# **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

ciri.illinois.edu

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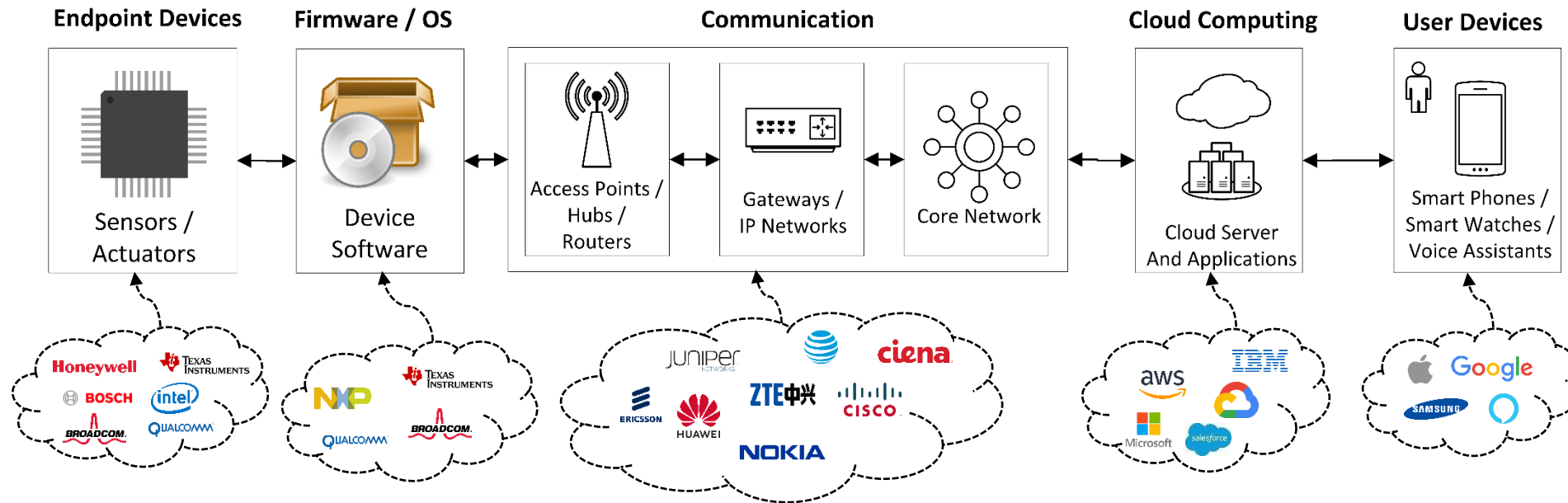
- **DHS Component:** CISA NRMC
- **Challenge Area:** ICT Supply Chain Risk Management (SCRM)

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

Our Approach:

- Analyze systemic risk as opposed to vendor risk

- Consider a composition of the component network and supplier network

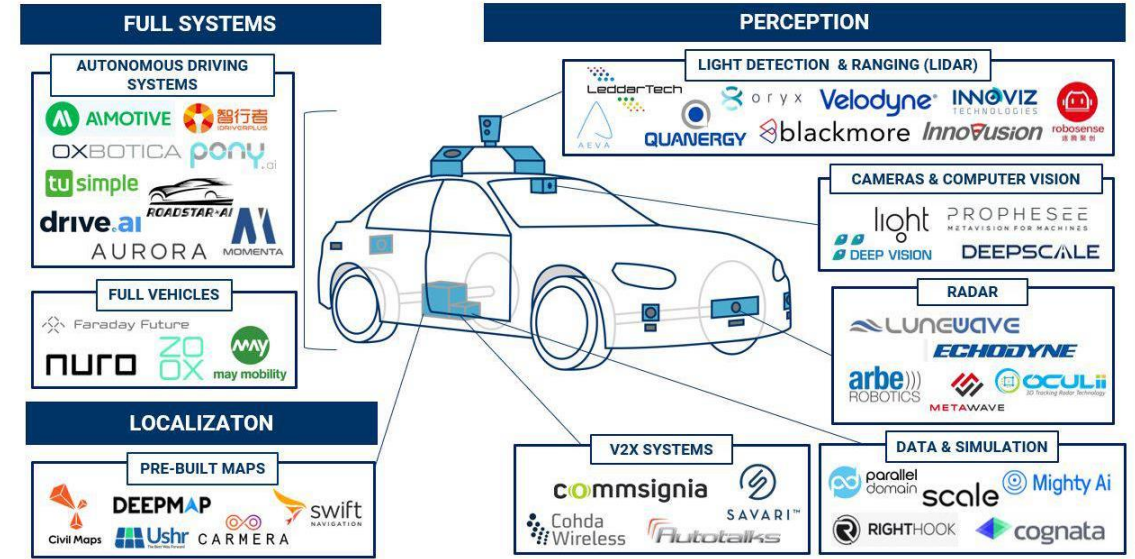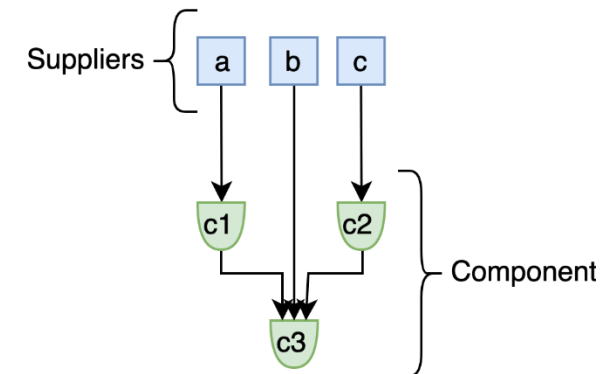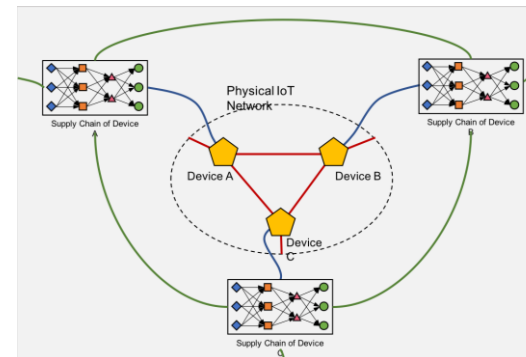- Decision support for vendor selection, onboarding, and upgradation

Figure: *Supply chain ecosystem for autonomous vehicles.*

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

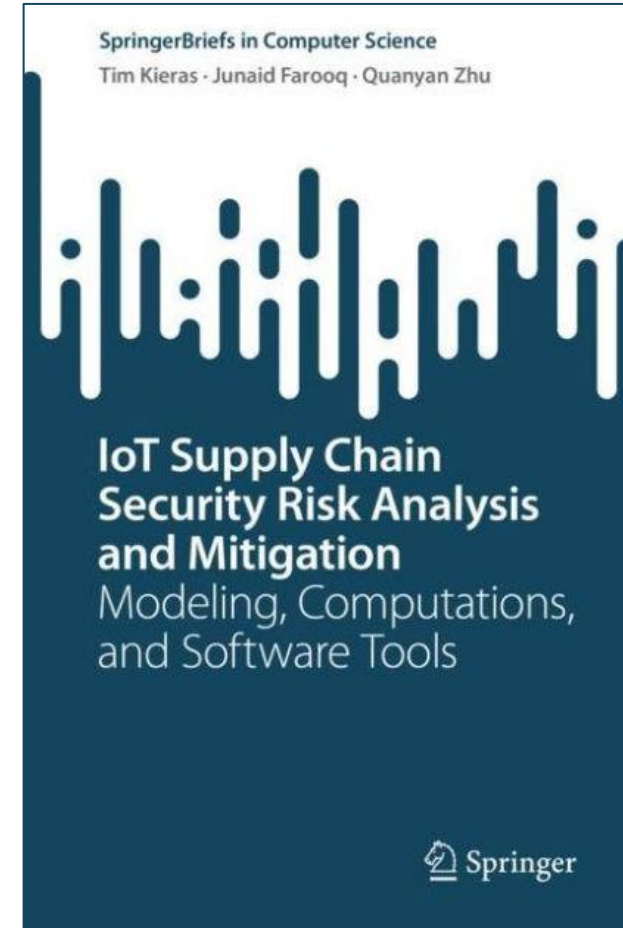**Supply chain of new Denver regional commuter rail**
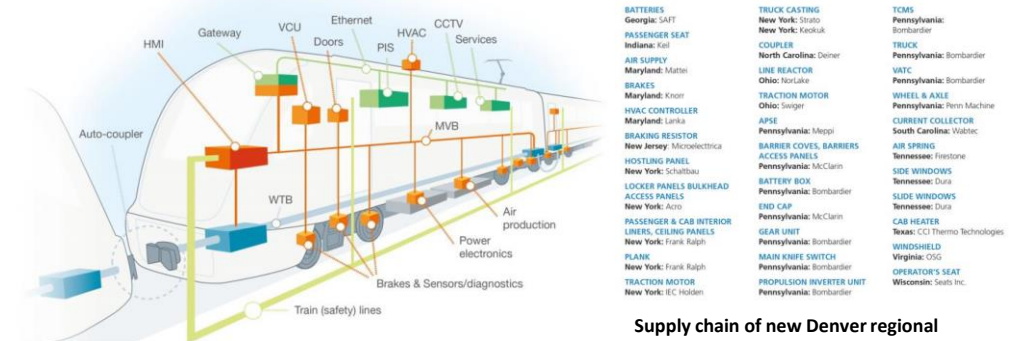
Source: Adapted from the paper J. Goikoetxea, "Shift2Rail CONNECTA: The Next Generation of the Train Control and Monitoring System", in Proceedings of 7th Transport Research Arena TRA 2018, April 16-19, 2018, Vienna, Austria

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

Available: www.i-scram.com

Product

Risk Summary and Statistics
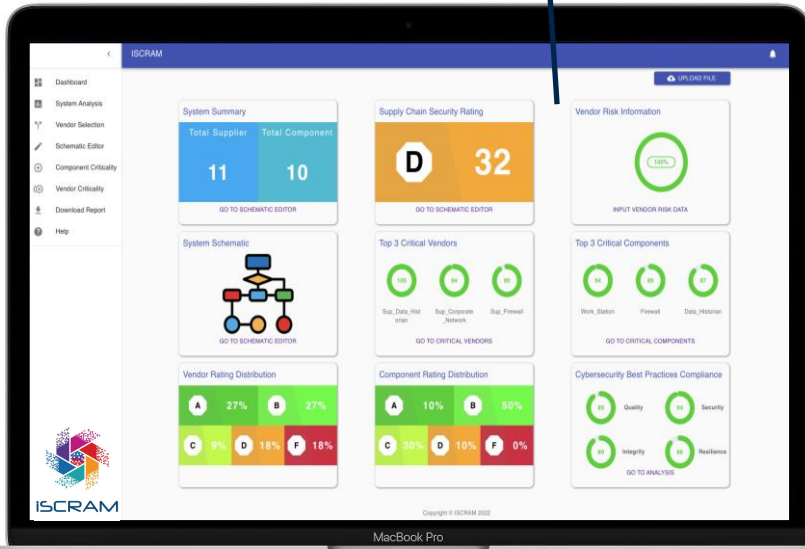
Risk-Centric Vendor Selection

Main Dashboard
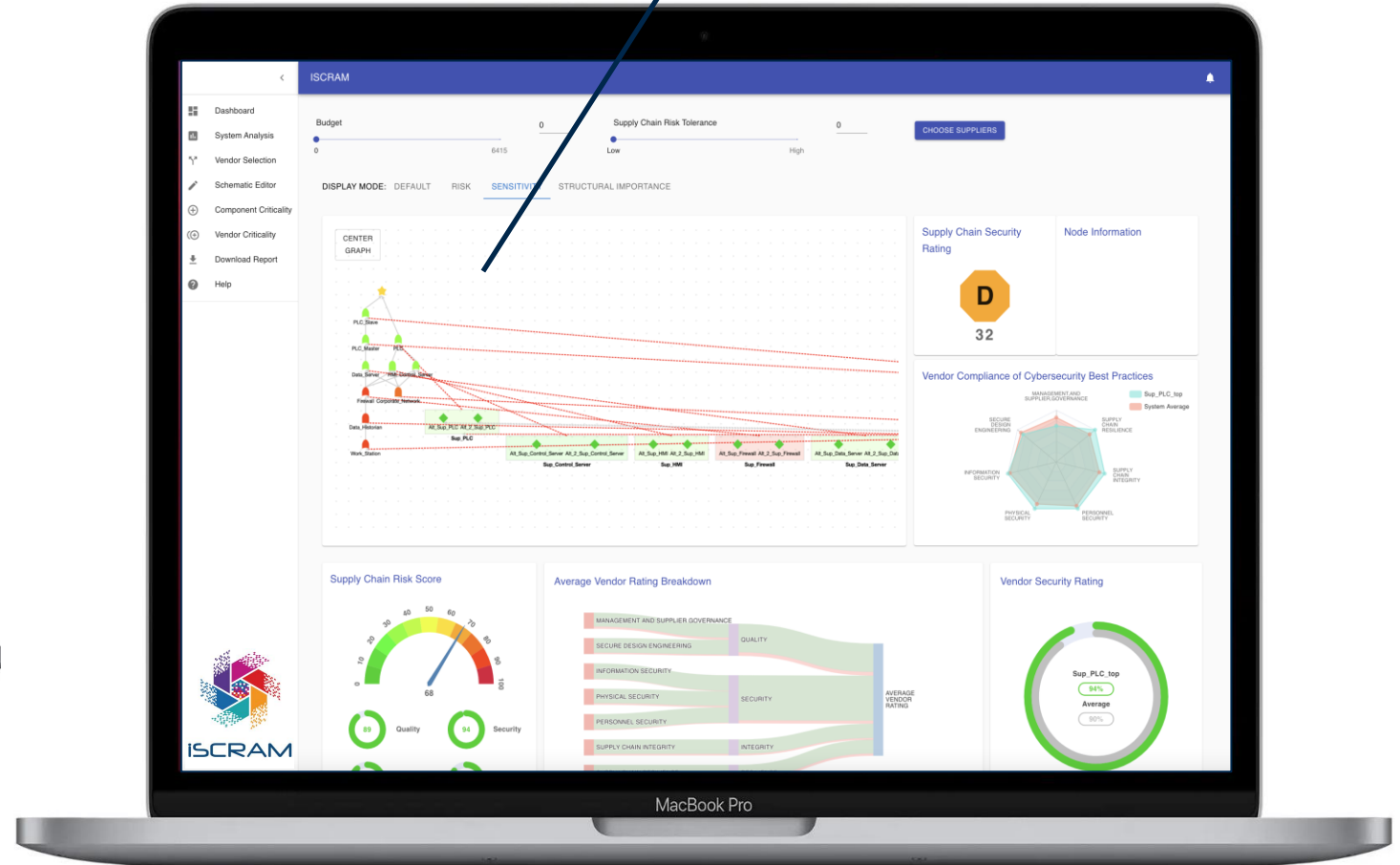
Vendor Selection

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
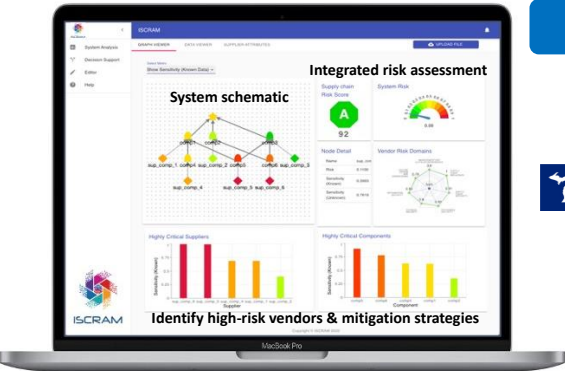
➤ Analyze systemic risk posture by ranking vendors by their individual cyber risks

➤ 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)

Funded by

Integrated risk assessment
System schematic
Identify high-risk vendors & mitigation strategies

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