Reliable and Resilient Digital Manufacturing

R2DM3 - 2024

(APRIL 18 – 19, 2024)

Sponsors:

NSF

IEEE

Organizers:

Dr. Nikhil Gupta
Dr. Ramesh Karri
Dr. Nektarios Tsoutsos

NYU TANDON SCHOOL OF ENGINEERING

UNIVERSITY OF DELAWARE

Keynote Speakers

Dr. Wayne Austad
Cheif R&D Officer
CymanII, Idaho National Laboratory

Mr. Zachary Tudor
Associate Laboratory Director
Idaho National Laboratory

Dr. Gaffar Gailani
Program Manager
NASA

Dr. Jian Yu
Convergent Manufacturing Lead
DEVCOM Army Research Laboratory

Dr. Bruce Kramer
Senior Advisor
Division of Civil, Mechanical and Manufacturing Innovation
National Science Foundation

The Workshop Schedule

Day 1, April 18, 2024

8:30-9:00	Breakfast		
9:00-9:10	Welcome	Nikhil Gupta	
9:10-9:20	Welcome	Katsuo Kurabayashi	NYU MAE Department Head
9:20-10:20	Keynote	Wayne Austad	CymanII, Idaho National Laboratory
10:20-10:40	Invited	Steve Feiner	Columbia University
10:40-11:00	Coffee Break		
11:00-12:00	Keynote	Zachary Tudor	Idaho National Laboratory
12:00-1:00	Lunch		
1:00-2:00	Keynote	Gaffar Gailani	NASA
2:00-2:20	Invited	Narasimha Reddy	Texas A&M University
2:20-2:40	Invited	Nektarios Tsoutsos	University of Delaware
2:40-3:00	Coffee Break		
3:00-3:20	Invited	Gabriela Ciocarlie	CymanII
3:20-3:40	Invited	Michael Powell	NIST
3:40-4:00	Invited	Aslam Sherule	MITRE
4:00-5:00	Panel Discussion		

The Workshop Schedule

Day 2, April 19, 2024

8:30-9:00	Breakfast		
9:00-9:20	Welcome	Nikhil Gupta	
9:20-10:20	Keynote	Jian Yu	Army Research Laboratory
10:20-10:40	Invited	Shamik Das	MITRE
10:40-11:00	Coffee Break		
11:00-11:20	Invited	Ashif Iquebal	Arizona State University
11:20-11:40	Invited	Adarsh Krishnamurthy	Iowa State University
11:40-12:00	Invited	David Paredes	ASTM
12:00-1:00	Lunch		
1:00-2:00	Keynote	Bruce Kramer	NSF
2:00-2:20	Invited	Dan Li	Clemson University
2:20-2:40	Invited	Chinmay Hegde	New York University
2:40-3:00	Coffee Break		
3:00-3:20	Invited	Nikhil Gupta	New York University
3:20-3:45	Closing session		
3:45-4:15	Makerspace Visit		

Table of Contents

Keynote Presentations: Page #

Invited Presentations: Page #

Keynote Presentation

CyManII: The Cybersecurity Manufacturing Innovation Institute

Dr. Wayne Austad

CTO, National & Homeland Security, Idaho National Laboratory Chief R&D Officer, Cybersecurity Manufacturing Innovation Institute

The Cybersecurity Manufacturing Innovation Institute (CyManII) is a Manufacturing USA national research institute with major leading research universities in cybersecurity, smart and energy-efficient manufacturing, and deep expertise in research and development, supply chains, factory automation, and workforce development. Led by The University of Texas at San Antonio, CyManII leverages the strongest Department of Energy (DOE) National Laboratories in this area, with Oak Ridge National Laboratory leading the nation in advanced manufacturing, Idaho National Laboratory leading in cybersecurity of industrial control systems, and physical infrastructure, and Sandia National Laboratory leading the nation in cybersecurity of supply chain management. Funded by the DOE, CyManII aggregates the most advanced research institutions in revolutionary manufacturing, securing automation and supply chains, workforce development, and cybersecurity. The research team brings to bear the most powerful expertise and infrastructure needed to ensure the digital transformation that will continue to propel the U.S. in innovative research in manufacturing for decades. The presentation will discuss the fundamental research challenges in cybersecurity outlined in our national roadmap, and a summary of CyManII's Secure Defensible Architecture, Shared R&amp;D Infrastructure, Cybersecure Energy and Emissions Quantification, and TrustWorks national workforce development efforts. https://cymanii.org/

Speaker Bio:

Wayne Austad has worked at INL for over 32 years building and executing impactful national security programs. As CTO for National &amp; Homeland Security Directorate he: 1) Acts as Chief R&amp;D Officer for CyManII to create economically viable and pervasive cybersecurity in manufacturing automation and across its supply chain; 2) Leads INL's Secure &amp; Resilient Cyber Physical Systems initiative to formalize and scale the science and practice of Cyber-Informed Engineering for infrastructure resilience; 3) Provides leadership and strategy for the cooperative R&amp;D, infrastructure, and innovation partnerships needed to launch initiatives that address national challenges. Previously, Wayne led efforts to build INL's Cybercore Integration Center and create an enduring cybersecurity innovation hub for the nation&#39;s critical control systems. Cybercore tackles the grand challenges in control systems security through collaborative, interdisciplinary teaming and formal cooperation between federal agencies, national labs, and academic institutions. He led a senior technical group that developed new methods for analysis of targeted cyber threats, provided technical context for mitigation priorities, and created new paradigms for information sharing between industry infrastructure owners, threat analysis teams, and government leaders. He also served as the Director of INL's Special Programs Division, which developed special technology and analysis in advanced materials, trace detection, nuclear non-proliferation, electronic warfare modeling, information operations, and wireless communications systems. Wayne was the founding program manager for communications R&amp;D at INL, coordinating multi- government agency efforts to create the industry-scale Wireless Test Bed to evaluate interoperability, performance, and security of new technologies within INL's Critical Infrastructure Test Range Complex.

Keynote Presentation

Mr. Zachary Tudor

Associate Laboratory Director, National & Homeland Security
Idaho National Laboratory

Idaho National Laboratory, managed by Battelle Energy Alliance, is one of 17 U.S. Department of Energy (DOE) national laboratories. Located in Idaho Falls, Idaho, INL employs more than 6,000 researchers and support staff with a common vision, to change the world's energy future and secure our nation's critical infrastructure. INL's national security mission focuses on protecting the nation's critical infrastructure, preventing the proliferation of weapons of mass destruction, and providing direct support to America's warfighters. From our decades-long work in building and testing more than 50 nuclear reactors in the high desert west of Idaho Falls, INL has developed a deep understanding of operational technology and the cybersecurity and engineering needed to secure systems and provide critical function assurance. For over a decade, INL has been conducting vulnerability assessments and developing technology and tools to increase infrastructure security and resilience. With a strong emphasis on industry collaboration and partnership, INL is enhancing power grid reliability, control systems cybersecurity and physical security systems. INL conducts advanced cyber training and oversees simulated competitive exercises for national and international customers. The lab supports cybersecurity and control systems programs for the departments of Homeland Security, Energy and Defense. INL staff members are also frequently asked to provide guidance and leadership to standards organizations, regulatory agencies, and national policy committees.

Speaker Bio:

Zachary (Zach) Tudor is the associate laboratory director of Idaho National Laboratory's National and Homeland Security Science and Technology directorate, a major U.S. center for national security technology development and demonstration, employing some 800 scientists and engineers across over $550 million in programs for the Department of Defense (DOD), Department of Homeland Security (DHS) and the intelligence community. He is responsible for INL's Nuclear Nonproliferation, Critical Infrastructure Protection and Defense Systems missions. Previously, Tudor served as a program director in the Computer Science Laboratory at SRI International, where he supported cybersecurity and critical infrastructure programs, such as DHS Cyber Security Division's Linking the Oil and Gas Industry to Improve Cybersecurity consortium and the Industrial Control System Joint Working Group R&D working group. He is the former board of directors' chair of the International Information Systems Security Certification Consortium (ISC2). He is a professor of practice in the computer science departments of the University of Idaho and Idaho State University and a member of Virginia's Commonwealth Cyber Initiative advisory board. A retired U.S. Navy submarine electronics limited duty officer and chief data systems technician, Tudor holds an M.S. in information systems, with a concentration in cybersecurity, from George Mason University, where he was also an adjunct professor teaching graduate courses in information security.

Keynote Presentation

NASA – MUREP Research Funding Opportunities in STEM

Dr. Gaffar Gailani

Program Manager at NASA

Finding the right opportunity to support your STEM research work is a big concern for researchers. The Minority University Research and Education Project (MUREP) of NASA is established to allow higher education academic institutions to collaborate with NASA Mission Directorates (MDs) in research. Besides MUREP the Office of STEM (OSTEM) in NASA has three more projects including the Space Grant, Next Generation STEM, and EPSCoR.

The Research Pillar of MUREP is focusing on improving research infrastructure and building capacity for minority serving institutions through different collaborative projects with NASA MDs. The research projects encompass different areas including manufacturing, earth science, robotics, data science…etc. These opportunities could lead to in-depth collaboration with NASA through contracts and long term partnerships.

Speaker Bio:

Gaffar Gailani, PhD is the activity manager NASA Minority Institutional Research Opportunity (MIRO) and the lead for the Research Infrastructure and Capacity Building pillar NASA MUREP. He is also serving as full professor in the department of Mechanical Engineering Technology at New York City College of Technology. He received his master's and PhD degrees in Mechanical Engineering from the City College of New York, while his BS. Degree is from Khartoum University in Sudan.

Keynote Presentation

Dr. Jian Yu

Convergent Manufacturing Lead, DEVCOM Army Research Laboratory

Speaker Bio:

Dr. Jian H. Yu is the current team leader for the Convergent Additive Manufacturing team in the Manufacturing Science & Technology Branch. He is leading S&T programs on operationalizing advanced manufacturing technologies, from rapid prototyping, small-scale production, materials by design, to on-demand distributed production of components and systems for Army Forces Readiness and Modernization. Jian Yu holds a Bachelor of Science Degree in Chemical Engineering from State University of New York at Buffalo (2001); and a Doctor of Philosophy Degree in Chemical Engineering (2007) from Massachusetts Institute of Technology.

During his 10 years of civilian service at DEVCOM Army Research Laboratory, he has performed research in ballistic property of soft armors and blast protection of underbody hulls and received two patents for blast containment designs. Recently, he has contributed to the development of high temperature conductive inks for printed electronic applications in extreme environments. His current research is in process workflow for the printing of electronic circuits on 3D conformal surface by integrating mechanical CAD and electrical CAD designs in concert in a Computer-Aided Manufacturing (CAM) digital twin for printing in 3D space.

Keynote Presentation

Research Opportunities for Realizing an AI Service Infrastructure for Manufacturing

Dr. Bruce Kramer

Senior Advisor in the Division of Civil, Mechanical and Manufacturing Innovation
National Science Foundation

A recent symposium under the joint auspices of the National Science and Technology Council Subcommittees on Advanced Manufacturing and Machine Learning and Artificial Intelligence has produced the outline of a strategy for achieving resilient manufacturing ecosystems through artificial intelligence, https://www.nist.gov/publications/towards-resilient-manufacturing-ecosystems-through-artificial-intelligence-symposium . That strategy emphasizes the potential to harvest network effects by gathering, classifying, and aggregating manufacturing data at a national scale. Similar models have transformed other industries in which the United States now leads the world but runs counter to the prevailing manufacturing culture, which emphasizes implementing proprietary solutions on the factory floor and keeping information close. That orientation exaggerates the importance of explicit domain knowledge and ignores the potential of AI methods to extract the implicit manufacturing expertise incorporated in the billions of parts that manufacturers are producing and have previously produced. It can also provide AI entrepeneurs an opportunity to adapt transformational business models successfully applied in other industries to the $2 trillion per year US manufacturing sector. The talk will illustrate how an AI-driven manufacturing service infrastructure might operate and suggest key research needs to enable it.

Speaker Bio:

BRUCE KRAMER is a graduate of MIT (S.B., S.M., Ph.D) and has served on the faculties of Mechanical Engineering of MIT and George Washington University. He is currently the Senior Advisor in the Division of Civil, Mechanical and Manufacturing Innovation of the National Science Foundation, coordinating NSF's participation in the National Advanced Manufacturing Program and co-leading the preparation of the 2018 and 2022 National Strategic Plans for Advanced Manufacturing by the National Science and Technology Council Subcommittee on Advanced Manufacturing. Dr. Kramer previously directed NSF's Divisions of Design, Manufacture and Industrial Innovation and Engineering Education and Centers. He co-founded Zoom Telephonics of Boston, a producer of communications products marketed under the Zoom and Motorola brands, holds three U.S. patents, and is a Fellow of the Society of Manufacturing Engineers and an International Fellow of the School of Engineering of the University of Tokyo. He has received the F.W. Taylor Medal of CIRP, the ASME Blackall Award, and the R.F. Bunshah Medal of the ICMC for his contributions to manufacturing research and the Distinguished Service Award, the highest honorary award granted by the NSF.

Invited Presentation

Developing an XR User Interface for High-Level Robot Teleoperation

Dr. Steve Feiner

Professor in Department of Computer Science Columbia University

Many real-world tasks carried out by robots require human participation, whether on-site or remote. However, operating robots typically demands that users undergo extensive robot-specific training to perform low-level tasks effectively and safely. I will describe an experimental XR user interface our team is developing to instead assign and manage assembly tasks remotely through high-level goal-based instructions rather than low-level direct control [Aoyama et al., 2024]. The user manipulates virtual replicas of task objects to prescribe 6DoF destination poses without needing to be familiar with specific robots and their capabilities. To make this possible, our user interface is integrated with a robot-planning system that determines, verifies, and executes robot-specific actions.

Speaker Bio:

Steve Feiner (Ph.D., Brown, '87) is a Professor of Computer Science at Columbia University, where he directs the Computer Graphics and User Interfaces Lab. He has been doing VR and AR research for over 25 years, designing and evaluating novel 3D interaction and visualization techniques, creating the first outdoor AR system using a see-through head-worn display and GPS, and pioneering experimental applications of AR and VR to fields as diverse as tourism, journalism, assembly, maintenance, construction, dentistry, and medicine. Steve is a Fellow of the ACM and the IEEE, a member of the SIGCHI Academy and the IEEE VGTC VR Academy, and the recipient of the *ACM SIGCHI 2018 Lifetime Research Award,* the *IEEE ISMAR 2017 Career Impact Award,* and the *IEEE VGTC 2014 Virtual Reality Career Award*. He and his colleagues have won the *IEEE ISMAR 2022 and 2019 Impact Paper Awards*, the *ISWC 2017 Early Innovator Award,* and the *ACM UIST 2010 Lasting Impact Award*.

Invited Presentation

Multidimensional Analysis of National Vulnerability Database

Dr. Narasimha Reddy

Truchard Foundation Chair Professor Department of Electrical and Computer Engineering Texas A&M University

Bring-your-own-device policies, Internet of Things (IoT) devices, and smart appliances are all contributing to the increasing diversity of connected devices. It has become imperative to understand the vulnerabilities of these diverse devices (along with traditional computer devices) to appropriately secure their use. In this paper, we conduct a detailed analysis of the vulnerabilities reported for the various hardware and software artifacts in the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). We analyze the details of vulnerabilities covering the period 2011-2022. We broadly categorize the vulnerabilities into three product categories: networking, IoT, and computing devices. The data is further classified into application, Operating System (OS), and hardware domains. We analyze the data across the aforementioned categories over four non-overlapping 3-year time periods. The analysis provides insights into salient trends in vulnerabilities across diverse products, and over time. Our work presents interesting findings based on the trends and persistence observed from the analyzed data. Our study points to insights that could lead to improved resource allocation for addressing security concerns.

Speaker Bio:

Narasimha Reddy received a B.Tech. degree in Electronics and Electrical Communications Engineering from the Indian Institute of Technology, Kharagpur, India in August 1985, and M.S. and Ph.D. degrees in Computer Engineering from the University of Illinois at Urbana-Champaign in May 1987 and August 1990, respectively. Reddy's research interests are in Computer Networks, Storage Systems, Multimedia Systems, and Computer Architecture. During 1990-1995, he was a Research Staff Member at IBM Almaden Research Center in San Jose where he worked on projects related to disk arrays, multiprocessor communication, hierarchical storage systems and video servers.Reddy holds five patents and and was awarded a technical accomplishment award while at IBM. He received an NSF Career Award in 1996. He was a Faculty Fellow of the College of Engineering at Texas A&M during 1999-2000. His honors include an Outstanding Professor award by the IEEE student branch at Texas A&M during 1997-1998, an Outstanding Faculty award by the Department of Electrical and Computer Engineering during 2003-2004, a Distinguished Achievement award for teaching from the Former Students Association of Texas A&M University, and a citation "for one of the most influential papers from the 1st ACM Multimedia Conference".Reddy is a Fellow of IEEE Computer Society and is a member of ACM.

Invited Presentation

REDsec: Running Encrypted Discretized Neural Networks in Seconds

Dr. Nektarios Tsoutsos

Director at the Center for Cybersecurity, Assurance, and Privacy. Assistant Professor in the Department of Electrical and Computer Engineering at the University of Delaware

Machine Learning becomes increasingly important for digital manufacturing, with many applications, including quality control, optimization, and analytics. Furthermore, Machine learning as a service (MLaaS) plays a pivotal role due to cost-effectiveness, pre-build models and expert tuning compared to custom in-house solutions. However, privacy concerns prevent the adoption of MLaaS for applications with sensitive inputs. A promising privacy preserving solution is to use fully homomorphic encryption (FHE) to perform the MLaaS computations. In this talk, we introduce the REDsec framework that optimizes FHE-based private machine learning inference by leveraging ternary neural networks, whose weights are constrained to {-1,0,1}, and have special properties that we exploit to operate efficiently in the homomorphic domain. REDsec bring new capabilities in private inference, including a new data re-use scheme that enables bidirectional bridging between the integer and binary domains for the first time in FHE. This enables implementing very efficient binary operations for multiplication and activations, as well as efficient integer domain additions. Our approach is complemented by a new GPU acceleration library, dubbed (RED)cuFHE, which supports both binary and integer operations on multiple GPUs. REDsec brings unique benefits by supporting user-defined models as input (bring-your-own-network), automation of plaintext training, and efficient evaluation of private inference leveraging TFHE. Our analysis includes inference experiments with the MNIST, CIFAR-10, and ImageNet datasets and we report performance improvements compared to related works.

Speaker Bio:

Nektarios Tsoutsos is an assistant professor with the Department of Electrical and Computer Engineering at the University of Delaware and holds a joint appointment in the Department of Computer and Information Sciences. He is currently serving as the associate director of the Center for Cybersecurity, Assurance, and Privacy at UD. His research interests are in cybersecurity and applied cryptography, with a special focus in trustworthy computing, privacy outsourcing, and digital manufacturing.

Invited Presentation

Dr. Gabriela F. Ciocarlie

Vice President for Securing Automation and Secure Manufacturing Architecture for CyManII

Existing methods for securing manufacturing production typically reflect a defense-in-depth approach in which cybersecurity controls are layered to provide system protection through redundancy and prevention. Provenance tracking along the supply chain has been used to provide traceability of the component's chain and typically record parameters such as BOMs, origin, and transportation history. Separately, post-production detection of counterfeit products (i.e., inspection and testing) is sometimes used to determine if components have been compromised, but only after they are produced. Unfortunately, none of these methods provides immutable assurance of a component's digital integrity. The only way to attain this level of guarantee is to validate that key physical steps in the manufacturing process have not been altered from the intended specification. In this talk, we introduce CyManII's novel cyber-physical passport (CPP) framework which integrates with the IT/OT equipment and network architecture of a production facility to capture critical information from machining parameters and production equipment, human operators who have interfaced with the manufacturing process, data exchanges, and hardware and software BOM's. Unlike traditional provenance tracking, the CPP also provides verifiable assurance of the product's physical and digital integrity. This key feature automatically verifies product build requirements against measurable physical properties of the production process in real time to detect anomalies.

Speaker Bio:

Gabriela F. Ciocarlie is an associate professor in the Department of Electrical and Computer Engineering at The University of Texas at San Antonio and Vice President for Securing Automation and Secure Manufacturing Architecture for CyManII. Her expertise is in anomaly detection, distributed alert correlation, network and application level security, cyber physical systems security, and distributed system security. Before UTSA, Gabriela was the Chief Product Officer at Elpha Secure and a senior technical manager of SRI's New York City research hub focused on cyberanalytics, which she established in 2016. Gabriela holds a Ph.D. and an M.S. in computer science from Columbia University, and a B.Eng. in computer engineering from Polytechnic University of Bucharest.

Invited Presentation

Cyber Risk Mitigation in a Small Manufacturing Environment via Security Segmentation

Dr. Michael Powell

Cybersecurity Engineer at the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST)

Small manufacturers tend to operate facilities with limited staff and limited resources. As a result, cybersecurity issues tend to slip through the cracks as something that takes too much time and cost. Mitigating cyber vulnerabilities is often viewed as a non-productive cost and an obstacle to efficient manufacturing operation. The lack of focus on cybersecurity leaves small manufacturers vulnerable to cyberattack and could impact production and revenue. Some assets used by a manufacturing company need more protection than other assets. The grouping of assets into security zones according to the protection they need and placing appropriate cyber protection measures around these groups of assets is security segmentation. This session provides an overview of security segmentation, and then presents a systematic yet simple six-step approach for security segmentation design. Security segmentation builds on the concept of network segmentation by including cyber risk mitigation into all aspects of the security zones. We will provide an overview of the building blocks of Security Segmentation. Then we will present how to mitigate the common cybersecurity weaknesses using a six-step approach to Security Segmentation design including typical deliverables.

Speaker Bio:

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

Dr. Michael Powell is a Cybersecurity Engineer at the National Cyber-Security Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) in Rockville, Maryland. His research focuses on cybersecurity for the manufacturing sector, particularly how it impacts industrial control systems.

Dr. Powell joined the NCCoE in 2017. In his previous positions, he was responsible for the management/oversight of building and commissioning of US Navy DDG-51 class ships. He also served in the United States Navy for over 20 years, retiring as a Chief Petty Officer. He holds a bachelor’s degree in information technology, a master’s degree in public administration, and a master’s degree in information technology. Dr. Powell completed his Doctorate degree in Applied Computing at Pace University in West Chester, New York.

Invited Presentation

Mr. Aslam Sherule

Lead Cyber Physical Security Engineer, MITRE Corporation

Speaker Bio:

Aslam Sherule is a Lead Cyber Physical Security Engineer at The MITRE Corporation. He is a co-author of NIST SP 800-82 R3, NIST SP 1800-10, and NIST CSWP 28. Currently he is working on practice guide for Responding to and Recovering from Cyber Attacks for NCCoE and other projects for DoD. His work focuses on OT/IIoT cybersecurity research and practice.

Prior to joining MITRE, Aslam was a Senior Technical Leader at Cisco focusing on OT & IoT Cybersecurity practice. During this period, he conducted several Security Segmentation, Risk Assessment, and Security Management Program services for clients in the oil & gas, mining, and manufacturing verticals. Prior to joining Cisco, Aslam was the trusted advisor and engagement lead at Verizon for a large utility company covering cybersecurity, M2M/IoT, networking, cloud, digital transformation areas.

He brings a wealth of skillset with over 25 years of experience in the fields of cybersecurity (IT & OT) and control systems engineering for energy, utility, and manufacturing verticals. Aslam's broad and deep skillet is backed up by rigorous education from leading universities in the US that covers cybersecurity, internetworking, control systems, and management topics.

Invited Presentation

Dr. Shamik Das

Chief Engineer, MITRE

The speaker will provide an introduction to MITRE Labs as well as capabilities and partnership opportunities to apply technological methods and measures from cybersecurity, supply chain risk management, and microelectronics domains to the security of advanced manufacturing and digital manufacturing. Example MITRE capabilities to be discussed include Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), and the Advanced Manufacturing Marketplace (AMM).

Speaker Bio:

Dr. Shamik Das is Chief Engineer of MITRE Labs at The MITRE Corporation in McLean, VA. He is responsible for technical execution, innovation, and quality management of the solutions developed and delivered by MITRE Labs' 4,000+ scientists and engineers. MITRE Labs' customers include the sponsors for MITRE's six Federally Funded Research and Development Centers (FFRDCs), as well as other Government, non-profit, and private-sector customers pursuing missions in the public interest.

In the course of his work, Dr. Das has led multiple formal independent assessments of global and domestic microelectronics programs and activities in the context of strengthening our national defense and security capabilities.

Dr. Das is a section chair for Beyond CMOS for the International Roadmap for Devices and Systems (IRDS), which is the roadmap for the worldwide semiconductor industry. He is a Senior Member of the IEEE.

Dr. Das received the Ph.D. in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology (MIT), Cambridge, MA. He received the M.Eng. and S.B. degrees in Electrical Engineering, as well as the S.B. degree in Mathematics, also from MIT.

Invited Presentation

Accelerating Qualification and Characterization in Smart Manufacturing Through Stochastic Inverse Modeling

Dr. Ashif Iquebal

Assistant Professor at Arizona State University

A wide range of problems in science and engineering necessitates estimating critical quantities of interest (QoIs) through indirect measurements. A pertinent example lies within advanced manufacturing, where pursuing comprehensive structure (including microstructure and geometrical dimensions) and properties for part qualification and certification involves either exorbitantly expensive experiments limited to laboratories or costly destructive testing. For instance, the definitive method for appraising elastoplastic properties entails destructive tensile testing, while microstructure characterization demands intricate electron backscatter diffraction with high fidelity. These challenges fueled the research on estimating QoIs using indirect measurements, leading to developments in solving ill-posed inverse problems. Yet, a fundamental limitation of classical inverse problems is that they consider material properties to be deterministic, lacking uncertainty quantification. Bayesian inverse models attempt to overcome this issue but assume that the variability in the indirect measurements arises from measurement noise, thereby failing to account for the variability in the QoIs. In this talk, we will explore the existing research on inverse problems and how they are limited in accurately estimating the QoIs and their variabilities. Subsequently, we will present our research on stochastic inverse problems that reformulate the classical inverse problem by considering the variability in the QoIs. This new approach leads to accurately estimating not just the QoIs but also the variabilities therein. Advances in stochastic inverse problems also open venues beyond material characterization, such as discovering the physics of complex processes via indirect measurements. We will show examples to demonstrate these applications.

Speaker Bio:

Ashif Iquebal is an assistant professor of Industrial Engineering in the School of Computing and Augmented Intelligence at ASU. Prior to this, he obtained his B.S in Industrial Engineering from Indian Institute of Technology Kharagpur, India and M.S. in Statistics and Ph.D. in Industrial Engineering from Texas A&M University. His research aims to bridge the gap between advanced manufacturing and statistical learning. More specifically, he is interested in stochastic inverse problems, active learning, and graphical models for accelerating materials characterization, discovering process physics, and generating causal inference. He received the NIH Trailblazer Award 2023, Finalist for NSF Blue Sky Competition 2022, Pritzker Doctoral Dissertation Award from the Institute of Industrial and Systems Engineering in 2021. His research papers have been winners/finalists for six best student paper/poster awards at INFORMS, IISE, IEEE and the American Statistical Association conferences. His research is funded by MxD-DoD, NIH, ERDC, and industry (Mayo Clinic, MK Morse, and Salt River Project).

Invited Presentation

Large Language Models for Manufacturing Automation Using G-Codes

Dr. Adarsh Krishnamurthy

associate professor in the mechanical engineering department at Iowa State University

Traditional manufacturing techniques operate on a lengthy timeline, including concept development, computer-aided design (CAD) modeling, tolerances, and manufacturing constraints, followed by process planning and manufacturing instructions. A process (or manufacturing) engineer converts the CAD designs to machine-tool specifications, which are typically expressed in G-Code, a set of instructions used in machine-tool-controlled manufacturing processes. Therefore, G-Code files encode both the design intent as well as manufacturing specifications for the part under consideration. This pipeline has several shortcomings - inability to optimize for time, inefficient design process, not allowing extensive design exploration, and the absence of robust quality assurance practices, among many others. Recent, powerful language models such as *GPT-4* demonstrate exceptional comprehension of human-authored text *and* code in various scripting languages, offering a ripe opportunity for their application in manufacturing. A multimodal *large language model* (LLM) that can natively ingest G-Code instructions and form bidirectional mappings with natural language will significantly reduce the manual effort needed to verify, debug, index, and retrieve G-Code. At a technical level, the LLM can be considered an information encoder that compiles the information from input data of various modalities into a shared numerical representation (or embedding). The multiple modalities in our database correspond to different representations of the part under consideration: design specifications, G-code, and CAD models. This embedding can be used for complex downstream tasks such as geometric reasoning, part retrieval, and shape matching. The goal of such an ecosystem is to become a fertile ground for small and medium-scale industries nationwide to quickly gain access to high-quality manufacturing services that would otherwise be out of reach due to the need for heavy manual intervention, excessive computing requirements, or high costs.

Speaker Bio:

Adarsh Krishnamurthy is an associate professor in the mechanical engineering department at Iowa State University, where he currently leads the Integrated Design and Engineering Analysis (IDEA) lab. His research interests include geometric modeling, additive manufacturing, machine learning, computer-aided design (CAD), GPU and parallel algorithms, biomechanics, patient-specific heart modeling, solid mechanics, and computational geometry. He is a fellow of the American Society of Mechanical Engineers (ASME) and the Plant Science Institute at Iowa State University. He was the recipient of the NSF CAREER award in 2018 for developing GPU-accelerated tools for patient-specific cardiac modeling. His research has been funded by several federal agencies, including NSF, USDA-NIFA, ARPA-E, NASA, NIH, and ONR.

Invited Presentation

An Overview of Standards in Additive Manufacturing: Qualification and Certification for a Reliable and Resilient Digital Manufacturing Ecosystem

Dr. David Paredes

Additive Manufacturing Project Engineer, ASTM, USA

Advanced Manufacturing technologies are an integral part of digital manufacturing as they are becoming more integrated in multiple industry sectors. For sustainable growth and adoption of the technology, quality assurance is critical. Qualification and certification are the way to demonstrate quality assurance. Standards form the backbone for developing qualification and certification programs. Innovative approaches are required in standardization to accelerate the path toward qualification and certification. This presentation discusses the research initiatives that propel the standardization process, and use of data in driving qualification and certification programs for Advanced Manufacturing. Topics of interest will include standards in Additive Manufacturing, Education Workforce Development and accredited programs that ensure a reliable and resilient digital manufacturing ecosystem.

Speaker Bio:

David Paredes is an Additive Manufacturing (AM) R&D Project Engineer for ASTM International. In his role, David is part of the ASTM Advanced manufacturing Center of excellence, supporting a diverse set of projects spanning different AM processes and industries from America Makes-AFRL Impact topic 9 to Boeing's GAMAT's Data Management Scope. Beyond the technical projects David is involved in supporting ASTM Global outreach team focused on LATAM technical business development for ASTM/ASTM AM CoE. His previous skills include mechanical design and product development for combustion systems tailored to industrial gas turbines. David received his bachelor's degree in mechanical engineering from the University of Florida in 2012 and his master's degree in AM and Design from Penn State University Fall 2022. Before joining ASTM, he served as a Lead Combustion Mechanical Design Engineer at Doosan ATSA, an AM Engineer at Beehive3D, and a Mechanical Design engineer at Power Systems Manufacturing. In these roles, he was a proponent of additive manufacturing to drive innovative solutions for complex applications, including the development of hydrogen combustion technology.

Invited Presentation

Integrated Cyber-Physical Security and Resilience of IIoT-Enabled Manufacturing Systems

Dr. Dan Li

Assistant Professor in the Department of Industrial Engineering at Clemson University

The emergence of Industrial Internet of Things (IIoT) technologies has significantly heightened societal and research interest in fortifying the security and resilience of manufacturing systems, especially in the context of industrial control. Within these systems, cyber-physical attacks exploit cyber network vulnerabilities to compromise operations with the objective of causing physical damage to the system operations. However, current solutions borrowed from other fields lack a holistic understanding of cyber-physical security resilience in these complex systems, failing to establish the connection between IIoT network vulnerabilities and system dynamics to assess risks and guide detection and control. In this talk, I will highlight my recent studies and future research directions related to manufacturing cyber-physical security and resilience from the aspects of risk quantification, cyberattack identification, and resilient control.

Speaker Bio:

Dan Li is an Assistant Professor in the Department of Industrial Engineering at Clemson University. She received her Ph.D. in Industrial Engineering and M.S. in Statistics from Georgia Institute of Technology in 2021 and 2020, and her B.S. in Mechanical (Automotive) Engineering from Tsinghua University, Beijing, China, in 2015. Her research interests include cybersecurity for Cyber-Physical Systems (CPS) / Industrial Internet of Things (IIoT), machine learning applications, sensor-based anomaly detection, and complex system modeling. Specifically, she is interested in developing new data-driven algorithms that are tailored for enhancing the cyber-physical resilience and security of critical infrastructures. Dan is the recipient of the NSF CAREER Award the IISE Transactions Best Application Paper Award. Dan has been recognized in multiple Best Track Paper and Best Student Paper Awards in Energy Systems, DAIS, and QCRE divisions at the IISE Annual Meetings.

Invited Presentation

Dr. Chinmay Hedge

Associate Professor at NYU Tandon, jointly appointed with the CSE and ECE Departments

Speaker Bio:

Chinmay Hegde is an Associate Professor at NYU Tandon, jointly appointed with the CSE and ECE Departments. His research focuses on foundational aspects of machine learning (such as reliability, robustness, efficiency, and privacy). He also works on applications ranging from computational imaging, materials design and manufacturing, and cybersecurity. He is a recipient of the NSF CAREER and CRII awards, the Black and Veatch Faculty Fellowship, multiple teaching awards, and best paper awards at ICML, SPARS, and MMLS.

R2DM3 - 2024

Organization Committee

Nikhil Gupta, New York University

Ramesh Karri, New York University

Center for Cybersecurity

Nektarios Tsoutsos, University of Delaware

Center for Cybersecurity, Assurance and Privacy

Special Thanks to:

Narasimha Reddy, Texas A&M University

Dr. Satish Bukkapatnam, Texas A&M University

Acknowledgment

National Science Foundation for funding the workshop through the grants:

CMMI-2036802 (Future Manufacturing Network)

CNS-2234973 (CISE Community Research Infrastructure)

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the presenter(s) and do not necessarily reflect the views of the National Science Foundation.

For technical sponsorship of the event:

IEEE Technical Committee on Cyber-Physical Systems

Lead Organizer & Editor:

Caleb Beckwith

Organization support:

Edna Taska

Marlett Lewis

Paule Dubreuze

R2DM3 - 2024

Website:

https://r2dm-workshop.github.io/

Workshop Location:
LC400, 5 MetroTech Center
Brooklyn, NY 11201 USA

Notes

Notes