CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

CIRI Annual Meeting
December 6-7, 2022

ciri.illinois.edu

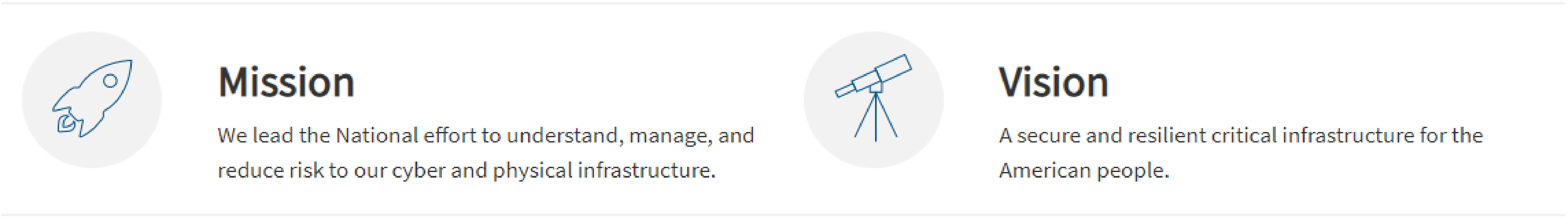
Keynote Speaker

Brian Gattoni
CTO, CISA

CELEBRATING PARTNERSHIP

CYBERSECURITY AND *INFRASTRUCTURE* SECURITY AGENCY
&
CRITICAL *INFRASTRUCTURE* RESILIENCE INSTITUTE

CISA 101



Mission

We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

Vision

A secure and resilient critical infrastructure for the American people.

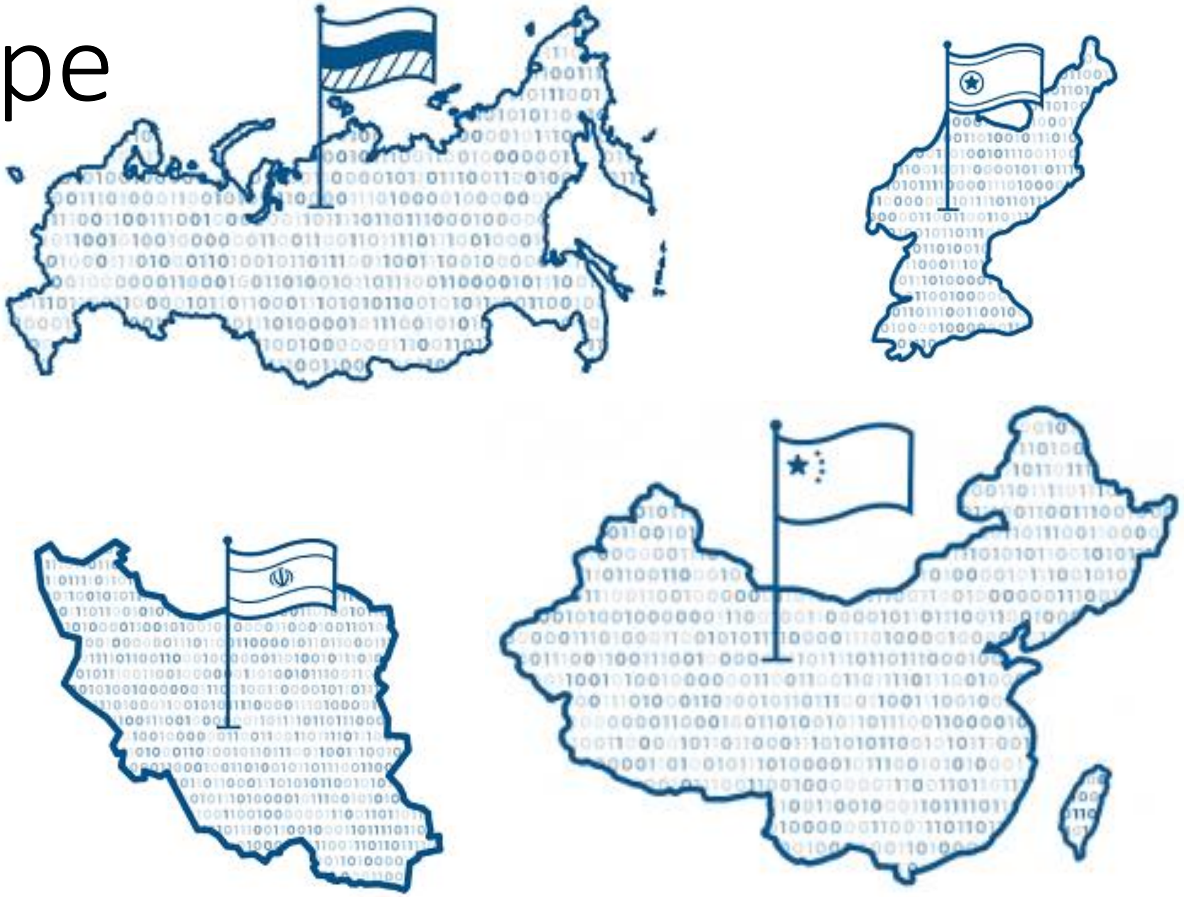
Current Threat Landscape

STOP RANSOMWARE

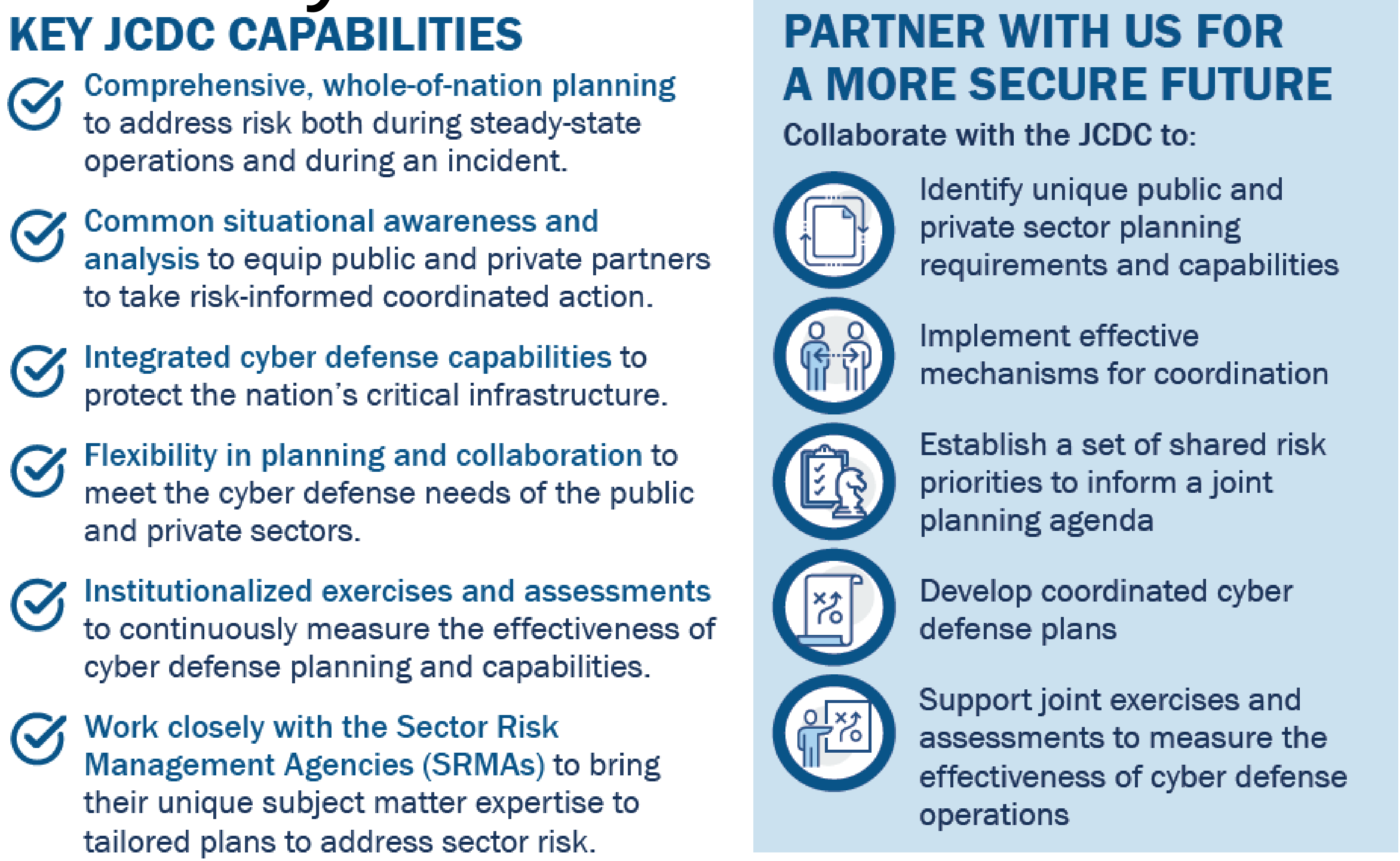
ALERT — UPDATED

APT Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

SHIELDS UP



Joint Cyber Defense Collaborative



KEY JCDC CAPABILITIES

- ✓ **Comprehensive, whole-of-nation planning** to address risk both during steady-state operations and during an incident.
- ✓ **Common situational awareness and analysis** to equip public and private partners to take risk-informed coordinated action.
- ✓ **Integrated cyber defense capabilities** to protect the nation's critical infrastructure.
- ✓ **Flexibility in planning and collaboration** to meet the cyber defense needs of the public and private sectors.
- ✓ **Institutionalized exercises and assessments** to continuously measure the effectiveness of cyber defense planning and capabilities.
- ✓ **Work closely with the Sector Risk Management Agencies (SRMAs)** to bring their unique subject matter expertise to tailored plans to address sector risk.

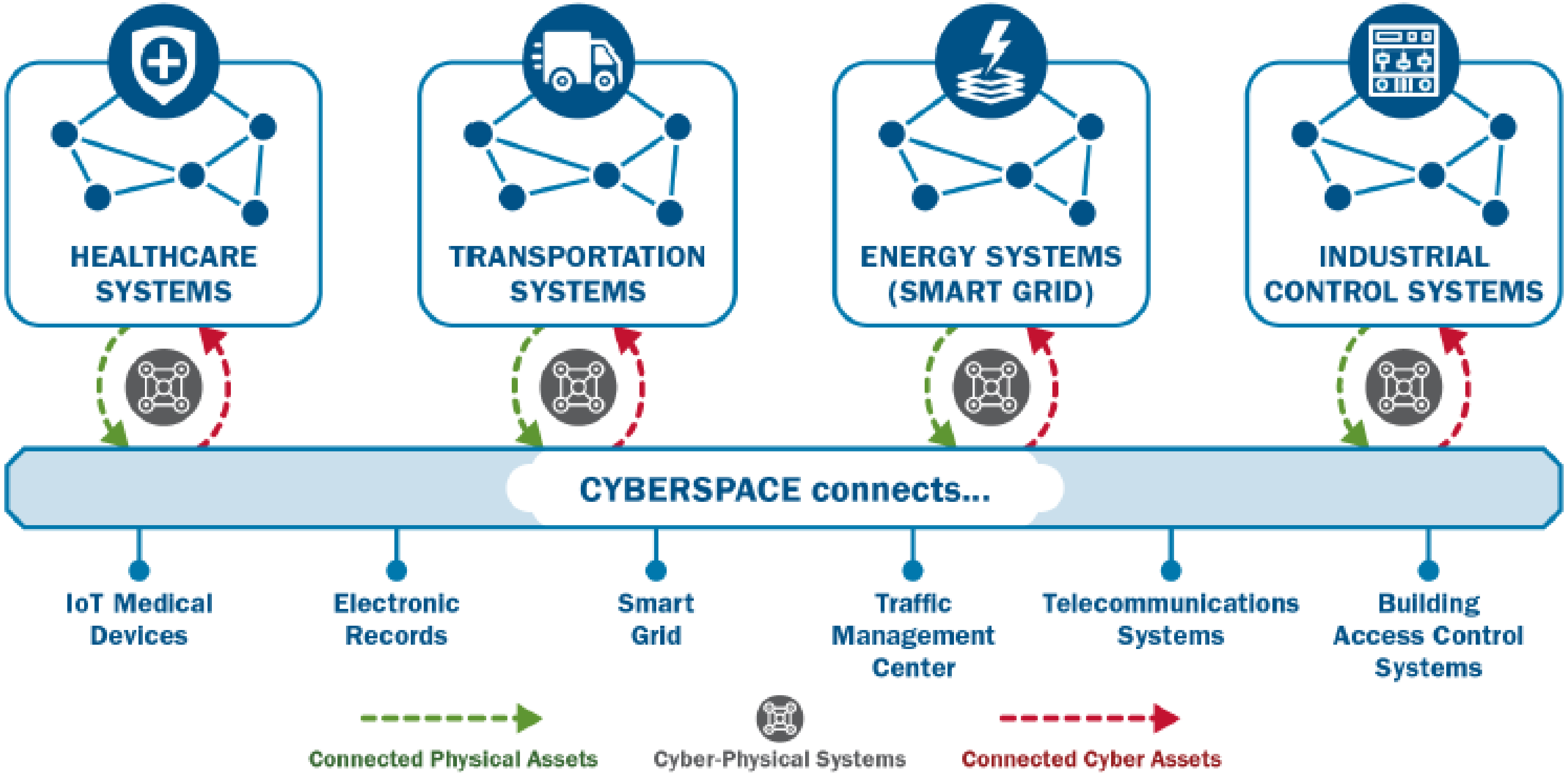
PARTNER WITH US FOR A MORE SECURE FUTURE

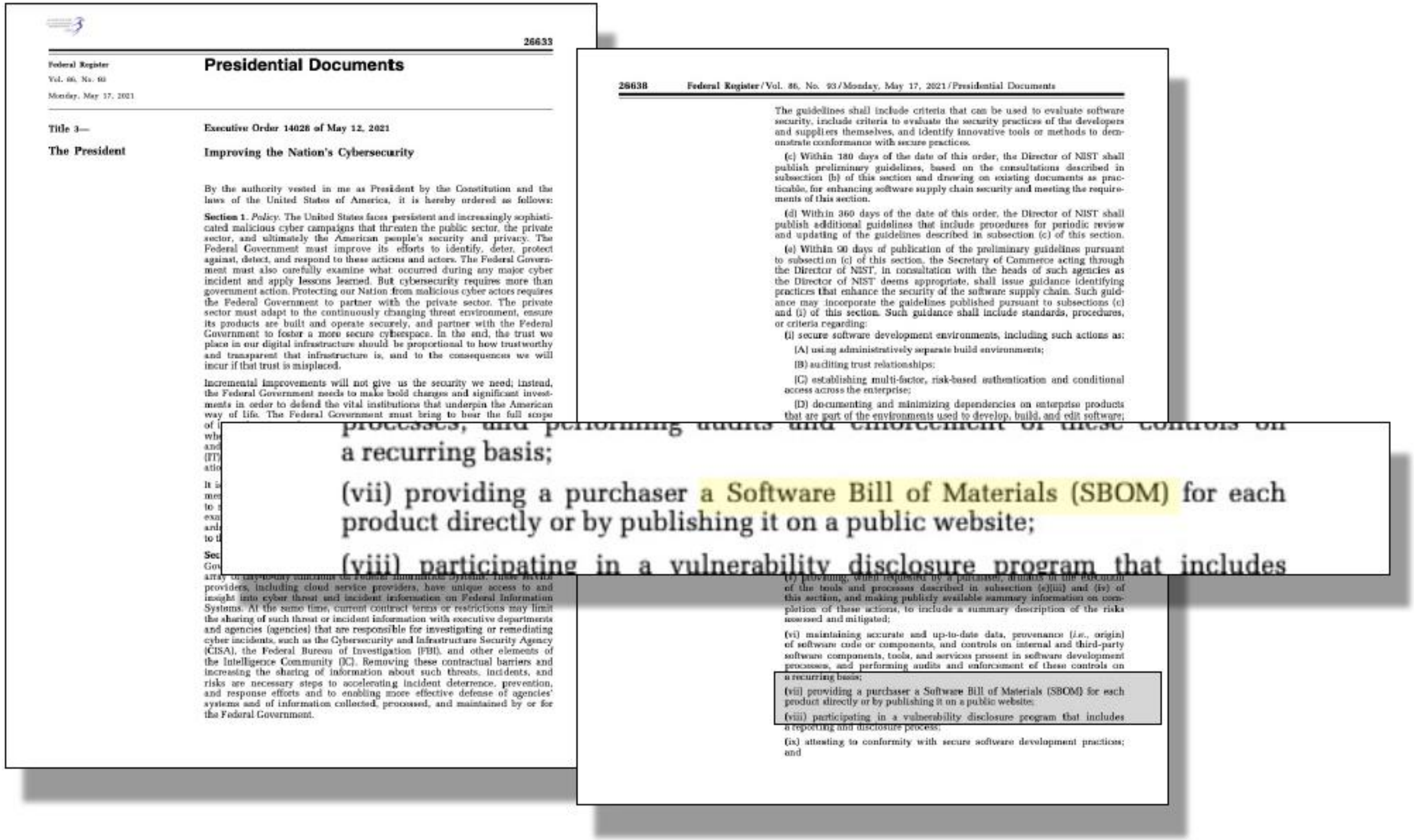
Collaborate with the JCDC to:

- Identify unique public and private sector planning requirements and capabilities
- Implement effective mechanisms for coordination
- Establish a set of shared risk priorities to inform a joint planning agenda
- Develop coordinated cyber defense plans
- Support joint exercises and assessments to measure the effectiveness of cyber defense operations

JOINT CYBER DEFENSE
COLLABORATIVE

Cy


HEALTHCARE SYSTEMS
TRANSPORTATION SYSTEMS
ENERGY SYSTEMS (SMART GRID)
INDUSTRIAL CONTROL SYSTEMS
CYBERSPACE connects...
IoT Medical Devices
Electronic Records
Smart Grid
Traffic Management Center
Telecommunications Systems
Building Access Control Systems
Connected Physical Assets
Cyber-Physical Systems
Connected Cyber Assets



26633

Federal Register
Vol. 86, No. 93
Monday, May 17, 2021

Presidential Documents

Title 3—

The President

Executive Order 14028 of May 12, 2021

Improving the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy*. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope

array of day-to-day functions on Federal Information Systems. These service providers, including cloud service providers, have unique access to and insight into cyber threat and incident information on Federal Information Systems. At the same time, current contract terms or restrictions may limit the sharing of such threat or incident information with executive departments and agencies (agencies) that are responsible for investigating or remediating cyber incidents, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and other elements of the Intelligence Community (IC). Removing these contractual barriers and increasing the sharing of information about such threats, incidents, and risks are necessary steps to accelerating incident deterrence, prevention, and response efforts and to enabling more effective defense of agencies' systems and of information collected, processed, and maintained by or for the Federal Government.

26638 Federal Register / Vol. 86, No. 93 / Monday, May 17, 2021 / Presidential Documents

The guidelines shall include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices.

(c) Within 180 days of the date of this order, the Director of NIST shall publish preliminary guidelines, based on the consultations described in subsection (b) of this section and drawing on existing documents as practicable, for enhancing software supply chain security and meeting the requirements of this section.

(d) Within 360 days of the date of this order, the Director of NIST shall publish additional guidelines that include procedures for periodic review and updating of the guidelines described in subsection (c) of this section.

(e) Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance may incorporate the guidelines published pursuant to subsections (c) and (i) of this section. Such guidance shall include standards, procedures, or criteria regarding:

(i) secure software development environments, including such actions as:

(A) using administratively separate build environments;

(B) auditing trust relationships;

(C) establishing multi-factor, risk-based authentication and conditional access across the enterprise;

(D) documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software;

(v) providing, when requested by a purchaser, artifacts of the execution of the tools and processes described in subsection (e)(iii) and (iv) of this section, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated;

(vi) maintaining accurate and up-to-date data, provenance (*i.e.*, origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

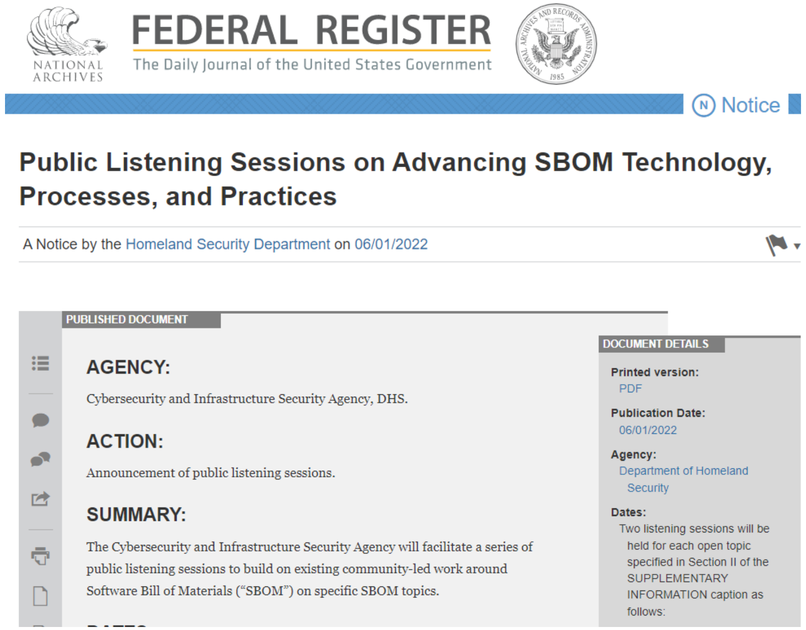
(viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

(ix) attesting to conformity with secure software development practices; and

processes, and performing audits and enforcement of these controls on a recurring basis;

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(viii) participating in a vulnerability disclosure program that includes



NATIONAL ARCHIVES
FEDERAL REGISTER
The Daily Journal of the United States Government

Public Listening Sessions on Advancing SBOM Technology, Processes, and Practices

A Notice by the Homeland Security Department on 06/01/2022

PUBLISHED DOCUMENT

AGENCY:

Cybersecurity and Infrastructure Security Agency, DHS.

ACTION:

Announcement of public listening sessions.

SUMMARY:

The Cybersecurity and Infrastructure Security Agency will facilitate a series of public listening sessions to build on existing community-led work around Software Bill of Materials ("SBOM") on specific SBOM topics.

DOCUMENT DETAILS

Printed version:
PDF

Publication Date:
06/01/2022

Agency:
Department of Homeland Security

Dates:
Two listening sessions will be held for each open topic specified in Section II of the SUPPLEMENTARY INFORMATION caption as follows:

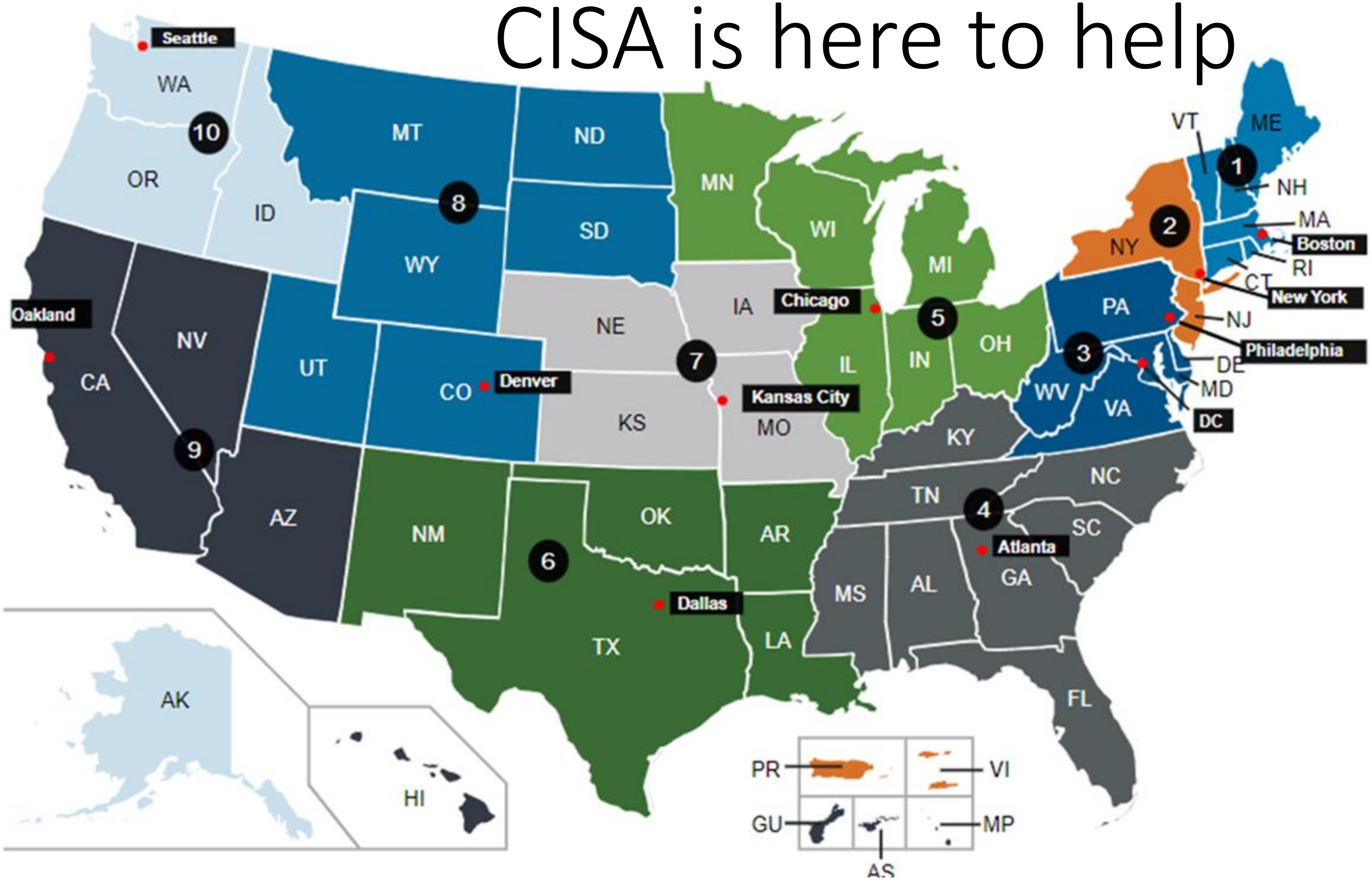
Risk and Resilience

- **Connections** by technologies that enable critical communications and capabilities to send and receive data (e.g., internet connectivity),
- **Distribution** methods that allow the movement of goods, people, and utilities inside and outside the United States (e.g., electricity distribution or cargo transportation),
- **Management** processes that ensure our national security and public health and safety (e.g., management of hazardous material or national emergencies), and
- **Supplies** of materials, goods and services that secure our economy (e.g., clean water, housing, and research and development).

Importance of R&D relationships

- Information Sharing
- Election Security
- Ransomware
- Securing Federal Networks
- Chemical Facilities
- Active Shooter Prep
- COVID-19
- Emergency Comms ★
- Partnerships
- Tips & Alerts
- Hometown Security
- Risk Assessments
- Federal Facilities
- State / Local Support
- Infrastructure Facilities
- Cyber Hygiene
- Technical Assistance
- Regional Support
- School Safety

CISA is here to help



For more information:
www.cisa.gov

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

David M Nicol, PhD

Herman M. Dieckamp Endowed Chair in Engineering

University of Ilinois at Urbana-Champaign

Director, Critical Infrastructure Resilience Institute

Director, Information Trust Institute

Building a Legacy

CIRI Annual Meeting
December 2022

First some stats…

57

…the total number of projects executed (including those underway)

More stats…

22

…the total number of unique partners – academic + private sector

More stats…

71

…the total number of “product” outputs

- Data sets, models, prototypes, software

More stats…

55

…the total number of academic papers & publications

More stats…

13/25/70

…the total number of unique MSIs/MSI faculty/MSI students supported

- 12 Summer Research Teams
- 5 Scientific Leadership Awards

More stats…

> 100

…the total number of students *directly* engaged

Our main challenges

- Identify key research needed for infrastructure resilience
- Execute impactful research possible at scale of CoE
- Make results useable --- **distill complexity** so that user can benefit w/o expert training

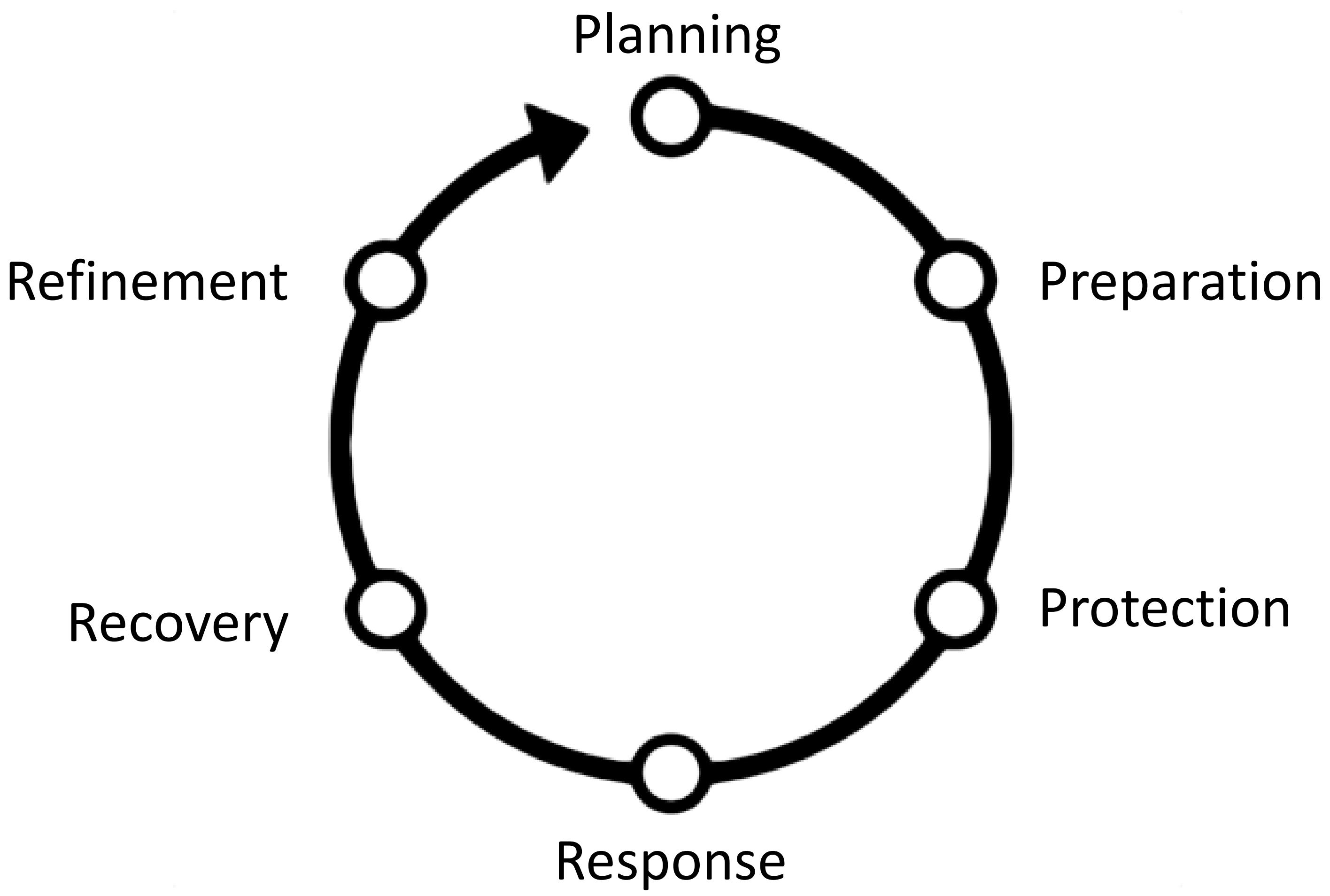
“We’re surrounded.
That simplifies our problem...”
- Col. Chesty Puller, USMC
(Battle of Chosin Reservoir)

CIRI has

Developed understanding of resiliency lifecycle

Applied each phase to efforts in

- Research
- Tech transition
- Education and Workforce Development



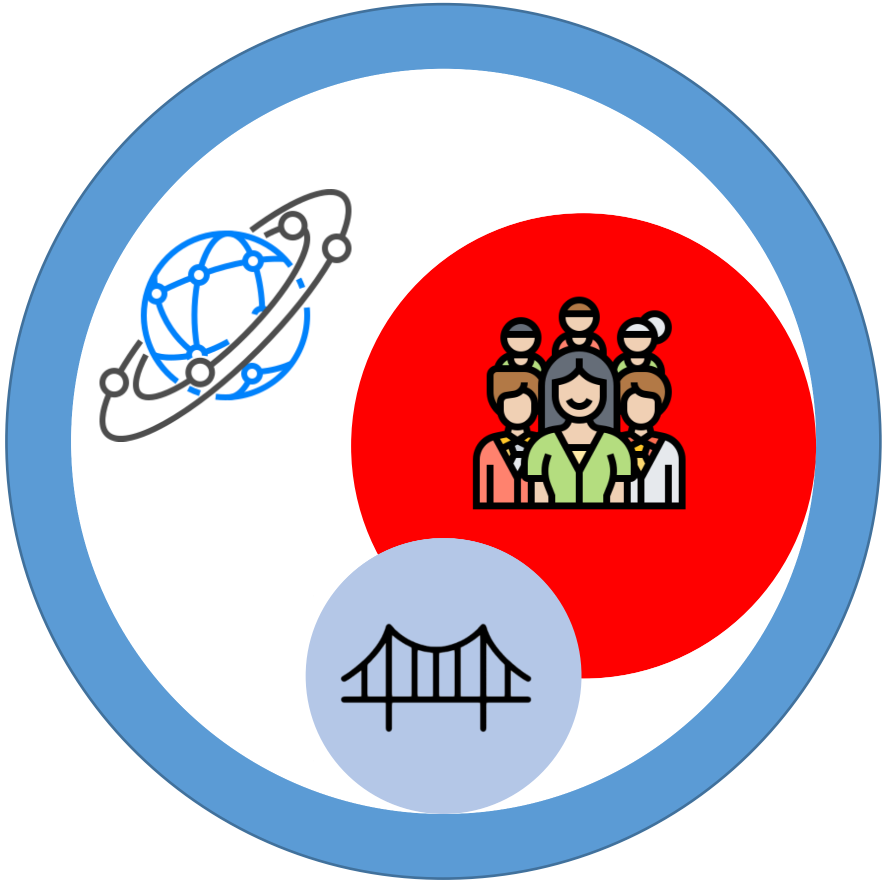
CIRI has

Developed a solid understanding of

- scope
- interconnectedness
- interdependence

of critical infrastructure

- physical, cyber, and human/social



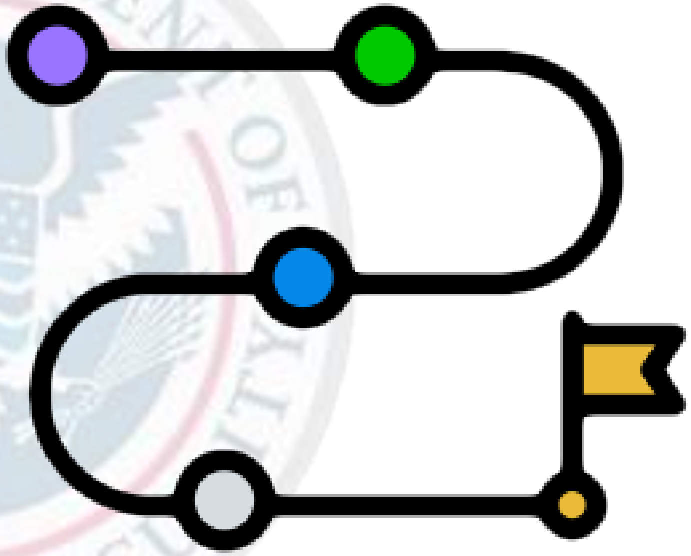
Examples

- Resilience Governance for Infrastructure Dependencies and Interdependencies; Flynn, NEU
- Identifying and Reducing Barriers to Infrastructure Insurance; Kunreuther, Wharton School, UPenn
- Regulatory Options for Managing Systemic Risks; Slayton, Cornell
- Scenario-based Flood Risk Mapping; Freitag, UW
- Community Resilience and Disaster Costs; McConkey, UIUC

CIRI has

Developed a solid understanding of the mission, strategic objectives, processes and culture of DHS

Appropriately mapped our research portfolio and technology development roadmap to DHS mission



Examples

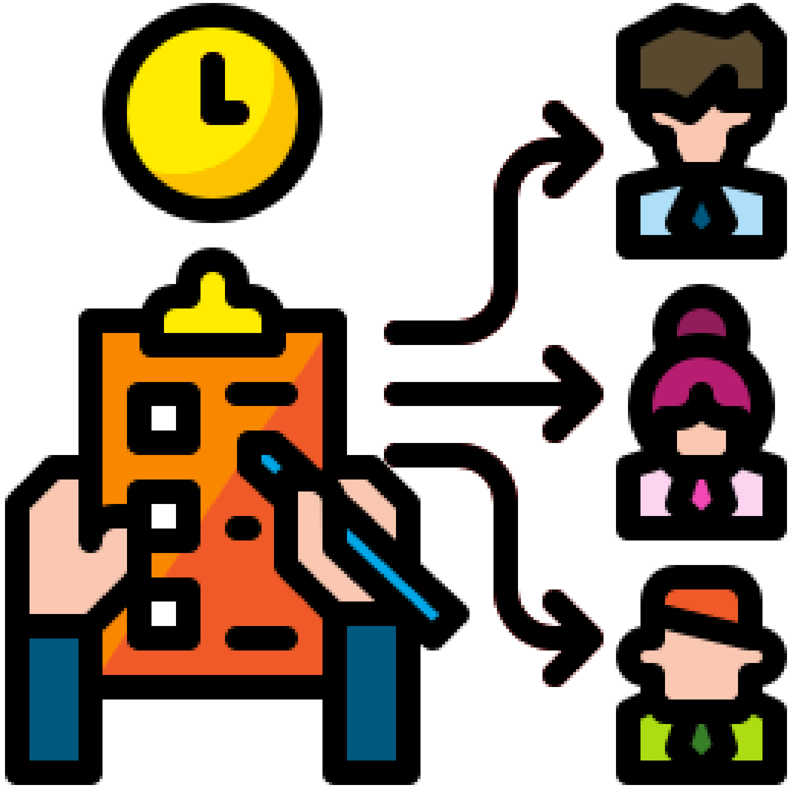
- Protecting the Nation’s 911 System from Cyber Attacks (UIUC, Karthik Consulting)
  - Researched requirements for PSAP cybersecurity
  - Developed & published NIST CSF-based PSAP Profile
  - Integrated Profile into Cyber Secure Dashboard
- NG911 Interoperability Testing (UIUC, TAMU)
  - Researched requirements for end-to-end testing of NG911 systems and components
  - Published recommendations for national interoperability testing framework
- Characterizing End-to-End Risks to 5G (GaTech)
  - Researched the end-to-end risks of 5G telecommunications infrastructure
  - How attacks on 5G can impact dependent infrastructure (i.e., connected autonomous vehicles)
  - Developed quantitative risk metrics

More Examples

- Safety & Security of Remote Bridge Operations (ABS Consulting)
  - Researched the cybersecurity risks to remote bridges
  - Developed & delivered Google Earth-based taxonomy of nations bridges
  - Developed & published NIST CSF-based Remote Bridges Profile
- Empirical Security Analysis of Wireless Emergency Alert System (Colorado Boulder)
  - Researched specific risk of spoofed message broadcast
  - Identified and tested mitigations to eliminate the risk
- EMP Risk Assessment & Mitigation (Synclesis, UIUC)
  - Researched EMP risk to 5G cell tower
  - Identifying mitigations to reduce risk

CIRI has

Demonstrated capability to successfully organize, scope, and manage multi-disciplinary, multi-institutional projects



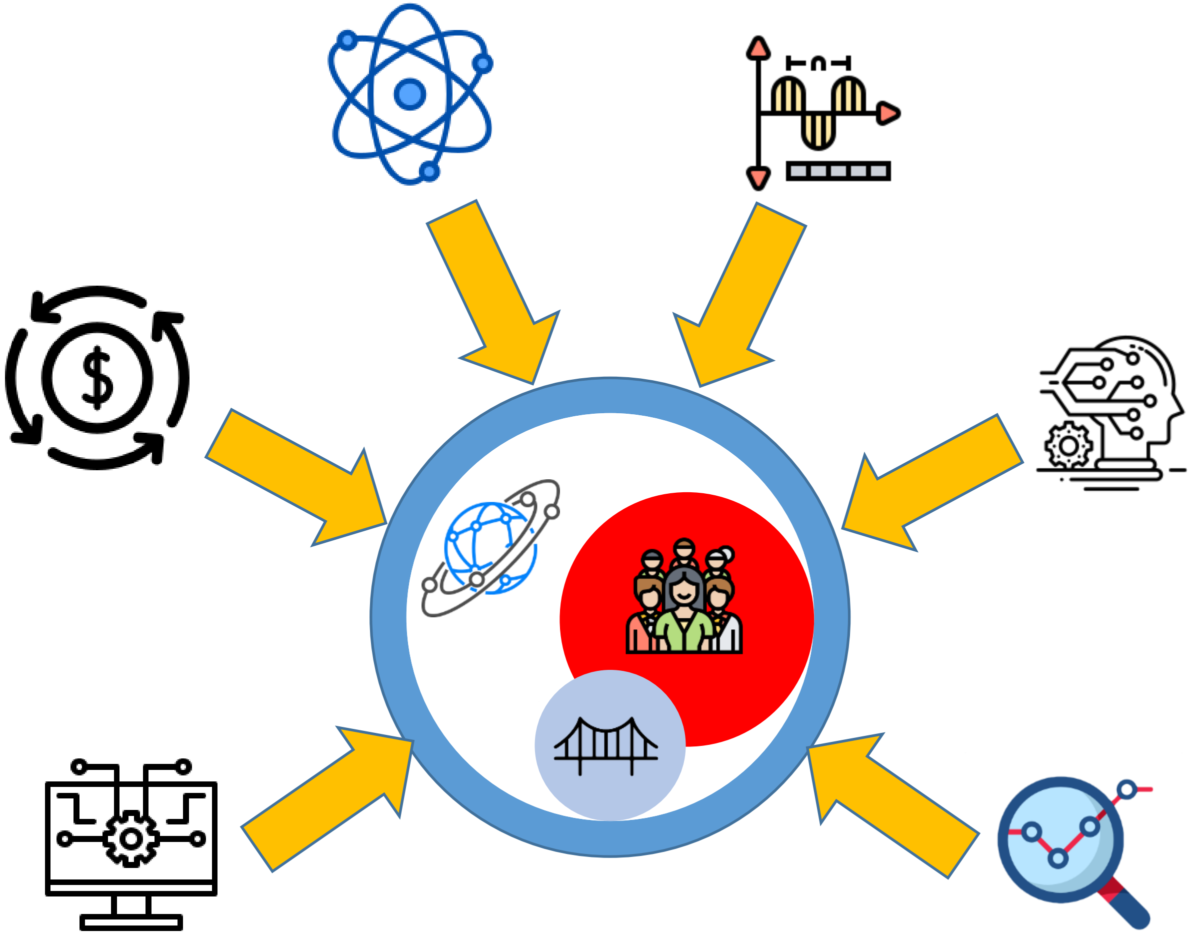
Examples

- Toward Community Resilience through Comprehensive Risk Assessment, USC, UIUC
- Hybrid Quantum-Classical Reinforcement Learning in Controlled Quantum Networks, UTenn, Ucalgary
- Leveraging AI for Disaster Response, USC, UIUC
- Interoperability Testing Program, Texas A&M, U. Washington, UIUC
- Multi-Layer Cyber-Physical Supply Chain Risk Analysis, NYU, U. Michigan
- Research and Deliverables on Utilizing an Academic Hub and Spoke Model for Education, UIUC, Purdue, U. Tulsa, Auburn Univ.
- Quantifying Interdependence of the Logical-Physical Internet Topologies, UIUC, UC San Diego
- Measuring Business and Economic Resilience in Disasters-Business Resilience Calculator, USC, Ohio State
- Cybersecurity Assurance for Critical Infrastructure, UCLA, Carleton Univ.
- Review and Assessment of the Usage of Computational Methods for Humanitarian Assistance and Disaster, UIUC, USC, Harvard

CIRI has

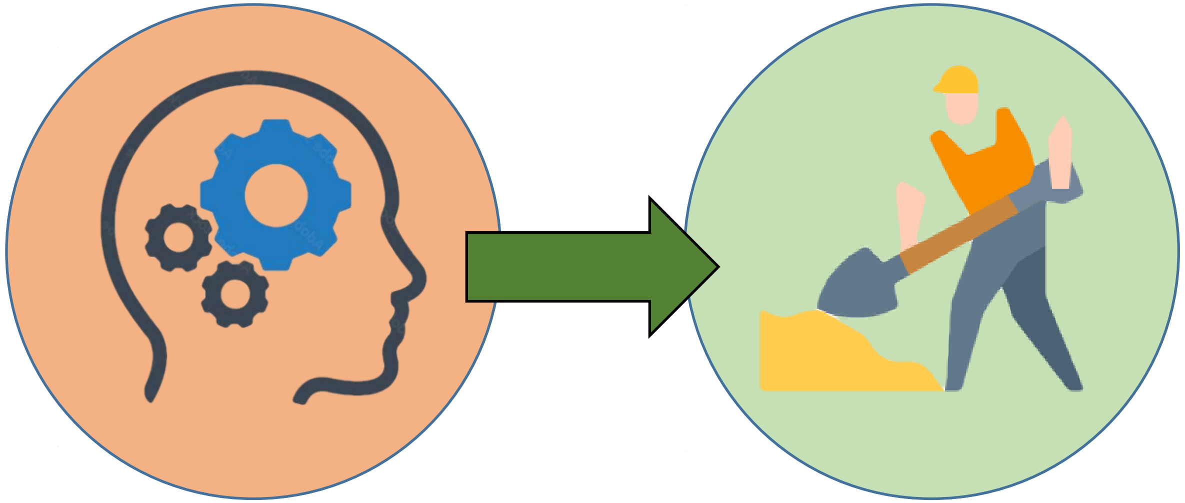
Brought cutting edge technologies to critical infrastructure resilience

- Software engineering
- Economics
- quantum information
- Electromagnetics
- Data analytics, AI, ML/DL
- Operations analysis



CIRI has

Demonstrated capability to transition research outputs to the field/market

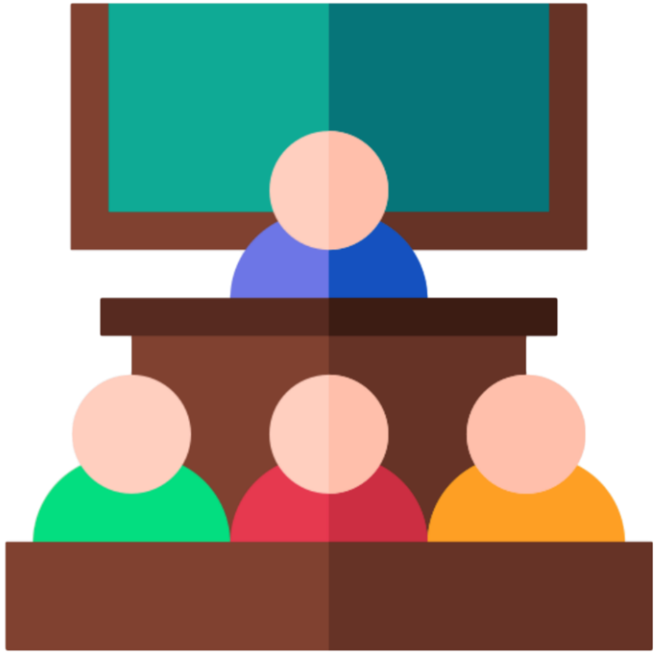


Sample Tech Transition Efforts

Project/Product	Status
CRISM (Cyber Risk Scoring & Mitigation)	Licensed to commercial company
Cyber Secure Dashboard	Pilot tests underway with PSAPs
Business Resilience Calculator	Completed RTI engagement Provisional Patent application filed Discussions with potential licensees underway
Port Disruptions Tool	Provisional Patent application filed NSF iCORPs completed RTI engagement completed HSSS engagement completed Discussions with potential licensees underway

CIRI has

Led significant efforts to enhance education and workforce development for the Homeland Enterprise



Examples

- Federal Law Enforcement Training Center (FLETC)
  - Researched requirements
  - Delivered recommendations for next-generation law enforcement education and training infrastructure
- Cybersecurity and Infrastructure Security Agency (CISA)
  - Completed research and developed requirements for a nationwide cybersecurity education and training network
  - Completed research and developed scalable cybersecurity curricula
    - 17 courses (credit-bearing and non-credit professional development)
    - 136 discreet training modules (“stackable”, for repurposing)
    - Cybersecurity fundamentals through advanced topics (ICS cybersecurity)

We’re looking forward to showing you examples of current accomplishments over the course of the next two days

Networking break

15-minutes

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Annual Meeting: Assessment and Measurement of Port Disruptions

Gabriel A. Weaver, Lavanya Marla
University of Illinois Urbana-Champaign

The Problem

Our nation’s economy and national security are highly dependent upon the Maritime Transportation System (MTS).

- *Nationally:* The MTS accounted for more than $4.6 trillion of economic activity (1/4 of US GDP in 2014, 2019).
- *Globally:* The MTS accounts for more than 80% of global merchandise trade in volume and 67% of its value.

To handle ever-increasing shipping volumes maritime ports have become highly automated

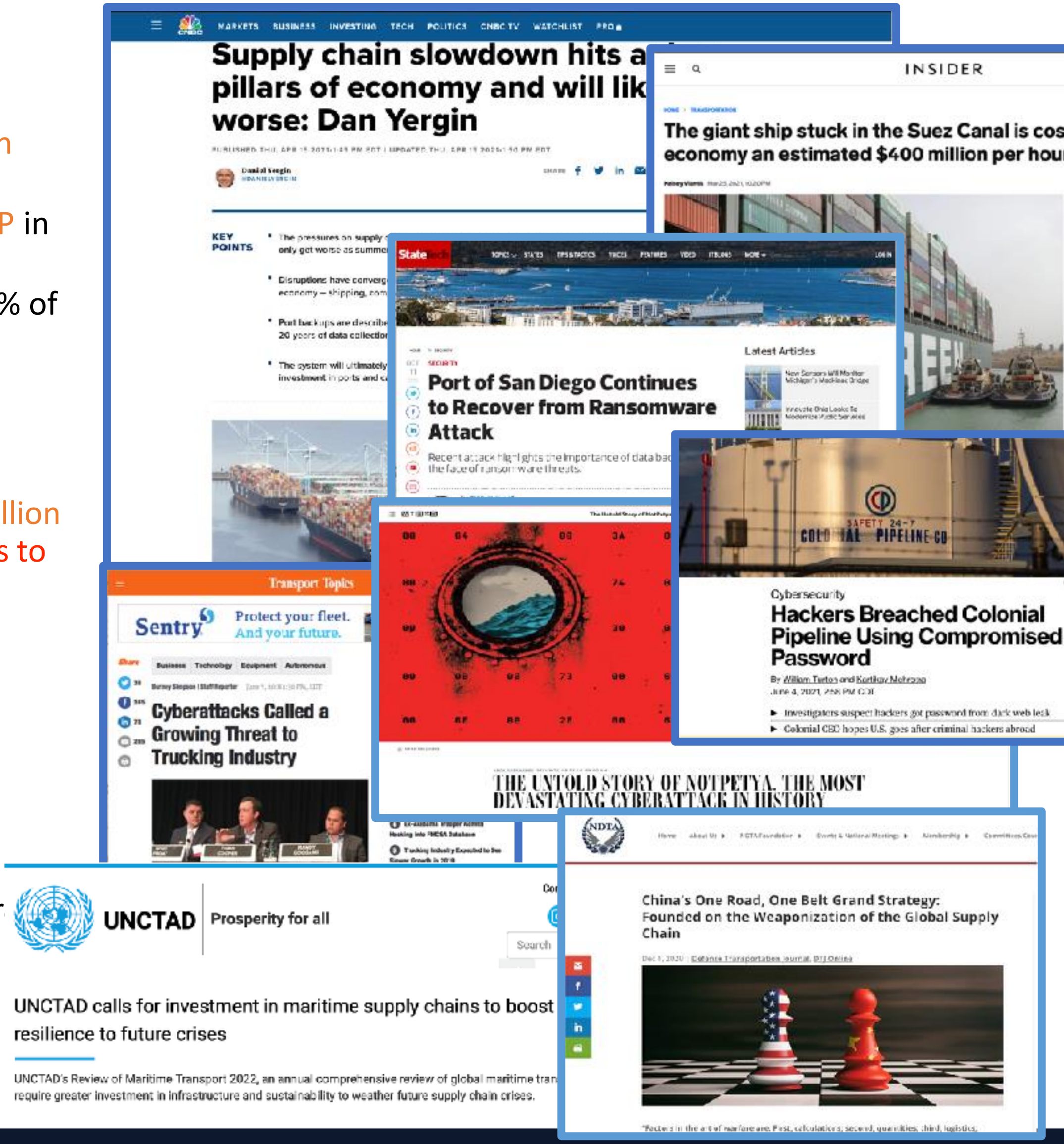
- Heavily reliant on information and communications technology
- “Between 2022 and 2027, the global smart ports market is projected to increase from $1.9 billion to $5.7 billion. Throughout this process the sector will need to attend to the associated threats to security in the use of IT.” [UNCTAD 2022]

Maritime ports are at risk of disruption from cyber attacks and natural disasters

- Superstorm Sandy
- NotPetya, etc.

<u>How to enhance the security and resilience of maritime ports?</u>

Our Contribution: The CIRI Port Disruptions Tool (PDT) enables data-informed decision making regar risk mitigation and management. Agile and resilient logistics.



Supply chain slowdown hits a pillars of economy and will lik worse: Dan Yergin

KEY POINTS

INSIDER

The giant ship stuck in the Suez Canal is cos economy an estimated $400 million per hou

StateTech

Port of San Diego Continues to Recover from Ransomware Attack

Latest Articles

Transport Topics

Sentry Protect your fleet. And your future.

Cyberattacks Called a Growing Threat to Trucking Industry

THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

UNCTAD | Prosperity for all

UNCTAD calls for investment in maritime supply chains to boost resilience to future crises

UNCTAD's Review of Maritime Transport 2022, an annual comprehensive review of global maritime tran require greater investment in infrastructure and sustainability to weather future supply chain crises.

NDTA

China's One Road, One Belt Grand Strategy: Founded on the Weaponization of the Global Supply Chain

Dec 1, 2020 | Defense Transportation Journal, DTJ Online

What Will Success Look Like?

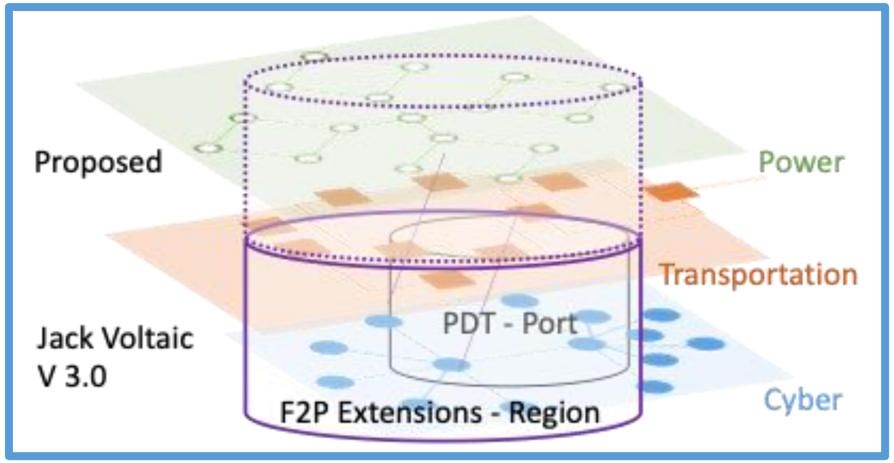
Via the Port Disruptions Tool (PDT), customers will:

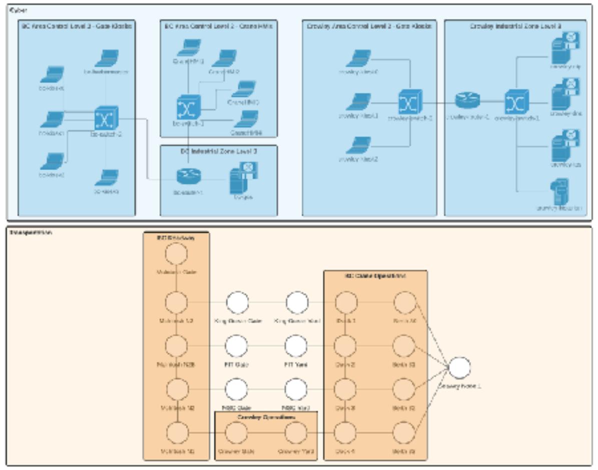
- Employ data-driven analyses to manage emerging risks and their relevance/impact within their specific operational contexts.
- Use those analyses to more efficiently plan and prioritize risk mitigation activities.
- Continually estimate seasonal, economic impacts of disruptions within the MTS.
- Proactively identify bottlenecks and single points of failure from adopting new technologies to drive efficiencies.
- Easily share data and analyses with other stakeholders in the intermodal ecosystem to coordinate mitigation and response.

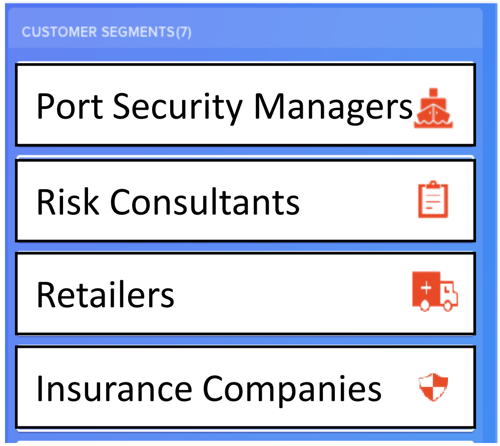
Year	Date	Event/ Article Title
2021	March	Suez Canal Obstruction
	July	"Supply-Chain Backlogs Turn Chicago into New Chokepoint" [Wall Street Journal]
	October	"America's Jammed-Up Ports Need Help" [Washington Post]
2022	July	"Record container ship traffic jam as backlog continues to build" [FreightWaves]
		"Russia strikes Ukraine's Black Sea port of Odesa hours after grain deals signed" [NPR]
		Cyber attacks on the Port of Los Angeles have doubled since pandemic [BBC]
	September	"Freight train worker strike could cause massive supply chain crisis as well as halt commuter trains" [CBS News]
	December	"Senate passes legislation to avert nationwide rail strike" [Axios]

Benefits to Users

- Enhanced, data-driven risk management for owners and operators of ports and shipping companies.
- Ability to quantify the risks and benefits of integrating emerging technologies into their long-term strategic planning.
- Re-prioritize infrastructure assets *continually* due to an evolving natural and adversarial landscape.
- Ability to quantify the financial impact of historically-attested disruptions within the context of their shipping ports or region.
- More efficient responses to local and regional disruptions to commodity flows.
- Reduced losses from disruptions when they do occur.






CUSTOMER SEGMENTS (7)

Port Security Managers

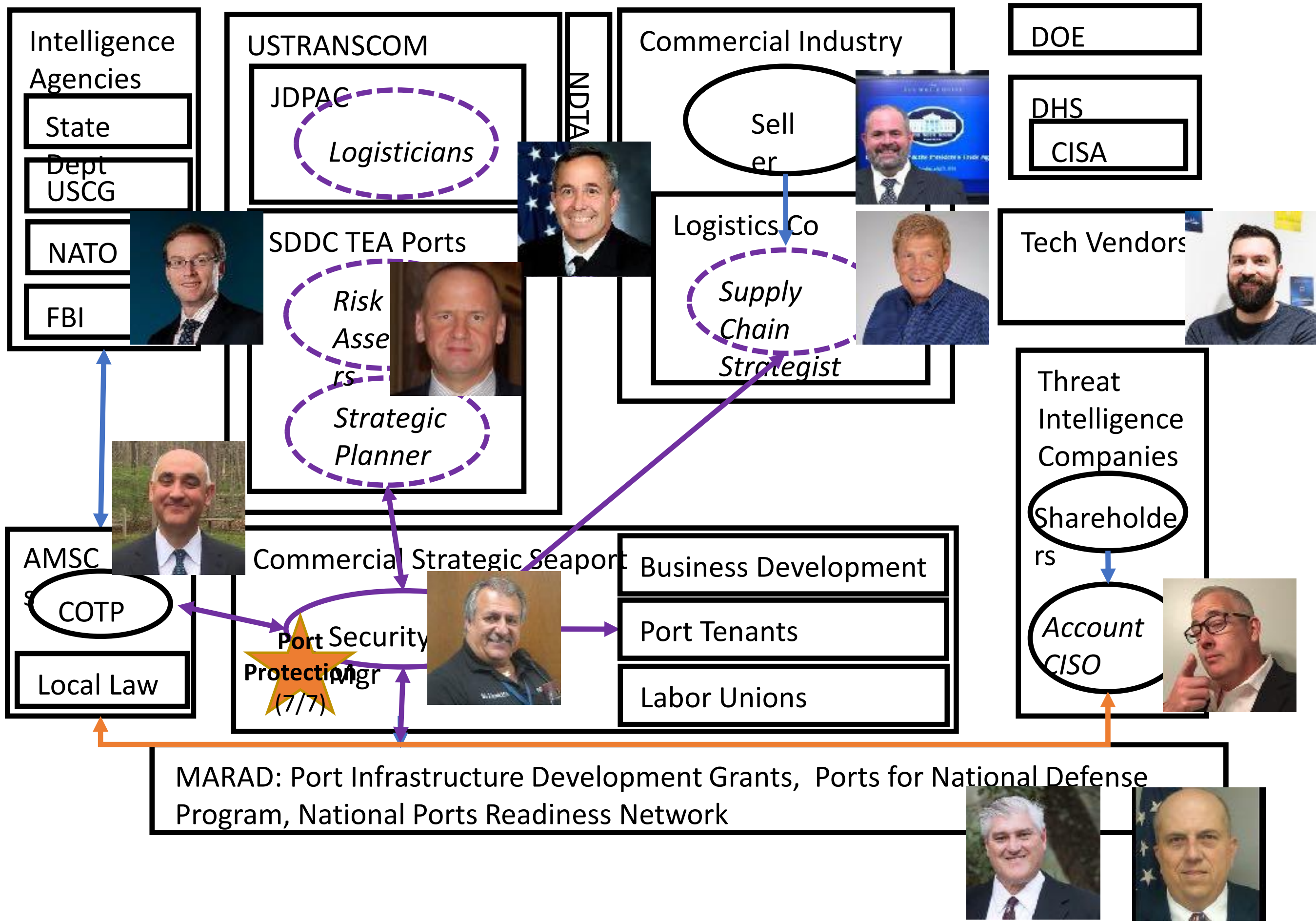
Risk Consultants

Retailers

Insurance Companies

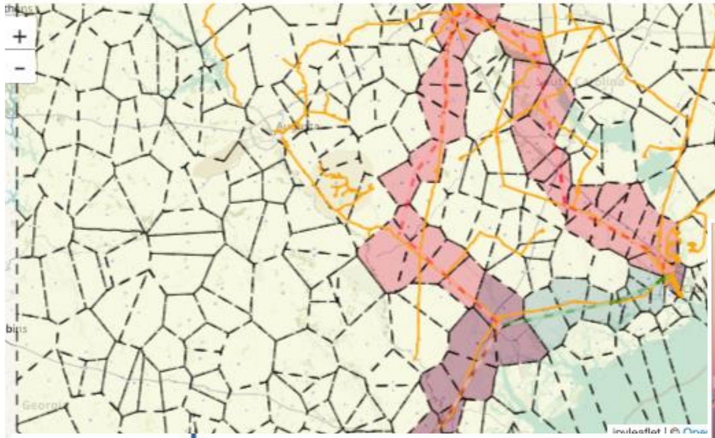
Benefits to HSE

- National Economy:
  - More efficient, more resilient maritime-dependent supply chains
  - Reduced economic losses from disruptions at maritime ports
- US Coast Guard
  - Assess a broader range of types of disruptions across the maritime stakeholder ecosystem, including cyber.
  - Prioritize potential targets relative to evolving threat intelligence that may exploit dependencies vital to critical functions.
  - Reduce the time spent by Port Security Analysts to model risk.
  - Data-driven approach to injects for Area Maritime Security Exercises, in particular the cybersecurity committee.
- National Defense and Security
  - More efficient, more resilient strategic maritime ports.
  - Integration of real-time data sources within the PDT can provide more timely, more accurate data to planners to better estimate evolving DoD capacity needs.
  - Improved readiness of strategic maritime ports to support force projection missions.



Technology Transition Accomplishments

- Fall 2020: Army Cyber Institute (ACI) Jack Voltaic v 3.0 Exercise Ports Table Exercise Coordinator and Fort to Port Analyses Report
- Spring 2021: Invited panelist to National Defense Transportation Association (NDTA) Surface Force Projection Conference.
- Summer 2021: National NSF I-Corps Summer Cohort Participant at NERIN (100 interviews). Invited panelist on DHS CoE Workshop on Suez Canal Incident.
- Fall 2021: Publications of PDT capabilities in WinterSim 2021, IEEE JCDL 2021, and Transportation Research, Part C. Invited speaker to NDTA Fall Meeting’s Transportation Academy. Invited panelist at Maritime Security Regimes Roundtable, NATO CoE.
- Winter 2021/22: RTI International Technology Screening
- Summer 2022: Homeland Security Startup Studio (HSSS) Cohort Participant and formation of Koru Ports
- Fall 2022: Invited Speaker to NDTA Fall Meeting’s Transportation Academy
- Winter 2022/23: Participant in British Telecom (BT) Regional Security Summit. UIUC Office of Technology Management (OTM) to resubmit Patent Application



Activities Remaining

- Continue to engage with customers and potential licensing partners to develop opportunities for CRADAs and funded pilots.
    - Improve usability via PDT Model Builder (Deliverable 1.1)
    - Address requirement gaps opportunistically with customer engagement to access data and work toward funded pilot (Deliverable 1.2)
- Entity formation to maintain and license PDT IP.

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

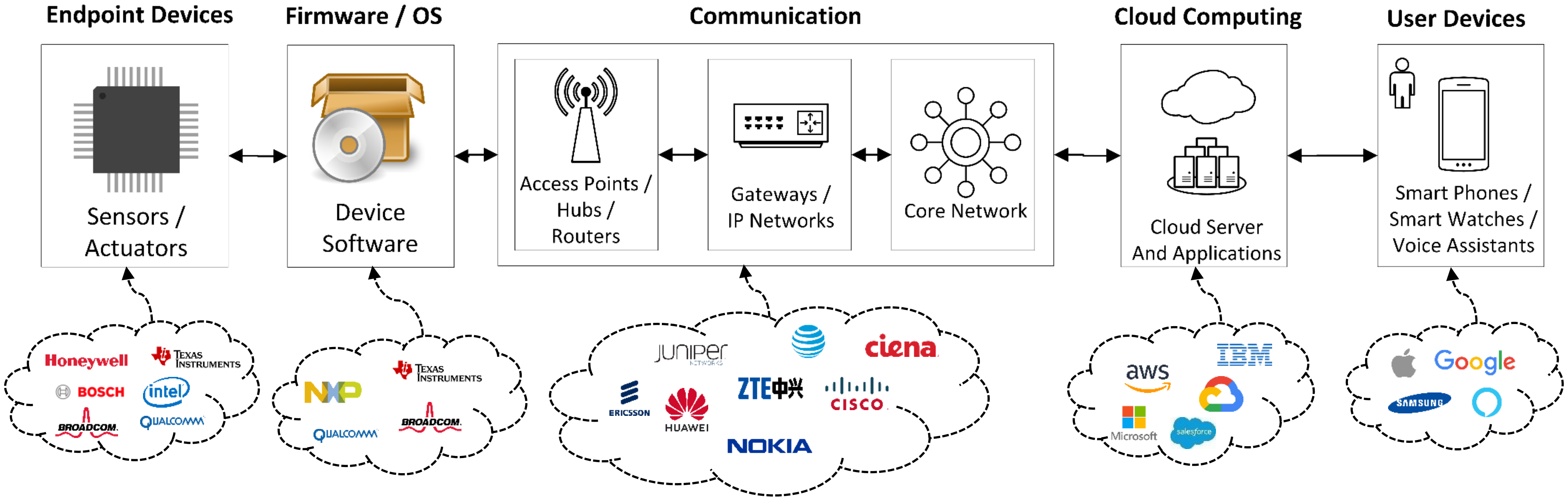
Annual Review: Multi-Layer Cyber-Physical Supply Chain Risk Analysis for Improving the Resilience of IoT-Enabled Critical Infrastructures

Junaid Farooq
University of Michigan
Dearborn, MI

Dec. 06, 2022
Arlington, VA

The Problem

- IoT / ICT systems comprise of an interconnection of multiple hardware and software components.
- Multiple entry points for vendor involvement in system safety and reliability.



Endpoint Devices

Sensors / Actuators

Firmware / OS

Device Software

Communication

Access Points / Hubs / Routers

Gateways / IP Networks

Core Network

Cloud Computing

Cloud Server And Applications

User Devices

Smart Phones / Smart Watches / Voice Assistants

- **DHS Component:** CISA NRMC
- **Challenge Area:** ICT Supply Chain Risk Management (SCRM)

The Problem

Challenge:

- Supply chain risk is non-linear
- Overall risk from the supply chain is convoluted
- Difficult to identify vendors that are most critical

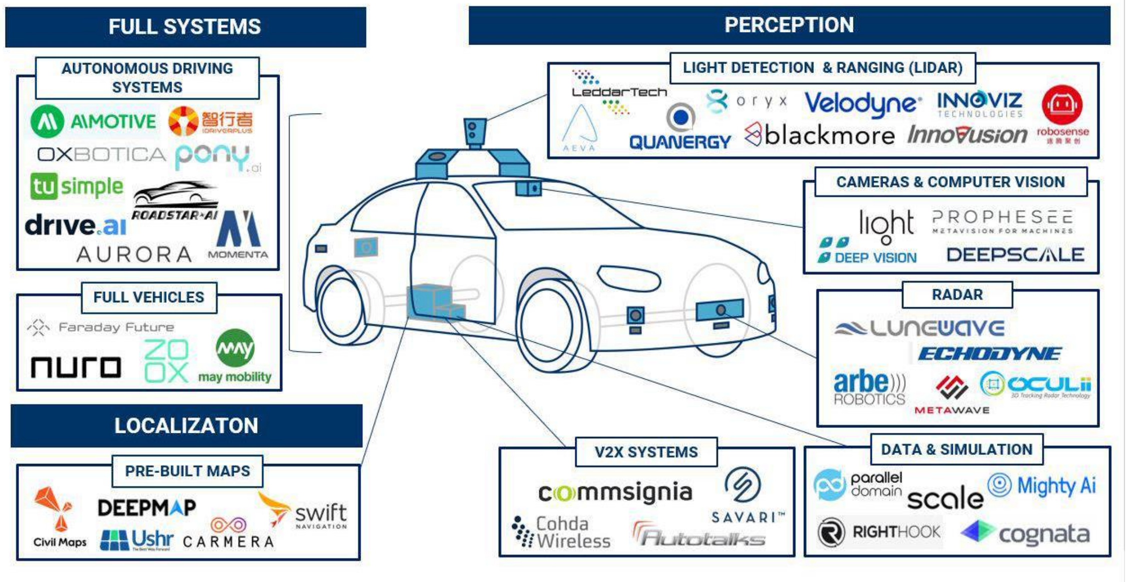
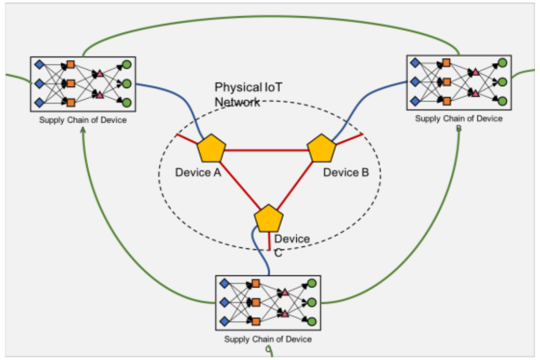
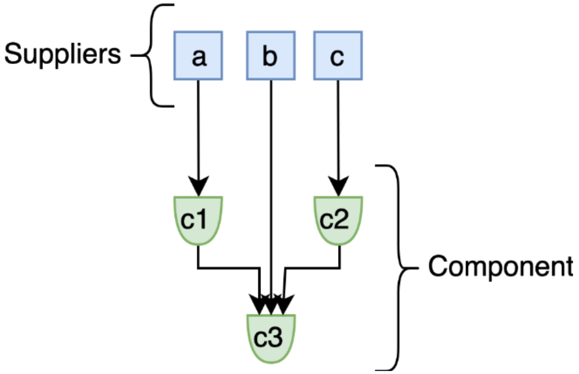


Figure: *Supply chain ecosystem for autonomous vehicles.*

Our Approach:

- Analyze systemic risk as opposed to vendor risk
- Consider a composition of the component network and supplier network
- Decision support for vendor selection, onboarding, and upgradation





What Will Success Look Like?

IoT Supply Chain Risk Analysis & Mitigation (iSCRAM) software tool can:

- Ingest a schematic of components, system interconnects, and vendors
- Assess vendors based on cybersecurity standards
- Provide a holistic understanding of system risk from the supply chain

Integrated Risk Assessment

Identify critical vendors and components

Risk Optimized Vendor Selection

What Will Success Look Like?

- Easy to use software tool that can be used by end users to make supply chain risk assessments

- Beta testing and commercial launch of the tool

- Metrics for Success:
  - Number of use cases / application scenarios
  - Testing and validation on actual customer data
  - Number of initial adopters

Benefits

Automotive Industrial Automation Communications Power Computing

Analyze Systemic Risk Posture

- Compute Systemic Risk Score and Rank Vendors / Components

Prioritize Security Resources

- Recommendations for Improvement of Vendor Risk

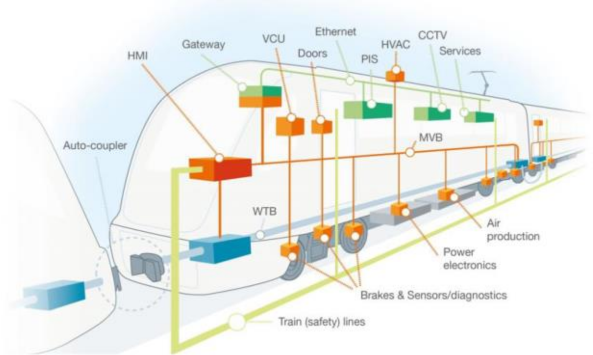
Enhanced Visibility of Supply Chain Risk

- Identify Vulnerabilities and track down risk sources

Benefits

Potential End-Users:

- **Mass Transit:** Ensuring that organizations such as MTA are aware of the risk by using equipment from third party vendors
- **Automotive Sector:** Understanding the risk in autonomous vehicles from supply chain actors
- **Cyber Insurance:** Decide insurance premiums and scrutinize vendors based on cyber risk of the supply chain



BATTERIES
Georgia: SAFT

PASSENGER SEAT
Indiana: Keil

AIR SUPPLY
Maryland: Mattei

BRAKES
Maryland: Knorr

HVAC CONTROLLER
Maryland: Lanka

BRAKING RESISTOR
New Jersey: Microelecttrica

HOSTLING PANEL
New York: Schaltbau

LOCKER PANELS BULKHEAD ACCESS PANELS
New York: Acro

PASSENGER & CAB INTERIOR LINERS, CEILING PANELS
New York: Frank Ralph

PLANK
New York: Frank Ralph

TRACTION MOTOR
New York: IEC Holden

TRUCK CASTING
New York: Strato
New York: Keokuk

COUPLER
North Carolina: Deiner

LINE REACTOR
Ohio: NorLake

TRACTION MOTOR
Ohio: Swiger

APSE
Pennsylvania: Meppi

BARRIER COVES, BARRIERS ACCESS PANELS
Pennsylvania: McClarin

BATTERY BOX
Pennsylvania: Bombardier

END CAP
Pennsylvania: McClarin

GEAR UNIT
Pennsylvania: Bombardier

MAIN KNIFE SWITCH
Pennsylvania: Bombardier

PROPULSION INVERTER UNIT
Pennsylvania: Bombardier

TCMS
Pennsylvania: Bombardier

TRUCK
Pennsylvania: Bombardier

VATC
Pennsylvania: Bombardier

WHEEL & AXLE
Pennsylvania: Penn Machine

CURRENT COLLECTOR
South Carolina: Wabtec

AIR SPRING
Tennessee: Firestone

SIDE WINDOWS
Tennessee: Dura

SLIDE WINDOWS
Tennessee: Dura

CAB HEATER
Texas: CCI Thermo Technologies

WINDSHIELD
Virginia: OSG

OPERATOR'S SEAT
Wisconsin: Seats Inc.

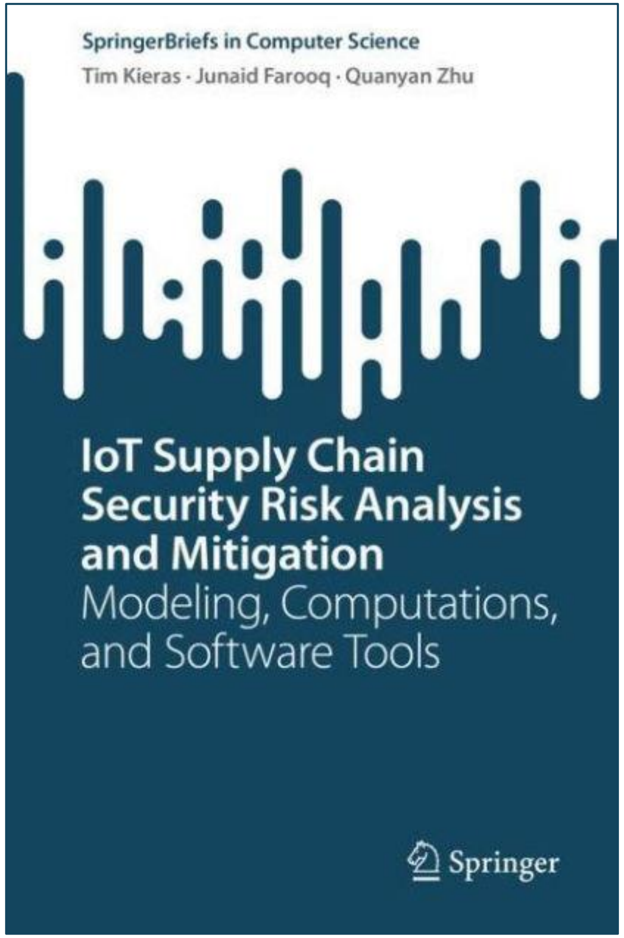
Supply chain of new Denver regional commuter rail

Source: Adapted from the paper J. Goikoetxea, "Shift2Rail CONNECTA: The Next Generation of the Train Control and Monitoring System", in Proceedings of 7th Transport Research Arena TRA 2018, April 16-19, 2018, Vienna, Austria

Figure: Components and vendors involved in a rail car of the mass transit system.

Accomplishments (Technical)

- Development of iSCRAM Backend and Frontend software
- Web Deployment and Access Management
- Publication and Dissemination
  - 3 research articles and 1 book
- Hands–on tutorial at IEEE MILCOM 2022



SpringerBriefs in Computer Science

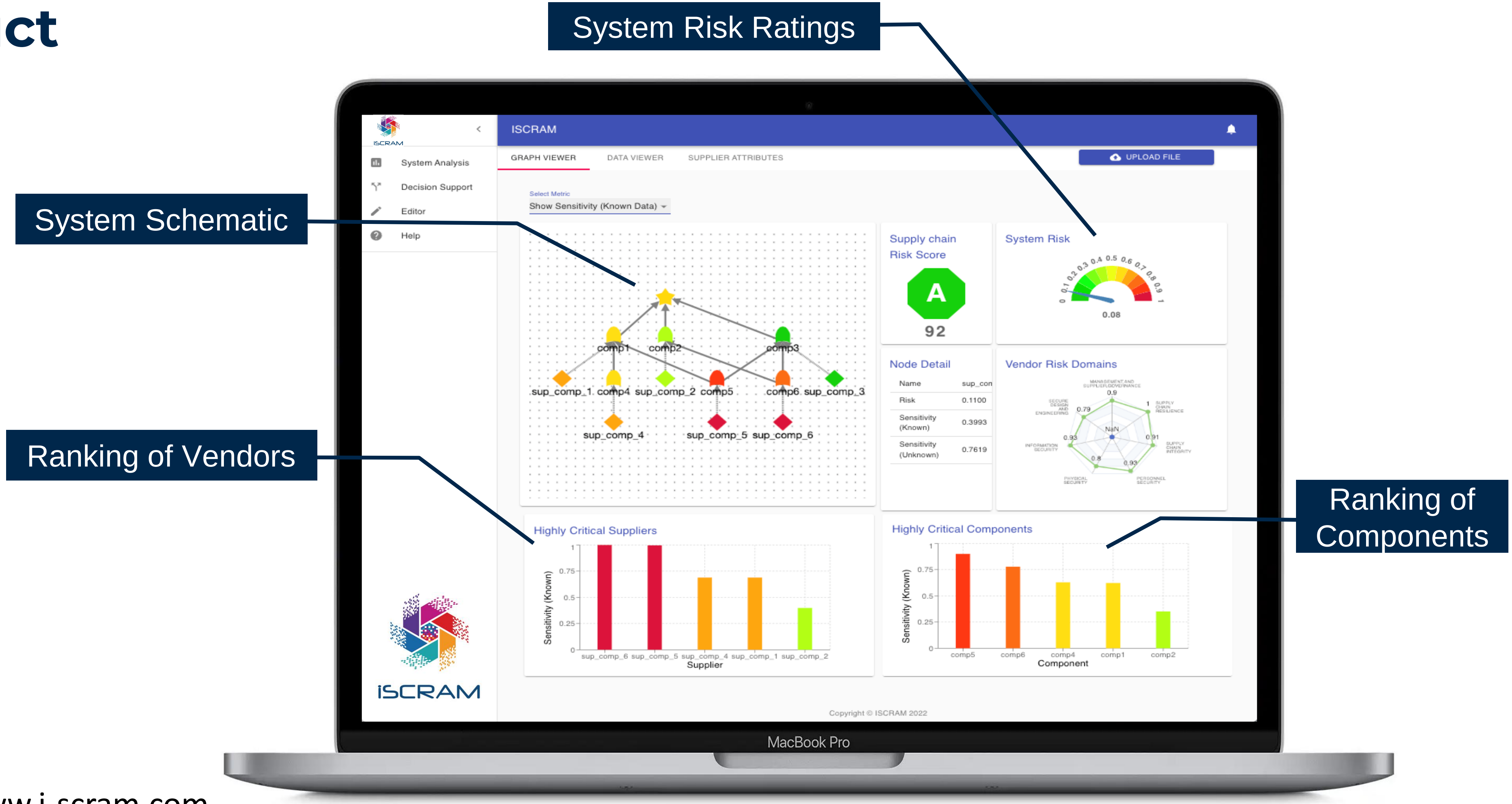
Tim Kieras · Junaid Farooq · Quanyan Zhu

IoT Supply Chain Security Risk Analysis and Mitigation

Modeling, Computations, and Software Tools

Springer

Product



System Risk Ratings

System Schematic

Ranking of Vendors

Ranking of Components

Node Detail

Name	sup_con
Risk	0.1100
Sensitivity (Known)	0.3993
Sensitivity (Unknown)	0.7619

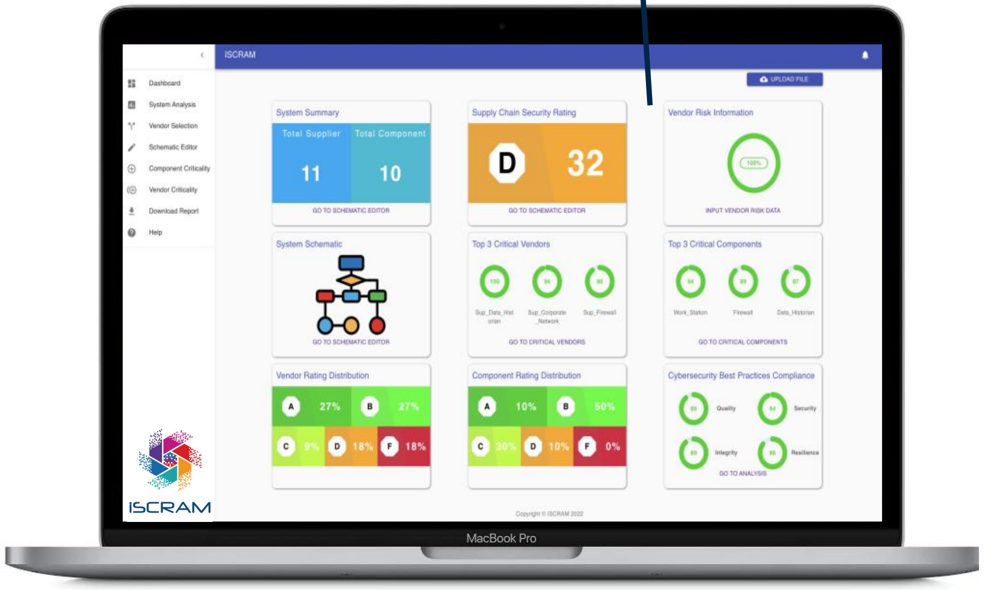
Copyright © ISCRAM 2022

Available: www.i-scram.com

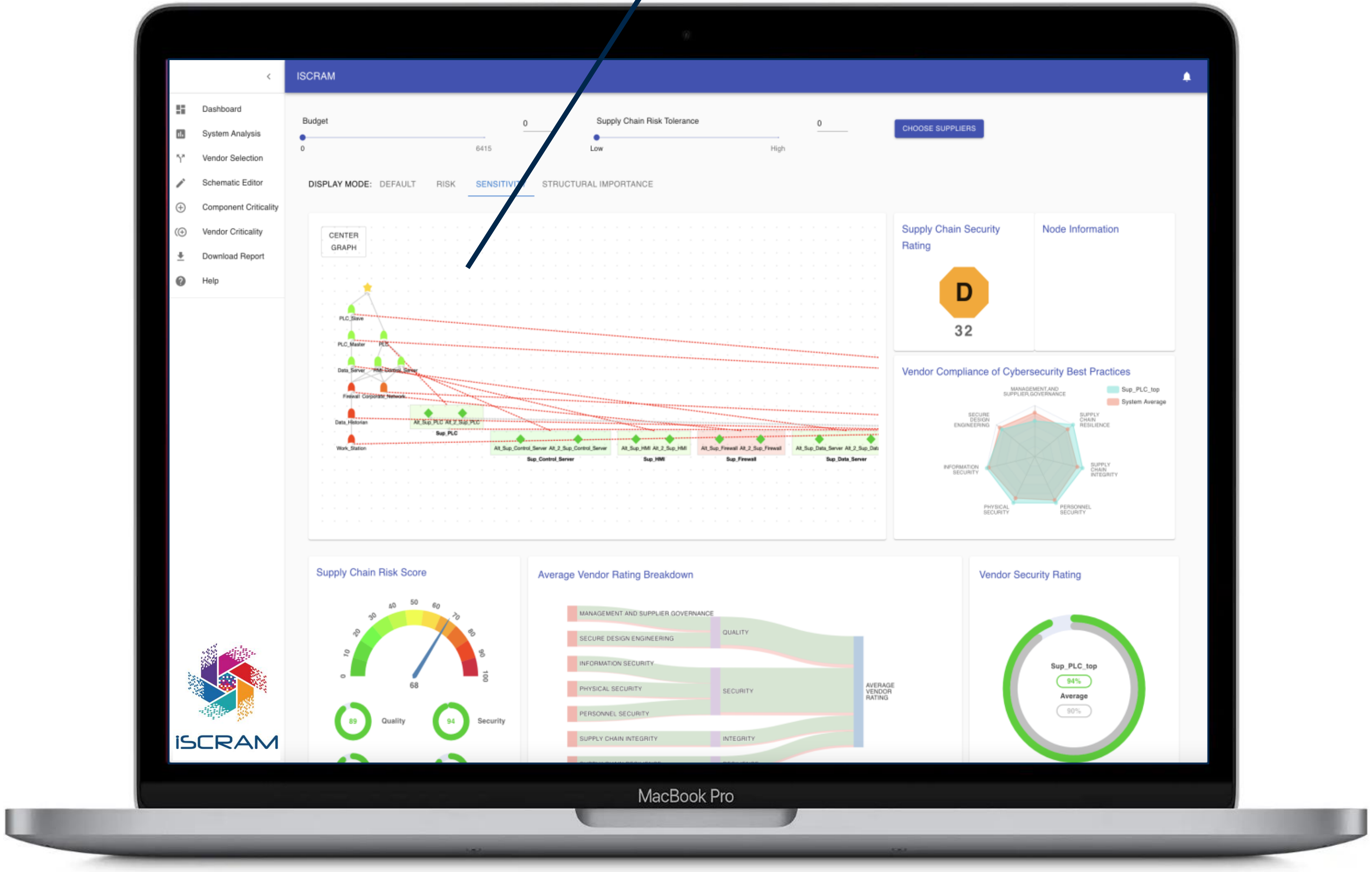
Product

Risk Summary and Statistics

Risk-Centric Vendor Selection



Main Dashboard



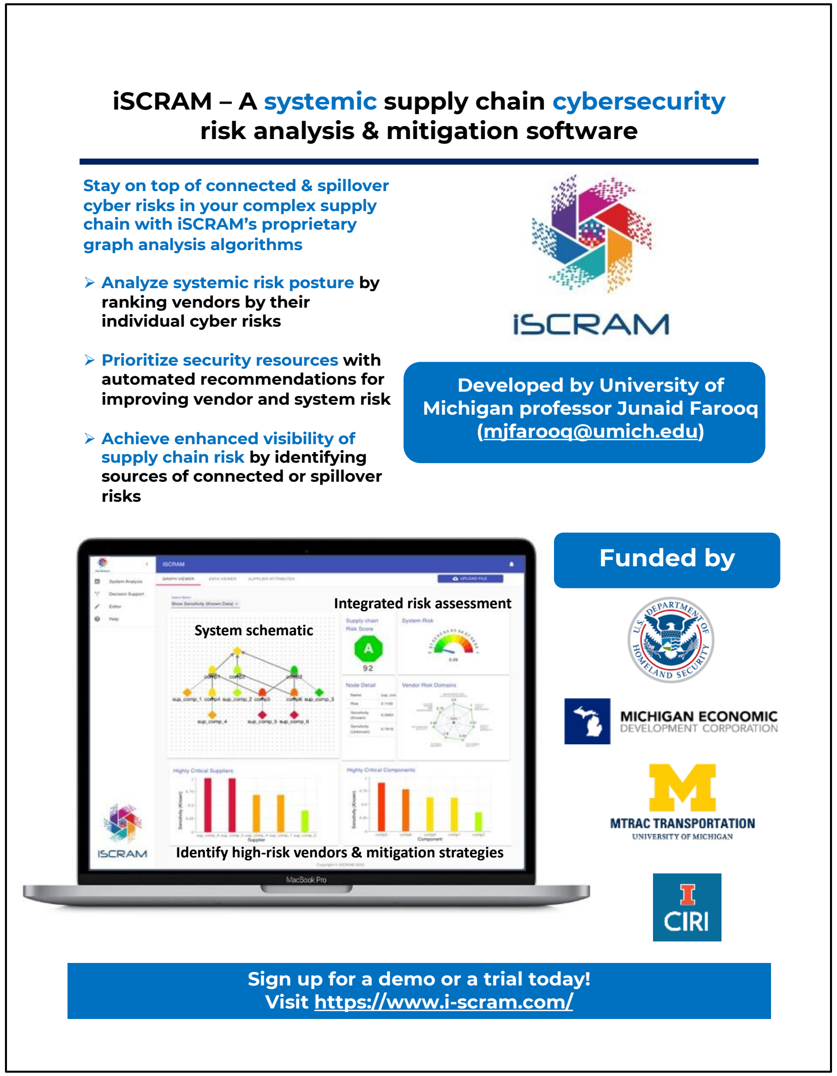
Vendor Selection

* Proprietary Copyright Software

Available: www.i-scram.com

Accomplishments (Commercial)

- Approx. 20 end-user interviews, 3 NDA signed
- Selected for DHS sponsored commercialization assessment through RTI Innovation Advisors
- Awarded MTRAC Advanced Transportation grant at University of Michigan funded by Michigan Economic Development Corporation
- Contacts Initiated with BlockHarbor Cybersecurity, Lear Corp., and Resilience Insurance



iSCRAM – A systemic supply chain cybersecurity risk analysis & mitigation software

Stay on top of connected & spillover cyber risks in your complex supply chain with iSCRAM's proprietary graph analysis algorithms

- Analyze systemic risk posture by ranking vendors by their individual cyber risks
- Prioritize security resources with automated recommendations for improving vendor and system risk
- Achieve enhanced visibility of supply chain risk by identifying sources of connected or spillover risks

Developed by University of Michigan professor Junaid Farooq (mjfarooq@umich.edu)

Integrated risk assessment

System schematic

Identify high-risk vendors & mitigation strategies

Funded by

Sign up for a demo or a trial today!
Visit https://www.i-scram.com/

Activities Remaining

- Beta Testing Partnership
  - NDAs have been signed
  - Testing and validation
- Licensing / Incorporation
- Sustainability: SBIR / STTR / Venture Capital

Thank You!

Contact: mjfarooq@umich.edu

Follow Us: www.i-scram.com

LUNCH BREAK
We will resume at 1:00 pm

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Annual Review:
Enhancing Water Distribution Networks Resilience with Scalable AI-based Planning

Bistra Dilkina

University of Southern California

The Problem

A water main break following a 6.0 earthquake in Napa, California.
https://www.cbsnews.com/pictures/strong-earthquake-knocks-napa-valley/17/

- In US, average age of a current water pipelines is **45 years old**; **C- on Infrastructure Report Card** from the American Society of Civil Engineers
- 143 million Americans live in areas vulnerable to earthquakes
  - Earthquakes disrupt critical infrastructures, and specifically water infrastructure.
  - Water Service Disruption compromises public access to water and reduces effectiveness of disaster response (fire departments, hospitals, disaster recovery centers)
- **Critical water customers**
  - hospitals, fire/police stations, emergency evacuation centers, power, sanitation, etc need resilient water supply to provide life-saving services during and post disasters.
- Relevant DHS Components: FEMA, USCG among others
- Proposed solution: data-driven AI-based decision support for water infrastructure mitigation planning to inform strategic infrastructure network fortification before the disaster strikes

AFP/GETTY IMAGES
Wellington is losing drinking water but it could take months to find and stop the leaks

Pipes in New Zealand's capital are leaking a million litres (220,000 gallons) of water a day as a result of the powerful November 2016 earthquake.

M 7.8 earthquake on San Andreas Fault, CA could cause **$24 billion in business interruption losses due to water supply interruption alone** (>13% of the total estimated costs)

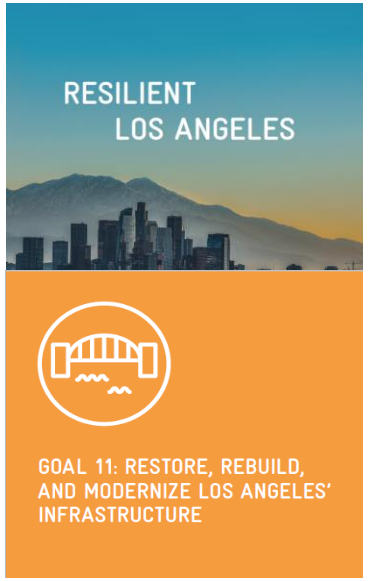
What Will Success Look Like?

L.A. Department of Water and Power workers install an earthquake-resistant water pipe in Northridge in January. DWP engineers estimate it will cost $15 billion to bolster water pipes throughout the city. (Gary Friedman / Los Angeles Times)

- Develop decision-support tool to strategically target infrastructure upgrades in water distribution networks
  - enable for the first time capability to **(automatically) generate** optimized service-zone-scale **master plans** for disaster-resilience mitigation planning
  - to meet the **resiliency requirements** of the local communities
  - **data-driven and cost-effective** by design
- **Modular, usable, robust software tool**
- Transition of our approach/tool to be **incorporated with existing data platforms and planning workflows used by a spectrum of end-users**

Benefits to end-users

- Los Angeles Department of Water and Power
  473 square miles, over 4 million residents, 733,900 active service connections
  - 23% of 2,742 critical customers at earthquake risk
  - 34% of 267,084 total pipes at earthquake risk
  - Pilot program using hand calculations – slow



RESILIENT
LOS ANGELES

GOAL 11: RESTORE, REBUILD, AND MODERNIZE LOS ANGELES' INFRASTRUCTURE

Action 61: Advance seismic safety, prioritizing the most vulnerable buildings, infrastructure, and systems

"**Expand Seismic Resilient Pipe Network** The City will expand development of the seismic resilient pipe network. … Resilient pipeline planning, design, and construction **requires the development of new informational tools and mapping of geohazards** …."

- Provide owners and operators of water infrastructure with data-driven hazard assessment and cost-effective planning tool
  - **Hazard assessment**: in addition to pipes, which critical customers are at risk?
  - **Automated planning**: coordinated upgrades across the network wrt joint needs and costs
  - **Faster speed** at developing mitigation plans
  - Ability to plan on a **larger scale** (thousands of pipes, 10s of sq miles)
  - More **cost-effective** plans by using algorithms to search for optimal upgrades
  - Agility to **re-calculate, re-optimize, what-if analysis**

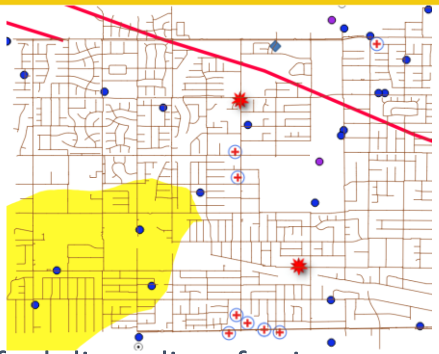
LA
DWP

Benefits to DHS

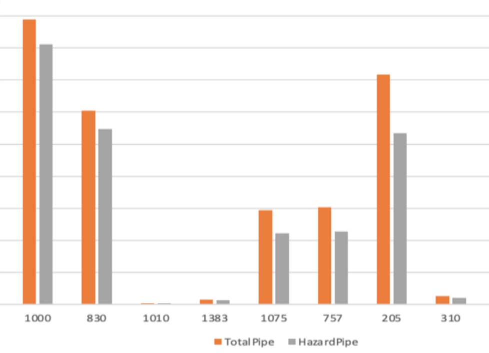
- Enhances the ability of local and state decision makers across the nation to perform mitigation planning
  - Enhances resilience by minimizing likely disaster disruptions
- Ways to show cost-effectiveness of planning – FEMA grant applications
- Help Disaster Response
  - Services critical to disaster response (hospitals, evacuation centers, fire/police departments) less likely to be compromised by water disruption
- Public Health and Damages
  - minimizes risks to public health and property damage (fire, water) through increased availability of water during earthquakes

Accomplishments

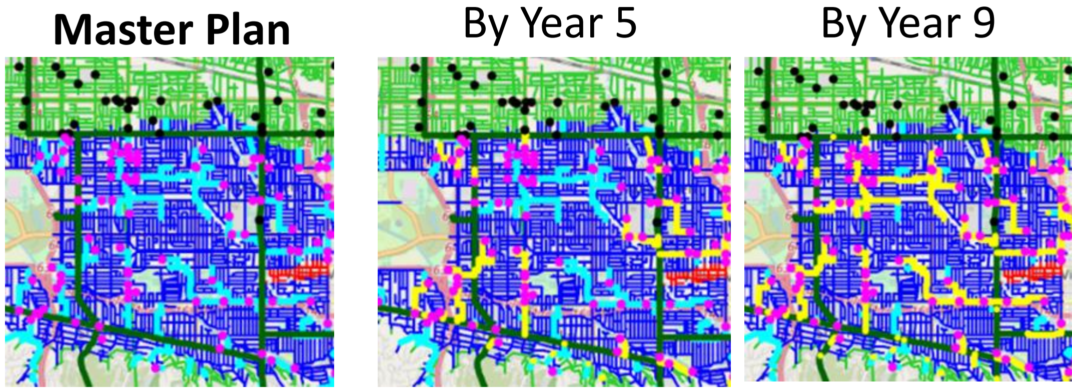
- **Flexible tool to aid in resiliency planning**
  - Highly parametrized: definition of hazards, costs, resilience needs
- **Map risk exposure:** hazard, infrastructure and customers
- **Master Plan**
  - Identify set of pipes that minimize costs to meet all resilience requirements
  - Showed NP-hard, developed **Mathematical Model**
  - **6%-23% more cost effective than baseline approach**
  - Scales to 1-3 service zones at a time
- **Sequential Planning** subject to yearly budget
  - Year by year pipes to be replaced that maximize resilience benefits as early as possible
  - **Dynamic Programming approach (optimal)**
  - **Cost benefit analysis** with various replacement budgets (miles/year) to quantify opportunity cost
- **Stakeholder engagement and requirement elicitation**
  - Los Angeles DWP, Seattle Public Utilities, East Bay Municipal Utility District (EBMUD)
  - Metropolitan Water District of Southern California, FEMA IX
  - C A Davis Engineering, Kubota Membrane USA
- **RTI Screening assessment completed**



fault lines, liquefaction zones, pipes and critical customers

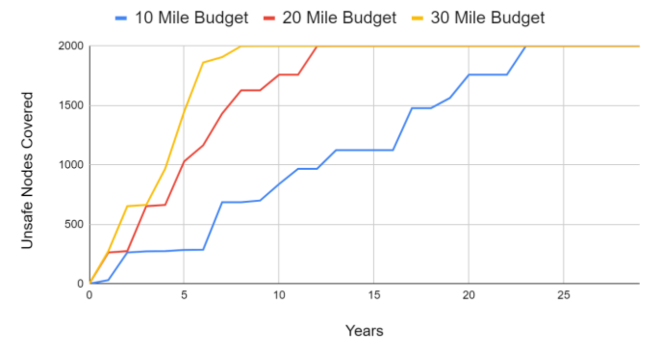


Pipes at risk in each service zone



- 🟩 Trunk line
- 🟩 Non-hazarded pipe
- 🟥 Pipe in fault zones
- 🟦 Pipe in lique areas
- 🟦 Pipes to be upgraded
- 🟨 Pipes already upgraded
- 🟪 Disconnected customer
- ⬛ Non-hazarded Customer

Unsafe Node Coverage under Various Budget Scenarios



Activities Remaining

- **Package** into a standalone tool with robust error checking, compatibility and documentation – improve usability
- **Pilot in-house training** and usage at LADWP with 5-10 engineers on site
- Address **requirements gaps** and design based on pilot feedback
- Continue to **engage with customers** and potential partners
- Explore pathways forward (funding, piloting, IP)

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

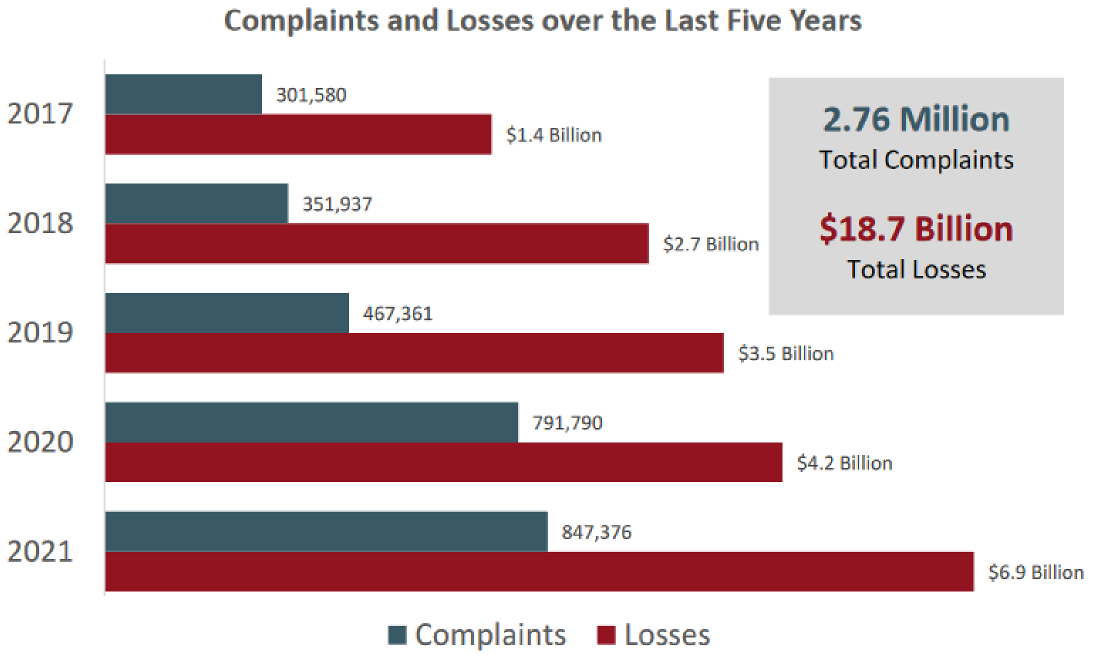
Technology Transition Project: Cyber Secure Dashboard

Glen Salo

Heartland Science and Technology Group

The Problem

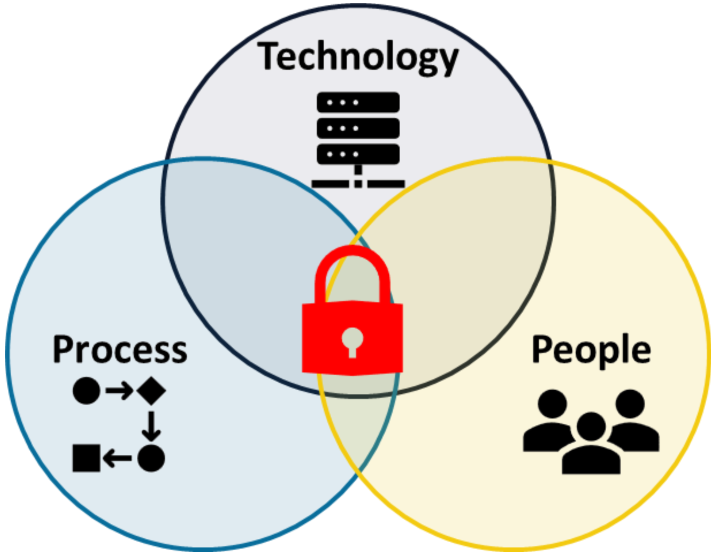
- The prevailing cyber risk management processes (in government and the private sector) are inconsistent, opaque, and insufficient
- The prevailing practices…
  - Impede our progress towards enhancing the security and resilience of our critical infrastructure
  - Lead to continued year-over-year financial losses
  - Are inadequate to address national security threats by nation-state actors



Federal Bureau of Investigation Internet Crime Report 2021

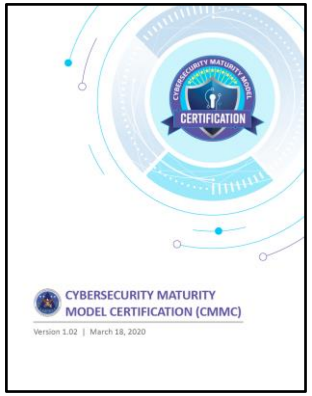
The Solution

- Technology solutions are necessary but insufficient
- Increased emphasis on people and process is required
- **Solution**: A standards-based assessment, monitoring, management, and reporting tool
- DHS Components: CISA, TSA, USCG



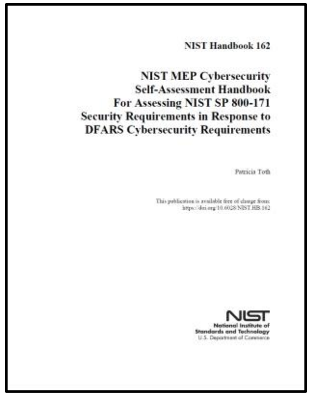
What Will Success Look Like?

- Owners and operators of critical infrastructure will adopt and conform to national **cybersecurity standards**, processes, and best practices
  - DHS (CISA) Cyber Security Performance Goals, NIST CSF, the DoD CMMC, …
- **Standardized assessment methodologies** will measure conformance
  - NIST SP 800-171A, NIST SP 800-53A, NIST 162 Handbook, etc.



CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Version 1.02 | March 18, 2020



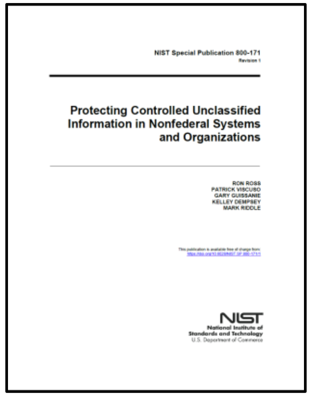
NIST Handbook 162

NIST MEP Cybersecurity
Self-Assessment Handbook
For Assessing NIST SP 800-171
Security Requirements in Response to
DFARS Cybersecurity Requirements

Patricia Toth

This publication is available free of charge from:
https://doi.org/10.6028/NIST.HB.162

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



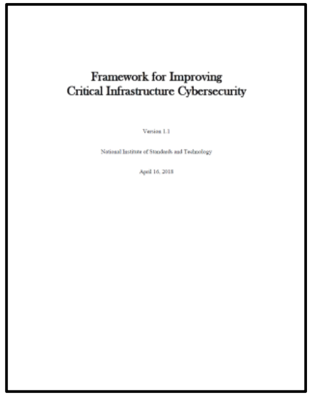
NIST Special Publication 800-171
Revision 1

Protecting Controlled Unclassified
Information in Nonfederal Systems
and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r1

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

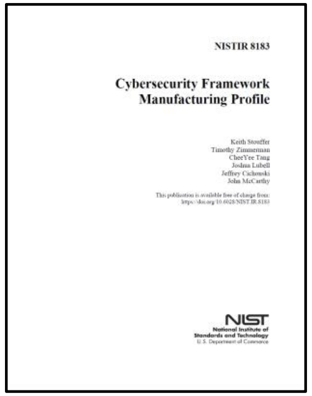


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018



NISTIR 8183

Cybersecurity Framework
Manufacturing Profile

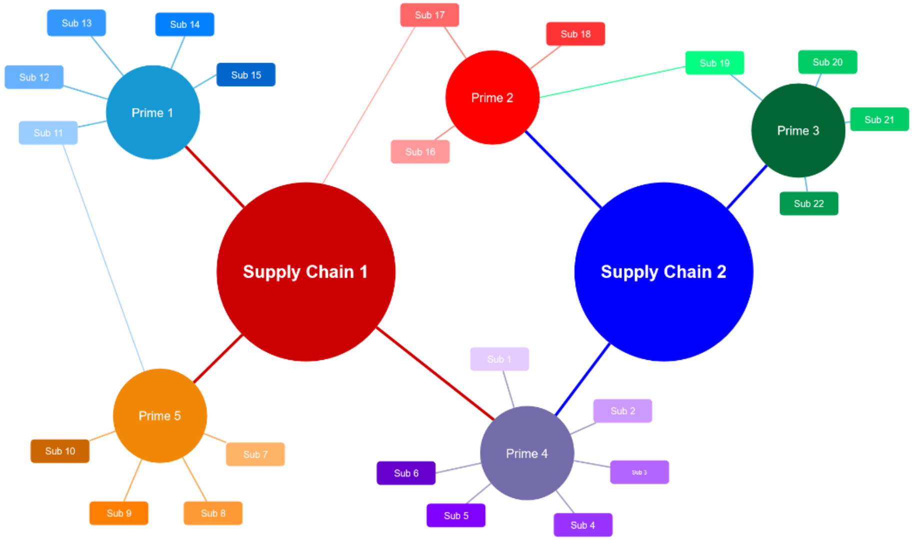
Keith Stouffer
Timothy Zimmerman
CheeYee Tang
Joshua Lubell
Jeffrey Cichonski
John McCarthy

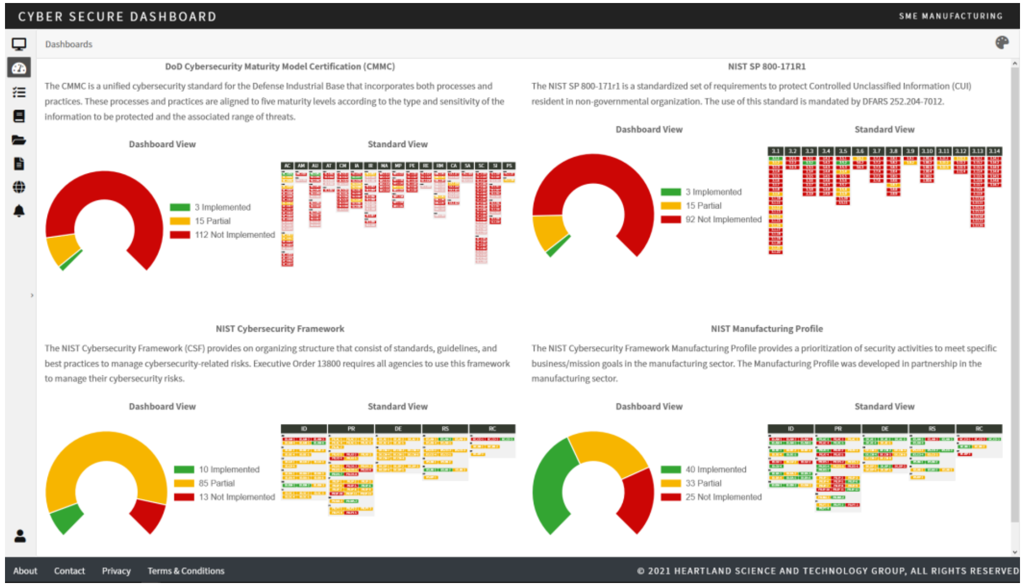
This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

What Will Success Look Like (cont’d)?

- Conformance will be measured for individual organization and entire supply chains
- Continuous improvement will be facilitated, monitored, reported




CYBER SECURE DASHBOARD

SME MANUFACTURING

Dashboards

DoD Cybersecurity Maturity Model Certification (CMMC)

The CMMC is a unified cybersecurity standard for the Defense Industrial Base that incorporates both processes and practices. These processes and practices are aligned to five maturity levels according to the type and sensitivity of the information to be protected and the associated range of threats.

Dashboard View

- 🟩 3 Implemented
- 🟨 15 Partial
- 🟥 112 Not Implemented

Standard View

NIST SP 800-171R1

The NIST SP 800-171r1 is a standardized set of requirements to protect Controlled Unclassified Information (CUI) resident in non-governmental organization. The use of this standard is mandated by DFARS 252.204-7012.

Dashboard View

- 🟩 3 Implemented
- 🟨 15 Partial
- 🟥 92 Not Implemented

Standard View

NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) provides on organizing structure that consist of standards, guidelines, and best practices to manage cybersecurity-related risks. Executive Order 13800 requires all agencies to use this framework to manage their cybersecurity risks.

Dashboard View

- 🟩 10 Implemented
- 🟨 85 Partial
- 🟥 13 Not Implemented

Standard View

NIST Manufacturing Profile

The NIST Cybersecurity Framework Manufacturing Profile provides a prioritization of security activities to meet specific business/mission goals in the manufacturing sector. The Manufacturing Profile was developed in partnership in the manufacturing sector.

Dashboard View

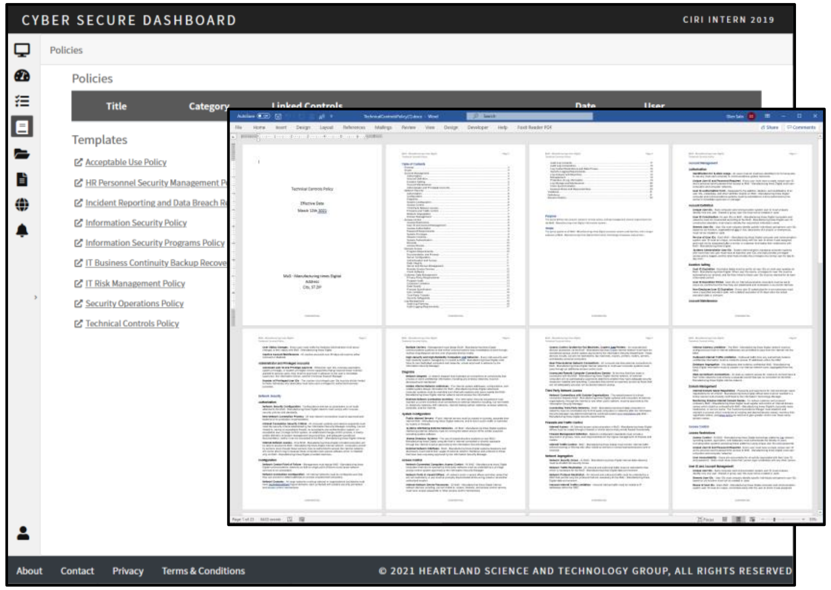
- 🟩 40 Implemented
- 🟨 33 Partial
- 🟥 25 Not Implemented

Standard View

© 2021 HEARTLAND SCIENCE AND TECHNOLOGY GROUP, ALL RIGHTS RESERVED

Benefits (to the user)

- Eases, accelerates, **lowers cost** of conformance to national standards
- **Operationalizes** standardized cyber management processes/practices
- **Harmonizes** internal and external (out-sourced) cybersecurity activities
- **Continuous visibility** of progress toward target posture
- Eases internal/external **stakeholder reporting**
- Supports individual organization and extended **supply chains**



CYBER SECURE DASHBOARD

CIRI INTERN 2019

Policies

Policies

Title	Category	Linked Controls	Date	User

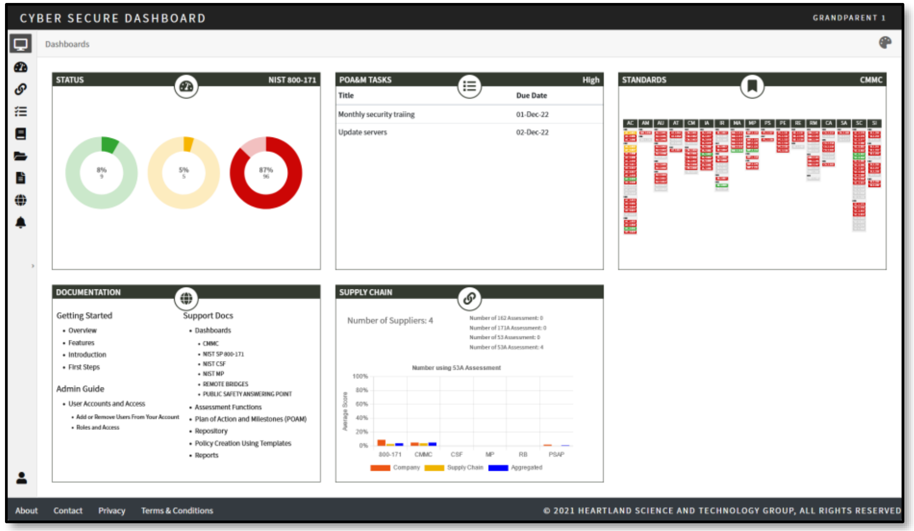
Templates

- Acceptable Use Policy
- HR Personnel Security Management P
- Incident Reporting and Data Breach R
- Information Security Policy
- Information Security Programs Policy
- IT Business Continuity Backup Recove
- IT Risk Management Policy
- Security Operations Policy
- Technical Controls Policy

© 2021 HEARTLAND SCIENCE AND TECHNOLOGY GROUP, ALL RIGHTS RESERVED

Benefits (to homeland security enterprise)

- Facilitates **broad-scale adoption** of national standards & best practices
- Provides **common metrics/criteria** for assessing & reporting progress
- Provides a **common language/lexicon** for all stakeholders
- Facilitates **sound governance** and **policy** implementation



CYBER SECURE DASHBOARD

GRANDPARENT 1

Dashboards

STATUS — NIST 800-171

POA&M TASKS — High

Title	Due Date
Monthly security traiing	01-Dec-22
Update servers	02-Dec-22

STANDARDS — CMMC

DOCUMENTATION

Getting Started

- Overview
- Features
- Introduction
- First Steps

Admin Guide

- User Accounts and Access
  - Add or Remove Users From Your Account
  - Roles and Access

Support Docs

- Dashboards
  - CMMC
  - NIST SP 800-171
  - NIST CSF
  - NIST MP
  - REMOTE BRIDGES
  - PUBLIC SAFETY ANSWERING POINT
- Assessment Functions
- Plan of Action and Milestones (POAM)
- Repository
- Policy Creation Using Templates
- Reports

SUPPLY CHAIN

Number of Suppliers: 4

Number of 162 Assessment: 0
Number of 171A Assessment: 0
Number of 53 Assessment: 0
Number of 53A Assessment: 4

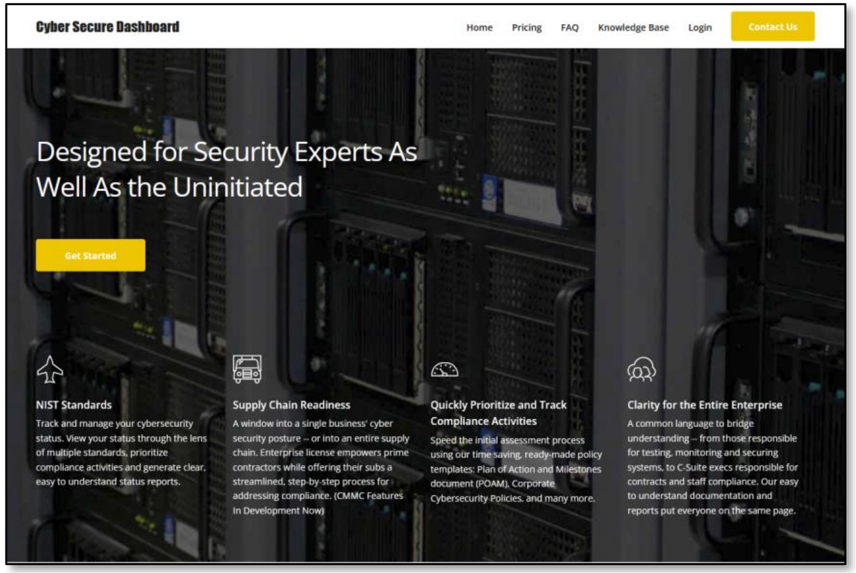
About Contact Privacy Terms & Conditions

© 2021 HEARTLAND SCIENCE AND TECHNOLOGY GROUP, ALL RIGHTS RESERVED

- Facilitates “ripple effect” as standards are enhanced/updated
- **Enhances the security and resilience** of our critical infrastructure

Accomplishments

- Software developed, tested, and available as a **SaaS offering**
  - Learn-by-doing, policies, standards-based assessment, monitoring
  - Plan of Action & Milestones (cybersecurity task management/harmonization)
  - Provides a pathway for continuous improvement and progress reporting
- Six cybersecurity standards
  - NIST CSF, MP, RBO, PSAP, CMMC, 171
- Four standards-based assessment methodologies
  - 171A, 53/53A, 162 Handbook
- Supply chain status aggregation/visibility



Designed for Security Experts As Well As the Uninitiated

NIST Standards
Track and manage your cybersecurity status. View your status through the lens of multiple standards, prioritize compliance activities and generate clear, easy to understand status reports.

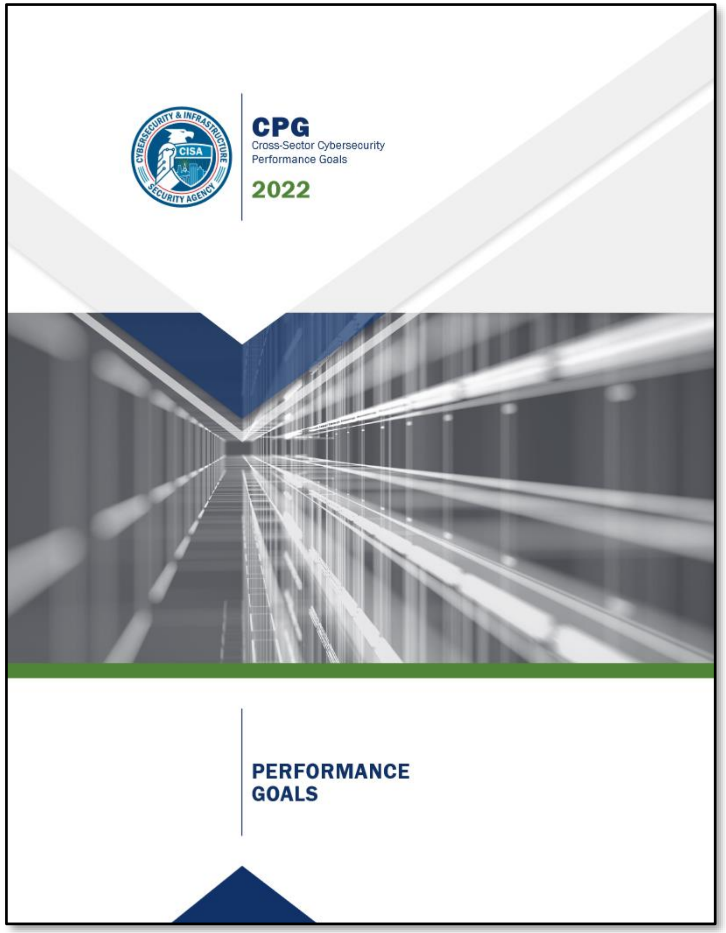
Supply Chain Readiness
A window into a single business' cyber security posture -- or into an entire supply chain. Enterprise license empowers prime contractors while offering their subs a streamlined, step-by-step process for addressing compliance. (CMMC Features In Development Now)

Quickly Prioritize and Track Compliance Activities
Speed the initial assessment process using our time saving, ready-made policy templates: Plan of Action and Milestones document (POAM), Corporate Cybersecurity Policies, and many more.

Clarity for the Entire Enterprise
A common language to bridge understanding -- from those responsible for testing, monitoring and securing systems, to C-Suite execs responsible for contracts and staff compliance. Our easy to understand documentation and reports put everyone on the same page.

Activities Remaining

- Integrate with Cyber Talent Bridge
  - NIST NICE-based workforce management
  - Alignment of knowledge/skills to cybersecurity task assignment
  - Identify & mitigate skills and/or training gaps
- Integrate DHS CISA CPG
- Integrate Trustmark framework (federated ICAM)
  - Emergency response, law enforcement, other sensitive communities
- Deploy with government approved containers
- Integrate education and training



CPG
Cross-Sector Cybersecurity
Performance Goals
2022

PERFORMANCE
GOALS

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Annual Review: CyberTalent Bridge

Anderson Wiese

2wav

ciri.illinois.edu

The Problem

What capabilities do I need?

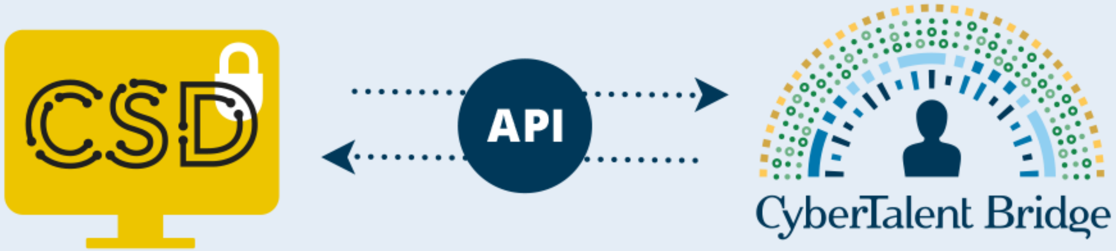
Cynthia Jefferson
Incoming CISO
SME Manufacturing

Who in my talent pool has these capabilities?

What missing skills do I need to develop or recruit?

What will success look like?

Cybersecurity teams use CTB with CSD to manage compliance and workforce development.

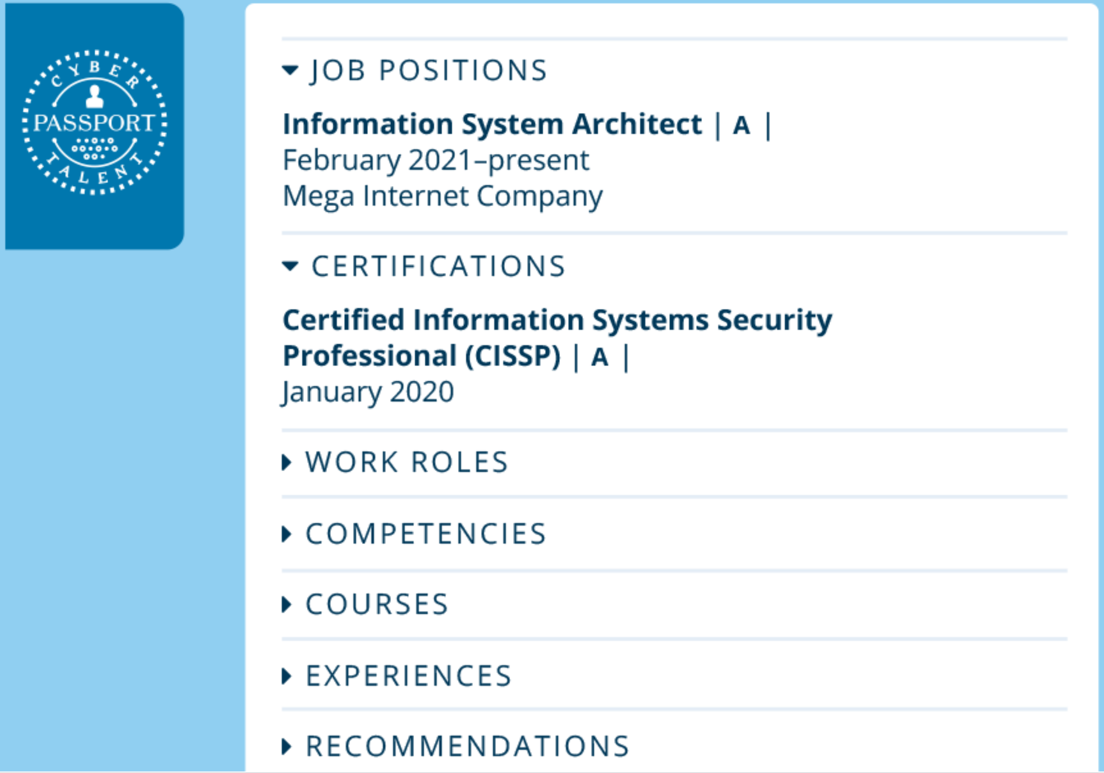


CSD

API

CyberTalent Bridge

CyberTalent Passports share skills-based capability statements.



CYBER PASSPORT TALENT

▾ JOB POSITIONS

Information System Architect | A |
February 2021–present
Mega Internet Company

▾ CERTIFICATIONS

Certified Information Systems Security Professional (CISSP) | A |
January 2020

▸ WORK ROLES

▸ COMPETENCIES

▸ COURSES

▸ EXPERIENCES

▸ RECOMMENDATIONS

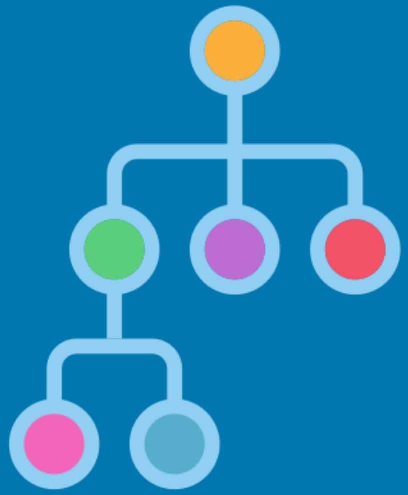
Benefits

Tasking

Requirements to recommendations

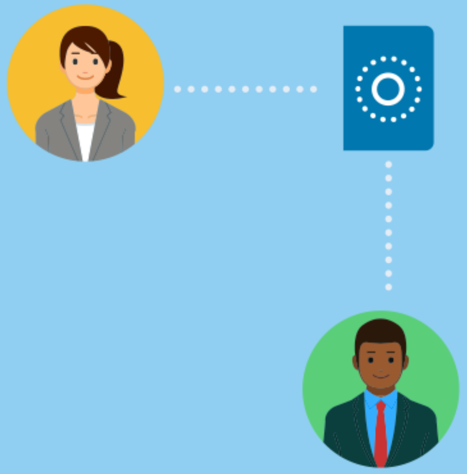
Workforce

Assessment, development, recruiting



Sharable Passports

Encourage cooperation and integration

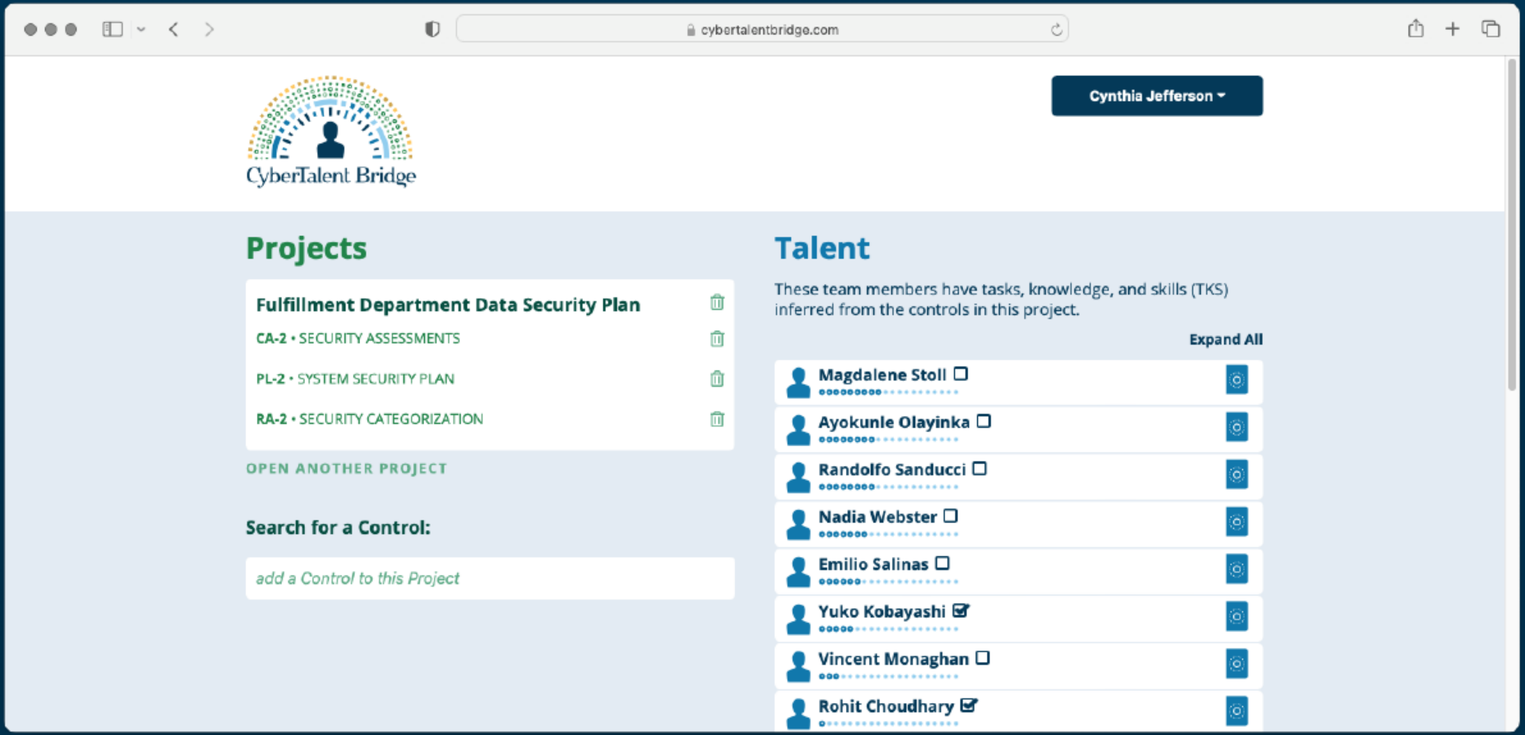


Frameworks

Connect cybersecurity frameworks

Accomplishments

CyberTalent Bridge works!



cybertalentbridge.com

CyberTalent Bridge

Cynthia Jefferson ▾

Projects

Fulfillment Department Data Security Plan

CA-2 • SECURITY ASSESSMENTS

PL-2 • SYSTEM SECURITY PLAN

RA-2 • SECURITY CATEGORIZATION

OPEN ANOTHER PROJECT

Search for a Control:

add a Control to this Project

Talent

These team members have tasks, knowledge, and skills (TKS) inferred from the controls in this project.

Expand All

- Magdalene Stoll ☐
- Ayokunle Olayinka ☐
- Randolfo Sanducci ☐
- Nadia Webster ☐
- Emilio Salinas ☐
- Yuko Kobayashi ☑
- Vincent Monaghan ☐
- Rohit Choudhary ☑

CTB is the first workforce tool engineered from the ground up in terms of the NICE Framework.

Bridges between isolated frameworks.

Realizes portable, sharable CyberTalent Passports

Evaluates talent capability by inference and confidence.

Activities Remaining

Commercial release integrated with Cyber Secure Dashboard.

CyberTalent Passport public release.

Optimize for scale.

Enhancements for potential industry partners:

Training agencies, community colleges, universities

Recruiters

Insurers

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Annual Review: **NG9-1-1 Interoperability Testing Program - Projects 2A & 2B**

Walt Magnussen, Ph.D.
Texas A&M University
Internet2 Technology Evaluation Center

The Problem

- Statement of the problem:
  - The United States has identified the 911 system as critical infrastructure. While a $15 billion national transition to NG 911 is occurring we currently have no way of ensuring interoperability of sub-systems.
  - DHS CISA has the lead responsibility in interoperability for critical infrastructure. They are working with the US DoT NG-911 office, the FCCs Public Safety Bureau, the National Emergency Number Association (NENA) and others.
- How are you approaching it, and what makes your approach unique?
  - We have created a Stakeholders group that will provide guidance on the Governance of, Technology used and Financial model of a DHS NG-911 Interoperability Certification process. The stakeholders group includes DHS, DoT, FCC, NIST, State Agencies, Industry Associations and Academia. It also includes international participation.

What Will Success Look Like?

- Success will include;
  - A conformance testing system that is in the public domain encouraging more testing facilities,
  - At least one test facility that operates under a sustainable model,
  - All jurisdictions procuring NG-911 components requiring DHS Certification,
  - Overwhelming acceptance by all stakeholders,
  - An ecosystem that is standards conformant and interoperable

Benefits

- How will success benefit the Homeland Security Enterprise?
  - The initial promises of NG-911 included;
    - Additional capabilities for emergency callers (video, text, additional data)
    - Lower costs through additional competition, the use of off the shelf hardware and the acceptance of standards
    - Higher reliability thru call redirecting, diverse routing and network-to-network interconnection.
  - None of these promises can be realized unless the underlying NG-911 subsystems are interoperable.

Accomplishments

- Phase 2a
  - Document 10 call scenarios for end-to-end testing (7 of 10 complete).
  - Install and document first complete ESInet with required NGCS functional elements.
  - Test call conformance through ESInet working with Verizon for call ingress.
- Phase 2b
  - Establish stakeholders group membership and structure and schedule first full member face-to-face meeting.
  - Initiate contract with consultant for ISO 17025 conformance.

Activities Remaining

- Phase 2a
  - Complete second i3 ESInet and PSAP for end-to-end testing.
- Phase 2b
  - Hold stakeholders face-to-face meeting (2 March)
  - Produce outreach video
  - Complete and document ISO 17025 Certification for TAMU ITEC
  - Validate end-to-end testing model
  - Document operational cost model

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Annual Review: EMP Risk Assessment and Mitigation Prioritization

Jose Schutt-Aine, Glen Salo, Daniel Shaw,
Aosheng Rong, Victoria Shao
University of Illinois, Synclesis, Inc.

5G Infrastructure Resilience

- Electromagnetic Pulse (EMP) attacks have the potential to disrupt and damage electronics throughout our nation’s critical infrastructure, posing a serious risk to that infrastructure. Assessing the risk of such events is extremely challenging due to the complexity of our systems.

- This project addressed the threat of EMP to our nation’s critical infrastructure, which includes our nation’s power grid and mobile communication systems.

Our Approach

- Use uncertainty and randomness as a means of tackling and overcoming complexity for the purpose of mitigation
- This approach differs fundamentally from traditional methods that cannot account for the multi-scale material and geometry complexity and the variabilities and uncertainties inherently present in the EMP problem due to the computational complexities.
- Our goals included both developing this capability and using it to assess EMP effects on the electronics in a 5G communications tower.

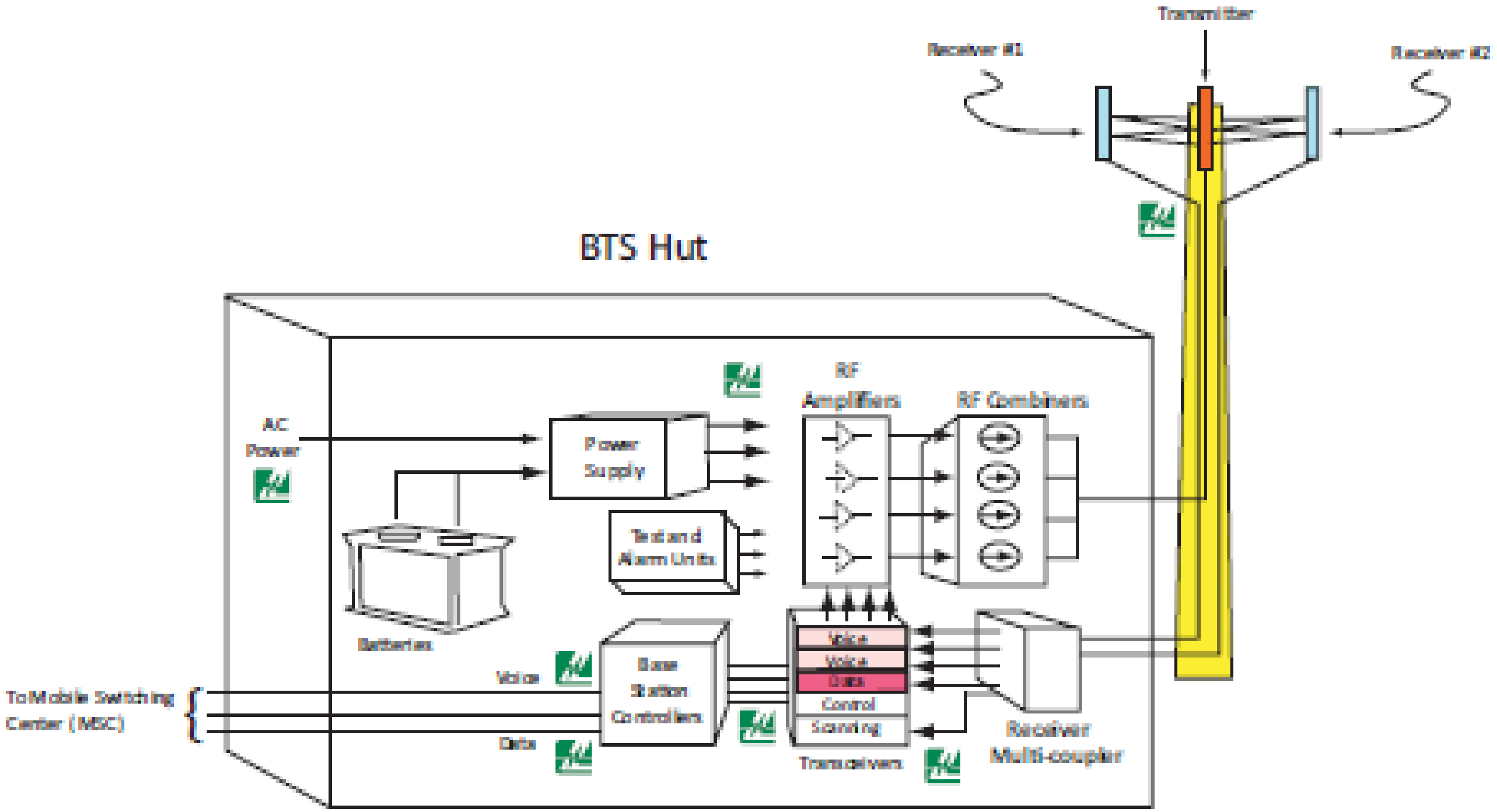
Objectives

- Ability to quickly assess and predict impact of an EMP attack on 5G infrastructure
- Ability to help preemptively mitigate effects of such attacks via Characterization, Validation, Simulation & Mitigation

Benefits & Potential Impact

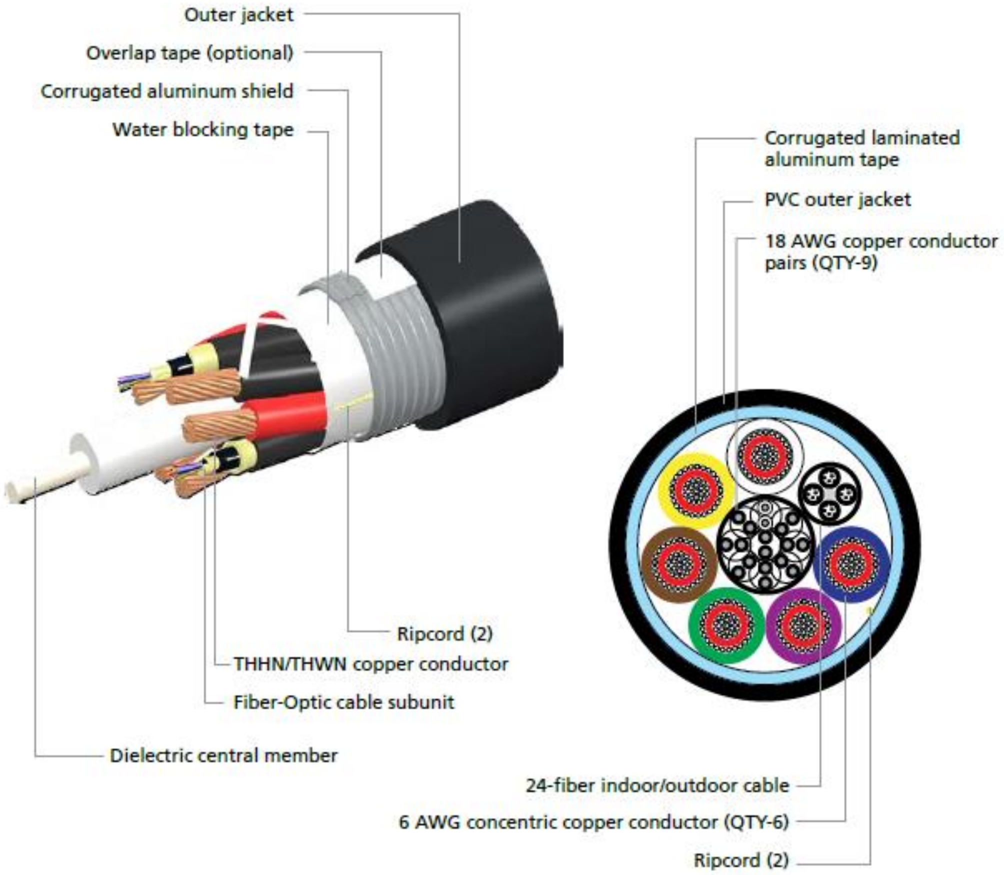
- Critical to CISA
- Accurate risk assessment of EMP attack
- Help increase resilience to EMP attack
- Facilitate mitigation measures

5G Infrastructure



Radio tower and BTS equipment used in a typical cell site location.

Hybrid Cable & Surge Protection Devices


Outer jacket
Overlap tape (optional)
Corrugated aluminum shield
Water blocking tape
Corrugated laminated aluminum tape
PVC outer jacket
18 AWG copper conductor pairs (QTY-9)
Ripcord (2)
THHN/THWN copper conductor
Fiber-Optic cable subunit
Dielectric central member
24-fiber indoor/outdoor cable
6 AWG concentric copper conductor (QTY-6)
Ripcord (2)

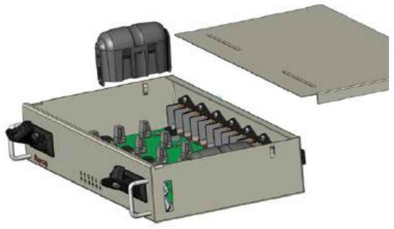
The internal structure of a hybrid cable

Typical surge protection devices (SPDs)

A gas tube surge arrestor used to ground the inner conductive layer

Inside an RRH surge protector module, cover removed

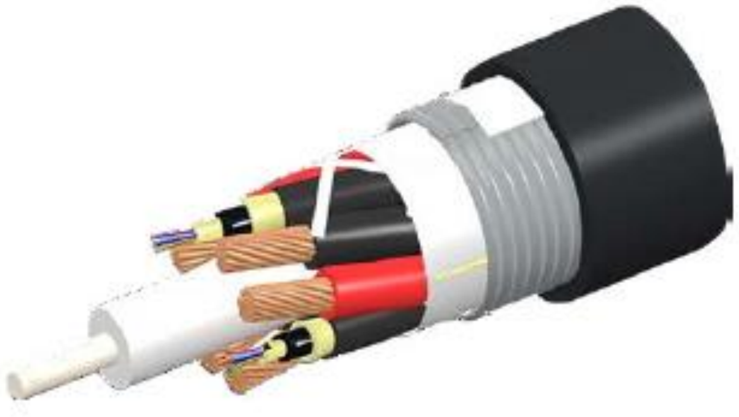
An SPD assembly mounted in a dc power and battery enclosure



The interior detail of an SPD unit designed to protect an RRH

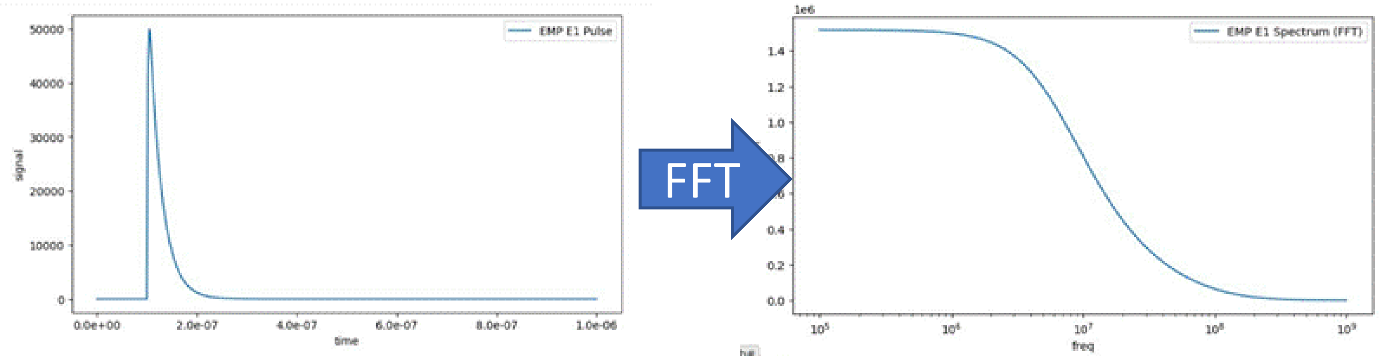
Hybrid Cable

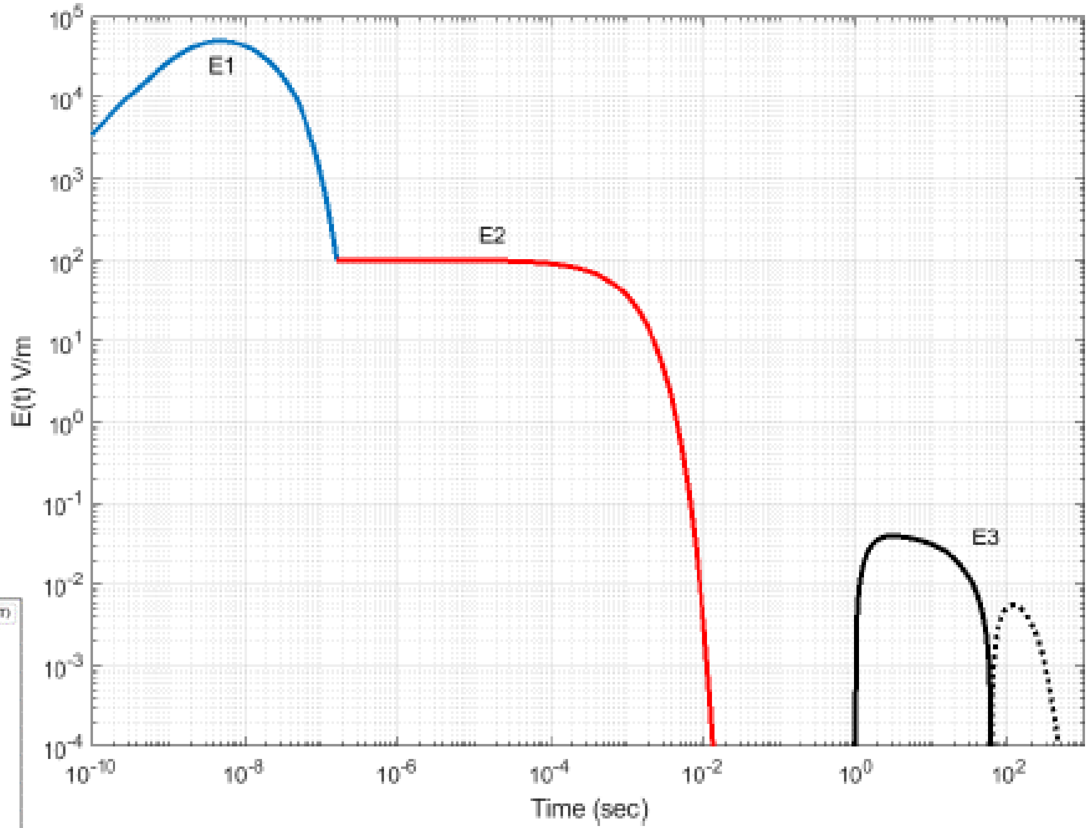
- Since fiber-optic cable uses light, not electricity, to propagate signals, it does not carry power to remote radios. A power cable must be added to provide the power to these devices: ➔ hybrid cable contains both types in a single sheath.



EMP Waveform

- Initial Focus on E1 Pulse:
  - $V = E_0 k\left(e^{-at} - e^{-bt}\right)$, where
  - $E_0 = 50kV$,
  - $k = 1.3$,
  - $a = 4e7$, and
  - $\mathrm{b} = 6\mathrm{e}8$



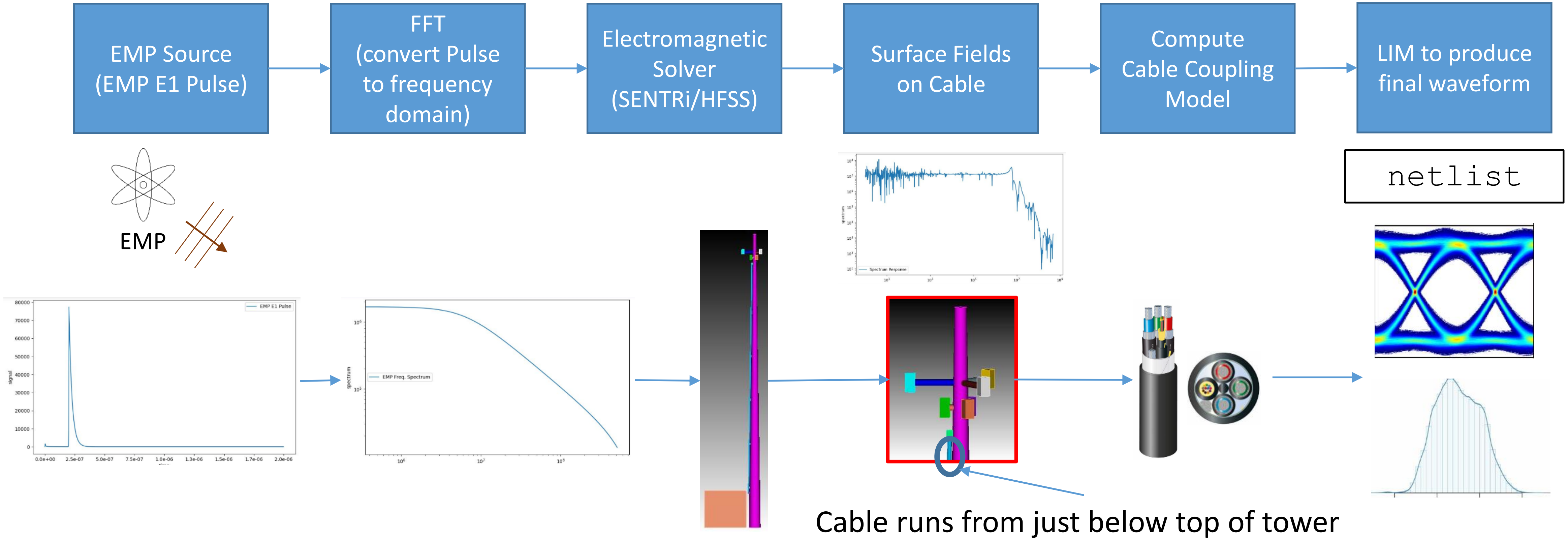


E1-EMP: 50kV/m - 400MHz

E2-EMP: 0.1kV/m - 100kHz-1MHz

E3-EMP: 10V/m - < 1Hz

Cellular Tower EMP Model Flow



EMP Source (EMP E1 Pulse) → FFT (convert Pulse to frequency domain) → Electromagnetic Solver (SENTRi/HFSS) → Surface Fields on Cable → Compute Cable Coupling Model → LIM to produce final waveform

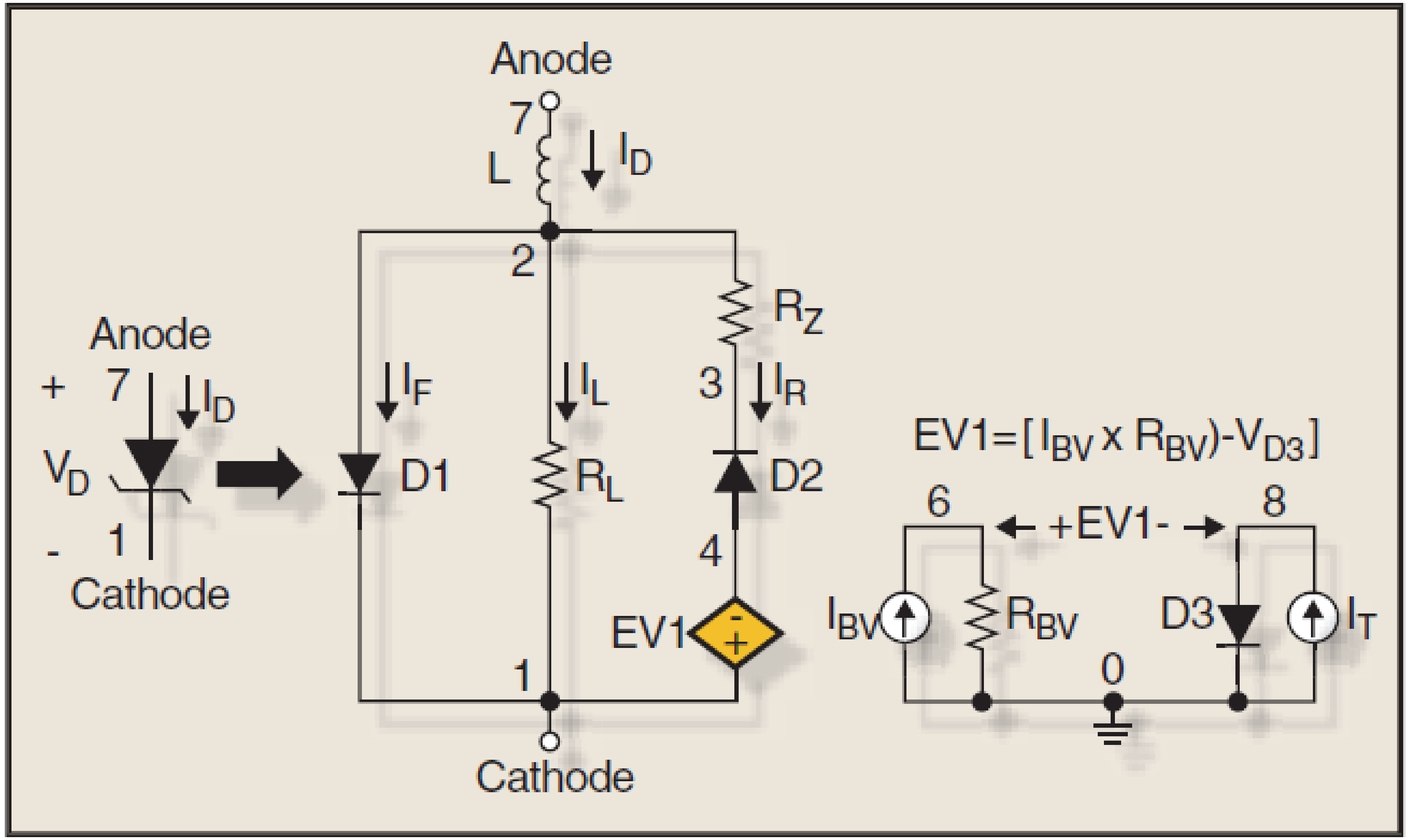
Cable runs from just below top of tower down to outside of the base station.

Accomplishments

- Extraction of Hybrid cable parameters as a function of frequency (code)
- Transient simulation of hybrid cable (code)
- Implement TVS device into simulator
- Implement MOV device into simulator
- Preliminary stochastic analysis of system

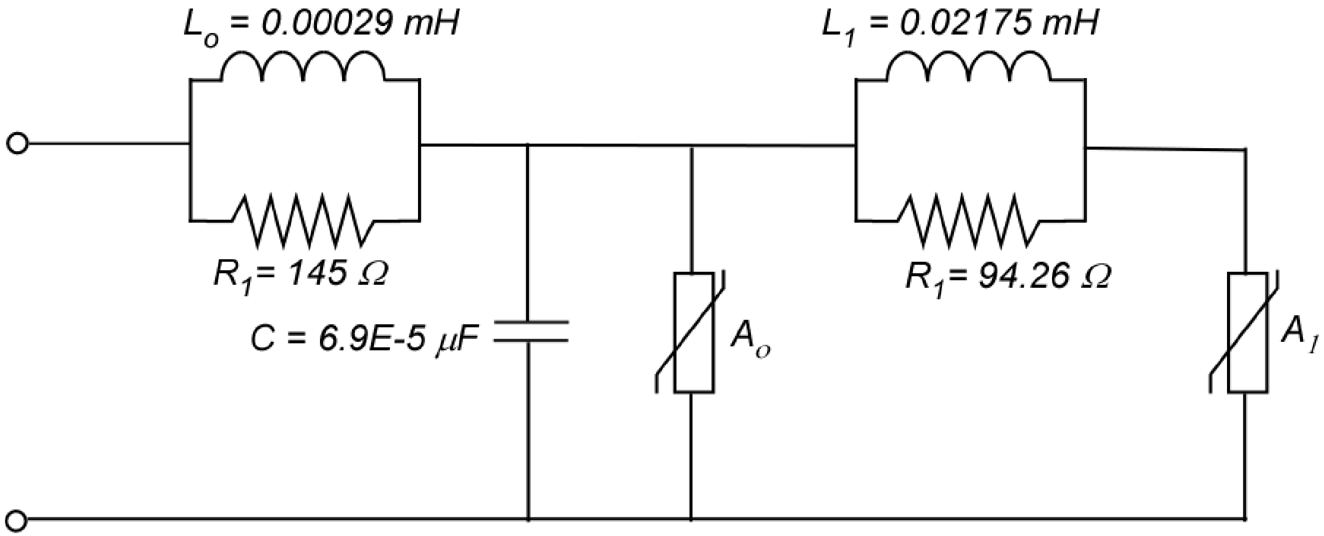
Transient Voltage Suppressors (TVS)

Circuit Model



Jim Lepkowski, Evaluating TVS Protection Circuits with SPICE, Power Electronics Technology January 2006

Modeling MOVs



Nonlinear Resistors

A0

I(kA)	V(pu)	V(kV)	
0.01	1.40	217.0	--- 21.7 kohms
0.1	1.54	238.7	-- 2.38 kohms
1	1.68	260.4	-- 260 ohms
2	1.74	269.7	--- 134 ohms
4	1.80	279.0	--- 69.75 ohms
6	1.82	282.1	--- 47.01 ohms
8	1.87	289.9	--- 36.23 ohms
10	1.90	294.5	--- 29.45 ohms
12	1.93	299.1	--- 24.91 ohms
14	1.97	305.3	--- 21.78 ohms
16	2.00	310.0	--- 19.37 ohms
18	2.05	317.7	--- 17.65 ohms
20	2.10	325.5	-- 16 ohms

A1

I(kA)	V(pu)	V(kV)	
0.1	1.23	190.50	--- 1.9 kohms
1	1.36	210.80	-- 210 ohms
2	1.43	221.65	-- 110.8 ohms
4	1.48	229.40	--- 57.35 ohms
6	1.50	232.50	--- 38.75 ohms
8	1.53	237.15	--- 29.64 ohms
10	1.55	240.25	--- 24.025 ohms
12	1.56	241.85	--- 20.1 ohms
14	1.58	244.95	--- 17.49 ohms
16	1.59	246.45	--- 15.4 ohms
18	1.60	248.00	--- 13.777 ohms
20	1.61	249.55	--- 12.47 ohms

LIM Simulator

synclesis

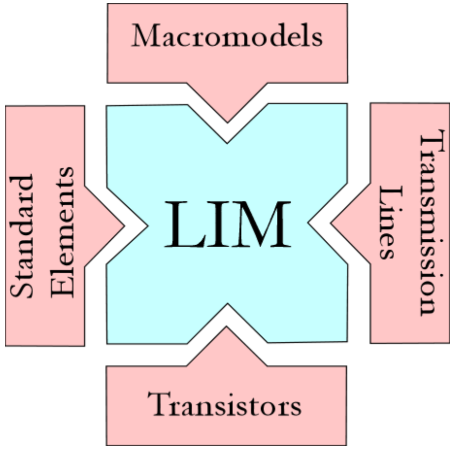
The LIM platform is optimal for accurate simulation of signals in hybrid cable

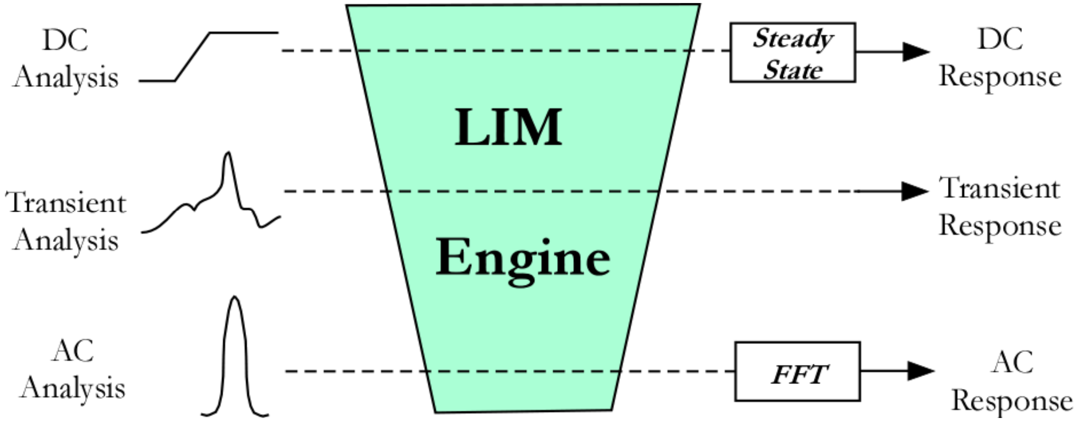
Features

- Rapid transient analysis
- Transistor-level simulations
- Frequency-dependent components
- Fast transmission-line analysis
- Large netlists
- Time step control
- Tunable accuracy and speed
- Chip, package or board

Applications

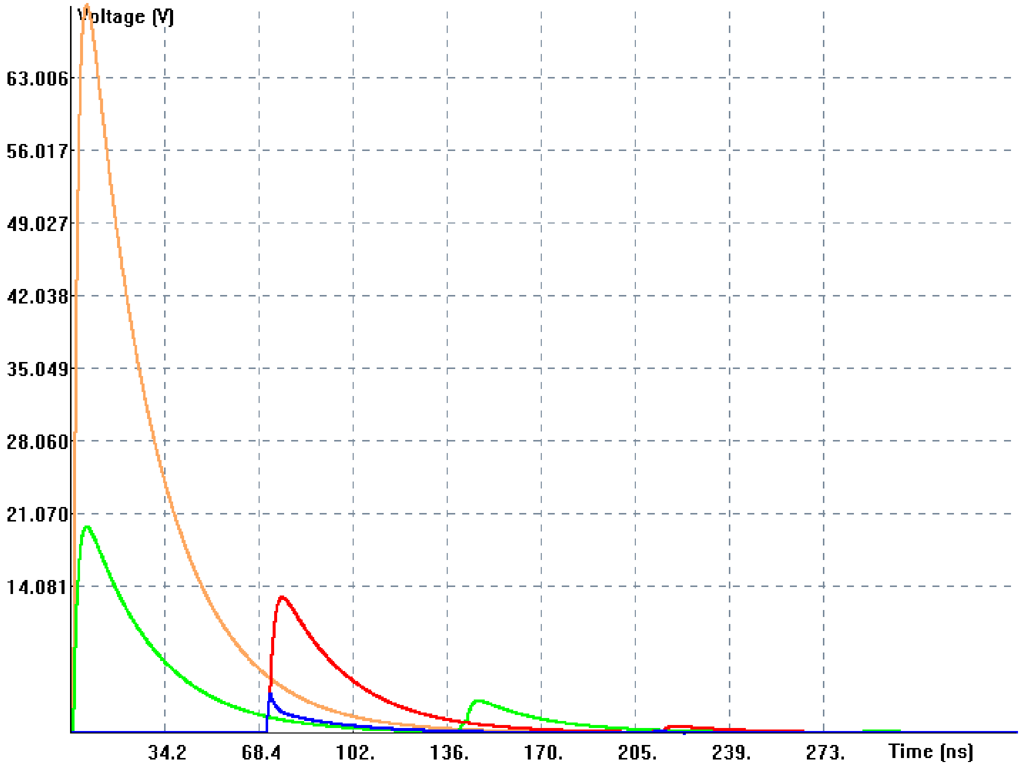
- Power Delivery Networks
- IR Drop Analysis
- Analog/Mixed Signal Simulation
- Macromodel Analysis
- IC Verification
- High-Speed Link Design



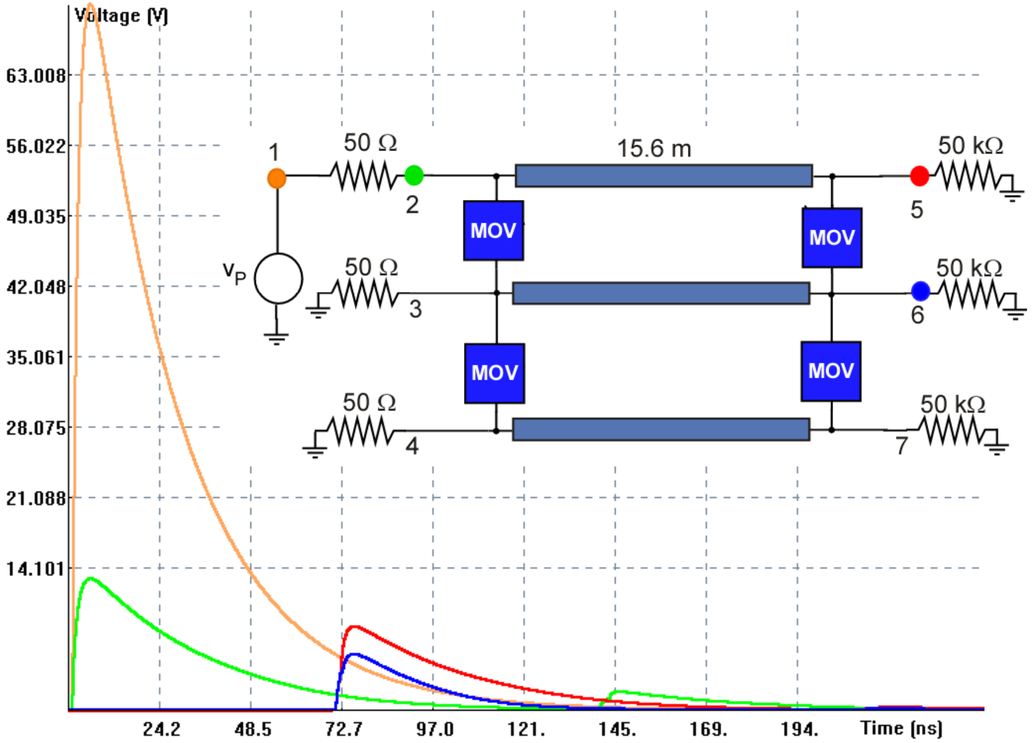


LIM Results

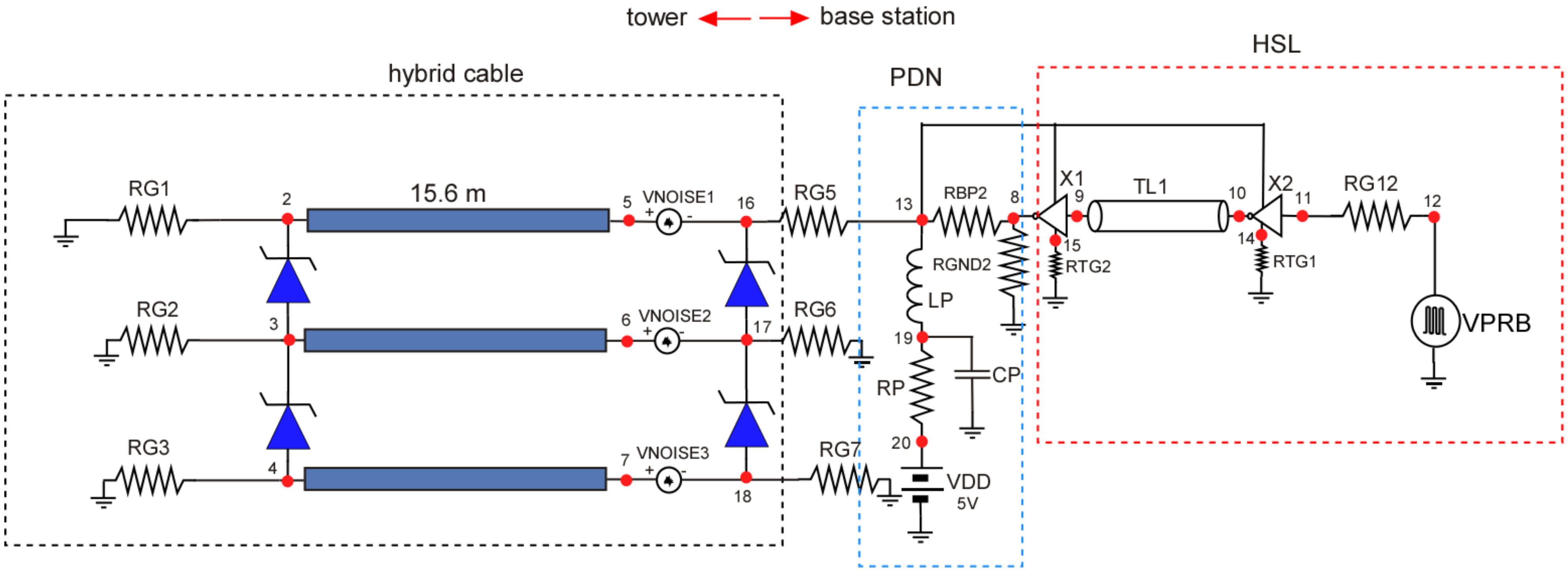
Hybrid Cable – No Suppression



Hybrid Cable – With Suppression

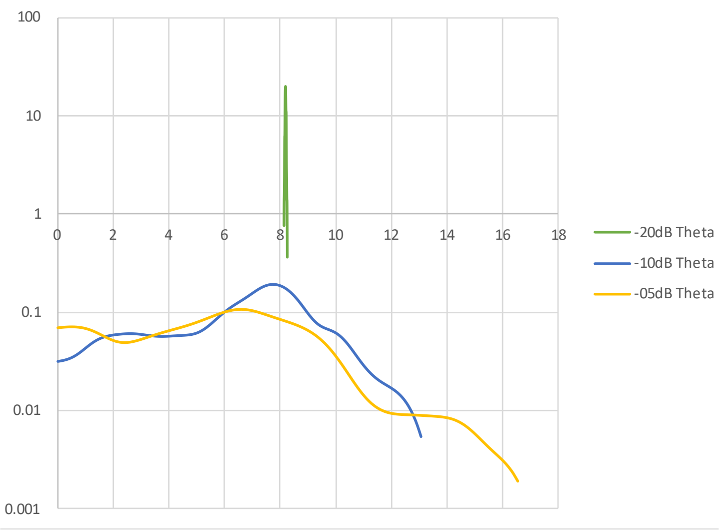


High-Speed Link Simulation

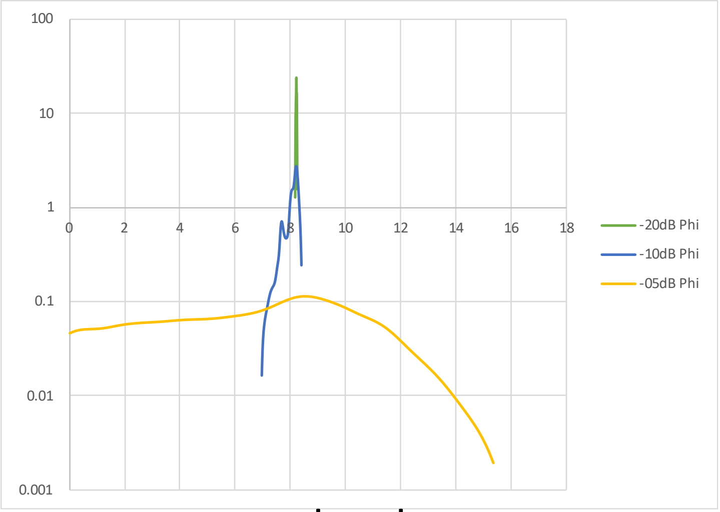


Initial Stochastic Results

- Varied Incident Angle of EMP
  - Θ and ϕ
- Evaluated at stochastic collocation points on sparse grid
  - Final Metric: Signal Eye Width
- Adjusted shielding level
  - 5dB, 10db and 20dB
- Created interpolant function from results and generated probability distribution function



Θ pol



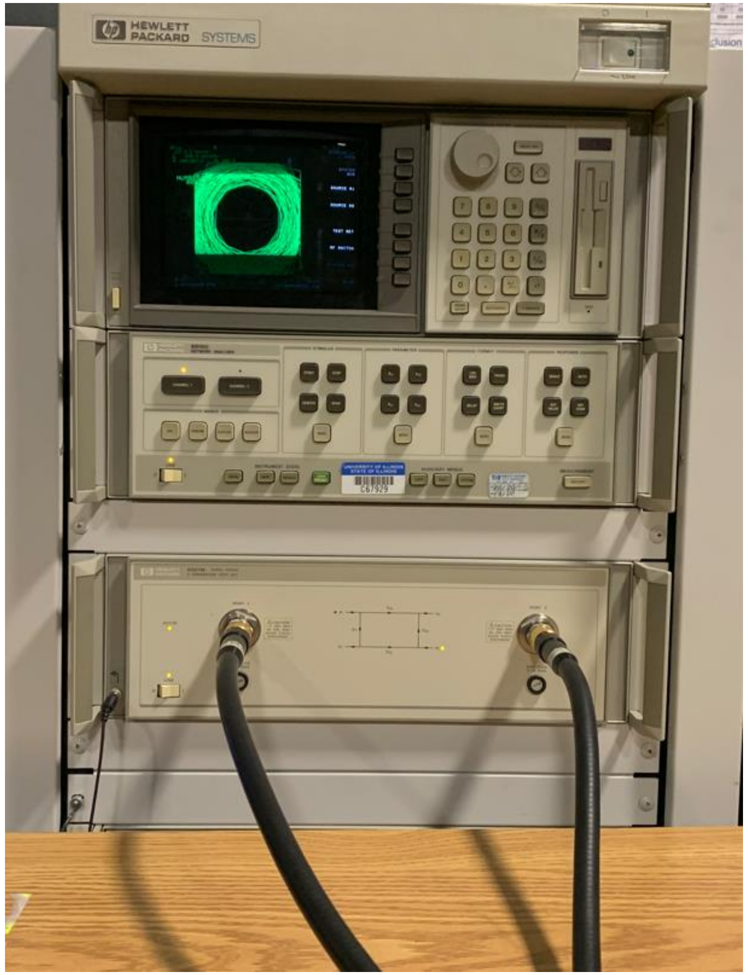
ϕ pol

Activities Remaining

- Validation & model enhancement of hybrid cable, arresters
- Behavioral modeling of PCB
- Refine EM coupling solution for surface currents
- Mitigation study via stochastic analysis→ LIM Enhancement

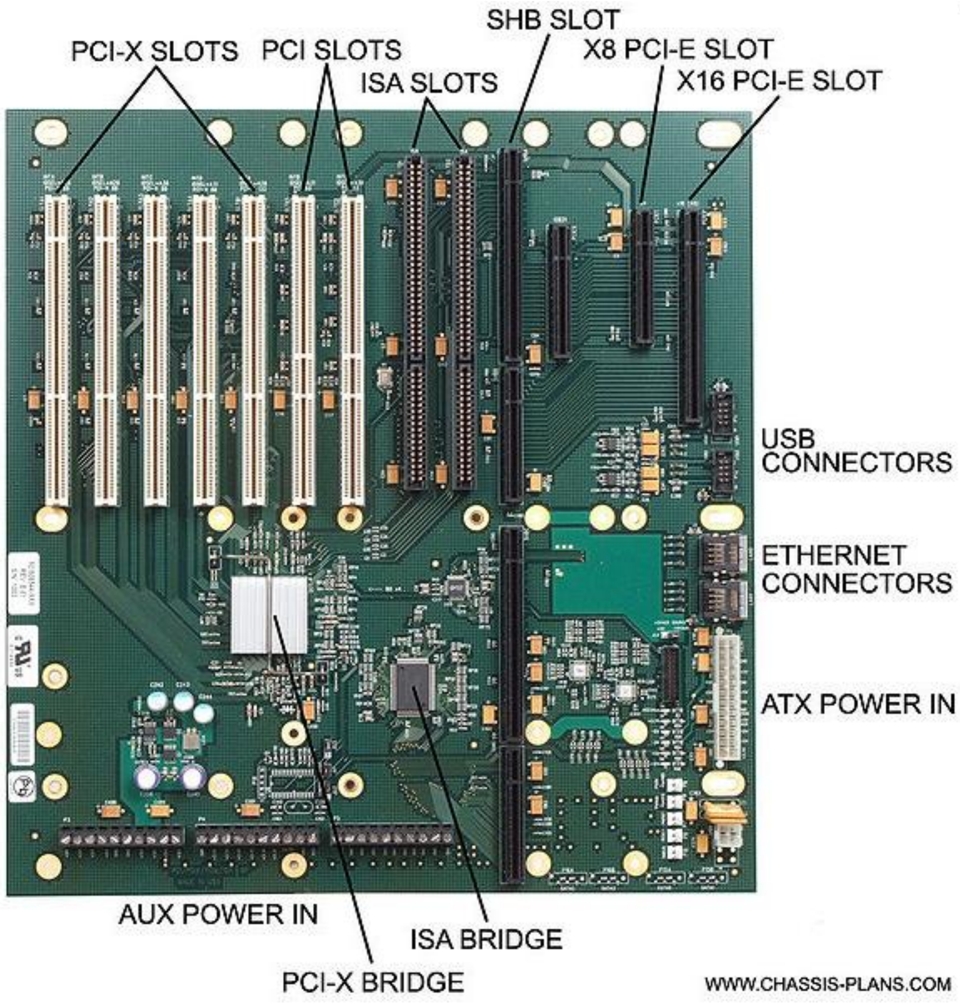
Hybrid Cable Model Validation

- Measure Cable S Parameters (VNA)
- Optimize with field solver
- Assess frequency dependence
- Perform iteration



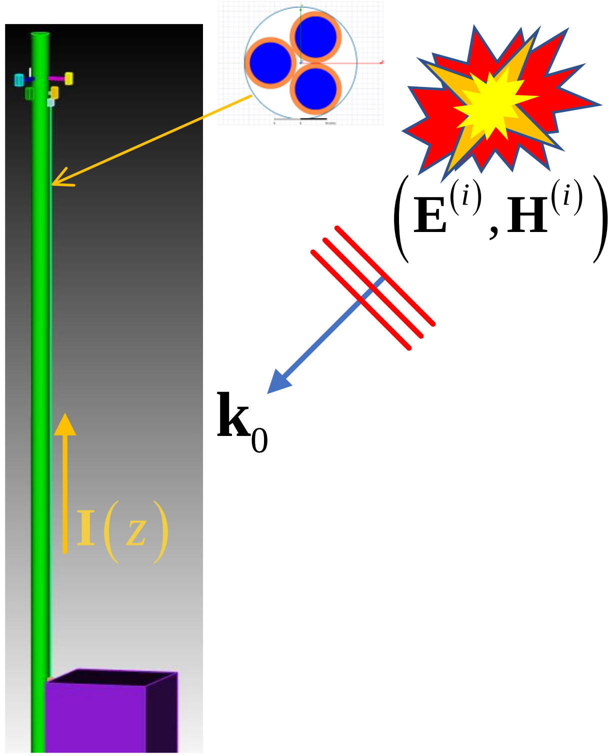
PCB Modeling

- Identify points of entry (e.g. PDN)
- Reduce complexity via behavioral modeling
- Macromodels via MOR
- IBIS model implementation
- X parameters



WWW.CHASSIS-PLANS.COM

Accurate Computation of the Surface Currents on Hybrid Cable over Lossy Ground Illuminated by EMP Waves



- Motivation
  - Hybrid cables with lean to an 5G RF tower is a multi-scale geometry. Finite element approximation of multi-scale geometries are prone to ill-conditioning over EMP frequency spectra range. Numerical experiments show that US Government code SENTRi and ANSYS' HFSS break down at EMP frequencies.
- Proposal and Implementation
  - We are developing a customized code that utilizes the mixed potential integral equation together with graph-based loop-tree decomposition technique, for the accurate computation of the external currents on the shielding conductor of the hybrid cables under EMP excitation at the whole EMP spectra range.
  - Lossy ground effects will be included.

Summary

- Proof of concept established
- Electromagnetic extraction and circuit simulation are key components
- FEM field solver
- LIM simulation engine
- Validation & refining of model will provide robust tool for mitigation

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Annual Review: **Protecting the nation’s 911 system from cyber threats - Present and Future**

Karthik Balasubramanian
Karthik Consulting, LLC

The Problem

- *The US 911 system (Public Safety Answering Point (PSAP)) is an essential part of the critical infrastructure of the United States, that spans several National Critical Functions, and needs to be protected from cyber-attacks.*
- CISA Emergency Communications Division (ECD) and the Emergency Public Safety Sector and more specifically PSAPs across the nation are intended to be the primary beneficiaries of this project

- Propose criteria for categorizing and developing a curated "PSAP Profile", using the NIST SP 800-53A controls and Cyber Security Framework (CSF) to measure and track the cybersecurity posture of PSAPs.
- Conduct consultative PSAP profile based "pilot" assessments of PSAPs

What Will Success Look Like?

- Following the CSF, conduct research and publish a curated list of tailored NIST SP 800-53A controls for measuring and monitoring the security posture and cybersecurity maturity of PSAPs
- Implement the PSAP Profile in the Cybersecure Dashboard (CSD) tool
- Conduct PSAP Profile based “pilot” assessments
- Understand the unique requirements of PSAPs migrating to NG911 and update the PSAP Profile, as necessary

Benefits

- As the PSAP threat landscape rapidly changes so does the urgency to secure and improve this critical infrastructure. This project addresses the Goals and Objectives identified in the CISA Strategic Intent document (published in August 2019) by proposing to enhance the current and ongoing security and resilience of the PSAP ecosystem
- Create a more secure nation-wide PSAP system through the PSAP Profile and mapped cybersecurity controls.
- The 6000+ PSAPs and the 1000+ federal/DoD PSAPs can benefit from the PSAP Profile to help understand and track their cybersecurity posture and risks.

Accomplishments

- Phase 1 research of PSAPs completed and final report published
- PSAP Profile published and approved by CIRI/CISA/DHS S&T
- PSAP profile implemented in the Cybersecure Dashboard tool
- PSAP Profile based “Pilot” assessments completed
- Phase 2, further research to understand the unique requirements of PSAPs migrating to NG911 completed

Activities Remaining

- Analyze the results from the Phase 2 research of PSAPs migrating to NG911
- Update the PSAP Profile, as needed, to support NG911 type PSAPs
- Publish the final report
- Publish the updated PSAP Profile curated list of NIST SP800-53A controls

Networking break

15-minutes

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Annual Review:
Cybersecurity Education & Workforce Development

Casey W. O’Brien, UIUC

December 6, 2022

.edu

A Two-Phase Project

- Phase 1: Developing a National Needs Analysis and Strategy: 2020-2021
- Phase 2: Curriculum Development: 2021-2022

CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY

PHASE 1

Hub & Spoke Project

- *"Research and Deliverables on Utilizing an Academic Hub and Spoke Model to Create a National Network of Cybersecurity Institutes"*
- 3 partners, plus a network of 2/4-year schools (Hubs and Spokes)
- Emphasis on underserved populations
- IR and ICS security-related education and training

Hub & Spoke Project Deliverables

- UIUC: Scalable National Network Plan & Hub School Guidance Document
- Auburn: Incident Response Curriculum Guidance Document
- Purdue: Industrial Control Systems Curriculum Guidance Document
- Tulsa: Spoke School Guidance Document

Principal Findings from Phase 1

- Demographic imbalances in access to cybersecurity education and training
- Failure of existing education and training to provide employers clear competency outcome information
- Weakness in education and training for "**post-boom**" cybersecurity capacity

Recommendations for a Phase 2

- Curriculum development that provides multiple pathways
- Practical learning experiences with demonstrated, employer-recognizable performance outcomes (e.g., context mapped to a work role's tasks)
- Flexible, modular architecture for incremental accredited learning progression (e.g., training > college/degree)

PHASE 2

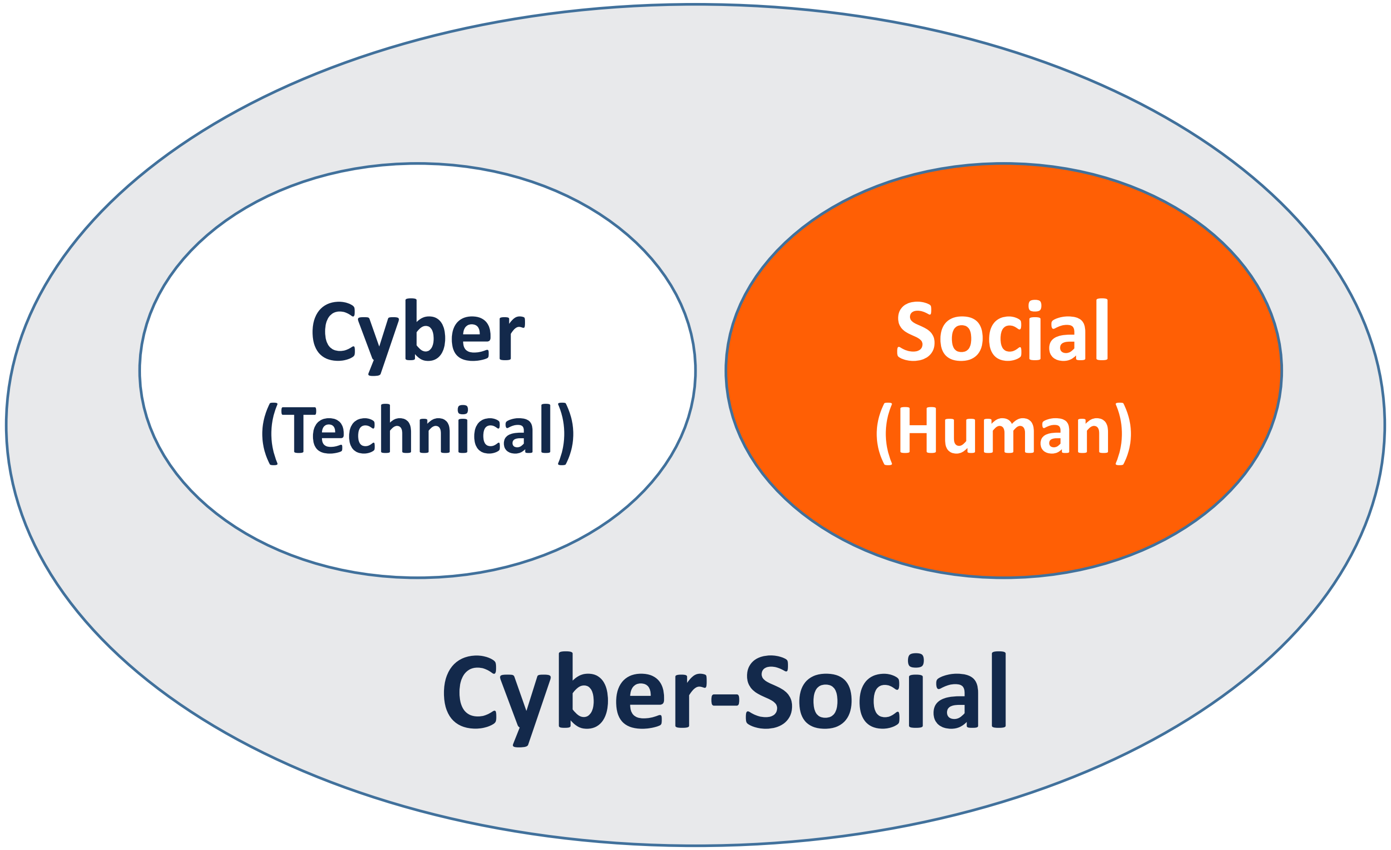
Curriculum Development Project

- *"Development of a Robust, Nationally Accessible Cybersecurity Risk Management Curriculum for Technical and Managerial Cybersecurity Professionals"*
- 5 partners
- Hybrid curriculum model

Curriculum Development Project: Learning Principles & Processes

- Dialogical: Learners respond to content inputs (lecture videos, readings, links) via discussions and select response surveys
- Collaborative: Projects and labs involve peer review
- Knowledge co-constructed by learners: Learners research topics, make posts, and comment on each others' posts
- Advanced Learning Analytics: Embedded formative assessments, mastery learning

Applying a Signature Orientation

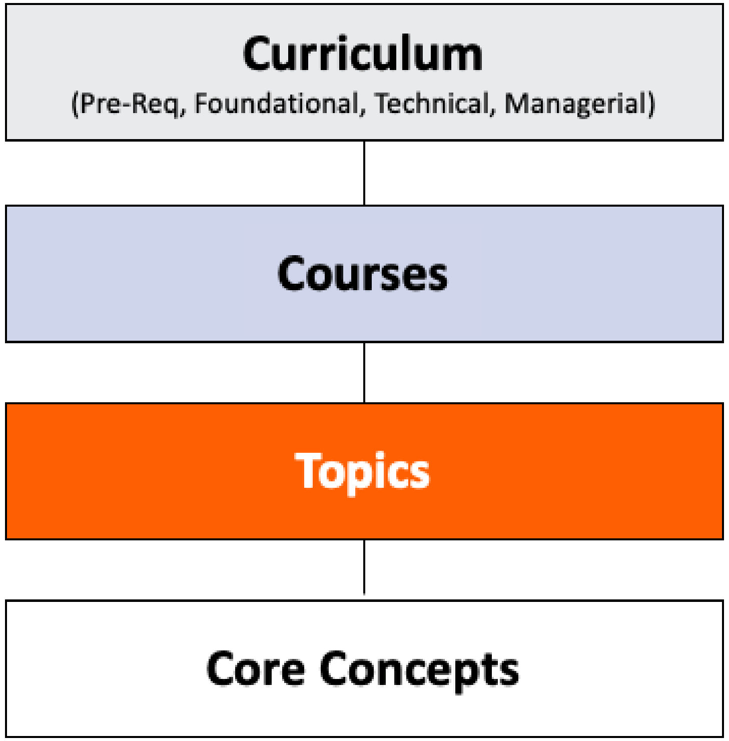


Cyber
(Technical)

Social
(Human)

Cyber-Social

Delivering a Stackable Program Architecture



4 — **Curriculum** (Pre-Req, Foundational, Technical, Managerial) — < Assembling courses into programs with varying durations and foci

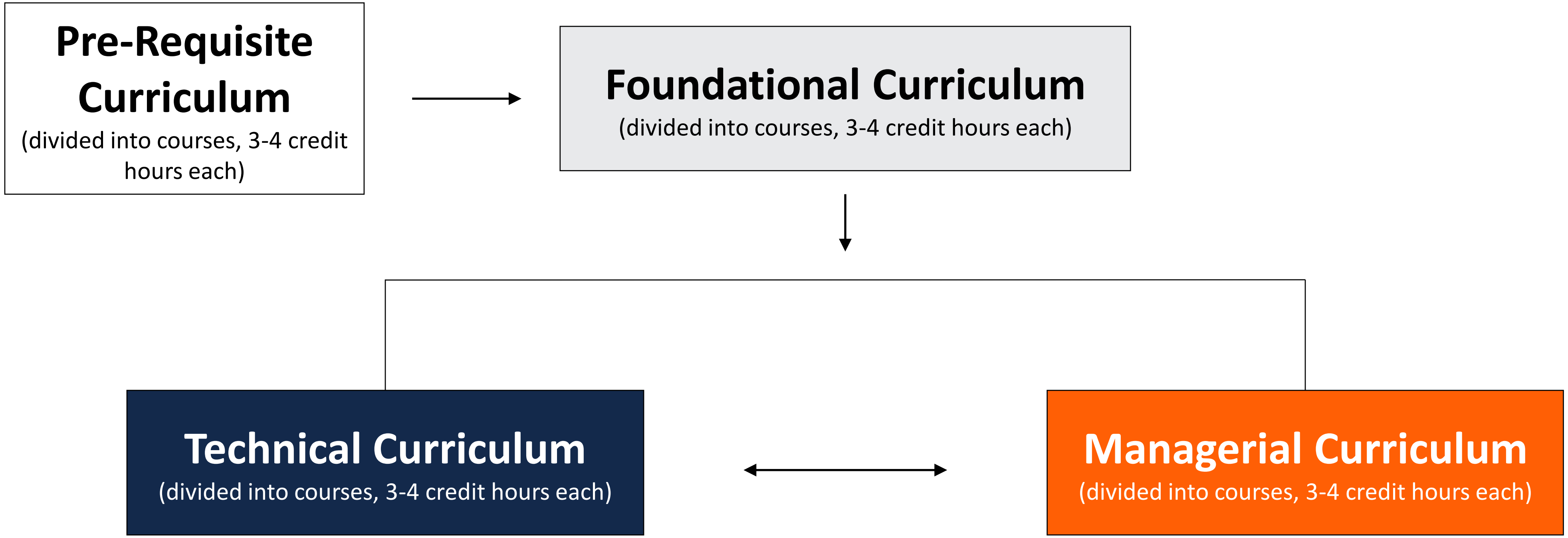
17 — **Courses** — < The equivalent of 3-4 credit hours each

17 x 8 — **Topics** — < Can be stand-alone training modules

Core Concepts — < Aligned with NICE, performance outcomes, workplace roles & tasks

Flexibility to serve diverse populations and needs

Providing Alternatives Pathways



Pre-Requisite Curriculum
(divided into courses, 3-4 credit hours each)

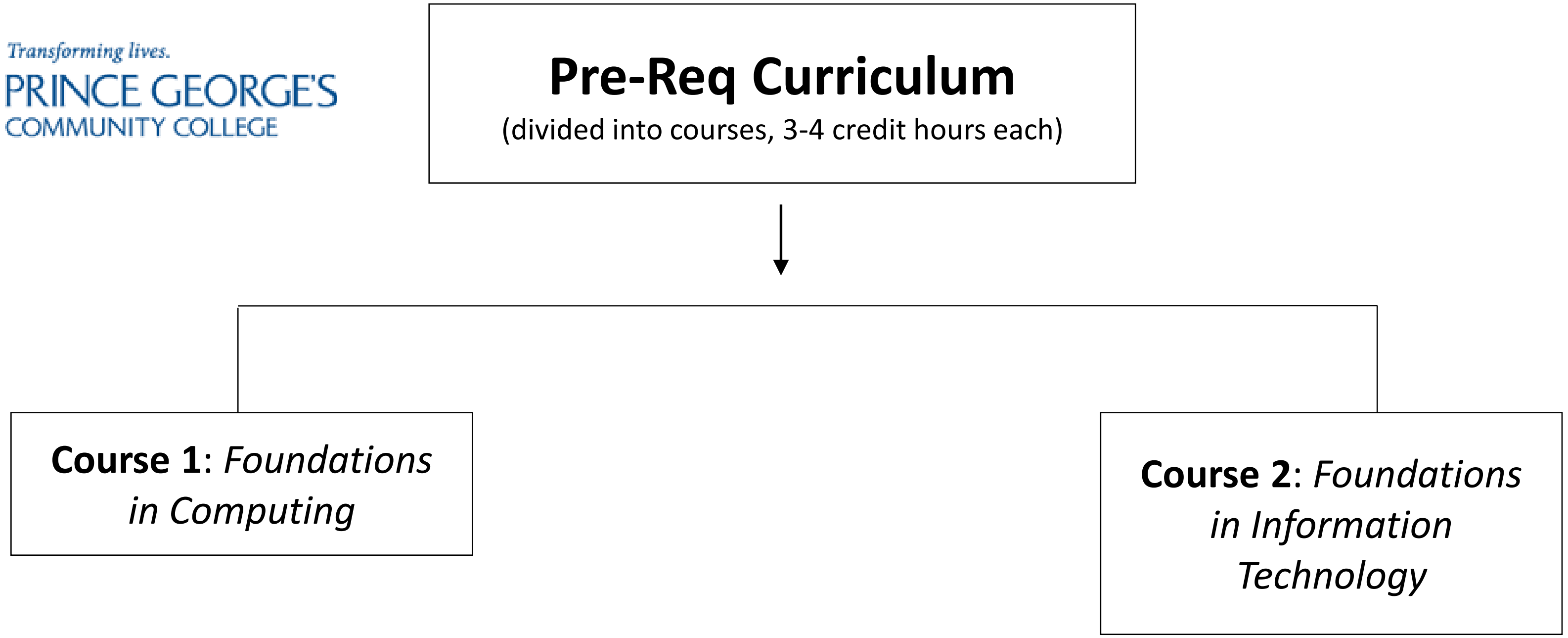
Foundational Curriculum
(divided into courses, 3-4 credit hours each)

Technical Curriculum
(divided into courses, 3-4 credit hours each)

Managerial Curriculum
(divided into courses, 3-4 credit hours each)

Hybrid Curriculum

Transforming lives.
PRINCE GEORGE'S COMMUNITY COLLEGE



Pre-Req Curriculum
(divided into courses, 3-4 credit hours each)

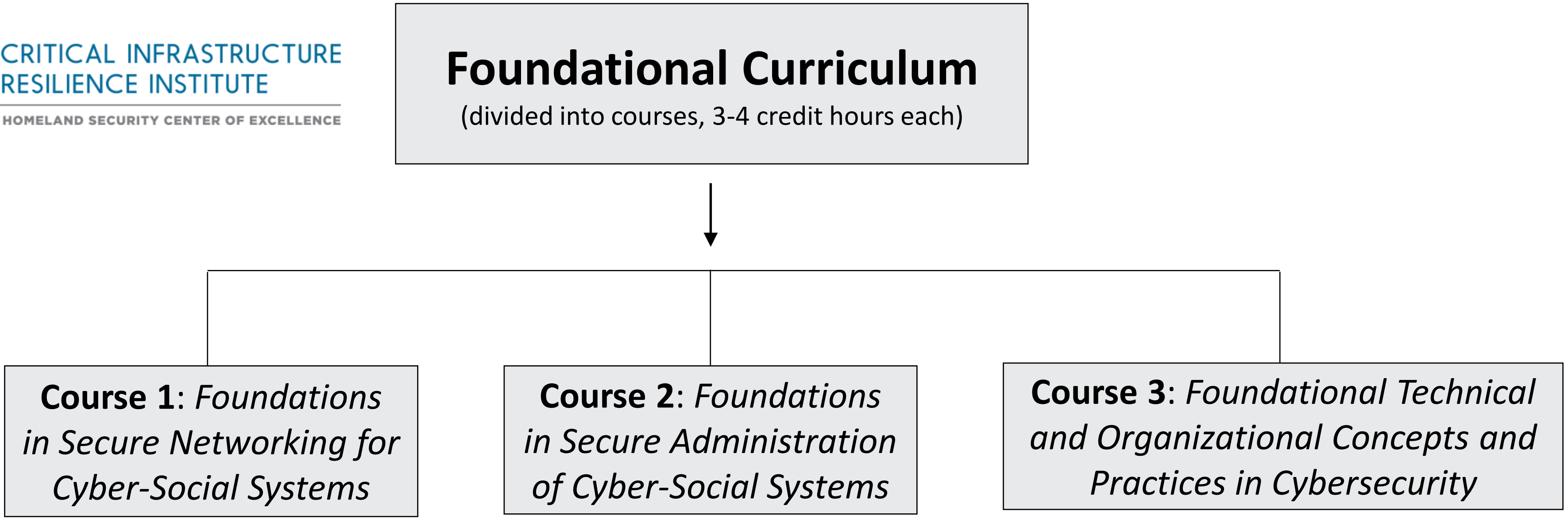
Course 1: *Foundations in Computing*

Course 2: *Foundations in Information Technology*

The Pre-Requisite Curriculum is comprised of these 2 courses

Hybrid Curriculum

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE
A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE



Foundational Curriculum
(divided into courses, 3-4 credit hours each)

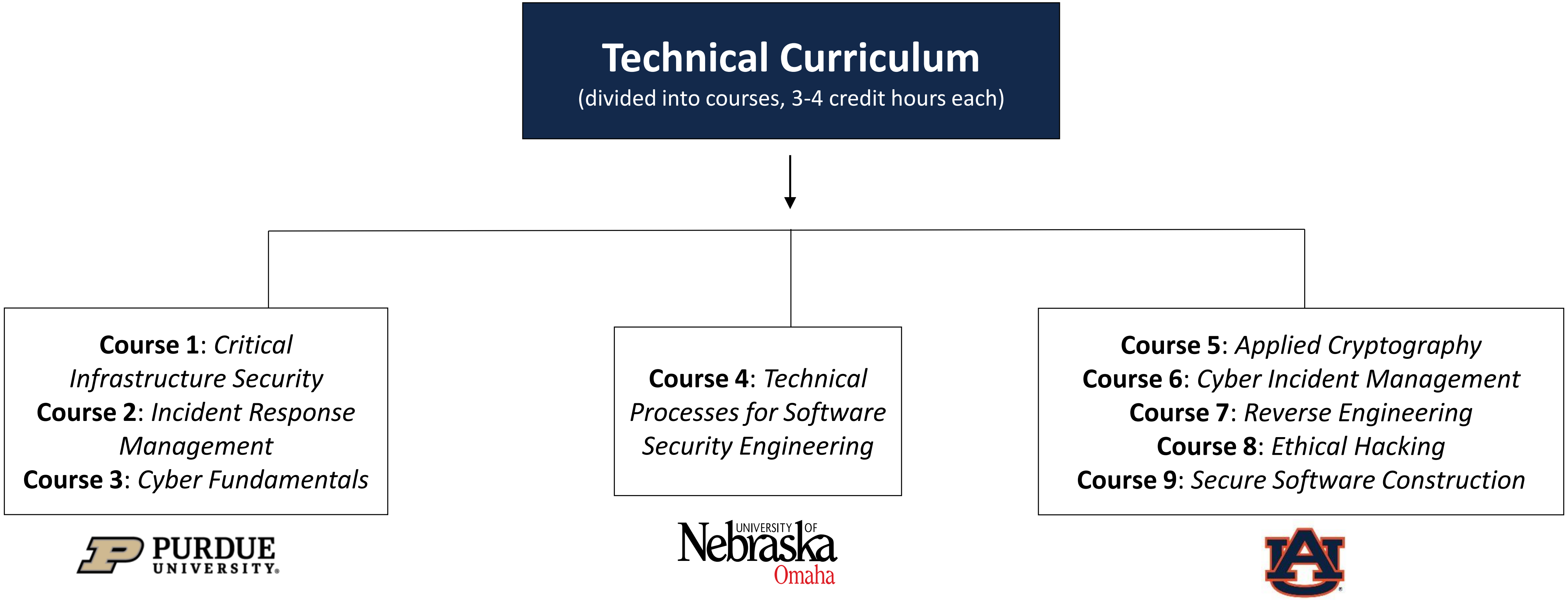
Course 1: *Foundations in Secure Networking for Cyber-Social Systems*

Course 2: *Foundations in Secure Administration of Cyber-Social Systems*

Course 3: *Foundational Technical and Organizational Concepts and Practices in Cybersecurity*

The Foundational Curriculum is comprised of these 3 courses

Hybrid Curriculum



Technical Curriculum
(divided into courses, 3-4 credit hours each)

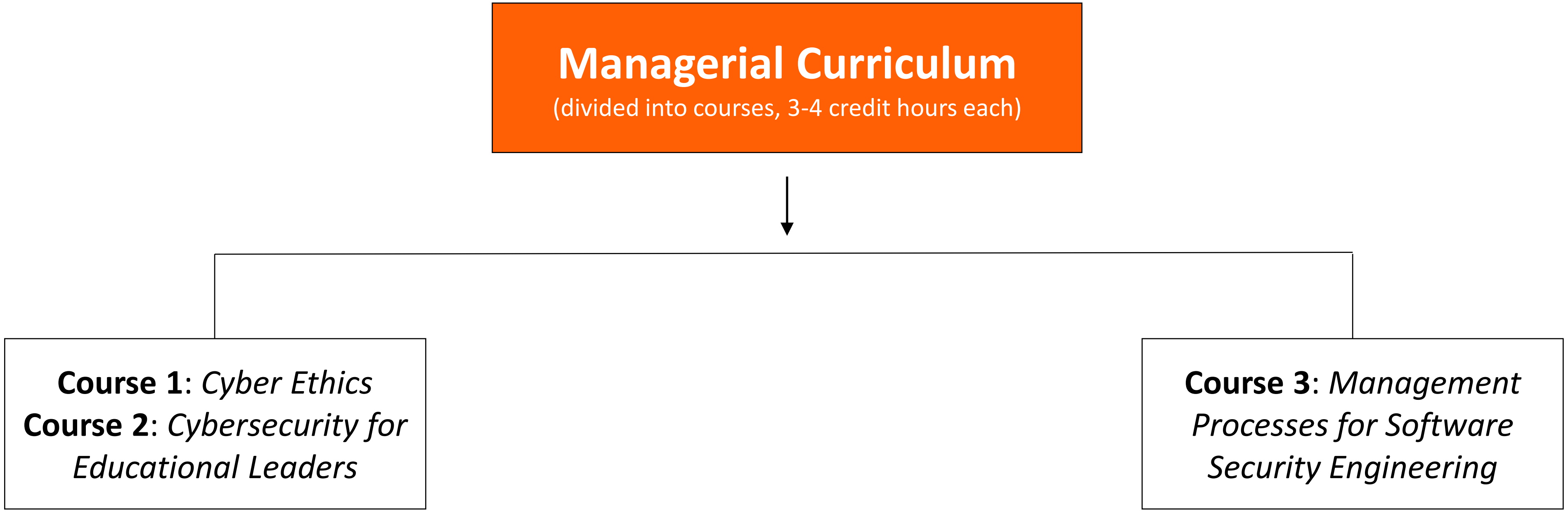
Course 1: *Critical Infrastructure Security*
Course 2: *Incident Response Management*
Course 3: *Cyber Fundamentals*

Course 4: *Technical Processes for Software Security Engineering*

Course 5: *Applied Cryptography*
Course 6: *Cyber Incident Management*
Course 7: *Reverse Engineering*
Course 8: *Ethical Hacking*
Course 9: *Secure Software Construction*

The Technical Curriculum is comprised of these 9 courses

Hybrid Curriculum



Managerial Curriculum
(divided into courses, 3-4 credit hours each)

Course 1: *Cyber Ethics*
Course 2: *Cybersecurity for Educational Leaders*

Course 3: *Management Processes for Software Security Engineering*

Wilkes University

University of Nebraska Omaha

The Managerial Curriculum is comprised of these 3 courses

Curriculum Development Project Deliverables

- Author Guide, Framework Mappings (NICE), Curriculum Development Lifecycle Recommendations
- 17 courses (136 training modules), with…
- …curriculum resources: Video lectures, hands-on activities, assessments, etc.
- Flexibly designed for both in-person and online delivery

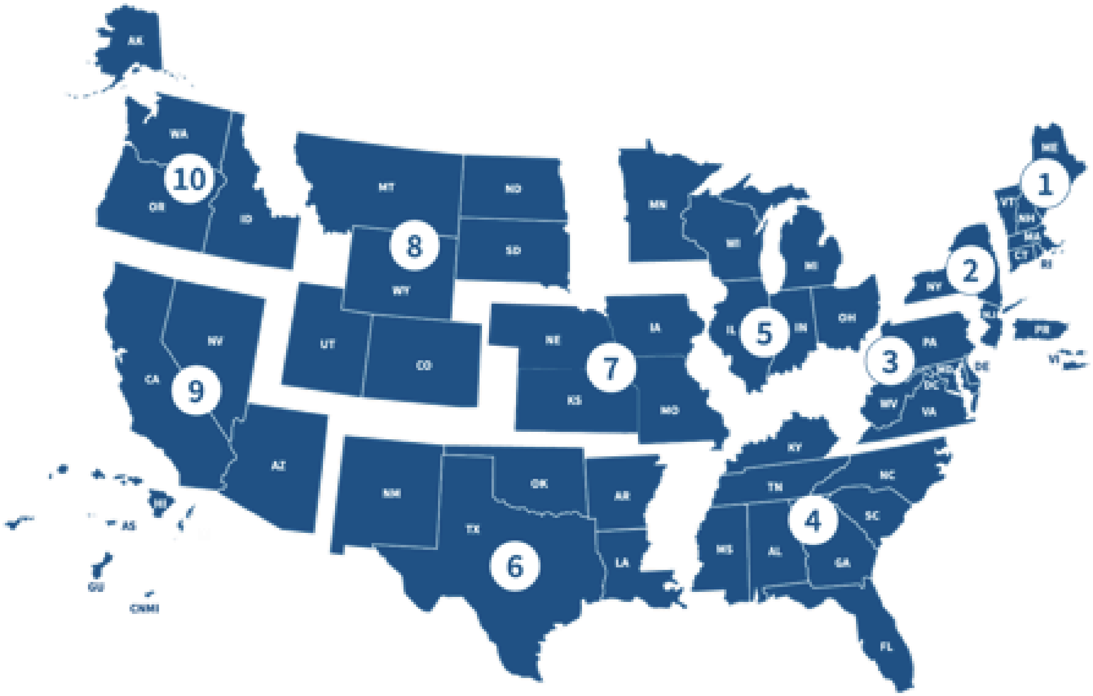
Recommendations for a Phase 3

- Implementation, pilot & dissemination of Phase 2 courses/content
- Curriculum sharing architecture & platform for delivery and dissemination of the course materials via a common infrastructure, **CyberEd Bridge**
- Chunking of course content into training module (136)

What’s Next?

Grow the CIRI National Network

- Support both the management and running of the national Hub & Spoke network, as well as the curation and delivery of the curricula developed



Implement Partner Education & Training Program

- **Executive Summary**:
  - Creating cutting-edge education, training delivery systems, and content that results in a diverse pool of talent with skills needed to protect organizations and improve national security

Implement Partner Education & Training Program

- **Problem Statement**:
  - Organizations struggle to find, develop, and retain desperately needed talent (e.g., Cybersecurity)
  - Aging workforce of highly-skilled and experienced workers
  - Attracting new and more diverse talent pools
  - Closing gaps in workers' skills and credentials

Implement Partner Education & Training Program

- **Problem Statement (con’t)**:
  - Investing in talent that can keep pace with the latest industry advances
  - Implementing workforce training models that effectively develop and "up-skill"

Implement Partner Education & Training Program

- **Problem Statement (con’t)**:
  - Current commercial training/offerings:
    - Focus on tip of the spear/specialists, in short supply
    - Don’t leverage Learning Science or evidence-based practices
    - One-size does not fit all

Implement Partner Education & Training Program

- Includes an interconnected set of solutions to meet employment needs:
  - *What are the populations being served?*
  - *What are these interconnected set of solutions?*
  - *What differentiates our solution from others in the marketplace?*

Implement Partner Education & Training Program

- **Populations Served**:
  - IT workers looking to transition into in-demand and hard to fill work roles (e.g., Cybersecurity) - 7 million IT workers in U.S.
  - Industrial Control Systems asset owners and operators
  - 911 call center operators

Implement Partner Education & Training Program

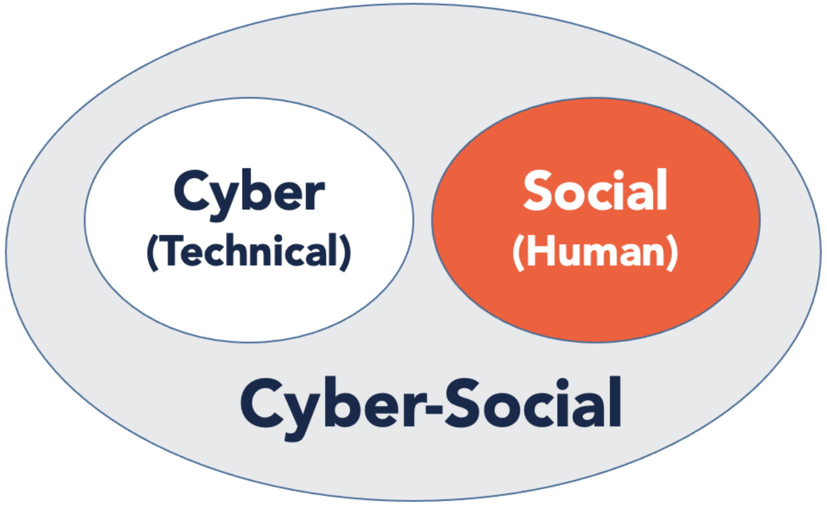
- **Additional Learner Populations**:
  - Career changers
  - Chief Human Information Capital Officers (CHICOs), HR
  - Underrepresented populations
  - Degree/certificate-seeking students

Implement Partner Education & Training Program

- **Employer Partners**:
  - Federal, State, Local, Tribal and Territorial government entities
  - K-12 and higher education
  - Regional technology councils
  - Professional & technology services
  - Non-profit organizations

Implement Partner Education & Training Program

- **Differentiators**: Cyber-Social:
  - Captures the relationship between computers (or computerized machinery) and their users
  - Technical + Human (Social) + Organizational

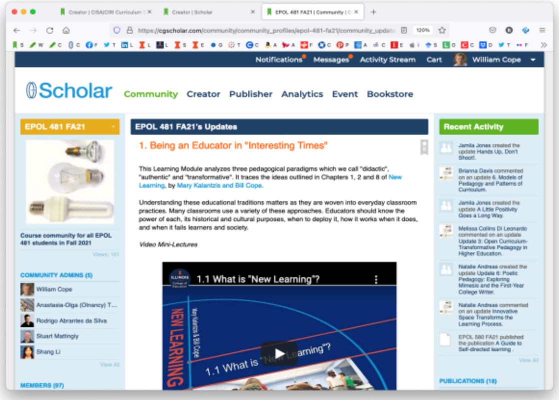


Implement Partner Education & Training Program

- **Differentiators**: Mastery-Focused:
  - *Mastery* of core concepts vs. *coverage* of 1,000s of concepts
  - Not trying to boil the ocean

Implement Partner Education & Training Program

- **Differentiators**: Blending Learning Science with Technological Advancements:
  - **Dialogical**: Learners respond to content inputs (lecture videos, readings, links) via discussions and select response surveys


Creator | CISA/CIRI Curriculum
Creator | Scholar
EPOL 481 FA21 | Community |
https://cgscholar.com/community/community_profiles/epol-481-fa21/community_update
120%
Notifications
Messages
Activity Stream
Cart
William Cope
Scholar
Community
Creator
Publisher
Analytics
Event
Bookstore
1.1 What is "New Learning"?
NEW LEARNING
Mary Kalantzis & Bill Cope
1.1 What is "New Learning"?

EPOL 481 FA21

Course community for all EPOL 481 students in Fall 2021

Views: 101

COMMUNITY ADMINS (5)

William Cope
Anastasia-Olga (Olnancy) T...
Rodrigo Abrantes da Silva
Stuart Mattingly
Shang Li

View All

MEMBERS (97)

EPOL 481 FA21's Updates

1. Being an Educator in "Interesting Times"

This Learning Module analyzes three pedagogical paradigms which we call "didactic", "authentic" and "transformative". It traces the ideas outlined in Chapters 1, 2 and 8 of New Learning, by Mary Kalantzis and Bill Cope.

Understanding these educational traditions matters as they are woven into everyday classroom practices. Many classrooms use a variety of these approaches. Educators should know the power of each, its historical and cultural purposes, when to deploy it, how it works when it does, and when it fails learners and society.

Video Mini-Lectures

Recent Activity

Jamila Jones created the update Hands Up, Don't Shoot!.

Brianna Davis commented on an update 6. Models of Pedagogy and Patterns of Curriculum.

Jamila Jones created the update A Little Positivity Goes a Long Way.

Melissa Collins Di Leonardo commented on an update Update 3: Open Curriculum-Transformative Pedagogy in Higher Education.

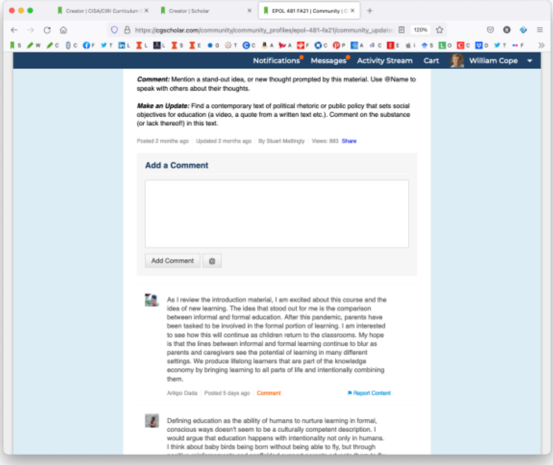
Natalie Andreas created the update Update 6: Poetic Pedagogy: Exploring Mimesis and the First-Year College Writer.

Natalie Andreas commented on an update Innovative Space Transforms the Learning Process.

EPOL 580 FA21 published the publication A Guide to Self-directed learning .

View All

PUBLICATIONS (18)


Creator | CISA/CIRI Curriculum
Creator | Scholar
EPOL 481 FA21 | Community |
https://cgscholar.com/community/community_profiles/epol-481-fa21/community_update
120%
Notifications
Messages
Activity Stream
Cart
William Cope
Add Comment

Comment: Mention a stand-out idea, or new thought prompted by this material. Use @Name to speak with others about their thoughts.

Make an Update: Find a contemporary text of political rhetoric or public policy that sets social objectives for education (a video, a quote from a written text etc.). Comment on the substance (or lack thereof!) in this text.

Posted 2 months ago | Updated 2 months ago | By Stuart Mattingly | Views: 883 Share

Add a Comment

As I review the introduction material, I am excited about this course and the idea of new learning. The idea that stood out for me is the comparison between informal and formal education. After this pandemic, parents have been tasked to be involved in the formal portion of learning. I am interested to see how this will continue as children return to the classrooms. My hope is that the lines between informal and formal learning continue to blur as parents and caregivers see the potential of learning in many different settings. We produce lifelong learners that are part of the knowledge economy by bringing learning to all parts of life and intentionally combining them.

Arikpo Dada | Posted 5 days ago | Comment ⚑ Report Content

Defining education as the ability of humans to nurture learning in formal, conscious ways doesn't seem to be a culturally competent description. I would argue that education happens with intentionality not only in humans. I think about baby birds being born without being able to fly, but through

Implement Partner Education & Training Program

- **Differentiators**: Blending Learning Science with Technological Advancements:
    - **Collaborative**: Projects and labs involve peer review

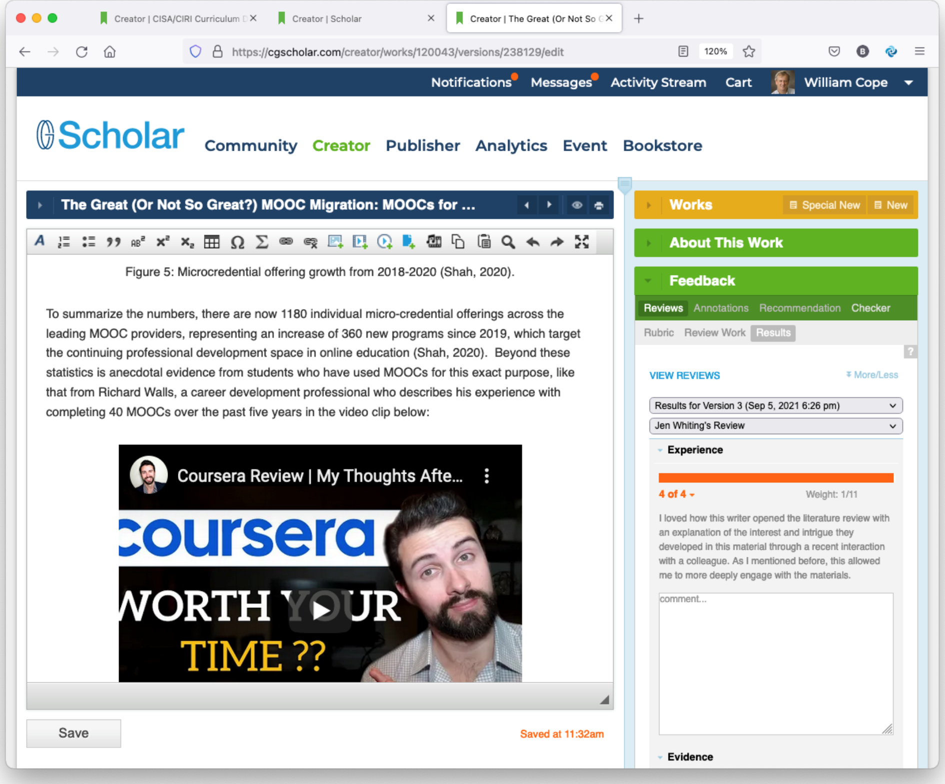


Figure 5: Microcredential offering growth from 2018-2020 (Shah, 2020).

To summarize the numbers, there are now 1180 individual micro-credential offerings across the leading MOOC providers, representing an increase of 360 new programs since 2019, which target the continuing professional development space in online education (Shah, 2020). Beyond these statistics is anecdotal evidence from students who have used MOOCs for this exact purpose, like that from Richard Walls, a career development professional who describes his experience with completing 40 MOOCs over the past five years in the video clip below:

Results for Version 3 (Sep 5, 2021 6:26 pm)

Jen Whiting's Review

Experience

4 of 4 Weight: 1/11

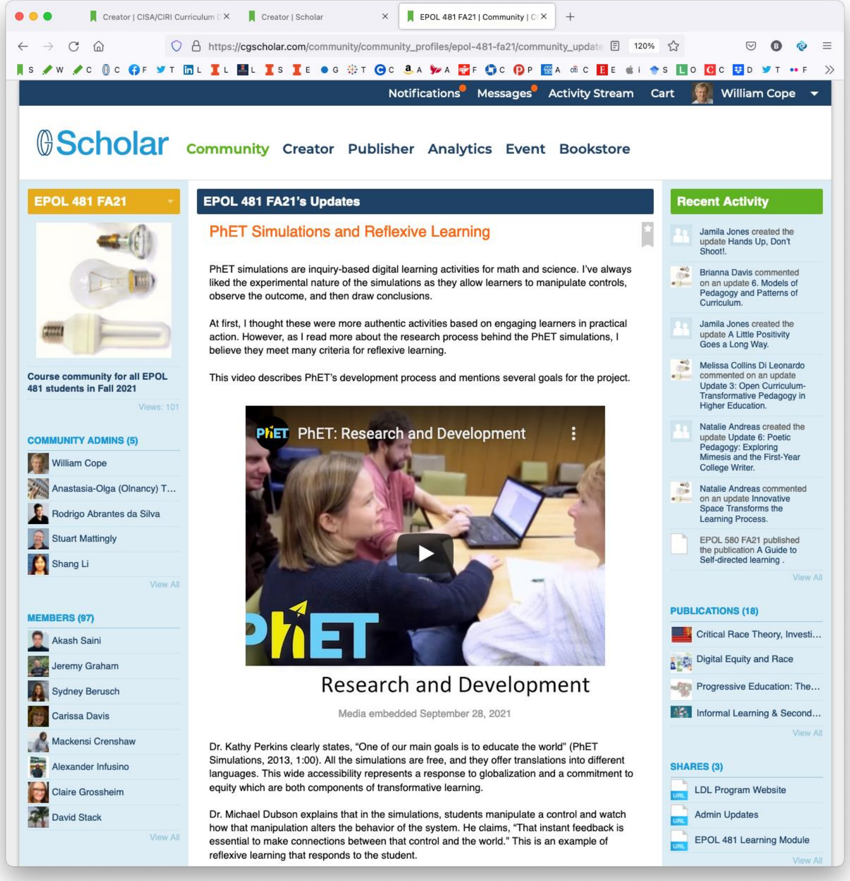
I loved how this writer opened the literature review with an explanation of the interest and intrigue they developed in this material through a recent interaction with a colleague. As I mentioned before, this allowed me to more deeply engage with the materials.

comment...

Evidence

Implement Partner Education & Training Program

- **Differentiators**: Blending Learning Science with Technological Advancements:
    - **Knowledge co-constructed by learners**: Everyone researches topics and contributes content


Creator | CISA/CIRI Curriculum D
Creator | Scholar
EPOL 481 FA21 | Community | C
https://cgscholar.com/community/community_profiles/epol-481-fa21/community_update
120%
Notifications
Messages
Activity Stream
Cart
William Cope
Scholar
Community
Creator
Publisher
Analytics
Event
Bookstore
PhET: Research and Development
PhET

EPOL 481 FA21

Course community for all EPOL 481 students in Fall 2021

Views: 101

COMMUNITY ADMINS (5)

- William Cope
- Anastasia-Olga (Olnancy) T…
- Rodrigo Abrantes da Silva
- Stuart Mattingly
- Shang Li

View All

MEMBERS (97)

- Akash Saini
- Jeremy Graham
- Sydney Berusch
- Carissa Davis
- Mackensi Crenshaw
- Alexander Infusino
- Claire Grossheim
- David Stack

View All

EPOL 481 FA21's Updates

PhET Simulations and Reflexive Learning

PhET simulations are inquiry-based digital learning activities for math and science. I've always liked the experimental nature of the simulations as they allow learners to manipulate controls, observe the outcome, and then draw conclusions.

At first, I thought these were more authentic activities based on engaging learners in practical action. However, as I read more about the research process behind the PhET simulations, I believe they meet many criteria for reflexive learning.

This video describes PhET's development process and mentions several goals for the project.

Research and Development

Media embedded September 28, 2021

Dr. Kathy Perkins clearly states, "One of our main goals is to educate the world" (PhET Simulations, 2013, 1:00). All the simulations are free, and they offer translations into different languages. This wide accessibility represents a response to globalization and a commitment to equity which are both components of transformative learning.

Dr. Michael Dubson explains that in the simulations, students manipulate a control and watch how that manipulation alters the behavior of the system. He claims, "That instant feedback is essential to make connections between that control and the world." This is an example of reflexive learning that responds to the student.

Recent Activity

- Jamila Jones created the update Hands Up, Don't Shoot!.
- Brianna Davis commented on an update 6. Models of Pedagogy and Patterns of Curriculum.
- Jamila Jones created the update A Little Positivity Goes a Long Way.
- Melissa Collins Di Leonardo commented on an update Update 3: Open Curriculum-Transformative Pedagogy in Higher Education.
- Natalie Andreas created the update Update 6: Poetic Pedagogy: Exploring Mimesis and the First-Year College Writer.
- Natalie Andreas commented on an update Innovative Space Transforms the Learning Process.
- EPOL 580 FA21 published the publication A Guide to Self-directed learning .

View All

PUBLICATIONS (18)

- Critical Race Theory, Investi…
- Digital Equity and Race
- Progressive Education: The…
- Informal Learning & Second…

View All

SHARES (3)

- LDL Program Website
- Admin Updates
- EPOL 481 Learning Module

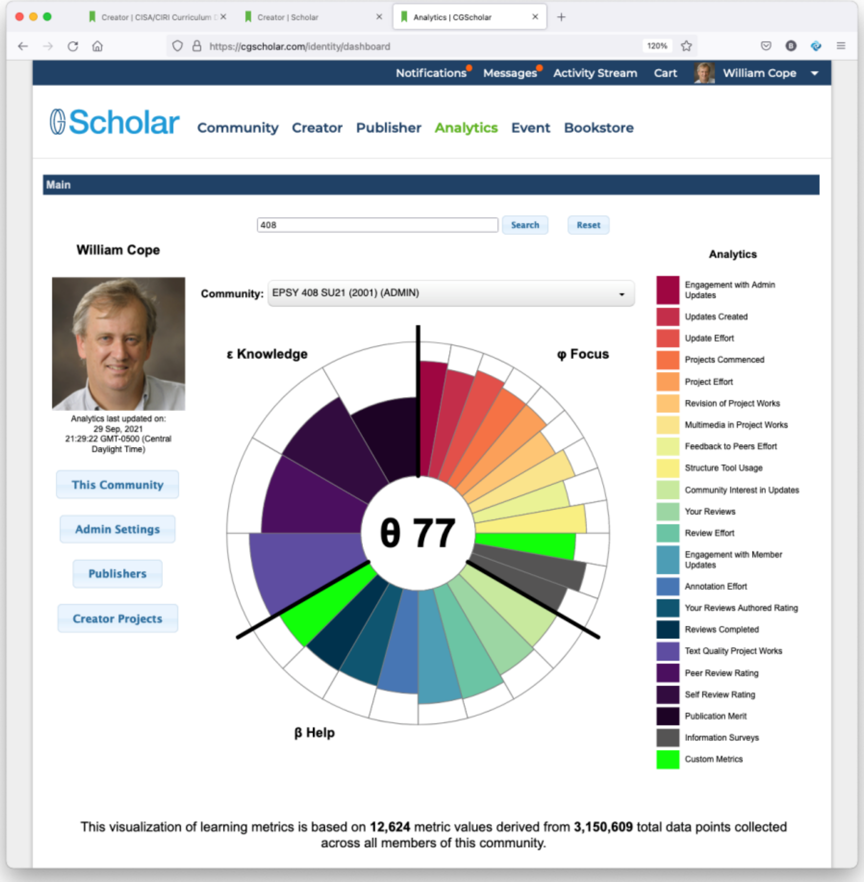
View All

Implement Partner Education & Training Program

- **Differentiators**: Advanced Learning Analytics:
  - Continuous assessment
  - Peer, machine, and instructor feedback
  - Formative assessments (for learning, not just of learning)
  - Incremental progress visualization - think “learning fitness tracker”

Implement Partner Education & Training Program

- **Differentiators**: Advanced Learning Analytics



Analytics last updated on: 29 Sep, 2021 21:29:22 GMT-0500 (Central Daylight Time)

Community: EPSY 408 SU21 (2001) (ADMIN)

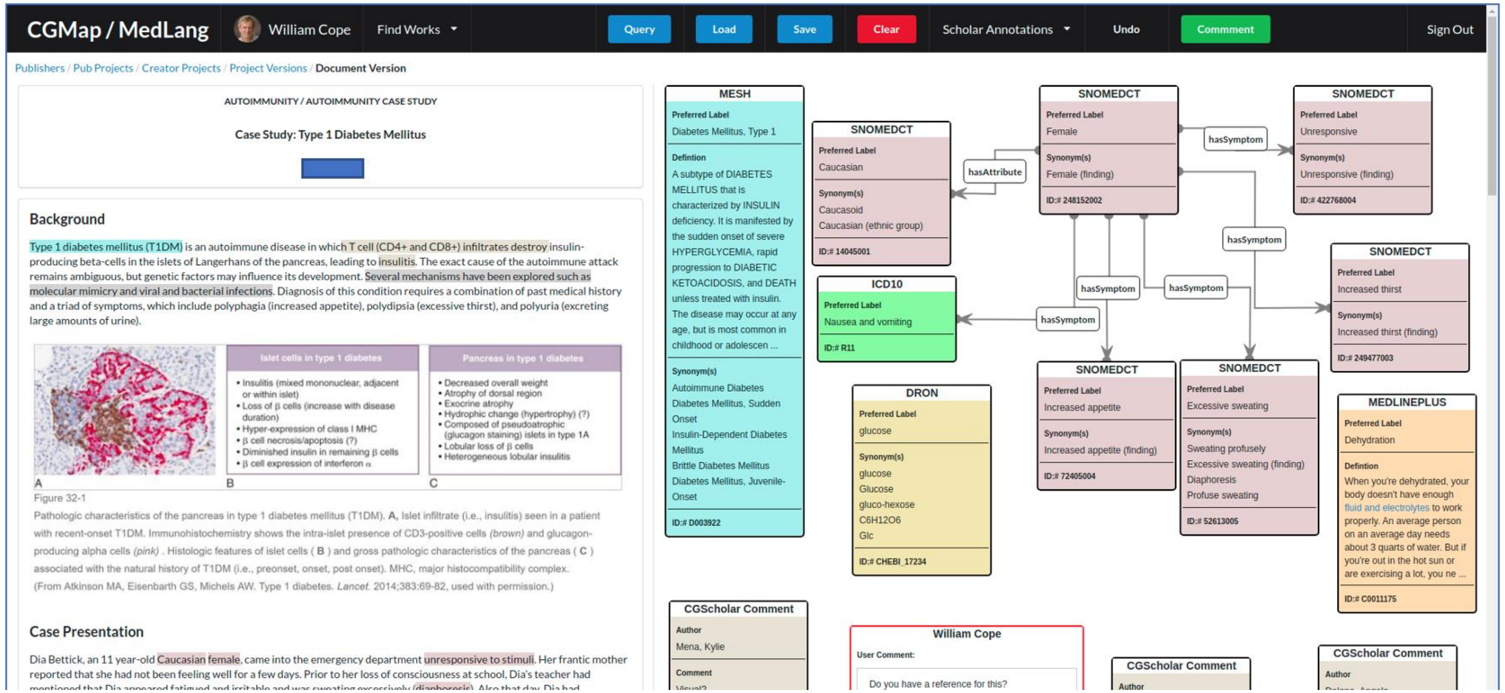
This visualization of learning metrics is based on **12,624** metric values derived from **3,150,609** total data points collected across all members of this community.

Implement Partner Education & Training Program

- **Differentiators**:

  Standards-Aligned

  Concept Mapping



AUTOIMMUNITY / AUTOIMMUNITY CASE STUDY

Case Study: Type 1 Diabetes Mellitus

Background

Type 1 diabetes mellitus (T1DM) is an autoimmune disease in which T cell (CD4+ and CD8+) infiltrates destroy insulin-producing beta-cells in the islets of Langerhans of the pancreas, leading to insulitis. The exact cause of the autoimmune attack remains ambiguous, but genetic factors may influence its development. Several mechanisms have been explored such as molecular mimicry and viral and bacterial infections. Diagnosis of this condition requires a combination of past medical history and a triad of symptoms, which include polyphagia (increased appetite), polydipsia (excessive thirst), and polyuria (excreting large amounts of urine).

A

B

Islet cells in type 1 diabetes

- Insulitis (mixed mononuclear, adjacent or within islet)
- Loss of β cells (increase with disease duration)
- Hyper-expression of class I MHC
- β cell necrosis/apoptosis (?)
- Diminished insulin in remaining β cells
- β cell expression of interferon α

C

Pancreas in type 1 diabetes

- Decreased overall weight
- Atrophy of dorsal region
- Exocrine atrophy
- Hydrophic change (hypertrophy) (?)
- Composed of pseudoatrophic (glucagon staining) islets in type 1A
- Lobular loss of β cells
- Heterogeneous lobular insulitis

Figure 32-1

Pathologic characteristics of the pancreas in type 1 diabetes mellitus (T1DM). **A,** Islet infiltrate (i.e., insulitis) seen in a patient with recent-onset T1DM. Immunohistochemistry shows the intra-islet presence of CD3-positive cells *(brown)* and glucagon-producing alpha cells *(pink)* . Histologic features of islet cells (**B**) and gross pathologic characteristics of the pancreas (**C**) associated with the natural history of T1DM (i.e., preonset, onset, post onset). MHC, major histocompatibility complex. (From Atkinson MA, Eisenbarth GS, Michels AW. Type 1 diabetes. *Lancet.* 2014;383:69-82, used with permission.)

Case Presentation

Dia Bettick, an 11 year-old Caucasian female, came into the emergency department unresponsive to stimuli. Her frantic mother reported that she had not been feeling well for a few days. Prior to her loss of consciousness at school, Dia's teacher had mentioned that Dia appeared fatigued and irritable and was sweating excessively (diaphoresis). Also that day, Dia had

MESH
Preferred Label
Diabetes Mellitus, Type 1
Defintion
A subtype of DIABETES MELLITUS that is characterized by INSULIN deficiency. It is manifested by the sudden onset of severe HYPERGLYCEMIA, rapid progression to DIABETIC KETOACIDOSIS, and DEATH unless treated with insulin. The disease may occur at any age, but is most common in childhood or adolescen ...
Synonym(s)
Autoimmune Diabetes
Diabetes Mellitus, Sudden Onset
Insulin-Dependent Diabetes Mellitus
Brittle Diabetes Mellitus
Diabetes Mellitus, Juvenile-Onset
ID:# D003922

SNOMEDCT
Preferred Label
Caucasian
Synonym(s)
Caucasoid
Caucasian (ethnic group)
ID:# 14045001

ICD10
Preferred Label
Nausea and vomiting
ID:# R11

DRON
Preferred Label
glucose
Synonym(s)
glucose
Glucose
gluco-hexose
C6H12O6
Glc
ID:# CHEBI_17234

SNOMEDCT
Preferred Label
Female
Synonym(s)
Female (finding)
ID:# 248152002

SNOMEDCT
Preferred Label
Unresponsive
Synonym(s)
Unresponsive (finding)
ID:# 422768004

SNOMEDCT
Preferred Label
Increased thirst
Synonym(s)
Increased thirst (finding)
ID:# 249477003

SNOMEDCT
Preferred Label
Increased appetite
Synonym(s)
Increased appetite (finding)
ID:# 72405004

SNOMEDCT
Preferred Label
Excessive sweating
Synonym(s)
Sweating profusely
Excessive sweating (finding)
Diaphoresis
Profuse sweating
ID:# 52613005

MEDLINEPLUS
Preferred Label
Dehydration
Defintion
When you're dehydrated, your body doesn't have enough fluid and electrolytes to work properly. An average person on an average day needs about 3 quarts of water. But if you're out in the hot sun or are exercising a lot, you ne ...
ID:# C0011175

CGScholar Comment
Author
Mena, Kylie
Comment
Visual?

William Cope
User Comment:
Do you have a reference for this?

CGScholar Comment
Author

CGScholar Comment
Author

Implement Partner Education & Training Program

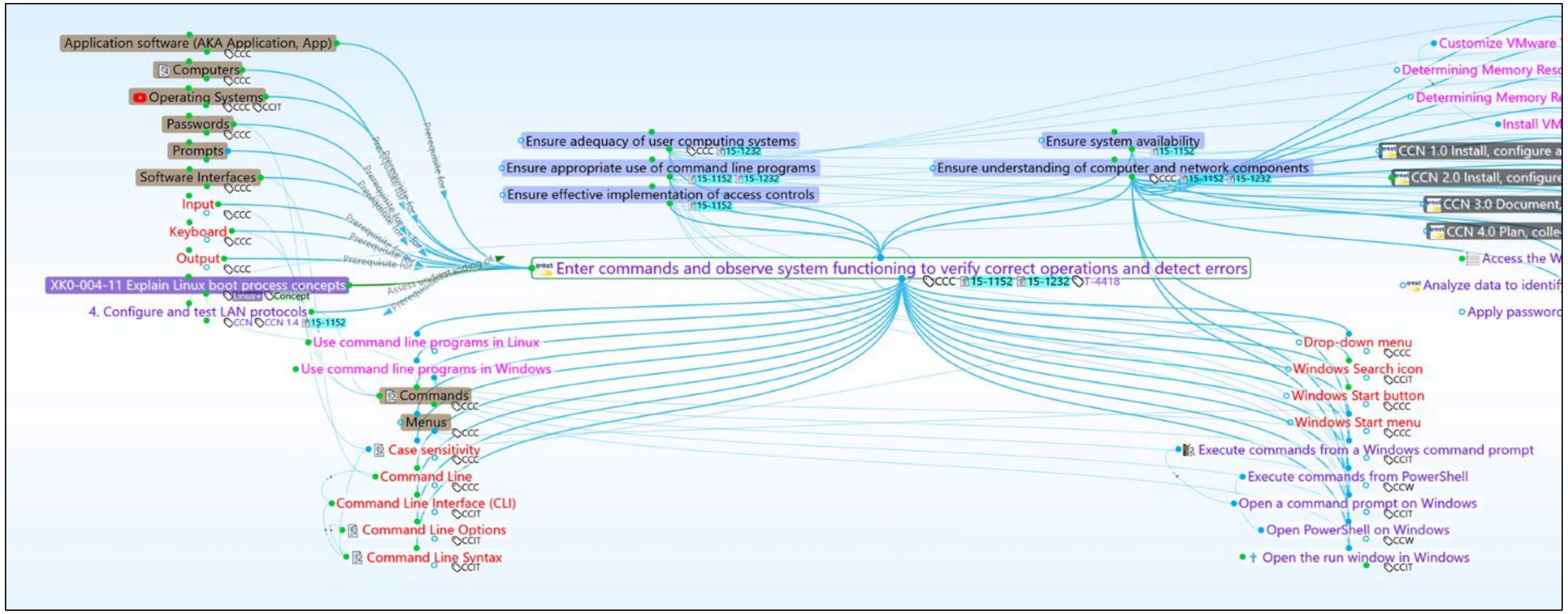
- **Differentiators**:

  Course Content

  Mapped to In-

  Demand Work

  Role Tasks


Application software (AKA Application, App)
CCC
Computers
CCC
Operating Systems
CCC CCIT
Passwords
CCC
Prompts
Software Interfaces
CCC
Input
CCC
Keyboard
CCC
Output
CCC
XK0-004-11 Explain Linux boot process concepts
Linux+ Concept
4. Configure and test LAN protocols
CCN CCN 1.4 15-1152
Prerequisite for
Assess understanding of
Ensure adequacy of user computing systems
CCC 15-1232
Ensure appropriate use of command line programs
15-1152 15-1232
Ensure effective implementation of access controls
15-1152
Ensure system availability
15-1152
Ensure understanding of computer and network components
CCC 15-1152 15-1232
Enter commands and observe system functioning to verify correct operations and detect errors
CCC 15-1152 15-1232 T-4418
Customize VMware
Determining Memory Reso
Determining Memory Re
Install VM
CCN 1.0 Install, configure a
CCN 2.0 Install, configure
CCN 3.0 Document,
CCN 4.0 Plan, colle
Access the W
Analyze data to identif
Apply passwor
Use command line programs in Linux
Use command line programs in Windows
Commands
CCC
Menus
CCC
Case sensitivity
CCC
Command Line
CCC
Command Line Interface (CLI)
CCIT
Command Line Options
CCIT
Command Line Syntax
CCIT
Drop-down menu
CCC
Windows Search icon
CCIT
Windows Start button
CCC
Windows Start menu
CCC
Execute commands from a Windows command prompt
CCIT
Execute commands from PowerShell
CCW
Open a command prompt on Windows
CCIT
Open PowerShell on Windows
CCW
Open the run window in Windows
CCIT

Implement Partner Education & Training Program

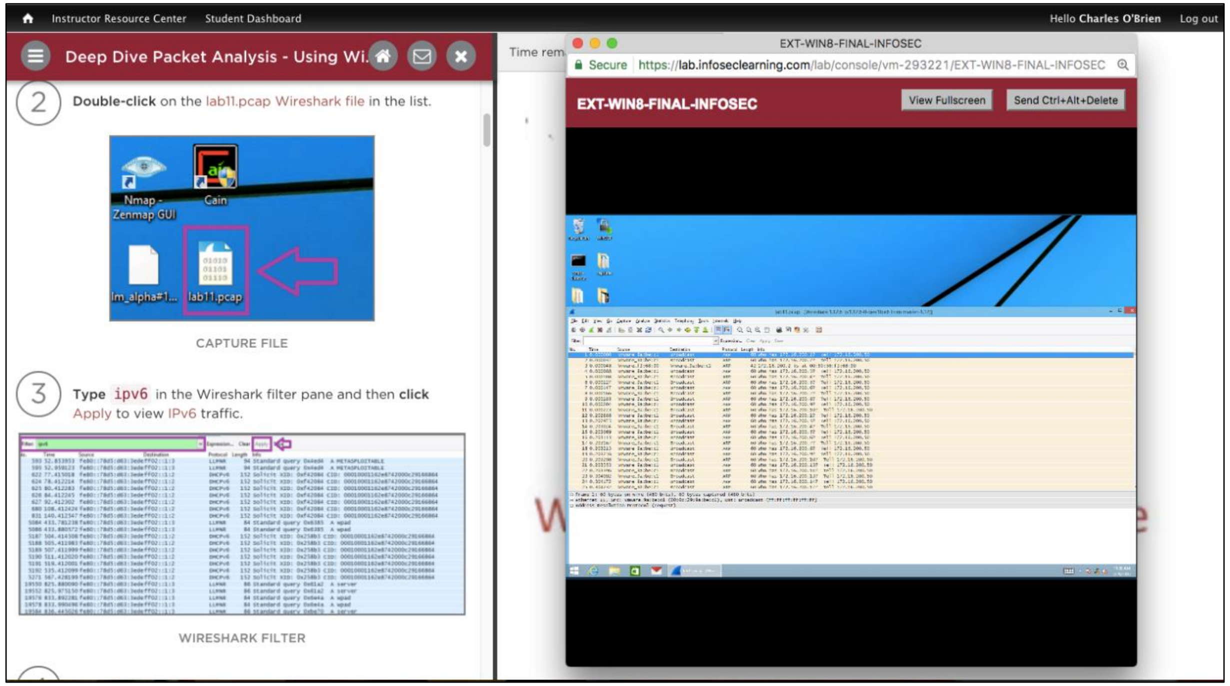
- **Differentiators**: Assessment-Driven:
  - Course Readiness Assessments
  - In-course diagnostic assessments
  - Personalizes the learning path

Foundational Tasks	Composite score	Comparative score
Identify ownership of gateway devices (16.77)	83.8	Average
Identify recon that is within project scope (15.63)	46.8	Low
Search online sources for useful information about a target (15.45)	53.5	Average
Differentiating Tasks (with weights)		
Analyze data found on compromised machines to enable exploitation deeper into the network (24.02)	36.0	Average
Identify major assets subject to attacks (23.67)	87.2	High
Identify targets for potential exploitation (23.67)	56.0	High
Analyze data found on compromised machines for strategic value as seen by a worst case attacker (23.60)	26.2	Low
Overall Score		
My Score	54.9	Average

Vmetrics

Implement Partner Education & Training Program

- **Differentiators**: Performance-Based:
  - Cloud-based lab platform
  - Real systems, tools
  - LTI, SSO
  - 24 x 7 support



2 **Double-click** on the lab11.pcap Wireshark file in the list.

CAPTURE FILE

3 **Type** ipv6 in the Wireshark filter pane and then **click** Apply to view IPv6 traffic.

WIRESHARK FILTER

Implement Partner Education & Training Program

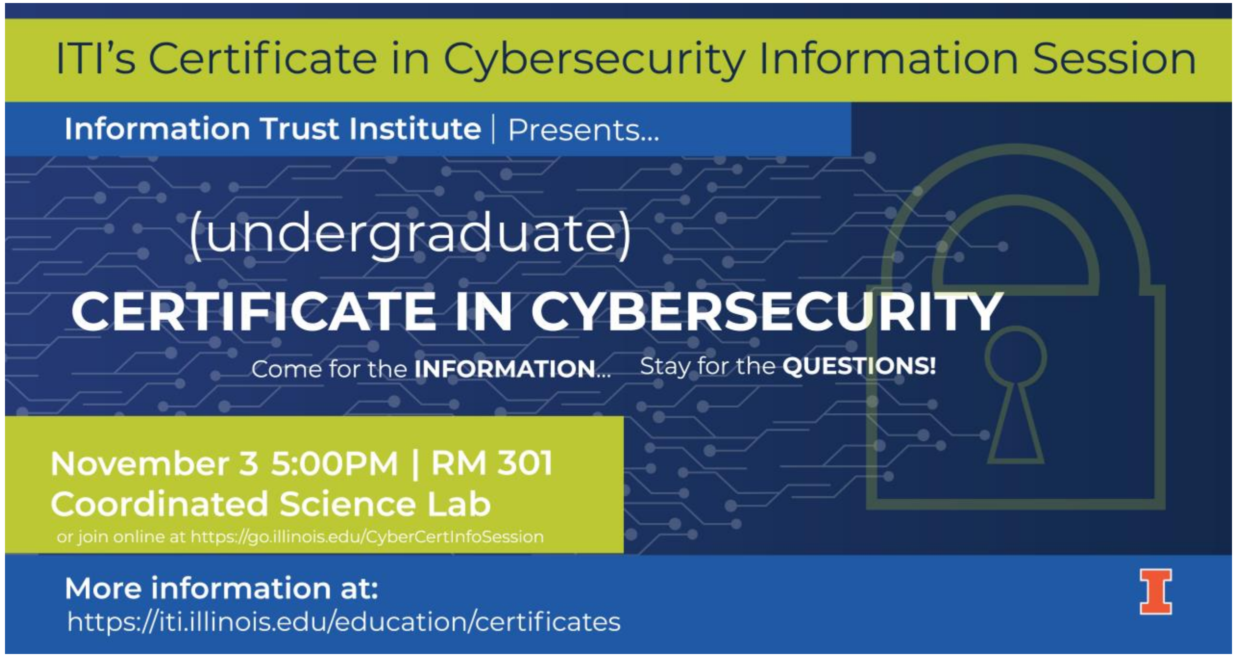
- **Courses**:
  - Credit and non-credit offerings
  - Fully online, in-person, hybrid

Implement Partner Education & Training Program

- **Courses (con’t)**:
  - *Foundations in Cybersecurity*: 1-2 hours
  - *NIST Cybersecurity Framework (CSF)*: 1-2 hours
  - *Cyber Secure Dashboard*: 1-2 hours

Implement Partner Education & Training Program

- **Specialized Certificates**:
  - Campus Graduate CERT in Cybersecurity
  - ITI small “c” certificate(s)
  - Multi-disciplinary: Gies, ECE, Education, iSchool



ITI’s Certificate in Cybersecurity Information Session

Information Trust Institute | Presents...

(undergraduate)

CERTIFICATE IN CYBERSECURITY

Come for the **INFORMATION**... Stay for the **QUESTIONS!**

November 3 5:00PM | RM 301
Coordinated Science Lab
or join online at https://go.illinois.edu/CyberCertInfoSession

More information at:
https://iti.illinois.edu/education/certificates

Contact Information

Casey W. O’Brien

Assistant Director, Cyber Defense Education and Training

Information Trust Institute

University of Illinois Urbana-Champaign

cwobrien@Illinois.edu

+1-443-610-7775

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

CIRI Annual Meeting
December 6-7, 2022

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Annual Review: Resilient Timing Requirement Study for 5G Networks and Interoperability with Equipment that Uses GPS/GNSS for Positioning, Navigation, and Timing

M. Scott Sotebeer, PhD
Endicott Consulting

The Problem

- Increasing reliance and overdependence on government-supplied GPS Positioning, Navigation, and Timing (PNT) signals. 5g is the multiplier.
- Unintended vulnerabilities and “blind spots” in critical infrastructure- from commerce to transportation, the power grid, and communications.

- CISA seeks to understand and evaluate from industry, current 5g timing requirements, alternative backup sources, and issues of government supplied backup sources.
- Approach: critical team/critical knowledge.
    - Only works with carrier technology leadership; industry PNT/Timing experts; academia (unbiased/unfiltered analysis); DHS CISA/S&T partner.

What Will Success Look Like?

- A comprehensive, technical analysis of 5g timing requirements from one or more of the major carriers: T-Mobile, Verizon, AT&T.
- Identification of alternative backup timing requirements/sources.
- A comprehensive analysis of any issues/vulnerabilities with proposed government alternate timing sources: physical/technical environment, social implications, legal implications and framework, and economic requirements and implications.
- Industry and expert supported go/no-go decision framework for lab evaluation and testing of government supplied alternative timing sources.

Benefits

- Technical insight and knowledge – 5g carrier timing and backup requirements.
  - New tools for risk and vulnerability analysis – Critical Infrastructure.
  - Evaluation of carrier backup and government solution.
  - If compatible/desirable, more robust back timing alternatives shared between government and industry– accelerated redundancy and resiliency.
- Comprehensive analysis of current state of alternative timing sources: LEO, eLoran, Networks/fiber, Signals of Opportunity, etc.
- Demonstration framework for lab evaluation of government backup timing sources.

Accomplishments

Organized advisory of essential industry PNT/Timing technical and thought leaders including:

- Resilient Navigation & Timing Foundation
- Institute of Navigation: Precise Time and Time Interval Systems and Applications
- Microchip Technology
- University of Washington Computer Sciences/STEM (lab eval)
- Senior Director of Product Security, Cybersecurity Trust and Protection (CTP), T-Mobile
- President, Technology, T-Mobile

Activities Remaining

This is an 18-month project. We are focusing on critical milestones and key decision points.

First 120 days

- Convene working group.
- Create topical knowledge library.
- Create technical approach and analysis framework.
- Begin initial inquiry and learning process with carrier.
- Evaluate inputs and process for carrier engagement on technical timing and backup requirements.

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Annual Review: **BACKUP NETWORK TIMING FOR MISSION CRITICAL P25 LMR NETWORKS**

Walt Magnussen, Ph.D.
Texas A&M University
Internet2 Technology Evaluation Center

The Problem

- Statement of the problem:
  - Many critical infrastructure systems are heavily dependent upon the Global Positioning System (GPS) system established in the 1970s for navigation. NG-911 relies on it for location in call routing, public safety communications systems require it for timing of Land Mobile Radio (LMR) and Public Safety Broadband Networks and many applications embed GPS based location services in their user interface. This GPS systems have vulnerabilities that stem from jamming, spoofing, inability to see enough of the constellation to determine an accurate location and other issues. This project does a survey of potential alternatives that could be used to mitigate these vulnerabilites.
  - This project has impact upon all DHS components (FEMA, Coast Guard etc.), Department of Defense, Department of Transportation, FCC and others.

- How are you approaching it, and what makes your approach unique?
  - We have engaged a faculty member with extensive background in PNT (Dr. Radu Stoleru) and we are leveraging the industry support that we have established over the years.

What Will Success Look Like?

- Success would be a comprehensive review of all of PNT requirements and a report documention of the potential alternatives for Positioning, Navigation and Timing (PNT) solutions
- A successful project would also include a recommendation for a PNT testbed that included at least two or three of the leading technologies. This recommendation would include a testbed design and projected pricing of both the testbed as well as a nation-wide implementation of recommended technologies.

Benefits

- How will success benefit the Homeland Security Enterprise?
- The results of this project should lead to recommendations that could help United States leadership make informed decisions on future investments in PNT augmentation and enhancement.

Accomplishments

- Project strategy meetings
- Determination of makeup of stakeholders group.

Activities Remaining

- Document network requirements for PNT data acquisition and distribution.
- Information gathering, data analysis and documentation of PNT alternatives.
- Provide a technology comparison matrix for the solutions researched.
- Provide recommendations for a potential Phase II testbed that would establish a PNT Testbed.

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

David M. Nicol, PhD
Herman M. Dieckamp Endowed Chair in Engineering
Director, Critical Infrastructure Resilience Institute
Director, Information Trust Institute
University of Illinois at Urbana Champaign

Virtualized ICS Testbed for Research, Training, and Education

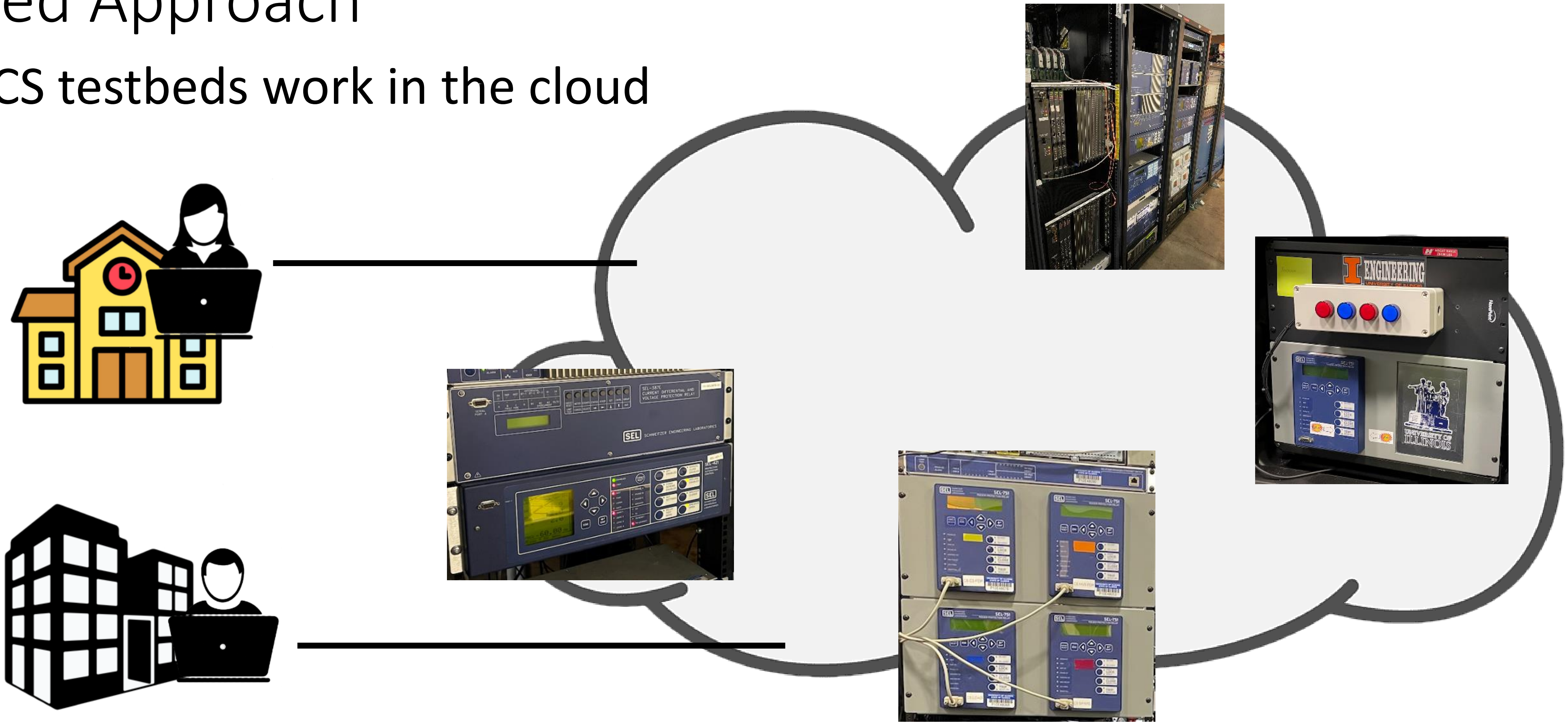
CIRI Annual Meeting
December 2022

The Problem

- Industrial control systems use specialized hardware/software
- ICS workforce desperately needs **hands-on** cyber-security training
- **On-site** training does not scale
- **Cloud-based** training is not currently feasible
  - Clouds uniformize operating systems and architectures

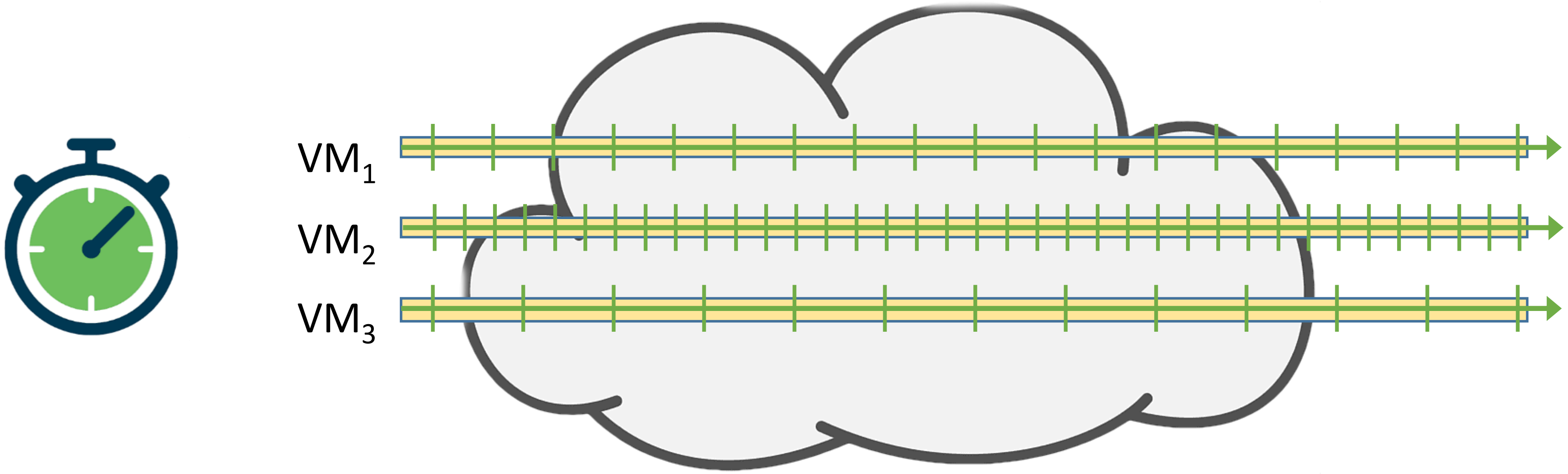
Proposed Approach

- Make ICS testbeds work in the cloud



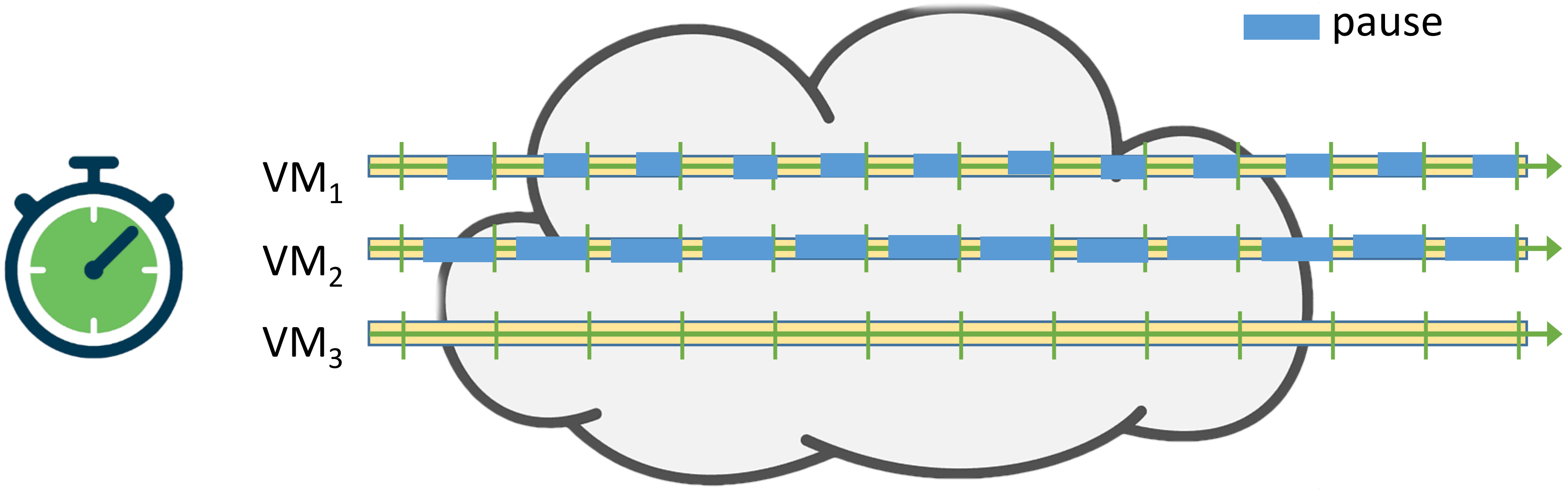
Key Technical Challenges

- Programs compiled for specialized processing chips don’t run natively
- Virtual machines need
  - To be embedded in virtual time
  - To be temporally correlated (so that all VMs advance in virtual time at the same rate)



Approaches

- Use instruction level emulation (e.g. QMU)
  - Working now with programmable logic controller (PLC)
- Leverage previous results to have software see 'virtual clock' rather than wall-clock
- Coordinate VM executions in time



Deliverables

- Prototype of working system, on models with 10 or more devices
- Performance studies of working system to identify bottlenecks and next steps
- Modules for security lab course that use prototype

Status

- Launch early 2023
- Two years duration
- Senior staff: Nicol, Levchenko, Luellen
- Half-time programmer
- Three graduate assistants

New Project: Promoting the Resilience of Communities and Critical Infrastructure Facing Wildfires

Presenter: Randall Sandone, University of Illinois Urbana-Champaign
PI: Paolo Gardoni, University of Illinois Urbana-Champaign

The Problem
Wildfires are a growing concern with significant annual losses

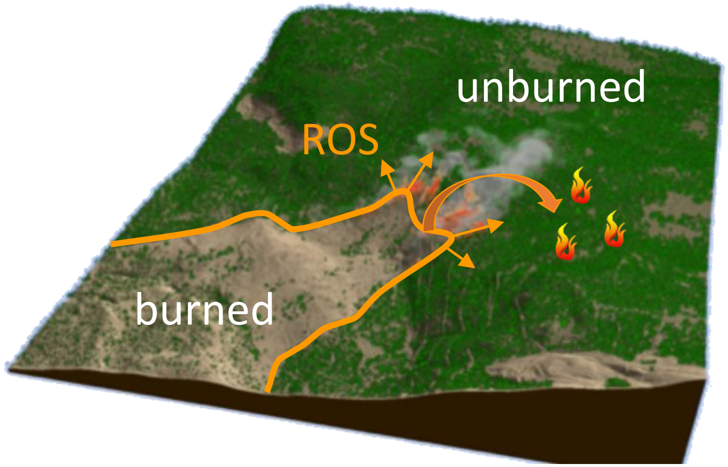
- Recent wildfires in California have become one of the deadliest and most destructive ones on record (killed 88 people, burned 14,000 residences and 530 commercial buildings, with over $12 billion insured losses)

- Wildfires can be caused by and interact with infrastructure like electric power
  - Transmission lines traversing heavily forested areas may trigger wildfires
  - Power outage or preventive shutoff can significantly affect communities and businesses (liability issues)

- Changes in the frequency and severity of wildfires and in exposure conditions contribute to the growing trend of annual losses
  - Climate change tend to favor extreme droughts, leading to longer fire seasons
  - Developments at the wildland-urban interface increase values at risk

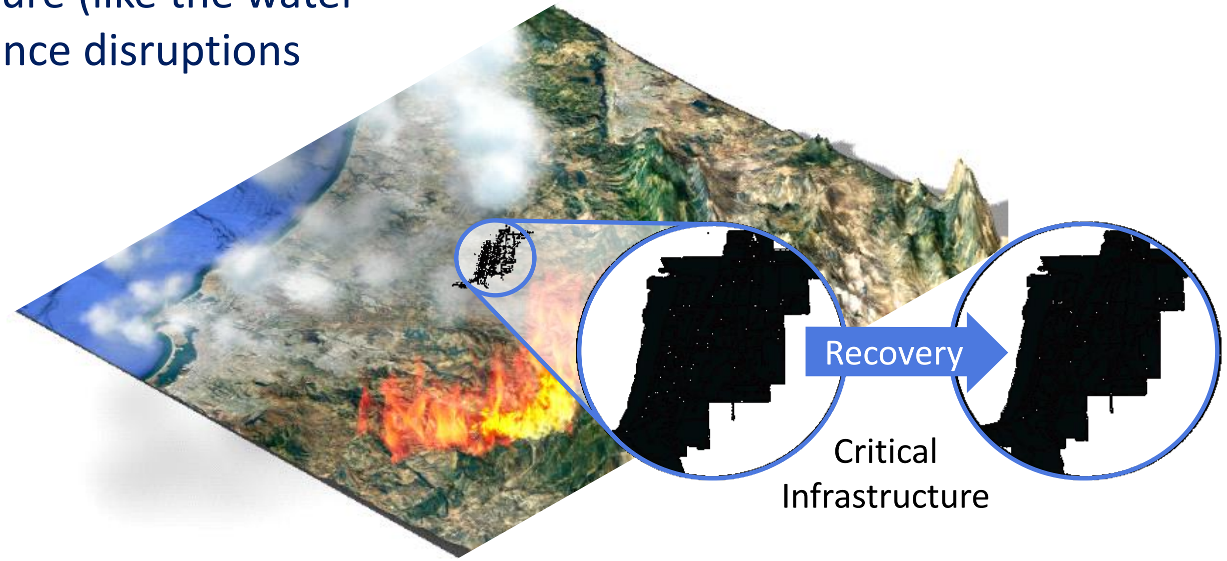
Wildfires present a front-like geometry propagating toward unburned vegetation

- The local propagation speed, called the rate of spread (ROS), depends on topography, environmental, and fuel conditions
  - Elevation, slope, and orientation of terrain
  - Wind speed and direction
  - Vegetation properties
- Wildfire can also propagate with firebrand advections
  - Lofted embers can potentially initiate spot fires far ahead of the fire front
  - It is one of the most dangerous spreading mechanisms for wildland/urban interface
- The direction and speed of propagation depend on multiple physical processes
- The challenge is to capture these physical processes at a manageable computational cost
  - Complex physics coupled with uncertainty renders fully physics-driven models computationally intractable
  - Empirical models are too simple to yield accurate results



Regions outside of the footprint of a wildfire can also experience loss of service from critical infrastructure

- Damage to infrastructure due to wildfires can affect the overall functionality of critical infrastructure
- Other infrastructure supported by damaged infrastructure (like the water network supported by the power network) can experience disruptions due to infrastructure interdependencies
- Differently from other hazards, infrastructure like power networks can be both damaged by wildfires as well as the source of wildfires
- This project will develop models to predict
  - wildfire propagation, and
  - damage to critical infrastructure
- The project will also develop a meaningful visualization of wildfire propagation and damage

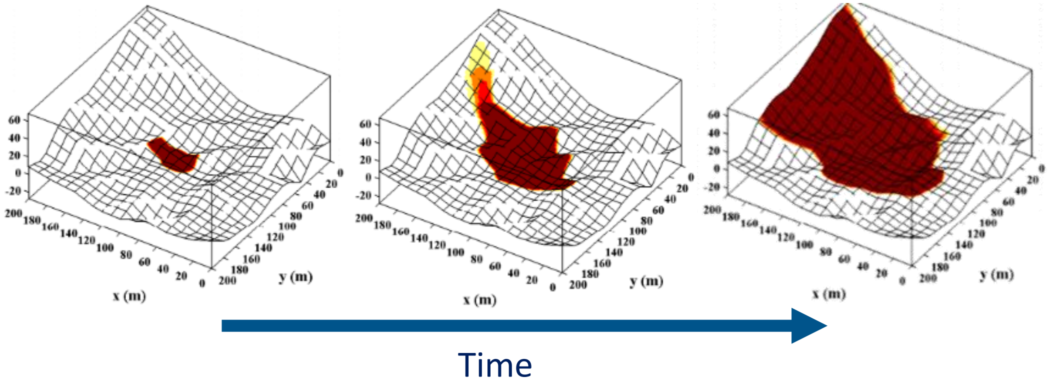


What Will Success Look Like?

For **future** wildfires, we will be able to

- predict the propagation pattern and impact areas for given conditions, like vegetation, terrain, and weather
- find the probability that a wildfire can reach specific targets

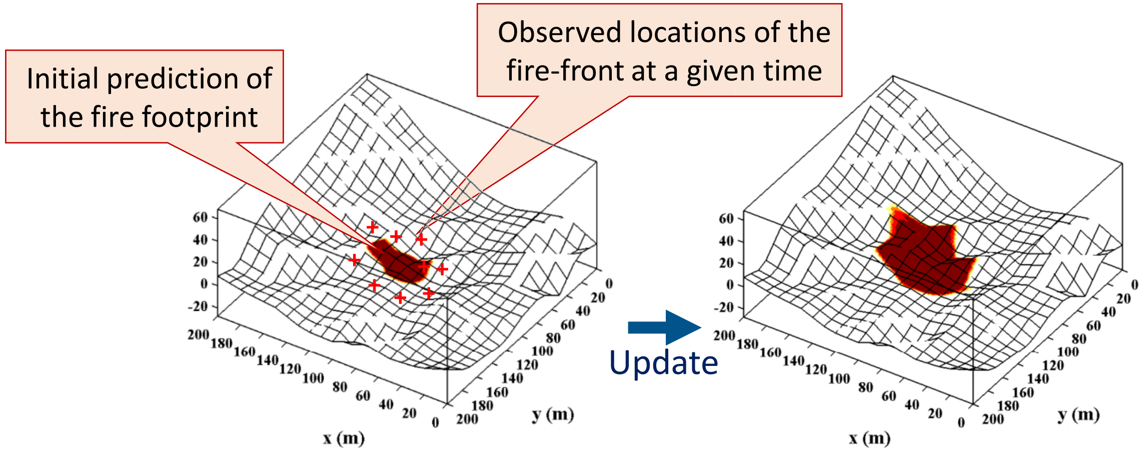
The formulation will also allow us to update predictions based on the effects of climate change



For **ongoing** wildfires, we will be able to

- provide real-time or faster predictions as a wildfire propagates
- update predictions in (near) real-time using the latest data on vegetation, weather, and fire propagation

The real-time updating will allow us to tailor the generic model to a specific region and time

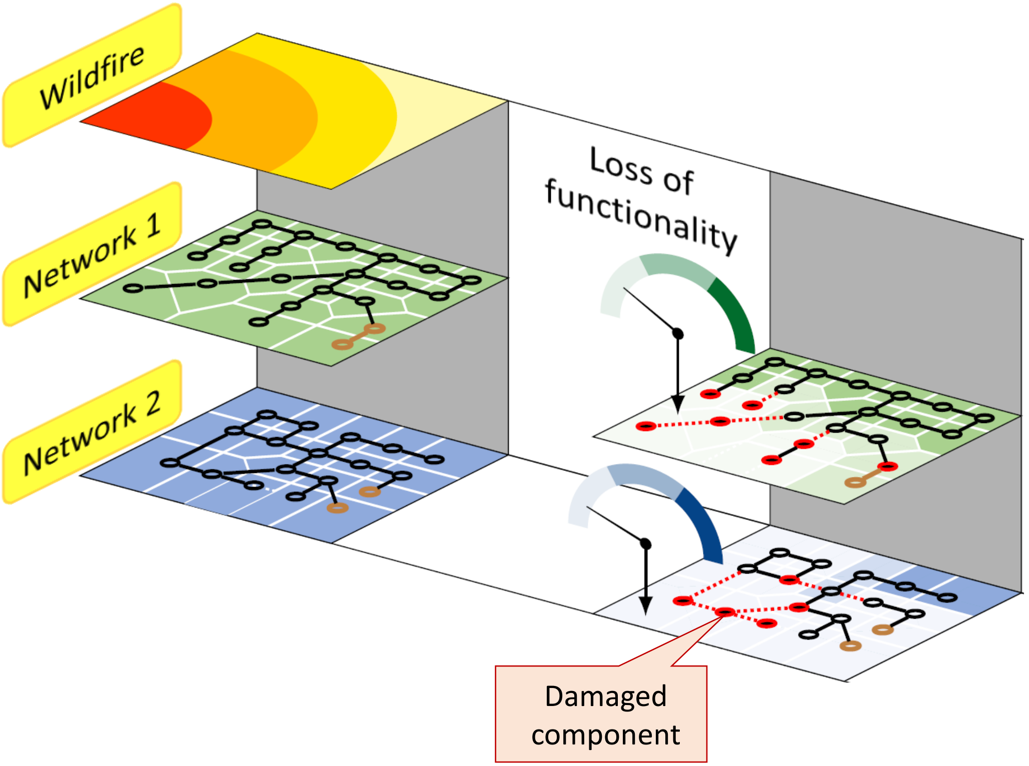

Initial prediction of the fire footprint

Observed locations of the fire-front at a given time

What Will Success Look Like?

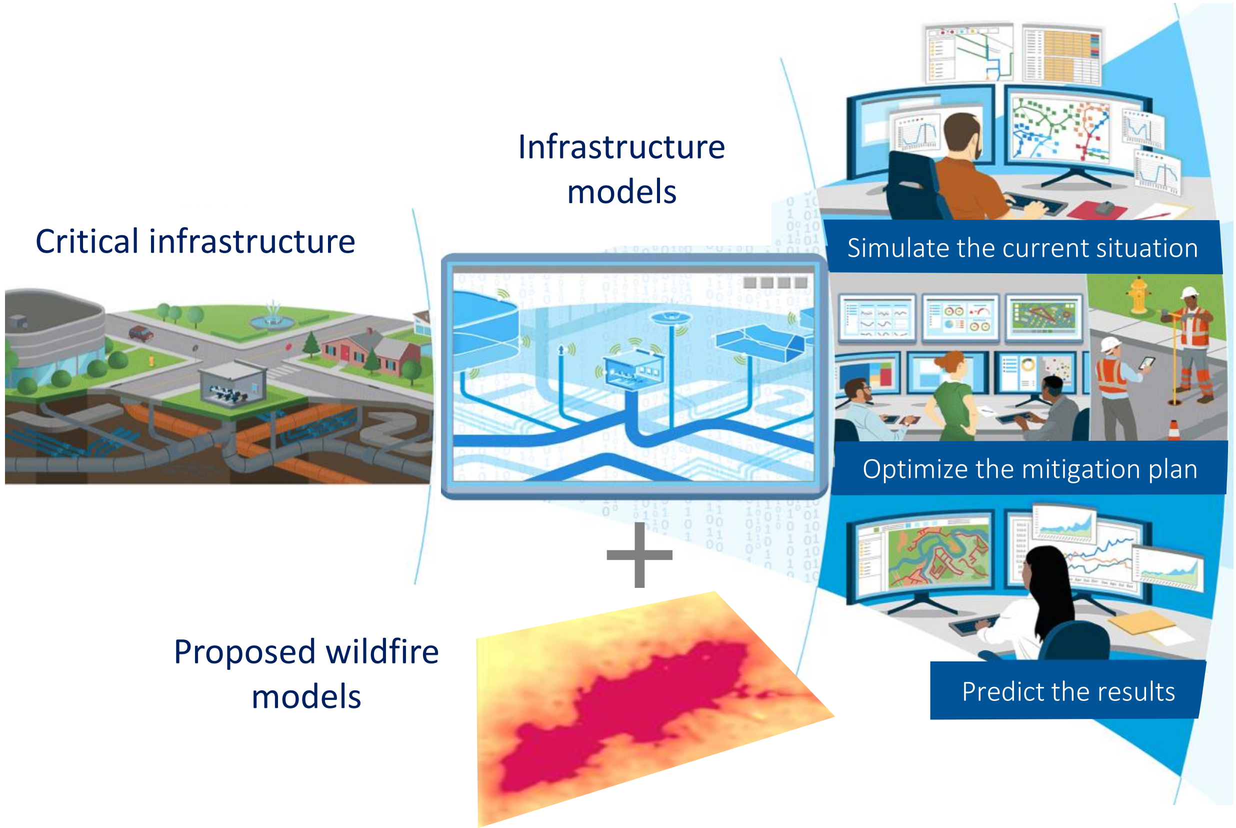
- For critical infrastructure, we will predict the damage to individual components and the effects on the infrastructure functionality

- The model and visualization will be demonstrated by prediction in hindcast the Camp Fire in Butte County, California



Benefits

- The developed models and visualization will be a milestone toward the identification of solutions and help prioritize mitigation strategies for reducing risks and promoting the resilience of communities and infrastructure
  - For future wildfires, the developed models will help achieve the desired infrastructure resilience by simulating the effects of mitigation plans to reduce wildfire losses
  - For ongoing wildfires, the real-time predictions of wildfire behavior and infrastructure damage will help optimize the management of human and economic resources



Critical infrastructure

Infrastructure models

Proposed wildfire models

Simulate the current situation

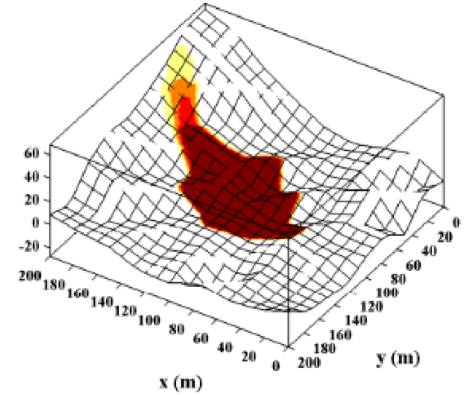
Optimize the mitigation plan

Predict the results

- Future work could extend these efforts to define a national wildfire risk index representing the long-term risk of communities to wildfires, and creating web-based maps for risk communication and decision making

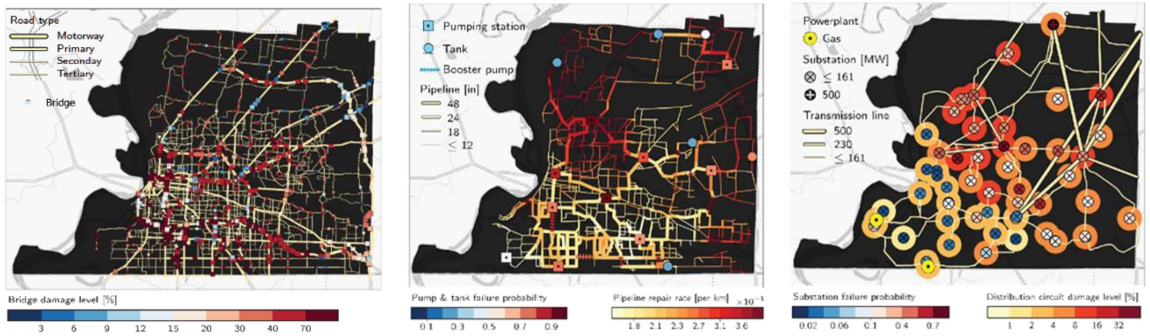
Past Work
The project will build on our past work on wildfire propagation and the modeling of critical infrastructure

- We have already formulated a preliminary system of differential equations to model fire front dynamics and its stochastic variations
  - The equations capture the effects of weather conditions, topography, and vegetation properties
- Also, we have been developing a numerical method to solve such stochastic differential equations and update the solution based on observed data



- We also have experience with the modeling of damage and functionality of critical infrastructure subject to other natural hazards like earthquake, wind, and hurricane

Damage and functionality

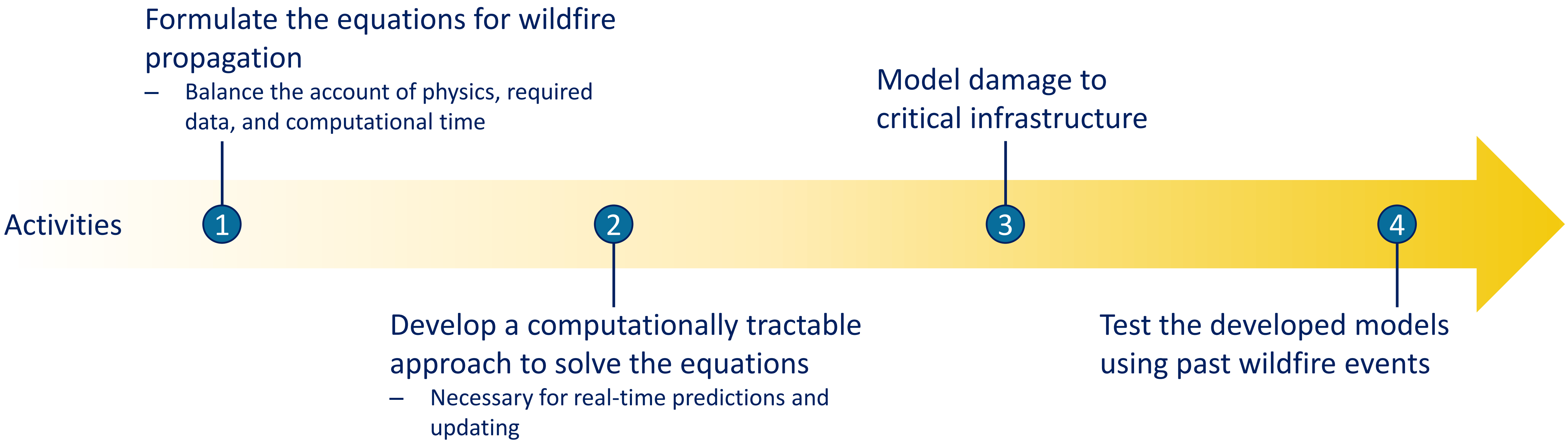


Transportation network

Water network

Power network

Planned Activities



Activities

1. Formulate the equations for wildfire propagation
   - Balance the account of physics, required data, and computational time
2. Develop a computationally tractable approach to solve the equations
   - Necessary for real-time predictions and updating
3. Model damage to critical infrastructure
4. Test the developed models using past wildfire events

Networking break

15-minutes

ON THE HORIZON

рахмат
danke
謝謝
ngiyabonga
شكراً جزيلاً
Баярлалаа
mersi
kia ora
barka
welalin
tack
spas
teşekkür ederim
mahalo
tapadh leat
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
kiitos
dankie
nanni
nandri
dhanyavad
thank you
gracias
хвала
asante
manana
obrigada
tenki
bedankt
bayarlalaa
gracie
hvala
maururu
köszönöm
akun
dankon
aciū
djiere dieuf
tau
mochchakkeram
murakoze
enkosi
dziękuję
дякую
mamnun
chokrane
chnorakaloutioun
gratias ago
gràcies
sulpáy
taiku
go raibh maith agat
sobodi
dėkuji
sagolun
sukriya
kop khun krap
arigatô
takk
dakujem
trugarez
obrigado
mèsi
didi madloba
najis tuke
ありがとう
tanemirt
grazie
terima kasih
rahmet
ευχαριστώ
diolch
dhanyavadagalu
shukriya
merce
мерси
kam sah hamnida
rahmat
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci