SAND2019-7737C

Exceptional service in the national interest

Sandia National Laboratories

Cybersecurity Experiment Design with Stochastic Game Theory

Author: Lee Maccarone; University of Pittsburgh; PhD Mechanical Engineering; August, 2020
Manager: F. Mitch McCrory ● Mentor: Christopher Lamb ● Organization: Energy Security (08851)

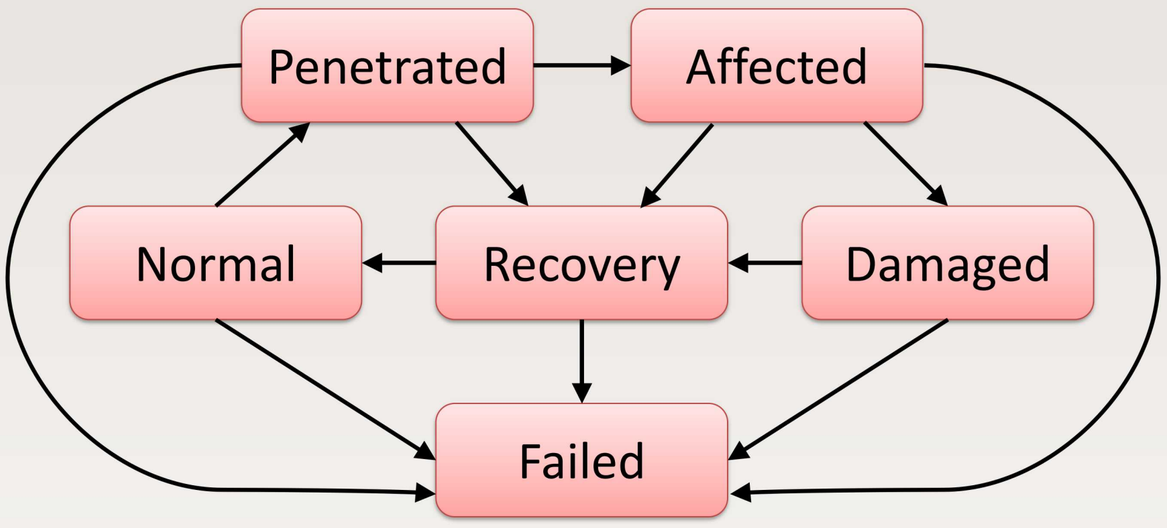
Introduction

The purpose of this research is to design an experiment that evaluates the efficacy of cybersecurity controls for industrial control systems. If this research is successful, we will be able to do the following:

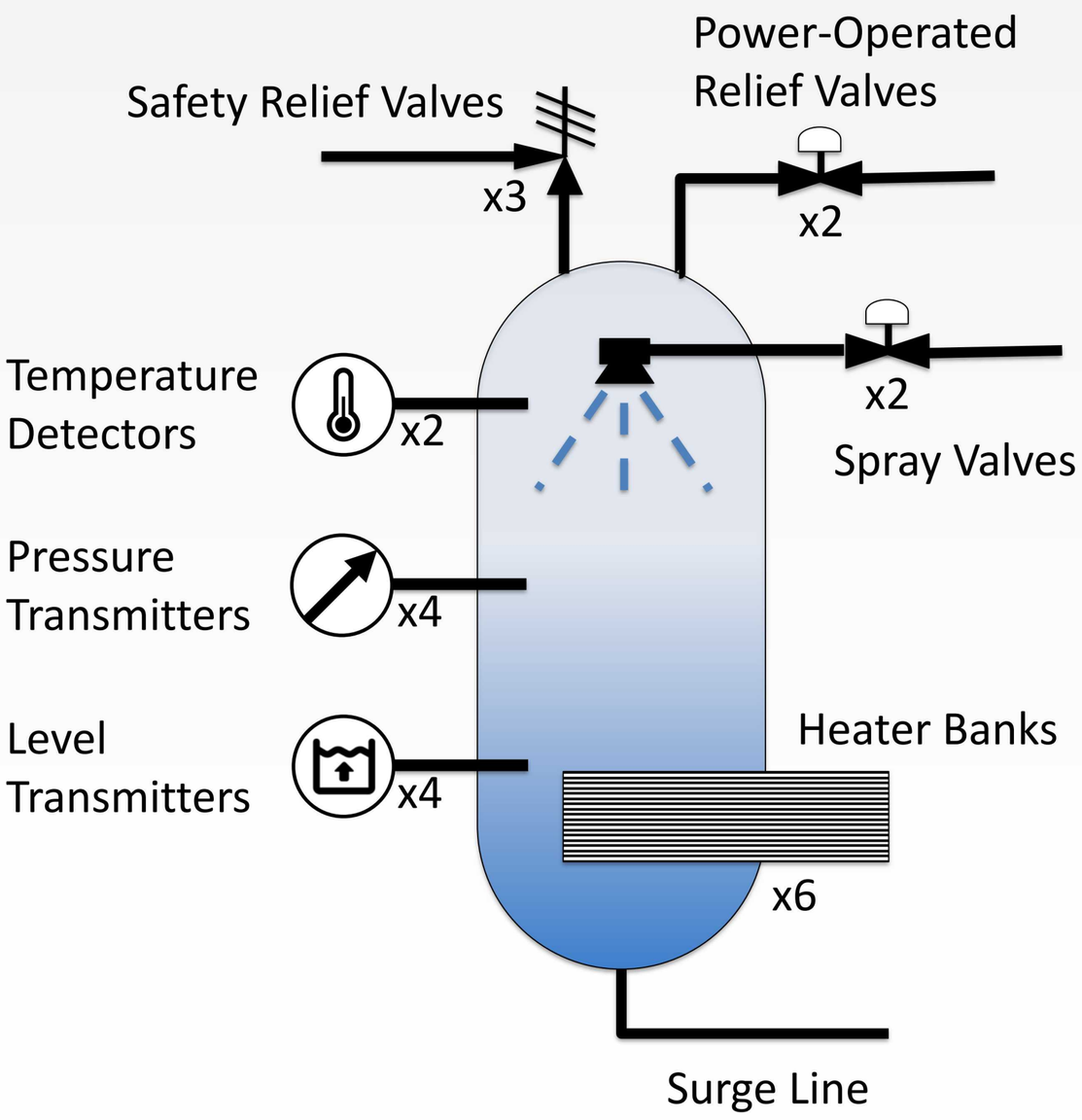
- Prioritize defense methods
- Defend against multiple threats
- Predict system performance

Stochastic Game Theory

Strategies chosen by a defender and attackers determine the probability of transitioning to another security state.
(Lalropuia and Gupta, Rel. Eng. & Sys. Saf., 2019)

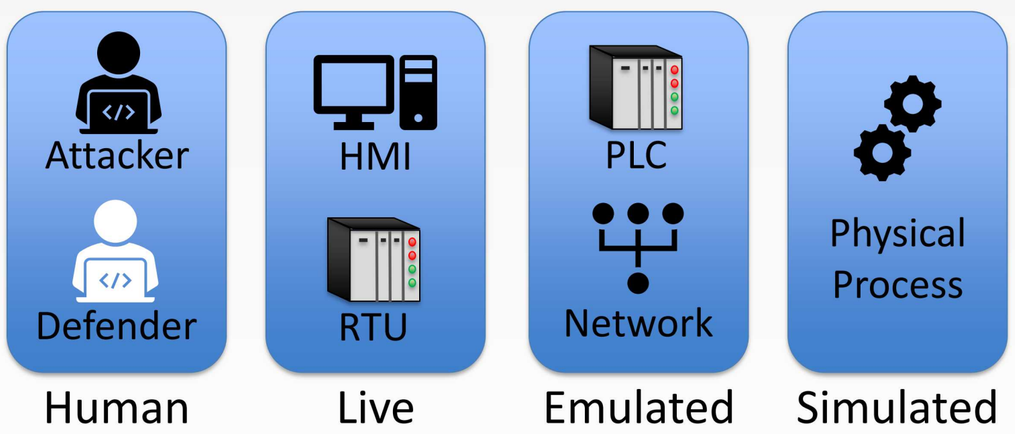


Candidate Pressurizer System



SCEPTRE Testbed

The SCEPTRE platform provides experimental data on security events and state transitions.



This method enables:

- Consideration of resources required for cybersecurity controls
- Analysis of process logic
- Research of malware effects on industrial control systems

U.S. DEPARTMENT OF ENERGY
National Nuclear Security Administration

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-NA-0003525. SAND #

Presented on: 7/25/2019