INL/MIS-19-54517-Revision-0

Enhancing Lifeline Infrastructure Resilience

June 2019

Ron E Fisher

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.

INL/MIS-19-54517-Revision-0

Enhancing Lifeline Infrastructure Resilience

Ron E Fisher

June 2019

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

~~INTERNAL USE ONLY~~
~~NOT REVIEWED FOR PUBLIC RELEASE~~

Enhancing Lifeline Infrastructure Resilience

Infrastructure Assurance & Analysis Division

Ron Fisher, Ph.D., Division Director

Find address or place
The Regional Resiliency Assessment Program (RRAP)
Common Topics and Conclusions Across Life-Line Infrastructure
Fiscal Years 2009-2014
Introduction
Life-line Infrastructure Summaries
The Information Technology Sector
RRAP Projects: IT-Cyber
LIFE-LINE INFRASTRUCTURE
IP Gateway
Dependency Profile Editor
Water Treatment Facility Dependency Profile
Chemicals
Fresh
Electric
IT/Comm
Raw Water
Agriculture
Commercial
Industrial
Emergency
Residential

N&HS Strategic Advisory Committee Meeting
June 19-21, 2019 – Idaho Falls, ID

www.inl.gov

Idaho National Laboratory

Progress in Achieving N&HS Strategic Plan Objectives

Assure Inherently Resilient Lifeline Infrastructure

- Establish operational critical infrastructure research environment with focus on control systems security
- Continue enhancement of critical infrastructure cyber-physical interdependency analysis and knowledge management capabilities

1. AICS R&D 100 Award
2. AHA R&D 100 Award Finalist
3. Leadership in developing analytical tools used to support natural disasters
4. Leadership in infrastructure dependencies and interdependencies analyses

Secure the Nation's Vital Cyber-Physical Systems

1. Premier infrastructure/ICS cyber-physical environment

Advance and Train the Workforce that Engineers, Operates, and Defends the Nation's Secure and Resilient Systems

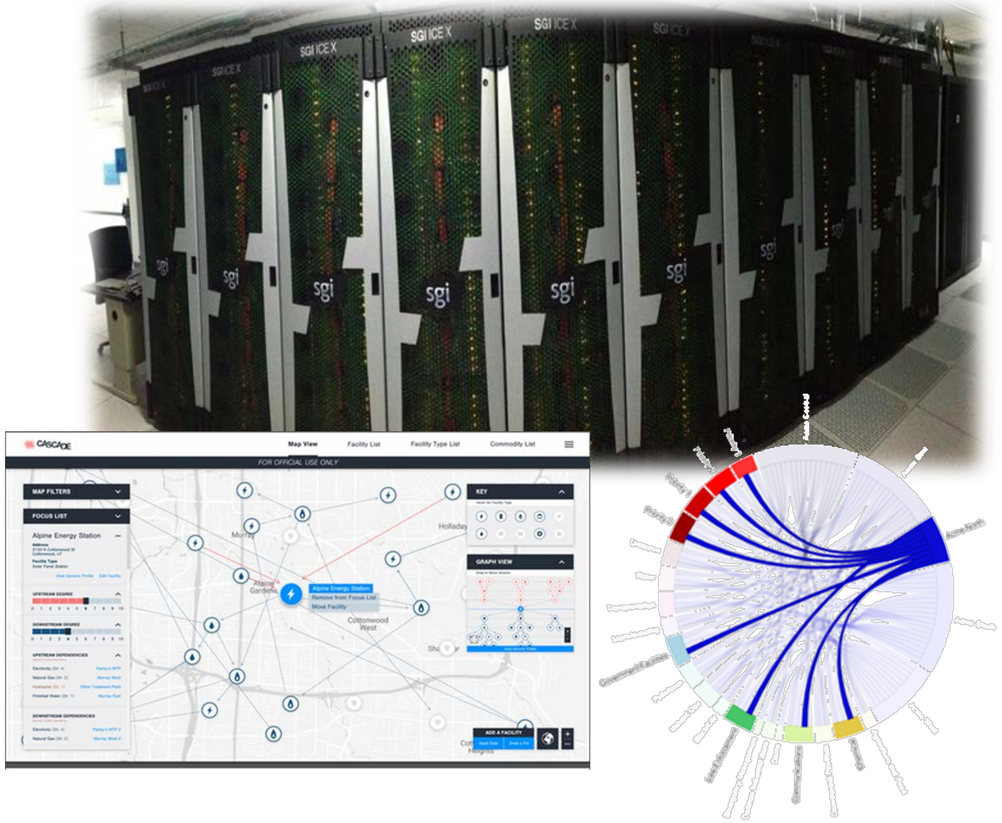
1. Army Cyber Command three-week OT course training for IT assessors

Support the Scientific Computing Initiative

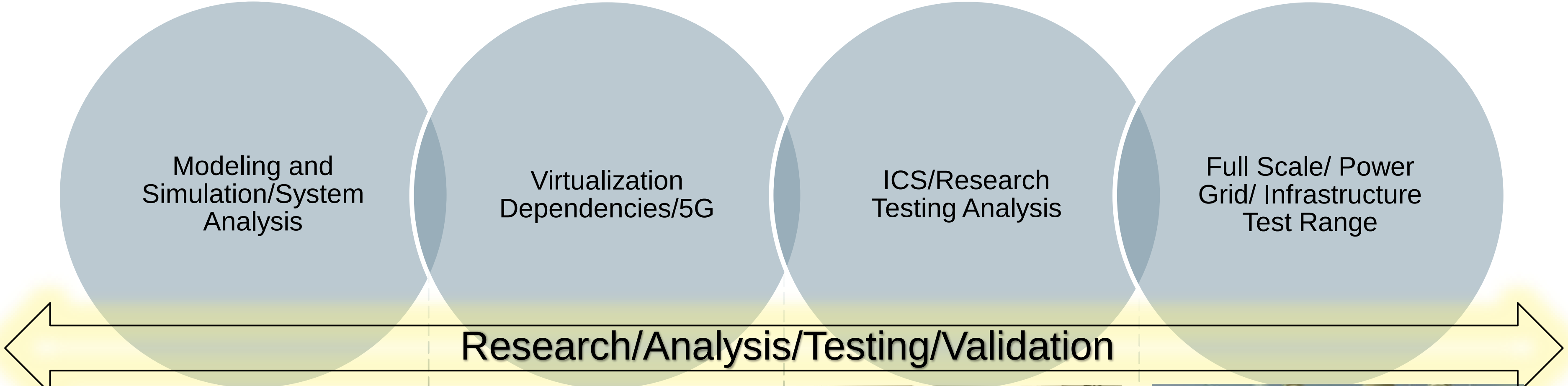
1. High Performing Computing Pilot of malware data

Aligning with INL Strategy: Support Scientific Computing Initiative

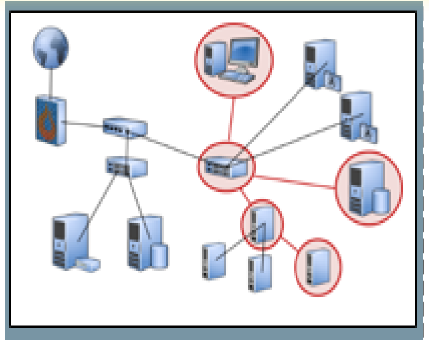
- Solving national and homeland security challenges through unique applications of High Performance Computing (HPC)
  - SMC classified HPC system
  - Pilot of HPC and malware
  - Infrastructure dependencies and interdependencies analyses
- Analyzing, Mapping and Visualizing Functional Relationships
  - New emphasis from Department of Homeland Security (DHS) for 55 critical functions
  - ESRI Cooperative Research and Development Agreement
- Advancing INL's Data Sciences Capabilities
  - Big data
  - Secure integration
  - Predictive analytics



INL has the Nation’s Premier Critical Infrastructure Environment for DHS, DOE, DoD, and Industry


Modeling and Simulation/System Analysis
Virtualization Dependencies/5G
ICS/Research Testing Analysis
Full Scale/ Power Grid/ Infrastructure Test Range
Research/Analysis/Testing/Validation

- Physics based computer modeling
- Visualization
- Big data analysis
- High Performance Computing



- State-of-the-art control systems virtualization
- Interconnections with HPC/scientific computing methods and techniques
- Control systems modeling and simulation

- Physical and virtual critical infrastructure representations
- Interconnections with full-scale testing
- Integration for cyber-physical-dependencies modeling

- 890 square mile test range
- 110 mile transmission and distribution lines
- 2G, 3G, 4G, LTE cellular, wireless range
- Water security testbed

INL Resilience Optimization Center (IROC)

IROC strengthens INL’s leadership position in resilience by leveraging our current and emerging capabilities, facilities, and staff with increased collaborations (internally and externally) to solve complex and challenging resilience problems.

- Builds upon extensive INL capabilities in resilience
- Provides a holistic cyber-physical-dependencies approach to resilience
- Bridges the gap between scientific research and the needs of industry/federal agencies
- Increases collaborations both internally and externally

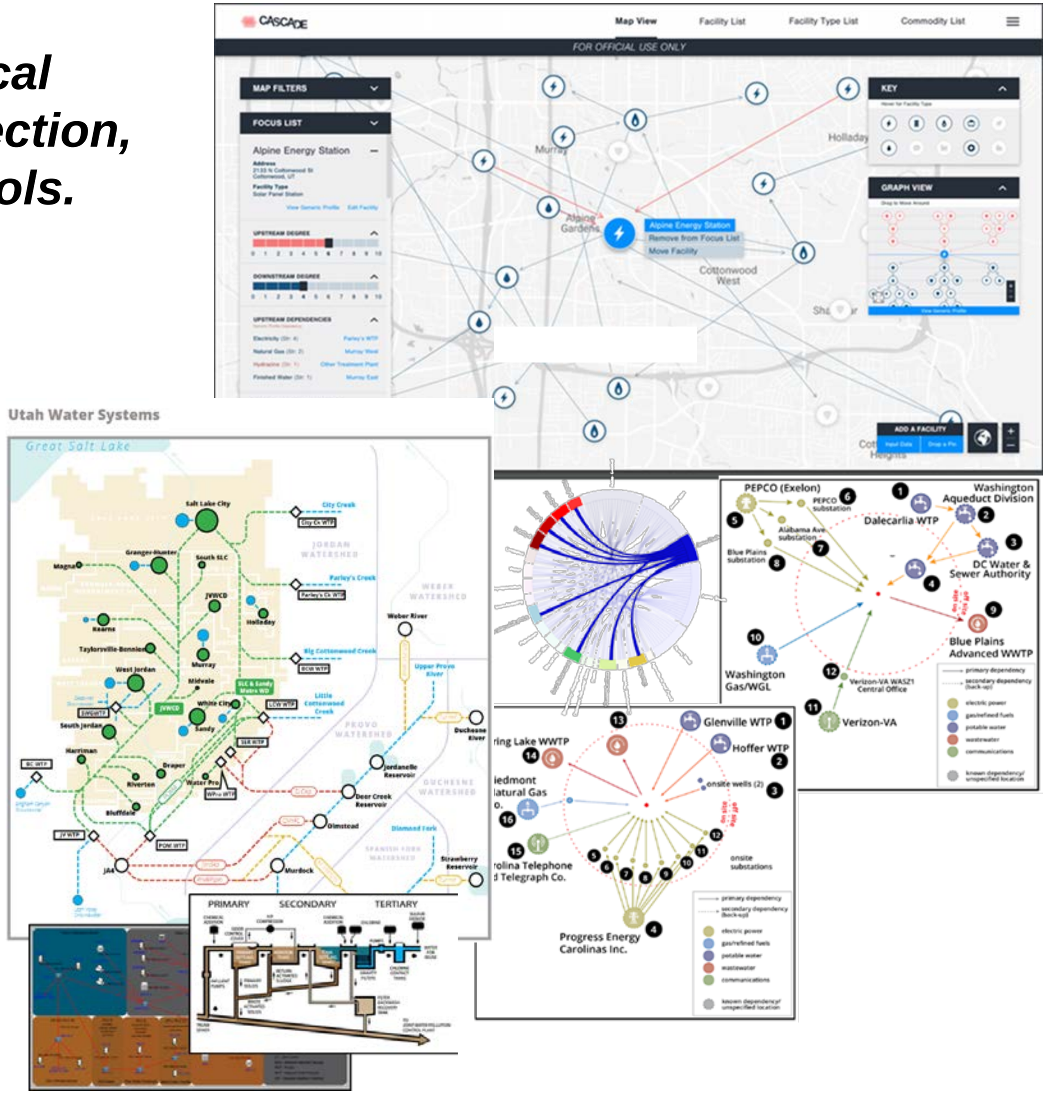
Extending INL Leadership in Resilience Through Internal and External Collaborations

Recognized Leader in Critical Infrastructure Cyber-Physical Interdependency Analysis

INL is a national leader in critical infrastructure cyber-physical interdependency analysis by providing innovative data collection, cascading analysis, and visualization methodologies and tools.

Sponsors and collaborators sustaining and developing:

- Growing with DHS Cybersecurity and Infrastructure Security Agency
  - National Risk Management Center
  - Infrastructure Security Division
- Increasing DOE and Department of Defense engagements
- Increased cross-laboratory collaborations
  - Cybercore, EES&T
- Emerging State and Local engagements
  - Idaho, Utah, Virginia emergency management agencies
- Building external partnerships
  - Argonne National Laboratory
  - Asset Partners
  - Resilient Solutions 21

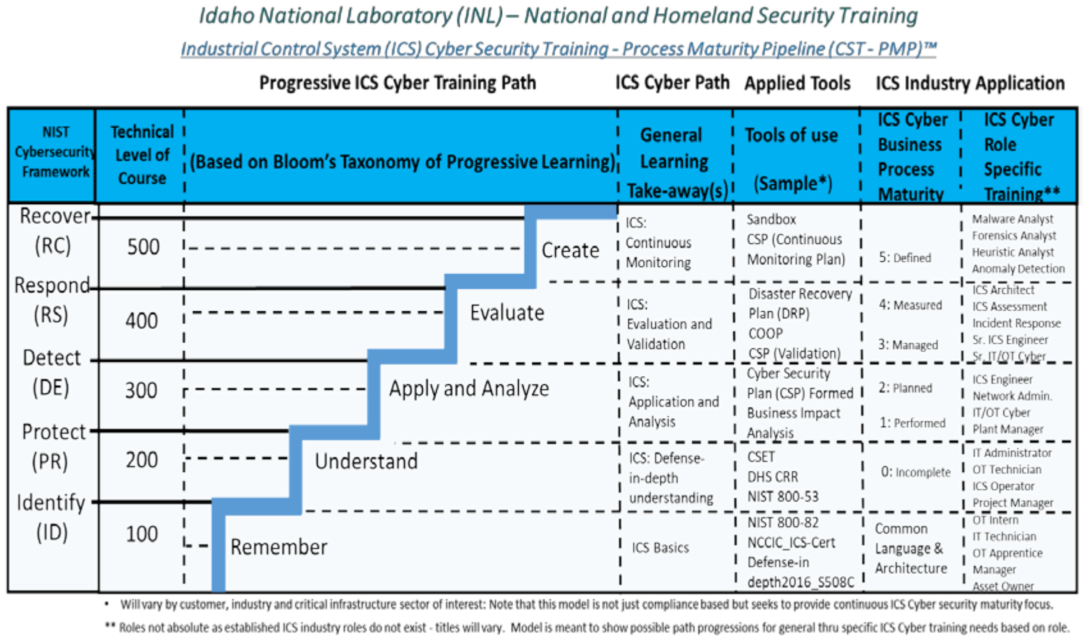


Solving a Vital Gap in Enhancing Workforce Development & Training

INL is creating an environment for the rapid and nimble exchange of ICS cybersecurity information with stakeholders, through dynamic training deliverables and development of cutting-edge education gateways.

Expanding Stakeholder Training Offerings:

- New DHS 401 Pilot Course builds on 301 (Red/Blue) foundation
- DoD (Army, Navy, Air Force, etc.) involved in 3-week ICS Assessor Course
- State, Local, Territorial, Tribal, Private Sector – dependencies, supply chain, wireless
- IROC-related training courses incorporate INL test range capabilities



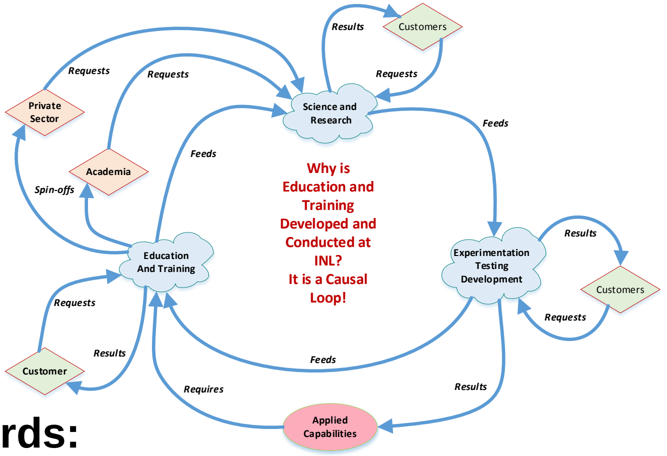
Idaho National Laboratory (INL) – National and Homeland Security Training

Industrial Control System (ICS) Cyber Security Training - Process Maturity Pipeline (CST - PMP)™

Progressive ICS Cyber Training Path			ICS Cyber Path	Applied Tools	ICS Industry Application	
NIST Cybersecurity Framework	Technical Level of Course	(Based on Bloom's Taxonomy of Progressive Learning)	General Learning Take-away(s)	Tools of use (Sample*)	ICS Cyber Business Process Maturity	ICS Cyber Role Specific Training**
Recover (RC)	500	Create	ICS: Continuous Monitoring	Sandbox CSP (Continuous Monitoring Plan)	5: Defined	Malware Analyst Forensics Analyst Heuristic Analyst Anomaly Detection
Respond (RS)	400	Evaluate	ICS: Evaluation and Validation	Disaster Recovery Plan (DRP) COOP CSP (Validation)	4: Measured 3: Managed	ICS Architect ICS Assessment Incident Response Sr. ICS Engineer Sr. IT/OT Cyber
Detect (DE)	300	Apply and Analyze	ICS: Application and Analysis	Cyber Security Plan (CSP) Formed Business Impact Analysis	2: Planned 1: Performed	ICS Engineer Network Admin. IT/OT Cyber Plant Manager
Protect (PR)	200	Understand	ICS: Defense-in-depth understanding	CSET DHS CRR NIST 800-53	0: Incomplete	IT Administrator OT Technician ICS Operator Project Manager
Identify (ID)	100	Remember	ICS Basics	NIST 800-82 NCCIC_ICS-Cert Defense-in depth2016_S508C	Common Language & Architecture	OT Intern IT Technician OT Apprentice Manager Asset Owner

- Will vary by customer, industry and critical infrastructure sector of interest: Note that this model is not just compliance based but seeks to provide continuous ICS Cyber security maturity focus.

** Roles not absolute as established ICS industry roles do not exist - titles will vary. Model is meant to show possible path progressions for general thru specific ICS Cyber training needs based on role.



Developing ICS Training Standards:

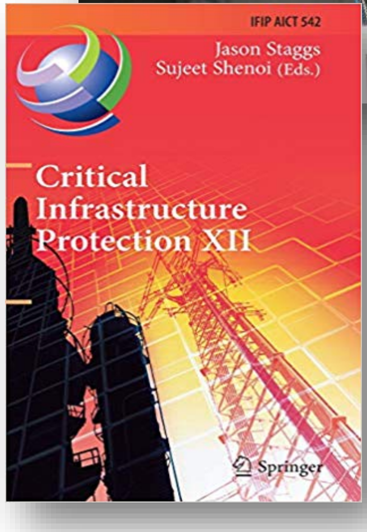
- Creating ICS Process Maturity Pipeline to guide progress
- Working with local college/university on formal ICS standards

Workforce Development Solutions:

- Establishing Cybersecurity Apprenticeship Program with partners from industry, academia, INL and workforce
- Utilizing INL ICS Cybersecurity expertise, new ICS Training Standards, CCE concepts to update academic curriculum
- Initiating INL-Developed Advanced Learning Environment platform for cutting-edge educational opportunities

Increased Publications, Presentations, and Collaborations

- N&HS-sponsored Idaho Cybersecurity Interdependencies Summit (Wayne Austad presented in Boise, ID)
- **Kevin Hemsley and Ron Fisher book chapter - "*A History of Cyber Incidents and Threats Involving Industrial Control Systems*", in Critical Infrastructure Protection XII**
- Kevin Hemsley - keynote address for the Norwegian Water Resources and Energy Directorate and Energy Directorate Workshop
- Ron Fisher - Outstanding Review Award from Academy of Management (Organization Development and Change Division) and chaired a panel session on Change Strategies
- Chris Dixon - 86th Military Operations Research Society (MORS) presentation



IFIP AICT 542

Jason Staggs
Sujeet Shenoi (Eds.)

Critical Infrastructure Protection XII

Springer

ACADEMY OF Management

Increased Publications, Presentations, and Collaborations

- N&HS sponsored an engineering capstone project with Brigham Young University
- **Ron Fisher briefed the Chair of U.S. Senate Homeland Security Committee (Wyoming U.S. Senator Ron Johnson) on INL portfolio with DHS**
- **Five division staff presented at Resilience Week**
- Ron Fisher presented at National Governor's Association's Idaho Energy Resilience Retreat
- Ollie Gagnon presented to National Rural Water Association Executive Director's Meeting on cybersecurity
- Ron Fisher reviewed articles for the Journal of Cybersecurity, Organization Development Journal, and Academy of Management

JOURNAL OF CYBERSECURITY

Organization Development Journal

"Guiding the future of people working together"

Featuring best internal OD practices from the following organizations around the globe including Europe, Asia, and Africa:
American Cancer Society
AT&T
Avnet
Blue Cross Blue Shield of Massachusetts
BP
Caterpillar Inc.
Constellation Energy
Disney ABC Media Networks
Lilly
Goldman Sachs
HSBC Group
Intel
Johnson & Johnson
Microsoft
Procter & Gamble
Raytheon
[illegible]
Sasol
Sony
Sun Microsystems
United States Army
U.S. Environmental Protection Agency
Yale New Haven Health System

In this issue you will find articles examining:
- Change Management
- Cultural Intervention
- Employee Engagement
- Executive and Leadership Development
- Mentoring & Coaching
- Merger/Acquisition Integration
- Organization Capability/Effectiveness
- Organization Design/Transformation
- Talent Management
- Team Building/Effectiveness
- Applying Six Sigma in HR

SPECIAL EDITION:
Best Global Practices in Internal OD

Published by
the Organization Development Institute

SUMMER 2007
VOLUME 25: NUMBER 2

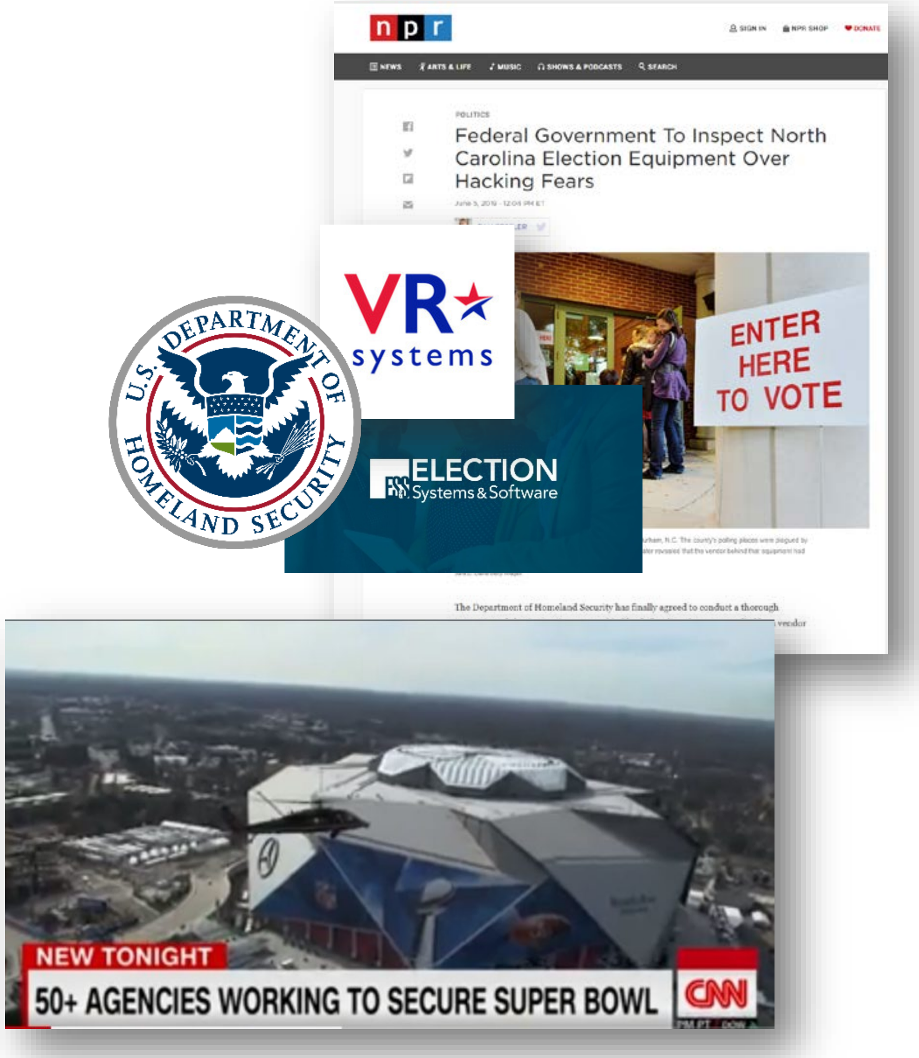
BRIGHAM YOUNG UNIVERSITY · FOUNDED BYU 1875 · PROVO, UTAH

NATIONAL RURAL WATER ASSOCIATION

NGA NATIONAL GOVERNORS ASSOCIATION

N&HS is Making A Strong Impact in Homeland Security

- **Exceeded $100M in FY18 of DHS funding (largest funded DOE national lab for DHS)**
- **Completed impactful vulnerability assessment pilots of election system equipment**
- **Awarded International Association for Continuing Education and Training (IACET) certification to issue continuing education credits for cybersecurity training**
- Trained more than 20,000 people over the past year through on-line cybersecurity courses
- Completed strategic high-speed network connection between Idaho Falls, Washington DC, and Pensacola
- Developed and deployed CASCADE situational awareness tool used by DHS to support multiple national disasters (e.g. Hurricane Florence)
- Conducted cybersecurity assessments for 2019 Super Bowl



npr

SIGN IN NPR SHOP DONATE

NEWS ARTS & LIFE MUSIC SHOWS & PODCASTS SEARCH

POLITICS

Federal Government To Inspect North Carolina Election Equipment Over Hacking Fears

June 5, 2019 · 12:04 PM ET

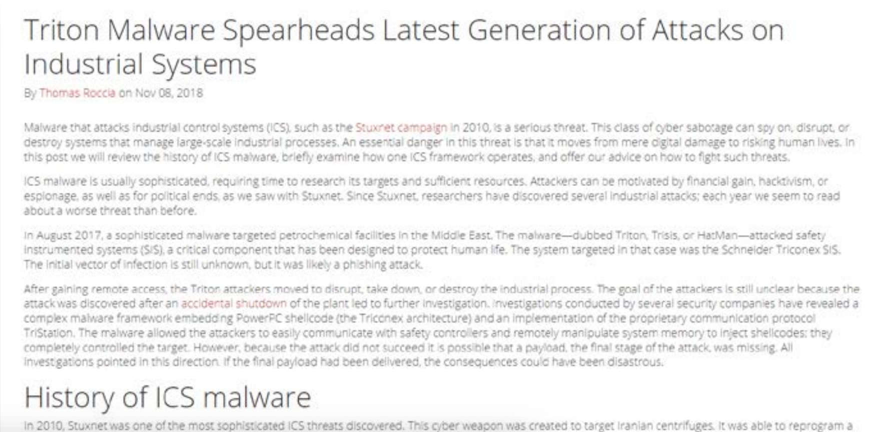
The Department of Homeland Security has finally agreed to conduct a thorough

U.S. DEPARTMENT OF HOMELAND SECURITY
VR systems
ELECTION Systems & Software
ENTER HERE TO VOTE
NEW TONIGHT
50+ AGENCIES WORKING TO SECURE SUPER BOWL
CNN

N&HS is Making A Strong Impact in Homeland Security

- Analyzed new variant of Hatman/Trition malware
- Trained Army Cyber Command IT assessors with 3-week OT assessment course
- Conducted 5-day cybersecurity training course for Japanese Cybersecurity Division of Commerce and Information Policy Bureau Ministry of Economy, Trade, and Industry (METI)
- Released CSET Version 9.0 via open-source web framework
- Developed a multi-million dollar ICS Lab funded by DHS
- Received letter of appreciation from DHS Secretary Kirstjen M. Nielsen calling out heroic actions to DHS/INL Hunt and Incident Response Team (HIRT)
- Received letter of appreciation from National Cybersecurity & Communications Integration Center Director John Felker on INL's leadership for HIRT response training

McAfee™ Together is power. | Securing Tomorrow. Today.



Triton Malware Spearheads Latest Generation of Attacks on Industrial Systems

By Thomas Roccia on Nov 08, 2018

Malware that attacks industrial control systems (ICS), such as the Stuxnet campaign in 2010, is a serious threat. This class of cyber sabotage can spy on, disrupt, or destroy systems that manage large-scale industrial processes. An essential danger in this threat is that it moves from mere digital damage to risking human lives. In this post we will review the history of ICS malware, briefly examine how one ICS framework operates, and offer our advice on how to fight such threats.

ICS malware is usually sophisticated, requiring time to research its targets and sufficient resources. Attackers can be motivated by financial gain, hacktivism, or espionage, as well as for political ends, as we saw with Stuxnet. Since Stuxnet, researchers have discovered several industrial attacks; each year we seem to read about a worse threat than before.

In August 2017, a sophisticated malware targeted petrochemical facilities in the Middle East. The malware—dubbed Triton, Trisis, or HatMan—attacked safety instrumented systems (SIS), a critical component that has been designed to protect human life. The system targeted in that case was the Schneider Triconex SIS. The initial vector of infection is still unknown, but it was likely a phishing attack.

After gaining remote access, the Triton attackers moved to disrupt, take down, or destroy the industrial process. The goal of the attackers is still unclear because the attack was discovered after an accidental shutdown of the plant led to further investigation. Investigations conducted by several security companies have revealed a complex malware framework embedding PowerPC shellcode (the Triconex architecture) and an implementation of the proprietary communication protocol TriStation. The malware allowed the attackers to easily communicate with safety controllers and remotely manipulate system memory to inject shellcodes; they completely controlled the target. However, because the attack did not succeed it is possible that a payload, the final stage of the attack, was missing. All investigations pointed in this direction. If the final payload had been delivered, the consequences could have been disastrous.

History of ICS malware

In 2010, Stuxnet was one of the most sophisticated ICS threats discovered. This cyber weapon was created to target Iranian centrifuges. It was able to reprogram a

Stuxnet was not to destroy but to take the control of the industrial

s collected a large amount of data and remotely monitored

n workstations and servers. In Ukraine, 230,000 people were left

functionalities similar to Stuxnet's. It is unclear if this was a proof

CSET® CYBER SECURITY EVALUATION TOOL

METI Ministry of Economy, Trade and Industry

INL

Idaho National Laboratory