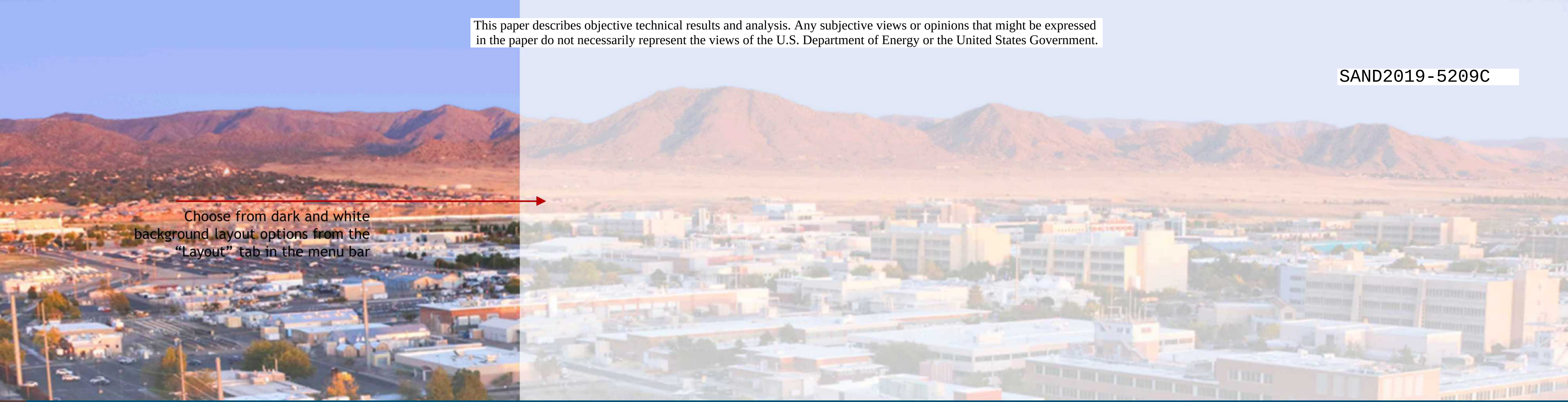
This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2019-5209C



Choose from dark and white background layout options from the “Layout” tab in the menu bar

Safeguards Information Assurance By Design

41st ESARDA Annual Meeting

Stresa, Italy

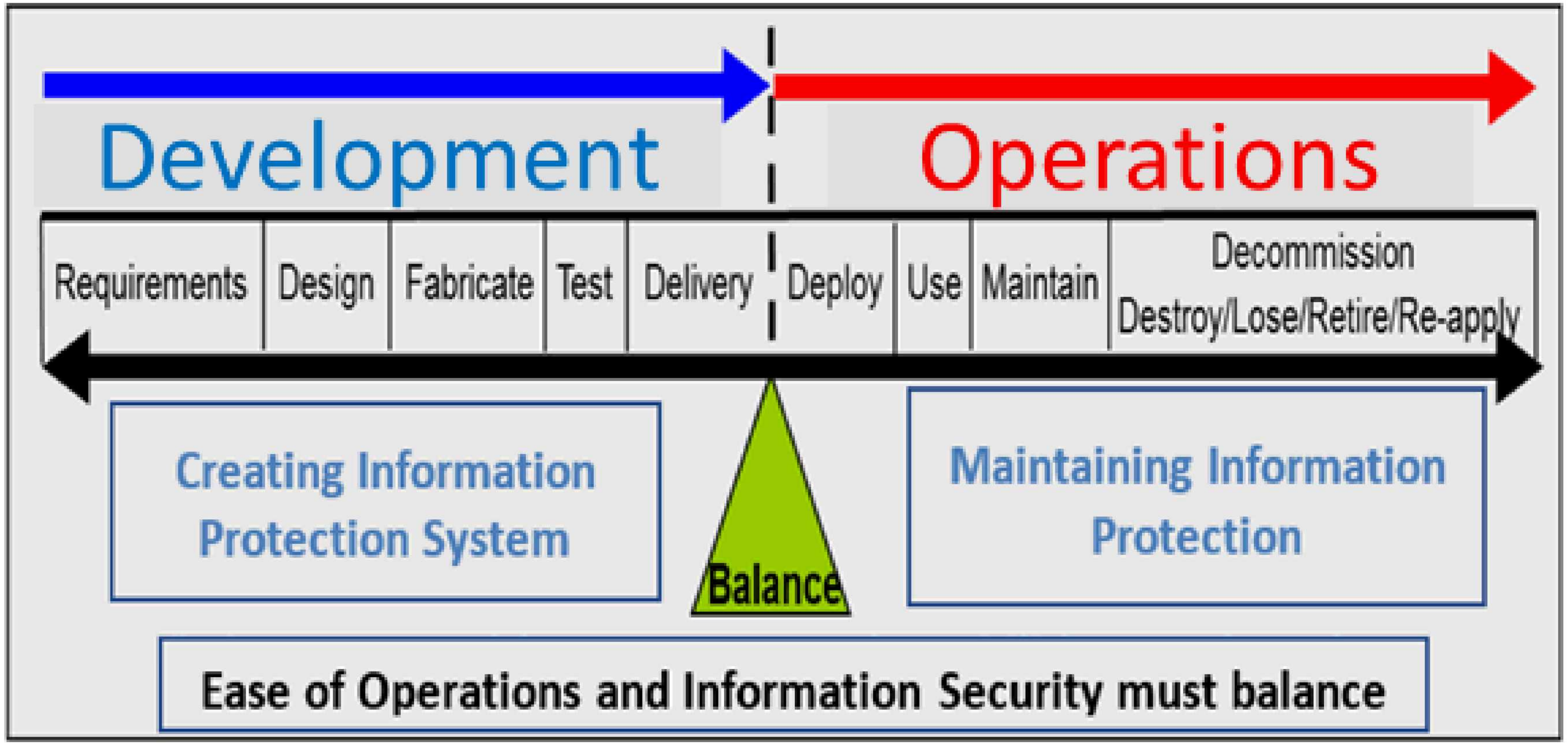
May 14-16, 2019

Dianna S. Blair
F. Mitch McCrory

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.

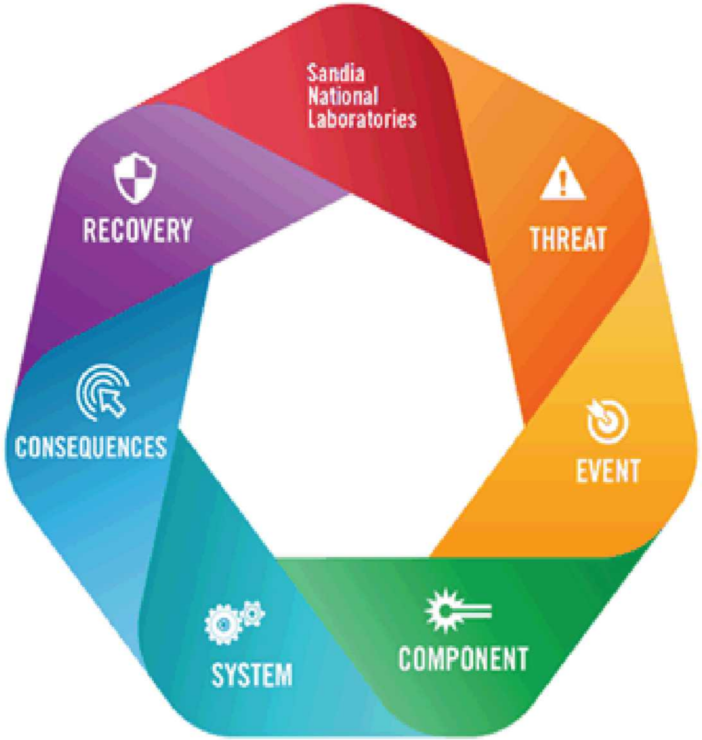
Safeguards Information Assurance by Design (SIAD)

- SIAD is intended to address information risks throughout the lifecycle of a safeguards system, instrument, or component


Development
Operations
Requirements
Design
Fabricate
Test
Delivery
Deploy
Use
Maintain
Decommission
Destroy/Lose/Retire/Re-apply
Creating Information Protection System
Balance
Maintaining Information Protection
Ease of Operations and Information Security must balance

SIAD utilizes various tools to manage information risks

- Assist in
  - Defining requirements
  - Validating effectiveness
- Including
  - **Risk management methodologies**
  - Supply chain risk management
  - **Secure Architectures**
  - **Modeling and Simulation**
  - Red teaming

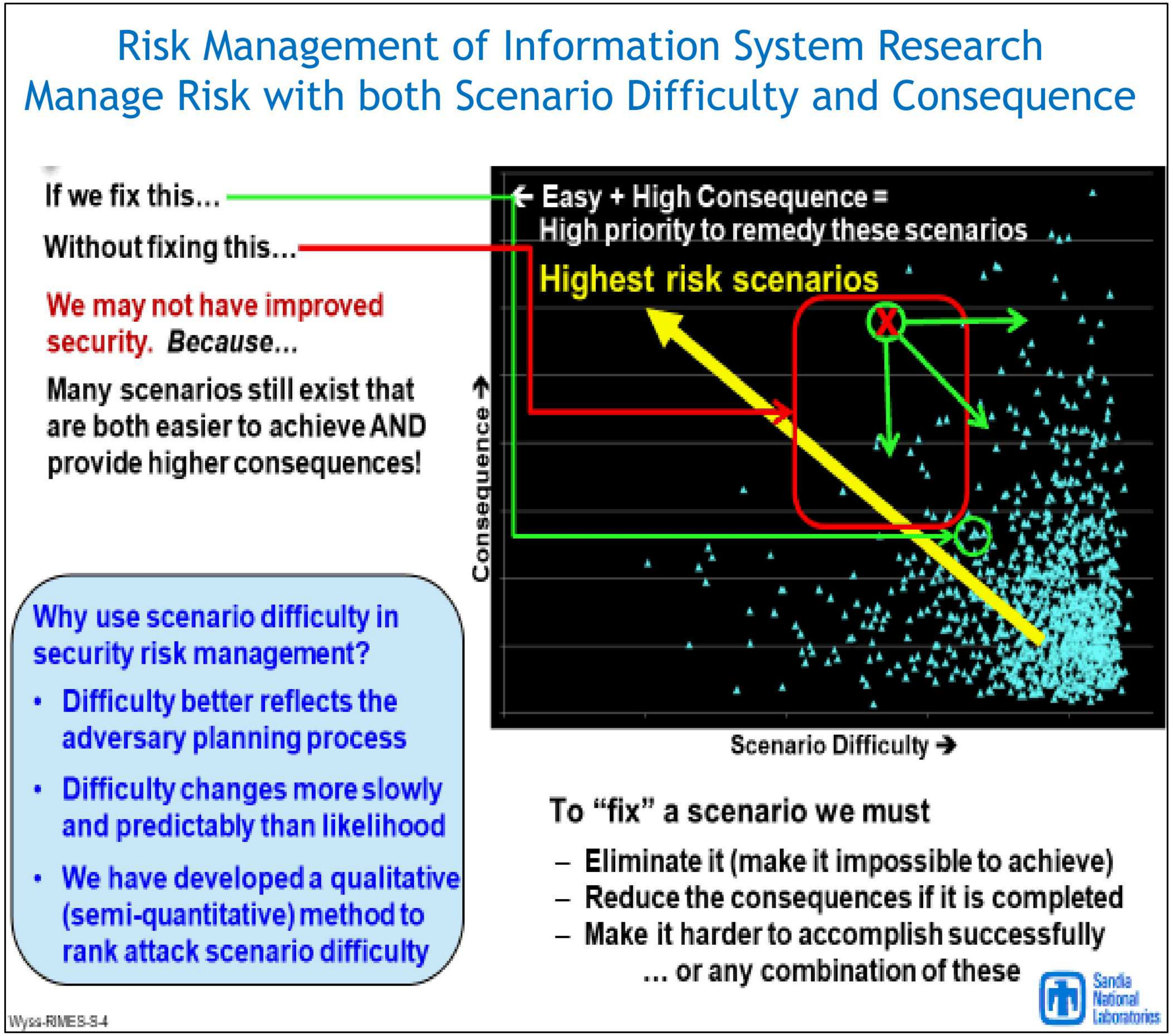


Integrated Cyber Physical Impact Analysis (ICPIA)™

Full Spectrum Modeling Framework

SIAD utilizes various tools to manage information risks

- Assist in
  - Defining requirements
  - Validating effectiveness
- Including
  - **Risk management methodologies**
  - Supply chain risk management
  - Secure Architectures
  - **Modeling and Simulation**
  - **Red teaming**



Risk Management of Information System Research
Manage Risk with both Scenario Difficulty and Consequence

If we fix this...

Without fixing this...

We may not have improved security. *Because...*

Many scenarios still exist that are both easier to achieve AND provide higher consequences!

Why use scenario difficulty in security risk management?

- Difficulty better reflects the adversary planning process
- Difficulty changes more slowly and predictably than likelihood
- We have developed a qualitative (semi-quantitative) method to rank attack scenario difficulty

To "fix" a scenario we must

- Eliminate it (make it impossible to achieve)
- Reduce the consequences if it is completed
- Make it harder to accomplish successfully

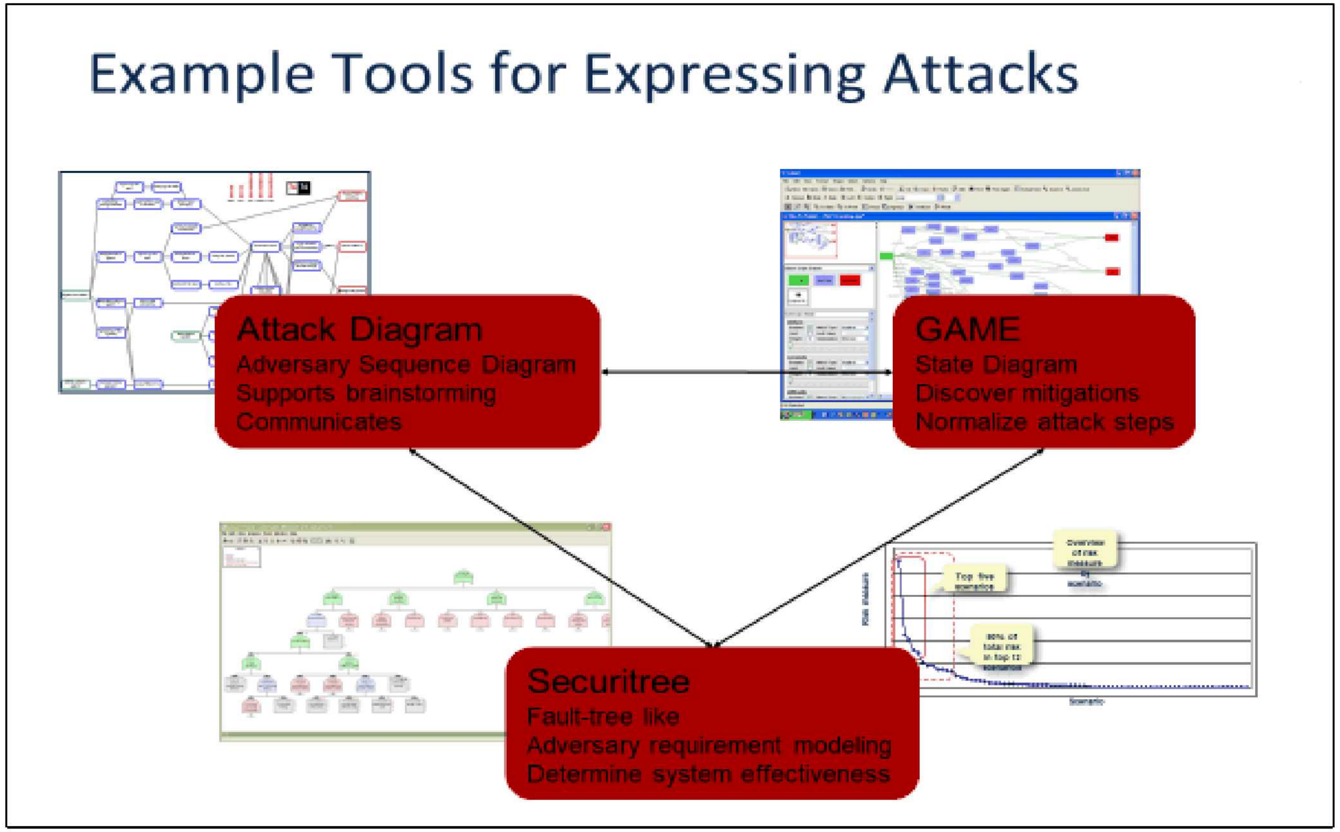
... or any combination of these

Sandia National Laboratories

Wyss-RIMES-S-4

SIAD utilizes various tools to manage information risks

- Assist in
  - Defining requirements
  - Validating effectiveness
- Including
  - **Risk management methodologies**
  - Supply chain risk management
  - **Secure Architectures**
  - **Modeling and Simulation**
  - **Red teaming**



Example Tools for Expressing Attacks

Attack Diagram
Adversary Sequence Diagram
Supports brainstorming
Communicates

GAME
State Diagram
Discover mitigations
Normalize attack steps

Securitree
Fault-tree like
Adversary requirement modeling
Determine system effectiveness

Main points

- Information systems present vulnerabilities and risks throughout their lifecycle. These do not end when designs are finalized, built, deployed or even decommissioned.
- It is necessary to control distribution of details regarding information system operations or vulnerabilities. Knowledge of the system arms an adversary.
- Adversaries evolve over time and continual reexamination of information system vulnerabilities and risks are critical to ensuring dependable performance.
- There is no such thing as a standalone or isolated system. Protection is needed for all sensitive digital assets with a graded approach applied.