturing -- Protecting the Digital Thread

Dr. Michael McGrath
National Defense Industrial Association (NDIA) Manufacturing Division
Arlington, VA, USA
mfm@mcgrath-analytics-llc.com

Abstract: Government and industry have focused much effort on protecting technical information in business and engineering information systems. Relatively less action has been taken to improve protection of technical data in factory floor networks and control systems, which are increasingly subject to cyber threats. NDIA's Manufacturing Division and Cyber Division jointly developed a White Paper in 2014 to heighten awareness of the need for better practices and technical solutions to protect against theft of technical data transiting or residing in manufacturing systems, alteration of the data (thereby compromising the physical parts produced), or interference with reliable and safe production operations. Direct digital manufacturing is not inherently more vulnerable than other types of manufacturing, but it presents a very inviting target for would-be Intellectual property thieves or counterfeiters -- the full set of product and process information is available in one place, and the barriers to entry are low. This presentation offers several recommendations for enhancing protection of technical data in factory floor networks and in direct digital manufacturing systems in particular.

Presentation:

NDIA
National Defense Industrial Association
Promoting National Security Since 1919

Cyber Division & Manufacturing Division
Joint Working Group

Cyber Security for Advanced Manufacturing

NIST Cybersecurity for Direct Digital Manufacturing Symposium
February 3, 2015

Michael McGrath
Consultant, Analytic Services Inc.
michael.mcgrath@anser.org

Manufacturing is a Cyber-physical Business

Common Visions
Smart Manufacturing, Industrial Internet, Industry 4.0, …
The Internet of Things!

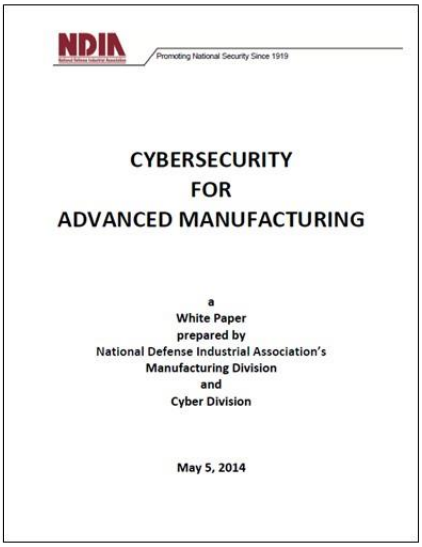
Advanced Manufacturing is:

- Driven by a "Digital Thread" of product and process information – ***valuable intellectual property (IP)***
- Networked at every level to gain efficiency, speed and quality
- Targeted by global cyber threats

2

NDIA White Paper

Protecting the Digital Thread


NDIA
Promoting National Security Since 1919

CYBERSECURITY
FOR
ADVANCED MANUFACTURING

a
White Paper
prepared by
National Defense Industrial Association's
Manufacturing Division
and
Cyber Division

May 5, 2014

www.ndia.org/Divisions/Divisions/Manufacturing

Manufacturing Concerns:

- **Theft of technical info** -- can compromise national defense and economic security
- **Alteration of technical data** -- can alter the part or the process, with physical consequences to mission and safety
- **Disruption or denial of process control** -- can shut down production

A risk management problem. Need resilience!

3

We Started with a Hypothetical Scenario

Use additive mfg to integrate power electronics with solar panel support structure

- OEM sends 3-D product data file to supplier for prototyping
- Intercepted by advanced persistent threat
- Prototype fabricated, delivered and successfully tested
- OEM sends new file, order for 12 parts
- Intercepted and modified by adversary to include a kill switch. Not detected.
- Parts fabricated, QC'd, delivered and installed
- Bird on orbit with kill switch controlled by adversary

We quickly learned there are plenty of real scenarios to learn from …

4

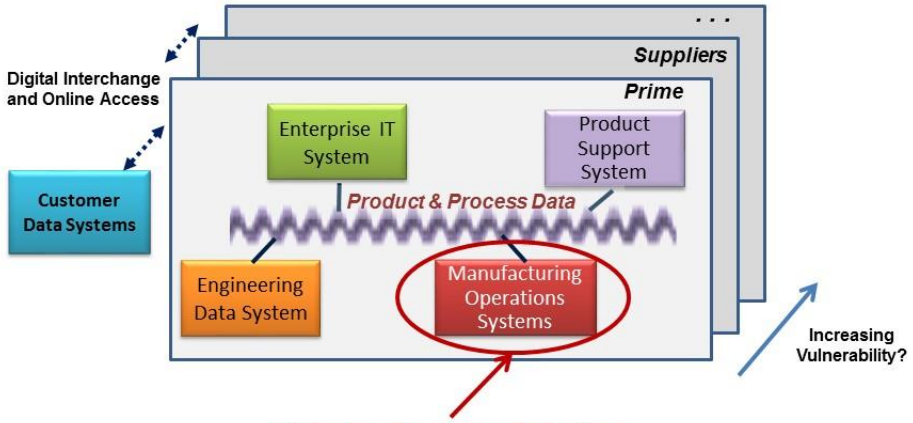

The Threat is Real, Global and Growing
Manufacturing is an inviting target
Global Cyber Threat Landscape
The Washington Post
Weapons designs compromised by Chinese hackers
Ellen Nakashima 10:54 PM ET
W32.Stuxnet Dossier
Version 1.4 (February 2011)
Symantec Security Response
Cyber Security
German jitters over cyber attacks
www.DW.DE , 8 Mar 2013
MANDIANT
APT1
Incident rates across monitored industries
Manufacturing 26.5%
Finance and insurance 20.9%
Information and communication 18.7%
Health and social services 7.3%
Retail and wholesale 6.6%
IBM Security Services Cyber Security Intelligence Index 2014
Manufacturing: a 1 in 3 chance of being targeted by at least one Spear Phishing attack in 2013
Symantec Internet Security Report 2014
intel Security
Cost to Global Economy > $400 B
KASPERSKY
WHO'S SPYING ON YOU?
verizon
2014 DATA BREACH INVESTIGATIONS REPORT
No business is safe from cyber-espionage
5


The Threat is Real, Global and Growing
Manufacturing is an inviting target
Global Cyber Threat Landscape
The Washington Post
Weapons designs
COUNTDOWN TO ZERO DAY
KIM ZETTER
… and the level of sophistication can be high!
Symantec Security Response
Cost to Global Economy > $400 B
Incident rates across monitor
Manufacturing
Finance and insurance
Information and communication
Health and social services 7.3%
Retail and wholesale 6.6%
IBM Security Services Cyber Security Intelligence Index 2014
Symantec Internet Security Report 2014
KASPERSKY
WHO'S SPYING ON YOU?
verizon
2014 DATA BREACH INVESTIGATIONS REPORT
No business is safe from cyber-espionage
6

Scope: Protecting the Digital Thread

Technical Data in the Advanced Manufacturing Enterprise

Targeted by nation states, terrorists, criminals and hacktivists.



IT Cyber Security Solutions May Not Fit Manufacturing Operations Needs

7

Operational Technology (OT) vs. IT

What's Different?

- **ICS systems are long-lived capital investments (15-20 year life)**
  - *Obsolete operating systems and software are common*
  - *New systems architected for security, but hard to interoperate with old*
- **"Production mindset" with little tolerance for OT down time**
  - *Operate in real time with critical safety implications – cannot install patches without scheduled downtime and testing*
  - *Weak privilege management among operators and maintainers. Growing use of wireless devices.*
  - *Nascent cybersecurity awareness and limited workforce training.*
- **Manufacturing differs from other ICS applications (e.g. Power Grid)**
  - *Every manufacturing job brings new executable code into system*
  - *Tech data flowing through the system is a target*

What We Heard from Interviews

Gov't, Industry, Academia

- CIOs/CISOs in the defense primes are implementing strong cyber risk management and sharing info through the DIB CS/IA and DSIE programs
  - *Concerned about suppliers and willing to work with them*
  - *Have not yet seen threat to factory systems, but acknowledge the possibility*
  - *Need cost/risk tradeoffs to arrive at an affordable solution*
- Industrial Control Systems (ICS) may be soft targets. Culture differs from IT.
  - *Standards and guides* for ICS provide good risk management approaches. Implementation is spotty.*
- DoD has mandated protection of critical information
  - *Primes address in the program protection plan, but ICS security is not emphasized in DoD guidance*
- Defense R&D for cybersecurity is not currently focused on factory floor vulnerabilities and solution needs

*E.g. ANSI/ISA99 standards and NIST SP 800-82

9

Recent Trends

- **Threat Sophistication Increasing**
  - Cyber as an Instrument of State Power
  - Know-how adopted by cyber-criminals
- **Attack Surface Increasing**
  - IT and OT convergence, wireless connectivity
  - Internet of Things (est. 50B devices by 2020)
  - Additive Manufacturing, ease of counterfeiting

"In our tests, attackers got through organizations' cyber Maginot line at least 97 percent of the time." – *FireEye/Mandiant, 2014*

- **Mitigation Approaches -- Beyond Perimeter Defenses**
  - New network appliances for dynamic analysis
  - NIST Special Pubs updates (e.g. 800-53, 800-82)
  - NIST Framework for Improving Critical Infrastructure Cybersecurity
  - DFARS 252.204-7012, Safeguarding Unclassified Controlled Technical Information

10

Contrast in Risk Mitigation Approaches

Commercial	*Defense*
NIST -- Framework for Improving Critical Infrastructure Cybersecurity ▪ Risk management framework ▪ Best Practices ▪ Informative References* ▪ Voluntary compliance and tradeoff analysis * Multiple guides and resources (ISO, ISA, NIST, …)	DFARS – Safeguarding Unclassified Controlled Technical Information ▪ Minimum mandatary cybersecurity controls* ▪ Prompt incident reporting and damage assessment ▪ Mandatory flow down to lowest level of supply chain ▪ Contractual compliance *From NIST 800-53

11

NDIA White Paper Summary

Findings:

- The threat is real and manufacturing companies are targets
- Factory floor systems are a weak link in safeguarding tech info
- Smaller manufacturers are not well equipped to manage the risks

12

NDIA Recommendations for DoD
USD(AT&L)

1. Work with industry on risk-based, voluntary standards and practices for factory floor cybersecurity.
   - Evaluate NIST framework as starting point.
2. Conduct forums with industry to help understand and implement DFARS clause, including factory floor implications.
3. Update DoD guidance on the Program Protection Plan (PPP) to include protection in factory floor systems.
4. Use red teams to expose vulnerabilities and R&D to fill gaps
5. Assist SME suppliers with training and investments
   - NIST Manufacturing Extension Partnership to deliver training
   - Defense Prod Act Title III and Manufacturing Technology investments
   - Training for DoD contracting officers

13

Observations re: Additive Manufacturing

- **Growing Importance to National Defense**
  - Examples -- cooling ducts in the F-35, fuel nozzles for turbine engines.
  - Ability to produce small quantities efficiently (lot size of one) is particularly attractive for DoD small production runs and spares.
- **Therefore an Inviting Target**
  - The digital product/process file is valuable intellectual property – for espionage, counterfeiting, or tainting parts.
  - 2013 experiments by Virginia Tech – AM is a soft target. Easy to alter the the manufactured item in hard-to-detect ways.
- **Window of Opportunity for Improved Security**
  - *Inherently no more vulnerable* than other manufacturing methods
  - Now is the time to build more security into these emerging systems

14


Questions?
15

Panel*: Opportunities for Secure 3D Printing*

Robert Zollo (moderator)
President, Avante Technology

Dr. Claire Vishik
Trust and Security Technology and Policy Director, Intel Corporation

Andre Wegner
Founder and CEO, Authentize

Key Discussion Points:

- There are many opportunities for building security into the design of DDM machines abound.
- During its development, security wasn't high on the list of priorities for the ISO Additive Manufacturing File Format (AMF)[3], but it has "hints" of security – there is a space in the metadata where security could be inserted. In the future, it may be added in.
- The Cyber Physical Systems (CPS) Public Working Group (PWG) considers manufacturing devices like 3D printers as cyber physical systems. AM devices are similar in that they use the same protocols and firmware.
- There are privacy concerns when considering cybersecurity controls. For example, putting in automatic, machine-generated ID numbers for asset inventory or forensic purposes could lead back to a particular printer and a particular person.
- One of the biggest impacts of AM may be on the supply chain. Distributed manufacturing with localized production can dramatically reduce logistics costs. AM provides an opportunity to enhance the resilience and security of the supply chain in ways not available before.
- The biggest obstacles to cybersecurity in manufacturing include: awareness; the culture; uninformed decision makers; loss of process control; people and organizations not working together; not willing to invest in security.
- Attendees disagreed as to whether the economy would need to provide an incentive for organizations to include cybersecurity in their processes. Some attendees stated that customers desire more secure solutions to protect their intellectual property and systems. Other attendees disagreed but were uncertain whether the market could be incentivized to be proactive or if solutions would always be reactionary.
- Attendees and the panel stated that there were no on-going activities regarding security standardization. It was noted that standards reduce costs significantly in the semiconductor and other fields, but the standards processes around AM devices have just begun and attendees were unsure how security standards could be applied.

"Virtual Part" Perspective on Cyber-Security

Designing Security Components into 3D Printing Hardware, Software & Printed Objects

Robert Zollo
President
Avante Technology, LLC
Bellevue, WA USA
bobz@avante-technology.com

I. INTRODUCTION

The author will provide a "ground up" view of security issues from the printer hardware and related control software perspective, and introduce the concept of the "virtual part", a term for the software and meta data that define the item to be printed, and its revisions as it moves and evolves throughout it's life in the integrated supply chains of future factories.

He will provide insight on how to employ the new ISO/ASTM standard for 3D printing file descriptions to begin building security components within the file meta data and use it with security functionality that can be designed in to the printer firmware and control software. He will propose some simple steps to begin building a cyber-security capable environment on the shop floor and in the engineering lab.

II. THE "BRILLIANT FACTORY" CONCEPT

A brief overview of the integrated "brilliant factory" of the future as described by GE in their recent white paper on DDM. The concept of integrating thousands of intelligent machines located in multiple locations by people within and without the manufacturing organization in a "completely transparent supply chain" is introduced. Security issues relating to the "virtual part" as it moves through the supply chain to the factory floor and back for revisions are highlighted.

III. THE "STATE OF THE PRACTICE"

A brief overview of some typical 3D printers will be offered to highlight areas of potential breach of security in the firmware, controlling software and the file description software. Opportunities for introducing simple security measures are identified.

IV. LEVERAGING ISO STANDARDS

An overview of two ISO standards relating to the definition, transfer and use of 3D files is provided. Ideas on how these standards may be used to begin building some security mechanisms into the "virtual part" package as it moves through the design and supply chain.

V. INTEGRATING SMALL SHOPS FOR SECURITY

Suggestions are made on how to implement a simple, scalable, integrated security mechanism using components embedded in the printer firmware, control software, file management software, and file description software that is applicable to small to small manufacturing shops as well as enterprise scale brilliant factories.

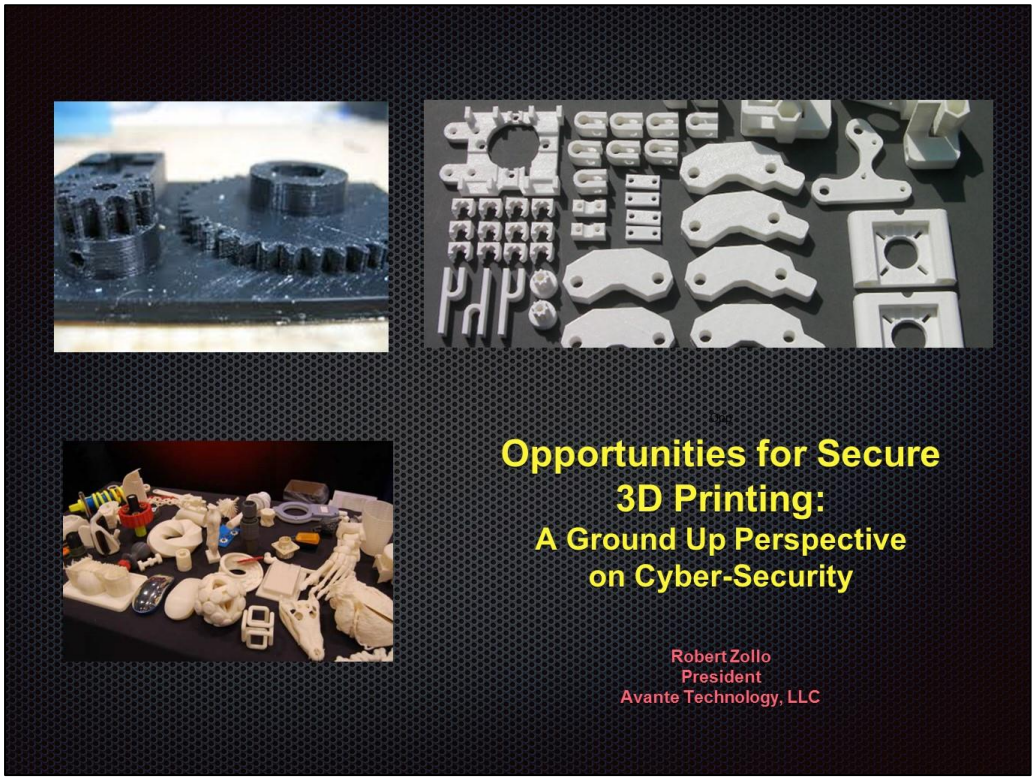
VI. INVITATION TO DIALOG

Panelists will be invited to comment on how the suggested
security mechanisms might fit within a larger scale security architecture in enterprise factories.

REFERENCES

1. *M. Annunziata and S. Biller, "The Future of Work", General Electric white paper; 2014.*
2. *ISO/ASTM 52915 standard framework for an interchange format to address current and future needs of additive manufacturing; 2013*
3. *ISO IS14306 standard for viewing and sharing lightweight 3D product information: 2012.*

Presentation by Robert Zollo:



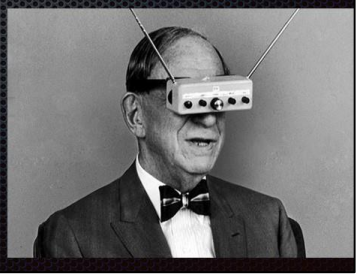
What We Do

- Design 3D Printing Systems
- Develop STL/AMF File Repair & Validation Software
- Develop Proprietary Materials for FDM Printing
- Install Custom Printing Solutions
- Technical Consulting

Avante
Advanced 3D Printing

A Slightly Different Perspective on Cyber-Security

- Ground Up View from the Shop Floor
- Start with most basic 3D Printing Machine
- Identify Simple Practical Approach
- Utilize Basic Security Building Blocks



Brilliant Factories of the Future Are *Here & Now*

A New Kind of Industrial Company…

GE Eyes Growth by Linking:

- **Machines**
- **People**
- **Data**

GE's Concept

The idea behind the Brilliant Factory:

Link design, engineering, manufacturing, supply chain, distribution & services into one intelligent system.

Eating the Proverbial Elephant

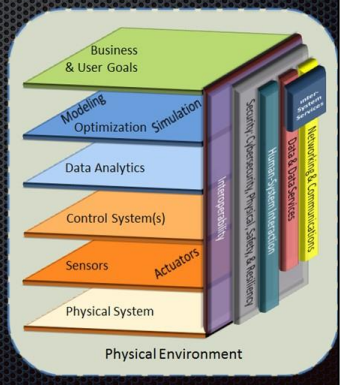
How Do You Secure a Massive, Dynamic Matrix of this nature?

Or even a small one?

Break Down this Enormous Challenge into Small, "digestible bites" of Security Components

Security Starts in the Physical System:

- **Printer Hardware**
- **System Firmware**
- **Control Software**



Security Starts in the Physical System:

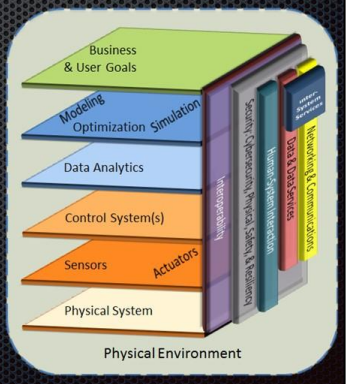
From Engineering Desktop

to Factory Floor….

Security in the Printing System Hardware

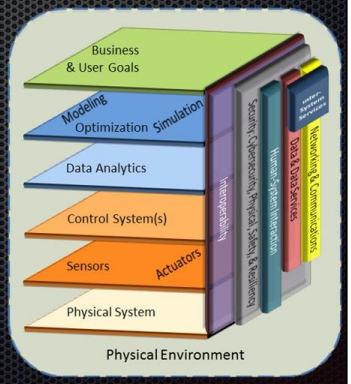
Physical Locks:

- **access to control panel**
- **access to memory**
- **access to ports**
  - **USB**
  - **Flash Cards**



Security in the Printing System Firmware

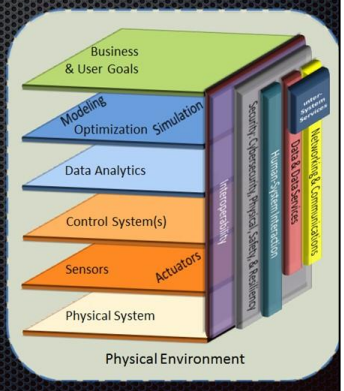
- Embedded ID Number
- Access Manager
- File ID Token Authenticator
- Serial Number Generator
- Part ID Token Generator
- Activity Log Manager



Security in the Printing Control Software

Incoming 3D file Package (JT ISO format*)

- authenticate (match file ID tokens)
- prepare for printing
- watermark the print
- control the printing process
- log each print
- Report print job log(with tokens)
- Retain separate log in print system firmware



Making Files Printable

File Prep:

1. Analyse File & Make Manifold
2. Input, Slice & Position
3. Convert to Machine Language

Opportunity For Adding Unique Info

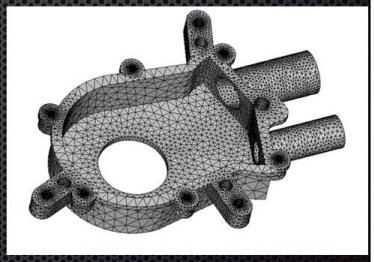
File Description Languages for 3D Printing

STL Files: Traditional "format"

to be replaced by:

AMF: ISO ISO/ASTM 52915

Standard specification for additive manufacturing file format (AMF)

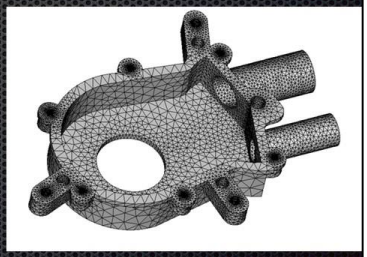


AMF: ISO ISO/ASTM 52915

Option for adding watermarks

No Current Security Specified

Potential for future Security Specification

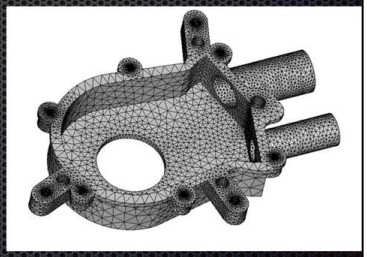


AMF: ISO ISO/ASTM 52915

Potential for future Security Specification:

The <metadata> element
Annex A1

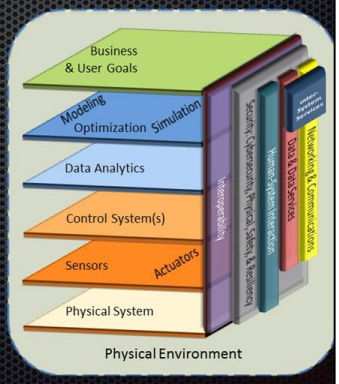
Allow for inclusion of copyright and other types of metadata



Integrate With Current Factory Methods & File Formats

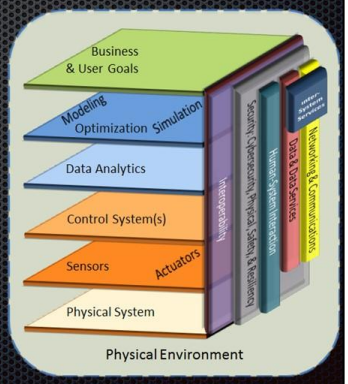
JT Open Format (ISO ISO 14306)

1. 3D file package
2. carry security tokens
3. transmit across network
4. deliver to printing system



A Simple, Cost Effective, Scalable Approach

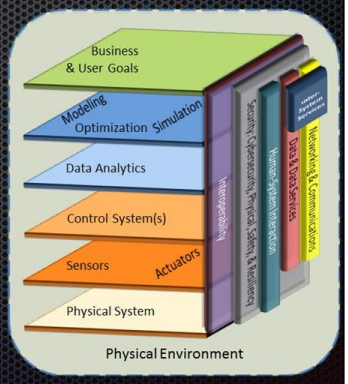
1. Utilize JT ISO & AMF ISO File Formats
2. Integate with Printer Mgt. Software
3. Provide A Token Based Automatic Authentication Process
   - Secure Embedded Authentication in Firmware
   - Secure Embedded Token Assignment in Firmware
4. Implement a Redundant Print Job Log System
   - stored in printer memory (locked)
   - publish to authorized recipients on network (JT)



A Simple, Cost Effective, Scalable Approach

Printer Management Software:

- Compare tokens in firmware with Incoming File
- Convert JT to AMF ISO format
- Prepare print job for printing
  - Generate unique part ID from printer firmware
  - create unique watermark for each part
  - slice and generate G code
- Save the print job info to Print Log



The Print Job Log

Includes:

- print job number
- prints by serial number
- Prints by ID token
- printer location & ID
- date/time of job
- additional data (optional)

A Simple, Cost Effective, Scalable Approach

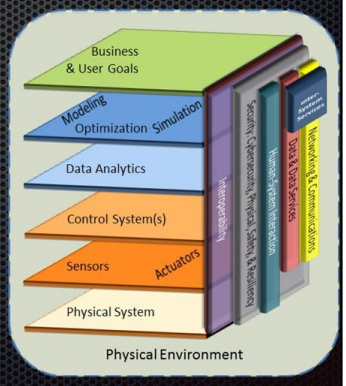
Redundant, Secure Records

- Save the print job info to Print Log
- Generate unique ID token for the Print log
- Convert to JT format file
- Distribute the print job log info
  - to printer memory (protected)
  - to requesting parties on the network

Leveraging Manufacturing Systems

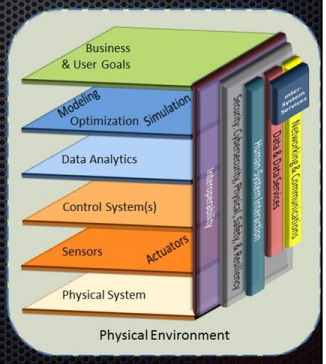
Systems for:

- **Revision Control**
- **Quality Control**
- **Customer Matching**
- **Product Tracking**
- **Quality Assurance**



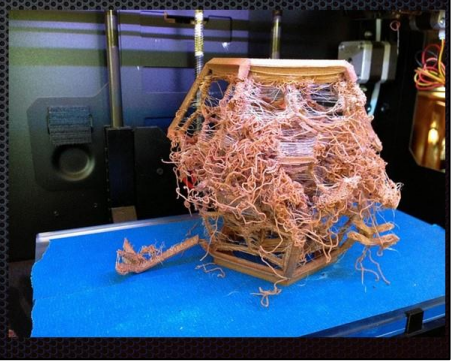
Materials Can Also Contain Security Components

- Chemical Tagging
- Physical Tagging
- Physical Watermarking



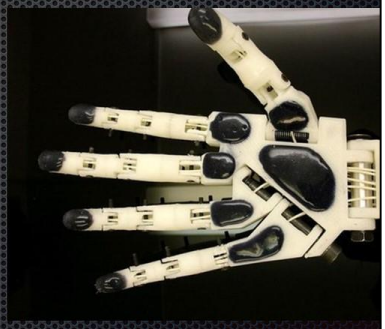
Making Printable Parts

Quality without Security =



Key Points

1. *Security Starts at the Printer*
2. *Leverage ISO Standards*
3. *Plan for Desktop to Large Printers*
4. *Security Does NOT have to be Expensive*
5. *Start NOW!*



Thank You!

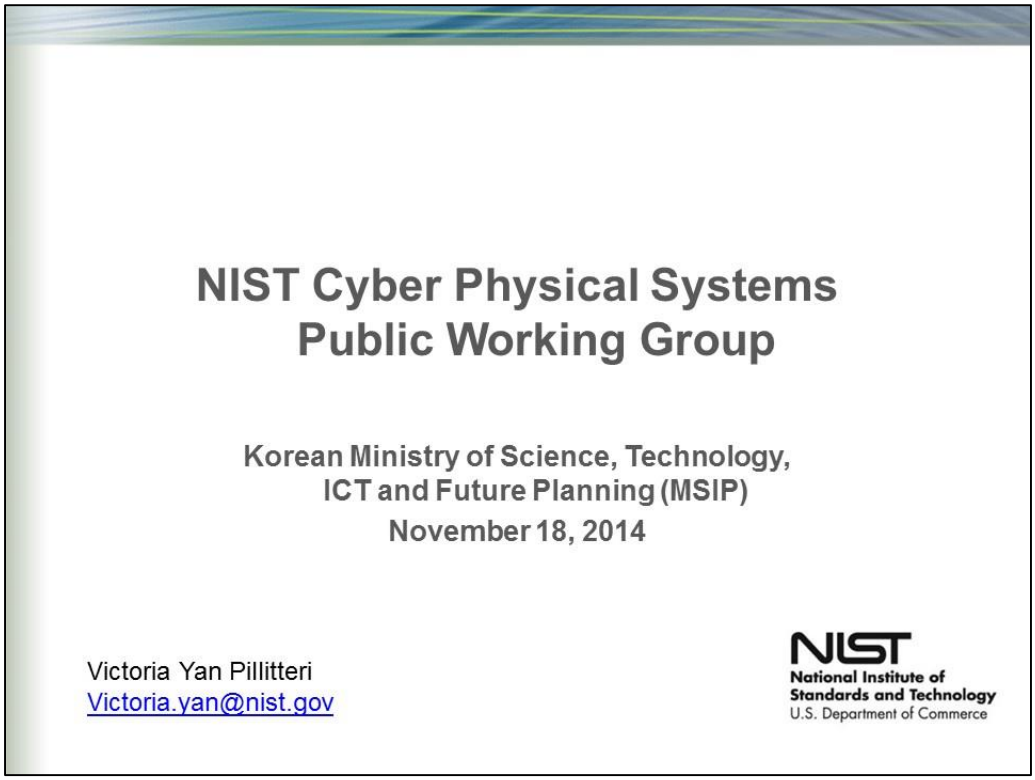
For More Information:

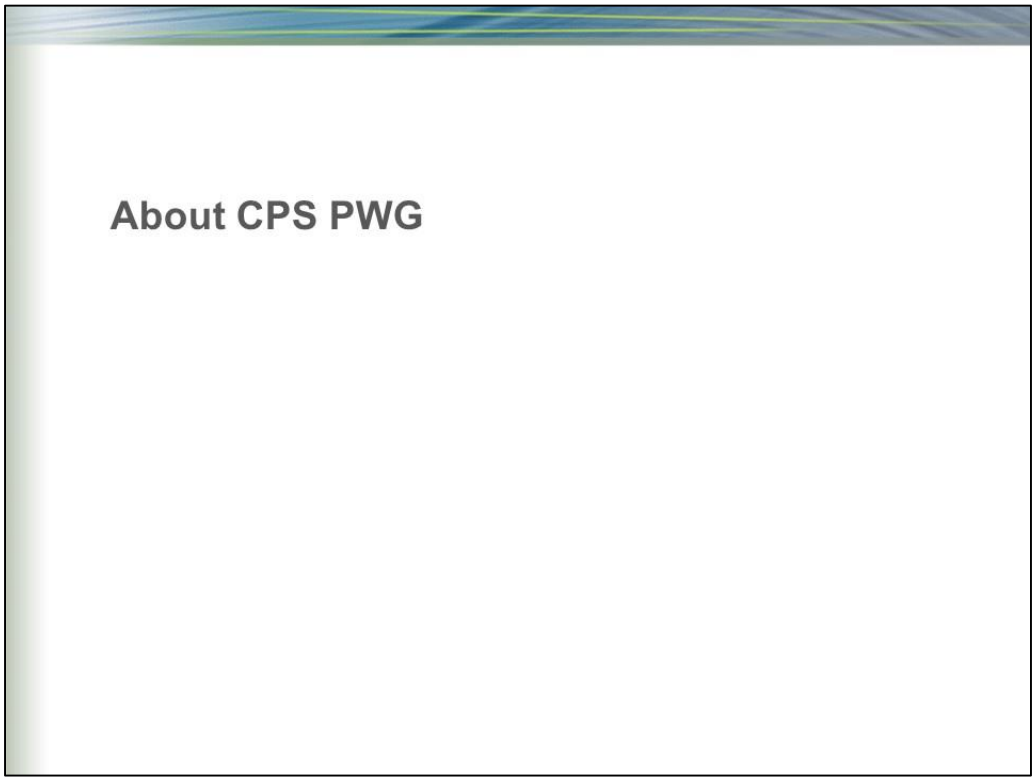
bob.zollo@gmail.com

Avante Technology, LLC.

Avante
Advanced 3D Printing

Presentation by Claire Vishik:





What are Cyber-Physical Systems (CPS)?

- Is a CPS any engineered system with a microprocessor?

- Do all CPS need to be connected to the internet?

- Are there a set of basic functions and architectural elements common to all CPS?

3

CPS – Notional Definition

- Integrated, hybrid networks of cyber and engineered physical elements
- Co-designed and co-engineered to create adaptive and predictive systems
- Respond in real time to enhance performance*

* Key metrics include: efficiency and sustainability, agility and flexibility, reliability and resilience, safety and security

Why is NIST convening the Public Working Group (PWG)?

- Accelerate progressing CPS across all sectors and domains.
- Currently lack a unified technical foundation for broad collaboration.

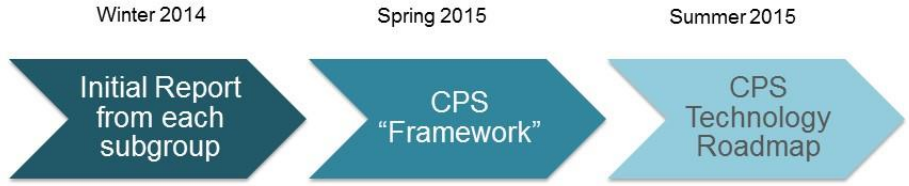
CPS PWG

Definition, Vocabulary, Reference Architecture	Use Cases	Cybersecurity & Privacy	Timing & Synchronization	Data Interoperability

Co-leads and Participation from Industry, Academia, Government

5

CPS PWG Goal and Deliverables



- Definition, Vocabulary, Reference Architecture
- Use Cases
- Cybersecurity & Privacy
- Timing & Synchronization
- Data Interoperability

- Integrate subgroup reports
- Publish as white paper on www.cpspwg.org

- Identify opportunities for a coordinated effort on key technical challenges from each subgroup area and across CPS

6

CPS Cybersecurity and Privacy Subgroup

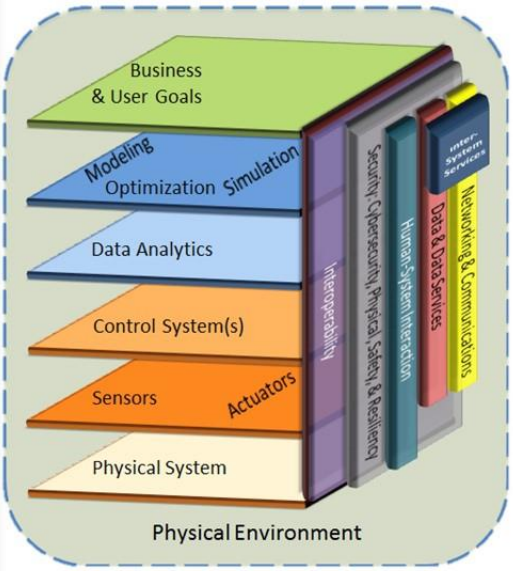
Goal/Objectives:

- Identify the unique challenges, properties and opportunities for CPS
- Develop appropriate cybersecurity objectives (e.g., confidentiality, integrity, and availability) for CPS
- Contribute to the overall reference architecture for CPS to ensure that cybersecurity is included and addressed
- Identify security and privacy requirements for the components of the reference architecture.

7

Defining Risk Management Approach for CPS

Notional Draft NIST CPS Reference Architecture

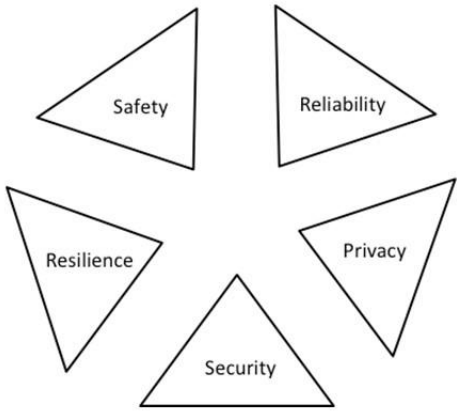


- Functional, multi-stack architecture
- All layers should be co-designed in the context of the Physical Environment
- Management function, not depicted, provides oversight and ensures coordination and composability

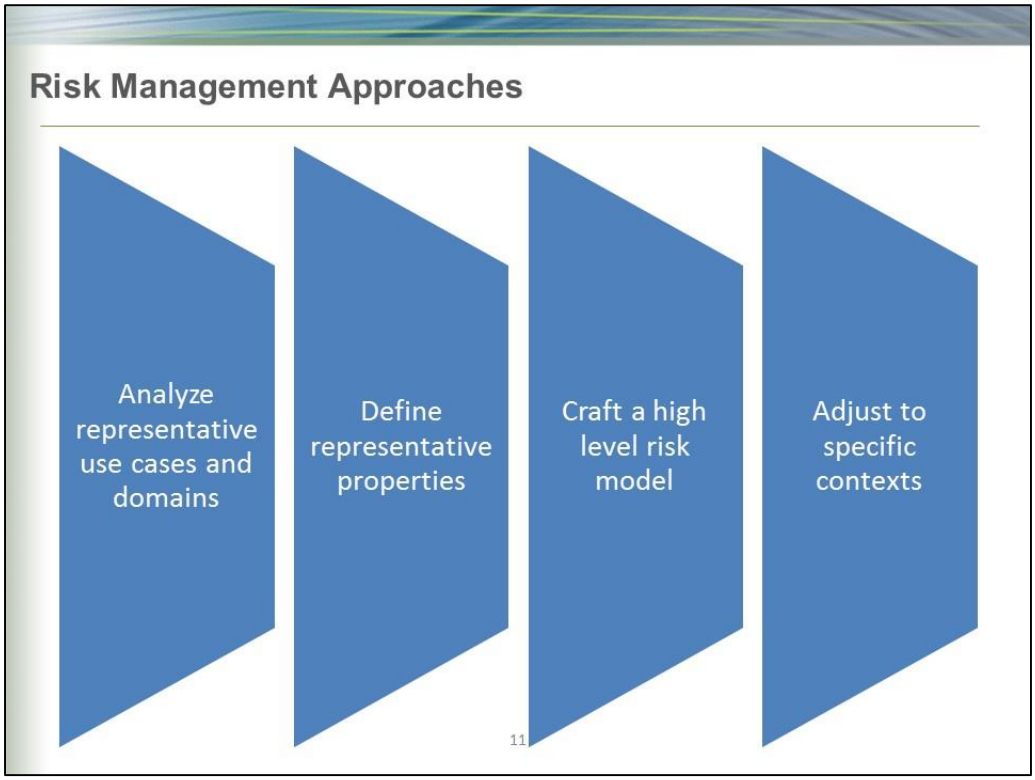
9

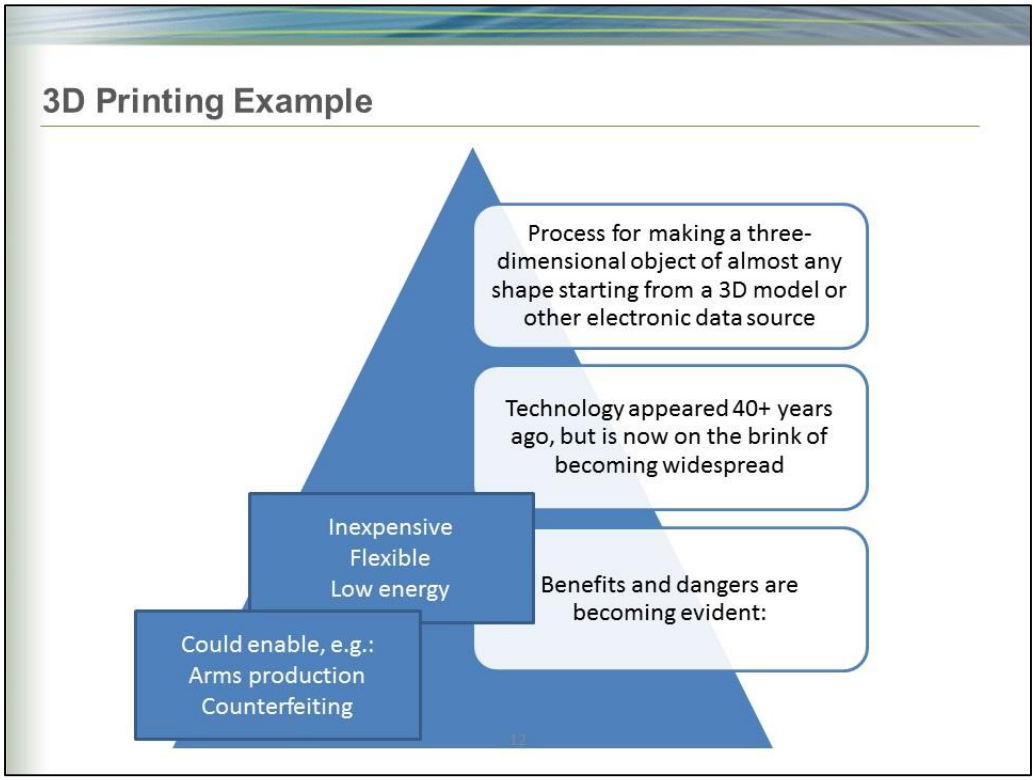
Some Properties of CPS: very early work

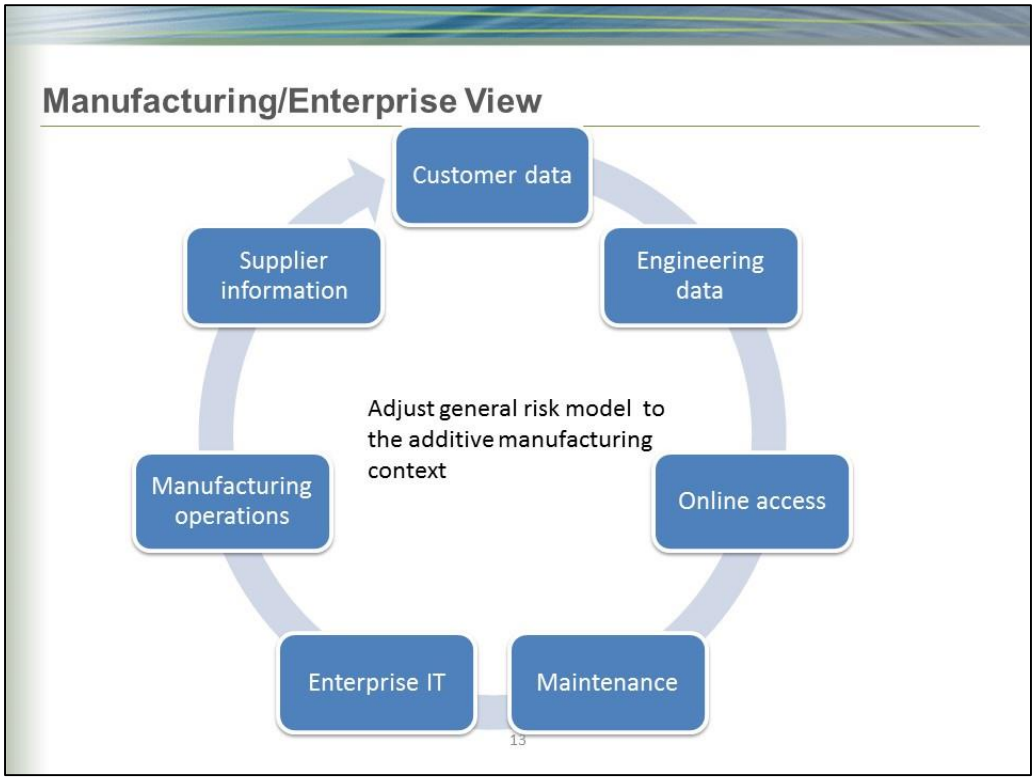
- Need for resilience, reliability, and safety in addition to security & privacy
- Wide range of operational contexts
- Lifecycle challenges, including differing lifespans
- "Systems of systems" resulting in inherent complexity
- Impact on physical world
- Time sensitive
- Resource constrained elements
- "Always on" requirements

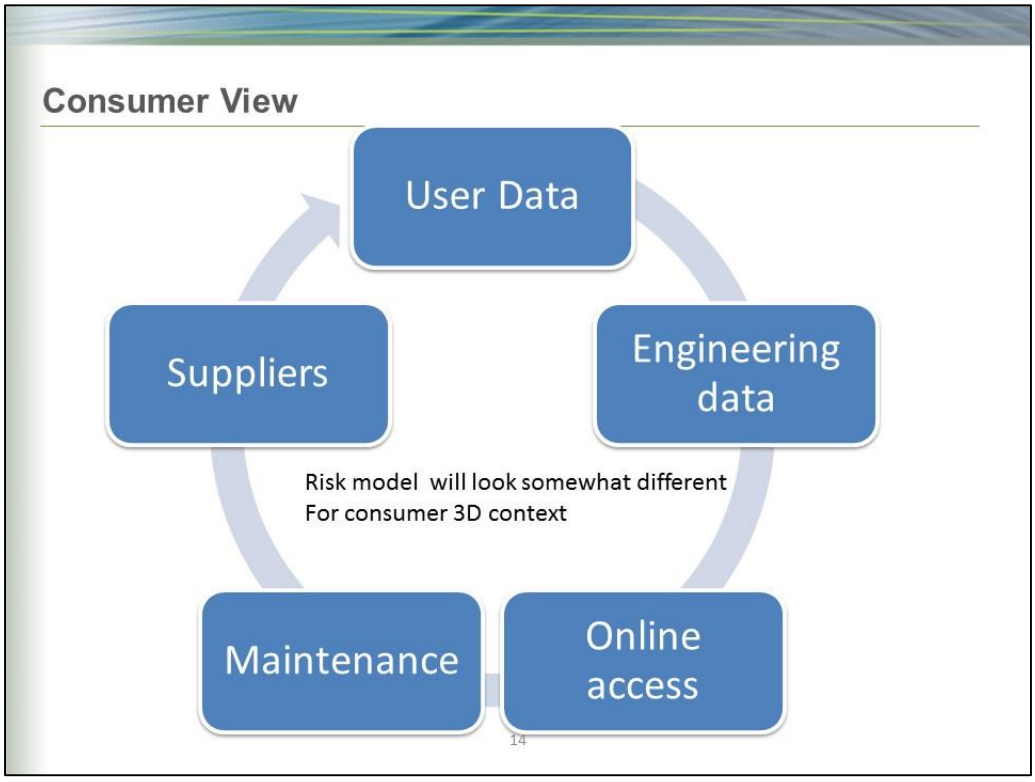


10


Risk Management Approaches
Analyze representative use cases and domains
Define representative properties
Craft a high level risk model
Adjust to specific contexts
11


3D Printing Example
Process for making a three-dimensional object of almost any shape starting from a 3D model or other electronic data source
Technology appeared 40+ years ago, but is now on the brink of becoming widespread
Benefits and dangers are becoming evident:
Inexpensive
Flexible
Low energy
Could enable, e.g.:
Arms production
Counterfeiting


Manufacturing/Enterprise View
Customer data
Engineering data
Online access
Maintenance
Enterprise IT
Manufacturing operations
Supplier information
Adjust general risk model to the additive manufacturing context
13


Consumer View
User Data
Engineering data
Online access
Maintenance
Suppliers
Risk model will look somewhat different
For consumer 3D context
14

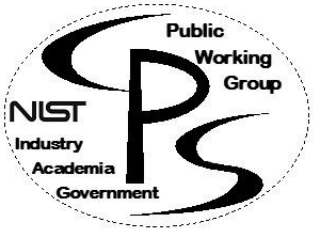
Thank you!

Questions?

15

For more information on CPS

www.nist.gov/cps



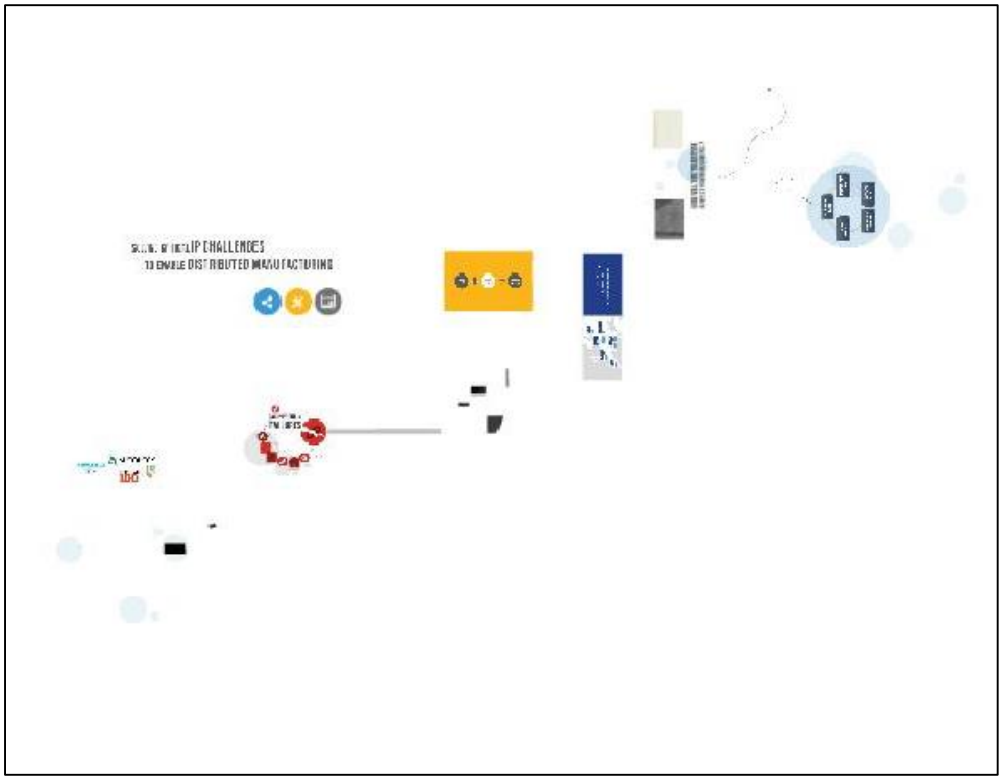
www.cpspwg.org

Smart Grid and Cyber-Physical Systems Program Office: nistcps@nist.gov

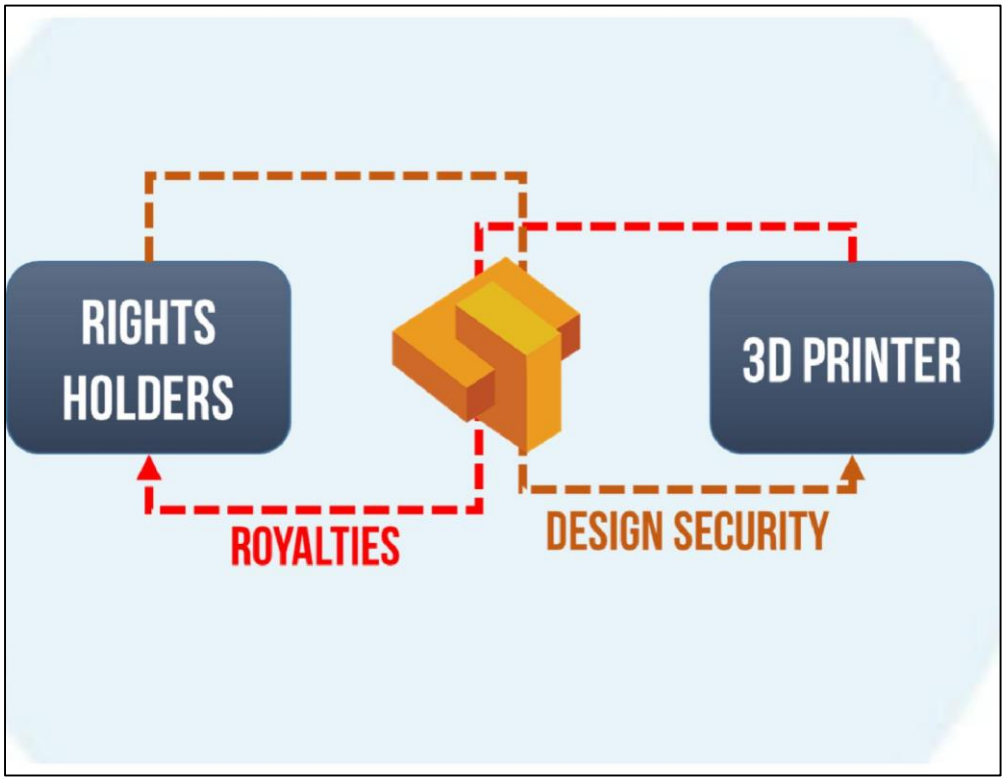
Definition, Vocabulary & Ref. Architecture	Use Cases	Cybersecurity & Privacy	Timing & Synchronization	Data Interoperability
Abdella Battou abdella.battou@nist.gov	Eric Simmon eric.simmon@nist.gov	Vicky Pillitteri victoria.pillitteri@nist.gov	Marc Weiss marc.weiss@nist.gov	Martin Burns maritn.burns@nist.gov

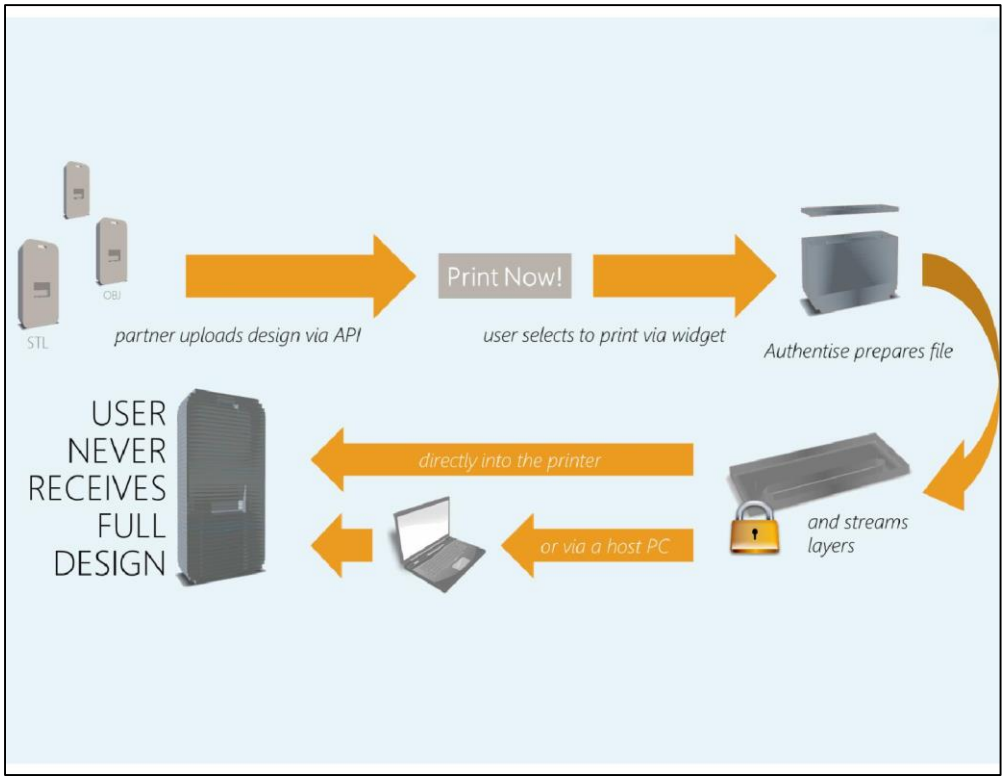
16

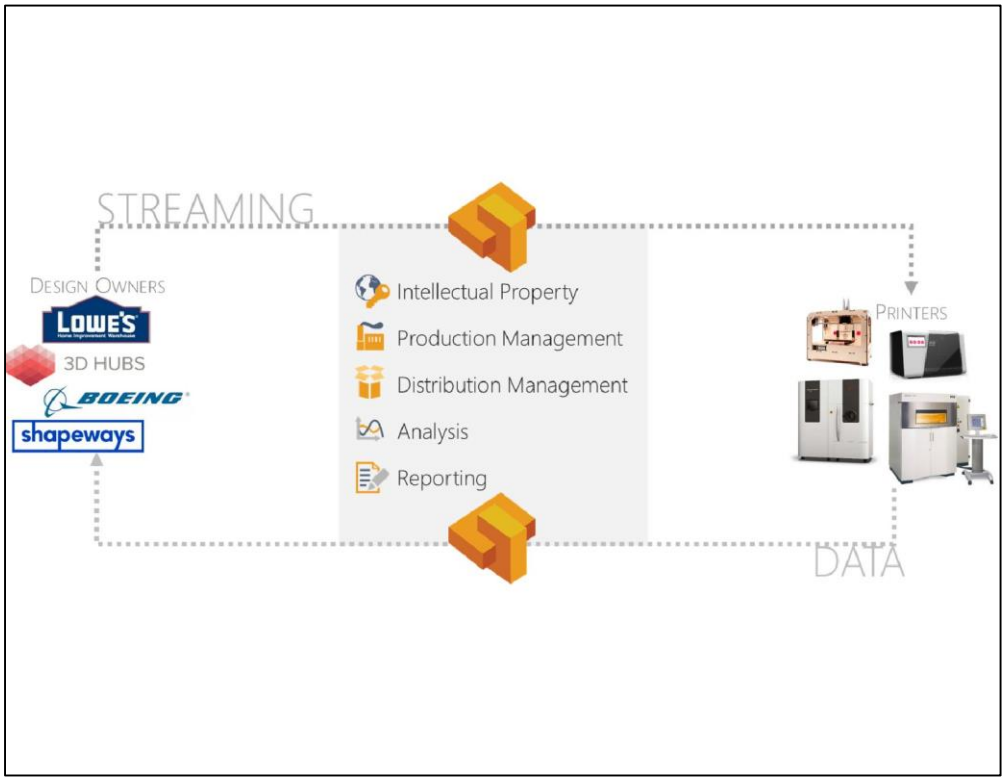
Presentation by Andre Wegner:



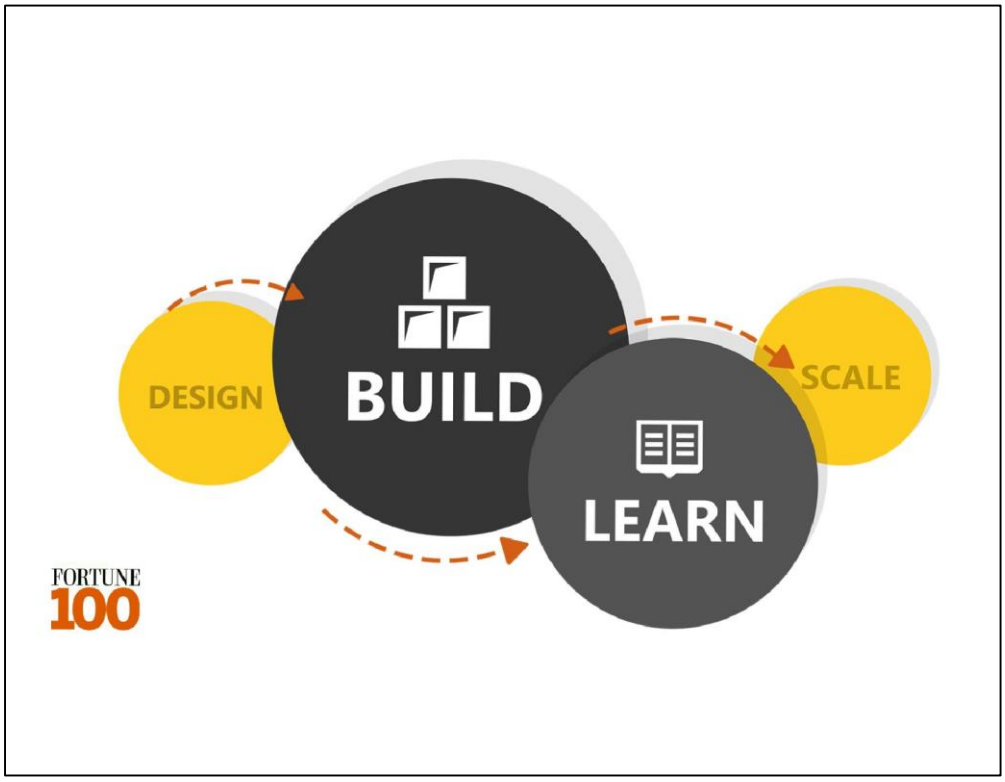

@AUTHENTISE // @APWEG
KWAMB.IO
pinshape
cgtrader
AUTODESK.
FORTUNE
100


RIGHTS
HOLDERS
3D PRINTER
ROYALTIES
DESIGN SECURITY


STL
OBJ
partner uploads design via API
Print Now!
user selects to print via widget
Authentise prepares file
USER NEVER RECEIVES FULL DESIGN
directly into the printer
or via a host PC
and streams layers

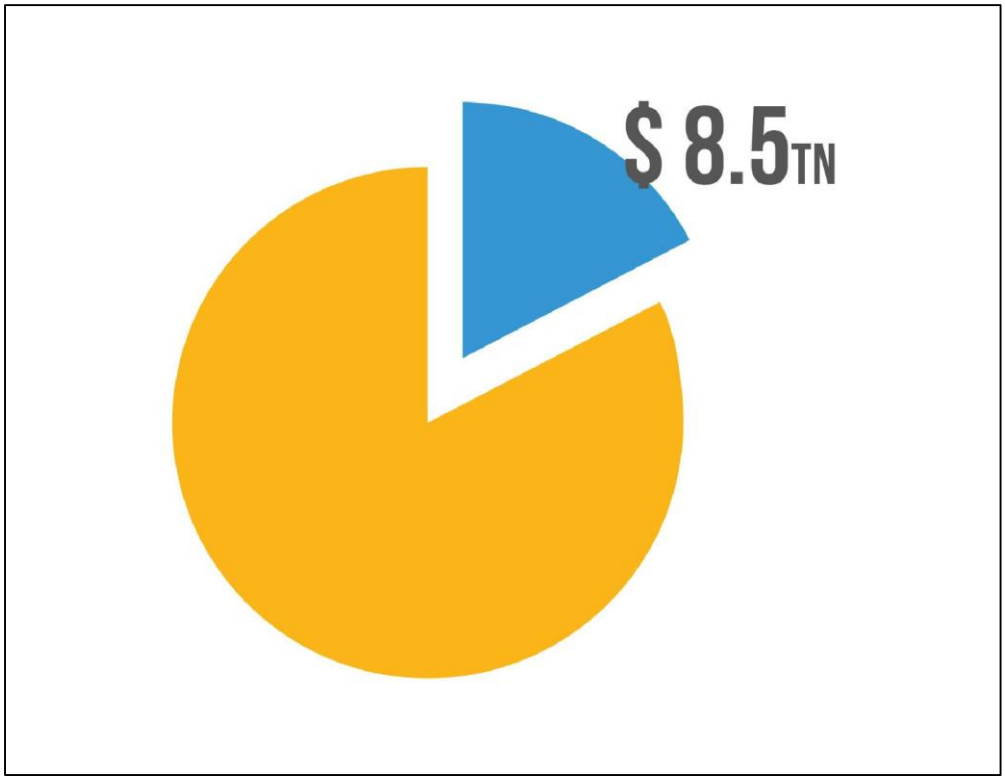

STREAMING
DESIGN OWNERS
LOWE'S
3D HUBS
BOEING
shapeways
Intellectual Property
Production Management
Distribution Management
Analysis
Reporting
PRINTERS
DATA


AUTHENTISE
COMPUTER VISION

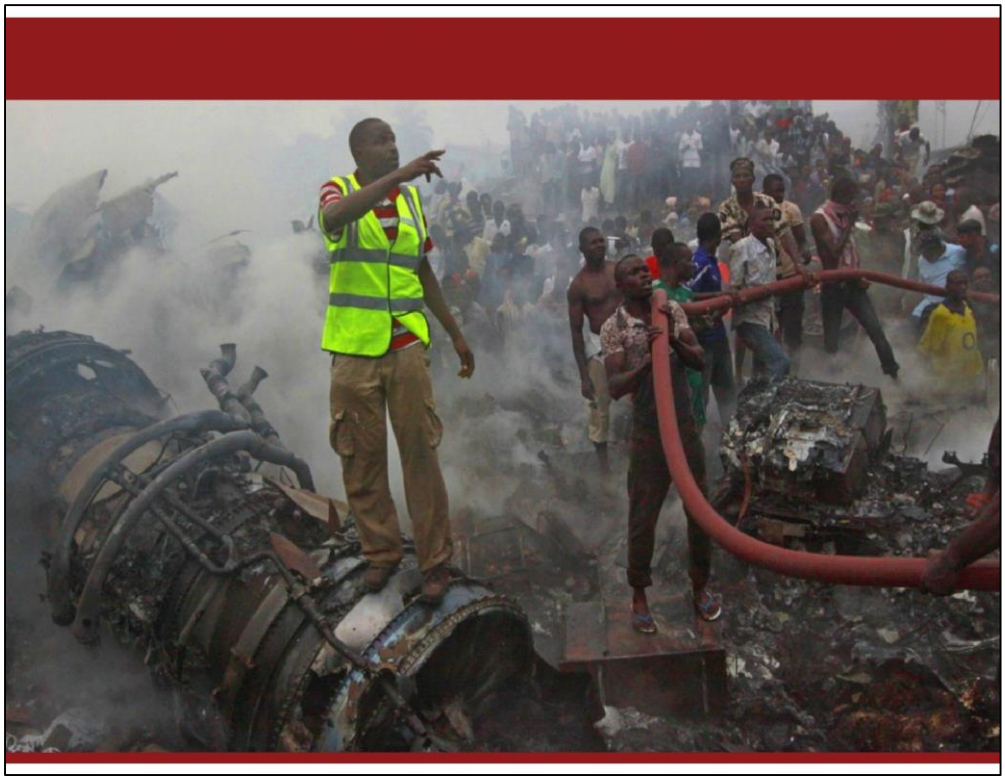

DESIGN
BUILD
LEARN
SCALE
FORTUNE
100

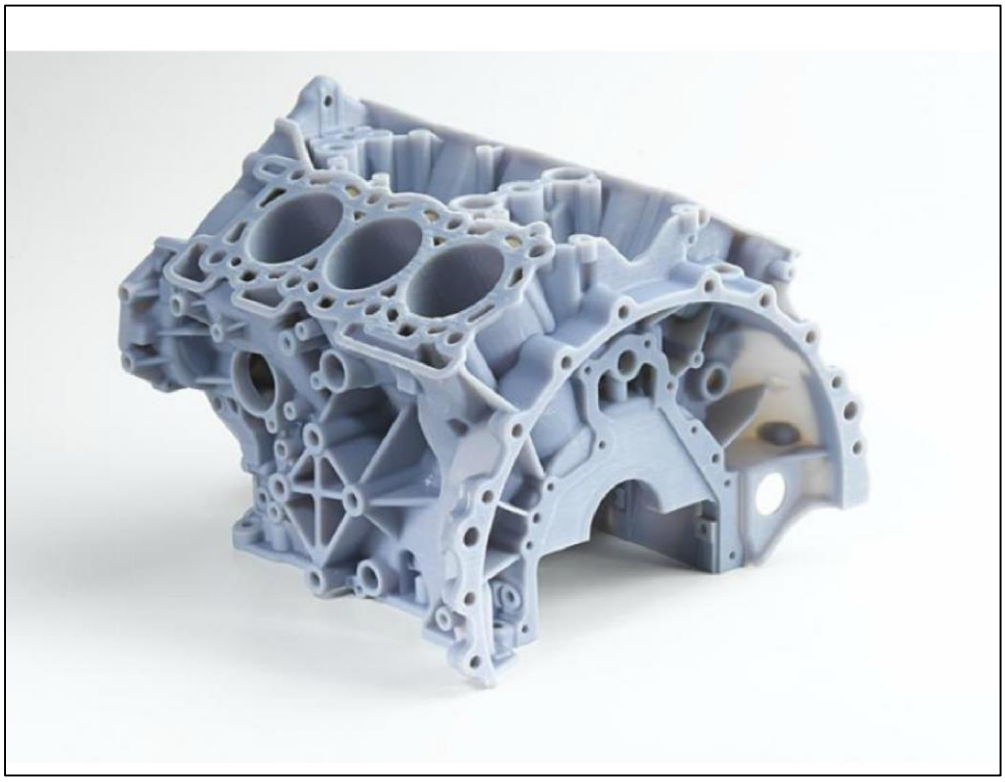

SUPPLY CHAIN
FAILURES
Lead Times
High Costs
Authenticity
FAKE
Standardization
Storage Needs
Availability


Lead Times
High Costs
Authenticity
FAKE
Standardization
Storage Needs
Availability

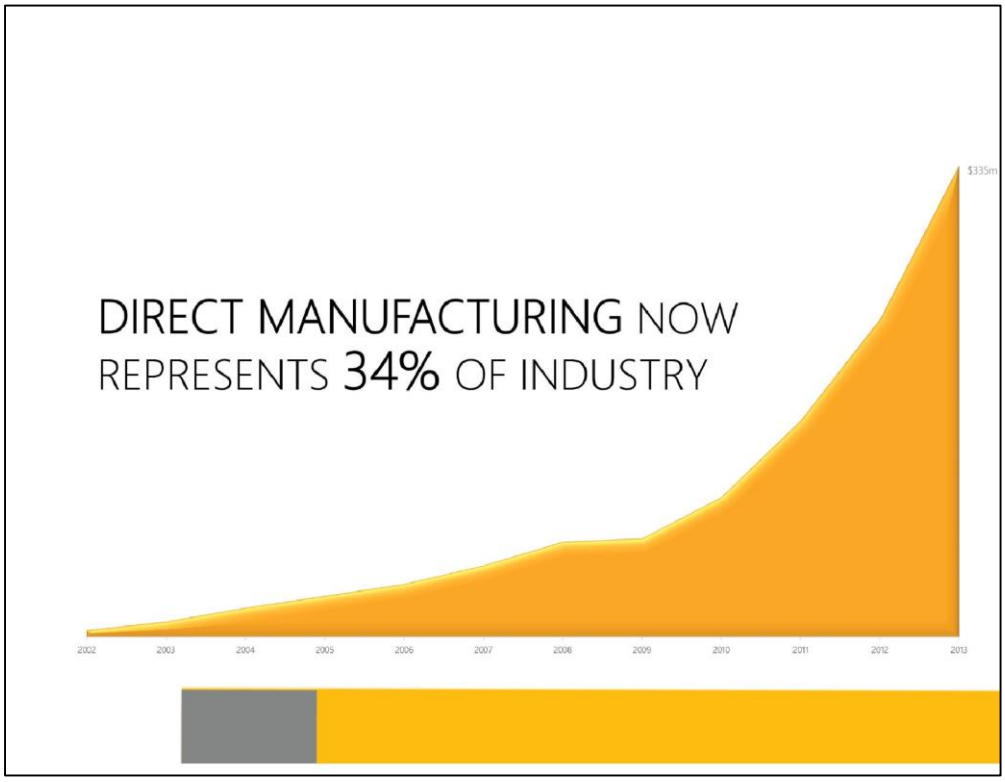

$ 8.5TN

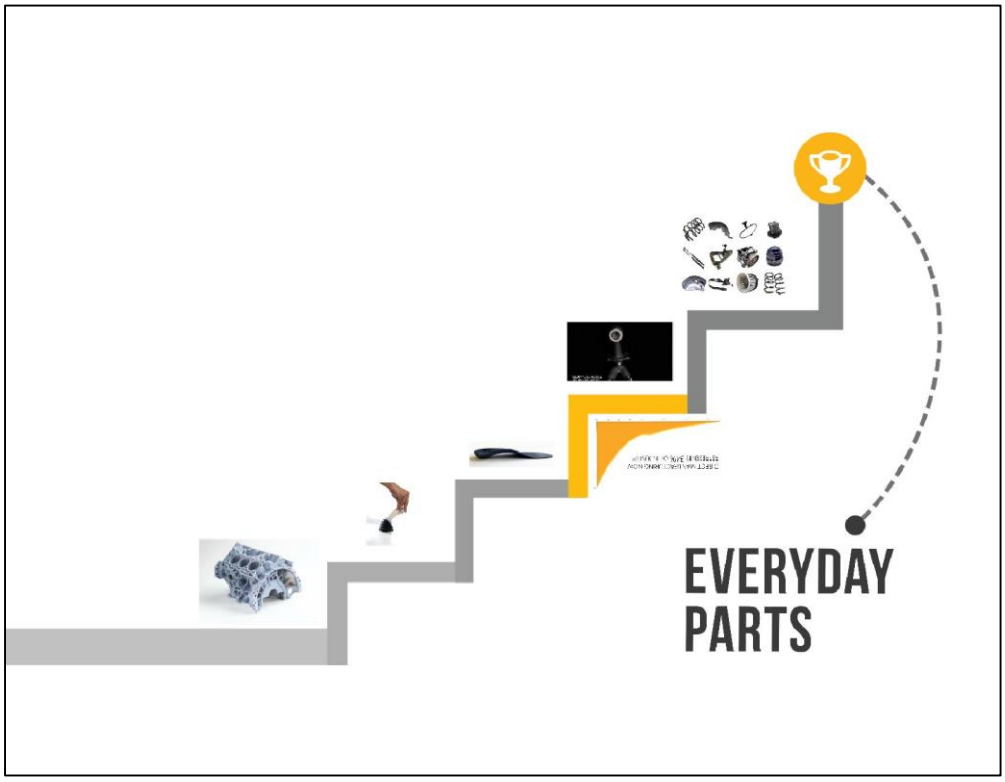

UNITED STATES

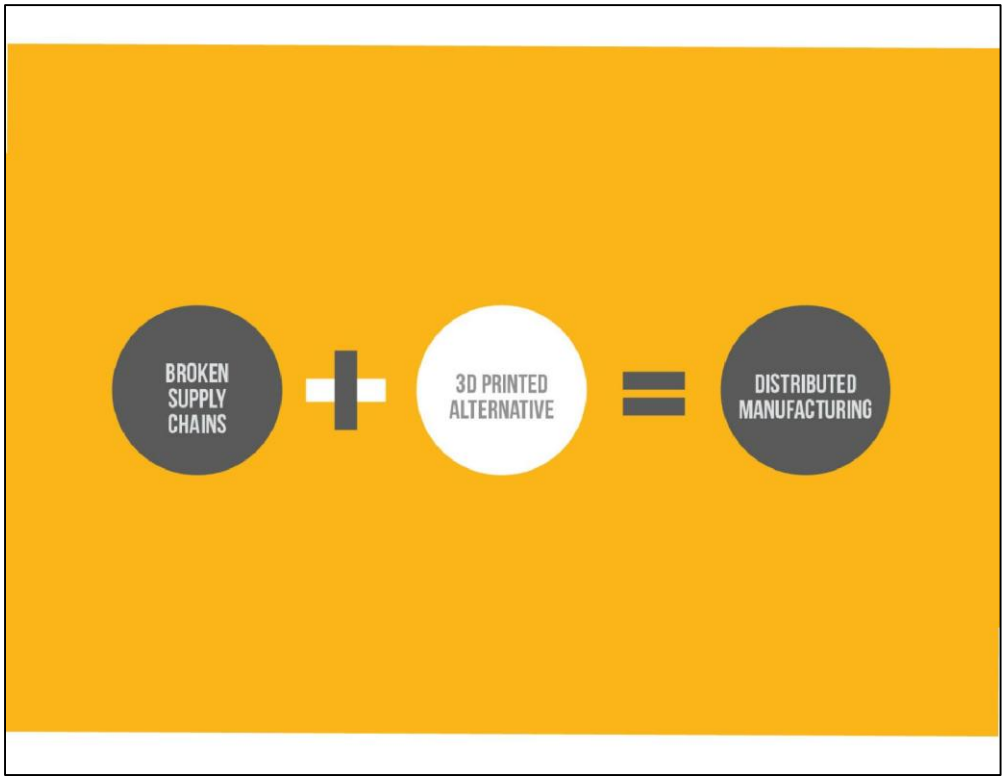


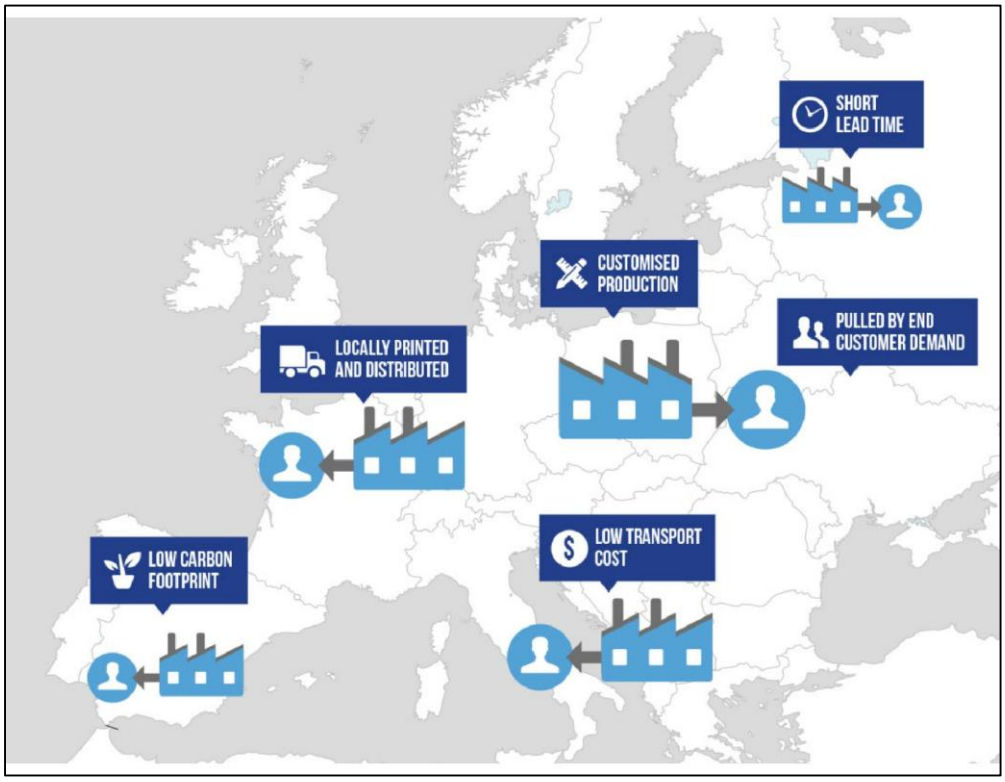



LEAP FUEL NOZZLE
ADDITIVELY MANUFACTURED


DIRECT MANUFACTURING NOW
REPRESENTS 34% OF INDUSTRY
$335m
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013


EVERYDAY
PARTS

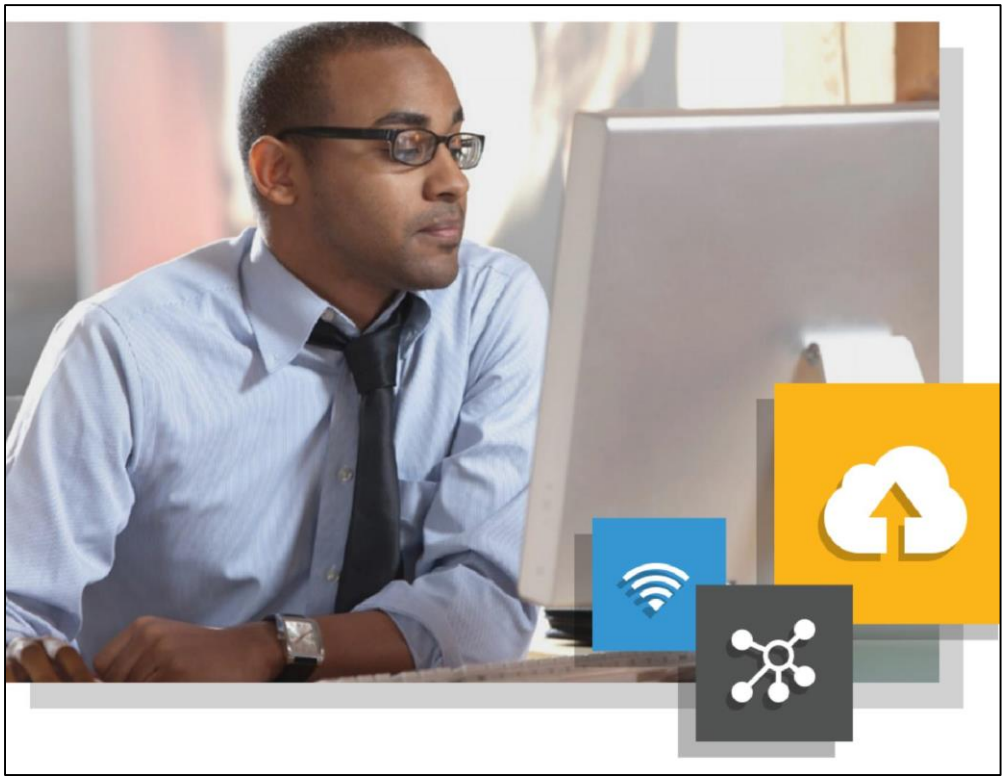

BROKEN SUPPLY CHAINS
3D PRINTED ALTERNATIVE
DISTRIBUTED MANUFACTURING

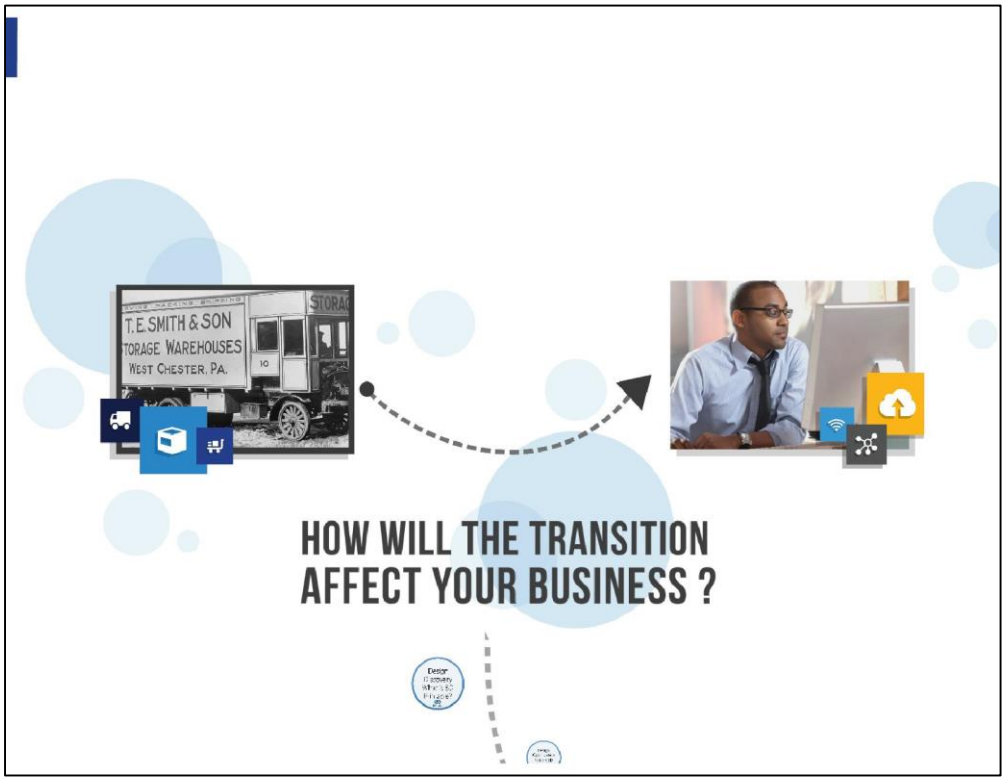

SHORT LEAD TIME
CUSTOMISED PRODUCTION
PULLED BY END CUSTOMER DEMAND
LOCALLY PRINTED AND DISTRIBUTED
LOW TRANSPORT COST
LOW CARBON FOOTPRINT

-3D Printing anchor technology

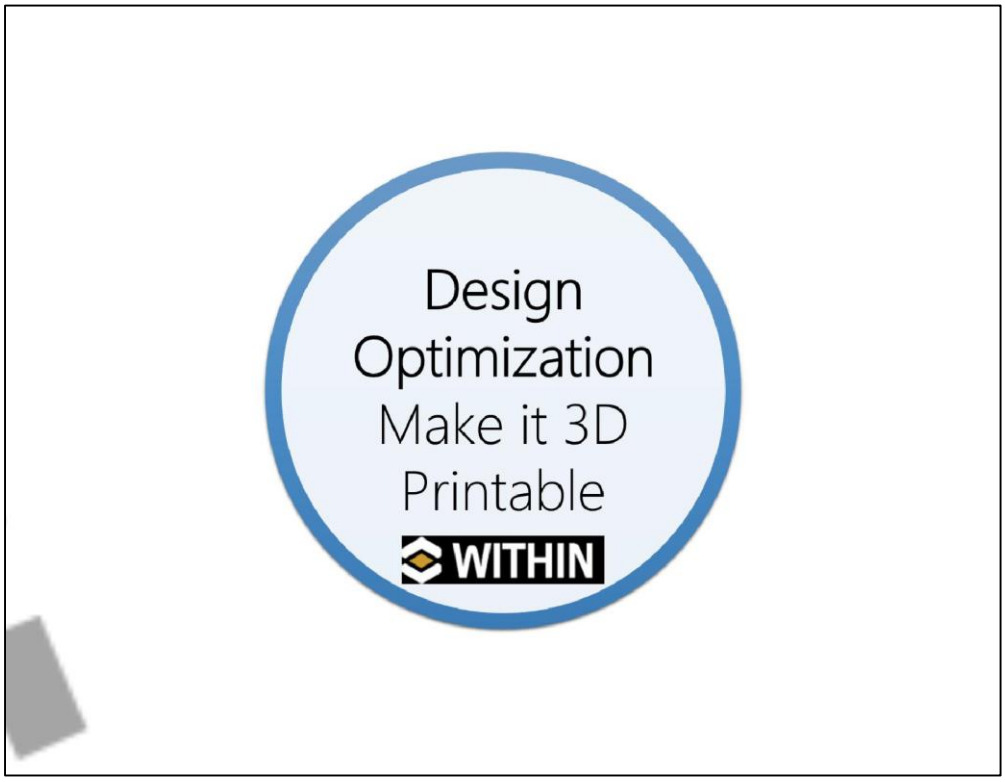
-Digital designs as currency

-Production near point of use



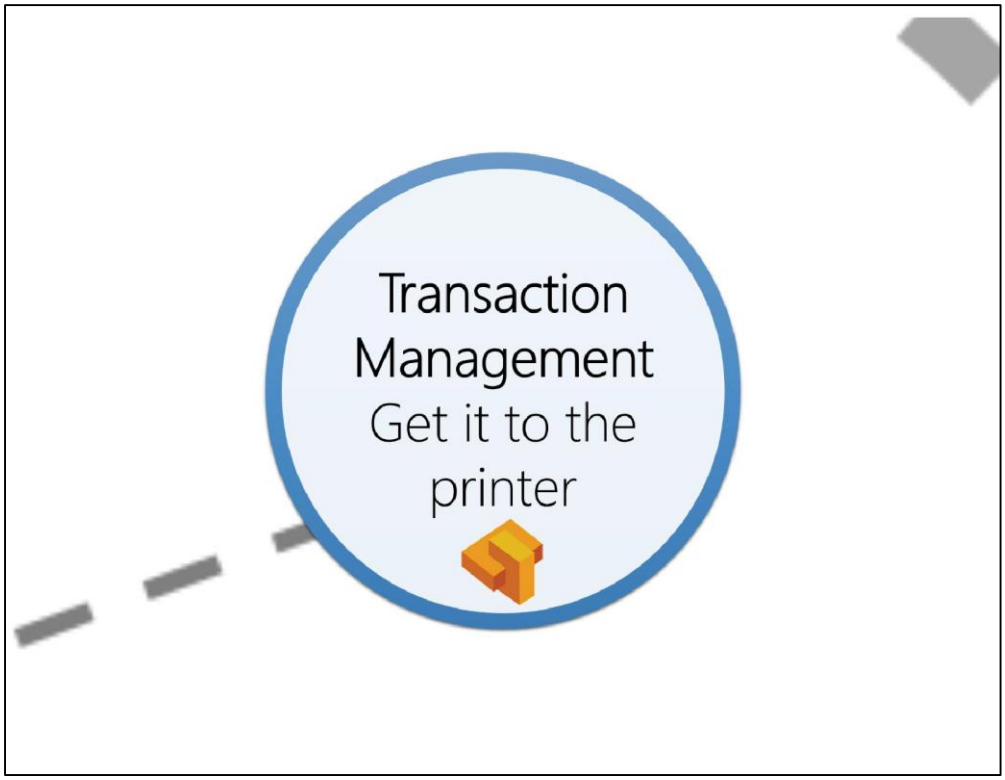

T. E. SMITH & SON
TORAGE WAREHOUSES
WEST CHESTER, PA.
HOW WILL THE TRANSITION
AFFECT YOUR BUSINESS ?


Design
Discovery
What is 3D
Printable?
SENVOL

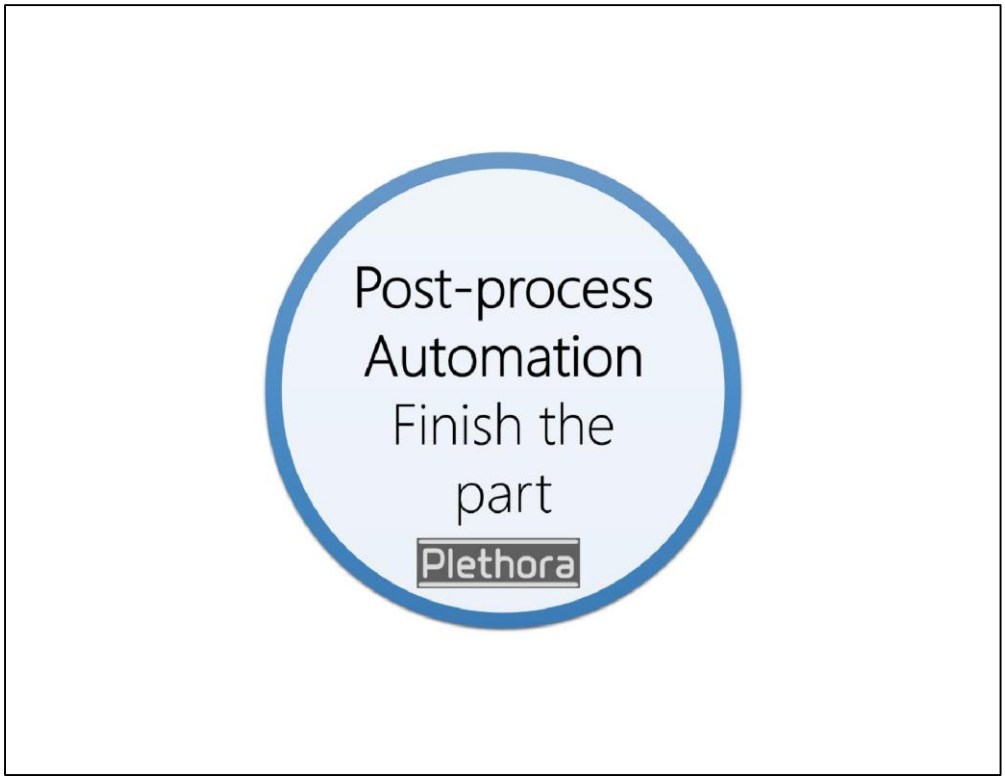

Design
Optimization
Make it 3D
Printable
WITHIN


Design
Certification
Can it Fly?
Lawrence Livermore
National Laboratory


Object
Purchase
Buying the
file


Transaction
Management
Get it to the
printer

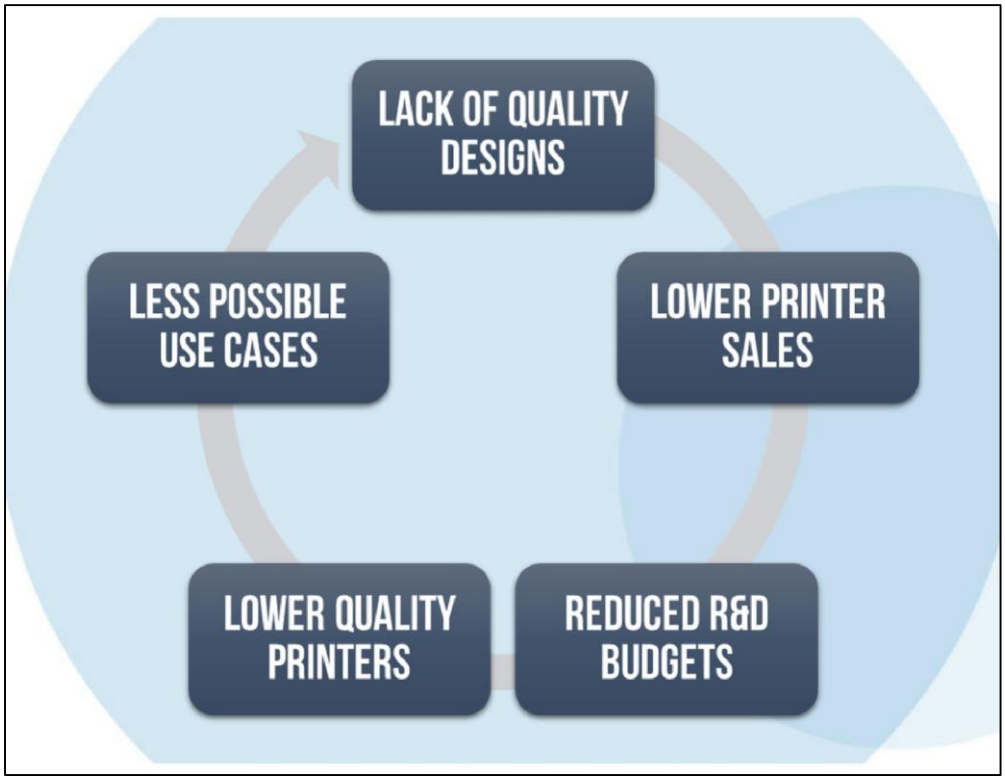

Local
Production
Making the
object
ups

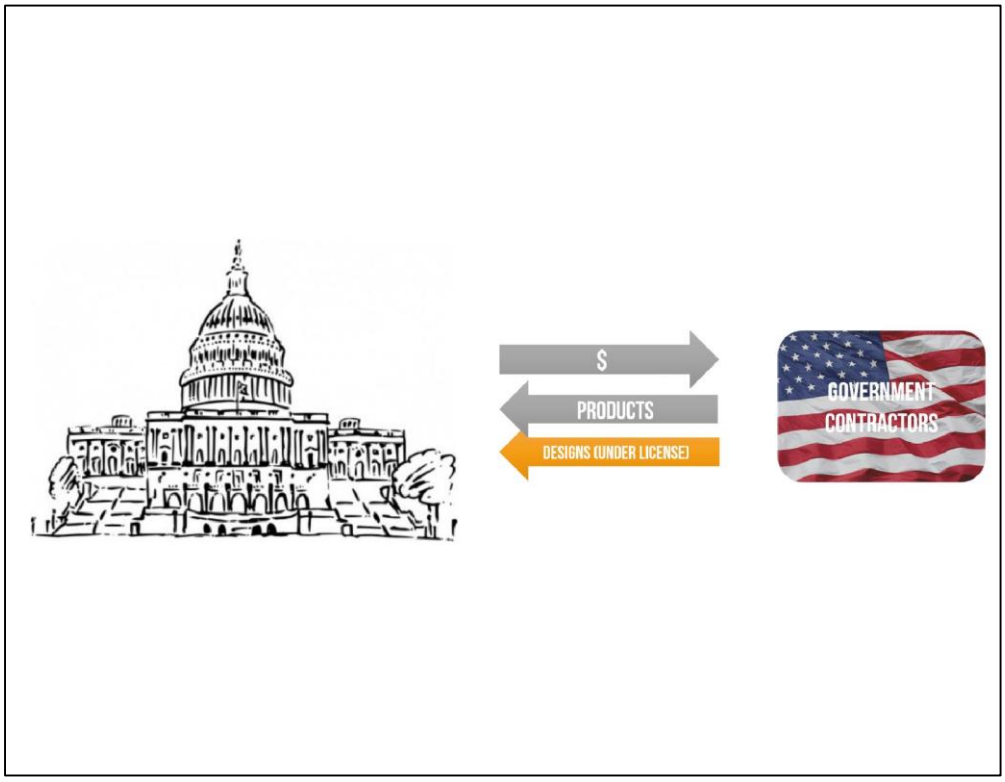

Post-process
Automation
Finish the
part
Plethora


Process
Monitoring
Is it printing
right?


FAIRPHONE
3D HUBS


AFFECT YOUR BUSINESS ?
Design Discovery
Design Certification
Local Production Making the object


LACK OF QUALITY DESIGNS
LOWER PRINTER SALES
REDUCED R&D BUDGETS
LOWER QUALITY PRINTERS
LESS POSSIBLE USE CASES


$
PRODUCTS
DESIGNS (UNDER LICENSE)
GOVERNMENT CONTRACTORS


AUTHENTISE
ANDRE@AUTHENTISE.COM // @AUTHENTISE

3 Summary of Attendee Perceptions

This section summarizes attendee perceptions as gathered throughout the symposium, including during presentations and through information gathering exercises. At the start of the symposium, attendees were asked to anonymously list as many thoughts / items as they could under each of the following categories:

- Risks;
- Challenges;
- Existing Solutions, and
- Potential / Theoretical Solutions.

20 percent of attendees submitted their responses, listed in Appendix A.

In addition, during the closing session, attendees were asked to identify thoughts / items under the following categories:

- Standards;
- Guidance;
- Tools, and
- Gaps.

The responses from this exercise are listed in Appendix B.

Several attendees identified culture / humans as a significant risk or challenge to the cybersecurity of DDM, and to cybersecurity in general. Cybersecurity education at all levels of a manufacturing organization was desired. Changing the priorities and culture of manufacturing organizations is challenging due to a lack of understanding of cybersecurity risks and benefits. Business cases or examples were desired. A few attendees mentioned legal requirements as a potential solution and there were a few comments questioning who bears the burden of the risk of an attack – the IP owners, the vendor(s), or the government.

Threats to the integrity of designs and systems were a common thread in responses. Some mentioned confidentiality of intellectual property as a concern and only a few identified availability concerns. Software vulnerabilities were called out a few times, but most responses focused on the final product. The nature of the digital supply chain was identified several times as a challenge with attendees specifically calling out the volume and types of data to be protected in a distributed and open manufacturing environment.

Quality control and event detection capabilities were desired. A few attendees mentioned the use of encryption throughout the manufacturing process as a potential solution. Other potential / desired technical capabilities identified by respondents included: distributed network security solutions, authentication mechanisms, automated and real-time monitoring and control, embedded security solutions, and residual data removal tools. It was stressed in responses and throughout the symposium that any technical solution must be simple and easy and preferably all-encompassing– “an easy button”.

Another common thread in responses was the suggestion for guidelines specific to DDM based on NIST SP 800-53 [1], the NIST Cybersecurity Framework [2], existing ISO standards, and industry best practices. Technical standards, such as protocols and formats, were also mentioned by several as representing a gap, or opportunity, for improving cybersecurity. Attendees provided the following list of standards and guidelines as providing a potential foundation for future DDM-specific cybersecurity standards and guidelines.

- IEC 62264-1:2013 - *Enterprise-control system integration -- Part 1: Models and terminology* [4]
- ISA-95, *Enterprise-Control System Integration* [5]
- ISO / ASTM52915 – 13, *Standard Specification for Additive Manufacturing File Format (AMF) Version 1.1* [3]
- ISO 10303 -242:2014, , *Industrial automation systems and integration -- Product data representation and exchange -- Part 242: Application protocol: Managed model-based 3D engineering* [6]
- ISO 14306:2012, *Industrial automation systems and integration -- JT file format specification for 3D visualization [7]*
- ISO 14739-1:2014, *Document management -- 3D use of Product Representation Compact (PRC) format -- Part 1: PRC 10001* [8]
- ISO/IEC 27000:2014, *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary* [9]
- NAS 9924, *Cybersecurity Baseline* [10]
- NIACAP-DIACAP (now obsolete, see DoDI 8510.01 and [11] CNSSP No. 22[12])
- NIST Framework for Improving Critical Infrastructure Cybersecurity [2]
- NIST IR 8023, *Risk Management for Replication Devices* [13]
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* [1]
- NIST SP 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security* [14]

4 Conclusions

Direct Digital Manufacturing is poised to revolutionize the manufacturing industry. A collaborative public and private approach is necessary to improving the cybersecurity of DDM processes and technology. This symposium was intended to be a step in that direction.

Although the presenters were from diverse backgrounds representing a variety of viewpoints, each made similar points:

- Cybersecurity risks to DDM are very real;
- Cybersecurity threats are the Achilles heel of the current manufacturing revolution;
- There is a real opportunity to make the manufacturing supply chain more secure than it has ever been, and
- The time to build cybersecurity in to the DDM process is now.

Attendees identified several risks and opportunities for building cybersecurity into DDM. Many attendees identified the integrity of designs and machines as a major risk while a few also mentioned intellectual property concerns. Gaps and potential solutions were grouped into four categories:

- Education / awareness of risks and cost/benefits;
- Technical solutions such as encryption capabilities and network monitoring;
- Technical standards such as a security option in existing standard file formats, and
- Guidance / best practice documents based on existing NIST publications.

With its expertise in advanced manufacturing and information technology, NIST is well poised to address these concerns. The NIST ITL has already developed cybersecurity guidance related to Cyber Physical Systems and Industrial Control Systems. There is an opportunity to include DDM cybersecurity considerations into future revisions of existing programs and publications. Also, the National Initiative for Cybersecurity Education (NICE) has begun to look at how to help manufacturers be more aware of cybersecurity risks that they may not have recognized. Additionally, the National Cybersecurity Center of Excellence (NCCoE) uses existing standards and technology to architect solutions to difficult cybersecurity problems and DDM may be a candidate. Results from this symposium will help guide future efforts in these areas.

Appendix A: Response Sheet Results

At the beginning of the symposium, attendees were asked to list as many items/thoughts as they could under the following categories: Risks, Challenges, Existing Solutions, and Potential / Theoretical Solutions. Attendees were not limited as to the scope of their responses and encouraged to write whatever came to mind. The following is a compilation of the responses received in each category. Responses are listed in alphabetical order and were transcribed as closely as possible, including grammar, abbreviations, and spelling. References have been added where possible and are included in Appendix F. An analysis of the responses, along with responses in Appendix B, is provided in section 3 of this publication.

Risks:

- Altering data to change specs of finish products
- Availability
- Components in sensitive applications may have unintended / undesirable performance characteristics that are undetectable
- Confidentiality
- Corruption of imbedded software @ machine
- Corruption of STL files
- Damage of manufacturing equipment
- Design tools vulnerability -> CAD & pre-cad part of
- Detection of inherent flaw - pilphereal IP is analyzed for existing flaw
- Ensure the small & medium enterprise have the tools are reasonable price point
- EtherCat or Industrial IP security?
- Getting tools to the right level capability at right price / affordable
- Government entities each seem to have their own program for cyber security. The risk is two-fold: (1) they are talking, but not WORKING together. Wasting resources and efforts (2) Government is way behind industry, and not bringing them in to address this substantial gap
- Integrity
- IT/OT convergence --> how do I secure this… …
- IVV of file transport from central storage to production facility
- Modification of model
- OEMs not ensuring security (& keeping backdoors open for "maintenance")
- Tainted products (additional functionality)
- The human aspect (social engineering)
- Theft of intell property
- Theft of IP
- Treats to RF specturm - wireless is increasing the comms component of choice on factory floor. 802.3, 802.11ad etc
- Understanding 3D printer, direct digital in the context of 3D phenomenon [i.e. same files could be used for manufacturing or decision support
- Uneducated workforce

- Un-maintained manufacturing equipment (outdated OS, virus definitions, firewall, firmware, etc.)

Challenges:

- 3D, HD, FMV
- Automated
- Automation security
- Balancing benefits of open-source / open architecture machines & file formats with dangers of cyber vulnerabilities
- Digital rights management / digital asset management
- Digital supply chain
- DISTRIBUTED manufacturing --> factory to factory
- eCommerce --> Will be part of the supply chain and will provide its own set of challenges
- Educating workforce about cyber-physical concerns
- Embedded system / PLC, SCADA, ACS security
- Front end costs of cyber controls are hard to justify
- Having the right folks be the custodian of data / system
- How to capture design intent for validation / certification
- Integration of various data warehouse within enterprise that have to interface with each other (i.e. PDM/PLM, MRP/ERP/MES and Accounting/HR) to provide the integrity, availability, & confidentiality
- Intellectual property management
- Lack of business case
- Manufacturing systems are not often updated (patches, firmware, more IT functionality than needed)
- Mfg culture, gap to IT culture
- Modeling and simulation precursor to decision to manufacture and design for manufacturing
- MOM [Manufacturing Operations Management Security]
- Organizational change management
- PCII - protected critical infrastructure Information
- PMI - production Manufacturing Information
- Poor acquisition policy that doesn't drive security
- Poor secure engineering design techniques (hardware & software)
- Prioritization of what is really important
- Quality control of microarchitecture
- Real-Time systems (synchrophasor, EtherCAT, etc)
- Role based access for M2M (machine to machine) exchanges
- Security as a requirement for the PLC and PLC of infrastructure and PLC of FW/SW
- Sensor network security
- The value proposition
- Trust

- Understand tools, techniques and processes to protect fidelity from design thru production - what tool, at what cost, at what reduction in efficiency
- Volume of 3D digital media

Existing Solutions

- 5 layer manufacturing protocol stack [5, 4]
- Encryption
- Fundamental best practices are available in 800 series SPs and some contemporary IT security publications
- NIST framework is good starting point
- Training / awareness
- Use of existing protocol for traditional manufacturing

Potential / Theoretical Solutions

- 20 Critical controls for manufacturers
- Anecdotal
- Benchmark DoD/DOE defense contractors for best practices
- Content distribution networks - edge computing security
- Encrypt lifecycle
- Encrypted streaming
- Factory of the future dialog
- Focus on model based ecosystems: provides an architecture and governance
- IACAP-DIACAP - 800-134 (guess at #) - DoD continues to evolve "mandatory" standard
- Increased use of encryption
- Need a single entity that government can use to advance itself in this area. To succeed needs non-government owner who can bring all gov. entities together pooling resources, and incorporate industry to get current best practices. Suggest DMDLL as they are already doing a project on this involving government and industry. Possibly a more comprehensive follow on project
- NEED AN EASY button for manufacturing floor
- NTSB and auto - safety - manufacturers are responsible for standards - policy and law follow recommendation but a federal law was necessary to institute the mandate for commercial sector
- Standards are probably the best way of balancing concerns of vulnerabilities, openness, & privacy (& business)
- What risk reduction strategies, tools, and solutions exist? - A primer for manufacturing would be great!! Perhaps a good project for NAMII?
- When we take people out of the loop a lot of vulnerabilities go away

Appendix B: Working Session Results

During the working session, attendees were asked to identify any standards, guides, or tools that could be applied to cybersecurity in DDM. They were also asked to identify any gaps in those areas, or anything that was missed during the symposium. Attendees were not limited as to the scope of their responses. The following is a compilation of the responses received in each category. Responses are listed in alphabetical order and were transcribed as closely as possible, including grammar, abbreviations, and spelling. References have been added where possible. An analysis of the responses, along with responses in Appendix A, is provided in section 3 of this publication.

Standards:

- AMF & ISO JT [7]
- IEC [16]
- IEEE [17]
- ISO ? Dealing with PDF / PRC format [8]
- ISO [18]
- ISO 10303 AP 242 [6]
- ISO 27000 [9]
- ITSI
- NAS 9924 [10]
- National Aerospace STDs published by Aerospace Industries Assoc. www.aia-nas.org [19]
- NIST 800-53 [1]
- Sector SIGs
- Security Spec for ISO AMF standard [3]
- See references to draft CPS PWG working group report [20]
- Step 242 [6]

Guides:

- Cyber awareness for the shop floor
- NIST SP 800-82 [14]
- Overlay for 800-53 [1] is important in bridging IT to OT thinking
- Risk Management adapted for DDM

Tools:

- DEA tools
- NICE [21]
- Residual data removal tool
- Threat data sharing mechanisms

Gaps:

- Authentication of Articles Connected to IoT
- Awareness of costs associated with NOT integrating security
- Breach Disclosure
- Drivers for secure hardware & software design
- Encryption approaches
- FBI is an active player in cybersecurity
- Flaw hack marketplace
- Formats
- Integration approaches
- International laws and agreement to prosecute the sources of cybersecurity event and bad actors
- Manufacturing Protocol Stack (Purdue) [15]
- Material quality standards - powder (distribution, properties), polymer
- NEED a guide for Business Case Analysis (for cybersecurity in mfg); NEED data/case examples to support
- Rule of unfettered Innovation / open software mode
- Transport protocols
- Who owns the problem
- Who owns what? - IP ownership
- Who will own the solution - if industry doesn't does it roll over to government

Appendix C: Speaker Biographies

The following are speaker biographies as included in the agenda for the symposium, in presentation order.

Michael F. Molnar
Director, NIST Advanced Manufacturing Program Office
Director, Advanced Manufacturing National Program Office (AMNPO)

Mike Molnar likes to be introduced simply as "a manufacturing guy from industry" with nearly 30 years of experience in advanced manufacturing. To help provide an industry focus in 2011 he was named the first Chief Manufacturing Officer of the National Institute of Standards and Technology. Today Mike leads the NIST Advanced Manufacturing Program Office for extramural manufacturing programs and also serves as the director of the interagency Advanced Manufacturing National Program Office. As called for by the Advanced Manufacturing Partnership initiative, the AMNPO's mission is to foster industry-led partnerships and to form a "whole of government" approach to strengthen competitiveness and innovation in U.S. manufacturing.

Mike's experience includes leadership roles in advanced manufacturing, metrology, manufacturing systems, quality, technology development, sustainability and industrial energy efficiency. His credentials include service as a Federal Fellow in the White House Office of Science and Technology Policy, and election as Fellow of both the American Society of Mechanical Engineers and the Society of Manufacturing Engineers. He is a licensed Professional Engineer, a Certified Manufacturing Engineer and a Certified Energy Manager. He received a Master of Business Administration from the University of Notre Dame, and both a Master of Science in Manufacturing Systems Engineering and a Bachelor of Science in Mechanical Engineering from the University of Wisconsin. He is an active member of professional societies, consortia and volunteer organizations.

Christopher B. Williams
Associate Professor, Virginia Tech Department of Mechanical Engineering

Christopher B. Williams is an Associate Professor with a joint appointment with the Department of Mechanical Engineering and the Department of Engineering Education at Virginia Tech. He is the Director of the Design, Research, and Education for Additive Manufacturing Systems (DREAMS) Laboratory and Associate Director of the Macromolecules & Interfaces Institute. His research contributions have been recognized by six Best Paper awards at international design, manufacturing, and engineering education conferences. He is a recipient of a National Science Foundation CAREER Award (2013), the 2012 International Outstanding Young Researcher in Freeform and Additive Fabrication Award, and the 2010 Emerald Engineering Additive Manufacturing Outstanding Doctoral Research Award. Chris holds a Ph.D. and M.S. in Mechanical Engineering from the Georgia Institute of Technology (Atlanta, Georgia) and a B.S. with High Honors in Mechanical Engineering from the University of Florida (Gainesville, Florida).

Scott Zimmerman CISSP-ISSEP
Principal IT Advisor, Concurrent Technologies Corporation (CTC)

Dominick Glavach CISSP, GCIH
Principle Fellow, Information Systems Security Engineer, CTC

Scott Zimmerman, CISSP-ISSEP is a Principal Technical Advisor at Concurrent Technologies Corporation with 20 plus years of Cyber Security experience. Mr. Zimmerman specialized expertise includes cyber security, cloud/mobile computing and systems engineering. Mr. Zimmerman's education includes a BS in Management Information Systems and AS in Electronic/Computer Technology. He is a Certified Information Systems Security Professional (CISSP); Information Systems Security Engineering Professional (ISSEP).

Mr. Glavach is a Principle Information Systems (IS) Security Engineer and CISO at Concurrent Technologies Corporation (CTC). He serves as the Cyber Security technical lead in CTC's Enterprise Infrastructure, provides CTC's clients with Cyber technical leadership and Subject Matter Expertise (SME). Mr. Glavach received his BS in Computer Science from the Indiana University of Pennsylvania, is a Certified Information System Security Professional (CISSP), an active member of the Information Assurance Technology Analysis Center SME Program and member of the Cloud Security Alliance (CSA).

The speakers specialize in cyber attack methods, attack warning and detection, and cyber countermeasures. They have presented numerous talks on cloud forensics, cyber adversaries and advanced persistent threats to a wide range of public and government audiences.

Concurrent Technologies Corporation (CTC) is an independent, nonprofit, applied scientific research and development professional services organization providing innovative management and technology-based solutions to government and industry. Established in 1987, CTC operates from more than 50 locations with a staff of over 1,400 employees. As a nonprofit 501(c)(3) organization, CTC's primary purpose and programs are to undertake applied scientific research and development activities that serve the public interest. We conduct impartial, in-depth assessments and technical evaluations that emphasize increased quality, enhanced effectiveness, and rapid technology transition and deployment. CTC offers a broad range of services and capabilities, coupled with real-world experience. For more information about CTC, visit www.ctc.com.

Dr. Michael McGrath
NDIA Manufacturing Division

Michael McGrath is an independent consultant who provides analytic support for government and industry technology programs. He is also a Senior Technical Advisor (and former Vice President) at Analytic Services Inc. (ANSER), a not-for-profit government services organization. He previously served as the Deputy Assistant Secretary of the Navy for Research, Development, Test and Evaluation (DASN(RDT&E)), where he was a strong proponent for improvements in technology transition, modeling and simulation, and test and evaluation. In prior positions, he

served as Vice President for Government Business at the Sarnoff Corporation, ADUSD for Dual Use and Commercial Programs in the Office of the Secretary of Defense (OSD), Assistant Director for Manufacturing at the Defense Systems Research Projects Agency (DARPA-DSO), and Director of the DoD Computer-aided Acquisition and Logistics Support (CALS) program. While at DARPA, he managed the Affordable Multi-Missile Manufacturing Program and the Agile Manufacturing program. He was also heavily involved in DARPA's dual-use Technology Reinvestment Project and has been a strong advocate for defense use of commercial technology advances. His early government career included positions in Logistics Management at Naval Air Systems Command and in Acquisition Management in OSD. He is a Senior Fellow at the Potomac Institute for Policy Studies, a director of South Carolina Research Authority Applied R&D, and a member of the National Research Council's Materials and Manufacturing Board, the Defense Materials, Manufacturing and Infrastructure Committee (chair), the Penn State ARL Materials and Manufacturing Advisory Board, and the Georgia Tech Manufacturing Institute Advisory Board.

Dr. McGrath holds a BS in Space Science and Applied Physics and an MS in Aerospace Engineering from Catholic University, and a doctorate in Operations Research from George Washington University.

Robert Zollo
President, Avante Technology, LLC

Mr. Zollo is President and Founder of Avante Technology, LLC, a privately held company that develops, markets and licenses advanced 3D printing technology to 3D printer OEM, manufacturers and engineering firms. Prior to that he was President and Founder of Software Architects, Inc. a developer of electronic systems for OEM in a variety of industries, including 3D printing, digital imaging and optical recording. As Chairman of the Optical Storage Technology Association, Mr. Zollo was responsible for the development of ISO 13346, the international standard that defines the digital file format used in all DVD's, Blu-ray discs, CAT scan, MRI and digital X-ray systems. He also led the development of four patents relating to digital file management, image manipulation and file interoperability, and is the inventor of a patent pending method for controlling the printing of new engineering grade composite materials in FDM printers. Mr. Zollo holds a Bachelor of Science degree in Engineering from the U.S. Military Academy at West Point, an MBA from Southern Illinois University and conducted his graduate technical studies at the University of Southern California's school of engineering. He is currently working on enhancements to the new ISO AMF standard defining the 3D file description language for additive manufacturing applications.

Dr. Claire Vishik
Trust and Security Technology and Policy Director, Intel Corporation

Dr. Claire Vishik's work at Intel Corporation focuses on hardware security, Trusted Computing, privacy enhancing technologies, some aspects of cryptography and related policy issues. Claire is a member of the Permanent Stakeholders Group (Advisory Board) of ENISA, the European Network and Information Security Agency. She is an advisor to a number of cybersecurity R&D and policy projects, initiatives, and organizations, including the cryptography program at the University of Bristol or Oxford Cybersecurity Center for Capacity Building and is on the leadership teams of several organizations and initiatives tasked with the development of R&D strategies in cybersecurity in the US, Europe, and beyond. Claire is active in standards development and is on the Board of Directors of the Trusted Computing Group and on the Council of the Information Security Forum. Claire received her PhD from the University of Texas at Austin. Prior to joining Intel, Claire worked at Schlumberger Laboratory for Computer Science and AT&T Laboratories. Claire is the author of numerous papers and reports and an inventor on 30+ pending and granted U.S. patents.

Andre Wegner
Co-founder & CEO, Authentise

Andre Wegner is co-founder and CEO of Authentise (www.authentise.com), the licensing and services platform for Distributed Manufacturing. Authentise secure streaming and quality assurance technology for 3D printing enables design owners to share their digital manufacturing designs with confidence, and get paid per print. Authentise Consulting also assists Fortune 100 corporations put 3D printing at the heart for their business. He is a frequent speaker on emerging intellectual property issues in 3D Printing and opportunities of distributed manufacturing at events such as Singularity University, Rapid, Designer of Things, Inside 3D Printing, 3D Print Show, Pacific Crest & WIRED. He has been quoted in publications such as BBC News, MIT Tech Review, Chicago Tribune, and Bloomberg. Prior to founding Authentise he managed a venture capital fund in Nigeria and advisory services in India. He is a graduate of St. Andrews University (UK), ESSEC (France) and Singularity University (California).

Appendix D: Attendees List

Registrant Name	Organization
Clara Asmail	NIST MEP
Lawrence Balash	Nova Corporation
David Barrett	Department Of Navy-Chief Of Naval Operations
Dean Bartles	UI Labs
Michelle Bezdecny	Anser - OSD/Mantech
Allen Egon Cholakian	IRDFproject Harvard / Columbia
Bill Coccoli	NGC
Thomas Conkle	G2, Inc.
Khershed Cooper	NSF
Charles Crum	Office Of Inspector General, Us Postal Service
Nicholas Deliman	MDA Information Systems
Tuong-Vy Do	
Gavin Garner	University Of Virginia
Dom Glavach	
Daniel Green	Space And Naval Warfare Systems Command
Ryan Hayleck	NAVSEA
Paul Huang	NIST
Brian Hubbard	G2, Inc.
Michele Hughes	
Lawrence John	Analytic Services Inc.
Waide Jones	Lockheed Martin
Ben Kassel	Naval Sea Systems Command
Bruce Kramer	NSF
Francis Lee	Howard County Public School Systems
Michael Mcgrath	Analytic Services Inc (Anser)
Mike Molnar	NIST
Ed Morris	NCDMM
Wesley Old Coyote	State Of Montana
Yaowe Ong	CSC

Celia Paulsen	NIST
Al Payne	Theta Solutions
Paul Petronelli	Palm Associates, Inc.
James Rentsch	Aerospace Industries Association
Chris Root	NAVAIR Fleet Readiness Center Southwest
Scott Storms	NAVSSES
Rebecca Taylor	NCMS
Joe Veranese	NCDMM
Patrick Violante	NAVSSES
Claire Vishik	Intel
R Wachter	
Andre Wegner	Authentise Inc
Eric Wilcox	SAIC
Craig Young	DDC-ITS
Scott Zimmerman	CTC
Robert Zollo	Avante Technology, Llc

Appendix E: Acronyms

ACS	Access Control System
AM	Additive Manufacturing
AMF	Additive Manufacturing File Format
CAD	Computer Aided Design
DDM	Direct Digital Manufacturing
DEA	Data envelopment analysis
DMDII	Digital Manufacturing and Design Innovation Institute
DoD	Department of Defense
DOE	Department of Energy
ERP	Enterprise resource planning
FMV	Full Motion Video
FW	Firmware
HD	High Definition
IoT	Internet of Things
IP	Intellectual Property
ISO	International Organization for Standardization
IT	Information Technology
IVV	Independent Verification and Validation
MES	Manufacturing Execution System
MOM	Manufacturing Operations Management
MRP	Material requirements planning
NAMII	National Additive Manufacturing Innovation Institute
NIST	National Institute of Standards and Development
NICE	National Initiative for Cybersecurity Education
NNMI	National Network for Manufacturing Innovation
NTSB	National Transportation Safety Board
OEM	Original Equipment Manufacturer
OS	Operating System

OT	Operations/Operational Technology
PCII	Protected Critical Infrastructure Information
PDM	Product data management
PLC	Programmable Logic Controller
PLM	Product Lifecycle Management
PMI	Production Manufacturing Information
RF	Radio Frequency
SCADA	Supervisory Control and Data Acquisition
SIG	Special Interest Group
STD	Standard
STL	Stereolithography
SW	Software

Appendix F: References

[1] NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Gaithersburg, Maryland, 2013, http://dx.doi.org/10.6028/NIST.SP.800-53r4

[2] Cybersecurity Framework, National Institute of Standards and Technology, http://www.nist.gov/cyberframework/, 2014

[3] ISO / ASTM52915 - 13, *Standard Specification for Additive Manufacturing File Format (AMF) Version 1.1*, Astm, 2013, http://www.astm.org/Standards/ISOASTM52915.htm

[4] IEC 62264-1:2013, *Enterprise-control system integration -- Part 1: Models and terminology*, International Organization for Standardization, 2013, http://www.iso.org/iso/catalogue_detail.htm?csnumber=57308

[5] ISA-95, *Enterprise-Control System Integration*, International Society of Automation, https://www.isa.org/isa95/

[6] ISO 10303-242:2014, *Industrial automation systems and integration -- Product data representation and exchange -- Part 242: Application protocol: Managed model-based 3D engineering*, International Organization for Standardization, 2014, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=57620

[7] ISO 14306:2012, *Industrial automation systems and integration -- JT file format specification for 3D visualization*, International Organization for Standardization,2012, http://www.iso.org/iso/catalogue_detail.htm?csnumber=60572

[8] ISO 14739-1:2014, *Document management -- 3D use of Product Representation Compact (PRC) format -- Part 1: PRC 10001*, International Organization for Standardization, 2014, http://www.iso.org/iso/catalogue_detail.htm?csnumber=54948

[9] ISO/IEC 27000:2014, *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*, International Organization for Standardization, 2014, http://www.iso.org/iso/catalogue_detail?csnumber=63411

[10] NAS9924, *Cybersecurity Baseline*, Aerospace Industries Association,2013, https://global.ihs.com/doc_detail.cfm?&rid=AIA&input_doc_number=NAS%209924%2

CNA&item_s_key=00601403&item_key_date=861003&input_doc_number=NAS%209924%2CNA&input_doc_title=#abstract

[11] Department of Defense Instruction (DoDI) 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, Department of Defense, 2014, http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

[12] *Policy on Information Assurance Risk Management for National Security Systems*, Committee on National Security Systems (CNSS), CNSSP No. 22, 2012, http://www.ncix.gov/publications/policy/docs/CNSSP_22.pdf

[13] Dempsey, Kelley and Paulsen, Celia. NIST Internal Report (IR) 8023, *Risk Management for Replication Devices*, National Institute of Standards and Technology, 2015, http://dx.doi.org/10.6028/NIST.IR.8023

[14] NIST Special Publication (SP) 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*, second public draft, National Institute of Standards and Technology, Gaithersburg, Maryland, 2008, http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_r2_second_draft.pdf

[15] Williams, Theodore J. "The Purdue Enterprise Reference Architecture", *Computers in Industry*, 24 (1994), pp. 141-158, http://dx.doi.org/10.1016/0166-3615(94)90017-5.

[16] International Electrotechnical Commission (IEC), http://www.iec.ch/, 2015

[17] IEEE, https://www.ieee.org/index.html, 2015

[18] ISO - International Organization for Standardization, http://www.iso.org/iso/home.html, 2015

[19] Aerospace Industries Association, National Aerospace Standards Aerospace Industries Association, http://www.aia-aerospace.org/national_aerospace_standards/, 2015

[20] Cyber-Physical Systems Public Working Group, http://www.cpspwg.org/, 2015

[21] The National Initiative for Cybersecurity Education (NICE), National Institute of Standards and Technology, http://csrc.nist.gov/nice/, 2015