SAND2021-9862C

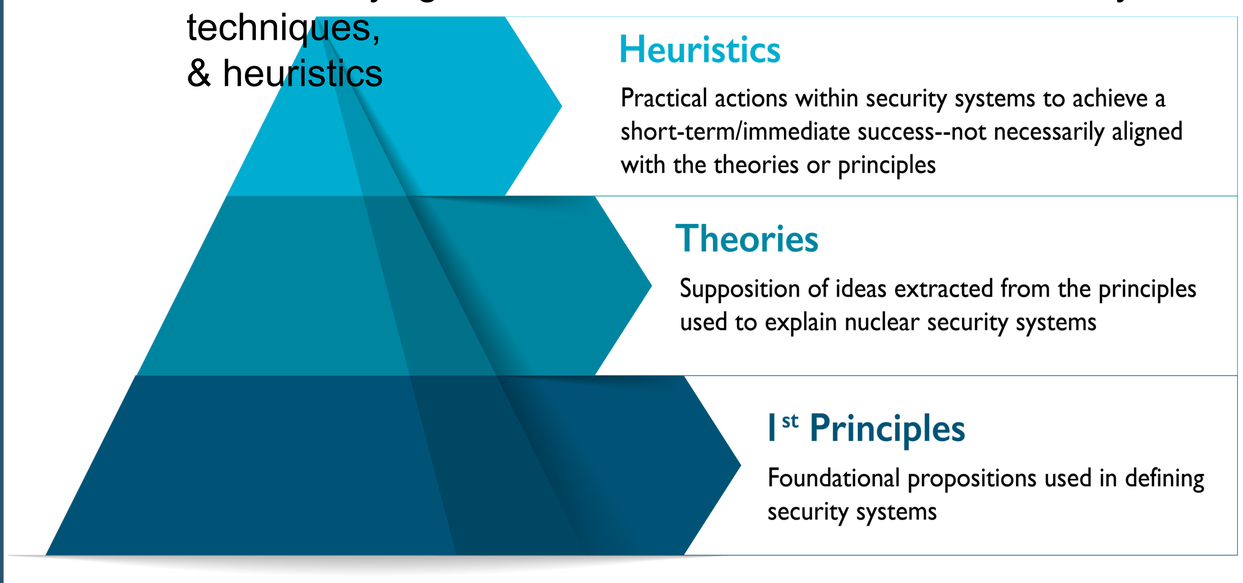
Sandia National Laboratories

Logical Foundations for Protecting Materials and Facilities from those with Malicious Intent—Proposed 1st Principles for Security Systems

Sue A. Caskey, Adam D. Williams, Lauren Crabtree, and John "JR" Russell Sandia National Laboratories, Albuquerque, NM, USA, sacaske@sandia.gov ; adwilli@sandia.gov ; lcrabtr@sandia.gov ; jlrusse@sandia.gov*

The ***1st Principles for Security Systems*** presented here are:

- Based on a dynamic, systems theoretic paradigm of nuclear security.
- Derived from both professional observation & empirical interviews with SMEs
- The underlying foundation for associated theories, analysis techniques, & heuristics



Conceptual hierarchy of logical elements for security systems

The 1st principles of security systems are defined as:

1. Security risk will never be zero
2. Security risk is dynamic
3. Threats are adaptive

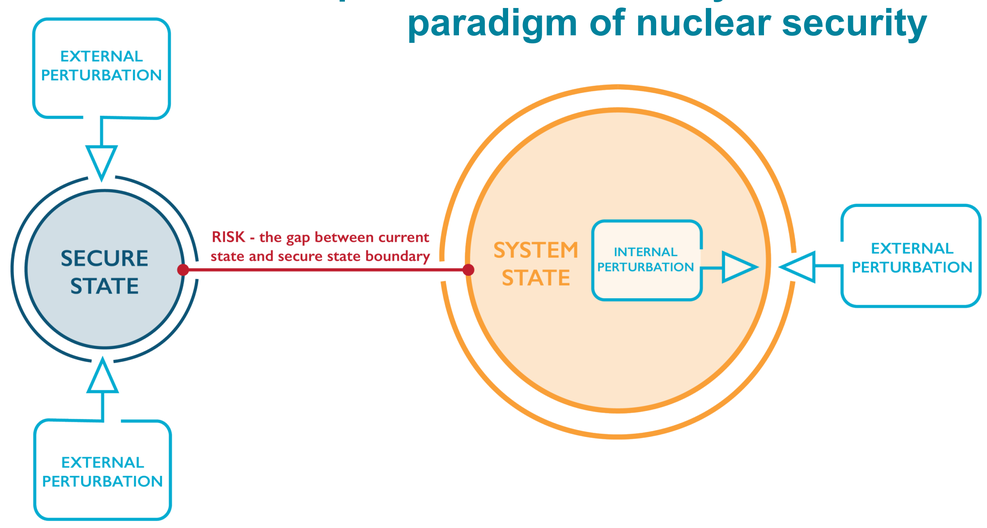
Representative Elements of Security Systems Theory

- Adequate security performance emerges from ***actively observing*** & ***proactively responding*** to security risk
- A security system should ***not be*** evaluated/analyzed as ***static***
- A security system must also be implemented ***to support & align*** with the ***operational objectives***

Representative Example Heuristics

- Without detection, physical security barriers are only a deterrence
  - Ex: *2005 Brazil bank heist*
- Without assessment and response to the detected threat there is no detection
  - Ex: *2012 security incident Y-12*
- Without resilience security risk will grow over time
  - Ex: *2016 Dyn DDoS Cyber Attack as compared to 2020 AWS DDoS attack*

Representation of the systems theoretical paradigm of nuclear security



Specific characteristics related to this ***paradigm of security*** include:

- Security = being in a state free from threat, not just the absence of attractiveness.
- The security state is dynamic, impacted by external perturbations (environment or threat)
- Security systems are *dynamic, complex systems* whose performance directs movement RE: a secure state
  - Any internal (e.g. component behavior) or external perturbations (e.g., weather, threat actor capabilities, etc.) can move the system closer or further from this state.
- Security *risks* are the gaps between current state and secure state.

Venn diagram reflecting the three 1st principles of security systems

U.S. DEPARTMENT OF ENERGY
National Nuclear Security Administration

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.
SAND No. _____

Sandia National Laboratories