SAND2022-6823C

Sandia National Laboratories

Exceptional service in the national interest






SANDIA NATIONAL LABORATORIES

CHEST May

William Zortman wzortman@sandia.gov (505) 401-1972
Vivian Kammler vgkamml@sandia.gov

UPDATED DECEMBER 2021

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND2019-11784 PE

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

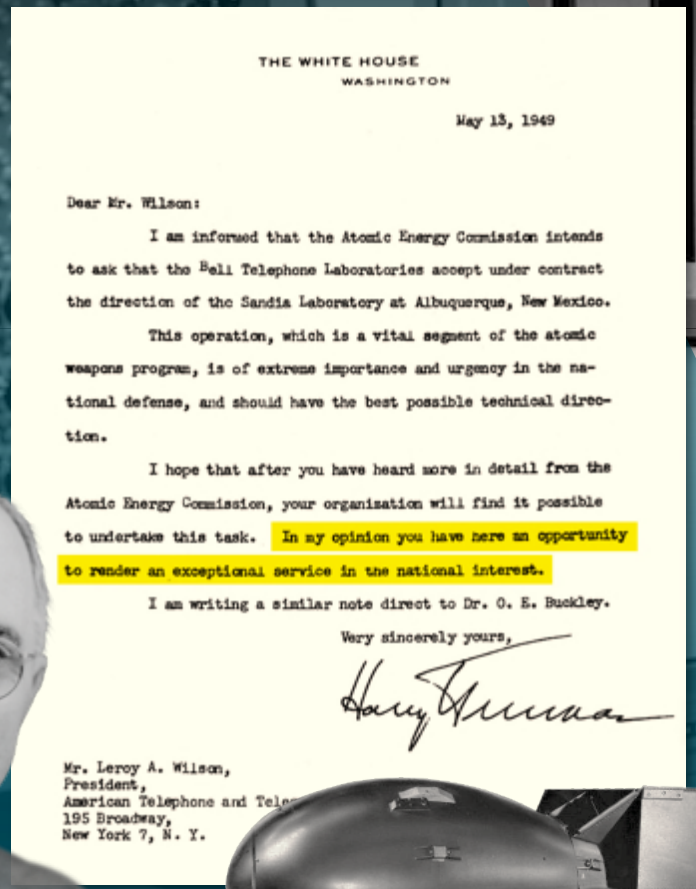
SANDIA IS A FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTER(FFRDC) MANAGED AND OPERATED BY

National Technology & Engineerin Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc.

Government owned, contractor operated

FFRDCs are long-term strategic partners to the federal government, operating in the public interest with objectivity and independence and maintaining core competencies in missions of national significance

SANDIA'S HISTORY IS TRACED TO THE MANHATTAN PROJECT



THE WHITE HOUSE
WASHINGTON

May 13, 1949

Dear Mr. Wilson:

I am informed that the Atomic Energy Commission intends to ask that the Bell Telephone Laboratories accept under contract the direction of the Sandia Laboratory at Albuquerque, New Mexico.

This operation, which is a vital segment of the atomic weapons program, is of extreme importance and urgency in the national defense, and should have the best possible technical direction.

I hope that after you have heard more in detail from the Atomic Energy Commission, your organization will find it possible to undertake this task. In my opinion you have here an opportunity to render an exceptional service in the national interest.

I am writing a similar note direct to Dr. O. E. Buckley.

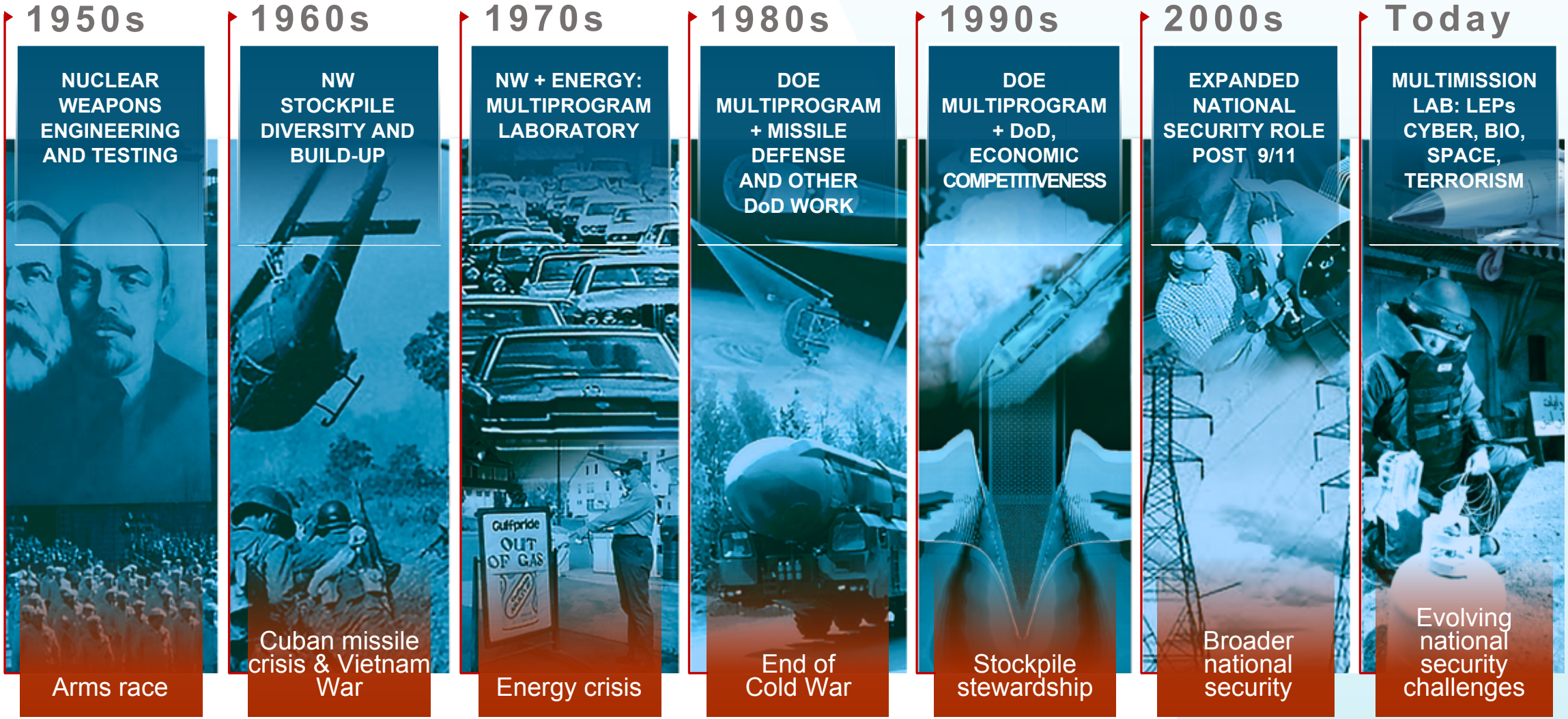
Very sincerely yours,

Harry Truman

Mr. Leroy A. Wilson,
President,
American Telephone and Tele
195 Broadway,
New York 7, N. Y.

- July 1945: Los Alamos creates Z Division
- Nonnuclear component engineering
- November 1, 1949: Sandia Laboratory established
- AT&T: 1949–1993
- Martin Marietta: 1993–1995
- Lockheed Martin: 1995–2017
- Honeywell: 2017–present

OUR MULTIMISSION ROLE HAS EXPANDED OVER THE DECADES

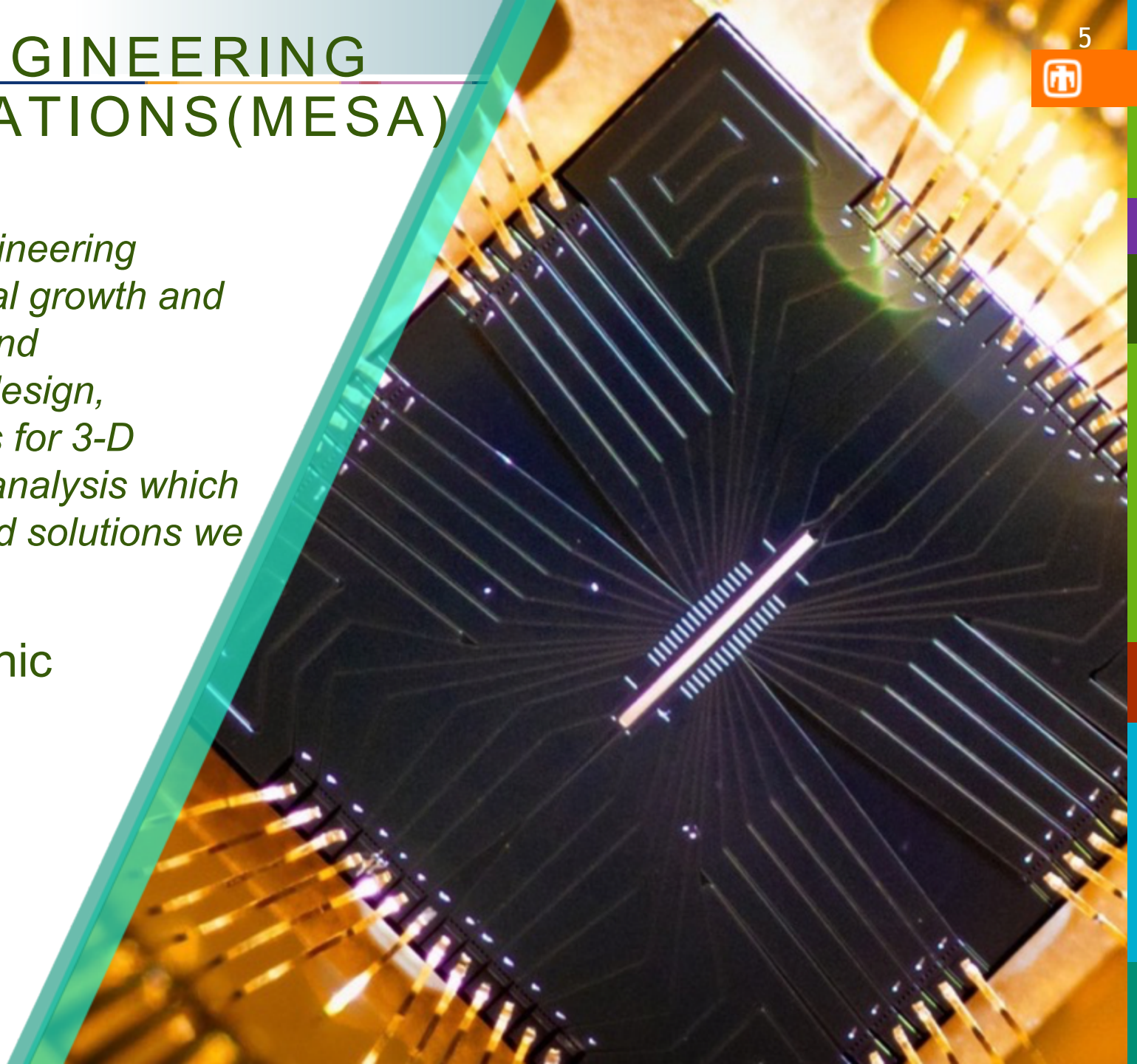


MICROSYSTEMS ENGINEERING SCIENCE & APPLICATIONS(MESA)

MESA provides scientific and engineering expertise in areas such as material growth and process development for silicon and compounds, device and product design, advanced packaging technologies for 3-D integration, reliability, and failure analysis which makes possible the custom trusted solutions we deliver to the nation today.

CAPABILITIES

- Microsystem and electronic technology research
- Trusted and rad-hard microelectronics foundry



Example projects available for university collaboration

Electromagnetic pulse interactions with microelectronics
- Collaboration with UC Boulder
- Modeling in COMSOL and lab experiments on test chips fabricated at Sandia

Understanding electromagnetic emanations from microelectronics
- Consultation with UC Boulder and UT Austin
- Modeling in Sandia developed microelectronics simulation environments and validation in test chips

<u>UNMCollaborations (Plusquelic):</u>

Design and resilience of strong Physically Unclonable Functions through data-driven models

Fault analysis on RISC-V microprocessors using advanced features of FPGAs

Fail-Safe RISC-V systems

FPGA applications to Quantum Computing

What we look for in a project

A good place to start

The Heilmeier Catechism

What are you trying to do? Articulate your objectives using absolutely no jargon.

How is it done today, and what are the limits of current practice?

What is new in your approach and why do you think it will be successful?

Who cares? If you are successful, what difference will it m

What are the risks?

How much will it cost?

How long will it take?

What are the mid-term and final "exams" to check for success?

George H. Heilmeier

DARPA operates on the principle that generating big rewards requires taking big risks. But how does the Agency determine what risks are worth taking?

George H. Heilmeier, a former DARPA director (1975-1977), crafted a set of questions known as the "Heilmeier Catechism" to help Agency officials think through and evaluate proposed research programs.
www.darpa.mil

What is your project about? Are you doing physics or engineering?

Discover – uncommon in HW security, since we are doing engineering, yet there is some fundamental discovery missing in the field of HW security

Create – this is very common since we are doing engineering and there are a lot of mitigations being proposed in research projects

- Going back to Heilmeir – what difference will it make?

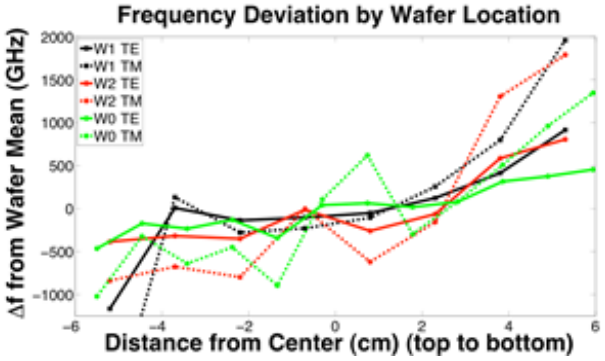
Prove – assess maybe

- If you are trying to prove that your mitigation works this may be the checkpoint you get at the end of your project, some level of independent assessment – so important in security because measurement can be elusive where in other disciplines it is straightforward.
- And a good assessment can lead to a new project

Fundamental discovery in HW security

PUFs – (a physics problem, Discover)

- What is driving the entropy?
  - Will you or the adversary find out first?
- Is the entropy durable through the development process? Is it discoverable? In some cases it is.
- Here is an example using optical resonators on silicon that shows how understanding the manufacturing process and the physical interactions can yield a prediction of the

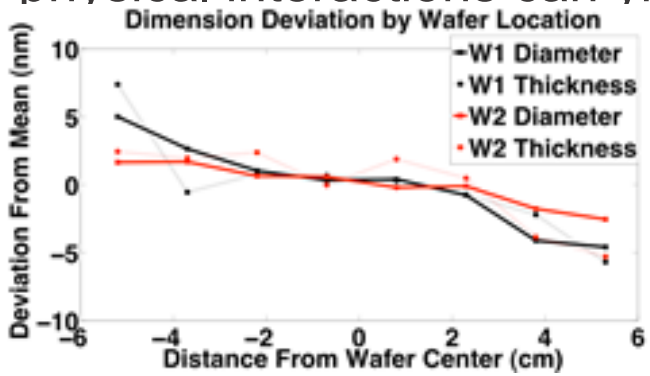


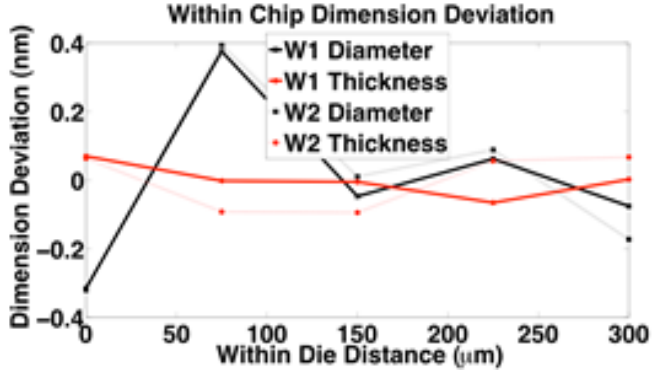
from modeling and test chips

unknown

measurement

$$\begin{bmatrix} \frac{df}{dT}\Big|_{TE} & \frac{df}{dD}\Big|_{TE} \\ \frac{df}{dT}\Big|_{TM} & \frac{df}{dD}\Big|_{TM} \end{bmatrix} \times \begin{bmatrix} \Delta T \\ \Delta D \end{bmatrix} = \begin{bmatrix} \Delta f_{TE} \\ \Delta f_{TM} \end{bmatrix}$$





frequency measurement changes across test wafers → matrix inversion → yields dimension deviations in nm

W. Zortman, D. Trotter, and M. Watts, "Silicon photonics manufacturing," Opt. Express 18, 23598-23607 (2010).

Using a representative design in a test chip, measuring it, understanding the physics of the oscillators and the manufacturing process a predictive model was built and biases were revealed that can be broadly applied.

Finally, the within chip deviations were extracted. The spike in device 2 was due to a mask snap grid error … we give the mask to the adversary.

Other hard problems in hardware security

Side Channel Analysis Countermeasures

- What problem are we trying to solve?
- Is the source of the signal at the gate level or in the power distribution layers?
- Can we do better than masking?

Finding credible supply chain threats

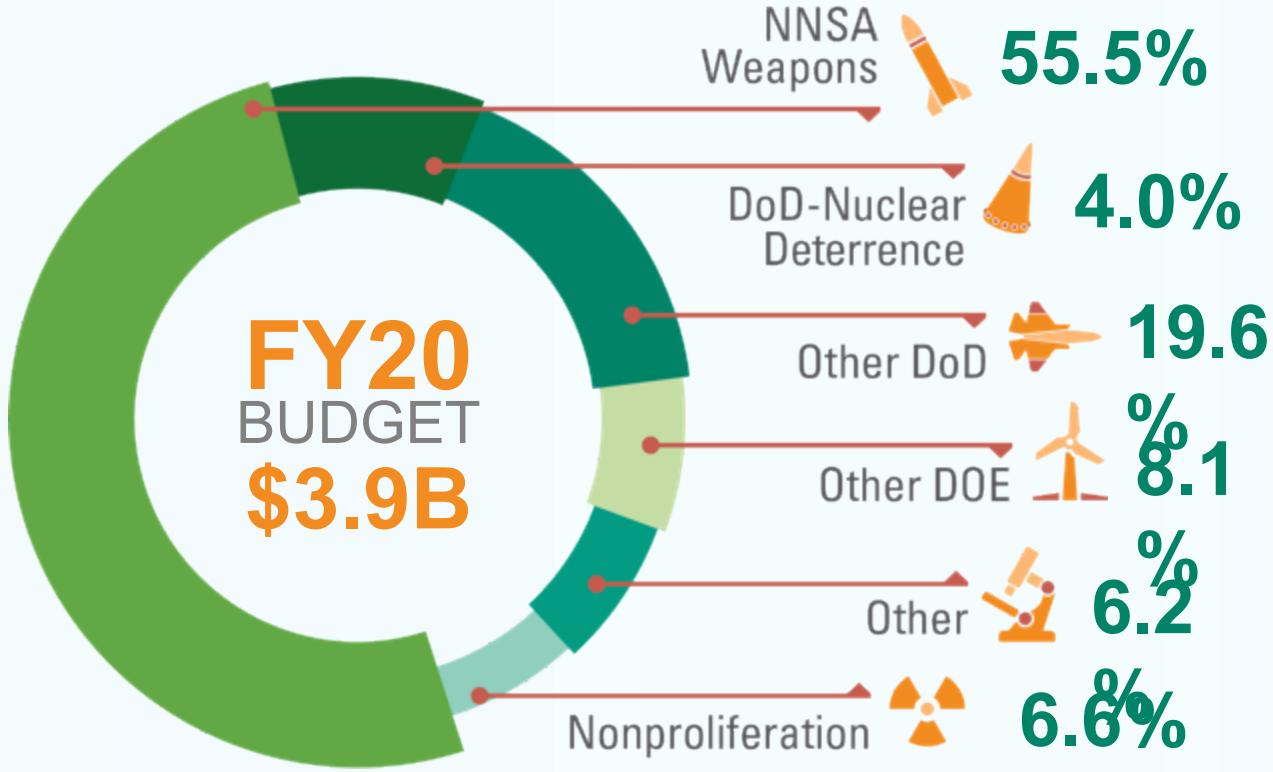
- Modifying a 5nm fabrication line is possible, but it's expensive and risky
- Adversarial projects should point the way
- How will the adversary carry out the attack?

If you are working on countermeasures

- What attack are you trying to defeat
- Consider having a colleague assess your solutions

BACKUP

SANDIA'S BUDGET COVERS A BROAD RANGE OF GOVERNMENT AND OTHER WORK



OTHER

Department of Homeland Security
Other federal agencies | Nonfederal entities
CRADAs, licenses, royalties | Inter-entity work

DoD

Air Force | Army | Navy
Defense Threat Reduction Agency
Ballistic Missile Defense Organization
Office of the Secretary of Defense
Defense Advanced Research Projects Agency
Intelligence Community

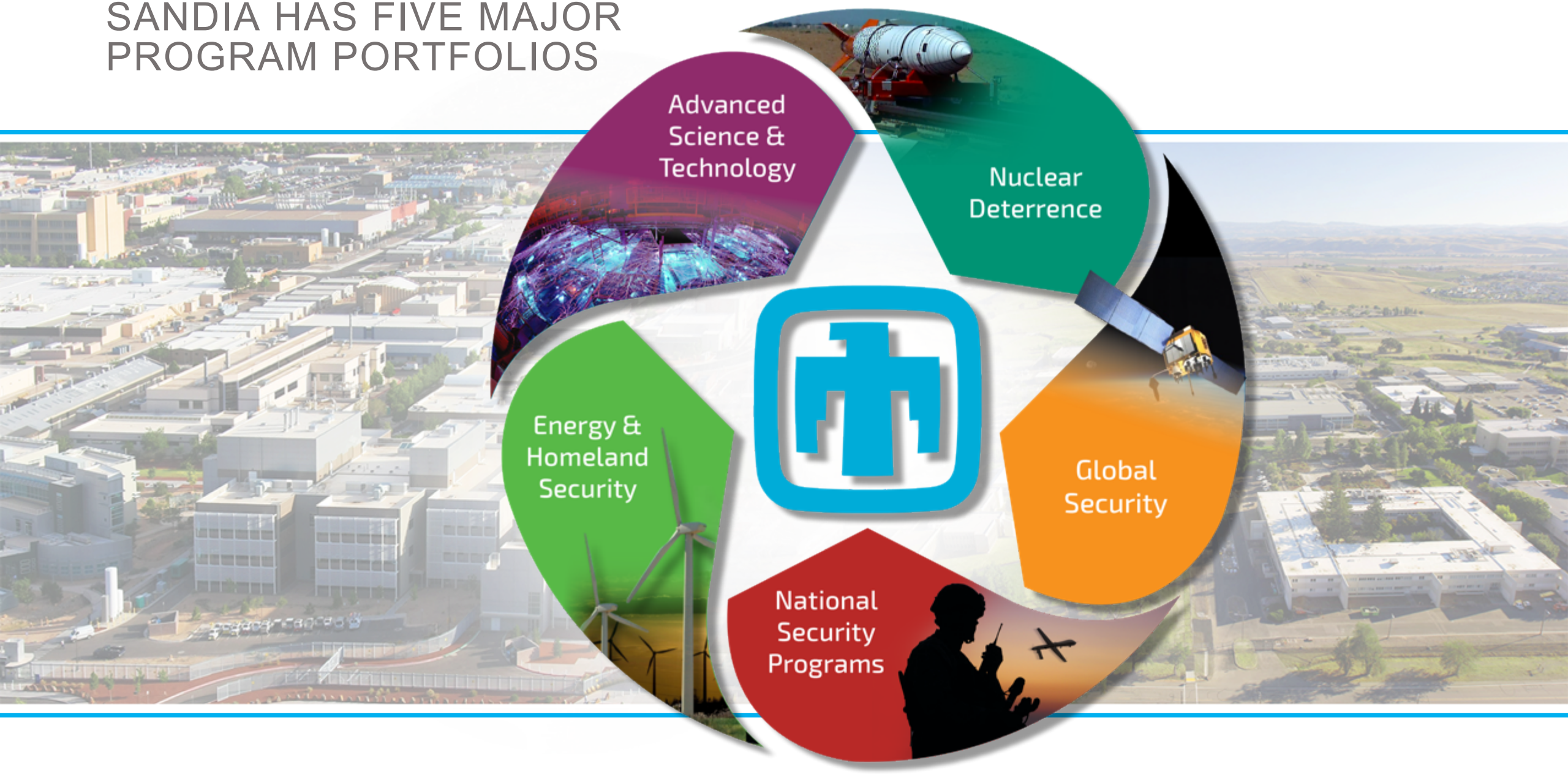
OTHER DOE

Science
Energy Efficiency and Renewable Energy
Nuclear Energy
Environmental Management
Electricity Delivery and Energy Reliability
Other DOE

NONPROLIFERATION

NNSA/NA20 | State Department

SANDIA HAS FIVE MAJOR PROGRAM PORTFOLIOS

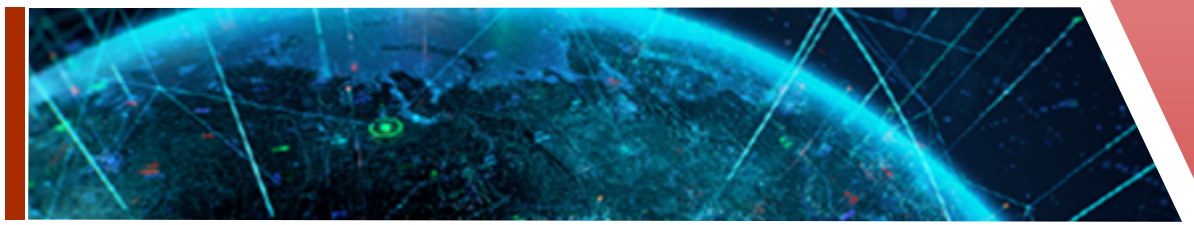


NATIONAL SECURITY PROGRAMS

Provide trusted, threat-informed pathfinder technology for national security

Information Operations

Proliferation Assessments

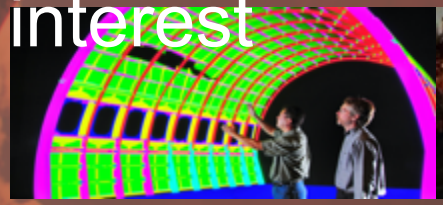


Science & Technology Products

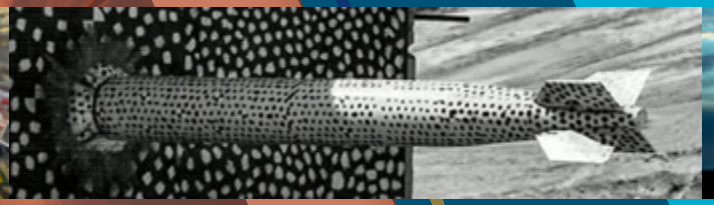
Surveillance & Reconnaissance

Integrated Military Systems

Exceptional service in the national interest








Sandia National Laboratories