Dear Colleague,

CyManII is actively pursuing new initiatives to secure manufacturing systems and processes, with a specific emphasis on the entire critical minerals, materials, and manufacturing (CM3) value chain. Additive and subtractive manufacturing, electronics fabrication, and critical-material processing are highly complex processes that play a vital role in national and economic security, and the adversaries targeting them are getting more sophisticated.

Throughout the years, CyManII developed multiple security mechanisms under the secure-defensible architecture, from digital provenance (a.k.a., cyber-physical passports) collection and analysis within automation nodes and across supply chains, to targeted formal modeling and verification, to manufacturing systems monitoring and digital twins, and more. Given the recent evolution of AI technologies, CyManII will expand its focus to include AI-driven cyber-informed resilience measures that prevent adversary access and, more importantly, counter subtle attacks that undermine manufacturing integrity, such as signal manipulations affecting product quality, operational technology (OT) intrusions that covertly steal process intellectual property (IP), and high-impact cyber incidents.

AI is essential for advancing cybersecurity in manufacturing, where cyber-informed resiliency engineering proactively designs systems to anticipate breaches and uses engineering controls to minimize impact. Our approach integrates AI to automatically generate tailored cyber-informed resilience plans for manufacturing processes, deploy live AI advisor agents within facilities to monitor operations and advise operators in real time, and extend these capabilities throughout the supply chain.

Purpose of this Letter

This dear colleague letter (DCL) helps us find collaborators to build an AI-enabled, cyber-informed resilience capability for manufacturing. Cyber-informed resilience means directly engineering manufacturing processes—including control loops, interlocks, and safety logic—such that any physical harm that an adversary attempts to cause is both hard to accomplish and quickly detected. This approach goes beyond traditional network defenses by making attacks on the process itself difficult and visible. Artificial intelligence (AI) is strategically integrated where its application is most effective: constructing process models, generating comprehensive resilience plans, and continuously monitoring operational activities. In short, we want to combine cyber-informed engineering with AI to achieve these capabilities:

(C1) characterize and model how processes are meant to behave, in both cyber and physical terms; connect process physics and cyber security formalisms.

(C2) turn those characterized models into verified cyber-informed resilience plans; and

(C3) deploy these plans as AI advisor agents that monitor, detect, diagnose, and offer guidance on how to respond to cybersecurity events in industrial setting.

We extend that AI-enabled, cyber-informed resilience capability across the supply chain, ensuring every node maintains integrity and that material quality and supply chain resiliency.

Topics

We're looking for collaborators with genuine expertise and active research in the areas below that CyManII can build on. You do not need to address every topic, we would rather see a focused response in something you know deeply than broad coverage.

The topics follow the three capabilities above. Topics 1 and 3 serve **(C1)**, characterizing how a process is meant to behave in cyber and physical terms. Topics 2 and 4 serve **(C2)**, generating resilience plans and proving them sound before they go live. Topics 5, 6, and 7 serve **(C3)**, fielding those plans as advisor agents that operators can use under attack.

1. Cyber-Informed Engineering (CIE) for Manufacturing in Critical Minerals, Materials, and Finished Products.

Cyber-informed engineering (CIE) (Wright et al., INL, 2023) is foundational to this program, and we would love to see how you've applied its principles in critical industrial manufacturing settings. Examples of relevant expertise include, but are not limited to:

- Applying CIE consequence-driven design to manufacturing, from additive and subtractive manufacturing to electronics fabrication and critical-material processing, pinpointing the worst-case consequences of an attack on a given process (e.g., lithium cell voltage manipulation, sintering furnace atmosphere compromise) and engineering controls that close the cyber pathways to them.
- Applying CIE engineered controls and design patterns to OT environments—Programmable Logic Controllers (PLCs), safety instrumented systems (SIS), and Supervisory Control and Data Acquisition (SCADA)—in CM3 processes.
- Building CIE-aligned design reviews, threat-modeling frameworks (e.g., STRIDE for cyber-physical systems), and tradeoff-analysis tools for CM3 processes.

2. AI-Driven Cyber-Informed Resilience Plan Generation for Manufacturing Processes and Supply Chains

We are interested in AI frameworks that read process and control specs, security configurations, architectural diagrams and threat intel to generate structured, sound resilience plans for these facilities. Examples of relevant expertise include, but are not limited to:

- Developing multimodal large language model (LLM) architectures that use multi-sourced process and control knowledge, grounded in CIE consequence analysis to prioritize cybersecurity measures by potential impact.
- Building ontology-driven models of process control architectures—control loops, interlocks, safety instrumentation system (SIS) logic solvers, and their connectivity—so AI can reason about attack surfaces and how consequences propagate.
- Building AI frameworks that read supply-chain and logistics systems, electronic chain-of-custody records, and inter-facility OT exchanges to generate resilience plans across multi-site operations, in line with Dept of Energy Office of Critical Materials & Energy Innovation (CMEI) goals for securing domestic supply chains.

3. Physics-Informed AI Models

We seek high-fidelity models of unit operations to set quantitative baselines of behavior—so you can prevent adversarial deviations or catch those that slip past conventional threshold alarms. Examples of relevant expertise include, but are not limited to:

- Building physics-informed neural networks (PINNs) and hybrid physics-based/data-driven models for manufacturing processes.
- Developing multi-scale digital twins from atomic/thermodynamic phenomena through unit-operation dynamics to plant-level balances, calibrated from historians with quantified uncertainty.

4. Formal Methods for Cyber-Physical Security Logic

We are interested in formal methods that prove AI-generated protection specs are correct, complete, and safe relative to the models and assumptions before they go live. Examples of relevant expertise include, but are not limited to:

- Applying model checking, temporal logic, and automated theorem proving to verify safety, liveness, and security properties across all reachable states for CM3 processes.
- Developing formal interaction contracts between AI agents and process control systems, to prevent unintended or unsafe behavior when agents act under attack.
- Developing engineering tools to support the application of formal methods to critical manufacturing processes and supply chains.

5. Anomaly Detection, Threat Attribution, and Cyber Incident Characterization

We are interested in real-time detection that spots process anomalies from cyber intrusion and tells adversarial manipulation apart from equipment wear, sensor faults, and normal variability. Examples of relevant expertise include, but are not limited to:

- Developing multivariate anomaly detection and causal inference systems for root-cause attribution, focused on attack patterns relevant to CM3 processes such as lithium extraction and permanent magnet manufacturing .
- Developing systems that detect slow, covert quality degradations in CM3 processes.
- Building sensor fusion and data validation under sensor failure, spoofing, or OT network disruption, keeping situational awareness in line with CIE defense-in-depth.

6. Deployment of AI Agents in Live Manufacturing OT Environments

We want practical ways to deploy AI-generated advisory logic into live facilities—with real-time performance, validated safety integration, and solid lifecycle management. Examples of relevant expertise include, but are not limited to:

- Deploying edge AI inference on constrained OT hardware (PLCs, controllers, historian gateways, edge nodes) with deterministic latency.
- Developing model compression, quantization, and hardware-aware optimization for embedded OT controllers, without giving up detection fidelity or real-time performance.
- Deploying pipelines for OT agents—shadow-mode testing, staged rollout, operator-in-the-loop validation, and authenticated rollback that meets both cybersecurity and safety rules.

7. Human-AI Teaming and Operator Situational Awareness

We care about human-AI interfaces that sharpen, rather than blunt, operator awareness and judgment under attack—true to CIE's human-factors pillar. Examples of relevant expertise include, but are not limited to:

- Developing explainable AI for control engineers and operators—plain-language attribution, causal process-cyber diagrams, and uncertainty shown in actionable form.
- Developing human-factors designs for control rooms that keeps operator trust well-calibrated under time pressure, novel attacks, and degraded sensors.

Response

We're especially keen on small, highly focused efforts that bring real depth in one or two of the topics above. Please cut/paste from existing materials, links, and bullet lists if needed. A timely, focused response is preferred over a comprehensive but delayed one.

- A 1-page cover letter (PDF) that includes the team details
  - Optionally, include a public link to your organization, team, CV, or Google Scholar.
  - Optionally, note current directly relevant sponsored research or relevant funding.
  - Include a table that informs what topics/capabilities (including new **relevant** ones that you propose) you respond to:

Capability	Topics	Expertise	CM3 Process
C1			
C2			
C3			
<new capability>	<new topic>		

- A maximum 4-page response document (PDF) that includes:
  - Exceptional or unique experience directly relevant to one or more topics in this DCL, including representative publications, fielded systems, datasets developed, or CIE implementations completed.
  - Responses to the specific topics for which your expertise is strongest. Do not feel bound to the exact tools or technologies named; if you believe alternative approaches better serve the stated goals, please explain why.
  - What might we be missing? Topics, capability gaps, or enabling technologies not addressed in this DCL that you believe are critical to achieving robust AI-enabled cyber protection for critical mineral manufacturing on a national scale.
  - **Any relevant testbeds, datasets, OT laboratory environments, AI toolkits/frameworks, capabilities that were not captured, or pilot-scale process platforms you have or could contribute to the collaboration**.

Please respond to: submissions@cymanii.org by **August 15th, 2026**. This DCL is issued for information and planning purposes only and does not constitute a solicitation for proposals or a commitment to fund any specific work.

Key References

- U.S. Department of Energy, Office of Critical Minerals and Energy Innovation (CMEI). https://www.energy.gov/cmei/office-critical-minerals-and-energy-innovation
- Notice of Funding Opportunity: Critical Minerals and Materials Accelerator, https://www.energy.gov/cmei/ammto/critical-minerals-and-materials-accelerator-0
- U.S. Department of Energy. "The Genesis Mission: Transforming Science and Energy with AI." DE-FOA-0003612 (March 2026). science.osti.gov.
- Department of Energy. "National Cyber-Informed Engineering Strategy." CESER, 2022.
- Wright, V.L. et al. "Cyber-Informed Engineering Implementation Guide." Idaho National Laboratory, September 2023. OSTI:1995796. https://www.osti.gov/biblio/1995796
- Office of Critical Minerals (CM3), Materials, and Manufacturing, https://www.energy.gov/cmei/office-critical-minerals-materials-and-manufacturing
- Cyber-Informed Engineering (CIE) – Engineered Controls Database and Use, https://www.osti.gov/biblio/3006995