



# Invite the Chaos Monkey: Test Effect Payloads for Tuning ICS Incident Response

January 2020

*Changing the World's Energy Future*

Virginia L Wright



*INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC*

#### **DISCLAIMER**

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

# **Invite the Chaos Monkey: Test Effect Payloads for Tuning ICS Incident Response**

**Virginia L Wright**

**January 2020**

**Idaho National Laboratory  
Idaho Falls, Idaho 83415**

**<http://www.inl.gov>**

**Prepared for the  
U.S. Department of Energy  
Under DOE Idaho Operations Office  
Contract DE-AC07-05ID14517**

# INVITE THE CHAOS MONKEY

## TEST EFFECT PAYLOADS FOR TUNING ICS INCIDENT RESPONSE

THIS RESEARCH WAS DEVELOPED WITH FUNDING FROM THE DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA).

THE VIEWS AND CONCLUSIONS CONTAINED IN THIS DOCUMENT ARE THOSE OF THE AUTHORS AND SHOULD NOT BE INTERPRETED AS REPRESENTING THE OFFICIAL POLICIES, EITHER EXPRESSED OR IMPLIED, OF THE DEFENSE ADVANCED RESEARCH PROJECTS AGENCY OR THE U.S. GOVERNMENT.

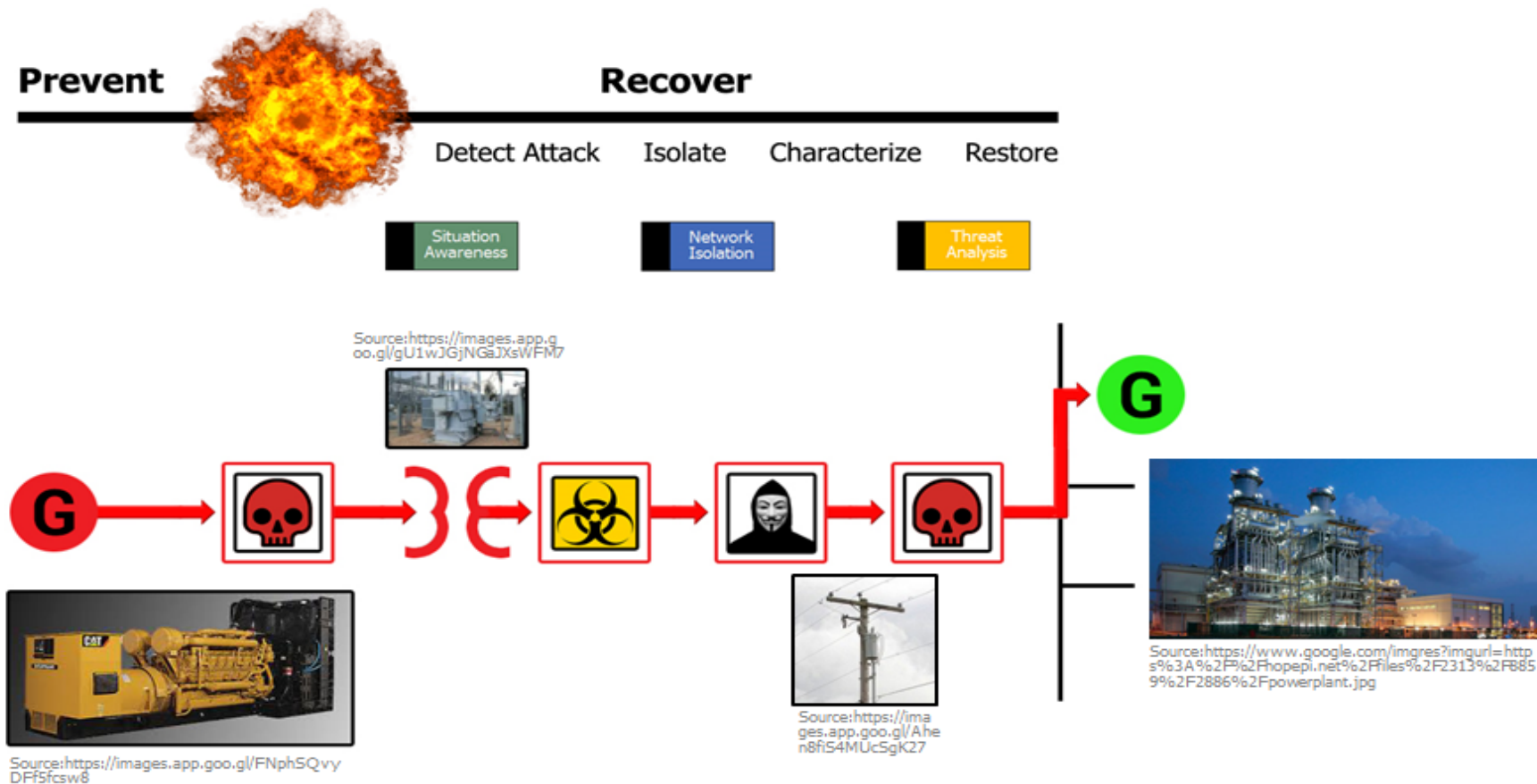
DISTRIBUTION STATEMENT A. DISTRIBUTION APPROVED FOR PUBLIC RELEASE, DISTRIBUTION UNLIMITED.

# Overview

- Summary of DARPA RADICS
- Meet the Monkeys (A history of Netflix)
- Test Effect Payloads (A DARPA RADICS Concept)
- Developing a strategy for Test Effect Payloads in Critical Infrastructure

# RADICS Program Objective and Goal

Objective: Enable black start recovery of the power grid amidst a cyber-attack on the energy sector's critical infrastructure.



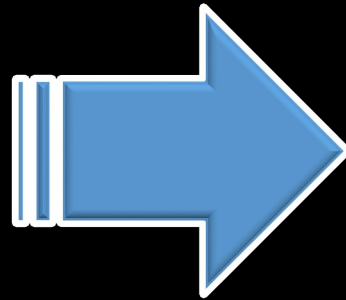
Goal: Seven Days to Isolate, Characterize & Restore Crank Pathways

# RADICS Exercise Assumptions

- Live ongoing cyber attack
  - Assets and network are owned by attacker
  - Attacker can prevent typical “Black Start” restoration
- Reflashing and restoration are not a viable solution
- Operating in manual mode is not a long-term option
- Defenders are detecting attacker tools and “reclaiming” territory



# First, a Case Study in Resilience - Netflix





# Meet the Monkeys

- Chaos Monkey - Instance fails
- Chaos Gorilla - Data center fails
- Latency Monkey – Introduces Lag
- Doctor Monkey – Repair “sick” instances
- Janitor Monkey – Clean up resources
- Conformity Monkey – Instance follows rules
- Security Monkey – Known vulnerabilities
- 10-18 Monkey – Internationalization
- *Others ...*
- Chaos Toolkit – Toolkit for cloud



# Chaos Engineering vs. Normal Testing

## Chaos Monkey

- Inside business operations
- In production
- Pseudo-random
- Failure modes
- Experiments
- Enhance resilience
- Embrace failure

## Normal Testing

- Outside business operations
- In development/test
- Scripted
- Requirements
- Tests
- Eliminate weaknesses
- Prevent failure

<https://medium.com/netflix-techblog/the-netflix-simian-army-16e57fbab116>

<https://www.gremlin.com/chaos-monkey/>

# RADICS Exercises (Overview)



Simulate black start recovery of a crank path amidst a cyber attack on the power infrastructure to enable grid restart operations

Source: <https://goo.gl/maps/wuwhz9QPf7C2>

# Sounds a lot like Chaos Engineering

## Chaos Engineering

- Inside business operations
- In production
- Pseudo-random
- Failure modes
- Experiments
- Enhance resilience
- Embrace failure

## RADICS

- ✓ Blackstart process
- ✓ Operational systems
- ? Scenario scripted
- ✓ Extended regional power outage
- ✓ Research effort
- ✓ Recovery resilience
- ✓ Systems compromised



# Test Effect Payloads

- Realistic effects
  - Highly coupled to system
  - Operational model
  - Security model
- Avoid
  - Damage to devices
  - Unintended consequences
- Could be:
  - Misconfigurations
  - Spurious traffic
  - Executable programs



# TEPS ARE NOT VULNERABILITIES

- Create observable effects on systems and networks.
  - NOT vulnerabilities or exploits
  - Presumptive access
  - Use system capabilities
- Not entire cyber kill chain
- Can represent net effect of combined attack stages
- Can represent physical effects
- Tunable for specific effects and behaviors
- Can be installed and removed through automated means
  - Automation requires development of infrastructure

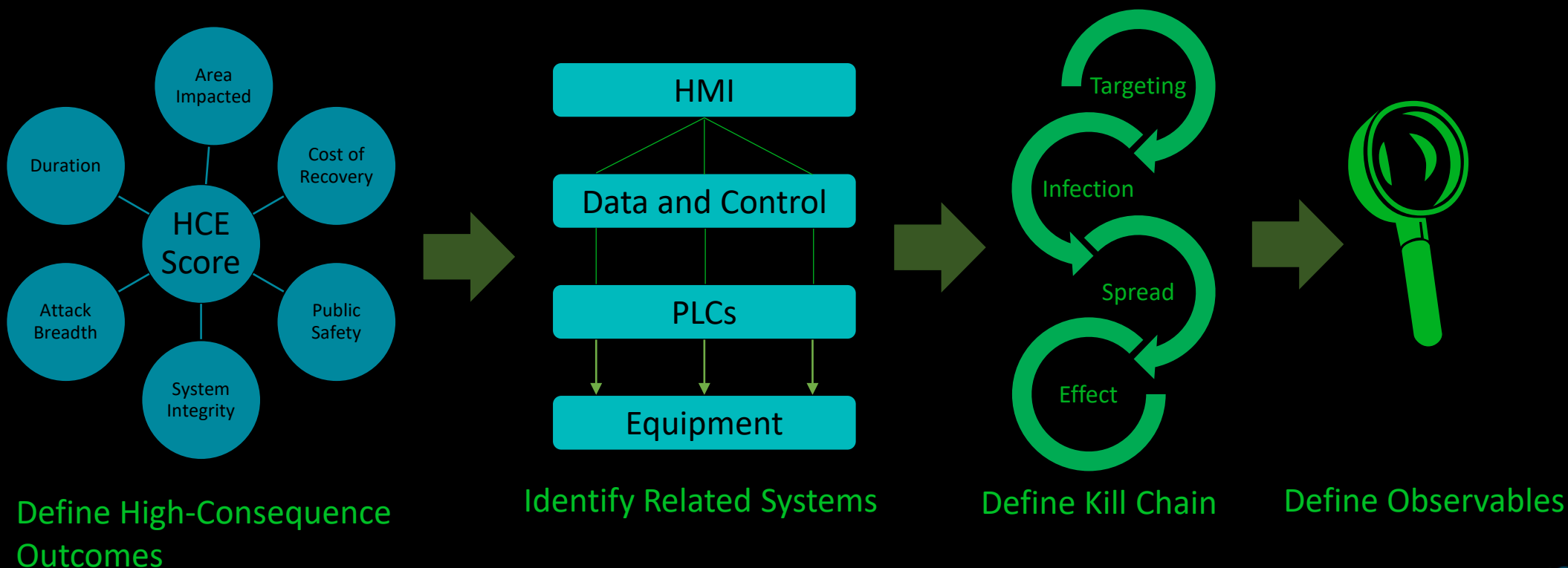
# TEP Examples

- New Host on Network
  - Sends DNP3 traffic to other hosts
  - Attempts telnet sessions to other hosts
- HMI Data poisoning
  - Uses structured text
  - Change voltages reported to HMI
  - DOES NOT AFFECT REAL DATA, ONLY HMI
- Relay Misconfiguration
  - Trigger overcurrent trip



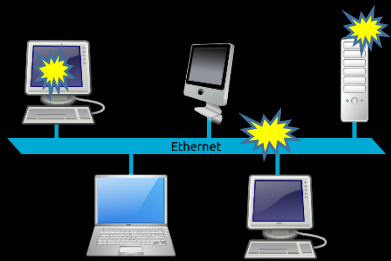
# Designing a TEP Campaign

- Phase 1: Consequence-based Engineering



# Designing a TEP Campaign

- Phase 2: Design Experiment



Define Expected  
Behaviors



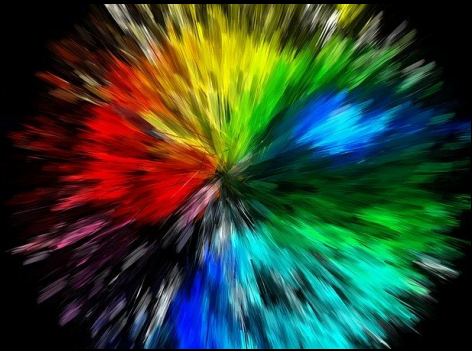
Define Expected  
Experiment  
Results



Plan Experiment Elements including  
Automation and Timing

# Designing a TEP Campaign

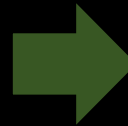
- Phase 3: Construct and Run Experiment



Blast Radius  
Analysis



Construct Test  
Effect Payloads



Run Experiments!



# Considerations for Success

- Think small - Be exact
- Minimize blast radius
- Tune People, Processes and Tools
- Test as close to production as possible
- For high-consequence systems, consider 'paper' TEP's
  - Validate with additional small-scale experiments
- For non-production environments, consider a full killchain experiment

# Next Steps

- Interested in going further?
  - DARPA exhibit upstairs