U.S. DEPARTMENT OF ENERGY

Idaho National Laboratory

DEPARTMENT OF ENERGY AND NATIONAL LABS

JULY 21ST, 2020 | 2:10PM EDT

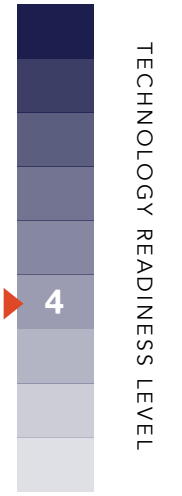
MASTERI

(Tech ID#: BA-1064)

A Computer-aided Technique for Assessing Infrastructure Reliability and Resilience and Related Systems, Methods, and Devices: MASTERI is an integrated suite of software that accurately calculates device dependency and the resulting expected Return on Resiliency Investment.

Business Problem

In Industrial Control Systems, its often difficult to determine which upgrades will deliver the best return on investment for reinvestment in device resiliency.



Development History

- **2017** Began
- **2018** Won best paper at Resilience Week
- **2019** Began joint Duke Energy project
- **2020** Entered R&D100 award contest
- **2021** Refinement with Duke Energy

Funding History

- $50,000 LDRD
- $1,100,000 DoE
- JV with Duke Energy (In Kind)

Intellectual Property: US provisional 62/720,618 on 8/21/2018

Principal Investigator

Bjorn Vaagensmith M.S & Ph.D. in Electrical Engineering from South Dakota State University; Power Systems, Electric Grid Hardening & Cybersecurity

Benefits

- ✓ Reduces compliance labor
- ✓ Reduces replacement labor costs on unanticipated failures
- ✓ Improved Uptimes

Research Team

Carol Reid Project Manager
James Case Systems Engineering Group Lead
Kurt Vedros Lead Risk Assessment Engineer
Tim McJunkin Senior R&D Engineer
Jesse Reeves Power System Researcher
Liam Boire Systems Engineer

Market Validation

- Won best paper at Resilience Week 2018
- MIRACL industry advisory board provided positive feedback
- Duke Energy teamed with Department of Energy to leverage MASTERI under joint venture

U.S. DEPARTMENT OF ENERGY

INL Idaho National Laboratory

DEPARTMENT OF ENERGY AND NATIONAL LABS

JULY 21ST, 2020 | 2:35PM EDT

OpDefender

(Tech ID#: BA-996)

Network Control and Monitoring System for Industrial Control Systems: OpDefender is a means of retrofitting industrial control systems with software defined networks to add cybersecurity functionality in legacy devices.

Business Problem

The threat to Industrial Control Systems is widespread, affecting many industries. The threat is growing and the defensive tools have not kept pace with their offensive counterparts.

Development History

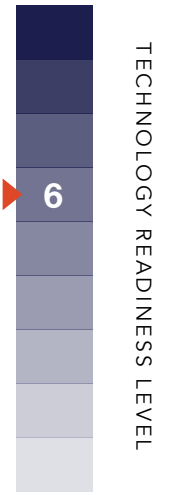
- **2015** Start
- **2018** Selected by INL for provisional patent
- **2019** Full utility patent app submitted by INL
- **2020** OpDefender participates in EMAPS testing on INL's test range; INL chooses OpDefender as a candidate for an R&D100 award

Funding History

$591,000 LDRD

$144,000 EMAPS Phase I

$207,000 EMAPS Phase II (ongoing)



IP Protection: Provisional Patent, June 2018 | Full Utility Patent, June 2019

Principal Investigator

Briam Johnson Chief Power Engineer, Cybercore

Research Team

Michael McCarty Senior Cyber Researcher, Cybercore

Benefits

- ✓ Added "smarts" to OT systems
- ✓ Scales
- ✓ Minimal Latency
- ✓ Reliable
- ✓ Cost Effective
- ✓ Versatile
- ✓ Security Benefits Outweigh New Risks
- ✓ Easy to Deployable & Maintain

Market Validation

- Recent full scale test on INL's test range
- Tested against 14 different test effect payloads (TEPs), targeting 4 different devices from multiple manufacturers: Successfully blocked all 14 test effect payloads
- Tested against malformed/unused & unauthorized

U.S. DEPARTMENT OF ENERGY

INL Idaho National Laboratory

DEPARTMENT OF ENERGY AND NATIONAL LABS

JULY 21ST, 2020 | 3:00PM EDT

WiFIRE

(Tech ID#: BA-961)

Spectrum Monitoring and Analysis, and Related Methods, Systems, and Devices: WiFIRE uses multiple sensor devices and integrated software to simplify wireless network spectrum monitoring for physical-cyber security.

Business Problem

Organizations are dependent upon wireless communications, but the general ability to monitor the communication frequencies along the spectrum create challenges. Malicious actors compromise and disable wireless systems for the purpose of industrial espionage or disrupting systems, resulting in loss of IP or downtime.

Development History

- **2015** Start of research partnership
- **2016** Interest in WiFIRE by Palo Verde Nuclear
- **2017** DOE Energy I-Corps Lite Program
- **2018** DHS Funding
- **2019** DoE TCF Topic 1 Funding awarded

Funding History

$745,000 LDRD

$300,000 DOE Technology Commercialization Funding, Topic 1

DHS, FY18 - FY20

IP Protection: Provisional: Plug and Play Flexible Signal Classification and Processing System, no. 62/928,834, 10/31/2019
Wireless Radio Frequency Signal Identification & Protocol Reverse Engineering, no. 16/569,565, 9/12/201

Principal Investigator

Kurt Derr Wireless Cyber Systems Researcher, M.S. and Ph.D. in Computer Science from University of Idaho

Research Team

Christopher Becker Lead Architect and Developer
May Chaffin Developer
Armando Juarez Developer
Samuel Ramirez Past Contributor
University of Utah Partners

Market Validation

- R&D 100, 2019
- Idaho Innovation Awards, Early-Stage Innovation of the Year Finalist, 2019
- Palo Verde Nuclear
- Exelon Generation (Nuclear Energy Provider), Letter of Support, Cyber Security Manager, 2018
- DOE Energy I-Corps Lite Program Customer Discovery Interviews

Benefits

- ✓ Improved safety and security of wireless communications
- ✓ Reduces operator training
- ✓ Reduces labor, equipment and training costs with one common toolset

U.S. DEPARTMENT OF ENERGY | Sandia National Laboratories

DEPARTMENT OF ENERGY AND NATIONAL LABS

JULY 23RD, 2020 | 2:10PM EDT

HADES

(Tech ID#: 13370)

Computer Network Defense System: HADES's AI produces high fidelity business documents and changing IT environments to create a live massive interactive "honeypot" aimed at deceiving an attacker for long durations.

Business Problem

Current deception solutions, known as "honeypots" are low fidelity, and therefor fail to deceive attackers for long enough durations to capture threat intelligence.

Development History

- **2015** Initial patent filing
- **2017** R&D 100 Winner Patent granted
- **2018** Government Innovation Award
- **2019** TechConnect Innovation Award

Funding History

Over $8,000,000 LDRD

Other Government funding

IP Protection: US Patent No. 9,742,804 Two additional patents pending

Principal Investigator

Vince Urias 20 Years of cyber experience at Sandia, Numerous national awards

Research Team

William Stout
Caleb Loverro

Benefits

- ✓ Scalable to any size environment
- ✓ Complete control of deception environment
- ✓ Actionable, real-time threat intelligence

Market Validation

- Government Innovation Award
- TechConnect Innovation Award
- 10 Installations

U.S. DEPARTMENT OF ENERGY

Pacific Northwest NATIONAL LABORATORY

DEPARTMENT OF ENERGY AND NATIONAL LABS

JULY 23RD, 2020 | 2:35PM EDT

Cybersecurity Framework

(Tech ID#: 31293, 31346)

Cybersecurity Framework and Compliance Tool: Cybersecurity Framework is a management and compliance tool to manage, train and improve the cybersecurity posture within industrial control organizations.

Business Problem

Organizations are dealing with evolving cybersecurity regulatory requirements, and the information to be gathered is dispersed across the various functional units - making it challenging to keep ahead of cybersecurity compliance.

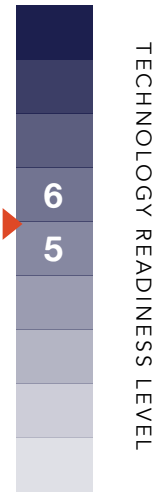
Development History

- **2017** Proof of concept
- **2018** Production tool development
- **2019** Live assessments with 20+ federal stakeholders
- **2020-2022** Enhancements: CMMC, C2M2 V2.0, RMF, Threat mapping, best practices mapping

Funding History

$50,000 LDRD

$700,000 DoE



IP Protection: US Patent 16/780,672, filed 2/3/2020: Cybersecurity Assessment and Risk Management Tool
Copyrights (to be filed): Cyber Arsenal web software

Principal Investigator

Sri Nikhil Gupta Gourisetti Ph.D. EE from Univ. of Arkansas-Little Rock, CISSP, GICSP, Energy Cybersecurity Researcher Smart Grid and Connected Buildings

Research Team

Julia Rotondo Project Manager
Jey Castleberry Cybersecurity Researcher
Devan Farrell Senior Software Engineer
Hayden Reeve Senior Buildings Controls Advisor
Paul Skare Energy Cybersecurity Advisor

Benefits

- ✓ Web-based software application
- ✓ Advanced user-friendly data analytics
- ✓ Lets user track mitigation progress over time
- ✓ Built-in Comparative analyzer

Market Validation

- Live assessments at federal facilities.
- Live demonstration with 20+ federal and commercial organizations.

U.S. DEPARTMENT OF ENERGY | Sandia National Laboratories

DEPARTMENT OF ENERGY AND NATIONAL LABS

JULY 23RD, 2020 | 3:00PM EDT

ADDSec

(Tech ID#: 13240.1)

Dynamic Defense and Network Randomization for Computer Systems: ADDSec brings an integrated suite of cybersecurity techniques together to create IP hopping capabilities to prevent and mitigate threats to the network.

Business Problem

Unlike dynamic networks, static networks use predictable communications and static configurations, making them vulnerable to attack.

Development History

- **2014** Initial patent filing
- **2018** US patent granted
- **2019** R&D100 Award Winner (Software/services)

Funding History

$3,800,000 DOE CESER Office

IP Protection: US Patent No. 9,985,984 Dynamic Defense and Network Randomization for Computer Systems

Principal Investigator

Adrian Chavez Ph.D. Computer Science
University of California, Davis, Principal Member of Technical Staff Cybersecurity R&D

Benefits

- ✓ Very low network load
- ✓ Improved cyber resilience
- ✓ Effective cyber attack detection

Research Team

Jason Hamlet
William Stout
Erik Lee
Mitchell Martin
James Obert

Market Validation

- 2017, Successful interoperability testing performed at SEL site (May)
- 2018, Technology demonstrated DoD Ft Belvoir microgrid, Washington Gas, Chevron, Lawrence Livermore National Laboratory, Schwietzer Engineering Laboratories, Grimm, DoD Ft. Belvoir Microgrid

U.S. DEPARTMENT OF ENERGY | Sandia National Laboratories

DEPARTMENT OF ENERGY AND NATIONAL LABS

JULY 28TH, 2020 | 2:10PM EDT

CHIRP

(Tech ID#: 14747)

Cloud Forensics and Incident Response Platform: CHIRP is a cloud incident response software package that captures breach data typically lost beyond the hypervisor to improve cybersecurity analyst visability into the cloud.

Business Problem

When cyber incidents occur in the cloud, the SOC Analyst has no visibility beyond the hypervisor.

Development History

- **2016** Initial development starts
- **2018** First disclosed (Dec)
- **2019** R&D100 Award Winner (May)

Funding History

$1,000,000 LDRD

IP Protection: Patent Application # 16/051,005 filed July 31, 2018
Copyright approved for commercial licensing – May 2018

Principal Investigator

Vince Urias 20 Years of Cyber experience at Sandia Labs, Numerous national awards

Research Team

William Stout
Caleb Loverro

Benefits

- ✓ Lightweight
- ✓ Real-time dynamic response
- ✓ Configurable logging for incident response or forensics

Market Validation

- R&D100 Award Winner
- Two government deployments

U.S. DEPARTMENT OF ENERGY | OAK RIDGE National Laboratory

DEPARTMENT OF ENERGY AND NATIONAL LABS

JULY 28TH, 2020 | 2:35PM EDT

SITU

(Tech ID#: 201703869)

Real-time Situational Understanding and Discovery of Cyber Attacks: SITU produces real-time anomaly alerting to allow for the timely discovery and understanding of new unknown/sophisticated cyber attacks.

Business Problem

Signature-based systems cannot detect unknown attacks. Supervised machine learning approaches require labeled data sets. Neither humans nor automated systems can detect all attacks as it is too much data to sort through. Need scalable, streaming anomaly detection to highlight suspicious activity within high data rates.

TECHNOLOGY READINESS LEVEL: 9

Development History

- **2012** Began Labratory Directed Research & Development (LDRD)
- **2016** Operational at ORNL in SOC
- **2018** R&D100 Finalist
- **2019** IEEE VIS paper

Funding History

$500,000 LDRD

$2,000,000 DoD/DHS/DoE

IP Protection: US9361463B2 – Detection of anomalous events (2016)
US9319421B2 – Real-time detection and classification of anomalous events in streaming data (2016)

Principal Investigator

John Goodall PhD in Information Systems from UMBC, 15 years of advanced cybersecurity

Benefits

- ✓ No labels or training data is required
- ✓ IIngests NetFlow v9, IPFIX, Argus or Apache Kafka, Nats, RabbitMQ
- ✓ Visualization works in any modern browser

Research Team

Joel Reed
Dave Richardson
Kelly Huffer
Erik Ferragut
Bobby Bridges

Market Validation

- ORNL SOC: 450M flows / day
- ORNL NCCS: 5.2M flows / day
- ORNL Significant Event Award (2018)
- Various Pilot deployments

U.S. DEPARTMENT OF ENERGY | OAK RIDGE National Laboratory

DEPARTMENT OF ENERGY AND NATIONAL LABS

JULY 28TH, 2020 | 3:00PM EDT

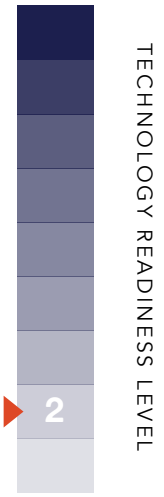
AXL

(Tech ID#: 201804113)

Automated Extraction of Malware Behavior from Logs: AXL utilizes advanced machine learning to identify which files have been impacted by malware, thereby expediting the incidence response by eliminating time spent sifting through massive log data.

Business Problem

Identifying malware behavior from logs manually takes many hours of highly trained cybersecurity labor from the already understaffed and overburdened Security Operation Centers teams.



Development History

- **2017** Algorithm pioneered with TFIDF, Fisher's LDA; Cuckoo (sandbox)
- **2018-2020** Follow-on testing with Decision Trees and Deep Learning indicate TFIDF still better for extracting attack log sequence

Funding History

$850,000 LDRD

IP Protection: Invention Disclosure #201804113, April 2018

Principal Investigator

Robert Bridges Ph.D. in Mathematics from Purdue, Cybersecurity Research Mathematician

Benefits

- ✓ Estimated 50% reduction in Incident Response Time
- ✓ Use on historic logs for discovery of false negatives (missed attacks
- ✓ Expedites dynamic malware analysis

Research Team

Professor Qian (Guenevere) Chen PhD, University Texas San Antonio

Market Validation

- First Publication in Dec 2017
- One "spin-off" publications in 2019, second accepted in 2020

U.S. DEPARTMENT OF ENERGY

Pacific Northwest NATIONAL LABORATORY

DEPARTMENT OF ENERGY AND NATIONAL LABS

JULY 30TH, 2020 | 2:10PM EDT

Cybersecurity Visualization

(Tech ID#: 31612)

Operations Technology Cybersecurity Visualization Tool: OT Cybersecurity Visualization Dashboard is a software tool that allows improved collaboration between OT operators and IT/cyber personnel to improve cybersecurity response times in operational technology environments.

Business Problem

When an attack occurs in the OT network, it can remain unresolved, posing the threat of millions of dollars in equipment damages and potentially billions of dollars from outages. One major cause is that the communication barriers between control room operators and cybersecurity professionals.

Development History

- **2015** Began project
- **2018** Successful usability testing with Operators in CA and Cyber in CO using simulated attacks, Presentation to Puerto Rico Electric Power Authority (PREPA)

Funding History

$2,000,000 DoE

Principal Investigator

Eric Andersen Project Manager, BS, Mechanical Engineering, Washington State University
Systems Integration

Benefits

- ✓ Improved communications
- ✓ Ability to gain visibility into OT in control room and in field

Research Team

Dr. Mark Rice, Lindsey Franklin, Dr. Aditya Ashok, Lisa Newburn, Greg Dayley, Dr. Jean Scholtz, Scott Dowson, Katya Le Blanc, Mike Cassiadoro, Dr. Jodi Heintz-Obradovich

Market Validation

- Dominion Power
- Western Area Power Administration
- Ernst & Young

U.S. DEPARTMENT OF ENERGY

Pacific Northwest NATIONAL LABORATORY

DEPARTMENT OF ENERGY AND NATIONAL LABS

JULY 30TH, 2020 | 2:35PM EDT

Shadow Figment

(Tech ID#: 31305)

High Fidelity Model Driven Deception Platforms for Control Systems: Shadow Figment brings high fidelity 'honeypot" deception techniques to physical devices in the operational technology environments.

Business Problem

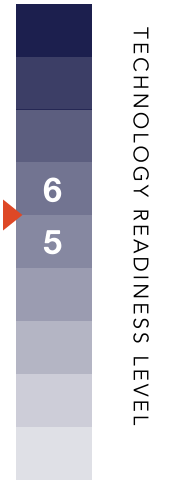
Physical-cyber system owners frequently have mandates to prioritize system uptimes and availability, which limits the opportunities to deploy security solutions. Protecting every asset is cost prohibitive and IT solutions are commonly not supported in these OT environments.

Development History

- **2017** Began internal research
- **2019** Began DOE TCF project
- **2019** IEEE HST publication

Funding History

$200,000 LDRD Internal
$150,000 DoE TCF
$150,000 Attivo Networks (In-Kind)



IP Protection: US Application No. 16/389,758 and CA CA3041865A1 (priority date: 4/2018)

Principal Investigator

Thomas Edgar Cyber Security Researcher, Security applications for critical infrastructure, Successfully licensed previous R&D100 winning technology

Benefits

- ✓ Orient attacker resources away from real CPS
- ✓ Bias attacker's beliefs on real CPS operation
- ✓ Enhance detection of adversarial behavior with reduced false positive rate
- ✓ Understand threat objectives

Research Team

William Hofer Cyber Security
Juan Brandi-Lozano Data Science
Garret Seppala Software Engineer
Katy Nowak Data Science
Draguna Vrabie Control Engineer

Market Validation

- DOE Technology Commercialization Fund Award
- Attivo Networks collaboration

U.S. DEPARTMENT OF ENERGY

Sandia National Laboratories

DEPARTMENT OF ENERGY AND NATIONAL LABS

JULY 30TH, 2020 | 3:00PM EDT

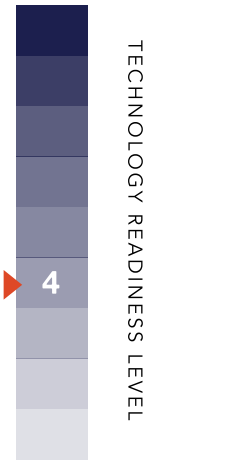
CAPSec

(Tech ID#: 13486)

Real-Time Software Upgrade: CAPSec applies continuous software security patching capabilities in high uptime environments through the use of containerized patching.

Business Problem

Software patching disrupts uptime, resulting in increased costs and lost revenue. As many industries require near continuous uptimes, this frequently delays patching, increasing the vulnerabilities to cyber attack.



Development History

- **2016** First filing (July)
- **2018** Project kick-off (May)
  US patent granted (July)
- **2020** Established proof-of-concept (Feb)

Funding History

$2,500,000 DOE CESER Office

IP Protection: US Patent No. 10,037,203 Real Time Software Upgrade

Principal Investigator

Adrian Chavez Ph.D. Computer Science
University of California, Davis, Principal Member of Technical Staff, Cybersecurity R&D

Benefits

- ✓ Improved resilience
- ✓ Active patching & remediation during cyber attack
- ✓ Decreased maintenance time

Research Team

Ryan Birmingham
Jasenko Hosic
Jaykumar Pate
Kandy Phan
William Stout

Market Validation

- Schweitzer Engineering Laboratories
- Pacific Northwest National Laboratories
- Grimm
- Chevron
- Ft. Belvoir