2023 ANNUAL REPORT

CYBERSECURITY FOR MANUFACTURING INNOVATION

Strengthening and Securing U.S. Manufacturing with Innovations in Cybersecurity and Energy Efficiency

CYMANII

the cybersecurity manufacturing innovation institute

2023 ANNUAL REPORT

TABLE OF CONTENTS

CYMANII

EXECUTIVE SUMMARY

2023 Year in Review

2023 marked another important year for the Cybersecurity Manufacturing Innovation Institute (CyManII). Building on the progress of the previous two years, CyManII continued to advance cutting-edge research in industrial security while increasing engagement with industry and growing its operational capacity. This year, CyManII expanded operations at the Cybersecurity for Manufacturing (C4M) hub to provide a research and development (R&D) platform and launched the Mobile Training Vehicle (MTV) to provide on-site cybersecurity training to students and manufacturers. In recognition of its initiatives and advancements, the Institute also won considerable new funding awards, receiving $1 million from the Department of Energy (DOE) for the creation of a Cybersecurity Modular Bootcamp and $500,000 from the U.S. Economic Development Association (EDA) to support the creation of the Secure Manufacturing Tech Hub, a Texas-based consortium dedicated to driving innovation in commercial-ready cybersecurity technologies.

Perhaps most importantly, 2023 represented an inflection point for the Institute and its efforts to drive innovation in industrial energy efficiency and cybersecurity technology. This year, we introduced Industry Use Cases (IUCs) to begin the work of translating the research associated with our Cybersecurity Energy & Emissions Quantification (CEEQ), Secure Defense Architecture (SDA), and Secure Research and Development Infrastructure (SRDI) projects into real-world applications. To that end, CyManII launched its first Request for Proposals (RFPs) to solicit projects from industry partners. We also released the latest update to our Roadmap to outline this process and provide a preview of our plans for our fourth year.

> ***“[CyManII is] an impressive team, leading a critical mission.”***
>
> *Michael Mylrea, Cybersecurity Executive and Ethical Hacker*

MESSAGE FROM THE CEO

Dr. Howard Grimes
CyManII CEO

The year 2023 will stand out in the history of the Cybersecurity Manufacturing Innovation Institute. We managed several major pivots with aplomb, flew through a rigorous peer review, added new great staff, and via competitive RFPs are validating our innovations on factory floors across the nation.

Today, I write in gratitude and appreciation of our many accomplishments that you'll find in this Annual Report. I am confident in our strategy and beyond confident in the team executing our strategy. We are ready and eager to embrace the next wave of grand challenges on our route of **Secure.*TOGETHER*.**

You will see across these pages our aggregate accomplishments and our continued ability to attract additional funding—perhaps the greatest acknowledgement of Institute success. Because of our dedication to the mission, our financial and technical foundations are stronger than ever.

WE TRANSITIONED TECHNOLOGY INNOVATIONS TO FACTORY FLOORS

CyManII technical innovations start at a basic research level and integrate fundamental mathematics and physics into creating a holistic, integrated approach to cybersecurity. In 2023, our leadership team embraced a new challenge: move these innovations to real factory floors and test them rigorously. In other words—prove they work in the real world. Several "Industry Use Cases" were selected based on our Roadmap. Thus, we are now testing **Secure Defensible Architectures**, **Cyber-Physical Passports**, **Energy and Emission Quantification**, and **Cyber Weakness Enumerations** in the manufacturing of energy controllers, a wide swath of smart manufacturing operations, and in additive manufacturing.

WE LIVED OUR VALUES

Cybersecurity is a team sport. We strengthened our team, added new positions, and grew Institute membership. We embraced the value of "One Team. One Fight" and operationalize this value every day.

We continue to operate a "hyper-dispersed organization" where we reject geographic distance as an obstacle to excellence. But we also enjoy each other on those times when we can meet face-to-face. We have extended our commitment to the mission "secure U.S. manufacturers" in every way imaginable by making each of us stronger.

Beyond these key observations, perusal of this Annual Report will provide insight into the depth and breadth of what we do. But it is important to note that CyManII is "The Institute of the Future." Unlike typical university centers or institutes, CyManII is a national institute, bringing a "whole-of-nation" approach to cybersecurity. We aggregate "best-in-class" research universities, DOE National Laboratories, and private industry.

Being a part of this brilliant, motivated, diverse community, as we exist today and as we evolve for tomorrow, is an honor. If you remember one thing about 2023, remember that this CEO felt deeply honored to lead CyManII. The CyManII team is making an impact that will protect and secure our nation for years to come.

INSTITUTE **OVERVIEW**

ABOUT CYMANII

The Cybersecurity Manufacturing Innovation Institute (CyManII—Cī-man-ē) was launched by the Department of Energy (DOE) in 2020 to advance cybersecure, decarbonized manufacturing. CyManII is focused on pursuing fundamental research and development (R&D) that advances our understanding of the evolving cybersecurity issues that threaten U.S. manufacturers. The results of this research aim to improve energy efficiency in manufacturing industries, inspire the development of new cybersecurity technologies and innovations, and enhance cybersecurity knowledge and awareness within the broader community of U.S. manufacturers.

OUR APPROACH

To realize these goals, we rely on a unique approach that considers the dynamic complexity of the U.S. manufacturing ecosystem. Securing and optimizing today's digital companies requires a dual focus on both technological challenges and business challenges, all of which must be underpinned by direct input from industry. The two key pillars of CyManII's transformative approach are the Agile Development Pathway and the Industry Information Ecosystem. The Agile Development Pathway for technological innovations facilitates the rapid development of critical concepts and deprioritizes less critical ones, ensuring that useful innovations reach the market quicker. The Industry Information Ecosystem aims to educate, train, and inform companies of current threats relevant to their enterprise. Together, these approaches allow companies to shift "left of boom" with access to purpose-built solutions and real-time training that meets them where they are.

Our vision for secure manufacturing relies on the parallel and collective development of innovations that together provide the foundation for the new tools, solutions and approaches that will shift the industry toward secure efficiency. These Integrated Foundational Technologies (IFTs) are the cornerstones for the disruptive solutions that companies need.

CyManII's approach to transformative R&D is based on an agile method that is heavily informed by industry needs. This collective consideration of government, research, and applied expertise is intended to yield security products that are revolutionary, yet guided and grounded—and most importantly, translational to the machine shop floor.

2023 GOALS

Continuous partnership with both industry and academia is the most vital component of CyManII's integrated approach to transforming the U.S. manufacturing industry. In 2023, CyManII made significant progress in its efforts to build this partnership and engage with industry to develop Industry Use Cases (IUCs) that demonstrate the possibilities for secure and energy-efficient advanced manufacturing and help chart a path for the deployment of transformational innovations in small and large manufacturing platforms across diverse industries.

As CyManII continued its mission to transform and secure the U.S. manufacturing industry, the following objectives outlined its strategic focus for 2023:

ONE — **Grow the Institute's operational capacity and thought leadership**

TWO — **Partner with U.S. industry**

- Work directly with industry to create products that are secure by design and secure by default, and make U.S. manufacturing **Secure.*TOGETHER.***
- Grow CyManII's engagement with private sector partners and vendors

THREE — **Promote education and workforce development**

FOUR — **Set the vision for Industry Use Cases**

FIVE — **Update CyManII's Strategic Plan and Roadmap**

CYMANII

VISION & MISSION

Secure.TOGETHER.

MISSION

CyManII will secure and sustain U.S. manufacturing through the development of partnerships and the deployment of innovative technologies that will empower a skilled workforce.

VISION

We will be the leading provider of integrated cybersecurity and energy efficient solutions for U.S. manufacturers as they undergo digital transformation. We are committed to empowering manufacturers with the tools they need to secure their physical systems from cyber threats, optimize energy usage, and improve operational efficiency. Through cutting-edge technology and innovative solutions, we aim to help U.S. manufacturers become more secure, competitive, resilient, and sustainable in a rapidly evolving global market.

We aim to support the transformation of U.S. manufacturers toward embedded security and energy efficiency by providing solutions that are pervasive, unobtrusive, and economical. We will:

- Research and develop new technologies and solutions that support cybersecurity, energy efficiency and decarbonization.
- Train and upskill U.S. workers in information technology (IT) and operational technology (OT) security.
- Inform stakeholders of cyber vulnerabilities and mitigations.
- Increase risk awareness of cyber threats among business decision makers.
- Accelerate adoption of technologies and solutions through industry engagement, demonstrations, and a measurable return on investment (ROI).

CORE VALUES

Preventative risk management investments can be challenging for small businesses to justify; therefore, to create a revolution in intelligent manufacturing, we must produce solutions that are Energy-Efficient (ε), Pervasive, Unobtrusive, Resilient, and Economical (ε-PURE). Together, these principles underpin our mission and guide our technical solutions.

PERVASIVE
throughout systems

Secure energy efficiency relies on high-density, real-time data collected throughout automated processes and the connected supply chain. Wireless networks, sensors, and smart meters must be pervasive throughout systems and accessible to small and medium manufacturers (SMMs) alike.

UNOBTRUSIVE
to the users

Solutions must be easy to use and unburdensome for non-security experts. Further, adoption should not impact production, but rather enhance it. Ideal solutions will be “baked in” to existing tools, systems, and processes, unobtrustive to the users.

RESILIENT
against disruptions

When disruptions do occur, process automation should be able to detect anomalies apart from appropriate production behavior and resume normal state operations. Embedding capabilities for state awareness and recovery will make systems resilient against attacks.

ECONOMICAL
for the manufacturer

For companies to adopt new cybersecurity risk mitigation solutions, a clear ROI must exist. Further, the investment commitment must be affordable for SMMs as well as large enterprises.

CYMANII BY THE NUMBERS: 3 YEARS

Roadmap published and updated

4 research publications

Published **Cyber Weakness Enumeration content** for critical infrastructure (with MITRE: https://cwe.mitre.org/)

2 invention disclosures (Cyber-Physical Passport and CyManII Attack Defense Annex)

45 members to date

23 in pipeline (22 are industry)

15 in cultivation (all industry)

50,000 SMMs in our Member Network

10,500 workers trained

$7M invested in competitive Industry Use Cases

Garnered over **$7M** in additional funding

- State of Texas (**$3M/year** for C4M and MTV)
- DOE (**$1M** for Cybersecurity Modular Bootcamp)
- EDA (**$500K** for Secure Manufacturing Technology Hub)

Launched **C4M** - including nation's only Cyber-Informed Engineering lab

Launched a secure facility known as **Lab Six**

Hosted **6** "Industry Days" across the United States

Launched **Manufacturing-ISAC**

Launched **Mobile Training Vehicle**

INSTITUTE **REPORT**

In 2023, the Institute enjoyed considerable growth across its initiatives. Our research efforts resulted in the publication of four research papers and the launch of Cyber Weakness Enumeration (CWE) content for critical infrastructure. Additionally, we made significant strides in innovation, with two invention disclosures: the Cyber-Physical Passport (CPP) and the CyManII Attack Defense Annex.

Our initiatives secured over $7 million in competitive Industry Use Case (IUC) investment, complemented by additional funding from key stakeholders. The State of Texas allocated $3 million annually for our Cybersecurity for Manufacturing (C4M) and Mobile Training Vehicle (MTV) initiatives, while DOE provided $1 million in funding for our Cybersecurity Modular Bootcamp. Additionally, the U.S. Economic Development Association (EDA) provided $500,000 for the Secure Manufacturing Technology Hub.

Our membership increased significantly in 2023, with 45 active members and 23 in the pipeline, primarily from industry. Our Member Network expanded to include 50,000 SMMs, with over 10,500 workers trained to date.

We also introduced several new initiatives, successfully launched C4M, the nation's first Cyber-Informed Engineering (CIE) lab, along with Lab Six. Additionally, we facilitated six nationwide industry days, established the Manufacturing Information Sharing and Analysis Center (MFG-ISAC), and debuted the MTV. However, amid these accomplishments, the manufacturing sector faces escalating ransomware attacks, underscoring the urgency of our mission to strengthen cybersecurity defenses.

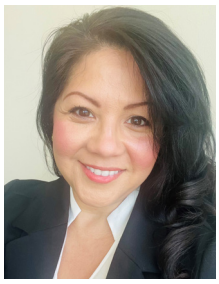
OUR PEOPLE

LEADERSHIP

Howard Grimes
Chief Executive Officer

Greg Shannon
Chief Scientific Officer

Wayne Austad
Chief R&D Officer

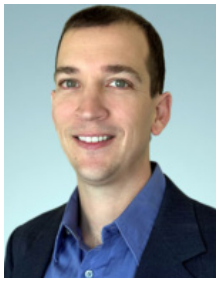


Rose Todd
Chief Operating Officer

Ken Fowler
Chief Information Security Officer & Director of Lab Six

Tom Kurfess
Chief Manufacturing Officer

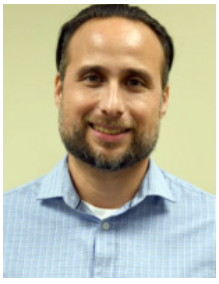
Stephen Laycock
Senior Director of Strategic Engagement



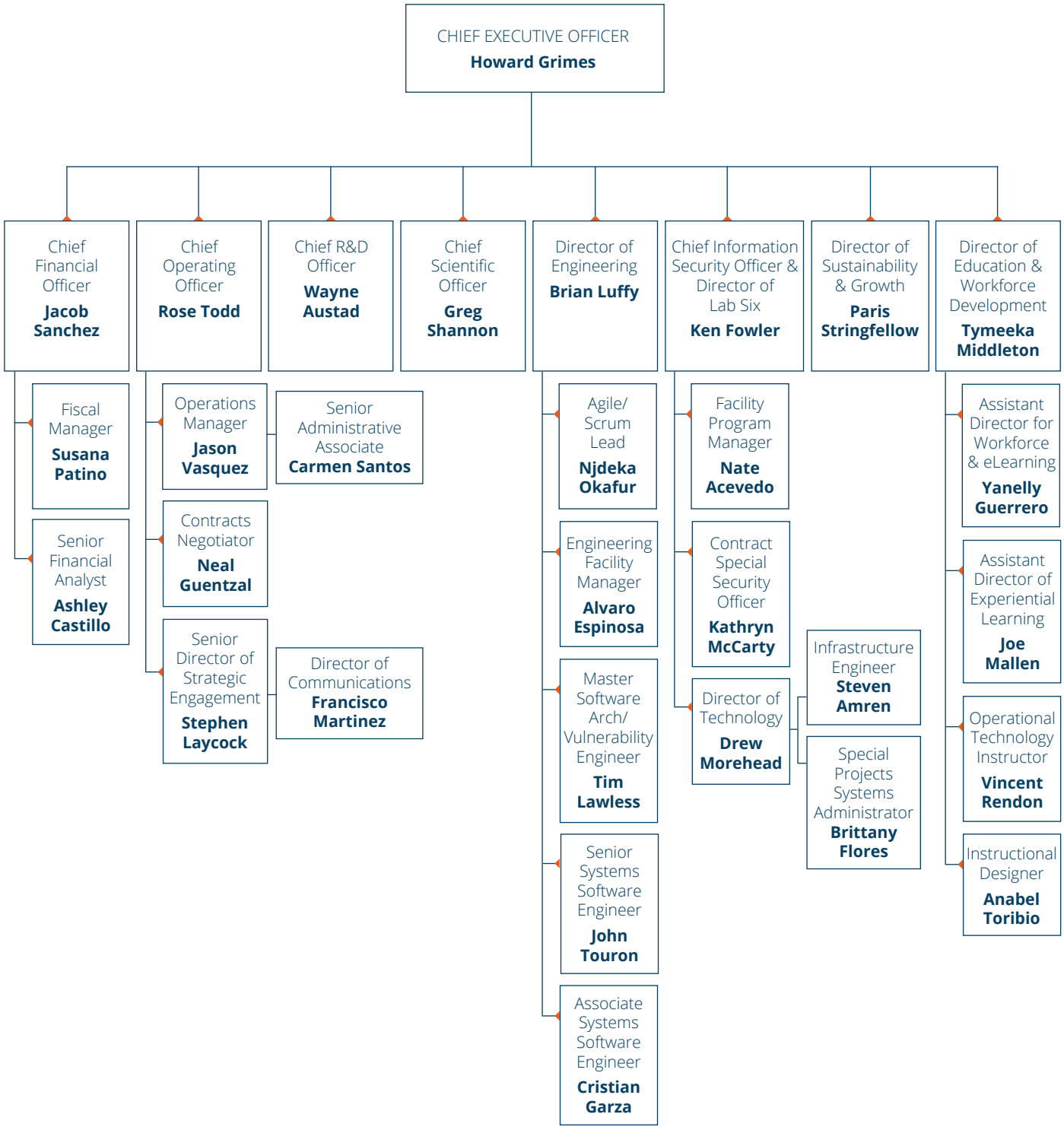
Brian Luffy
Director of Engineering

Paris Stringfellow
Director of Sustainability & Growth

Tymeeka Middleton
Director of Education & Workforce Development



Jacob Sanchez
Chief Financial Officer


CHIEF EXECUTIVE OFFICER
Howard Grimes
Chief Financial Officer
Jacob Sanchez
Fiscal Manager
Susana Patino
Senior Financial Analyst
Ashley Castillo
Chief Operating Officer
Rose Todd
Operations Manager
Jason Vasquez
Senior Administrative Associate
Carmen Santos
Contracts Negotiator
Neal Guentzal
Senior Director of Strategic Engagement
Stephen Laycock
Director of Communications
Francisco Martinez
Chief R&D Officer
Wayne Austad
Chief Scientific Officer
Greg Shannon
Director of Engineering
Brian Luffy
Agile/ Scrum Lead
Njdeka Okafur
Engineering Facility Manager
Alvaro Espinosa
Master Software Arch/ Vulnerability Engineer
Tim Lawless
Senior Systems Software Engineer
John Touron
Associate Systems Software Engineer
Cristian Garza
Chief Information Security Officer & Director of Lab Six
Ken Fowler
Facility Program Manager
Nate Acevedo
Contract Special Security Officer
Kathryn McCarty
Director of Technology
Drew Morehead
Infrastructure Engineer
Steven Amren
Special Projects Systems Administrator
Brittany Flores
Director of Sustainability & Growth
Paris Stringfellow
Director of Education & Workforce Development
Tymeeka Middleton
Assistant Director for Workforce & eLearning
Yanelly Guerrero
Assistant Director of Experiential Learning
Joe Mallen
Operational Technology Instructor
Vincent Rendon
Instructional Designer
Anabel Toribio

GOVERNANCE BOARD

Made up of 20 board seats, the Governance Board guides and informs CyManII operations, technical directives, and strategic planning.

Mr. John Dyck
Chief Executive Officer
Clean Energy Smart Manufacturing Innovation Institute (CESMII)

Ms. Julie Wulf
Cisco

Dr. Tanju Karanfil
Vice President of Research
Clemson University

Mr. Anthony Holden
U.S. Army General Engineer at ManTech
U.S. Department of Defense

Dr. Sudarsan Rahuri
Technology Manager, Advanced Manufacturing Office, DOE GF Office
U.S. Department of Energy; Cybersecurity, Energy Security, and Emergency Response (CESER)

Mr. Justin John
Executive Technology Director at GE Global Research
General Electric

Dr. Andre Marshall
Vice President of Research, Innovation & Economic Impact
*George Mason University***

Mr. Zach Tudor
Associate Lab Director, National Homeland Security
Idaho National Laboratory

Ms. Lisa Strama
President & Chief Executive Officer
National Center for Manufacturing Sciences

Dr. Xin Sun
Associate Laboratory Director for Energy Science and Technology
Oak Ridge National Laboratory

Mr. Jake Wertz
Director of Cybersecurity Engineering
Lockheed Martin

Dr. Marcey Lee Hoover
Vice President for Research and Partnerships
Purdue University

Mr. Andy McIlroy
Associate Lab Director for Integrated Security Solutions
Sandia National Laboratory

Dr. Prasant Mohapatra
Vice Chancellor for Research
University of California, Davis

Dr. Susan Martinis
Vice Chancellor for Research & Innovation
University of Illinois Urbana-Champaign

Dr. Howard Grimes
Chief Executive Officer, CyManII
University of Texas at San Antonio

Mr. Ken Fowler
Chief Operations Officer and Chief Information Security Officer, CyManII
University of Texas at San Antonio

Dr. JoAnn Browning
Interm Vice President for Research
University of Texas at San Antonio

Dr. Rob Rutenbar
Senior Vice Chancellor for Research
University of Pittsburgh

Ms. Janis Terpenny
National Science Foundation

MEMBERSHIP BY THE NUMBERS:

7 Large manufacturers (i.e., industrial members with more than 500 employees)

10 Small manufacturers (i.e., industrial members with less than 500 employees)

INSTITUTE MEMBERSHIP

Institute members are comprised of companies, academic institutions, and organizations in the manufacturing domain. CyManII offers four membership levels, with different benefits for each level. As of December 2023, CyManII membership is represented by 46 organizations. New members who joined in 2023 are shown in **bold**.

Managing Members (21)

- U.S. Department of Energy
- CESMII: Smart Energy Manufacturing Innovation Institute
- Clemson University
- Dynics, Inc.
- General Electric
- George Mason University
- Idaho National Laboratory
- Indiana University
- Lockheed Martin
- National Center for Manufacturing Sciences
- Oak Ridge National Laboratory
- Purdue University
- Sandia National Laboratory
- Texas Tech University
- University of California, Davis
- University of California, Irvine
- University of Illinois Urbana-Champaign
- University of Pittsburgh
- University of Texas at Austin
- University of Texas at San Antonio
- **Siemens**

Strategic Members (9)

- National Renewable Energy Laboratory
- Rutgers University
- University of Nebraska-Lincoln
- University of New Hampshire
- University of Tennessee
- University of Texas at El Paso
- Veracity Industrial Networks
- Virginia Commonwealth University
- Texas Tech University

Collaborative Members (11)

- Cynalytica, Inc.
- International Society of Automation
- Technology Advancement Center
- Omnigence
- Port San Antonio
- Boise State University
- **Humtown Products**
- **Formlabs**
- The MITRE Corporation
- **Mazak**

Community Members (5)

- **C5MI**
- Association for Manufacturing Technology
- MTConnect
- Nexight Group
- University of Texas at Arlington

21 Academic members (e.g., universities, community colleges)

8 Other entities (e.g., government, national laboratories, non-profits)

46 Total number of members for calendar year 2023

FACILITIES AND RESOURCES

C4M

Located in the heart of Port San Antonio, the Cybersecurity for Manufacturing (C4M) hub is a 17,000-square-foot training and technology demonstration facility that supports manufacturers by providing access to applied research, engineering support, and hands-on workforce training in secure smart manufacturing. Through our partnerships and memberships in 2023, CyManII has grown its capabilities to further enhance our cybersecurity training, including hosting events, hiring an engineering manager, and creating a strong communications link between the hub and Port San Antonio.

MTV

The Mobile Training Vehicle (MTV) provides all the advantages of the Cyber Range but in a remote capacity, meeting SMMs and university students where they are. Team training, individual on-demand labs, and a crisis simulation experience are offered to upskill the workforce in cybersecurity awareness. In 2023, CyManII, in collaboration with the Cyber Warrior Network, created a Cybersecurity eSports League for students at underrepresented high schools in the San Antonio area to participate and learn cybersecurity fundamentals.

San Pedro I

The University of Texas at San Antonio (UTSA) unveiled San Pedro I (SPI), a world-class data science facility that will usher in a new era of high-tech education, research, and innovation in Texas. CyManII has offices in the facility where, according to UTSA President Taylor Eighmy, CyManII and other stakeholders “will attract unique government-university-industry partnerships in the fields of data science, cybersecurity, and national security.” As the data science building evolves, CyManII will continue to meet the needs in the cybersecurity for manufacturing field.

"Mazak's role as a CyManII collaborative partner gives us the opportunity to share the knowledge and expertise we've developed in advanced data protection and cybersecurity. Our proven technologies advance the ability to develop and implement secure technologies required to detect and prevent cyberattacks."

Paul Robinson, North America Manager of Applications Engineering, Mazak

EDUCATION AND WORKFORCE DEVELOPMENT **REPORT**

CyManII's education and workforce development (EWD) initiatives made substantial progress this year, culminating in the award of a $1 million grant from DOE to develop a Cybersecurity Modular Bootcamp. CyManII also successfully trained more than 14,000 incumbent and emerging workforce learners through internal training offerings, as well as our CyManII Sealed training. These trainings were delivered through various modalities, including live sessions, on-demand courses, and experiential training opportunities.

Over 14K Trained!

Number of individuals participating in Institute EWD projects or Institute-led activities:

Calendar Year	*K-12 Participants*	*Post-Secondary Participants*	*Manufacturing Workforce Participants*
2022	*0*	*1,250*	*150*
2023	*1,334*	*2,804*	*10,683*

Number of individuals completing an Institute-aligned professional development certification, apprenticeship, or training program:

Calendar Year	*K-12 Participants*	*Post-Secondary Participants*	*Manufacturing Workforce Participants*
2022	*0*	*0*	*1,400*
2023	*19*	*12*	*14,794*

CYMANII TRAINING

First Classroom Training at New Cyber Range Facility – SPI

CyManII hosted its inaugural training session at the new Cyber Range facility located at SPI at the downtown campus of UTSA. The Cyber Range is a new hands-on learning lab designed to facilitate both individual and team exercises. Led by Joe Mallen, the first class consisted of incumbent workforce members who engaged in experimental learning opportunities including a live fire exercise and a simulation lab.

MTV reveal at SOUTHTEC

In October 2023, CyManII's MTV, the first-of-its-kind for experiential and classroom training, made its debut at SOUTHTEC, an event attended by over 4,500 participants from over 400 companies. At the exhibit, the EWD team demonstrated live learning and group training experiences, as well as individual on-demand workstation training.

CyManII EWD Awarded $1M for Bootcamp

DOE awarded $1 million to CyManII's EWD program to develop the Cybersecurity Modular Bootcamp. This initiative will focus on developing and deploying an operational technology (i.e., industrial control systems [ICS]) bootcamp for SMMs, with an emphasis on training incumbent and emerging workforce members to identify and reduce cyber threats.

CyManII eSports League Pilot Program

Launched in the fall of 2023, the CyManII eSports League began with participation from five high schools in underrepresented communities in San Antonio, Texas. The League offers students the opportunity to compete against one another by playing a cybersecurity-focused videogame over a six-week period, gaining an understanding of how hackers can exploit systems. Hosted inside CyManII's MTV, the League provides all the advantages of our Institute's Cyber Range in a remote capacity. CyManII partnered with the Cyber Warrior Network to develop the content of each interactive game. CyManII will expand the league to 15-20 local high schools in the fall of 2024 and introduce games that teach students about cybersecurity in the manufacturing industry. This will be followed by a national campaign, working with high schools in cities where CyManII has partners.

PARTNER PROGRAMS

CyManII Member Inducted into Inaugural Manufacturing USA Modern Makers Program

Modern Makers are individuals who exemplify the Manufacturing USA mission of securing the future of U.S. manufacturing through innovation, education, and collaboration. The Modern Makers Program is a marketing and communications initiative aimed at encouraging the American workforce, both incumbent and emerging, to pursue career opportunities in the manufacturing sector.

CyManII EWD Partnership with San Antonio Chamber of Commerce (SA CoC)

CyManII developed a partnership with the SA CoC to support the San Antonio Ready to Work Program. As part of this partnership, we have provided learning pathway training to dozens of program participants to upskill the cybersecurity workforce.

CyManII/Amatrol Partnership Established

CyManII established a partnership with Amatrol to develop cybersecurity training content for the CESMII Smart Manufacturing System, as well as the Amatrol Mechatronics System. This partnership will enable hundreds of thousands of learners in the workforce gain the OT cybersecurity skills needed to safeguard their cyber-physical systems.

“Our partnership with CyManII will support its mission to secure and sustain advanced manufacturing in the U.S.”

Nick Graham, Chief Revenue Officer, Formlabs

ENGAGEMENT **REPORT**

Cybersecurity represents not only a financial threat but also a significant national security concern, particularly evident in today's landscape. The evolving threats from foreign adversaries and industry competition have become increasingly sophisticated and complex. In 2023, the United States saw an increase in threats across all manufacturing sectors. The key to mitigating these risks and countering our adversaries is creating partnerships and deep relationships across the manufacturing industry, academia, and the U.S. Government. With SMMs accounting for nearly 99 percent of the U.S.' 600,000 manufacturers, CyManII dedicated 2023 to outreach and collaboration with these enterprises. Continuing to enhance our understanding of the complex threats and challenges posed by cybersecurity requires active engagement in the industry, and CyManII is committed to continuing this momentum in the years to come.

CYMANII EWD ENGAGEMENTS

EWD Presents at HOUSTEX: CyManII had the privilege of speaking at SME's HOUSTEX Conference hosted in Houston, Texas, an event boasting over 3,000 participants from more than 200 Texas-based companies. CyManII's Director of Education and Workforce Development Ty Middleton was a featured speaker on the future of the cyber workforce in the manufacturing sector.

EWD at HI-TEC Conference: Supported by the National Science Foundation's Advanced Technological Education (NSF ATE) program, HI-TEC is a national conference on advanced technological education where secondary and post-secondary educators, counselors, industry professionals, trade organizations, and technicians can update their knowledge and skills. Charged with preparing America's skilled technical workforce, the event focuses on the preparation needed by the incumbent and emerging workforce to work with companies in the high-tech sectors that drive our nation's economy. The CyManII EWD team presented on the future of the OT cybersecurity workforce and participated in several presentations focused on advancements in the manufacturing sector.

EWD Invited to Department of Labor ETA Event: On May 16, 2023, the U.S. Department of Labor (DOL) hosted "ETA Vision 2030: Investing in America's Workforce," a three-day event that connected 500 key stakeholders from across the broader workforce ecosystem. The event, dedicated to leveraging the Biden administration's investments in infrastructure, climate, and advanced manufacturing sectors, focused on developing talent pipelines and creating pathways to good jobs for workers across America. This "invite-only" event was attended by over 300 participants who represented the nation's premier EWD programs, dedicated to executing the National Manufacturing Workforce Strategy. ETA Vision 2030 featured First Lady Jill Biden as one of the keynote speakers.

2023

TSA SCHOOL
Officially opened TSA School of Data Science at SPI

JAN

C4M HUB
Launched C4M Demonstration and Training Hub

HOUSTEX
CyManII EWD attended HOUSTEX Conference

FEB

CYBER RANGE
First Cyber Range training at SPI

MAR

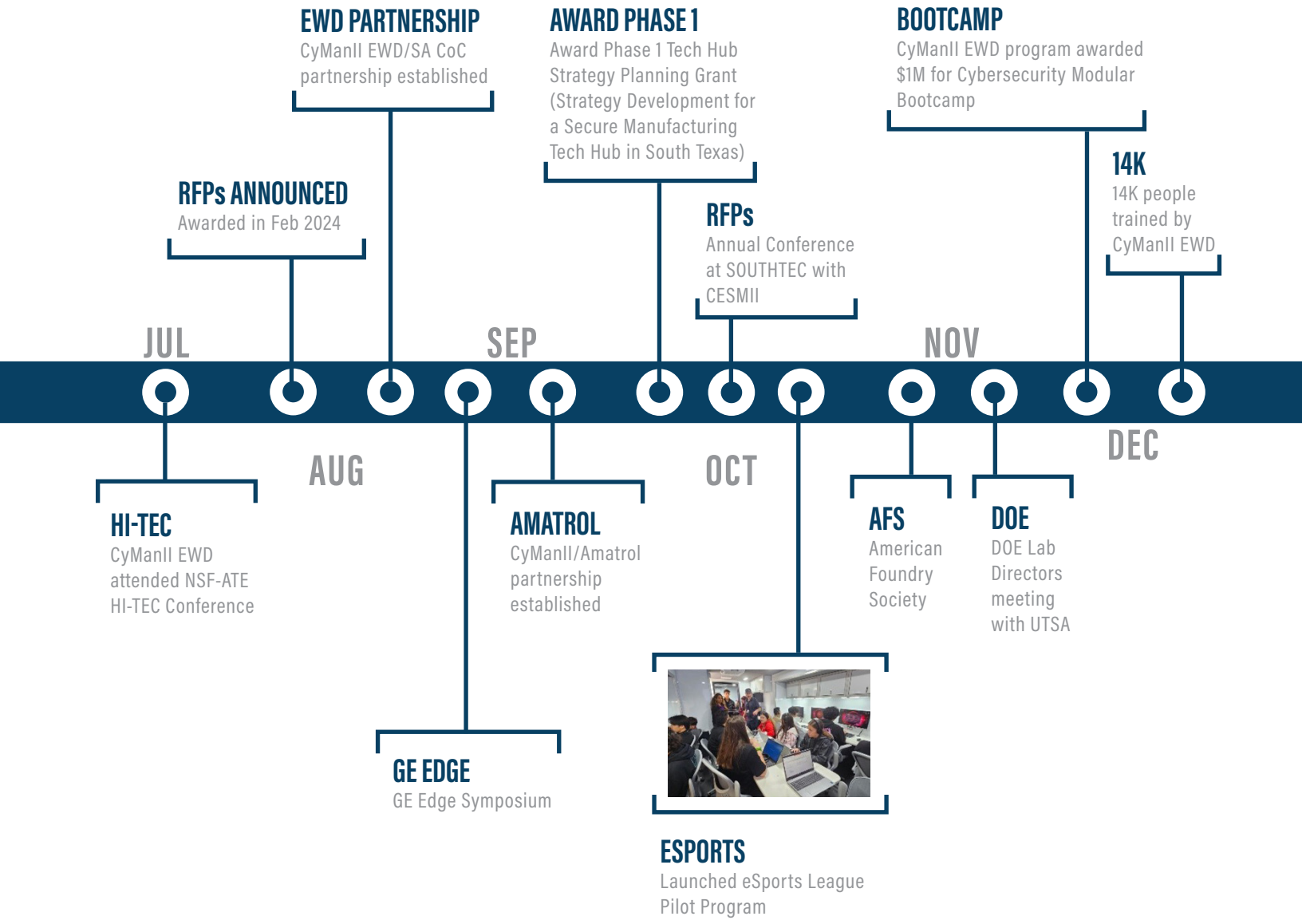
METALCASTING
Participated in Metalcasting Congress 2023

APR

DOL ETA
CyManII EWD attended DOL "ETA Vision 2030" event

MAY

JUN


EWD PARTNERSHIP
CyManII EWD/SA CoC partnership established
AWARD PHASE 1
Award Phase 1 Tech Hub Strategy Planning Grant (Strategy Development for a Secure Manufacturing Tech Hub in South Texas)
BOOTCAMP
CyManII EWD program awarded $1M for Cybersecurity Modular Bootcamp
RFPs ANNOUNCED
Awarded in Feb 2024
RFPs
Annual Conference at SOUTHTEC with CESMII
14K
14K people trained by CyManII EWD
JUL
SEP
NOV
AUG
OCT
DEC
HI-TEC
CyManII EWD attended NSF-ATE HI-TEC Conference
AMATROL
CyManII/Amatrol partnership established
AFS
American Foundry Society
DOE
DOE Lab Directors meeting with UTSA
GE EDGE
GE Edge Symposium
ESPORTS
Launched eSports League Pilot Program

CYMANII PUBLICATIONS AND MEDIA REPORTS

Journals

Keith, Kolton, Krystel K. Castillo-Villar, and Tanveer H. Bhuiyan. "Attack graph-based stochastic modeling approach for enabling cybersecure semiconductor wafer fabrication." Computers & Industrial Engineering 188 (February 2024). https://www.sciencedirect.com/science/article/abs/pii/S0360835224000330.

Conference and White Papers

Shusko, J. W., Weaver, G.A., Hansenbein, J.J., Costa, P. C. G., Castillo-Villar, K. K. "Deciding start rates and cybersecurity investment for semiconductor fabrication facilities under cyberthreat scenarios." In proceedings of the 2023 IISE Annual Conference & Expo, May 21-24, 2023.

Grimes, Howard, Aaron Tantleff, and Alex Misakian. "Recommendations For Managing Cybersecurity Threats in The Manufacturing Sector." Cyber Manufacturing Innovation Institute; Foley & Lardner LLP, September 2023. https://cymanii.org/wp-content/uploads/2023/09/Cybersecurity-in-Manufacturing-Foley-and-CyManII.pdf.

Grimes, Howard, Aaron Tantleff, and Alex Misakian. "So, You Think of Cybersecurity Only as a Cost Center? Think Again." Cyber Manufacturing Innovation Institute; Foley & Lardner LLP, November 2023. https://cymanii.org/wp-content/uploads/2023/11/Cybersecurity-Cost-Center-Think-Again-FINAL.pdf.

In the News

Bryson, Amy. "Making Cybersecurity a Team Sport: CyManII." Society of Manufacturing Engineers, February 10, 2021. https://www.sme.org/technologies/articles/2023/february/making-cybersecurity-a-team-sport-cymanii.

Miller, Jen. "So your manufacturing company was hacked. What's next?" Manufacturing Dive, March 29, 2023. https://www.manufacturingdive.com/news/manufacturing-company-cyber-attack-what-to-do/644403/.

Gottlieb, Zoe. "Local group wins federal grant to advance secure manufacturing." San Antonio Business Journal, October 25, 2023. https://www.bizjournals.com/sanantonio/news/2023/10/25/cymanii-wins-tech-hubs-strategy-development-grant.html.

Powers, Halee. "UTSA's cybersecurity program continues to grow as cyberattacks become more frequent." KSAT-TV, October 27, 2023. https://www.ksat.com/news/local/2023/10/27/utsas-cybersecurity-program-continues-to-grow-as-cyberattacks-become-more-frequent/.

The White House. "FACT SHEET: To Launch Investing in America Tour, the Biden-Harris Administration Kicks off Sprint to Catalyze Workforce Development Efforts for Advanced Manufacturing Jobs and Careers." October 26, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/06/fact-sheet-to-launch-investing-in-america-tour-the-biden-%E2%81%A0harris-administration-kicks-off-sprint-to-catalyze-workforce-development-efforts-for-advanced-manufacturing-jobs-and-careers/.

"UTSA receives $500,000 U.S. Economic Development Administration grant to build Secure Manufacturing Hub in South Texas." UTSA Today, October 24, 2023. https://www.utsa.edu/today/2023/10/story/unviersity-receives-grant-to-build-secure-manufacturing-hub.html.

"TX Secure Manufacturing Hub to Boost Tech Innovation." Industrial Safety and Security Source, November 1, 2023. https://www.isssource.com/tx-secure-manufacturing-hub-to-boost-tech-innovation/.

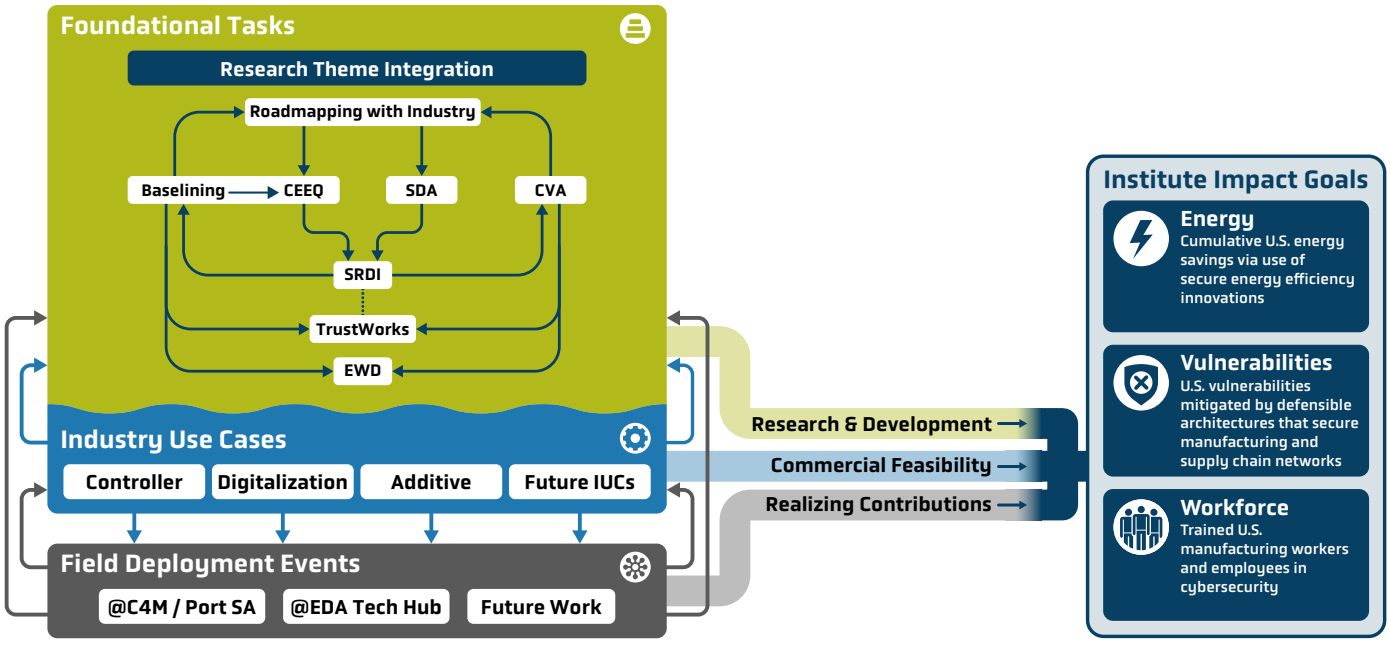
Gordon, Jonathan. "Cyber Risk in Manufacturing – A Closer Look." Industrial Cyber, December 19, 2023, https://industrialcyber.co/analysis/cyber-risk-in-manufacturing-a-closer-look/.

"Each of these projects represents a significant investment into American manufacturing resiliency. By working with CyManII and each of our project partners to build secure and sustainable processes that evolve with new innovations, we can help ensure a robust and cybersecure manufacturing sector here in the United States."

Christopher Saldana, Director
The Advanced Materials & Manufacturing Technologies Office (AMMTO)

RESEARCH **REPORT**

As a Technology Readiness Levels (TRL) 2-6 institute focused on driving a whole-of-nation transformation towards secure U.S. manufacturing, CyManII plays a critical role as a bridge for transitioning best-in-class innovations onto the manufacturing floors of our partners and into critical domestic supply chains. To this end, CyManII's core research teams (Integrated Foundational Technologies: Cybersecurity Energy & Emissions Quantification [CEEQ], Secure Defense Architecture [SDA], Secure Research and Development Infrastructure [SRDI], Coordinated Vulnerability Awareness [CVA]) have focused on developing several key innovations that incorporate fundamental mathematics and physics, laying the groundwork for a comprehensive, integrated approach to cybersecurity. To accelerate the development and deployment of these secure innovations, CyManII's research teams employ IUC projects, pilots, and demonstrations as mechanisms to mature research and to invite industry into the development process as product owners. Each of these IUC partnerships significantly reduce the cycle time between design and deployment, enabling CyManII to rapidly develop the solutions necessary for both SMMs and Original Equipment Manufacturer (OEMs) to integrate fundamental, secure manufacturing technologies into their operations platforms.



CyManII's Foundational Tasks integrate research into IUCs, informed by the Institute's Impact Goals. The graphic depicts three focus areas for IUCs with an additional workstream for identifying future IUC topics. The Field Deployment Events section identifies areas where technology can be deployed to validate IUCs.

CYBERSECURITY ENERGY & EMISSIONS QUANTIFICATION (CEEQ)

This year, CEEQ focused on enhancing the modeling required to calculate cyber ROI. It developed existing machine level models (micro) for sand casting and other additive operations, alongside long-term (macro) models designed to maximize a profit rate. These were mapped by decision variables, objective functions, and constraints for each of the IUCs. Additionally, attack graph models were created using a two-stage model to assess cyber risk and vulnerability paths on various systems, including a Computer Numerical Control (CNC) milling machine.

SECURE DEFENSE ARCHITECTURE (SDA)

In 2023, SDA developed AVOID, a system that analyzes design files en masse to provide early validations of designs and prevent potential malicious alterations (e.g., voids and vertex shifting) that can lead to failing physical parts. This work provides a reference implementation for design and recipe verification before parts are manufactured, with outcomes captured in an analysis CPP.

SDA containerized all passport modules with SRDI and completed the full setup of the containerized CPP framework demonstrated in December 2023. Additionally, the SDA team finalized a reference implementation for the design passport generation application. For this reference implementation, we generate both design and product passports for subtractive and additive manufacturing inside Autodesk Fusion 360.

SECURE RESEARCH AND DEVELOPMENT INFRASTRUCTURE (SRDI)

SRDI's Manufacturing Internet of Things Hub (MITH) is the edge device that securely interconnects manufacturing systems to CyManII R&D applications and CyManII's cloud, policy permitting. As the MITH device has evolved, it has been deployed on hardware from small embedded applications to desktop clusters. In BP3, the SRDI team extended the set of devices by deploying a graphics processing unit (GPU)-enabled edge device using NVIDIA's Jetson Nano devices. The cluster included three GPU's that were shown to train and execute a Machine Learning (ML) model at the edge.

The SRDI team demonstrated how energy can be used to detect attacks on a CNC manufacturing machine during operation, and used SRDI's MITH device to showcase how high-fidelity energy measurements can be used to detect stealthy control injection attacks on CNC machines while manufacturing a part.

SRDI also demonstrated the capability of using Software Defined Networking (SDN) to dynamically send network traffic for inspection and block based on payload content. Prior to this, SDN would only have been used to block certain traffic a priori based on static flow information and not the payload content.

DEVELOPING INDUSTRY USE CASES

This year marked an important turning point for CyManII in developing applications for the technologies described above. Throughout 2024, CyManII research teams will explore these applications by deploying SDA, CPP, CEEQ, and CWE innovations in IUCs focused on the manufacturing of energy controllers, a wide swath of smart manufacturing operations, and additive manufacturing facilities. In 2025, CyManII will initiate a new, expanded round of IUCs to deploy these innovations and more in a new set of critical manufacturing focus areas named in RFPs scheduled for release on September 1st, 2024.

Digital Controllers in Energy

This project will demonstrate industry-relevant security controls surrounding the production and supply chain of ICS such as integrated circuit design, firmware, and associated network communications protocols to ensure digital integrity and supply

chain traceability while improving resilience to a cyber event. Working directly with industry partners in strategy and brainstorming sessions, CyManII developed new metrics to measure energy baselines and identify the data necessary to quantify the energy efficiency and decarbonization ROI when utilizing secure ICS systems. Continuing work in this IUC will include user-friendly microkernel implementations for advancing the security of ICS and provenance tracking for the manufacturing of energy controllers.

Additive Manufacturing Supply Chain

This project will demonstrate how an additive manufacturer can implement security provenance tracking of their products' digital thread to ensure product integrity and supply chain traceability in the production of both components and system, while reducing costs. Working directly with industry partners, CyManII research teams identified the software and hardware requirements and implementation frameworks for instrumentation to collect data on product integrity, quality, and energy signature of a 3D printing process. The research teams simulated an attack against the G-code of the 3D printing machine and developed a numerical experimentation on different synthetic attack graph sizes and security investment amounts. Continuing work in this IUC will include testing the approach for attack graph generation in an advanced manufacturing environment.

Digitalization of Legacy Systems

This project will demonstrate the application of secure digitalization technologies in an SMM's operation, while identifying and developing best practices and implementing security controls under a CIE paradigm. Working directly with industry partners, CyManII research teams drafted optimization models (i.e., tool, facility, and supply chain levels), defined the energy measurement sensors needed for energy baseline and CEEQ energy efficiency analysis, developed a CyManII Attack-Defense Annex (CADA) model and attack paths for the SMM's manufacturing systems, and prepared to deploy a MITH cluster in an SMM partner's operations to support future IUC work. Continuing work in this IUC will include using the CEEQ sensor architecture and models in combination with the MITH cluster to enable both energy baselining with real-time current monitoring and secure design transfer to manufacturing systems.

“CyManII applies REAL TIME 360 IT PROTECTION surrounding your IT investment. Not having them fully integrated into your system is like holding onto a bare live wire and thinking you won’t get shocked.”

Mark Lamoncha, CEO & President, Humtown

STRATEGY **REPORT**

SUSTAINABILITY STRATEGY

As CyManII continues to advance its research and transition along the TRL spectrum, new opportunities for sustainability continue to emerge. In 2023, CyManII entered its third year and began operationalizing the strategy for growth and sustainability outlined in the TrustWorks Sustainability Roadmap. This includes pursuing cultivated funding opportunities, participating in open federal funding opportunities, advancing services and solutions, and furthering development in the standards and certification space.

Funding Opportunities

Outside of our institutional funding contract, CyManII successfully secured additional opportunities:

U.S. Department of Energy-Directed Funding – Education and Workforce Development: CyManII applied for competitive funding to support continued EWD activities. The DOE awarded CyManII $1 million to develop and deliver an OT Cybersecurity Modular Bootcamp for manufacturing professionals.

State of Texas Legislator Funding: CyManII received $2 million in annual allocations from the State of Texas to further develop and deliver workforce training to Texas-based manufacturers. These resources support our regional outreach efforts such as the MTV and the Cyber Range.

U.S. Economic Development Association Regional Technology and Innovation Hub Funding: CyManII secured a $500,000 Strategy Development Grant from the EDA to establish a Regional Technology Hub focused on advanced manufacturing and supply chain security. This initiative includes the establishment of a Texas-based consortium focused on translating these groundbreaking innovations into commercial-ready technologies. The goal for the South Texas Secure Manufacturing Tech Hub is to enable manufacturers to secure their digital manufacturing processes across the supply chain with cybersecure technologies and a cyber-ready workforce.

Secure Manufacturing Tech Hub

The Tech Hub aims to:

1. Cultivate a skilled and ready workforce capable of supporting a secure advanced manufacturing ecosystem.
2. Translate cutting-edge cybersecurity and advanced manufacturing innovations into commercial-ready solutions for SMMs.

Services and Solutions

Although CyManII primarily focuses on addressing TRL 2-6 research under the DOE cooperative agreement, it recognizes the need to provide front-facing services and solutions to support manufacturers on their digitalization journey. The capacities at C4M and our innovative EWD programs play a key role in this outreach. These types of offerings are key to our long-term sustainability strategy, and will be further developed over the next few years, with market demonstrations planned for 2024 and 2025.

Certification

As outlined in our Sustainability Strategy, the development of cybersecurity certification programs is critical to our outreach, impact, and long-term sustainability. Ensuring cyber readiness has historically posed a challenge for the industry at large and, like other sectors, is generally a function of accepted standards and guidelines. In the manufacturing space, where digitalization has rapidly evolved over the last decade, such standards are relatively nascent. As industry thought leaders in ICS/OT and process cybersecurity, we are paving the way of establishing these conventions alongside other leaders in the field. We see the potential to establish uniformity and best practices for the cybersecurity of people, processes and products.

People

Does the workforce have the knowledge, skills, and abilities to implement cybersecurity practices and principles in their jobs? In addition to our own CyManII Sealed training certifications, we are collaborating with the Smart Automation Certification Alliance (SACA) to develop and introduce CyManII-informed credentialling to SACA's tremendous manufacturing training library.

CYMANII ROADMAP UPDATE

As we enter our third period of roadmapping, CyManII is excited to share an update on how future iterations of the Roadmap will guide the Institute to innovate, transform, and inspire secure domestic manufacturing technologies, processes, and partners. The forthcoming iterations of the Roadmap are crucial for ensuring that CyManII researchers remain informed and focused on the most pressing needs of our nation's manufacturers, integrating CyManII's vision and perspective into the innovation pipeline and fostering a future **Secure.*TOGETHER*.** manufacturing ecosystem with principles that are rooted in trust.

In the first Roadmap, we established CyManII's core research teams tasked with diving into the fundamental technical underpinnings of the challenges and opportunities that U.S. manufacturers face when approaching and navigating the digital transformation. We also outlined a vision and an integrated technical approach to steer our manufacturing stakeholder ecosystem towards a more secure and competitive future state. In our 2023 Roadmap update, we outlined the Institute's progress in research, deployment, and partnerships, providing insights into our vision and integrated technical approach (i.e., IUCs) for transitioning fundamental innovations out of the labs of top research teams across the country, across the proverbial innovation valley of death, and into the manufacturing operations platforms of our development partners.

This new mechanism, the IUC, is also the tool that allows CyManII leadership to execute a comprehensive strategy for driving our manufacturing partners and their larger domestic supply chains to **Secure.*TOGETHER*.** Subsequent Roadmaps will explain how CyManII will focus its innovation pipeline and expand its portfolio of IUCs and their secure manufacturing ecosystem. Like all roadmaps, it will act as a critical strategy and information sharing conduit, serving to connect industry with CyManII's core research and thought leaders.

The next CyManII Roadmap update will enable the Institute to identify and assess the most critical U.S. manufacturing sectors, processes, and technologies to determine the highest priority focus areas for CyManII researchers to develop and deploy innovations in partnership with our secure manufacturing ecosystem and IUC pilot partners. This Roadmap will allow CyManII to designate key focus areas, within which we will initiate a new, expanded round of IUCs to deploy SDA, CPP, CEEQ, and CWE innovations, and more. These critical manufacturing focus areas will be named in RFPs scheduled for release after the roadmapping research is completed. Future CyManII IUCs and associated RFPs will be identified and defined in future Roadmaps and strategically selected to quickly and effectively transform the U.S. manufacturing industry.

“Siemens’ partnership with CyManII will help bring industry and infrastructure online. To do this successfully, cybersecurity is an integral part of our mission, and Siemens Technology is at the forefront of developing innovations that strengthen the nation’s competitiveness in the critical area of cybersecurity for manufacturing."

Dave Rapaport, Head of U.S. Research and Collaboration Management, Siemens

CYMANII IN **YEAR 4**

Protecting U.S. manufacturing while promoting energy efficiency and decarbonization has become imperative for both economic prosperity and national security, and CyManII is leading the way with ambitious strategic objectives.

Security must be embedded within the entire manufacturing supply chain to ensure the creation of products that are secure by design from inception to production. CyManII offers defensible architectures that are verifiable, integrate cyber-physical energy objectives, and span the entire design-build lifecycle. At the same time, CyManII's innovations help manufacturers address global challenges associated with energy efficiency and decarbonization by providing a verifiable ecosystem where embodied energy and emissions for components and products are tracked and traded across the manufacturing supply chain, ensuring a secure digital transformation.

The economic leaders in manufacturing will be those capable of simultaneously addressing cybersecurity, energy, and the environmental security and resilience of their manufacturing industrial base, benefiting both economic and national security. This requires both large OEMs and SMMs to work within an ecosystem where security and efficiency tools are Energy-Efficient (ε), Pervasive, Unobtrusive, Resilient, and Economical—CyManII's ε-PURE philosophy, transforming security technology from a cost center into an ROI and market enabler.

Working collaboratively with DOE, we released up to $4.7 million in grant awards in 2023 to enhance the cybersecurity landscape within U.S. manufacturing. These RFPs will directly support the development of IUCs in 2024, advancing projects related to ICS, secure industrial digitization, and industrial additive manufacturing. We look forward to issuing additional RFPs and working with our partners in 2024 and beyond.

Even as these IUCs begin to demonstrate the potential applications of CyManII technology, we will maintain our strategy of broader engagement with our industry partners to gain insights from various sectors, identify major cybersecurity concerns and vulnerabilities in manufacturing, and develop new ideas for IUCs and grant opportunities.

Cybersecurity is a team sport. We look forward to continuing to work with our partners in industry, academic, and government to make U.S. manufacturing **Secure.*TOGETHER***.


SLM


ETAL POWDER
WORKS


Manufacturing USA
2022 Network Meeting


TCMA
INTERNATIONAL TRADE CENTER


CYMANII
the cybersecurity
manufacturing
innovation institute
cymanii.org