Trusted Microelectronics

Cyber and Intelligence

The continued globalization of the microelectronics supply chain has placed the security of defense and industrial microelectronics at considerable risk. Examples of potential vulnerabilities include counterfeit devices, malicious hardware trojans, intellectual property theft, and leakage of sensitive information. Conventional microelectronics development has focused on the optimization of power, performance, and area constraints. These optimizations often come at the expense of hardware security. For this reason, the mitigation of these hardware security vulnerabilities requires drastic changes to the status quo of microelectronics design, assessment, validation, and verification. Effective research in these areas calls for multidisciplinary teams capable of developing novel techniques for a broad array of state-of-the-art microelectronics systems.

AREAS OF EXPERTISE

Turning quantified assurance and "zero-trust" concepts into a technical reality.

Digital Design Research

- Trust and assurance
- Custom design, proof-of-concept research ICs
- Synthesis, back-end, floor planning, timing, optimization, asynchronous circuits
- Quantify effectiveness of secure design and analysis techniques

Design Architecture and Tooling

- FPGA design and rapid hardware prototyping
- Design redaction for split manufacturing
- Tooling for rapid design
- Best-practices for secure design

Analog / RF Design

- Process authentication
- Custom RF circuits
- Power optimization for circuits

Assurance & Provenance

- Secure and flexible HW/SW co-design environments
- Cloud-based architectures for pre-silicon V&V
- Pre-silicon test automation
- Shifting verification into design and attack countermeasures

Packaging and Integration

- Board integration and physical layout
- ost-fabrication test design
- Embedded Security and Verification
- Firmware security and trust
- Design and SW reverse engineering and security assessment
- Attacks, vulnerabilities, and countermeasures
- Full-stack pre-silicon V&V

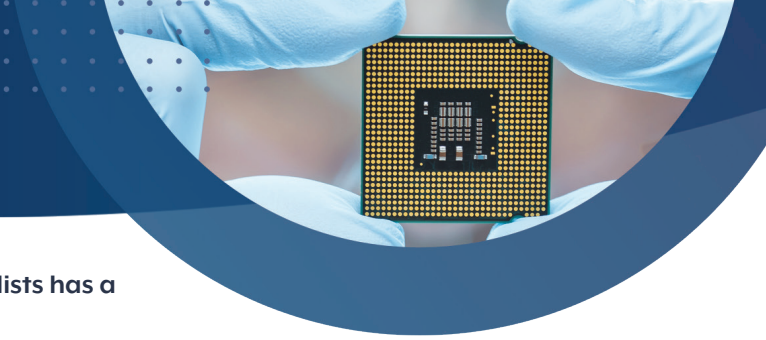
Verification & Verification

- Large scale data collection, analysis, and test automation
- Device characterization, machine learning
- Functional test for postproduction ICs and test articles
- Assessment of Second Order Effects (2OE) Systems (ASSESS)

Situation Awareness & Autonomy

- Human machine teaming
- Visualization tools and data comprehension

Trusted Microelectronics



PROVEN PERFORMANCE

KBR's team of expert microelectronics and cyber-R&D specialists has a trusted set of experience ready to assist you with:

Core Competencies

- Custom microelectronics design, analysis, and engineering
- Cyber security assessment, improvement, and risk mitigation
- Advanced test & evaluation
- Rapid, correct, and custom – digital and analog design, specialty is ASIC/SoC
- Specialized software and tooling

Key Technical Capabilities

- Agile SW/HW design, configuration management, DevOps
- Analog circuit design, implementation, and analysis
- Antenna fabrication and tuning
- Avionics test engineering
- Binary and system reverse engineering
- Chip process node authentication
- Cyber operations, cyber effects, security engineering
- Data visualization and exploration
- Design of experiments
- Device test, measurement, and evaluation
- Digital circuit design, implementation, and analysis
- Embedded systems design and analysis
- Hardware and software verification
- Human-computer interaction, teaming, autonomy
- Machine learning, AI, data science, and robotics
- Packaging, chip and PCB fabrication
- Project and program management
- RF and Mixed-signal circuits
- Software defined radio
- Software engineering and systems architecture

WHY KBR?

KBR has built a research and development team to derive a fundamental understanding of hardware security vulnerabilities and establish novel design and verification techniques for state-of-the-art defense and industrial microelectronics. The team aims to develop best-practices for microelectronics development to ensure security throughout the global supply chain. This includes the fabrication of integrated circuits in untrusted foundries without compromising intellectual property, the detection and prevention of counterfeits and hardware trojans, and the mitigation of side-channel leakage of sensitive information.

To maximize the impact of this work, the trusted microelectronics team collaborates with government agencies, academic researchers, and commercial businesses to tackle the toughest problems across all areas of hardware security.

NEXT STEPS

Let's talk about your security goals and how KBR can help you achieve them. Contact us to learn more and schedule a consultation at kbr.com/TrustedMicroelectronics.

ABOUT US

We deliver science, technology and engineering solutions to governments and companies around the world. KBR employs approximately 28,000 people performing diverse, complex and mission critical roles in 34 countries.

KBR is proud to work with its customers across the globe to provide technology, value-added services, and long-term operations and maintenance services to ensure consistent delivery with predictable results. At KBR, we are the Team Behind the Mission.

kbr.com