Center for Prediction of the Reliability, Integrity, and Security of Microelectronics (PRISM 2.0)

P. Bermel (ECE), M. Alam (ECE), J. Appenzeller (ECE), Z. Chen (ECE), E. Delp (ECE), C. Handwerker (MSE), G. Klimeck (ECE), A. Shakouri (ECE), P. Ye (ECE)
A. Strachan (MSE), G. Subbarayan (ME)
High Priority Project Areas for PRISM 2.0

Combining NSWC Crane needs with Purdue & IU expertise:

- Fraud detection: characterizing the age of electronics via rapid, self-referenced measurements (Alam, Appenzeller, Bermel)
- Protection from malicious attack: TMD FETs for secure circuits through polymorphic logic gates (Appenzeller, Chen, Hu, Niemier)
- Lifetime prediction: Multiscale end-to-end reliability modeling of electronic and MEMS devices (Strachan, Klimeck)
- Reliability failure: High-resolution thermal characterization for early fault detection in power electronics (Shakouri, Ye, Bermel)
- Radiation-endurance modeling of floating gate and charge-trapping non-volatile memory (Alam)
- Microbump Reliability of 3D Packages: Accelerated Testing and Lifetime (Handwerker, Blendell)
- Techniques for software vulnerability detection (Delp)
Growing threats in microelectronics come from multiple directions and multiple sources along the supply chain, and for multiple reasons:

- **Quality escape** – products failing to meet specifications or required performance
- **Reliability failure** – failure during use or from environmental factors
- **Fraudulent products** – counterfeit or other than genuine devices from relabeling, cloning, out-of-spec, etc.
- **Malicious insertion** – by hard or soft coding or defects to enable physical attack or to cause mission failure
- **Anti-tamper** – unauthorized extraction of sensitive intellectual property
- **Emerging threats** combining two or more categories

-- Kristen J. Baldwin, Principal Deputy, Office of the Deputy Assistant Secretary of Defense (NDIA PPP Summit/Workshop, May 20, 2014)
Partnerships (particularly, Crane-Purdue-Indiana) will cover 3 areas:

- **Research**
  - Crane role: needs assessment, testing capabilities, funding & advocacy
  - Purdue role: intensive R&D for pressing needs; multiple white papers written

- **Workforce development**
  - Crane: Provide personnel skill set requirements and funding (e.g., NEEC)
  - Purdue: train students from Purdue and other IN universities to understand and develop critical technologies needed by DoD

- **Critical technologies**
  - Crane: identify government needs and convene stakeholders
  - Businesses: identify needs of DoD and non-DoD clients
  - Purdue: build/join broad consortia (iNEMI); use existing and nascent research, including IP, to attack key problems; promote commercialization

- **Microelectronics Integrity Conference – 26-28 July 2016**
  - Ernesto Marinero gave 15 minute presentation entitled: “Spintronic Devices for Trusted Microelectronics”
  - Purdue students awarded 1st, 2nd, 3rd in poster competition
  - Wide range of DoD agencies in attendance
  - DoD stakeholders in attendance: Lockheed Martin, Ball Aerospace, General Dynamics, Boeing, and more
Purdue Offers Unique Capabilities to Address These Challenges

Decades of leadership in microelectronics: theory, simulation, characterization, and fabrication

- Intrinsic reliability in nanoscale CMOS electronics
- Interconnect design and reliability for existing and emerging technologies
- Relate complex nanostructures to circuit performance - microstructures to device performance
- Connect characterization and simulation

Multiple Delivery and Collaboration Mechanisms

- Technology agnostic, end-to-end approach
- Web-based platform to share tools and resources
- Joint research, standards and guideline development
Challenge: Today’s Microelectronics can be Hacked, Counterfeited, and Degraded

- Threats emanate from nation-states, terrorist organizations, and rogue individuals
- Solutions:
  - Early lifecycle identification of critical & trusted components
  - Protect critical components through trusted companies and system design
Prior Work and Remaining Gap

- DARPA SHIELD program: developed dielets to prevent counterfeiting

- DARPA IRIS (Integrity & Reliability of Integrated Circuits): use hyperspectral microscopy to “X-ray” ICs

- No program can detect age without references, identify device-level problems, or predict for new devices
Conclusions / Next Steps

• Trusted electronics are a key economic and national security priority for government, universities, and business

• Purdue can offer the full spectrum of research capabilities in microelectronics -- theory, modeling, fabrication, and characterization – to help tackle this problem in both existing and emerging electronic designs and packages

• We have created partnerships with Crane, Notre Dame, SRC, NSF, and the microelectronics industry (e.g., iNEMI) to develop timely and relevant solutions

• We have assembled a targeted set of projects based on their input to address these issues, which we are ready to pursue immediately with ARI support