SAND2015-2139C

Exceptional service in the national interest

Sandia National Laboratories

Secure Processing Design & Development

Sandia's Engineering Design and Integration Center has developed NSA-approved secure processing systems for U.S. Government customers for over two decades. Leveraging technology and processes established in support of our primary mission as steward of the U.S. nuclear stockpile, Sandia has developed and implemented trusted design practices and partnered with other trusted organizations to provide the U.S. Government with secure hardware and software solutions for a number of national security applications.

Sandia's secure processing systems are primarily embedded systems that include security-based hardware architectures incorporating custom-designed Application-Specific Integrated Circuits (ASICs) that provide the hardware trust anchor necessary for meeting NSA's stringent security requirements for Type-1 cryptographic systems. Sandia's Engineering Design and Integration Center performs the systems engineering and design for the secure processing systems, and develops the specification and test bench for the custom ASIC. The test bench includes an initial field-programmable gate array (FPGA) emulation of the custom ASIC for specification validation and early software development, and ultimately provides a system-level host for validation of the custom ASIC upon fabrication. Sandia's Engineering Design and Integration Center also develops the operational software using formal, established software engineering methods and rigorous, multi-layered verification techniques in a fully-trusted development environment.

Typical Security Design Features Implemented:

Hardware Security Features

- Built-In self test
- Early error detection
- No single-bit security decisions
- Parallel error detection
- Serial error blocking
- Separation of data paths
- Multiple redundant processors
  - Work together to transmit data
- Watchdog timers
- Analog sensors
- Test Interface control
- Hardware AES decryption
- Masked BOOT ROM

Software Security Features

- Self test
- Early error detection
- No single-bit security decisions
- Limit retries
- Presumption of failure
- Verify proper processing paths
- Maintain positive data control
- Zeroization
- Known-good-answer tests
- Halt operations on error
- Modernized cryptography

APPLICATION SPECIFIC

Our expertise is in providing fully-programmable yet secure cryptographic processing systems that can host a wide variety of user-defined applications. We follow NSA's Fail-Safe Design & Assurance principles to protect against compromise of critical program information with a high level of assurance, and we conduct highly-detailed fault-tree analyses of our security-critical systems and perform NSA-witnessed security verification to ensure that any faults that would lead to an unauthorized event are detected and handled appropriately.

U.S. DEPARTMENT OF ENERGY

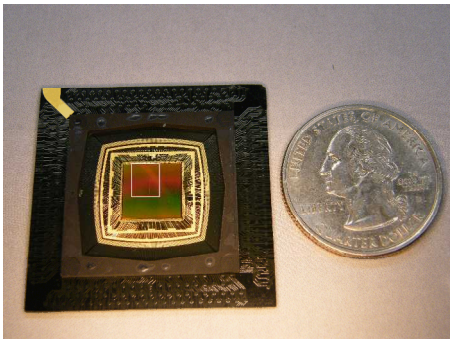
NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

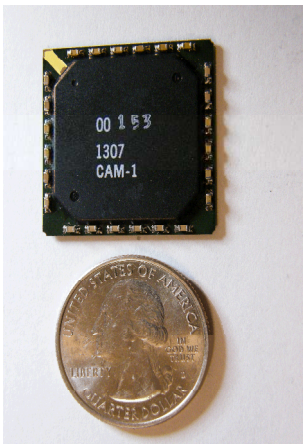
Sandia National Laboratories

ENGINEERING DESIGN AND INTEGRATION CENTER

The Sandia-designed Key Data Processor (KDP) cryptographic engine mandated by the Joint Chiefs of Staff for use in all military Global Positioning System (GPS) receivers has been programmed for use in over 1,000,000 units. Sandia worked with internal and external organizations to develop this system-on-chip, National Security Agency certified security architecture enabling GPS receiver manufacturers to securely integrate the KDP into their custom ASICs realizing cost, size, and power reductions necessary for insertion into constrained applications including precision guided munitions and artillery shells. The KDP-IV shown at the right was fabricated at the IBM Trusted Foundry using the 90nm CMOS9LP Trusted Flow. Sandia has also fabricated a KDP-III chip on IBM's 130 nm CMOS8RF-LP Trusted Flow.

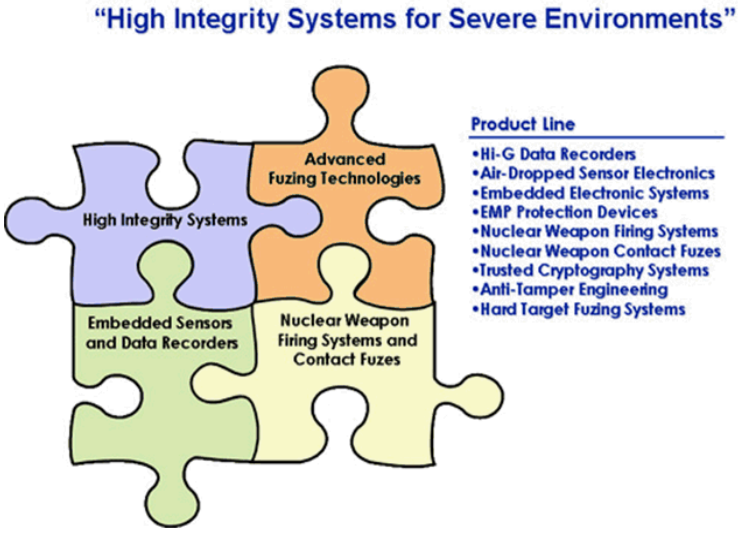


Using Sandia's own Trusted Flow, the Engineering Design and Integration Center has developed and fabricated the Common Authentication Module (CAM) ASIC, a secure processing platform meeting strict National Security Agency security requirements for Nuclear Command and Control and similar high consequence applications. Built on Sandia's 350nm CMOS7 rad-hard process, the CAM ASIC engineering development followed best practices including requirements traceability, formal verification, and Universal Verification Methodology (UVM) to deliver fully functional parts within 15 months of the design start.



Selected Engineering Design and Integration Center Capabilities:

- **Extreme Environment Devices -** Engineering, designing, integrating, and field support of data recorder instrumentation used to characterize impact events and other harsh high-G environments. Data acquired is used to support specifications, design verification, and model validation.
- **Initiation Subsystems -** Designing and developing advanced electrical and optical components, ultra-miniature high voltage or optically-driven capacitive discharge units, and fully integrated fuzes and firing systems.
- **Low-Power Sensor Systems -** Designing and developing extreme low power and harsh environment survivable sensor systems capable of detecting, identifying, and communicating events of interest through local networks or long-range communications links.



- **NW Firing Systems and Contact Fuzes -** Designing and developing state-of-the-art, ruggedized, high reliability subsystems and components to support the nation's stockpile modernization programs.
- **"Trusted" Systems –** Designing national security systems exhibiting integrity of the underlying hardware and software, and resistance to exploitation through Fail Safe Design Assurance and Anti-tamper methods.

For more information email mwbrown@sandia.gov or dljense@sandia.gov

U.S. DEPARTMENT OF ENERGY
NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories