The Cybersecurity Manufacturing Innovation Institute

Secure. TOGETHER.

Summary of Foundational R&D for RFP

Dr. Howard Grimes
CEO, CyManII
Howard.Grimes@cymanii.org

Wayne Austad
Chief R&D Officer, CyManII
Wayne.Austad@cymanii.org

This presentation does not contain any proprietary, confidential, or otherwise restricted information
Challenge & Strategic Teaming Approach
MANUFACTURING IS undergoing a **DIGITAL TRANSFORMATION**.

**Vulnerability attack surfaces are increasing exponentially**

- **2010**: 6.8 billion
- **2015**: 12.5 billion
- **2020**: 25 billion

**Smart Devices**

- **2010**: 20%
- **2015**: 25%

**World Population**

- **2010**: 6.8 billion
- **2015**: 7.2 billion
- **2020**: 7.6 billion

**Annual energy savings by manufacturers who digitize.**

- **20%**

**Manufacturers are digitizing at twice the rate of other businesses.**

- **2x**
Today’s “Secure Architectures”

Presently a **Misleading terminology**

- Connotes a conjoining of *perimeter defense* + *data security*
- Poor security controls that are applied only to a **limited aspect** of operations or supply chain
- Little, or no, context of **real physical** world consequences
- Often aligned to **compliance** requirements only
The Digital Engineering Lifecycle must be addressed across the entire supply chain

- Every operation, machine, and person is a “node” in this digital design (supply chain is seamless with operations)
- Every node is captured in a cyber-physical identity (passport) that is used for:
  - Guarantees of physical functions
  - Linkage of security to product quality and energy / emissions efficiency (embodied energy)
- Verifiable security properties that are extensible to multiple domains

Cyber-Physical Passport: makes your supply chains “born qualified” and “rooted in trust”
Cyber attackers are becoming increasingly funded and resourced, and therefore more sophisticated and agile.

The risk we face is that we are not able to maintain the necessary agility needed to meet these threats.

We must be more agile than our adversaries.
CyManII’s Vision

is to secure U.S. manufacturers as they digitize by fortifying their physical systems with embedded cybersecurity and energy-efficient solutions.
Secure the digital thread

- Build defensible architectures
- Create identity-centric cyber-physical passports
- Secure supply chain for decarbonized ecosystem

Secure. TOGETHER

- Partner across industry’s supply chain
- Cooperate across Govt stakeholders within:
  Manufacturing Sectors
  Critical Energy Infrastructure
  Data sciences and beyond …

Create a cyber-informed workforce

- Focus on OT / ICS security
- Leadership on CIE
- Empower current workers
- Expand emerging workforce
Our Team

300+ technical staff scientists and engineers with over 100 FTE developing SDA and other secure by design products and architectures

Our Members

60+ members from industry, DOE Laboratories, non-profits, other MII’s, and universities
CyManII’s Expansive Membership Network
Foundational Results & Demonstration Project Achievements
Secure Defensible Architecture (SDA)

Unify security across the digital thread of design, build, deliver for industries of all sizes

Integrated Model of Automation & Supply Chain
- Perimeter defenses insufficient in modern digital design lifecycle
- We treat Automation as nodes in Supply Chain network

Framework for Security & Efficiency Across “Sectors”
- Digital identity = physical + cyber + energy (Cyber-Physical Passport)
- Automation activities validated across supply chain

Agile, Adequate, & Consequential Formalism to Validation
- Targeted formal methods and evidential basis for design & implementation
- Continuous Integration/Deployment (CI/CD) in manufacturing context
THE Cyber-Physical Passport enables digital provenance tracking through **verifiable security guarantees**.

**Traceability across supplier boundaries.**
Using a global ledger as well as physical and *virtual* watermarks, the CPP follows a product through its value chain, crossing suppliers and staying with the end product.

**Verification of the digital thread.**
Formal verification methods are used to continually assess the critical code along the product’s lifecycle for accuracy and evidence of compromise.

**Tamper-proof ledger.**
The data captured in the CPP is protected and anonymized with use of a unique hash and permissioned blockchain where entities logging transactions are first authenticated.

**Improved protection & system hardening.**
A secure manufacturing architecture along with a multi-physics digital twin provide enhanced cyber protection and high-fidelity monitoring.
Results to Date: A key concept in SDA is automatically deploying a Cyber-Physical Passport (CPP) to support system hardening, provenance tracking, process verification, and attack monitoring:

- Needed both locally at the manufacturing site and across companies along the product's supply chain.
- CyManII demonstrated the CPP on a CNC’s aluminum parts productions and verification of the parts’ digital authenticity against intended design (@ONRL MDF).

Future Work: Expand SDA framework and tools to support multiple innovations through Industrial Use Case pilots.

- Additive Manufacturing
- Smart Manufacturing enterprise (CESMII)
- Energy components supply chain
Secure Research and Development Infrastructure (SRDI)

**Inherently** incorporates security, agility, and automated updates

- **Innovation-independent** ecosystem to automate adding cybersecurity across “domains”
- **Rapidly share innovations** between researchers and product owners for collective benefit
- **Secure build chain** with code quality and security checks
- **CI/CD**: Continuous integration/continuous deployment
- **Legacy** protocols secured as new verifiably secure architectures incrementally developed and deployed
- **Local/scalable compute** and secure storage supporting new secure architectures, whitelisting, and enforcement tools

Enable, **accelerate**, and **securely share** innovations across industry partners
SRDI Project Update: Secure Pilots at ORNL MDF

Results to Date: SRDI provides the secure development environment needed to accelerate, integrate, and validate innovations.

- CyManII architected and operationalized key features of SRDI, with secure FedRAMP cloud hosted at UTSA linked to ORNL’s Manufacturing Demo Facility (MDF).
- SRDI was used to conduct **12 different demonstrations** of how it can be used to support secure research.

Future Work: Expand research nodes to additional partners, additional code check tools, **Industry Use Case** integrations
Cybersecurity Vulnerability Challenge
Beyond Just Awareness and Patching ...

Challenge:
• Vulnerability trends significantly favor the attackers, present systems are not "defensible".
• If we continue to reactively chase and patch vulnerabilities, we will “lose the war” for national & economic security.
• Manufacturing more behind in patching than general IT sector.

Current defenses are orders of magnitude behind:
- 10’s days vuln-to-exploit, 100+ days to patch, 200+ days to detect
- 10’s active vulnerability instances / device, 100-1000 latent vulnerabilities
- 100x the cost to fix in implementation vs design

New Approach:
• Identify Cyber Weakness Enumerations that capture thousands of vulnerabilities at a time (1:1,000+)
• Create methods and tools that can systematically identify and eliminate/mitigate weaknesses earlier in lifecycle

4/2018 100k CVEs, ~600 CWEs
4/2023 214k CVEs, 933 CWEs
Across 1,063,482 platforms
100s-to-1000s : 1 of #CVEs to #CWEs
CVA Project Update: Define Fundamental Cyber Weaknesses

Results to Date: Cyber Weakness Enumeration (CWE) is a method for grouping classes of cyber vulnerabilities (CVEs) according to common threats and features.

- Established a **Special Interest Group** with MITRE to develop new CWEs specific to ICS/OT environments (initial 20).
- Developed **CyManII Attack Defense Annex (CADA)** to proactively investigate and systematically eliminate/mitigate weaknesses

Future Work: Structure CWEs to support **formal methods approaches for automated “discovery”** and mitigation earlier in the design-implement-operate lifecycle.

- Creates more coordinated approach Vulnerability Awareness (CVA).
- Applicable long term to both new ICS/OT CWEs and past IT CWEs.
Creating Consequential Cybersecurity-ROI

CEEQ: Transform from cyber “cost center” to an ROI-enabler

Maximize Production, Quality, & Profit margin

Maximize Intelligent Efficiency
Maximize Production
Minimize Risk

Analysis
Modeling
Optimization

Modular & Extensible Approach:
- Cybersecurity risk and impact measures
- Embodied energy and emissions quantification
- Data-driven, informed decisions, all trackable & verifiable

Create a secure verifiable ecosystem for energy efficient and decarbonized supply chains

CEEQ = Cybersecurity Energy & Emissions Quantification
Impacts to Date: Developing Cybersecurity Energy & Emissions Quantification (CEEQ) approach with industry input and testing on physical systems.

- One use case modeled fluid catalytic cracking in an oil refinery against both energy and security parameters to achieve **12% energy savings** with secured digitization.
- Energy flow was modeled throughout the process, optimal head exchanger temperature was calculated, developed method to detect ransomware impacts.

Future Work:
- Expand SDA’s CPP & CEEQ methods/tools across variety of manufacturing sectors and processes.
- Create a secure **verifiable ecosystem** for energy efficient and **decarbonized supply chains**.
Workforce Development

Why 1 million workers?

We must aggressively reach the growing workforce with training that scales.

13 million manufacturing workers in March 2023

7.6% Of the US manufacturing workforce
TrustWorks Update: Cybersecurity Training Manufacturers

Results to Date: Cybersecurity workforce training specific to manufacturing ICS/OT environment is in short supply.
- Efforts focused on developing novel cybersecurity training geared specifically toward manufacturers.
- Includes new asynchronous online content, in-person, virtual reality, and cyber range experiences.
- Piloted 1st of several Regional Hubs (C4M) with state of Texas funds for workforce / economic development.
- Developed a nation-wide network and a “CyManII Sealed” program to partner and scale for impact.

Future Work: Scaling in quantity of courses, regional hubs, and proactive impacts as SDA is advanced.
- Meet SMMs where they (& technology) are at now.
- Prepare for future Secure Defensible Architectures.
- University of Texas System-wide curriculum.