MONTANA STATE UNIVERSITY

Software Engineering & Cybersecurity Laboratory (SECL)

MSU SECL

SECL Co-Directors
Professors Clemente "Clem" Izurieta &
Ann Marie Reinhold

We are an interdisciplinary team of computer and data scientists who take aim at vexing problems using convergent scientific and engineering approaches.

The SECL comprises six faculty members, approximately 20 students (undergrad, M.S., and Ph.D.), a research scientist, a developer, and a lab manager. We work closely with the MSU Applied Research Lab, TechLink, MilTech, and have multiple university, government, industry, and national lab partners. Our physical space is located in Norm Asbjornson Hall on the Bozeman Main Campus.

APPLIED RESEARCH & OPERATIONAL TECHNOLOGY HIGHLIGHTS

Protecting Critical Systems with Hierarchical Software Quality Assurance

Deficiencies in software quality cause billions of dollars in losses and degrade organizational reputation. To address these deficiencies, we have developed technologies that implement Hierarchical Software Quality Assurance (HSQA)—including our flagship technology of PIQUE. PIQUE is effective because it provides a systematic approach for identifying deficiencies in software quality—including the crucial characteristic of cybersecurity. This technology is enhanced with artificial intelligence that predicts important markers associated with low-quality software. Thus, developers can use PIQUE to identify deficiencies and make necessary adjustments to ensure best practices are fully implemented—such as modifiability-by-design and security-by-design. These best practices are critical for securing the software supply chain and protecting the complex digital systems at the core of our industry, government, and military sectors—systems that cannot afford to fail. By providing a means for the thorough evaluation, PIQUE catches defects early to prevent weaknesses in code from becoming crises. Project funded by DHS S&T. Project Lead: Dr. Clem Izurieta; clemente.izurieta@montana.edu.

PIQUE

Platform for Investigative software Quality Understanding and Evaluation

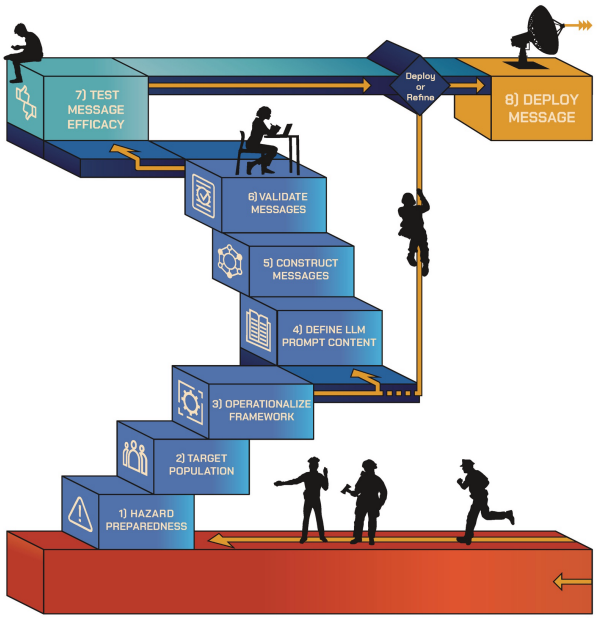
www.montana.edu/cyber
clemente.izurieta@montana.edu | reinhold@montana.edu

MONTANA STATE UNIVERSITY

Software Engineering & Cybersecurity Laboratory (SECL)

Improving Hazard Preparedness with Precise Risk Communication

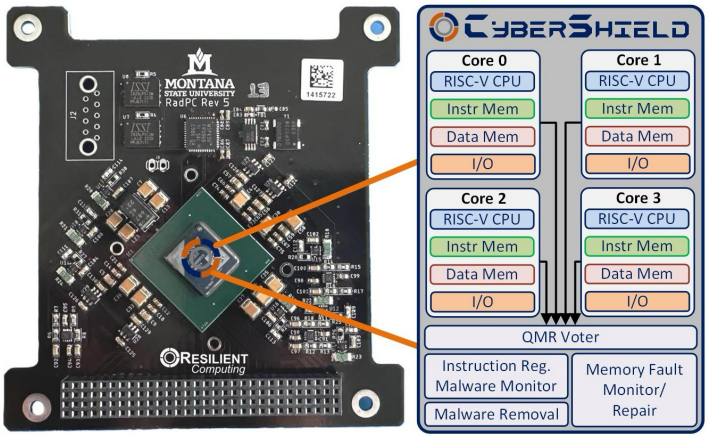
Advances in messaging systems, like automated text alerts, have improved the speed of hazard communications and the number of people who can be reached. However, the content and structure of risk messages are crucial for motivating message recipients to take protective actions. Federal messaging strategies inform but fail to motivate action, leading to inadequate preparation and, consequently, loss of lives and property. To address this, we developed the Domain Agnostic Risk Communication (DARC) Framework. The DARC Framework builds upon several decades of social science research and incorporates advancements in artificial intelligence to create impactful hazard messages. Currently, we are seeking funding to operationalize DARC as a software tool that will help FEMA and other government agencies craft messages rapidly that are effective at saving lives, property, and money. Funded by the National Science Foundation and DHS S&T. Project Lead: Dr. Ann Marie Reinhold; reinhold@montana.edu.



Conceptual Overview of the DARC Framework

Imparting Resilience in Critical Systems with CyberShield

Malware can cause the hardware of critical systems to fail. We pioneered the development of technologies that enable the recovery of hardware systems from sophisticated attacks. Attacks are thwarted because we build our hardware to be resilient-by-design. Resilience is achieved through a combination of keeping the design of the chip hidden and scrambling the hardware codes. This technology is the backbone of our patented CyberShield solutions. If malware attacks our chips, CyberShield detects the attacker's instructions and switches to a safe mode to keep the hardware of critical systems running. Funded by MSU spin-out Resilient Computing, LLC and DHS S&T. Project Lead: Dr. Brock LaMeres; lameres@montana.edu.



Malware-Resistant Hardware

www.montana.edu/cyber
clemente.izurieta@montana.edu | reinhold@montana.edu