2023 NEWSLETTER

Secure, Trusted, and Assured Microelectronics (STAM) Center

Ira A. Fulton Schools of Engineering

Arizona State University

Message from the Director

Just last week, two stories came out that exemplify the need for establishing the STAM Center. One, it was reported that US officials are searching for Chinese malware hidden in various defense systems that could disrupt military communications and other system operations. Second, TSMC announced that it will delay the start of Arizona chip production due to a skilled worker shortage.

Our mission is to provide an experiential training environment for secure and trusted microelectronics and electronics research and development that advances national security.

Across our six research laboratories, STAM Center members are actively investigating new microelectronics security primitives, methodologies, and devices and addressing security threats that result from the evolving landscape of the semiconductor industry, including outsourced fabrication and increased need for hardware IP protection.

The center serves as the convergence point to conduct fundamental research in three technical areas meant to establish the foundation for future secure and trusted microelectronics technologies: (1) new substrates, synthesis, and fabrication, (2) new computing paradigms and architectures, and (3) integrated sensing, edge computing, and secure communications. The center focuses on creating effective workforce development programs for students, working professionals, and government personnel, while ensuring that these programs reach all Arizona communities,

Executive Summary

In less than two years, the center has secured more than $3 Million in research funding. We have graduated two doctoral students, one thesis Masters student, and several publications. We have recruited more than ten new PhD students in the engineering doctoral program, with more than half being underrepresented minorities. We have organized multiple conferences, workshops, and outreach programs around secure and trusted microelectronics research and training.

These accomplishments did not happen in a vacuum. We would like to express our sincere gratitude to the Department of Defense, in particular the U.S. Air Force, Dean Kyle Squires and the Dean's Office, Vice Dean for Research and Innovation Sridhar Seetharaman and his office, the Provost's Office, and my colleagues Professors Sandeep Gupta and Sarma Vrudhula, and the the SCAI front office, especially Beverly Naig, Lisa Christian, and Lincoln Slade and his team.

Warm regards,

Michel A. Kinsy, PhD
Associate Professor,
School of Computing and Augmented Intelligence (SCAI)

CONTENTS

Effects of Globalization of Microelectronics

Trusted and Assured Microelectronics ... in an Increasing Distrustful World – M. Kinsy

At a recent workshop bringing together members of the US Government, Industry, and Academia to discuss the technologies and policies needed to enhance the US microelectronics capabilities and supply chain resilience, I gave a presentation to provide some context to the larger challenge. In my talk, I highlighted the evolution of the field in the last five decades and some of the policies, market forces, and technology trends working in concert.

Time to Market Driven Development Cycle

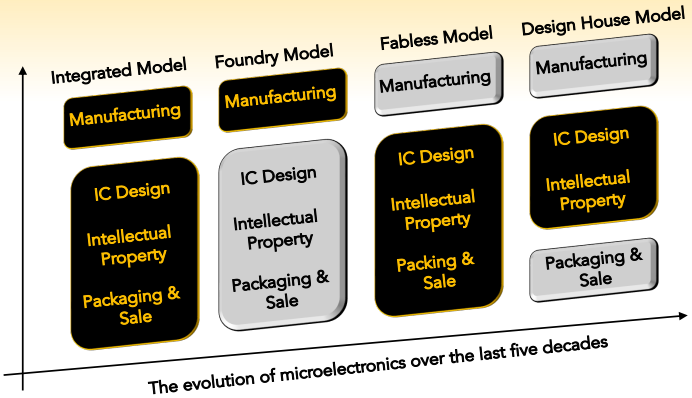
The microelectronics supply chain has enabled greater specialization of core functions from Integrated Circuit (IC) research and design, to manufacturing, packaging and distribution. Its economic gain is significant reduction to the Time to Market for new microelectronics products. It also gave rise to extensive Intellectual Property (IP) reuse and a larger role to fabless participants.

Impacts on Microelectronics Trust and Assurance

Even before the current geopolitical challenges, this model of production and distribution exhibited key vulnerabilities. Along this supply chain route, malicious circuits or components could be inserted in the design, key intellectual property components of the design could be stolen, the design could be reverse engineered and leveraged later, quality control information could be manipulated where a non–military grade microchip could be labeled as such for higher resale price.

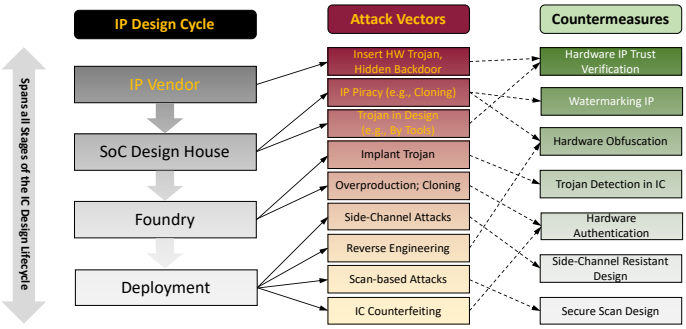
Experiential Learning Approach with Real–world Relevance

It is now imperative that we redress some of the vulnerability of this model, especially as related to medical devices, critical infrastructure electronics, and military systems.



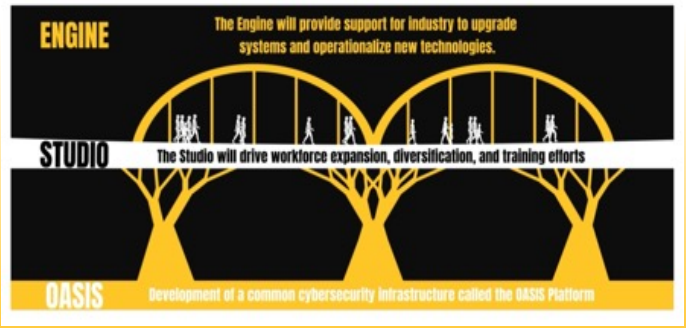
Globalization of Microelectronics Manufacturing

Perhaps, no other field has benefited from the global commerce momentum like microelectronics design, fabrication, and distribution. According to the Semiconductor Industry Association's supply chain map, a typical semiconductor production spans multiple continents and 3+ trips around the world – around 25 thousand miles.



Impacts of IP Reuse on Microelectronics Security

IP Reuse is littered with security risks, including lack of data exchange with third party IP designers, testbenches for IPs not adequately shared, lack of bug reports from IP designers, and clear verification standards not in place or enforced.



Vision & Mission

The *Secure, Trusted, and Assured Microelectronics (STAM) Center* is a research, development, and education unit focusing on establishing the foundation for future secure and trusted semiconductor/microelectronics technologies. The center's key research foci are (1) new substrates, synthesis, and fabrication, (2) new computing paradigms and architectures, and (3) integrated sensing, edge computing, and secure communications. The center couples its research mission with the active recruiting and training of students, especially domestic and minority students, targeting applications of national security importance. These applications are secure embedded systems, radar, post-quantum cryptosystems, smart dust, exoskeleton, edge AI, self-healing systems, autonomous cars and robots, and biochips.

Synergistic Interactions

RESEARCH AND DEVELOPMENT THRUSTS

Investigate new computation paradigms, emerging microelectronics technologies, and new secure hardware root-of-trust designs.

- **Emerging Computing**
  - . Quantum/ Cryogenics/ Probabilistic Computing
  - . Post-CMOS/Bio Substrates
- **Trust & Security Foundations**
  - . Zero-Trust IC Design
  - . Self-repair / Watermarking
  - . Primitives (PUF, ORAM, RNG)
- **Hardware & System Security**
  - . Secure Situation-Aware & Adaptive Architectures
  - . Techniques for Secure Designs

IMPACTS

Aim

Improve the security, trust, reliability, of microelectronics systems

- New Secure & Trusted Architectures
- Post-Quantum Secure Systems Design
- Secure AI/ML Deployment & Acceleration

1. Emerging technologies & techniques
2. 6.1 to 6.3 Research & Development for secure & trusted Microelectronics
3. Transition & Commercialization

EDUCATIONAL FUNDATIONS

Courses and hands-on projects in microelectronics design and usage in computing systems for trust, security, power, and performance.

- **Computer Engineering**
  - . Computer Architecture
  - . Embedded Systems
  - . VLSI & ASIC Design
- **Computer Science**
  - . Operating Systems
  - . Formal Methods
  - . Compilers
- **Applied Mathematics**
  - . Complexity Theory
  - . Applied Cryptography
  - . Number Theory

OUTCOMES

Objective

Prepare students in practical hardware-centric secure systems design

- Government/DoD Career Placements
- Project-Driven & Hands-on Courses
- CE/CS/Math Multi-Instructor Courses

1. Excellent knowledge of secure microelectronics technologies and techniques
2. Strong exposure to government application needs and constraints

OUTREACH & SERVICE

Broadening participation in microelectronics training by engaging a diverse group of students in experiential learning of relevant topics.

- **Undergraduate Research**
  - . Complement classroom learning with exciting and engaging research
- **Summer/Winter Programs**
  - . Rigorous math, science & engineering topics coupled with admissions counseling
- **Mentorship Programs**
  - . Saturday hardware design workshops & Lab visits
  - . Pairing with graduate student

SUSTAINABILITY

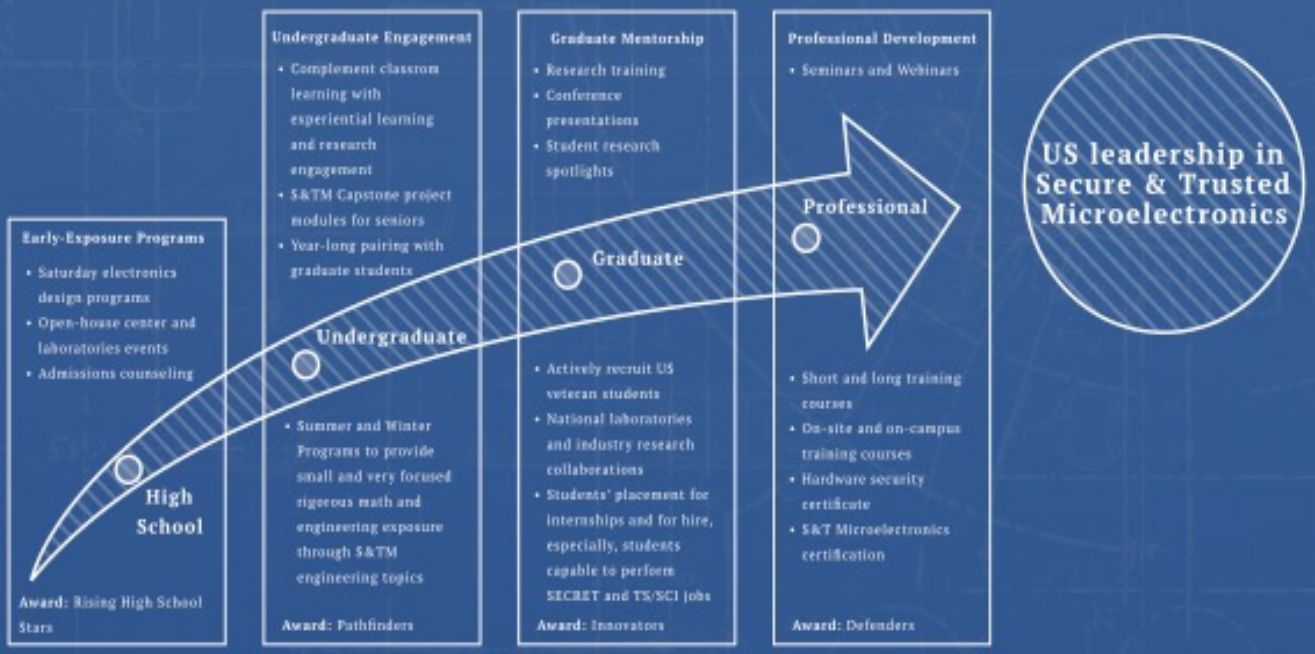
Goal

Create a programmatic administrative structure to increase early exposure

- Special Seminars & Lectures
- Government Apprentice Programs
- DoD Undergraduate Research Site

1. Microelectronics Engineering topics exposure for K-12, pre-college, & undergraduate junior & seniors
2. Quantitative periodical program assessments

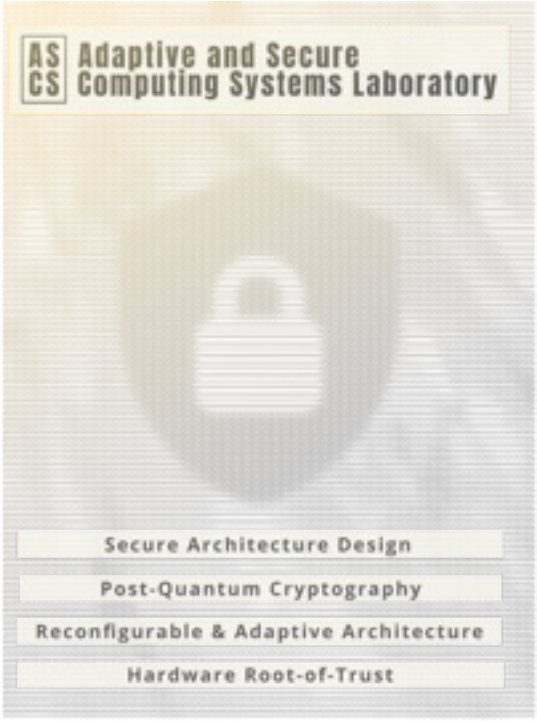
Creating a sustainable leadership training program in Secure and Trusted Microelectronics (S&TM)

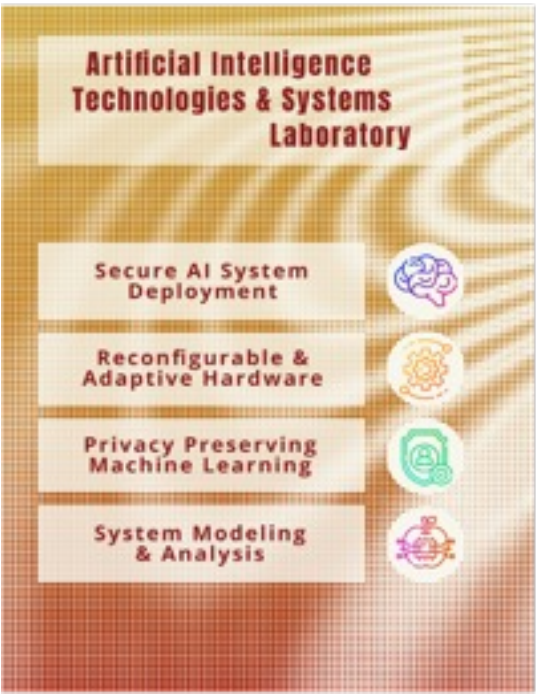


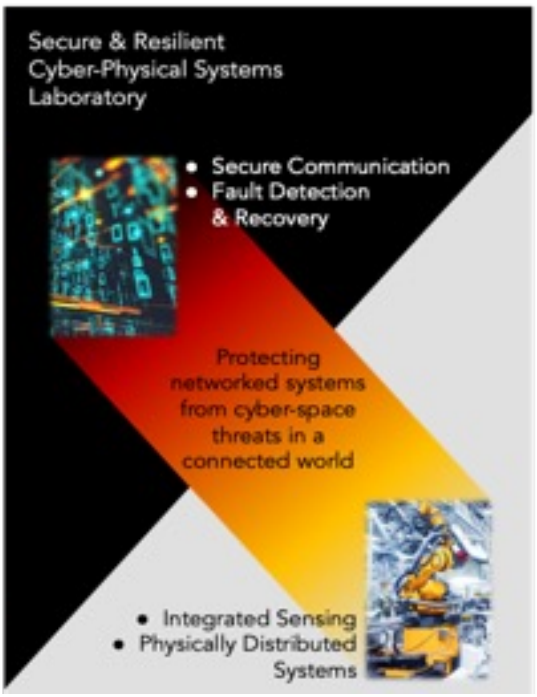
Developing a workforce capable of making security, privacy, trust and performance trade-offs in computer system design

	Computer Engineering Core	Computer Science Core	Applied Mathematics Core
	• Secure Computer Architectures • Embedded Systems • Advanced Complex Digital Design • Digital / Analog VLSI Circuit Design	• Operating Systems • Formal Methods • Compilers • Digital System Design • Computer Organization • Computer Architecture	• Complexity Theory • Applied Cryptography • Number Theory • Statistical Analysis Methods • Information Theory
S&TM Courses	• Microelectronics Design and Testing • Hardware Security and Trust • Advanced Hardware Security	• Physical Attacks in Microelectronics • Secure Architecture Design • IoT Security	• Supply Chain Security • Hardware IP Protection • Side-channel Attacks and Countermeasures

Laboratories



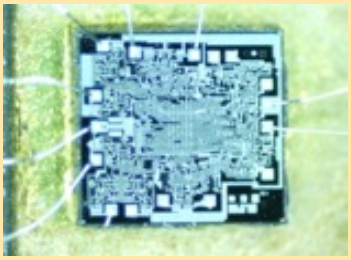




Center Research Capabilities

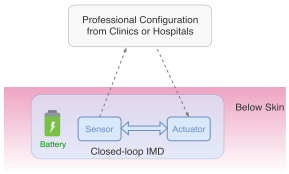
Advanced Microelectronics Counterfeit Detection

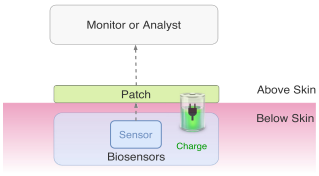
The STAM center is developing new advanced physical inspection techniques. The team performs both destructive and nondestructive device and subsystem characterization, scanning optical microscopy (SOM) and scanning electron microscopy (SEM), focused ion beam (FIB) imaging, preparation and circuit editing, probe station with laser circuit edit, wire–bonding and physical and chemical de–packaging equipment. We develop electrical tests for FPGAs, SRAMs, DRAMs, Flash, etc. that detect counterfeits with high confidence.



Experimental Design and Prototype of miniaturization of IC for unconventional locations

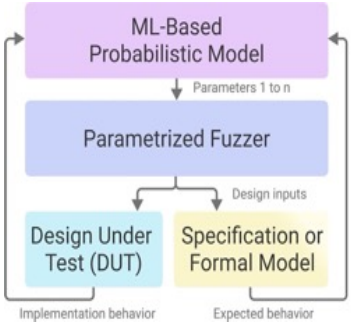
In the Unconventional Computing Substrates Laboratory, we explore unique and innovative compute substrates and microelectronics, including optical, analog, cryogenic, reversible, stochastic, and asynchronous computing concepts. These research efforts target usage modalities such as highly miniaturized microelectronics to be deployed in programmable cartridges, complex autonomous sensor movements, automated projectile drift compensation, and implantable medical devices, among others.

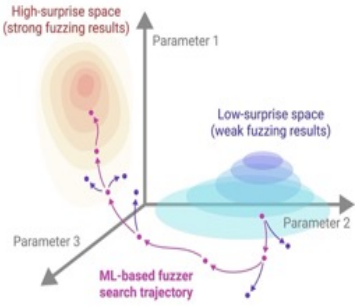




Trustworthy and Assurance Validation and Analysis of Microelectronics

The team designs and implements a field–programmable gate array (FPGA) based emulation platform for high–fidelity trustworthy and assurance validation of ASIC designs beyond the capability of current commercially available tools. The platform can (1) perform fast, high–fidelity emulation of an ASIC design in terms of functionality, modules states, and state transitions, (2) simulate associated physical or electrical properties of the design, and (3) support real–time parallel testing and validation of an emulated design and its physical design over long–running application workloads or stress–tests.

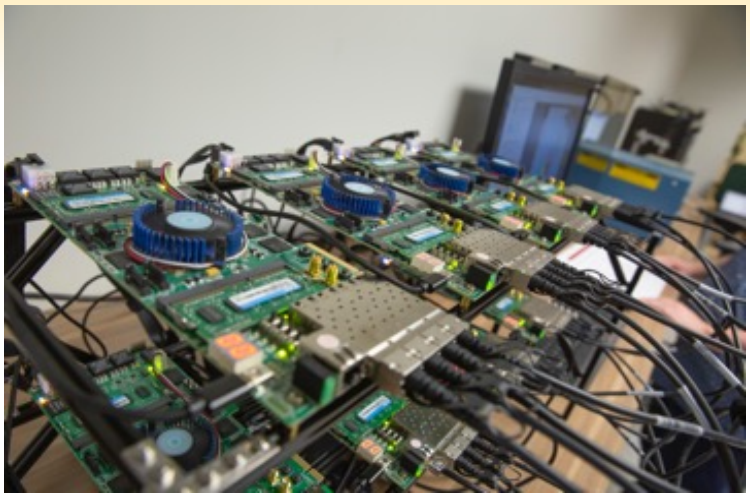




Anti–Tamper Active and Passive Sensors for Microelectronics

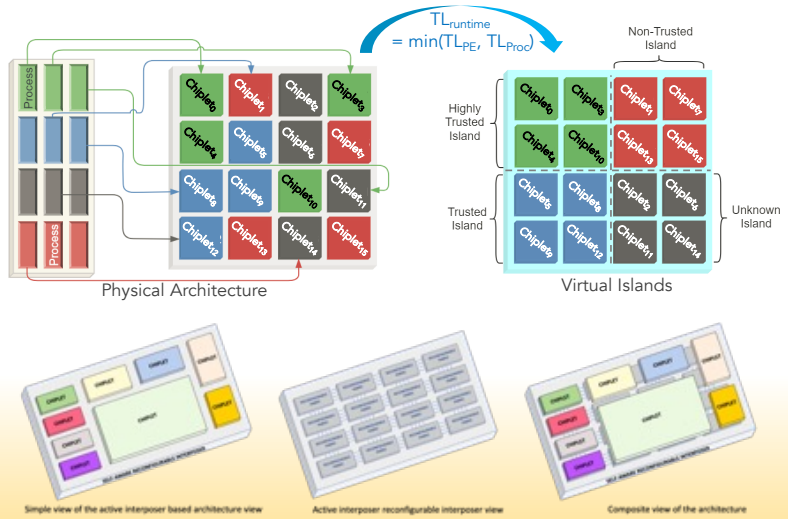
We examine different anti–tamper and anti–reverse engineering techniques and have developed a set of unique capabilities in this domain, including fiber–optic seals, nvSRAM (non–volatile random–access memory) solutions, polyvinylidene fluoride (PVDF) tamper detection sensors).

Center Research Capabilities



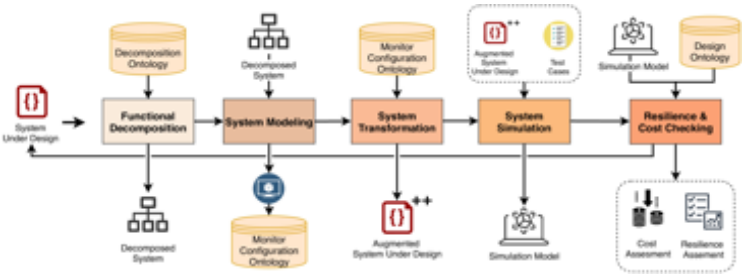
Building Secure & Trusted Microelectronics out of Untrusted Components

The team is working on a new active interposer based 2.5–D design methodology using reconfigurable logic targeting security applications. The methodology enables integration–time or user–side, hardware–assisted security feature programming. It decouples the security of the chiplet–based design from the individual chiplet fabrication or provenance, or even the interposer itself. It does this by imbuing the active interposer with reconfigurable fabric that can be programmed at integration and end–use stages to provide hardware root–of–trust security guarantees.



Ontology–Driven, Secure, High–Assurance Electronics Design

The Ontology–driven Application and Security Intent Specification (OASIS) tool provides the representational choices that best capture the relevant security and assurance characteristics or features of the design specifications and constraints at the highest level of abstraction and provides the logical expression of terms and parameters of the design to be sent through the rest of IC design–flow.



Analog Circuits Emulation of Quantum Gates

Quantum Emulating Analog Circuit (QEAC) aims to enable concurrent development of quantum devices and quantum computer systems with high–fidelity. Emulation makes design and development of quantum system architectures, algorithms, memories, co–processing with classical computer techniques, security, and student training more tractable. We are implementing the analog equivalent of certain universal quantum gates like the Square root of NOT Gate and Phase Shift (Twist) Gate, as well as select elementary circuits like an adder.

Center Research Capabilities

Secure–by–Construction Techniques to Processors and Systems Design

The team investigates and develops secure and efficient implementations for a broad range of processors, ASICs, radiation–hardened, and FPGA–based embedded solutions.

Multi-Party Computation (MPC)

Pros
- Low compute requirements
- Easy to accelerate
- Provably secure
- Supports multiple threat models
- Easy to map existing algorithms

Cons
- High communication costs
- High latency
- Information theoretic proofs are weaker than PKE ones

Fully Homomorphic Encryption (FHE)

Pros
- Very low communication costs
- Requires a single round of communications, i.e., "fire and forget"
- Useful when one side is limited in compute / memory / storage
- Provably secure – relies on strength of PKE

Cons
- Very high computational requirements
- Harder to accelerate
- Mapping existing algorithms to FHE may be difficult

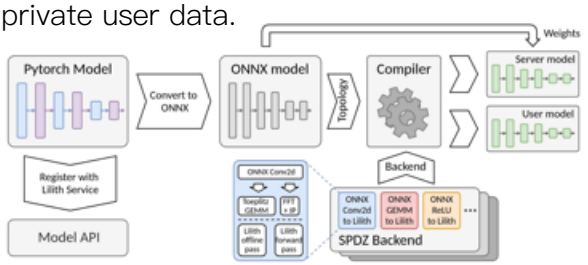
Trusted Execution Environments (TEE)

Pros
- No communication required
- Trivial to accelerate
- Great support for existing DNN models

Cons
- Weaker security guarantees
- Cannot stop determined adversaries
- Historically plagued by vulnerabilities and breaches
- Long term deployment is difficult – TEE's can 'run out' of entropy / CRP's, etc.

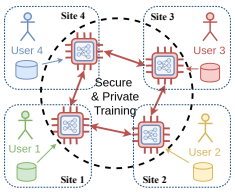
Methods for Computation on Private Inputs

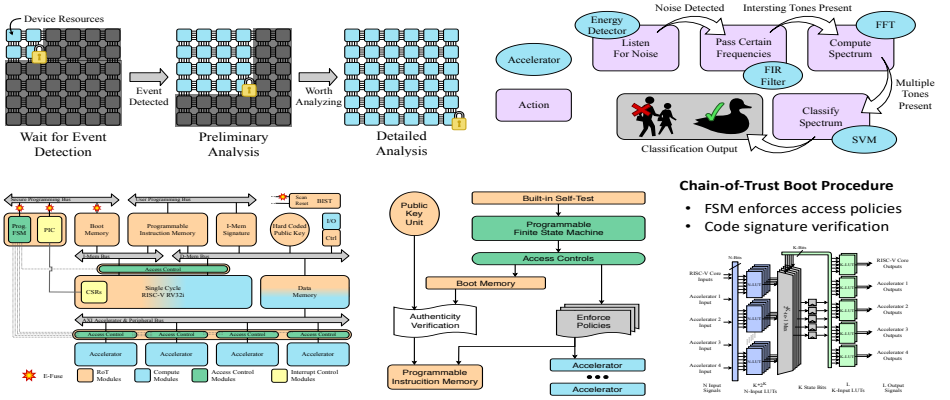
Executing third–party applications, e.g., deep neural networks (DNN), in the cloud on user data puts private user information at risk. Similarly, executing an application like neural networks on edge devices puts these models at risk from model theft. In our work we investigate methods to practically compute private applications on private user data.



Secure Open–Interface Distributed IoT Testbed System

Having one of the largest academic real–time distributed system testbed enable us and our partners to investigate, design, and validate real–world, large–scale, distributed, secure, compute applications.





Hardware Root–of–Trust Approaches for Secure Edge Computing

These approaches include e–fused boot memory to ensure the boot code and other security critical software is not compromised after deployment, digitally signed programmable instruction memory to prevent execution of code from untrusted sources, a programmable finite state machine to enforce access policies to device resources even if the application software on the device is compromised, access policies to isolate the execution states of application and security–critical software.

Chain-of-Trust Boot Procedure
- FSM enforces access policies
- Code signature verification

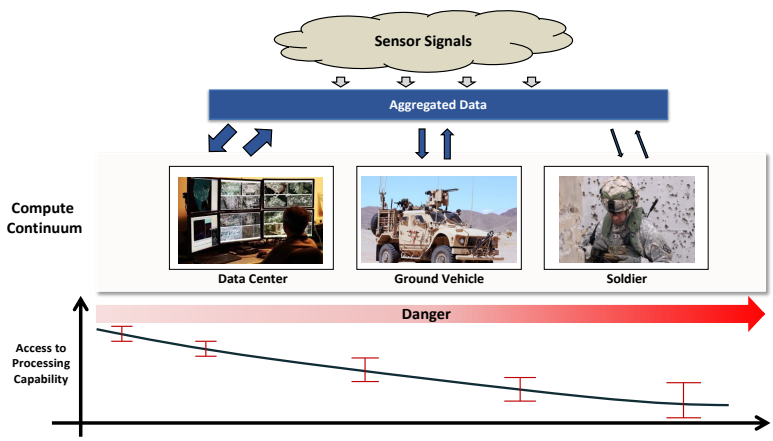
End–to–End Secure Full–System Prototyping

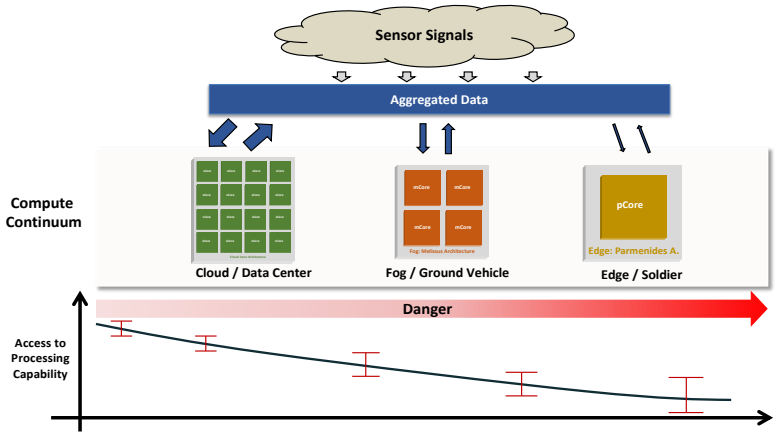
Our expertise, tools, and partnerships have enabled us to engage in fast turn–around full system prototyping projects.

Center Research Capabilities

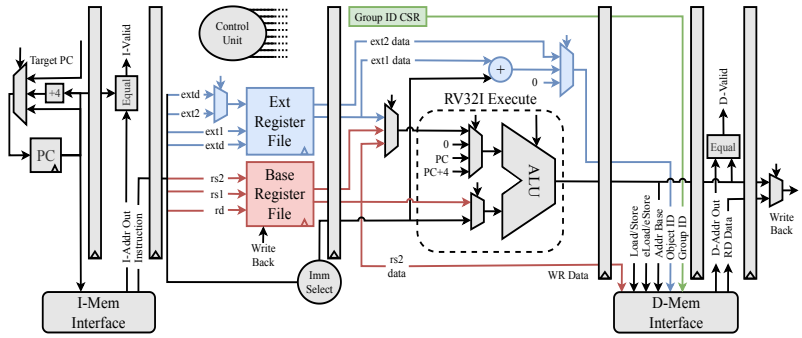
Tape-Out of Full-System Multicore Secure RISC-V Processors

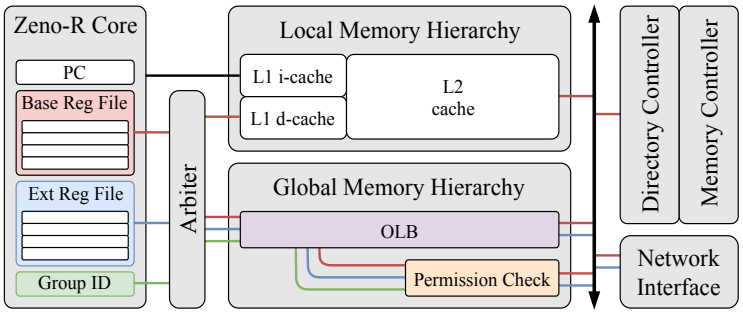
Real-world applications from our partners ground our research efforts. We use a multidisciplinary approach to deliver new capabilities. Our emphasis on field-ready prototyping projects provides students a rich experiential learning environment.

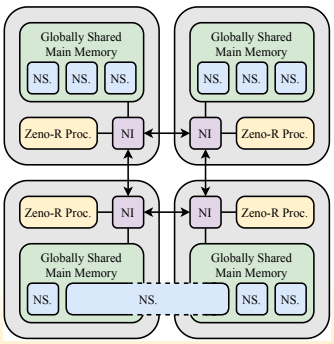


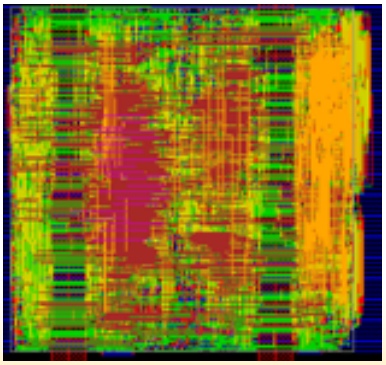


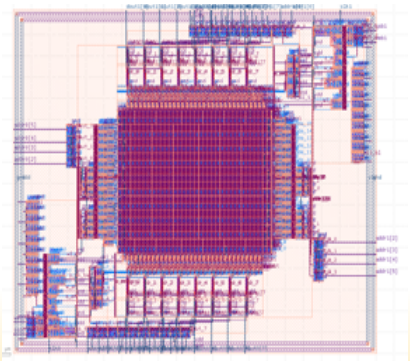
Solving the compute challenge associated with the processing asymmetry of the edge-to-cloud continuum





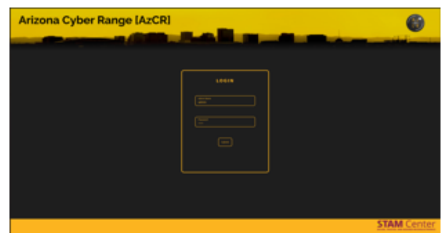


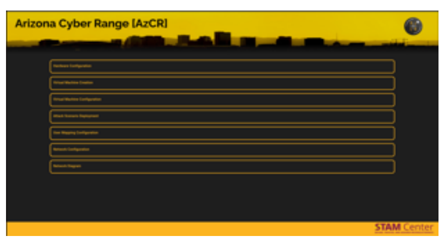


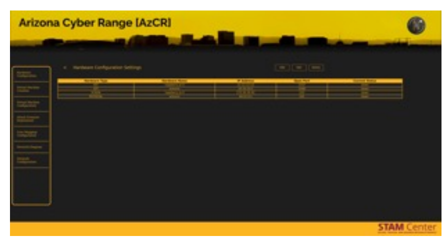


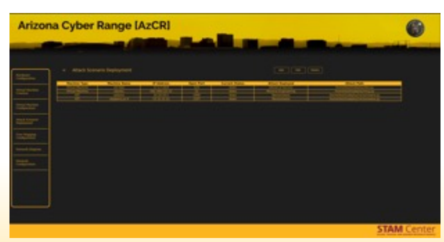
Center Research Capabilities

Research Impacts and Collaborations
With our research collaborators and partners, we have released and maintain several design tools.







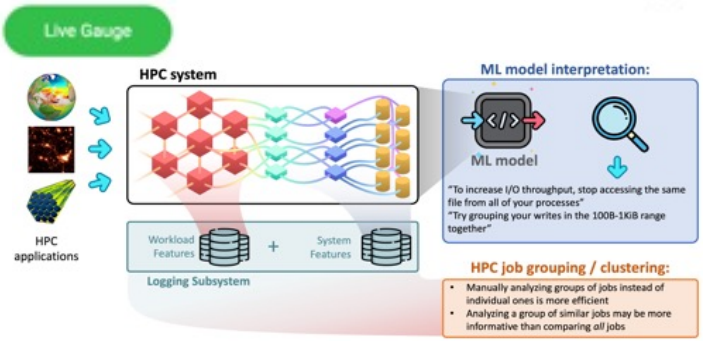


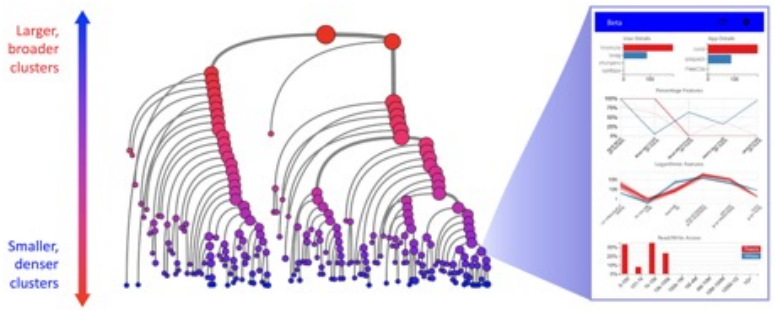
https://azcyberrange.asu.edu/

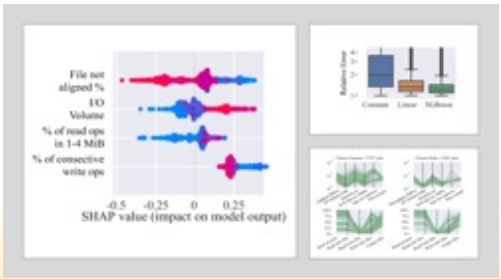
Center Research Capabilities

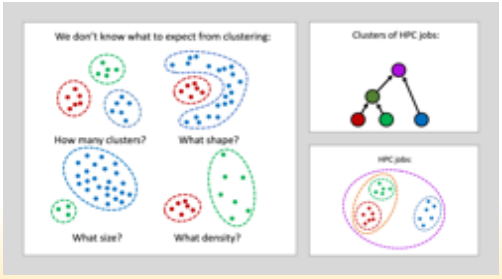
Research Impacts and Collaborations

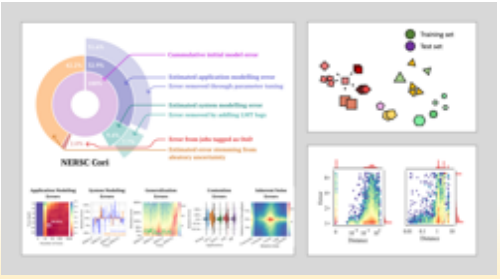
With our research collaborators and partners, we have released and maintain several design tools.









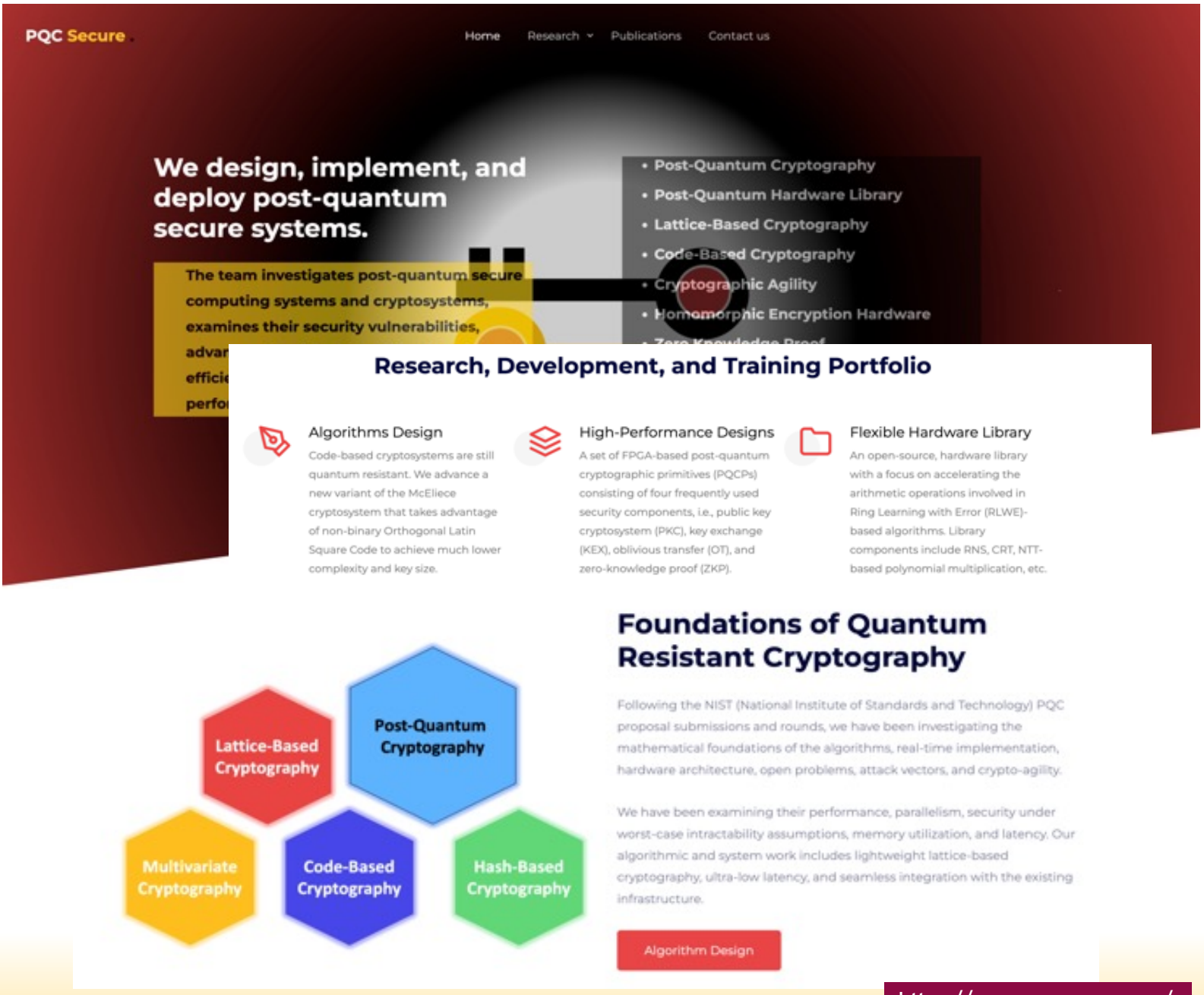


https://www.gaugeviz.org/

Center Research Capabilities

Research Impacts and Collaborations

With our research collaborators and partners, we have released and maintain several design tools.

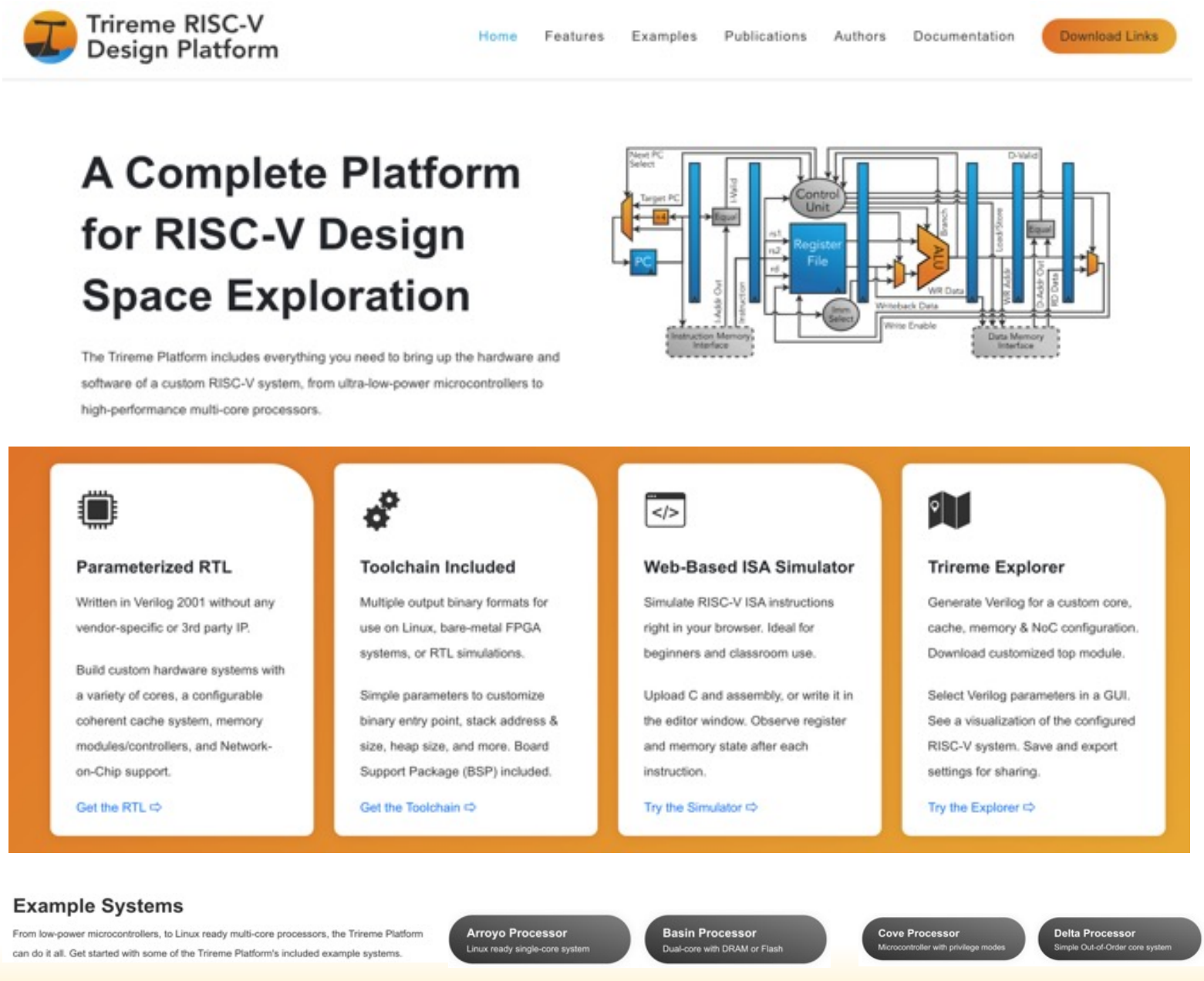


https://www.pqcsecure.org/

Center Research Capabilities

Research Impacts and Collaborations

With our research collaborators and partners, we have released and maintain several design tools.



https://www.trireme-riscv.org/

Education & Training

Course Development

STM 180: Advanced Hardware Security – Advanced techniques, i.e., imaging technologies and classification algorithms, to efficiently evaluate state–of–the–art commercial microelectronics components, fast and accurate IC reverse engineering methods, attacks on microprocessors, etc.

STM 200: Microelectronics Design and Testing – Microscopy methods to detect defects, non–destructive testing for integrity analysis, PCB reverse engineering, image filtering and segmentation methods for netlist extraction, reading non–volatile memory data and key extraction, laser–based fault injection, and anti–probing techniques.

STM 210: Microelectronics Attacks and Defenses – Logic locking and IC camouflaging, IP encryption, 2.5/3D split manufacturing, automated counterfeit detection, and IC counterfeit avoidance techniques.

STM 250: Supply Chain Security – Use of microelectronics component markers to tag/mark ICs and subassemblies to authenticate and track supply chain movements., including hardware IP protection techniques to prevent exploitation, including control of use, concealment, reconfiguring, partitioning, or deployment.

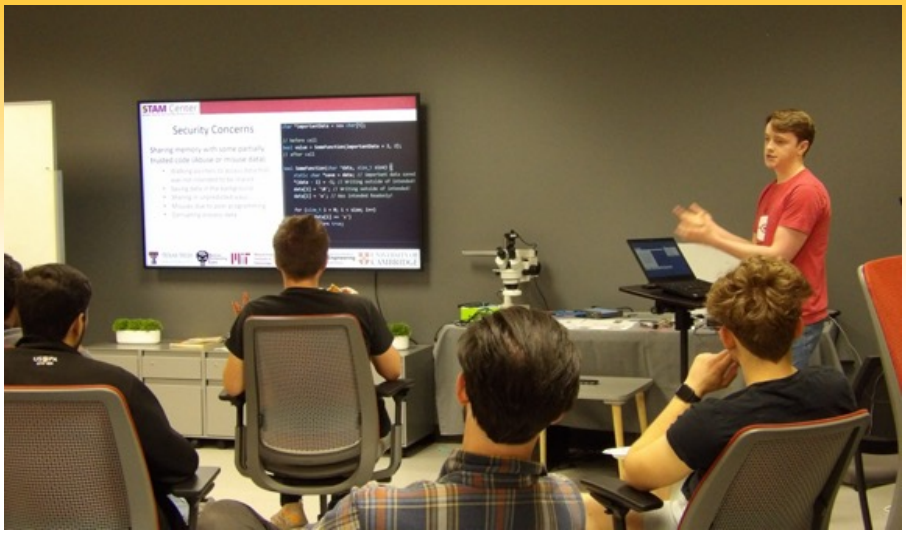
Graduations

Ph.D. in Computer Engineering, Thesis Title: Self–Aware Adaptive General–Purpose Computing Architectures
Mihailo Isakov

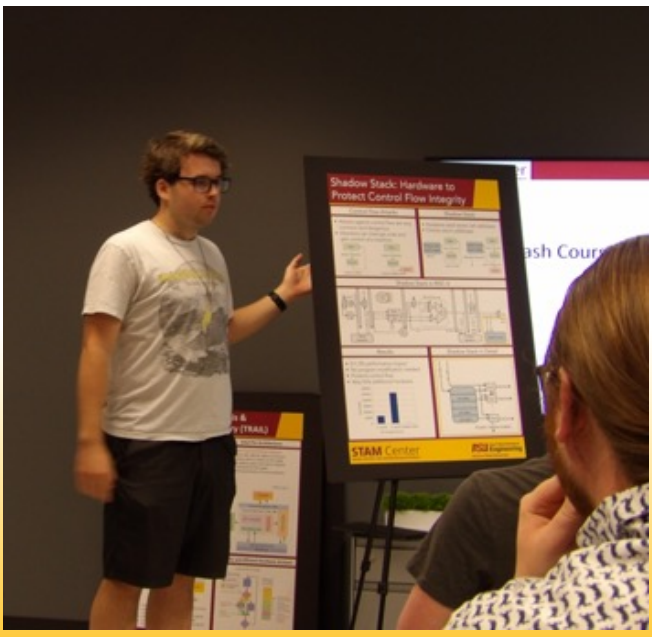
Ph.D. in Computer Engineering, Thesis Title: Eleatic: Secure Architecture Across the Edge–to–Cloud Continuum
Alan Ehret

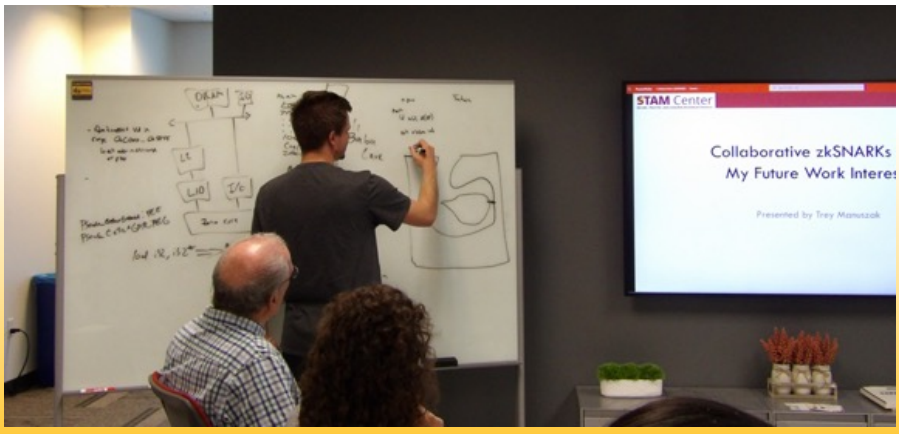
Master of Science in Computer Science, Thesis Title: Code Generation Techniques for Emerging Capability Architectures
Jacob Abraham

Education & Training



Technical Presentations

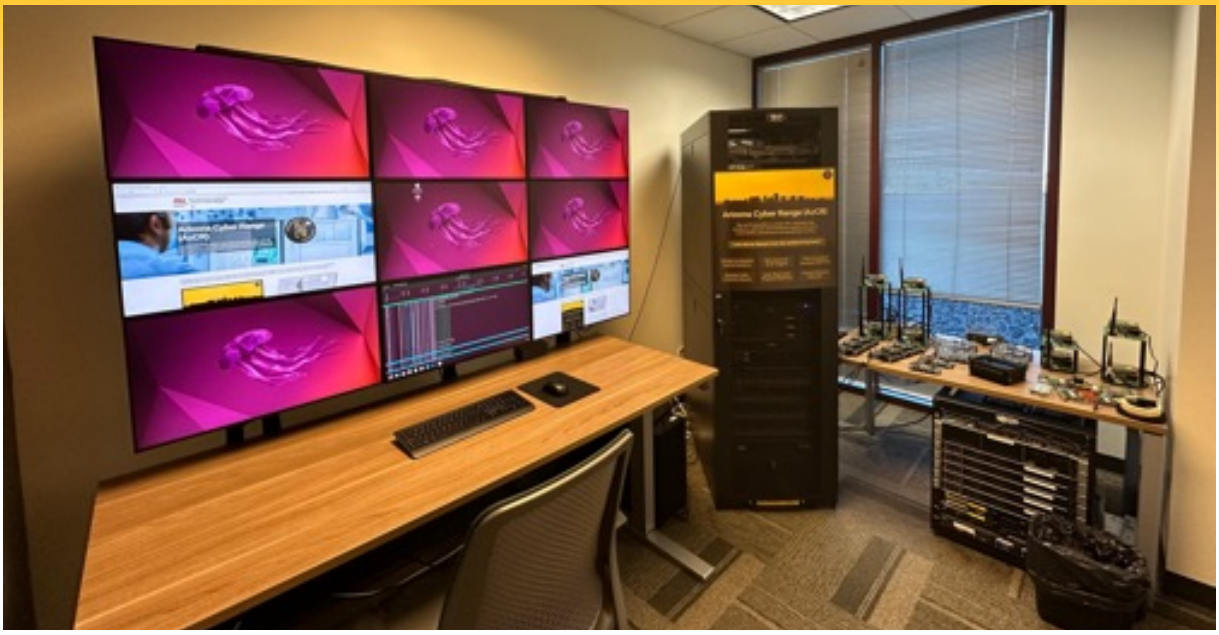


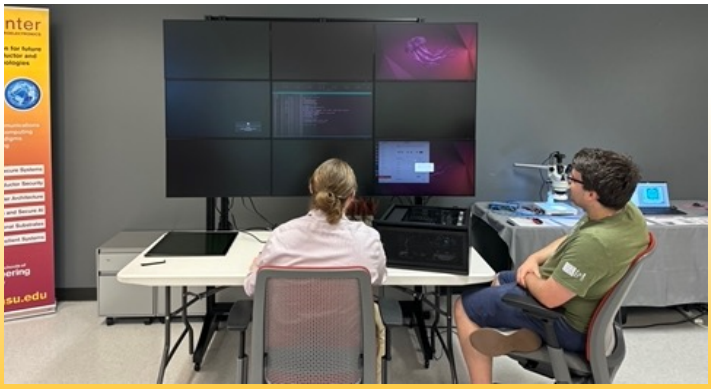


Education & Training

Leveraging the AzCR Capabilities

Critical infrastructure cybersecurity training with greater integration of real Security Operations Center (SOC) concepts and conditions.





Experiential Educational Platform

Designing Operational Cyber Security Strategies

- Conduct a cyber security risk assessment
- Measure the performance and troubleshoot cyber security systems
- Implement cyber security solutions — software, hardware, and network

Conceptual

- Introduction to Information Security
- Cybersecurity Foundations
- Hacker Techniques & Tools

Strategic

- Penetration Testing
- Monitoring & Detection
- Cloud Security
- Software & Network Forensics

Operational

- Industrial Control Systems
- Hardware System Forensics
- System Security Architecture

Cloud-Based | **Cloud-Based** | **Hybrid**

Education & Training

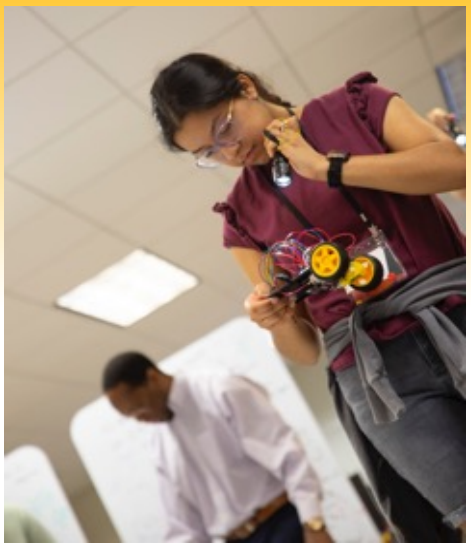
Education & Training

FACULTY OF TECHNICAL SCIENCES

UNIVERSITY OF NOVI SAD

Lecture Series

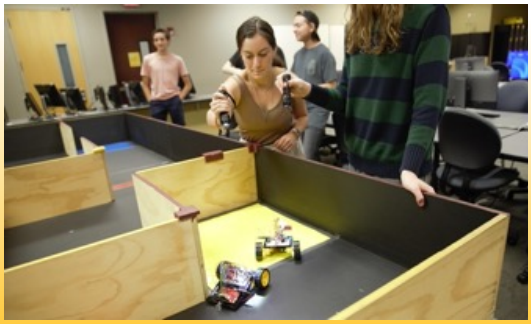
Outreach & Service



2023 high school outreach activities

Outreach & Service

2022 high school outreach activities



Outreach & Service

2023 Microelectronics Education and Workforce Development (MEWD) The workshop brought together experts from academia, industry, and government to strategize about microelectronics workforce expansion and training programs.– ***https://tinyurl.com/2s36949b***

Outreach & Service

Secure RISC-V (SECRISC-V) Architecture Design Exploration

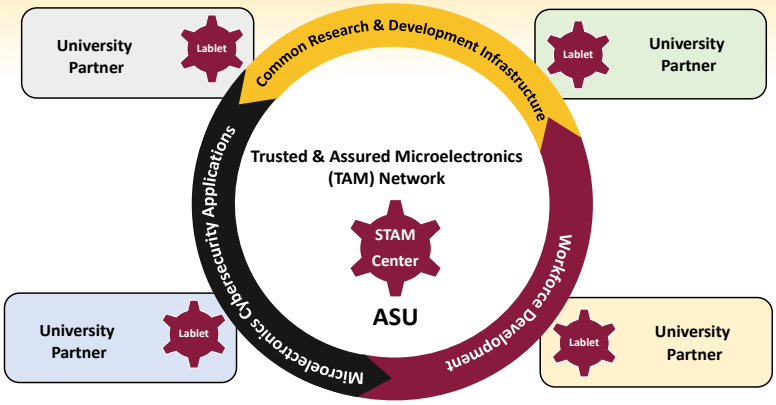
The Center organized as part of Embedded Systems Week (ESWEEK) a full-day event on ***Secure & Trusted Microelectronics for High-assurance Embedded Systems*** to bring researchers around the world to Phoenix. The event was anchored by the SECRISC-V Workshop – ***https://secriscv.org/highlights.html***

Outreach & Service

Reception by the Rector of the University of Novi Sad, prof. Dr. Dejan Madić during the International Cybersecurity Seminar (ICW) 2023.

Broadening our Collaboration Network

With the support of sponsors, we are developing a network of lablets around a collective framework of trusted microelectronics research and education.



A network to amplify our collective research and training capacity, expand research and project funding opportunities, and increase internships, research assistantships, research visits, training opportunities for students and researchers.

Outreach & Service

Noteworthy Events

Start Students Early to Build Semiconductor Talent Pipeline
At the 2023 GovExec's Cyber Summit, we highlighted for federal and state officials ideas for early–exposure to build a robust US semiconductor talent pipeline – ***https://tinyurl.com/wewkkvy7***

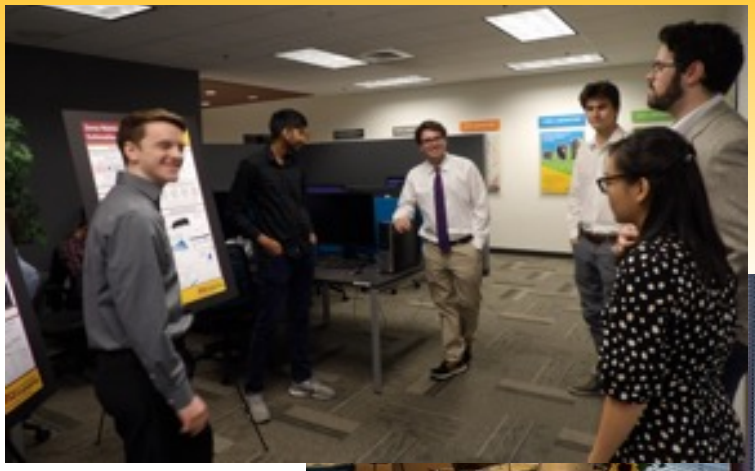
Rethinking Engineering Education In The U.S.
Contributing to the national discussion around engineering education in the U.S., especially around microelectronic education. Our experiential education and training approach is growing in appeal – ***https://tinyurl.com/4zj42pwf***

CHIPS and Changemakers
Celebrating retired U.S Congresswoman Eddie Bernice Johnson and her contribution to the CHIPS and Science Act – ***https://tinyurl.com/3cnscx5t***

Early–Exposure Experiential to IC Design
As part of our efforts to provide early–exposure to microelectronics design education, we are developing the concept of *IC Design & Fabrication Studio* with the complete list and equipment needed – at the cheapest cost under $200k – for learners to fabricate they own simple IC (integrated circuits).

They will be exposed to the over 60 discrete stages involved in the IC fabrication process, including steps, chemicals, and equipment used – e.g., PMOS versus NMOS, wet thermal oxidation, oxidized wafer, patterned and etched gates, vacuum chamber, and lithography process. They will also learn how to fabricate their own presensitized/photopositive PCBs (printed circuit boards).

Outreach & Service



Outreach & Service

Industry & Government Sponsor Visits

Administrative

Meet Our New Staff Members

José Moreno
Associate Research Technologist
Interim Assistant Director of Education & Outreach

Mr. Moreno leads the center's educational and outreach programs. He is a US Army Signal Officer Veteran with experience leading and developing teams in IT–related operations and management. He served the US Army in many theaters including deployments to Iraq to establish and manage communication and information networks and directing network operations for the US Army Japan mission. In his role, Mr. Moreno focuses on a greater alignment of the center's experiential learning in secure microelectronics with the DoD technical training needs.

Maleinda Fields
Proposal/Grant Manager

Mrs. Fields manages the center's proposals and financial activities. She has over 16 years of experience with preparing budgets and financial reports. She works closely with the director, researchers, students, affiliated faculty, academic collaborators, and industry partners in reviewing calls for proposal, preparation and submission of proposals, and managing the financial aspects of projects, including expenditure forecasting, strategic planning, sub–contracting, and spending plan reporting. Ms. Fields has studied communications, business accounting, and office administration.

Dr. Milan Stojkov
Security Researcher

Dr. Stojkov is investigating and developing distributed systems security models and protocols, especially industrial systems of IoT devices, to enable collective aggregated security capabilities and coordinated services. Dr. Stojkov has a Ph.D. in Computing and Control Engineering – Information Security, an M.Sc. in Computing and Control Engineering, and a B.Sc. Computing and Control. From 2016 to 2023, Dr. Stojkov was a Cybersecurity Consultant for Schneider Electric in the Digital Energy Division.

Administrative

2023 CENTER LEADERSHIP AWARD
Dr. Alan Ehret
Asst. Research Professor

An Emerging Leader in Secure & Trusted Microelectronics Research & Education

In essence, Dr. Ehret represents the spirit and the success of the Department of Defense SCALE (Scalable Asymmetric Lifecycle Engagement) microelectronics workforce development program. Although Dr. Ehret had more lucrative offers, as a trainee of the program, he decided after graduation to join the ASU faculty and assist in leading the STAM Center research and outreach efforts and to mentor other students through the SCALE program. With his colleagues, he also co–founded a new company to provide unique security–aware microelectronics solutions to the U.S. government.

Each year, the center selects a member of the senior personnel team who exemplifies excellence in research, education, outreach, and teamwork to honor their contributions.

Welcome to our new Ph.D. students – Katherine M. Rejas, Eric Jahns, Mark Amobi, Davi De Almeida, Robert Doe, Luigi Mastromauro, Edwin Kayang, Zhenqi Wu, N. Brian Njungle, and Mishel J. Paul.

Closing Remarks

An Experimentation in Experiential Education & Training in Trusted & Assured Microelectronics

Since its inception, we strive to ensure that the center focuses not only on the security, trustworthiness, and assurance of the chip, but also the development of the human capital needed to drive the U.S. microelectronics resurgence! It is our imperative that our efforts reach and serve all segments of our community.

THANKS TO OUR SPONSORS

Sincere thanks to the Department of Defense, the Department of Energy, and national laboratories for their support and to allow us to make our work stand behind something larger than ourselves.

STAM CENTER 2023 NEWSLETTER

Ira A. Fulton Schools of Engineering
Arizona State University