erVa | NSF Engineering Research Visioning Alliance

Engineering Research Opportunities for Tomorrow’s Unhackable Infrastructure

GUIRR Webinar | March 22, 2023

Presented by
Saurabh Amin, Associate Professor and Pierce Lab Director, MIT and
David Ott, Senior Researcher and Program Director, VMware

info@ERVAcommunity.org

NSF Award #2048419

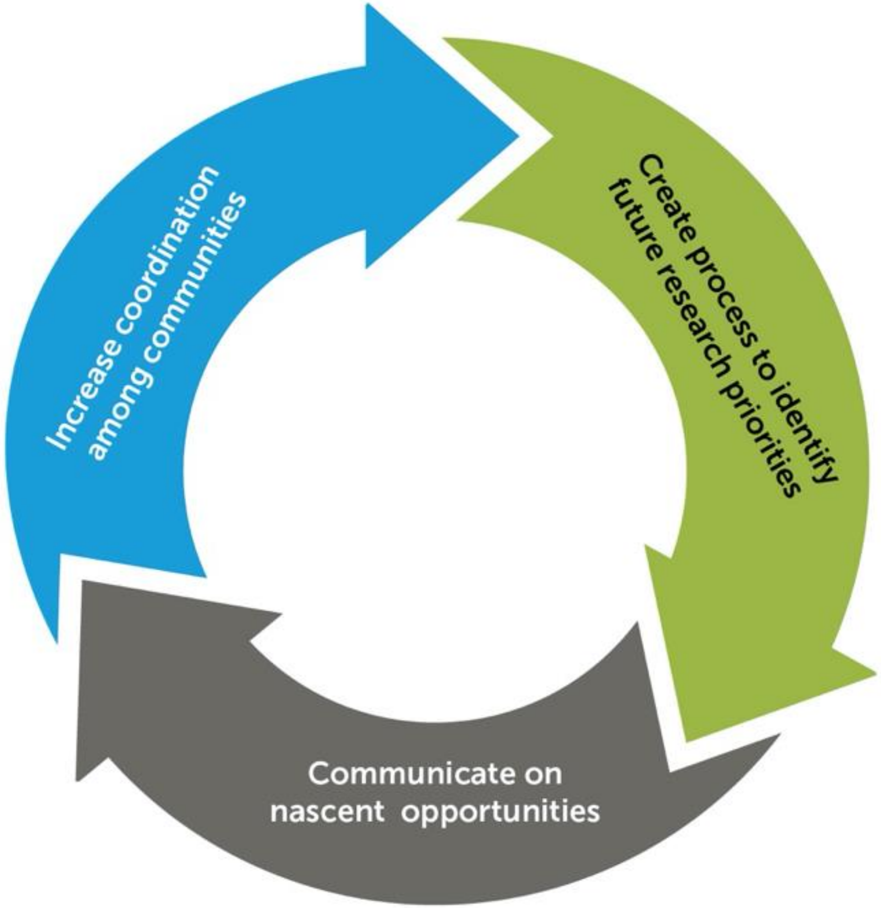
ERVA BACKGROUND

- Launched in April 2021
- 5-year cooperative agreement funded by NSF
- Awarding Organizations – BTAA, EPSCoR/IDeA Foundation, UIDP

MISSION

To identify and develop bold and transformative new engineering research directions and to catalyze the engineering community's pursuit of innovative, high-impact research that benefits society.

GOALS


Increase coordination among communities
Create process to identify future research priorities
Communicate on nascent opportunities

- Facilitate generation of engineering research visions
- Articulate high-impact future research visions
- Enable new opportunities

- Communicate research visions and nascent opportunities

- Synthesize ideas
- Cultivate relationships
- Engage new, diverse voices

PI TEAM

Dorota Grejner-Brzezinska
The Ohio State University
Principal Investigator

Charles Johnson-Bey
Booz Allen Hamilton
Co-Principal Investigator

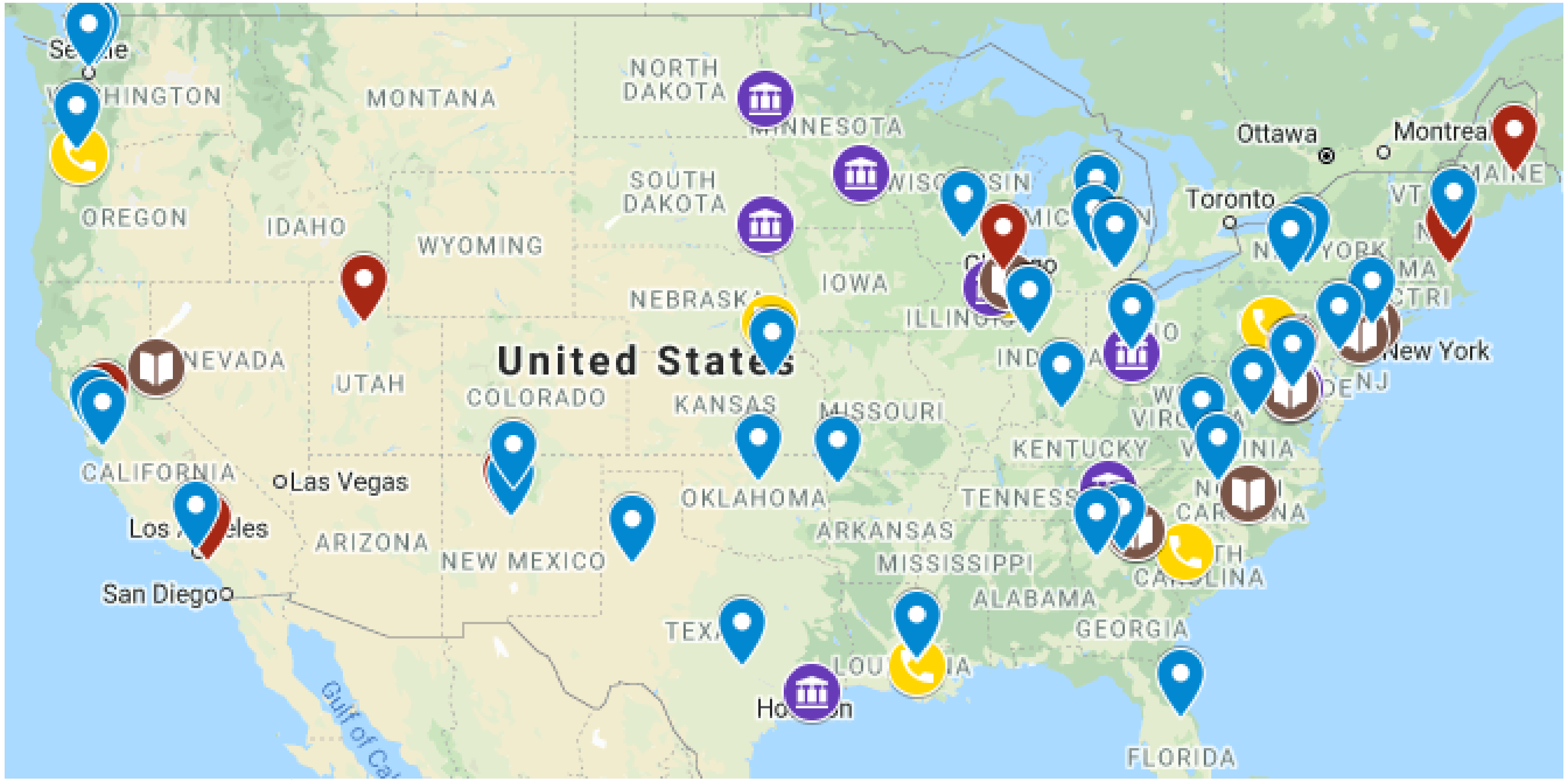
Edl Schamiloglu
University of New Mexico
Co-Principal Investigator

Anthony Boccanfuso
UIDP
Co-Principal Investigator

Pramod Khargonekar
UC Irvine
Co-Principal Investigator

erVa | NSF Engineering Research Visioning Alliance

BROAD BASE OF INDIVIDUAL SUPPORTERS



STANDING VOLUNTEER LEADERSHIP

- ● Advisory Board (11)
- ● Standing Council (36)
- ● Communications (8)
- ● Government Engagement (11)
- ● Research Intelligence (7)

1100+ Champions

erVa | NSF Engineering Research Visioning Alliance

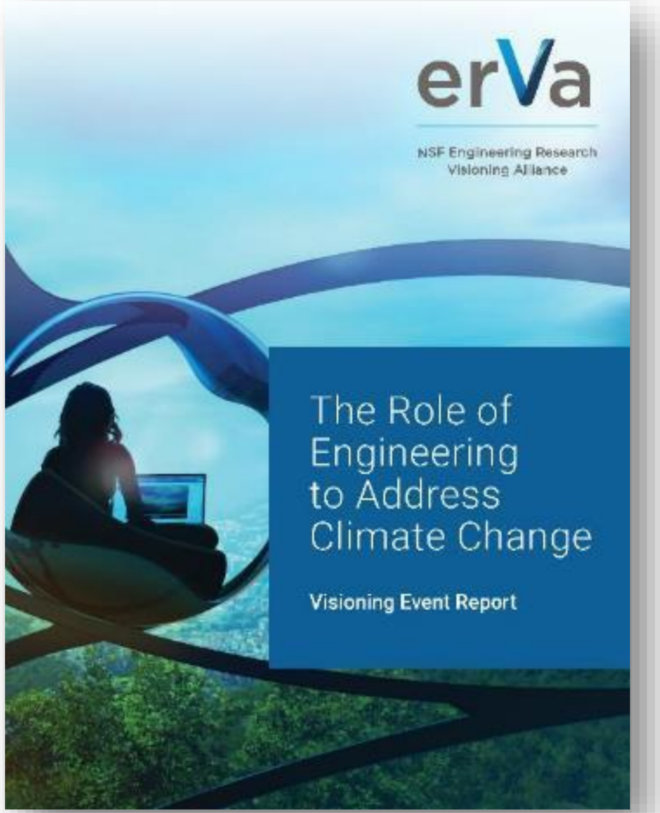
VISIONING

Goal: identify specific areas that are nascent or require additional exploration with the potential for the greatest return on investment.

Attendees: cross-sector researchers who can help ERVA identify less-explored, basic, and use-inspired lines of research ripe for engineering community pursuit.

Format: expert, informed discussion and interactive thematic breakout sessions.

VISIONING REPORTS



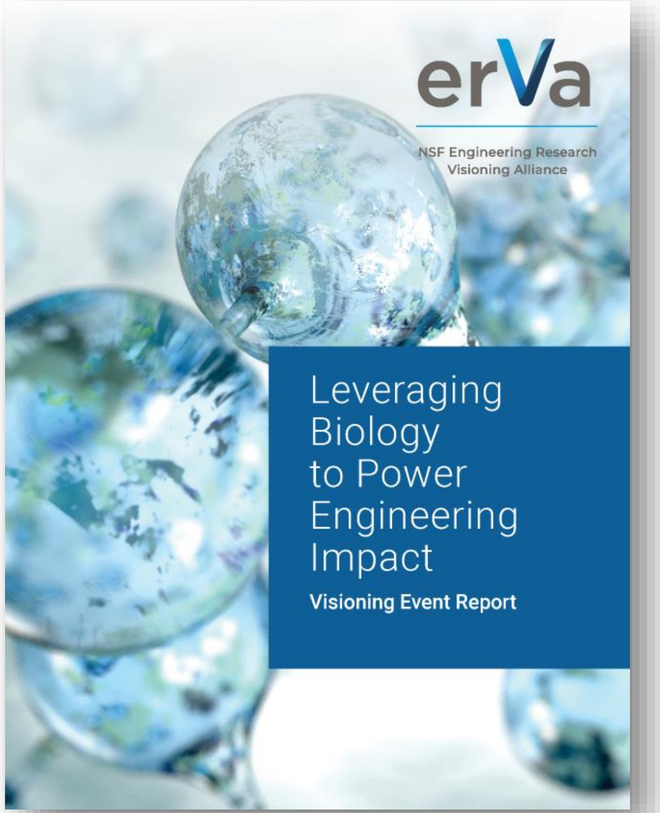
erVa

NSF Engineering Research Visioning Alliance

The Role of Engineering to Address Climate Change

Visioning Event Report

Released: August 17, 2022



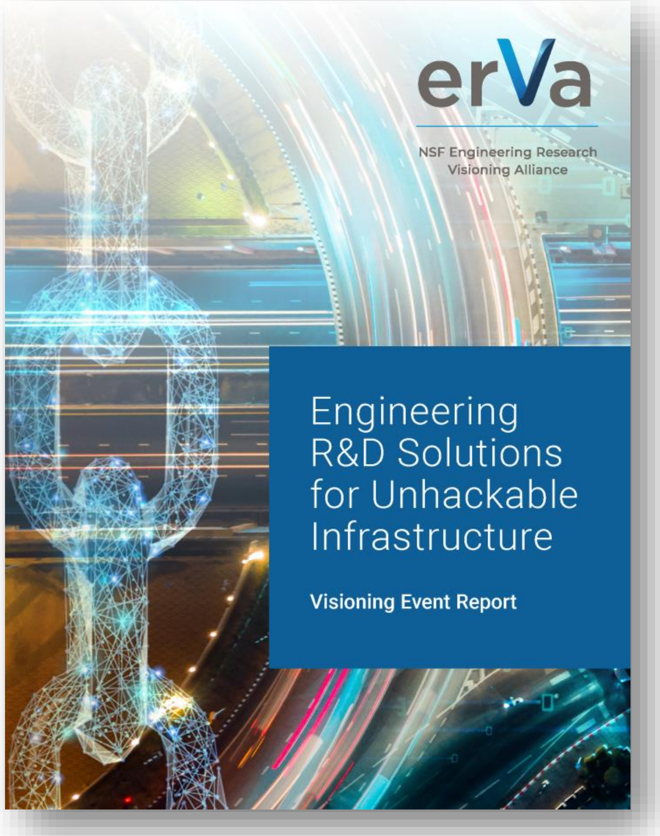
erVa

NSF Engineering Research Visioning Alliance

Leveraging Biology to Power Engineering Impact

Visioning Event Report

Release: October 27, 2022



erVa

NSF Engineering Research Visioning Alliance

Engineering R&D Solutions for Unhackable Infrastructure

Visioning Event Report

Release: February 16, 2023

SETTING THE STAGE

Thematic Task Force: 8 leading voices in engineering, cybersecurity, computing fields.

- Frame the event—select 5 subtopics and the questions that will drive the discussion toward goal

Participants: 35 selected, based on their research and expertise (engineering and other disciplines). From academia, industry, and government.

Charge: Identify specific areas that require exploration → greatest ROI potential.

EXCELLENCE *AND* DIVERSITY

Visioning event: Engineering R&D Solutions for Unhackable Infrastructure, MIT, August 2022

THEME: Engineering R&D Solutions for *Unhackable Infrastructure*

Key question: *What could tomorrow's "unhackable infrastructure" look like with non-incremental advances in engineering R&D?*

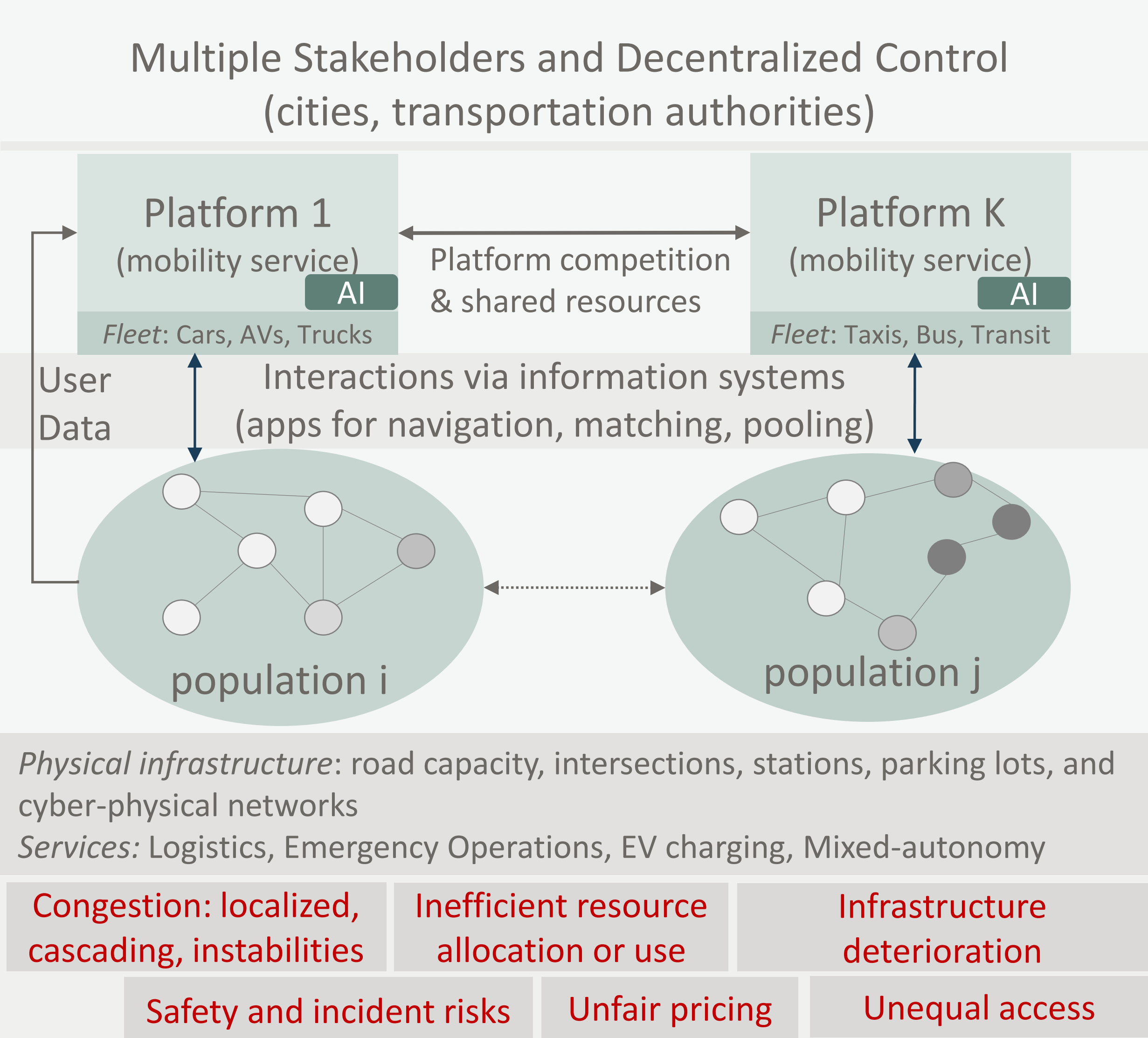
"Infrastructure"

- Physical infrastructure (assets, hardware)
- Software and algorithms
- Data and communication networks
- Human beings: users, operators, security administrators, adversaries

"Unhackable"

- Safety, security, and trust in all essential systems and services
- Robust, resilient, adaptive in the face of unexpected change
- Trustworthiness in a wide range of situations – including adversarial

Societal-Scale CPHS Domain: Transportation



Multiple Stakeholders and Decentralized Control (cities, transportation authorities)

Platform 1 (mobility service) AI — *Fleet*: Cars, AVs, Trucks

Platform competition & shared resources

Platform K (mobility service) AI — *Fleet*: Taxis, Bus, Transit

User Data

Interactions via information systems (apps for navigation, matching, pooling)

population i

population j

Physical infrastructure: road capacity, intersections, stations, parking lots, and cyber-physical networks

Services: Logistics, Emergency Operations, EV charging, Mixed-autonomy

Congestion: localized, cascading, instabilities

Inefficient resource allocation or use

Infrastructure deterioration

Safety and incident risks

Unfair pricing

Unequal access

Backdoor attacks and platform compromise

Non-robust AI/ML algorithms (potential unintended consequences)

Data integrity compromise and denial of service

Malicious entities and/or strategic (selfish) behavior

Network interdependencies, involving both legacy and modern infrastructure

resulting impacts

Engineering-Informed Infrastructure Cybersecurity

Key question: *How can we leverage deep engineering knowledge and expertise to lead security and resilience research in cyber-physical-human infrastructure systems?*

Analogy: Physics-Constrained ML

ML: good at recognizing patterns, anomaly detection, prediction

Physics/Engineering:

- Leverage traditional modeling
- Specialized domain knowledge/representations
- Informed design constraints

Engineering Domains:

- Specialized design specifications, requirements, constraints
- Safety, security, resilience definitions tailored to context and stakeholders
- Nature of the infrastructure (medical vs. energy vs. transportation vs. critical vs other)

Engineering R&D Solutions for Unhackable Infrastructure

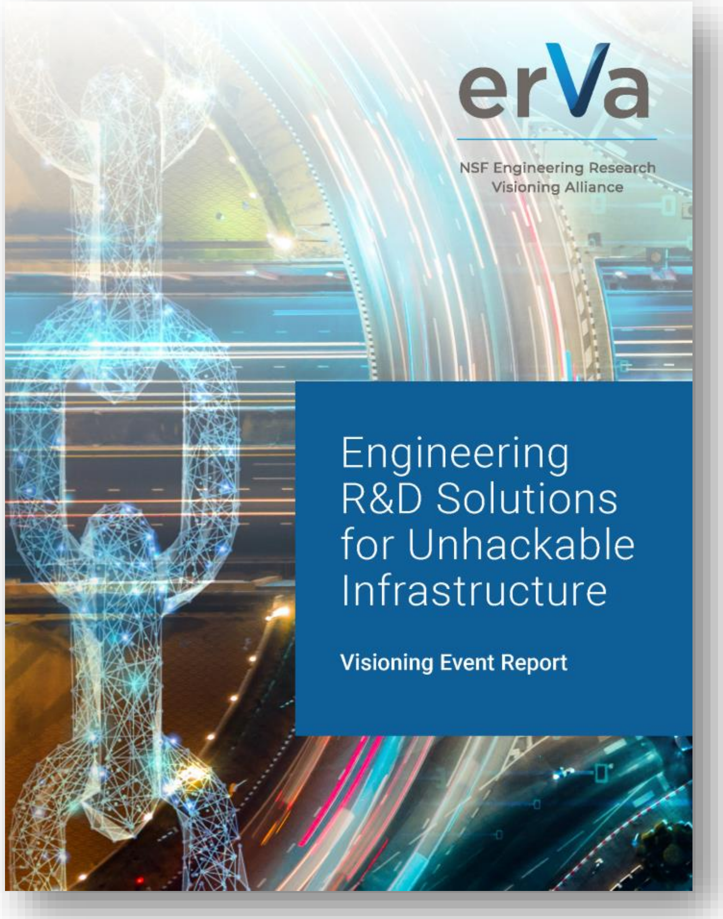
#1 **Human-Technology Interface Considerations**

#2 **Measuring and Verifying Security (Metrics)**

#3 **Future Approaches to Autonomous Security**

#4 **New Approaches to Resilience in Interdependent Infrastructures**

#5 **Architecting Trustworthy Systems**



erVa

NSF Engineering Research Visioning Alliance

Engineering R&D Solutions for Unhackable Infrastructure

Visioning Event Report

#1 Human-Technology Interface Considerations

Sampling of engineering research opportunities:

- Extensive work needed on **human incentives** and the **economics of security and resilience for engineered infrastructures**.
- **Security usability research in engineered infrastructures** is needed to address unwanted tradeoffs with functionality, convenience, cost, and more.
- Integrating **frontier user interface technologies** (e.g., AR/VR, NLP, biometric monitoring) into security interfaces.
- Use of **immersive human-computer environments** in CPHS needs threat modeling, vulnerability mitigation, and more.

Human-Technology Interface Considerations
erVa
NSF Engineering Research Visioning Alliance

#2 Measuring and Verifying Security (Metrics)

- Challenges in **measuring, evaluating,** and **verifying security** in complex, scaled CPHS are considerable.
- **Continuous monitoring** and **automated response** research at CPHS interfaces given changing threat landscapes and unpredictability.
- **Observability** is a key design issue. Foundational research and practical tools are needed to observe, estimate, and update the dynamic security state of a CPHS.
- **Fully automated mechanisms** are needed to maintain functionality (resilience) while recovering to an operational state (recovery).
- Incorporating **specification and verification techniques** into design cycles for large-scale infrastructure systems.

Measuring and Verifying Security (Metrics)
erVa
NSF Engineering Research Visioning Alliance

#3 Future Approaches to Autonomous Security

- **Autonomous security** is needed address the scale and complexity of tomorrow's CPHS infrastructures and adversarial threats.
- Research should include how **intelligent automation** and **human intelligence** interact.
- The future of AI-driven security research in CPHS infrastructure context is to add **automated decisions and response**.
- A key challenge in future autonomous security is the need for more sophisticated **contextual awareness**.
- **Some key applications:** virtual security assistants, automated configuration agents, real-time security risk analyzers, adversarial agents for design analysis.

Future Approaches to Autonomous Security
erVa
NSF Engineering Research Visioning Alliance

erVa | NSF Engineering Research Visioning Alliance

#4 New Approaches to Resilience in Interdependent Infrastructures

- A key design challenge is managing insecurities arising from **correlated software bugs** and **hardware malfunctions**.
- Research is needed on the complex interplay between **coordinating entities** in CPHS infrastructures.
- Develop a design approach that maintains **system-level properties of safety and security** after integration of modular components.
- **Compositional and learning-based approaches** to quantify system-level safety properties based on data-driven models of CPHS.
- Tomorrow's systems will be deployed in contested environments that require far more **active cyber defense strategies and tactics**.

New Approaches to Resilience in Interdependent Infrastructures
erVa
NSF Engineering Research Visioning Alliance

#5 Architecting Trustworthy Systems

- Transforming ill-defined notions of trustworthiness into well-defined, robust notions of **provable correctness and security**.
- Expanding the role of **design specification** for a more verifiable CPHS.
- Research on security and reliability in both **centralized and decentralized** infrastructure contexts.
- Scaling **confidential computing techniques** (attestation, isolation) to complex component hierarchies and cross-domain interactions.
- **Trustworthy architectures** for many **new infrastructure domains**.
- Applying **quantum-resistant cryptography** to future CPHS infrastructure.

Architecting Trustworthy Systems
erVa
NSF Engineering Research Visioning Alliance

ERVA: Call to Action

Share

- **Share** ERVA reports broadly to anyone interested in the future of engineering.

ervacommunity.org/ visioning reports

Align & Pursue

- **Align** report priorities and insights with your research goals.
- **Pursue** aligned research directions.

Engage

- **Engage** in ERVA ideation and visioning events.
- July 25-26: *Engineering sustainable materials for a circular economy*
- --Nominate attendees

Got Ideas?

Submit your visioning theme ideas!

Please share!

JOIN US!

- Become an **ERVA Champion** at www.ervacommunity.org/get-involved

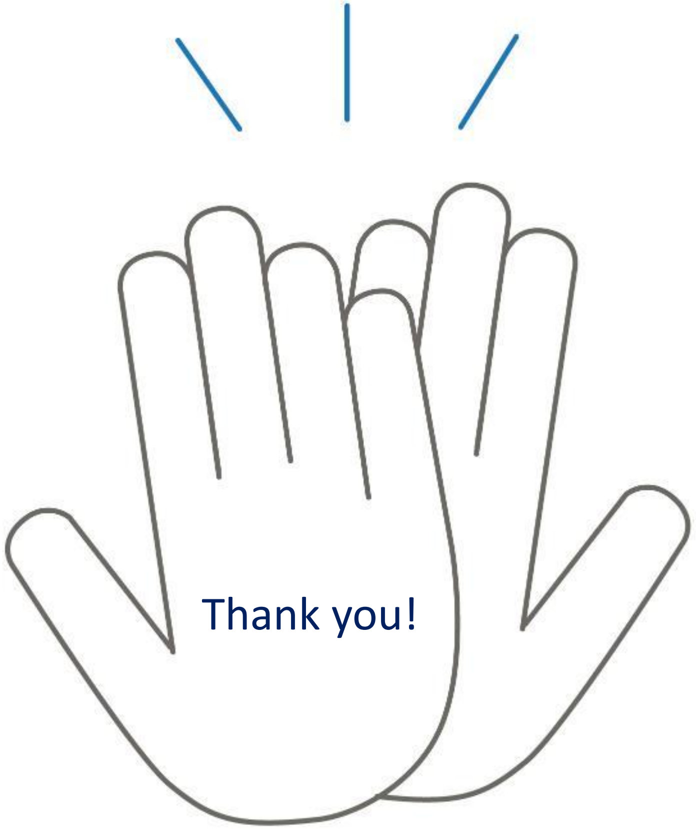
- **Follow us:**

  ERVAcommunity.org

  @ERVAcommunity

  #ERVAcommunity

  info@ervacommunity.org



This material is based upon work supported by the National Science Foundation under Grant #2048419. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

erVa | NSF Engineering Research
Visioning Alliance

Q&A