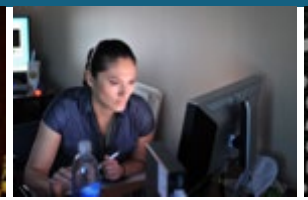
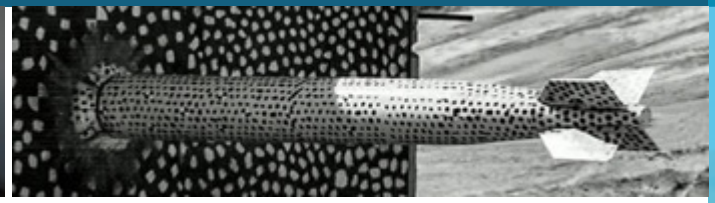
SAND2021-0813C

Emulation Platform for Evaluating the Resilience of Space Systems Against Ground Station Attacks





PRESENTED BY

McKade Umbenhower/Sandia National Labs, Meghan Sahakian/Sandia National Labs

Ground System Architectures Workshop, March 1-11, 2021

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.

Outline

- Motivation
- Simulation Scenario
- Simulation Platform
  - Data Collection
  - Data Processing
- Resilience Analysis
- Summary

Motivation

"Longstanding **technological and cost barriers to space are falling**, enabling more countries and commercial firms to participate in satellite construction, space launch, space exploration, and human spaceflight… Having seen the benefits of space-enabled operations, some **foreign governments are developing capabilities that threaten** others' ability to use space."

- "Challenges to Security in Space", U.S. Defense Intelligence Agency, 2019

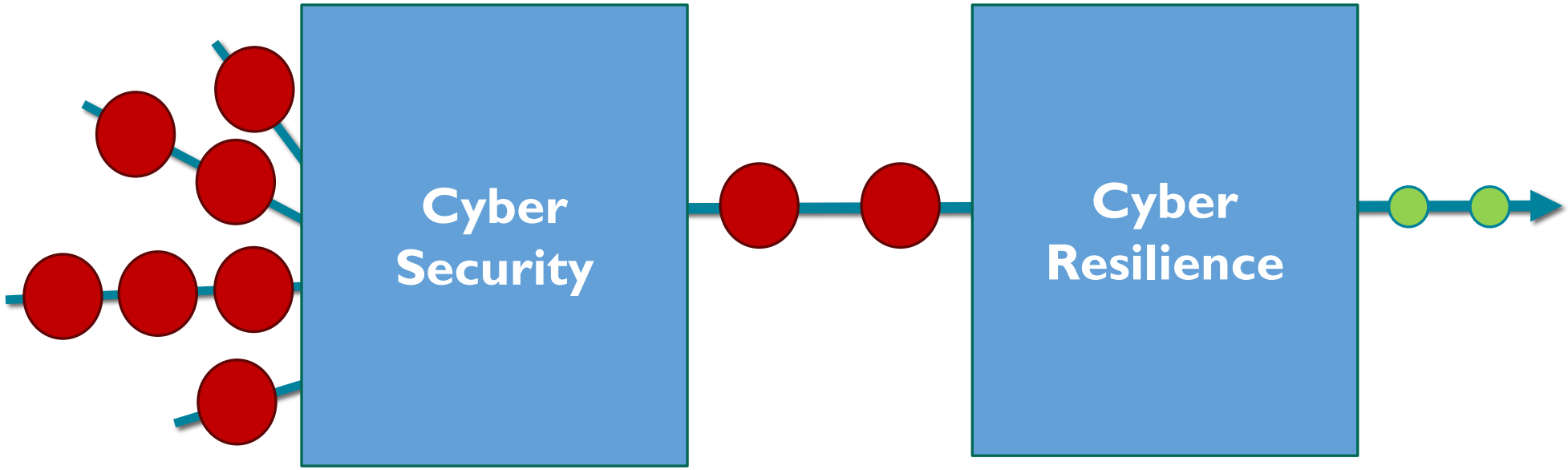
"Space systems should be developed **to continuously monitor, anticipate, and adapt to mitigate** evolving malicious cyber activities that could **manipulate, deny, degrade, disrupt, destroy, surveil, or eavesdrop** on space system operations. Space system configurations should be resourced and actively managed to achieve and maintain an **effective and resilient cyber survivability posture** throughout the space system lifecycle."

- "Memorandum on Space Policy Directive-5 – Cybersecurity Principles for Space Systems", The White House, 2020

Testing and analysis environments are needed to make informed design decisions to mitigate threats.

Cyber Security versus Cyber Resilience

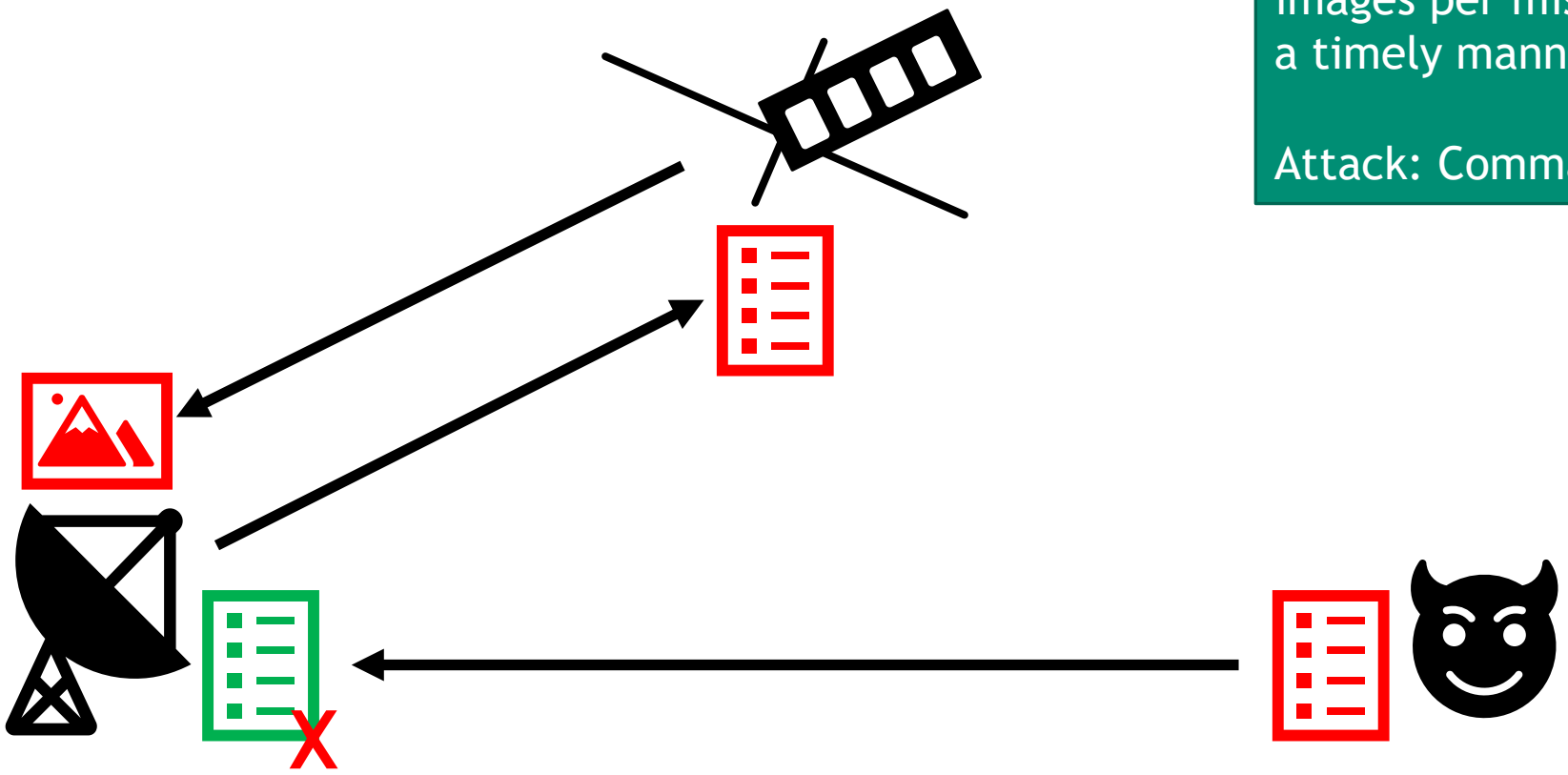
- Cyber Security
  - Decisions work to keep attacks out
  - Goals: confidentiality, integrity, availability
- Cyber Resilience
  - Decisions work to provide mission assurance despite the presence of an attack
  - Goals: fast recovery, limit damage, continue operations



Scenario Outline

Mission: Collect remote sensing images per mission parameters in a timely manner

Attack: Command table injection*

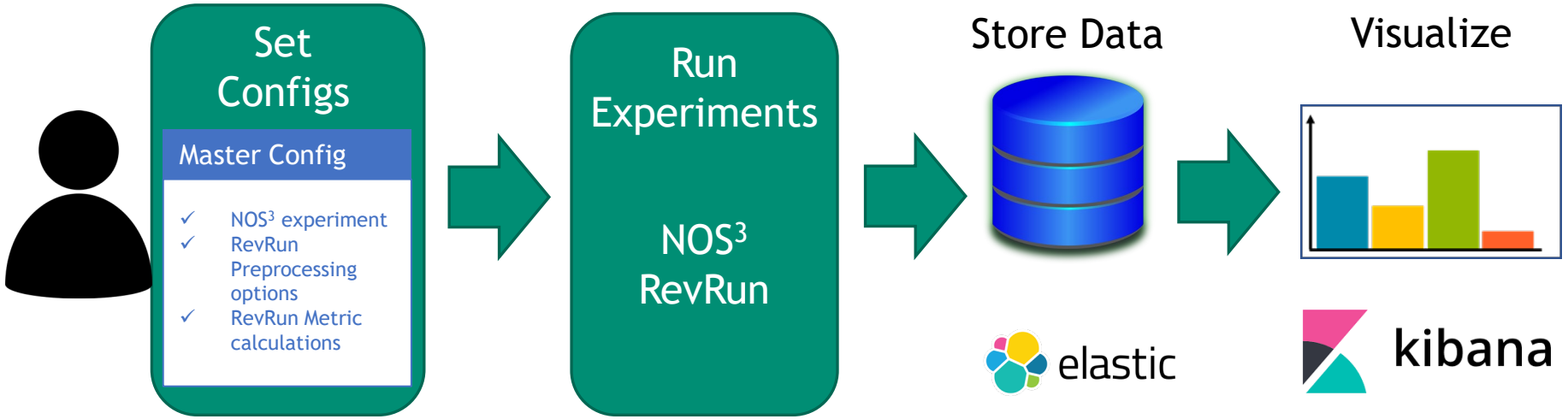


During this ground station attack, which mitigation strategy results in the most resilient system?

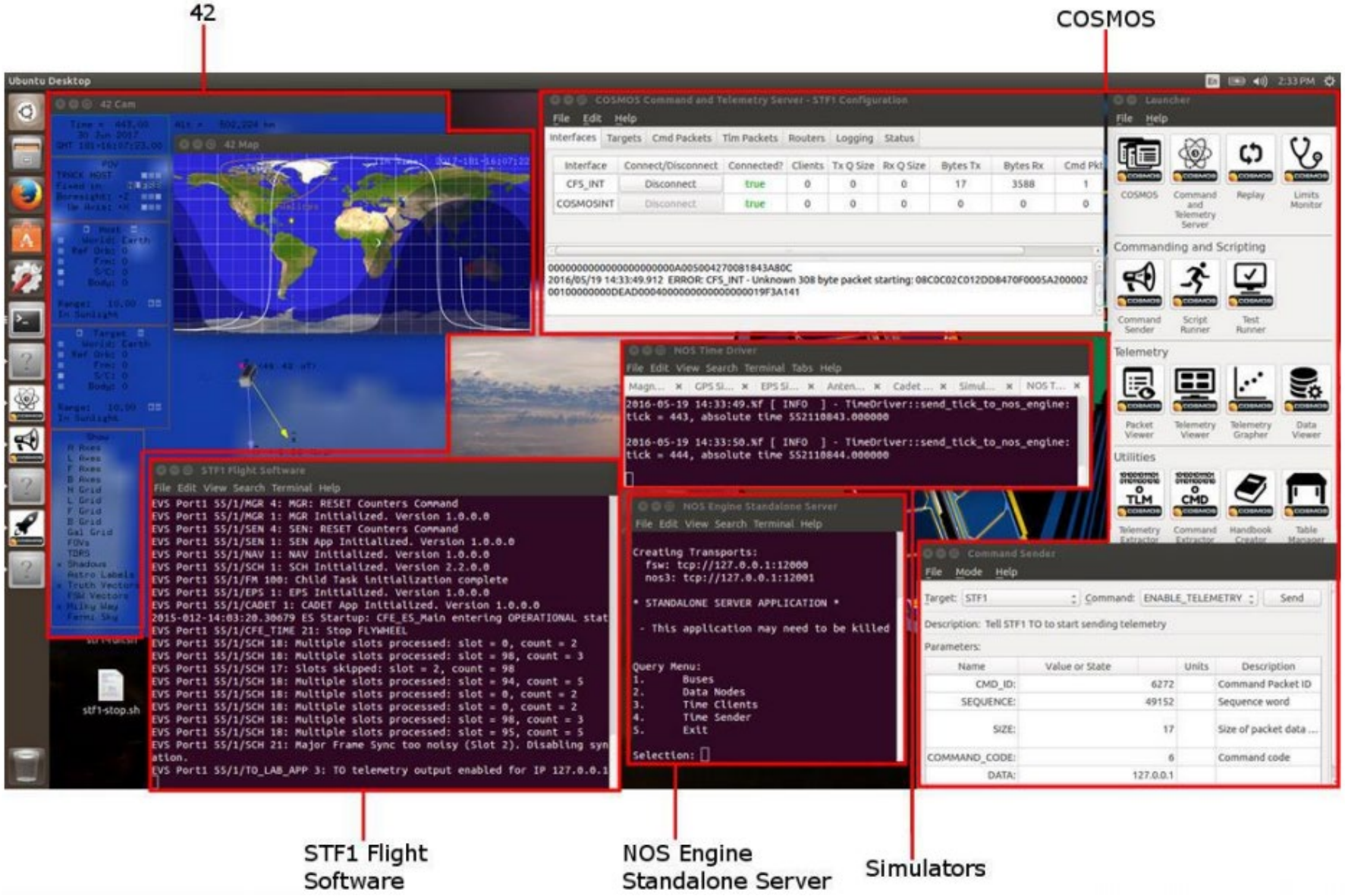
* This attack is notional and only intended for illustrative purposes

Simulation Platform

- NOS^3 [4]
  - NASA developed simulation platform for small satellites
- RevRun[5]
  - SNL developed toolset to quantify cyber resilience
- Elastic Stack
  - Elasticsearch, Kibana



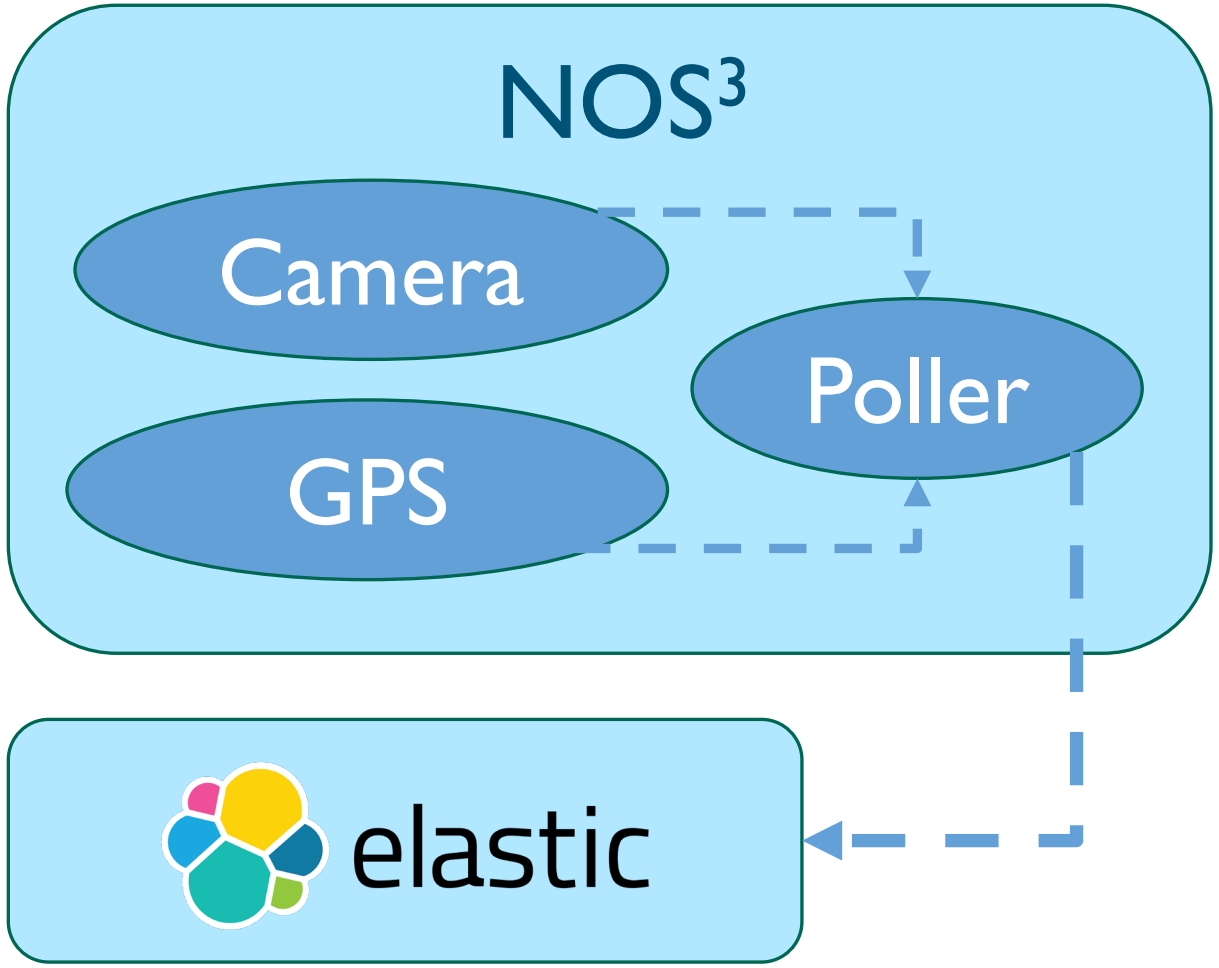
NOS³ Emulation Platform



M. Grub. "NOS3: Tools for Software Based Validation and Verification of Small Satellites." Small Sat Workshop, 2016.

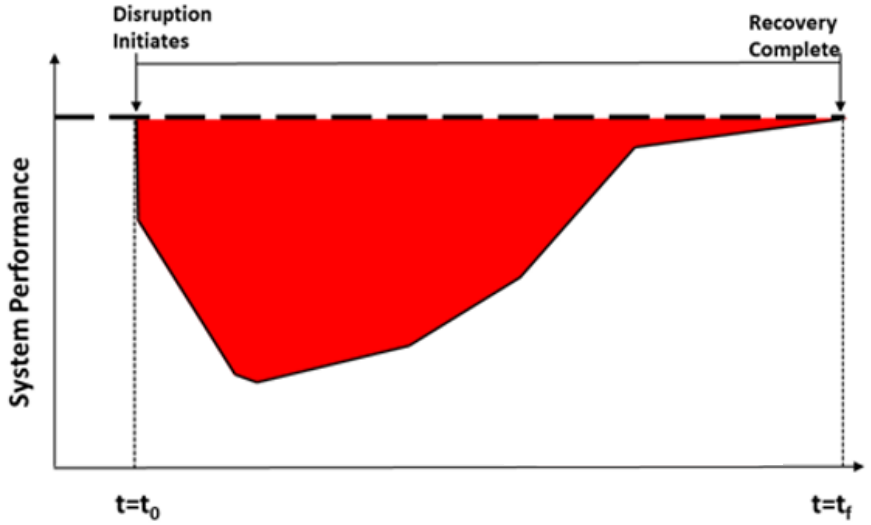
Sandia Provided NOS³ Extensions

- Data Collection
- Extra hardware capabilities
  - Camera memory
  - Downlinking
  - Camera configuration
- Cyber Mitigations
  - Reboot
  - Safe Mode
  - Command verification
  - Reflashing command table

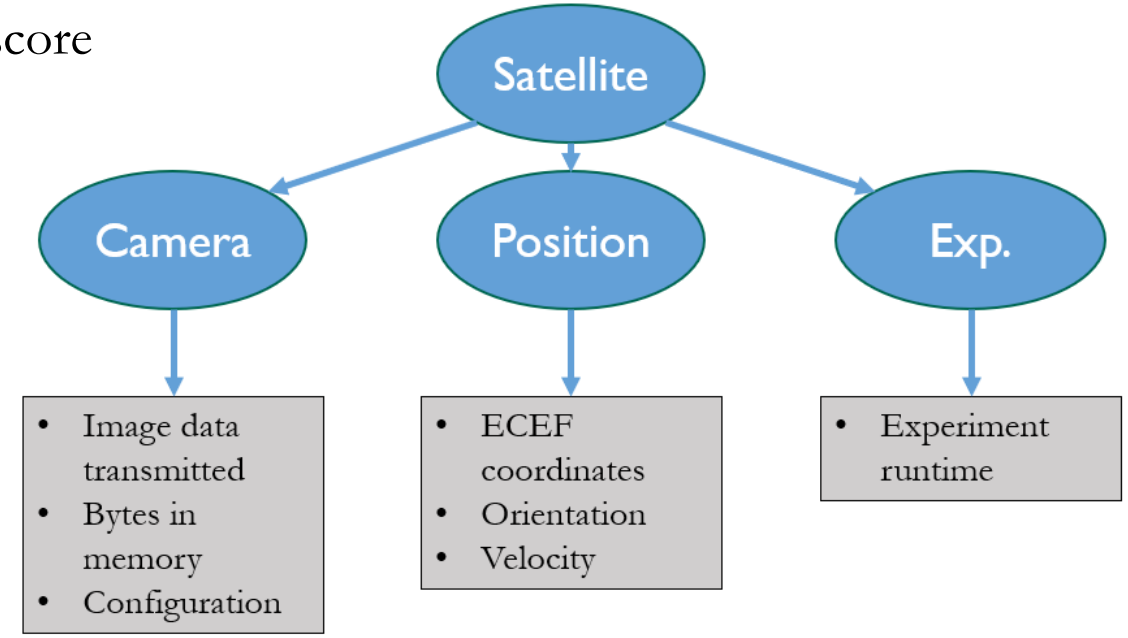


REsilience VeRification Unit (RevRun)

- Toolset used to measure and quantify cyber resilience of a system
  - Ingests raw experimental data
  - Preprocesses data if needed
  - Uses analyst-defined metrics to compare data to a baseline
  - Aggregates quantitative scores into overall score



Integral Resilience Metric



Resilience Metric Aggregation

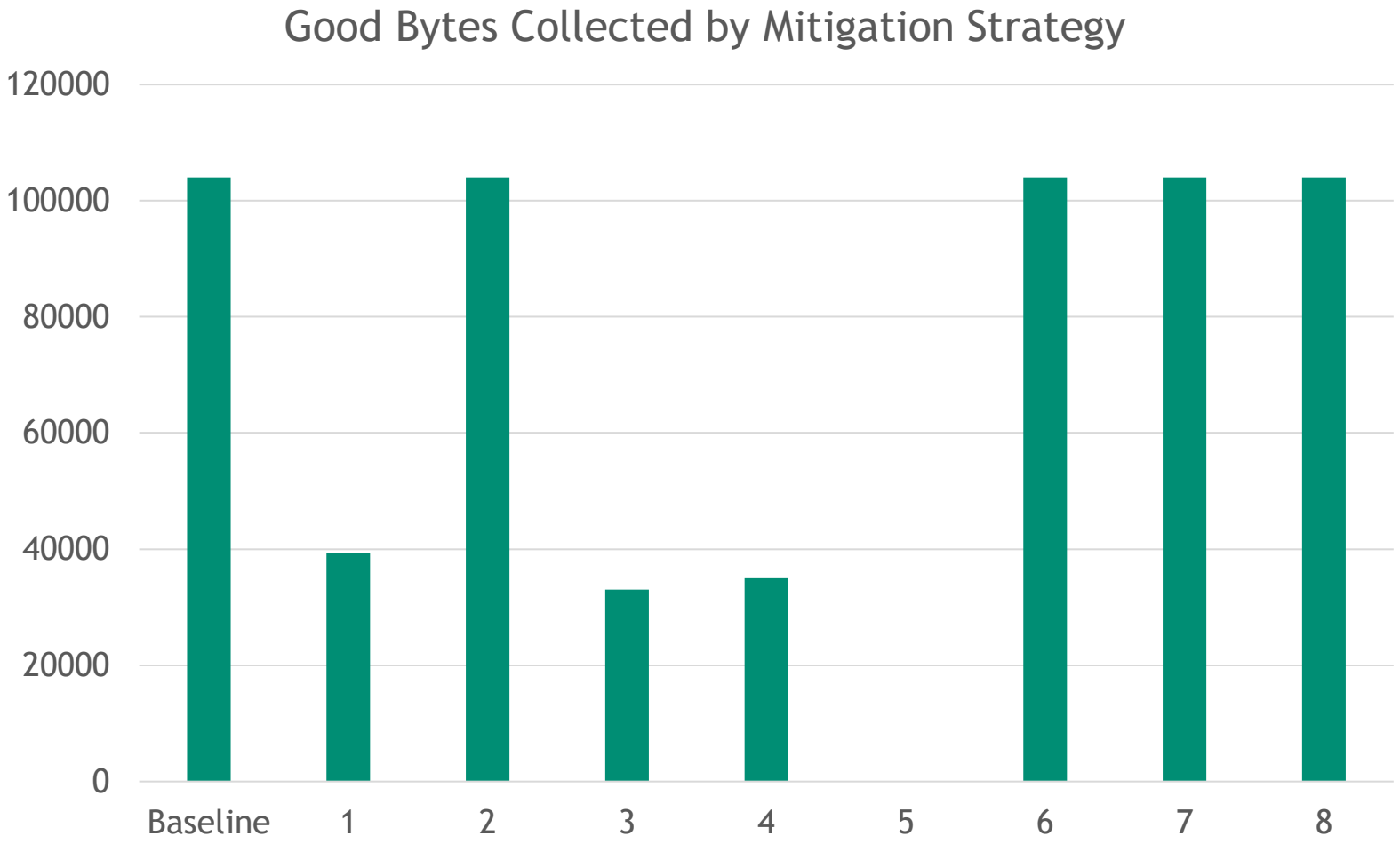
Mitigation Experiments

- Baseline: Collect image data from time t=100-400
- Attack: Camera configuration adjusted at time t=200

- Strategy 1: Do nothing
- Strategy 2: With command table verification on
- Strategy 3: After detecting the attack, reboot the camera component
- Strategy 4: After detecting the attack, enter safe mode
- Strategy 5-8: Repeat Strategies 1-4 after reflashing the command table from a backup on the next orbit

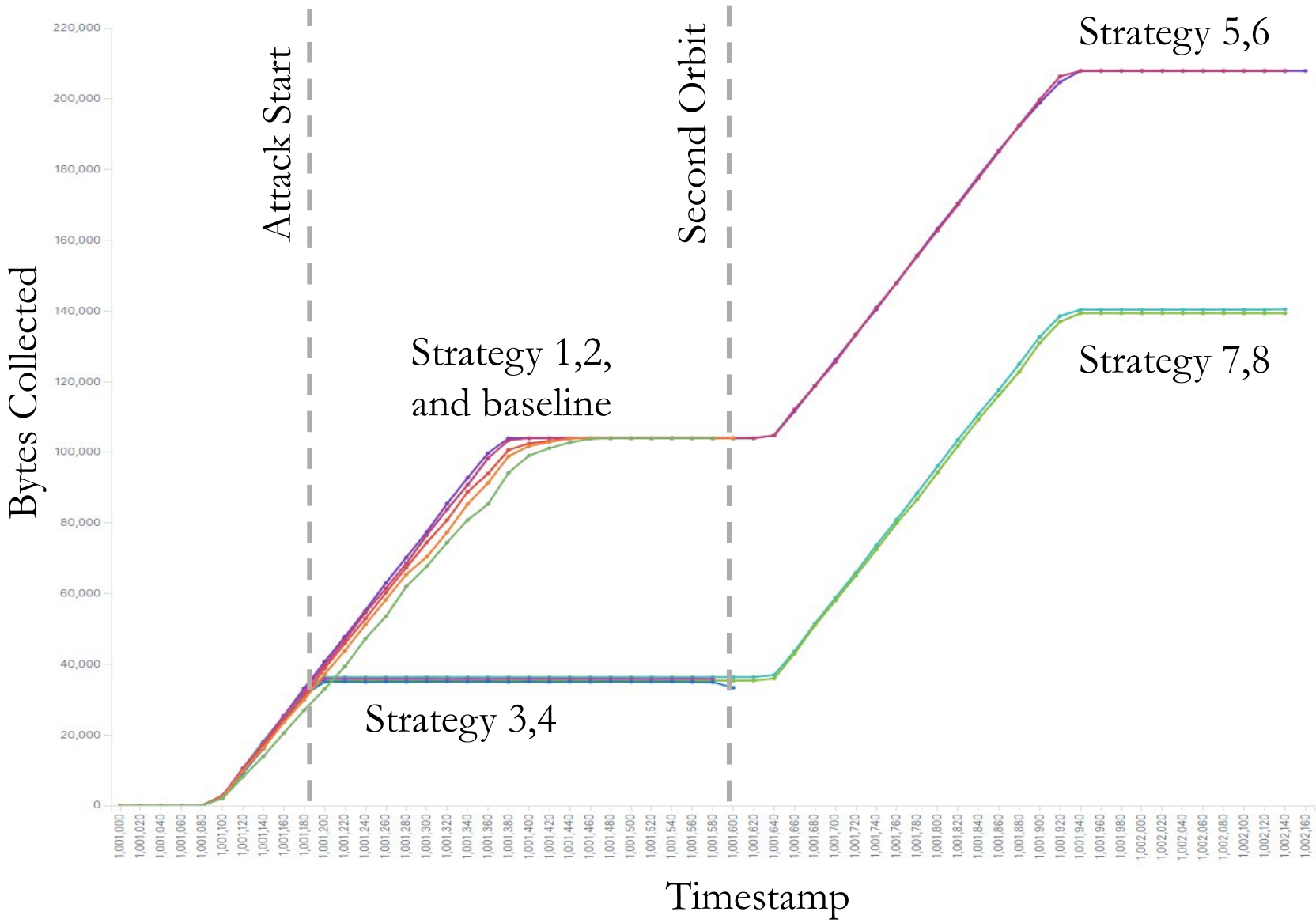
- Metrics
  - Amount of good data
  - Satellite location
  - Experiment time

Experimental Results



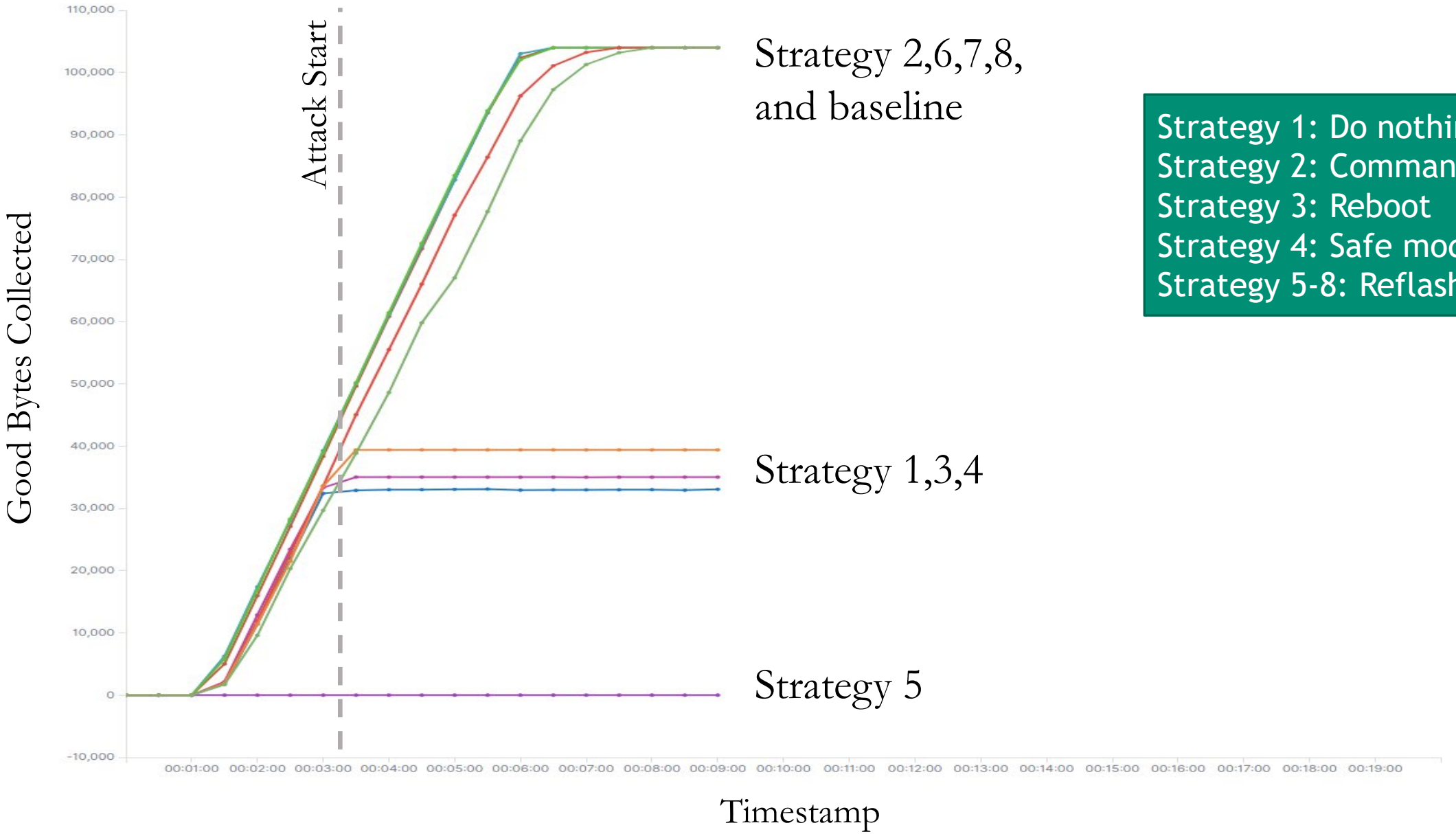
Strategy 1: Do nothing
Strategy 2: Command verification
Strategy 3: Reboot
Strategy 4: Safe mode
Strategy 5-8: Reflash and retry

Raw Experimental Data



Strategy 1: Do nothing
Strategy 2: Command verification
Strategy 3: Reboot
Strategy 4: Safe mode
Strategy 5-8: Reflash and retry

Preprocessed Experimental Data



Strategy 1: Do nothing
Strategy 2: Command verification
Strategy 3: Reboot
Strategy 4: Safe mode
Strategy 5-8: Reflash and retry

Resilience Results

Strategy 1: Do nothing
Strategy 2: Command verification
Strategy 3: Reboot
Strategy 4: Safe mode
Strategy 5-8: Reflash and retry

Summary

- With the growing usage and complexity of space systems, simulation and testing environments are critical
  - Better informs design decisions
  - Work through mitigation strategies
- Existing tools can be extended and pieced together to create robust simulation platforms

References

Resilience Metrics

- [1] B. Biringer et al. 2013, *Critical Infrastructure System Security and Resiliency*, CRC Press: Boca Raton, Florida, 2013.
- [2] N. Jacobs et al. "Measurement and Analysis of Cyber Resilience for Control Systems: An Illustrative Example," 2018 Resilience Week (RWS), Denver, CO, 2018, pp. 38-46.
- [3] S. Hossain-McKenzie et al. "Performance-Based Cyber Resilience Metrics: An Applied Demonstration Toward Moving Target Defense," *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, Washington, DC, 2018, pp. 766-773.

NOS^3

- [4] D. Geletko et al. "NASA Operational Simulator for Small Satellites (NOS^3): The STF-1 CubeSat Case Study." *arXiv preprint arXiv:1901.07583* (2019).

RevRun

- [5] M. Galiardi et al. "Cyber Resilience Analysis of SCADA Systems in Nuclear Power Plants," *International Conference on Nuclear Engineering*. Vol. 83778. American Society of Mechanical Engineers, 2020.

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.