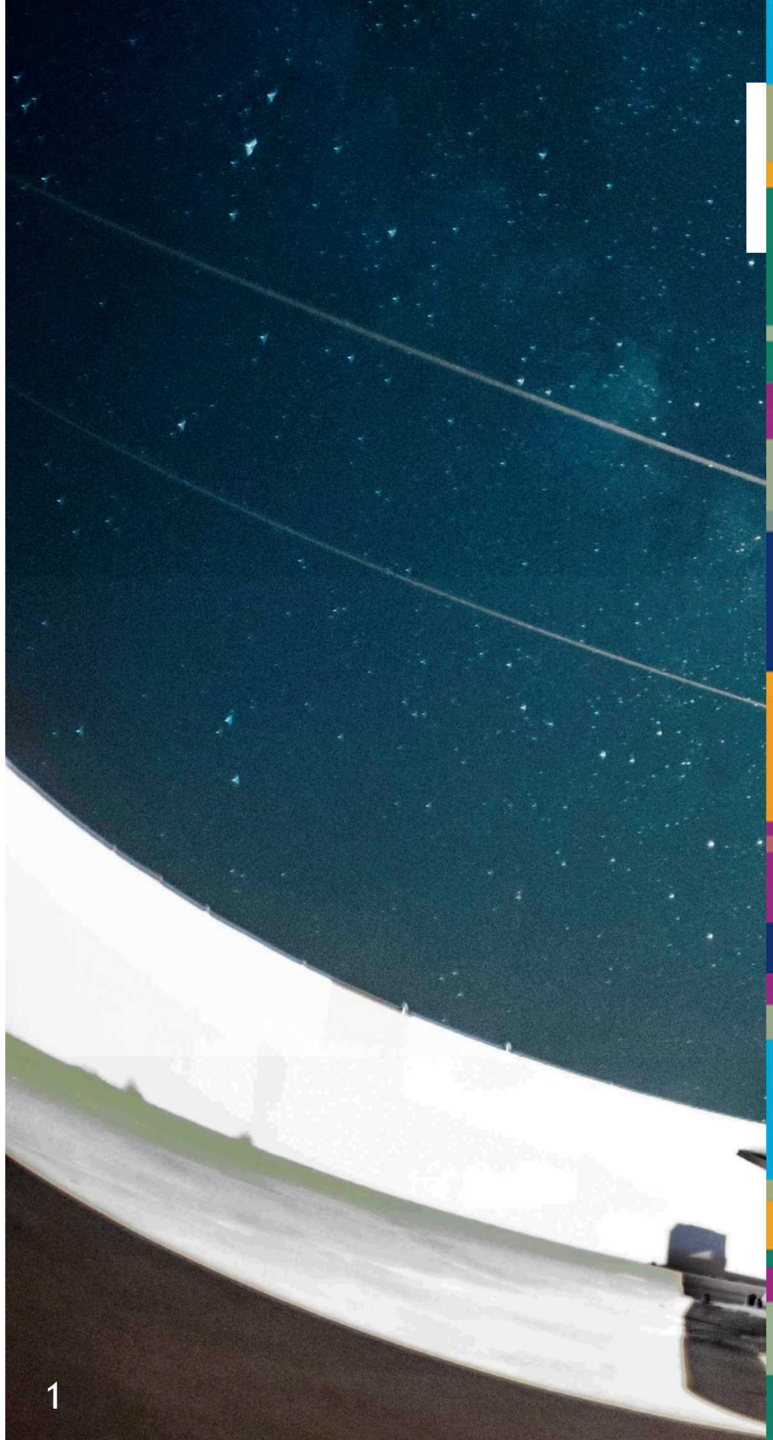
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.



New Mexico Research Spotlight Forum

SAND2019-4140PE

4/17/2019 Advancing Resilience for Space Systems

Cyber Resilience for Space Systems

PRESENTED BY:

Eric Vugrin

Cyber Resilience R&D Org. 5821,Sandia National Laboratories

Email: edvugri@sandia.gov Ph: 505-284-8494

THE UNIVERSITY OF NEW MEXICO

NM STATE UNIVERSITY

NEW MEXICO TECH
SCIENCE • ENGINEERING • RESEARCH UNIVERSITY

ABOUT YOURSELF

- Background
  - Degrees in (applied) mathematics
  - 15 years at Sandia, performing numerical modeling and analysis across a variety of systems
- Current research areas
  - Security and resilience modeling design, and analysis for cyber applications
  - Applying these techniques to space platforms…
- Research group
  - Interests: “all-things” cyber security and resilience for industrial control systems (modeling, experimentation, intrusion detection, defenses, etc.)
  - Size: variable, but my “group” consists of ~80 folks, with outreach across SNL
  - Demographics: info/cyber security, engineers, computer scientists, industrial controls,

Keywords:

Cyber security and resilience, threat modeling, intrusion response

Experiences at Sandia

United States Department of Energy
Waste Isolation Pilot Plant

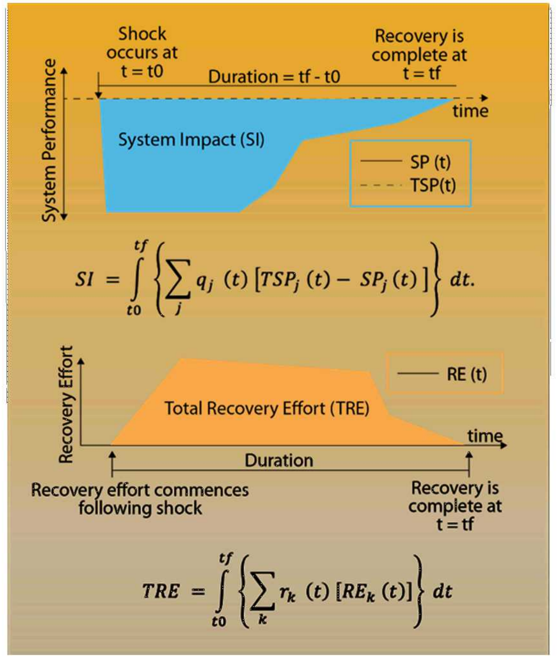
Risk Analysis for the WIPP

Infrastructure Consequence Modeling & Analysis

Cyber Security & Resilience

CURRENT WORK IN ADVANCING RESLIENCE FOR SPACE SYSTEMS

- Quantitative resilience analysis: how can we rigorously evaluate and design resilience into critical systems?
  - Metrics, mathematical modeling and optimization
  - Design of experiments and validation
- Modeling the cyber threat: how do we credibly represent threats in cyber experiments?
  - Development and validation of game theory & network interdiction models
  - Generation of synthetic data sets to represent previous and potential threats
- Automated, intrusion response algorithms: how do we create systems that (more) "automatically" respond to cyber threats without disrupting normal operations?
  - Leveraging mathematics of control, game theory, optimization
  - Operate in real-time, subject to size, weight, and power limitations


Shock occurs at t = t0
Recovery is complete at t = tf
Duration = tf - t0
System Performance
time
System Impact (SI)
SP (t)
TSP(t)
Recovery Effort
RE (t)
Total Recovery Effort (TRE)
time
Duration
Recovery effort commences following shock
Recovery is complete at t = tf

$$SI = \int_{t0}^{tf} \left\{ \sum_j q_j\ (t)\ [TSP_j\ (t) - SP_j\ (t)] \right\} dt.$$

$$TRE = \int_{t0}^{tf} \left\{ \sum_k r_k\ (t)\ [RE_k\ (t)] \right\} dt$$

RESEARCH NEEDS & FUNDING SOURCES

Research Needs

- Data, data, data …of satellite function performance: normal and “attack” conditions
  - Obtaining data
  - Generating synthetic data sets
  - Development of benchmarks
- Simulation and emulation of space systems
  - Communications
  - Satellite buses
  - Payloads
- Cyber threats to space systems: understanding and representing concerns specific to space systems

Funding sources: best option for collaboration is likely Laboratory Directed Research and Development (internal SNL research funds)