NATIONAL ACADEMIES Sciences Engineering Medicine

TRB TRANSPORTATION RESEARCH BOARD

TRB Webinar: AI's Impact on Systems, Enterprise, and Cyber Resilience in Transportation

March 26, 2025

12:00 – 1:30 PM

PDH Certification Information

1.5 Professional Development Hours (PDH) – see follow-up email

You must attend the entire webinar.

Questions? Contact Andie Pitchford at TRBwebinar@nas.edu

The Transportation Research Board has met the standards and requirements of the Registered Continuing Education Program. Credit earned on completion of this program will be reported to RCEP at RCEP.net. A certificate of completion will be issued to each participant. As such, it does not include content that may be deemed or construed to be an approval or endorsement by the RCEP.

ENGINEERING
RCEP
REGISTERED CONTINUING EDUCATION PROGRAM

AICP Credit Information

1.5 American Institute of Certified Planners Certification Maintenance Credits

You must attend the entire webinar

Log into the American Planning Association website to claim your credits

Contact AICP, not TRB, with questions

Purpose Statement

This webinar will explore AI's benefits while also addressing significant risks such as cyber threats, ethical concerns, and unintended consequences. A key focus will be the challenge of AI-driven decision-making with fewer humans in the loop, which can lead to undetected errors, system failures, and safety risks.

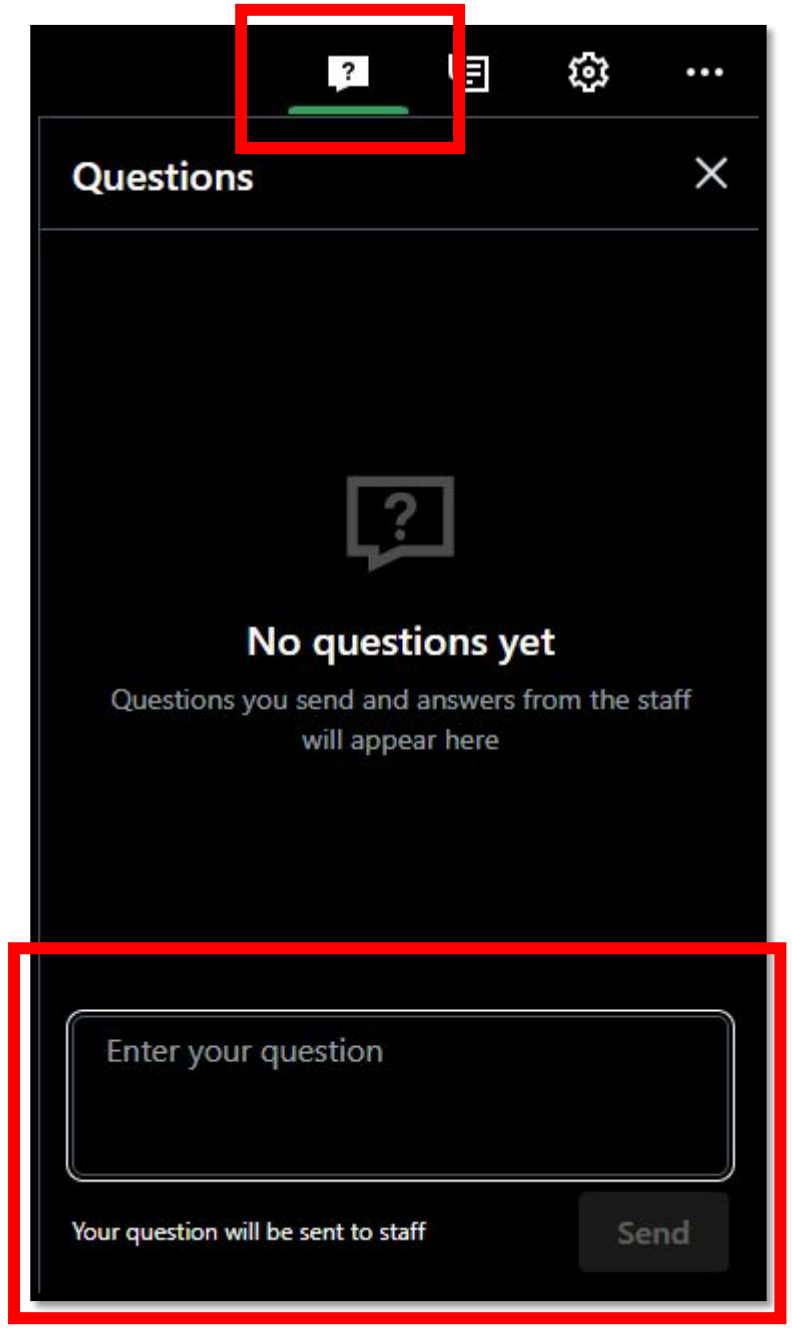
Learning Objectives

At the end of this webinar, you will be able to:

- Weigh the impacts and potential outcomes of AI on transportation agencies from an enterprise and cyber resilience vantage
- Analyze multisector perspectives on AI from academia, private, and the public sector

Questions and Answers

- Please type your questions into your webinar control panel
- We will read your questions out loud, and answer as many as time allows



Today's Presenters

Urban Jonson
ujonson@serjon.com
Serjon, LLC

John Haller
jhaller@cert.org
The CERT Division, Carnegie Mellon University

Kaan Ozbay
kaan.ozbay@nyu.edu
New York University

Matt Miller
mmiller@camsys.com
Cambridge Systematics

IMPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES FOR SYSTEMS, ENTERPRISE, AND CYBER RESILIENCE IN TRANSPORTATION

FREIGHT AND SAFETY PERSPECTIVES

URBAN JONSON

ujonson@serjon.com

Current

- SVP Information Technology and Cybersecurity, SERJON
- US FBI InfraGard Transportation Subject Matter Expert
- FBI Automotive Sector Specific Working Group (SSWG)
- Board of Directors, Cyber Truck Challenge
- Program Committee, ESCAR USA
- SAE Vehicle Electrical System Security Committee Member
- Technology & Maintenance Council (TMC) S.5 and S.12 Study Group Member

Experience

- Over 35 years of experience in IT and Cybersecurity, including strategic planning, assessments, AI/expert systems, and algorithm development
- Various papers, talks, and research on hacking, AI, as well as defending trucks and transportation in general

- Abusing and defending systems since the 1980s

AGENDA

- AI Taxonomy
- Data Science
- Opportunities
- Challenges
- Wrap-up

AI TAXONOMY

OVERVIEW

NIST AI Use Taxonomy*:

- Decomposes complex human-AI tasks into activities that are independent of technological techniques (e.g., neural network, large language model, reinforcement learning) and domains (e.g., finance, medicine, law).
- Provides a flexible means of classifying an AI system's contribution to a specified human-AI task.
- Intended to be a living document that is updated periodically with feedback from stakeholders, such as those in the AI evaluation and human factors communities.

*NIST Trustworthy and Responsible AI NIST AI 200-1,AI Use Taxonomy: A Human-Centered Approach, by Theofanos, Choong, and Jenson, March 2024, http://doi.org/10.6028/NIST.AI.200-1.

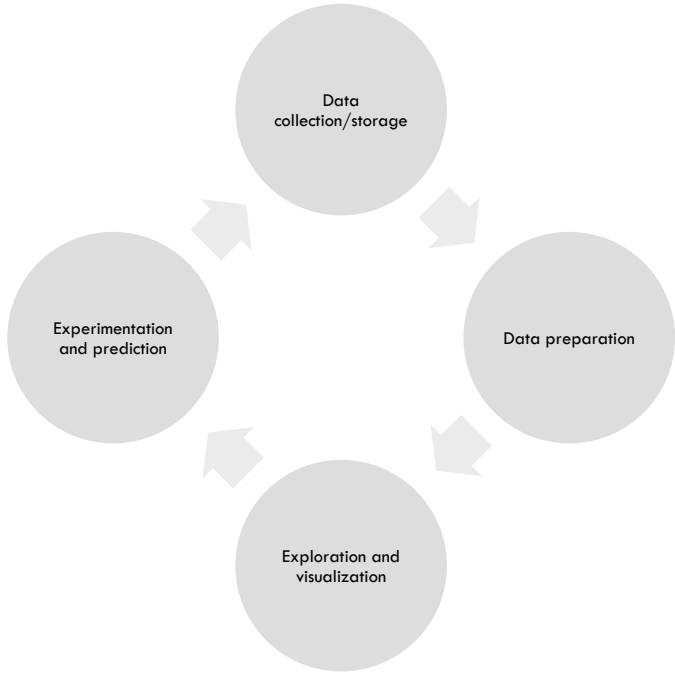
AI TAXONOMY - TRANSPORTATION

- **Connectionist** – Learning algorithms based on neural networks
- **Bayesians** – Probability-based inference systems
- **Symbolists** – Logic-based algorithms such as rules-based programming, decision trees, fuzzy logic, and rational agents
- **Analogizers** – Similarity-based classifiers, such as support vector machines
- **Optimizations** – Algorithms performing iterative updates and comparisons to discover optimum solutions, e.g. Genetic Algorithm (GA)

Jon Perez-Cerrolaza, Jaume Abella, Markus Borg, Carlo Donzella, Jesús Cerquides, Francisco J. Cazorla, Cristofer Englund, Markus Tauber, George Nikolakopoulos, and Jose Luis Flores. 2024. Artificial Intelligence for Safety-Critical Systems in Industrial and Transportation Domains: A Survey.
ACM Comput. Surv. 56, 7, Article 176 (July 2024), 40 pages. https://doi.org/10.1145/3626314

DATA SCIENCE

DATA SCIENCE LIFECYCLE



- Data collection and storage
  - Define project objectives
  - Collect data
  - Normalize storage and format
  - Data labeling
- Data preparation
  - Missing or inconsistent data
  - Cleaning and augmenting data
  - Removing duplicates
  - Normalization
  - Data labeling
  - Data type conversation
- Exploration and visualization
  - Statistical data analysis
  - Graphs and charts for understanding
- Experimentation and prediction
  - Try different models and approaches
  - Identify data trends and patterns
  - Discover insights
  - Build model

Source: https://www.datacamp.com/blog/what-is-data-science-the-definitive-guide

OPPORTUNITIES

OPPORTUNITY

- Rapid positive changes in analytics
- Ability to optimize existing systems and resources
- Force multiplier for the workforce
- Leaps in predictive analytics for all aspects of transportation
- Infrastructure cost and safety optimizations

SYSTEMS RESILIENCE

- **Predictive Maintenance** – Forecast equipment failures in trucks, rail, infrastructure, and other transportation systems and assets
- **Traffic Management** - Optimize routing based on real-time conditions, reducing congestion and improving delivery timelines

SYSTEMS RESILIENCE

- **Supply Chain Optimizations -** Predict and mitigate supply chain disruptions (e.g., fuel, weather events or labor shortages)
- **Incident Response -** Detect anomalies and trigger emergency protocols, enhancing rapid response capabilities during infrastructure failures or accidents

ENTERPRISE RESILIENCE

- **Operational Efficiency** - Enhances load forecasting, warehouse automation, and asset management, improving productivity and reducing operational costs
- **Risk Mitigation** – Identify and assess potential risks with early warning systems and operational risk forecasting in logistics and infrastructure

ENTERPRISE RESILIENCE

- **Autonomous Freight Systems** - Autonomous transportation modes powered by AI provide redundancy and flexibility in logistics networks, reducing reliance on human operators
- **Event Monitoring** – Identify and alert businesses about events such as upcoming regulations, changes in laws, social unrest, company-related posts and news

CYBER RESILIENCE

- **Threat Detection** - Detection of threats through real-time monitoring and anomaly detection in transportation networks
- **Data Protection** – Automated data encryption and recovery to ensure data is protected and quickly restored in the event of failure or breach

CYBER RESILIENCE

- **Resilient Architectures** - Supports the design of decentralized and fault-tolerant systems, reducing the impact of cyberattacks on critical infrastructure
- **Automated Incident Response** - Automate responses to cyber incidents, such as isolating affected systems, to minimize damage

SAFETY

- **Traffic Management and Accident Prevention** – Optimize traffic flow and hazard detection using smart traffic signals and real-time alerts
- **Collision Avoidance** - Enhances real-time hazard detection and collision avoidance systems in vehicles, other modes, and transportation infrastructure

SAFETY

- **Advanced Driver Assistance Systems (ADAS)** - Supports human operators through advanced driver-assistance systems (ADAS) that monitor fatigue and ensure compliance with safety regulations
- **Accident Analysis** - Analyze vast datasets to identify patterns in accidents and recommend safety improvements such as accident hotspot analysis

CHALLENGES WITH MODERN AI

NON-DETERMINISTIC

- The same inputs will not always generate the same outputs
- Random data selection based on probability curves
- Anytime you add random data selection in connectionist models, you run the risk of non-deterministic outcomes
- If your model continues to learn, for example linear regression, the outputs will vary over time as model learns
- Expert systems generally do not suffer from this problem, but anything that has a neural network will run the risk

INSCRUTABLE

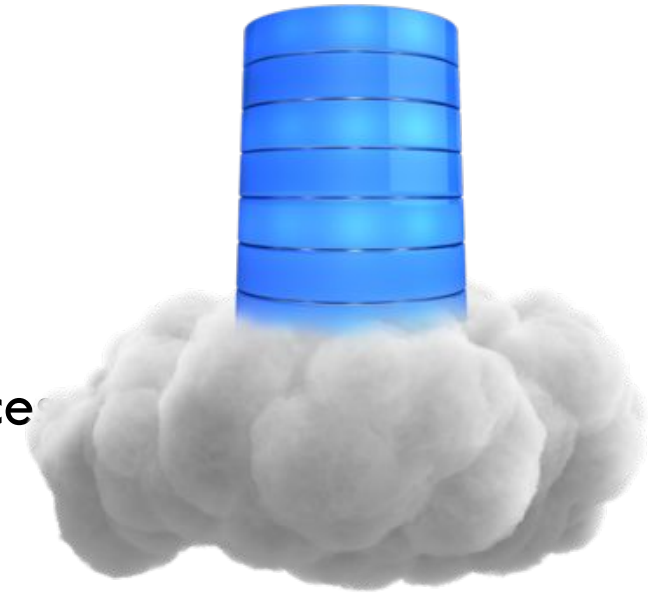
- The math and code for AI is completely understandable …..and “human-ish” readable
- The data that you use to train the model is understandable (hopefully, if you have done your job right)
- The problem is when you use the code to generate a **model** based on the data
- Due to how the model learns (developing a complex web of probabilistic weights) and is expressed, it is not possible to look at the model and understand how it works

UNEXPLAINABLE

- Since the model is non-deterministic and inscrutable, it is not easily understood
- Makes explaining “why” a model produced the exact output exceedingly difficult for neural networks
- Explainable and Trustworthy AI is an area of intense research
- Trustworthy AI can generate a trusted explanation that humans can understand

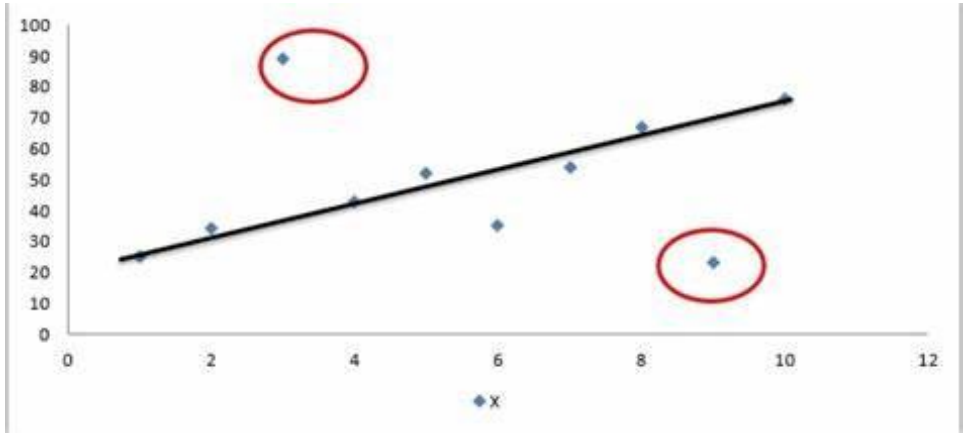
DATA PROBLEM

- Our models are only as good as our data
- Transportation data sets are in their infancy
- We are still in the great “data ownership” battle
- Our vehicle platforms lack the sensors to collect the nece
  (possible exception… Tesla)
- Models are very limited in what they can do



EDGE CASES

- Edge cases are statistical outlier events that are not part of the training data
- Though they may be rare, they can result in unexpected and undesirable outcomes
- Edge cases are where tragedy lives



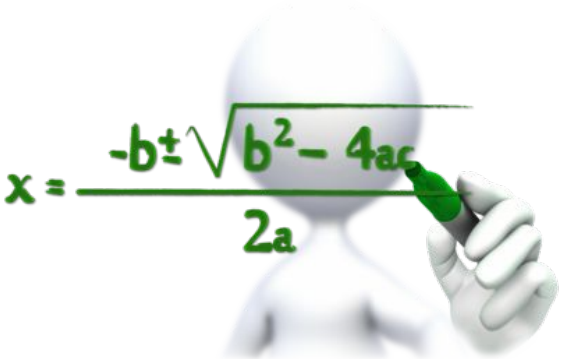
Source: Projectguru.in

AI IS NOT EXEMPT FROM ATTACK

- AI is a target of adversarial attacks
  - Data poisoning
  - Model evasion
  - Denial of Service
  - Social Engineering
  - AI software/deployment stack attacks
- Complexity if the enemy of security
- MITRE Adversarial Threat Landscape for AI Systems (ATLAS™)
- OWASP Top 10 Machine Learning Risks

LACK OF UNDERSTANDING

- Math is hard, and libraries are easy
- There are TONS of different AI models and approaches
- Poorly understood complex AI systems can increase and permeate flawed analysis and output (AI is built on data, so bad input data yields bad models)
- Overreliance on complex and poorly understood AI models can lead to vulnerabilities across the supply chain



OTHER CONSIDERATIONS

- **Interoperability** between legacy transportation systems (AS/400) and more complex AI-driven systems
- Adopting and implementing AI models requires **significant investment** in infrastructure, services, and workforce training
- Lack of consistent **regulatory and legal frameworks** can hinder implementation, especially in cross-border operations
  - Many regulations on AI, Data, and Privacy, which at times conflict with each other

AGENDA

- AI Taxonomy
- Data Science
- Opportunities
- Challenges
- Wrap-up

Thank You

Urban Jonson
ujonson@serjon.com
www.serjon.com

SERJON

Transportation Services

- Defensive Cybersecurity Advisory
- Cybersecurity Assessments
- Cybersecurity Training
- Vehicle Cybersecurity Standards and Regulatory Advisory
- General Industry Research
- Custom Threat Intelligence
- IT Operational Assessments
- AI Modelling and Security Testing

C2SMARTER
CONNECTED COMMUNITIES WITH SMART MOBILITY TO EQUITABLY REDUCE CONGESTION

NYU

TRB WEBINAR

AI's IMPACT ON SYSTEMS, ENTERPRISE, AND CYBER RESILIENCE IN TRANSPORTATION

Dr. Kaan Ozbay, Professor and Director
C2SMARTER University Transportation Center Led by New York University

Smart Cities and AI

Smart Cities: AI Solutions Powered with Big Data

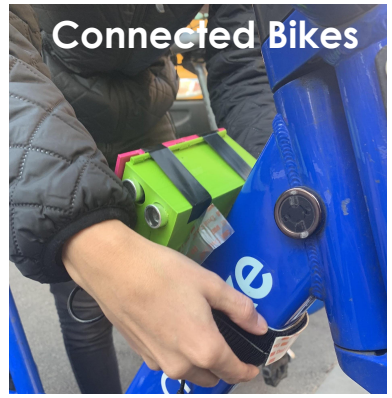
- Increase **mobility**, reduce **congestion** and improve traffic **safety** in *cities*
- **Deployments** fueled by AI/ML, big data, connected & autonomous vehicles, and ubiquitous mobile devices, sensors, fixed-, and drone-based cameras

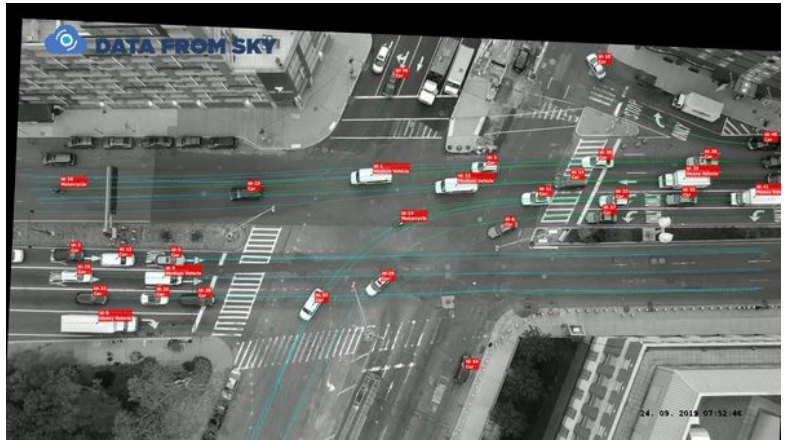
Digital twins, Cyber-physical testbeds

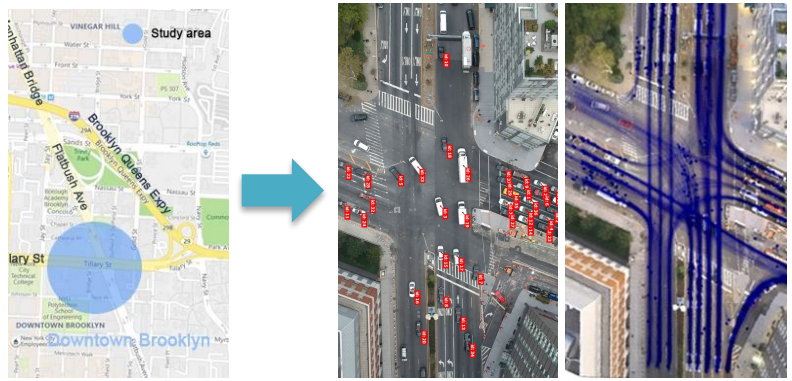
Advanced computing & communications: 6G, HPC, Edge

Emerging tech: Robotics, CAVs, AR/VR

Big data analytics: AI, Machine learning





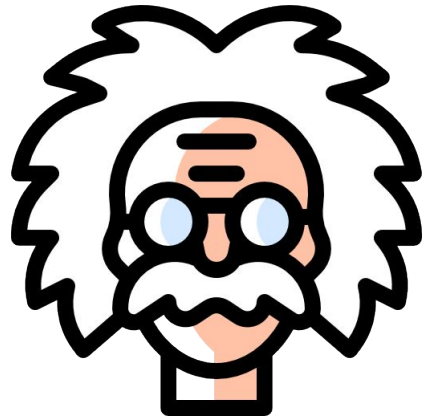


What is the future of smart cities and urban mobility in the next several decades?

Student

Dr. Einstein, Aren't these the same questions as last year's [physics] final exam?

Yes; But this year the answers are different.



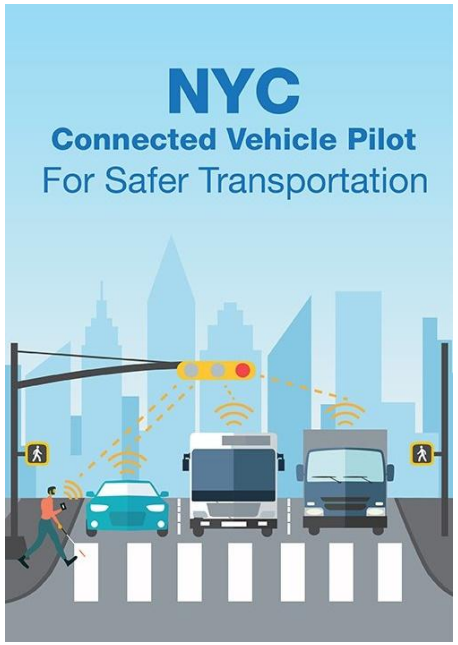
Dr. Einstein

Emerging AI/ML and other high-tech & big data solutions?

AI & Big Data for Smart Cities

NYU TANDON SCHOOL OF ENGINEERING

U.S. Department of Transportation | NEW YORK STATE OF OPPORTUNITY. Department of Transportation | NEW YORK CITY DOT



Connected Vehicle Pilot Deployment

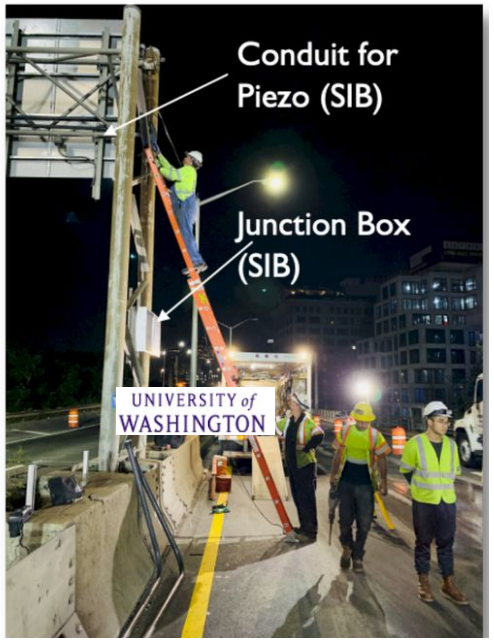
1 of only 3 U.S. DOT pilot sites in the nation

NYU CUNY

Computer Vision for Transportation Data

AI/ML retraining for decision-support data based on any camera feeds

NYU UNIVERSITY of WASHINGTON



BQE Urban Roadway Testbed

Leading partner with NYCDOT to monitor/rehab multi-billion dollar asset

NYU RUTGERS

Flood Sensors

Seed project led to deployment of a flood sensor network in NYC

NYU N.C. A&T STATE UNIVERSITY

Agent-based Digital Twin testbeds

Only available model in NYC for emerging technologies, replicated at partners' cities

NYU UTEP UNIVERSITY of WASHINGTON

C2SMARTER

Computer Vision Solutions for Smart Cities

NYU TANDON SCHOOL OF ENGINEERING

Accuracy 85%-96% depends on use case

3-Year of historical data for training

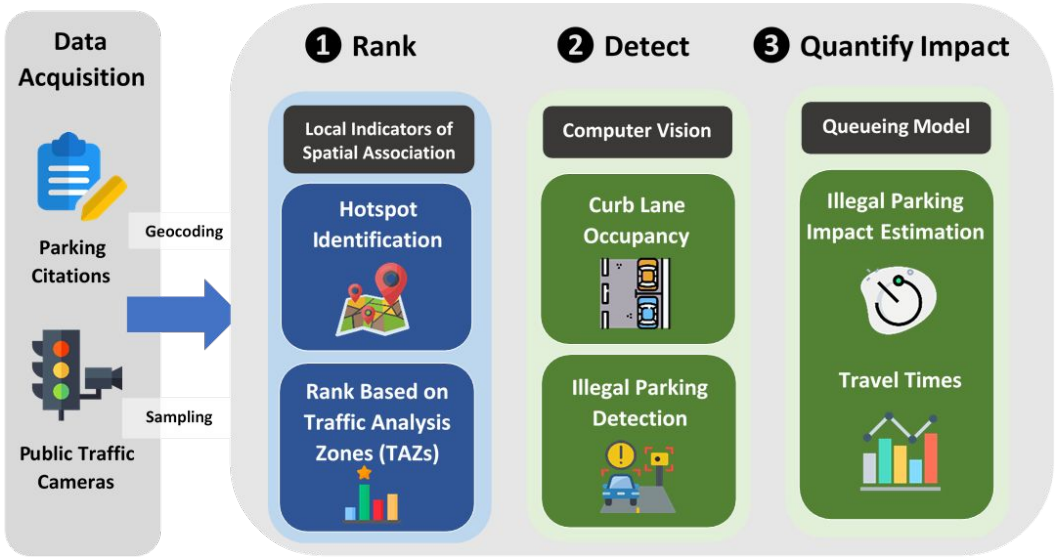
How does it work?

✔Leverages existing **~1,000 public traffic cameras** in NYC

✔Real-time object detection for vehicles and VRUs

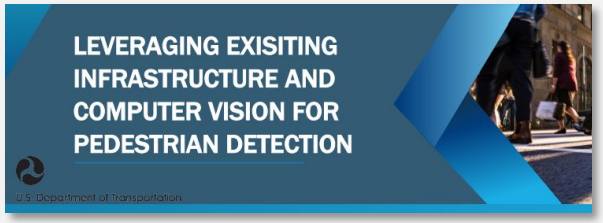
✔Post-processing filters and customized trained model for NYC

Example: Data-Driven & AI-Based Curb Lane Monitoring



Deployment Case Study Highlighted in **USDOT ITSJPO** Deployment Evaluation Database

U.S. Department of Transportation



Partnerships between **academia, agencies and industry**

NEW YORK CITY DOT

NYC DDC Department of Design and Construction

PORT AUTHORITY NY NJ AIR LAND RAIL SEA

NYC PLANNING

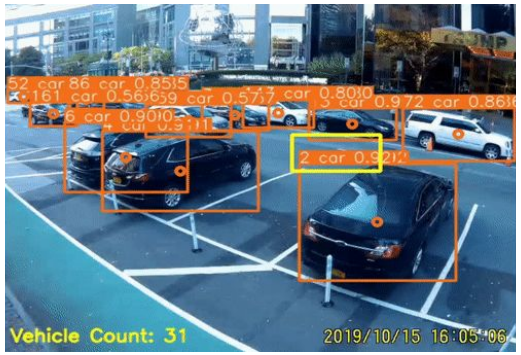
NYCOTI Office of Technology & Innovation

mobileye An Intel Company

C2SMARTER

AI-Driven Use Cases

Vehicle Counts & Speed Est.



Queue Length

Near Misses

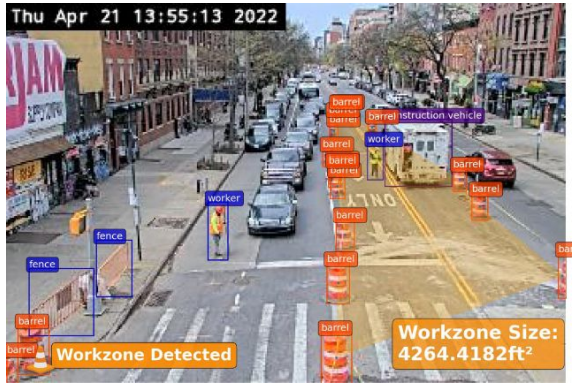
Curb/Bus Lane Occupancy

Illegal Parking

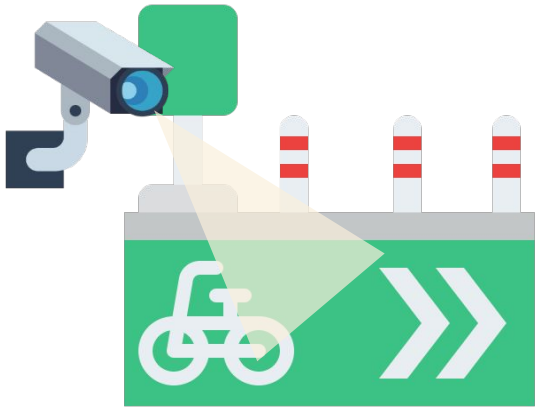
Privacy-Preserving Pedestrian Detection

Ped w Mobility Aids

Work Zone



Detection from a Bike



Use Case: Automated Inspection Technologies for Bike Lanes


Alligator Cracking


Transverse Cracking


Edge Cracking


Patching


Pothole


Drain

Image source: n-ix

C2SMART ER

ALFRED P. SLOAN FOUNDATION

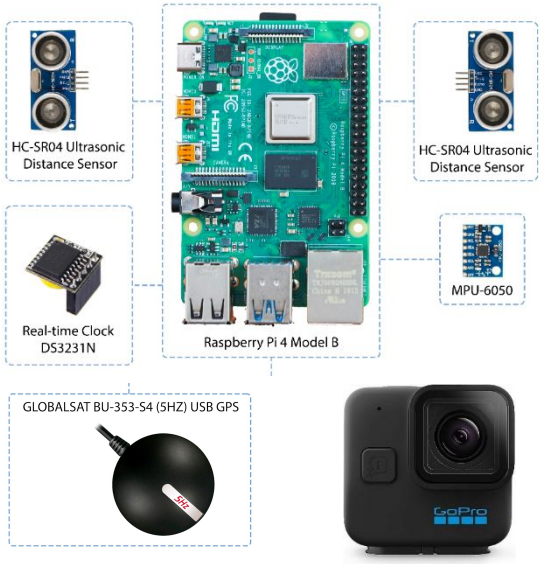
NEW YORK CITY DOT

This project is supported by Alfred P. Sloan Foundation via the Cornell Tech Pilot Policy Studio and collaborated with NYCDOT.

Research Objectives

- Test and evaluate image recognition technologies for detecting and assessing the severity of pavement distress in protected bike lanes
- Use cameras, enhanced by the team's previously developed bike sensors, mounted on both regular and cargo bikes to gather data.
- Analyze the collected data to determine the presence and severity of various distress types.
- Assist in developing bike lane pavement condition ratings (e.g., good, fair, and poor) and their thresholds.

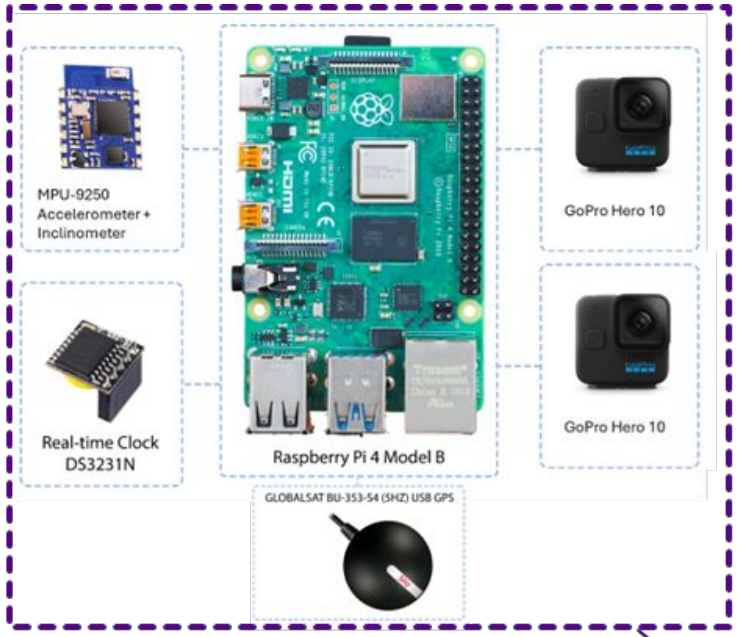
BSAFE Bike Sensor



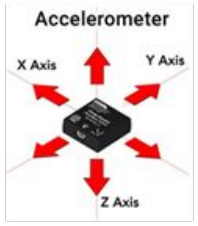
Expected Outcomes:

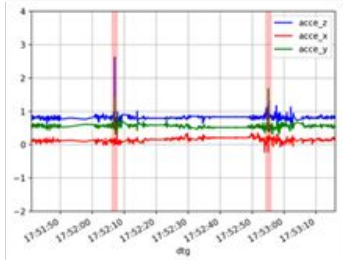
- Validated tech for assessing bike lane conditions with detailed imagery and shapefiles for NYC DOT.
- Insights for establishing suitable thresholds for bike lane pavement condition ratings (e.g., good, fair, poor)
- Actionable tech integration recommendations for NYC DOT's inspection workflows.

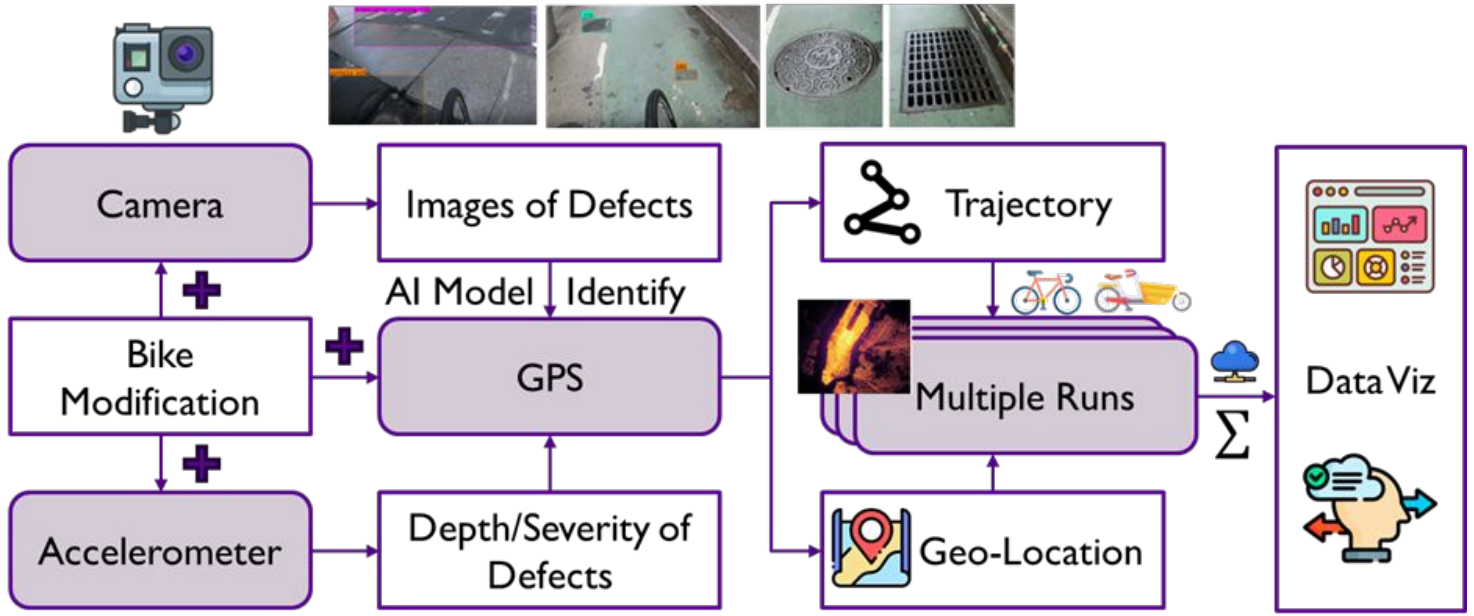
Proposed AI driven Framework



Bsafe-360
Bike Sensor System



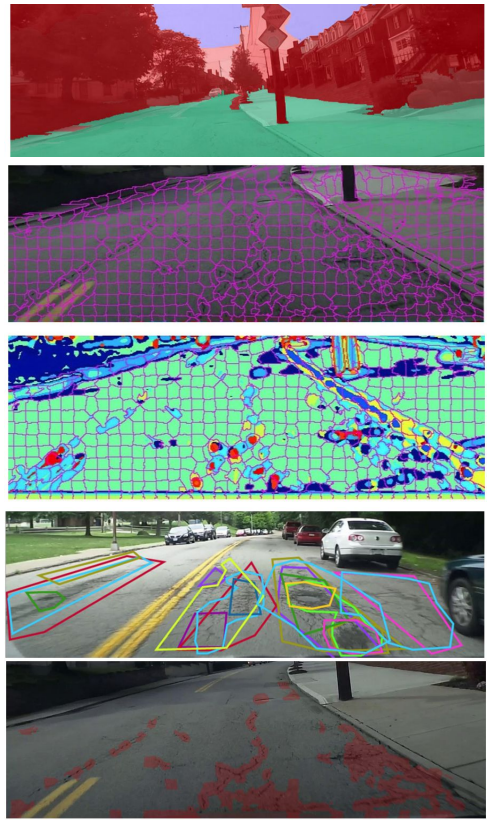




Computer Vision-Based Road Inspection

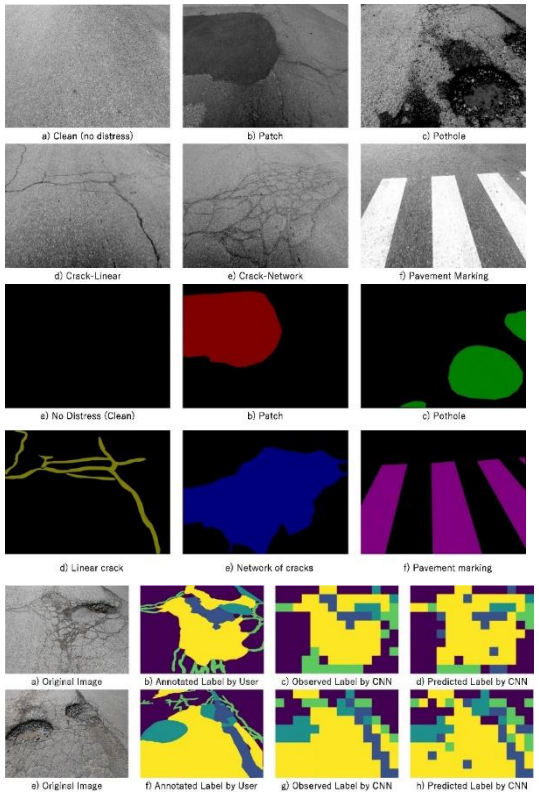
Examples of current state-of-the-art inspection algorithms for roads (not Bike Lane)

Segment the ground plane and use texture & color to detect



Varadharajan, S., Jose, S., Sharma, K., Wander, L. and Mertz, C., 2014, March. Vision for road inspection. In IEEE winter conference on applications of computer vision (pp. 115-122). IEEE.

Convolutional neural network based detection

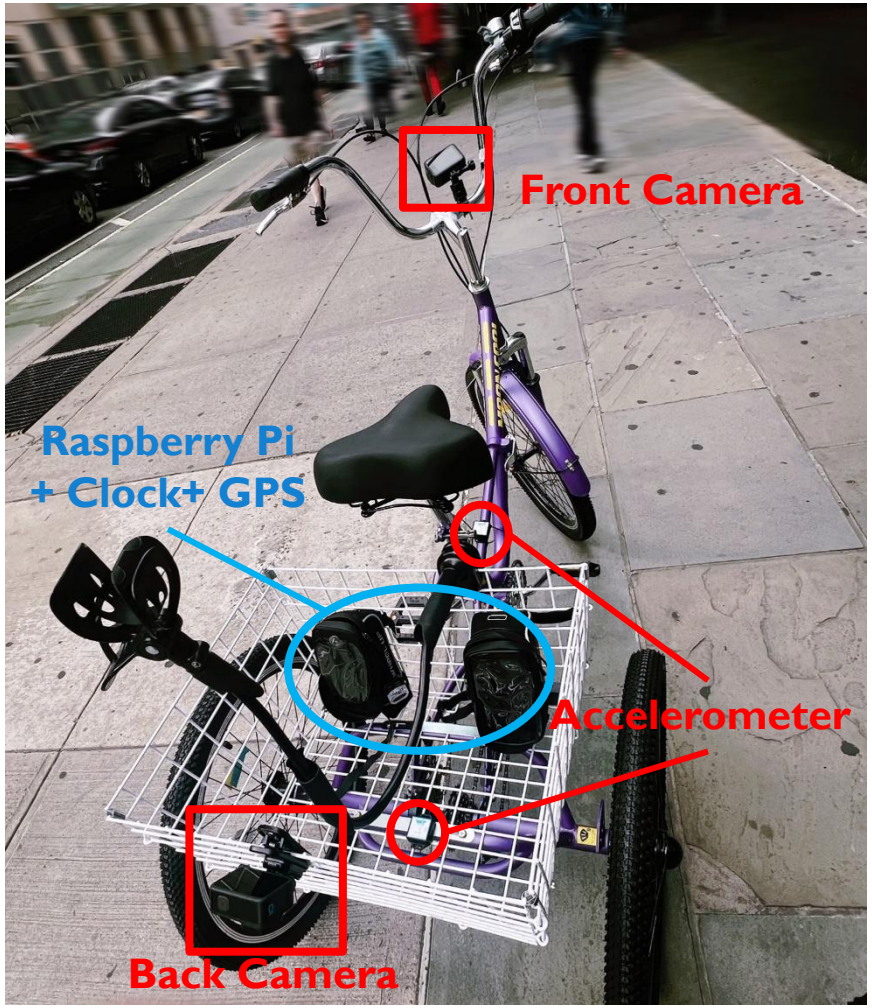


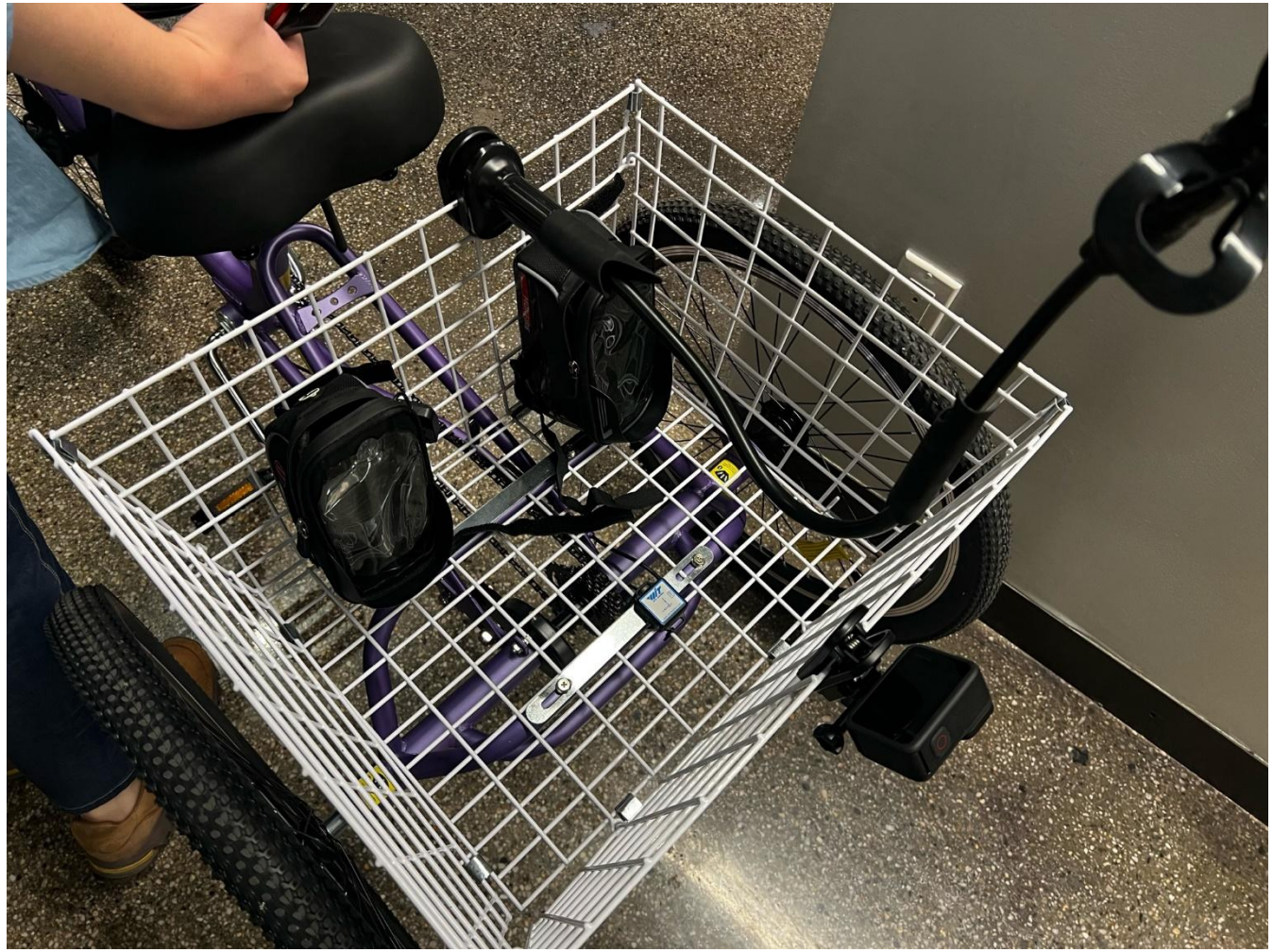
Zhang, C., Nateghinia, E., Miranda-Moreno, L.F. and Sun, L., 2022. Pavement distress detection using convolutional neural network (CNN): A case study in Montreal, Canada. International Journal of Transportation Science and Technology, 11(2), pp.298-309.

However, automated bike lane pavement assessment faces unique challenges, including:

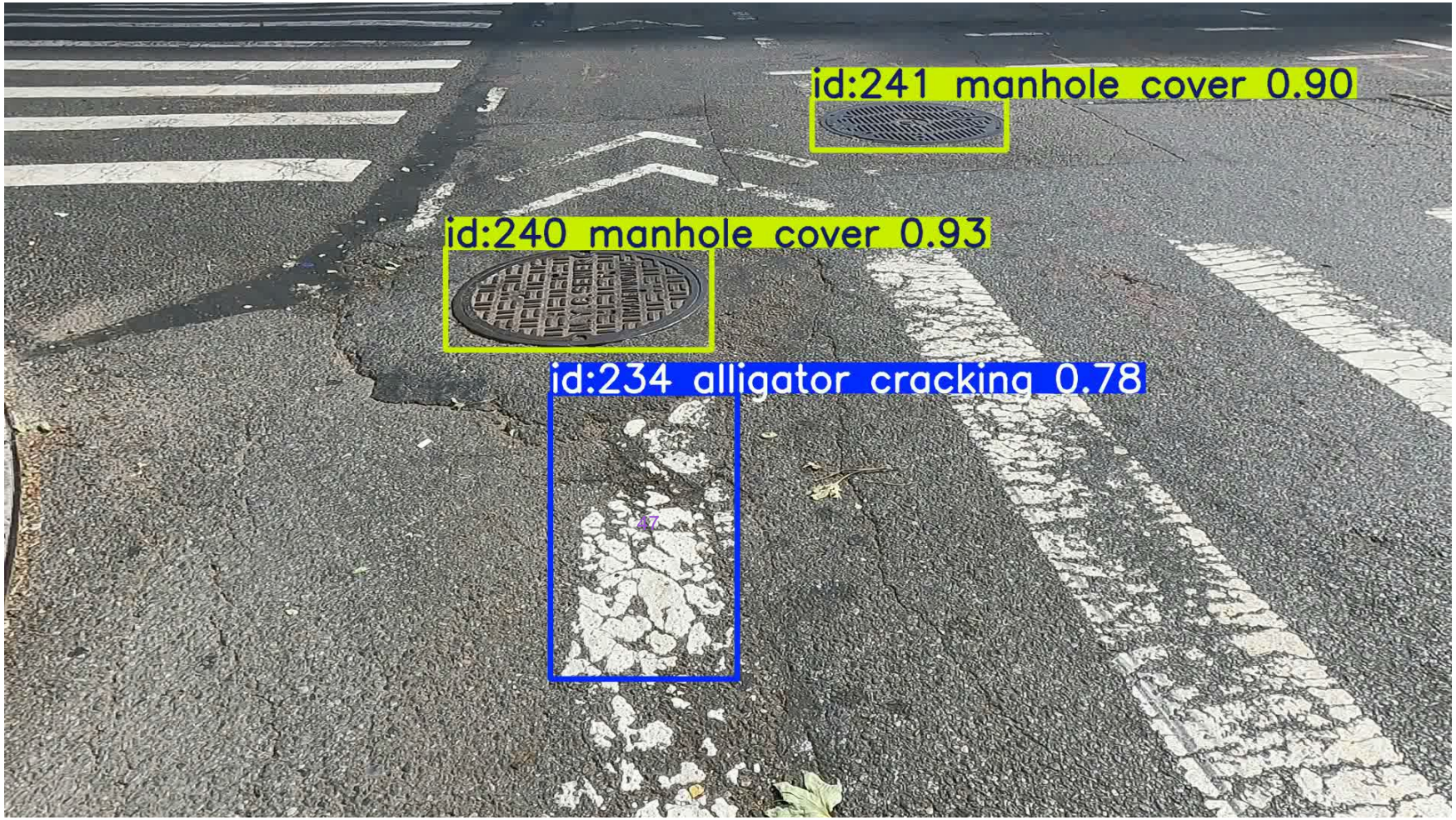
- **limited training data**
- the need to detect **both pavement distress and street hardware** (e.g., drains, grates)
- **ambiguity in defining "poor" conditions**, which differ from vehicle lanes.

Outdoor Test Setup with All Sensors

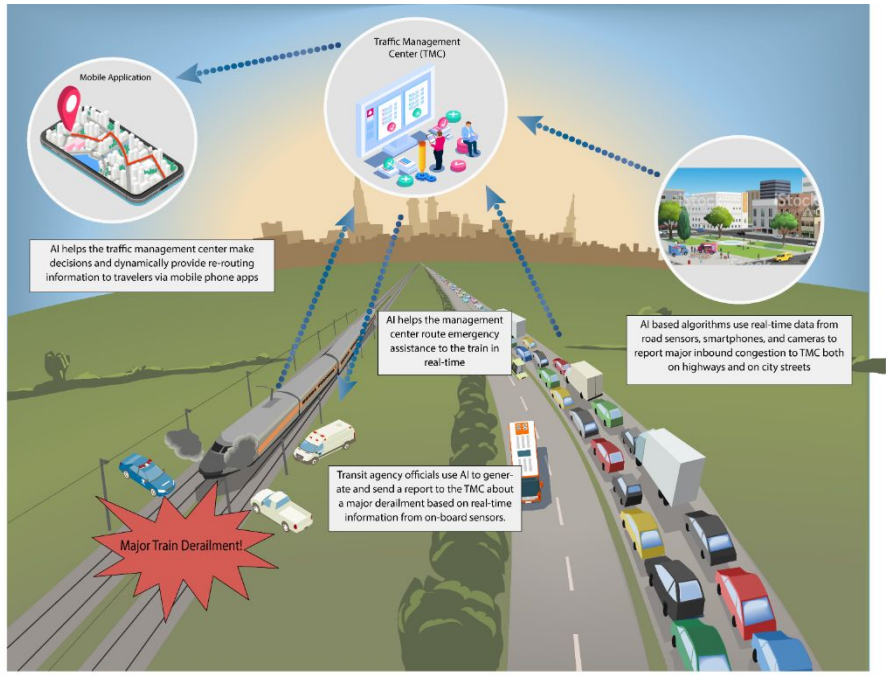




Detection Output - Video with distress ID



Potential AI Applications to Address Urban Multimodal Corridor Challenges



- **OBJECTIVE:**
  - Real-time interagency collaboration using DSS and KBES.
- **DESCRIPTION:**
  - A Knowledge Based Expert System (KBES) as part of a DSS will be used to identify participating agencies and determine response strategies and resource needs.
    - Ex: Deployment and allocation of incident removal response crews specific to the incident especially for Hazmat or major incidents, deployment of medical resources
    - The rule base can be updated and /or improved based on the past experience.
  - **BENEFITS:**
    - Reduced clearance times will reduce delays, emissions, & energy consumption across modes.
    - Risk of secondary accidents will be reduced as a result of quick clearance.

Highway Agency
(Possible Resources: Tow trucks, VMS, repair crews)

Transit Agency
(Possible resources: Track engineers, repair equipment & crews)

Train Agency
(Possible resources: Trach and train engineers, train towing equipment, etc.)

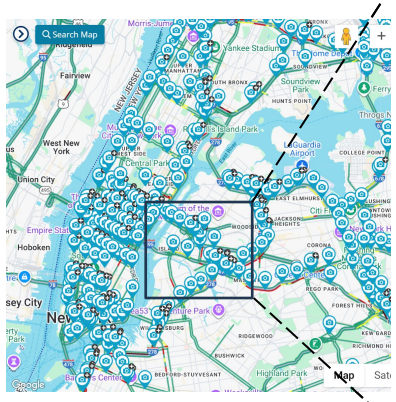
Other City Agencies
- Police Dept.
- Fire dept.
- Heath / Hospital Dept.
- OEM

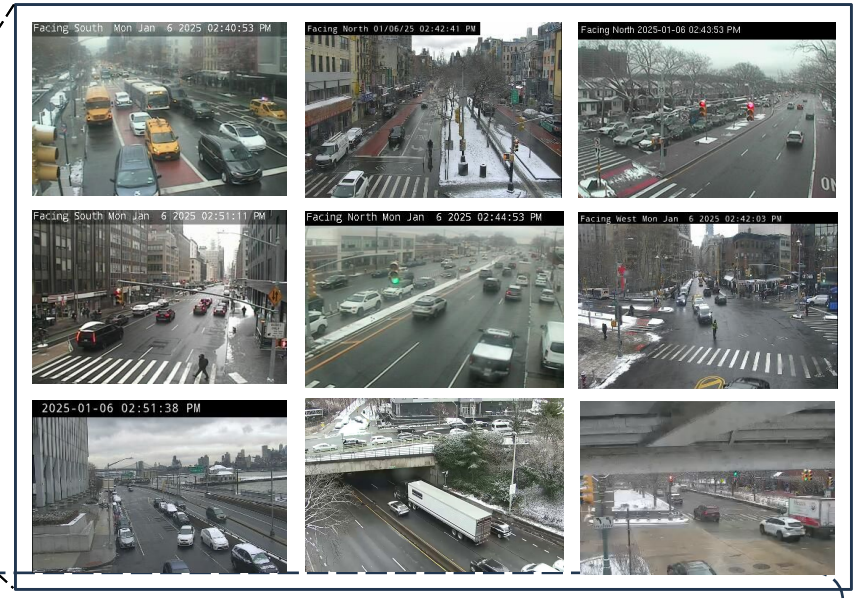
Vasudevan et al., (2020) Identifying Real-World Transportation Applications Using Artificial Intelligence (AI)-Real-World AI Scenarios in Transportation for Possible Deployment, Final Report – July 2020: FHWA-JPO-20-810

Traffic Incident Management in the Era of Generative AI and Big Data

Given existing thousands of traffic camera streaming 24/7:

1. How to find rare but safety-critical traffic incidents in large-scale video streams?
2. How to prioritize human decision-making over manual data processing?





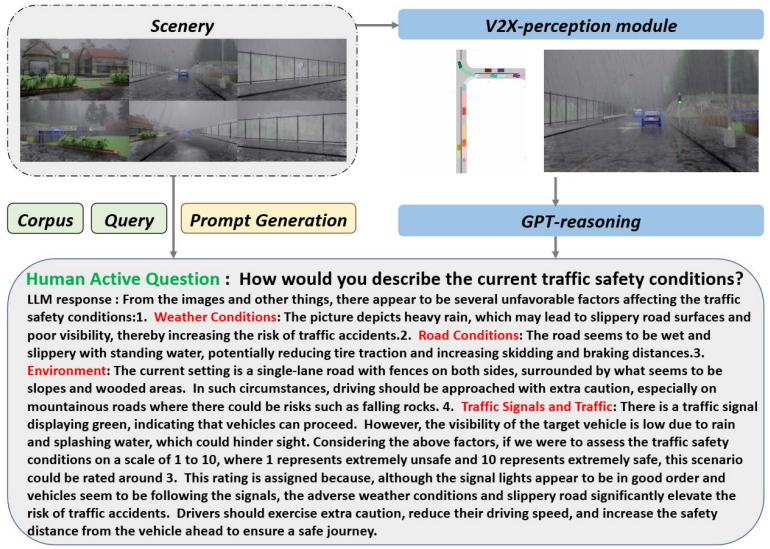
User > *Please find videos of pedestrian-vehicle conflict given this region in the past month.*
System > *There are <NUMBER> qualified videos…this conflict is from camera <ID> at <TIME>. The weather was rainy… The white truck was too close to the pedestrian in black…*

…

User > *Please export to files…*
System > …

GenAI, Vision, Language and Traffic Incident Management

- Vision and language are naturally favored by humans.
- **Multimodal Large Language Models (MLLMs)** shows promising reasoning capability:
  - Richer Understanding + Better Interaction + Versatile Applications
- We propose An MLLM-empowered Framework **SeeUnsafe** to help traffic incident management



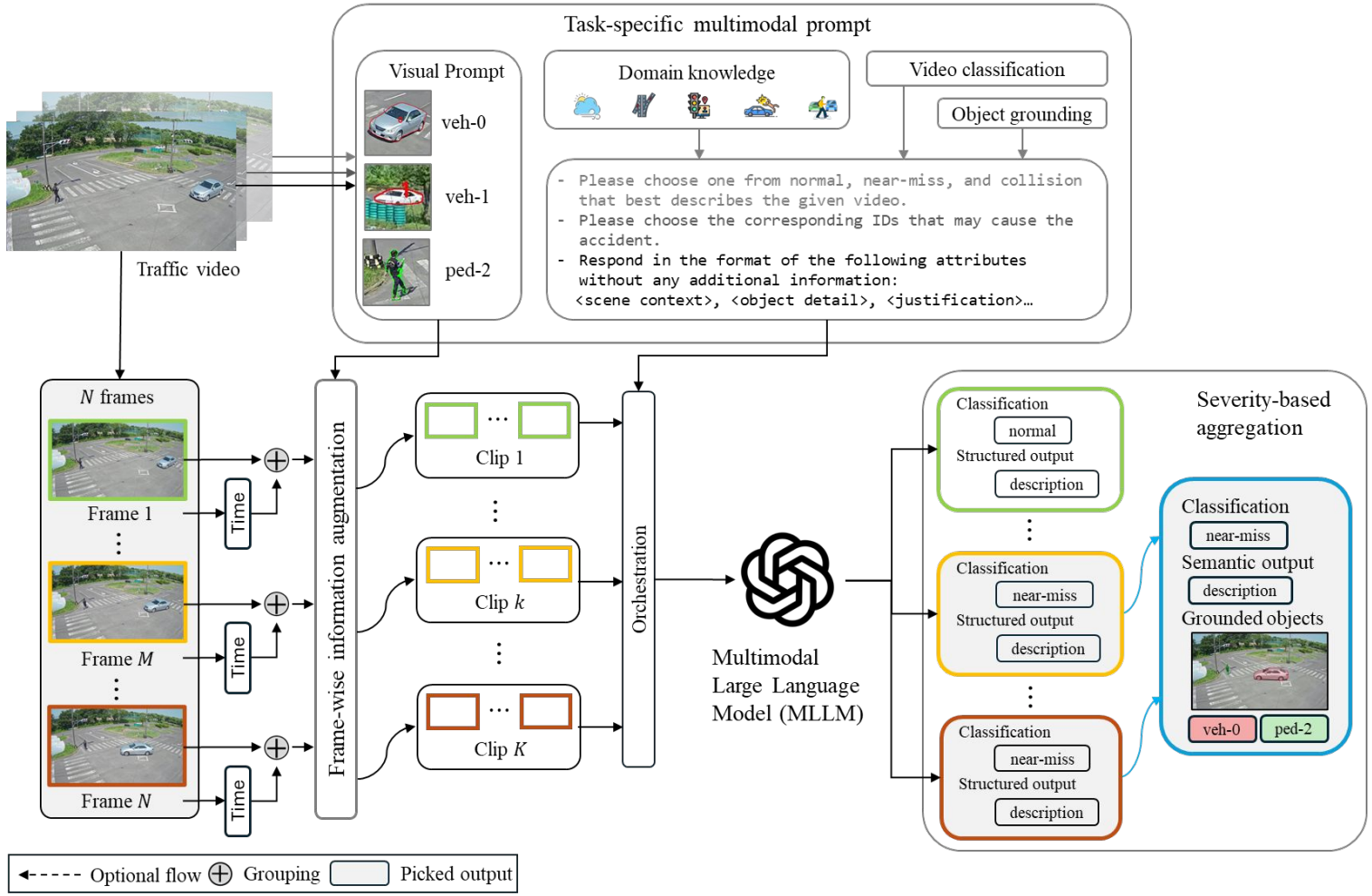
AccidentGP [Wang et al., 2024]

OmniDrive [Wang et al., 2024]

SeeUnsafe: An MLLM-empowered Framework

Methodology Highlights

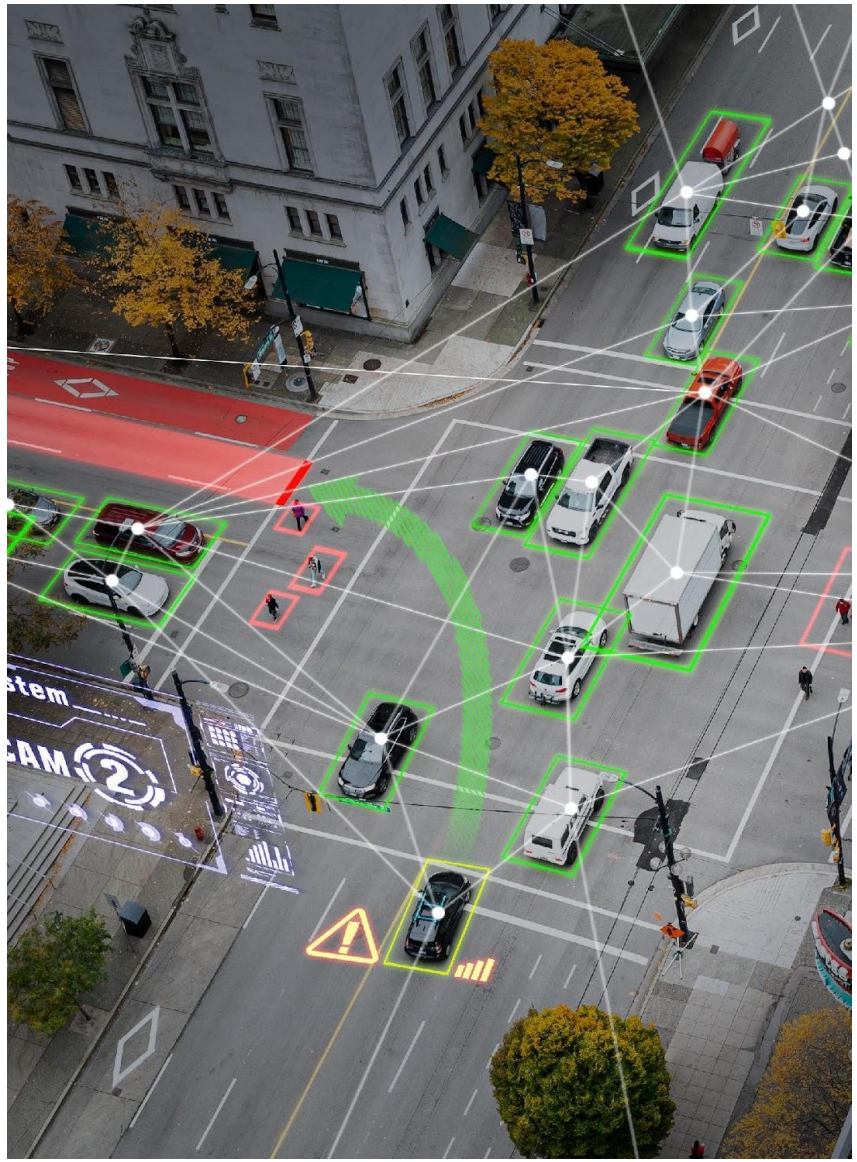
- Inject object boundary and ID on the image as visual prompt.
- Decompose video sequence into shorter clips for reasoning.
- Aggregate risky clips for visual grounding* and output summarization.



* Visual grounding: locate the most relevant object or region in an image, based on a natural language query

Final Thoughts on AI and Smart Cities

- AI+ML powered by big data continues to change the urban mobility landscape
- The rate of this change is magnitude of order faster than traditional transportation engineering applications especially to the game changing innovations in AI
  - GenAI
  - Physics Informed AI
- Academia is still playing an important role but companies of different size and capabilities are becoming important actors in the implementation and application of AI in our cities
  - Google – Simulation Calibration for Digital Twin
  - NVIDIA – Autonomous vehicles
  - Siemens Mobility –AI-driven traffic signal optimization and smart rail systems
  - GridMatrix – Near Misses and digital infrastructure
  - Goodvision – Live traffic monitoring



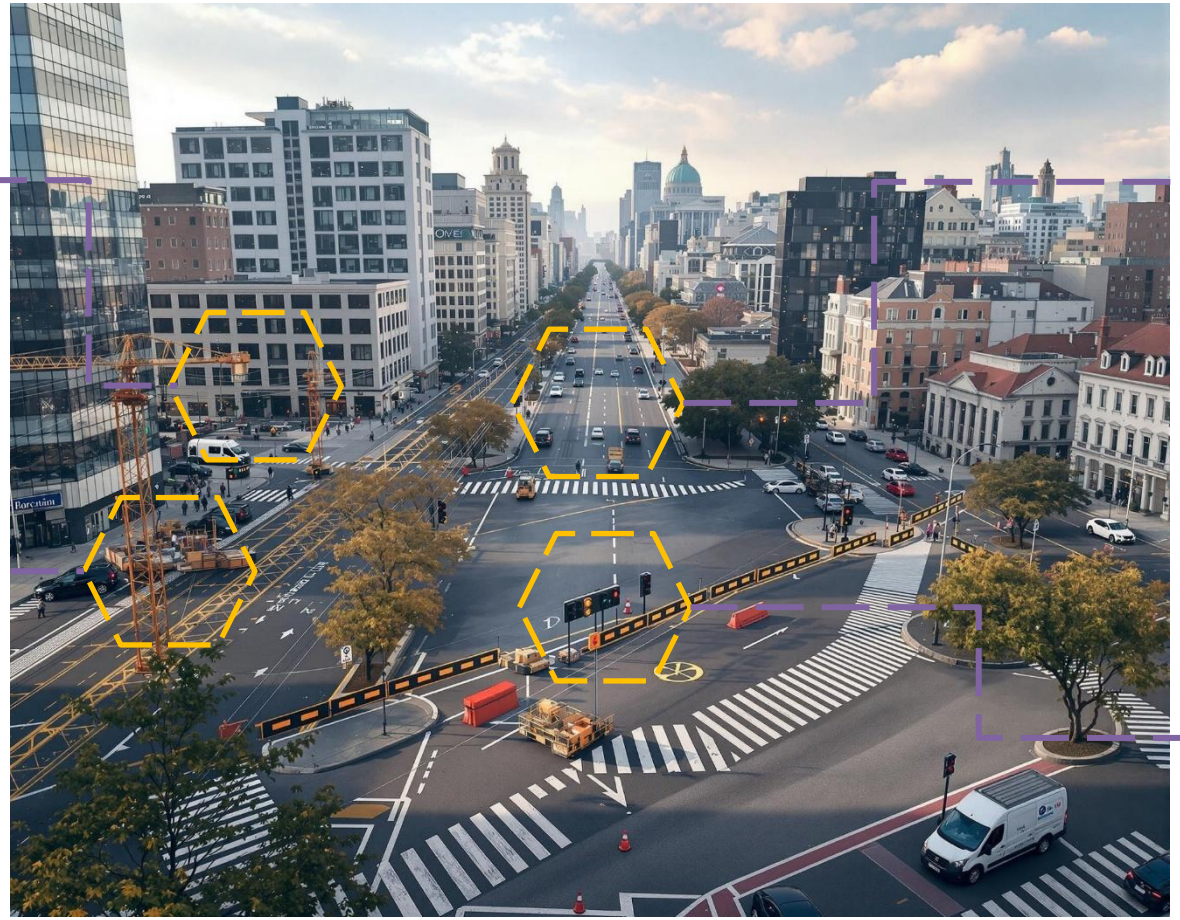
Challenges

- However, all these developments due to AI do not come without some warnings. Some of the important issues when it comes to using AI for real-world applications are
  - How do we evaluate and validate AI based systems?
  - How we guarantee fairness and ethical behavior of AI based systems?
  - What are the resources needed to maintain and upgrade AI based systems in the context of TSMO and other real-world applications
  - What are the training needs for transportation engineers to use AI effectively?
  - Many other questions…

- **Future directions:** **Human expert knowledge** is crucial to enforce common sense and cause-effect relationships.

The Road Ahead for Generative AI in Transportation

GenAI: A hero or a villain



C2SMARTER
CONNECTED COMMUNITIES WITH SMART MOBILITY TO EQUITABLY REDUCE CONGESTION

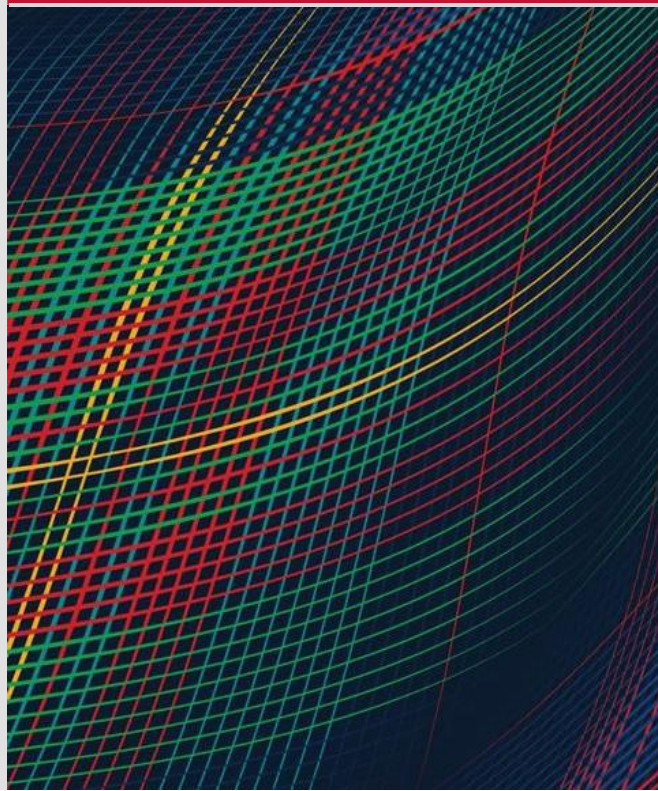
NYU

New York University
Tandon School of Engineering
6 MetroTech Center, 4th Floor
Brooklyn, NY 11201

c2smarter@nyu.edu
c2smarter.engineering.nyu.edu

Carnegie Mellon University
Software Engineering Institute

Cybersecurity Implications of Artificial Intelligence



MARCH 26, 2025

John Haller

Agenda

Carnegie Mellon University Software Engineering Institute

- Managing the Risks of Using Artificial Intelligence to Support Critical Services
- Artificial Intelligence in Support of Cybersecurity
- Threat Actor Use of Artificial Intelligence

Carnegie Mellon University
Software Engineering Institute

Managing the Risks of Using Artificial Intelligence to Support Critical Services

CERT-Resilience Management Model (RMM)

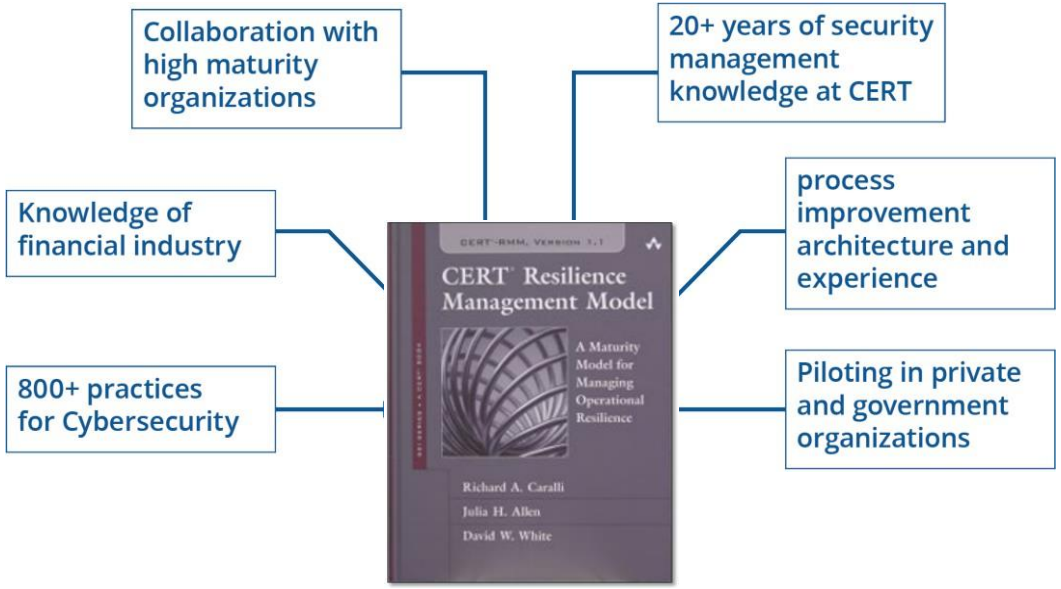
Carnegie Mellon University Software Engineering Institute

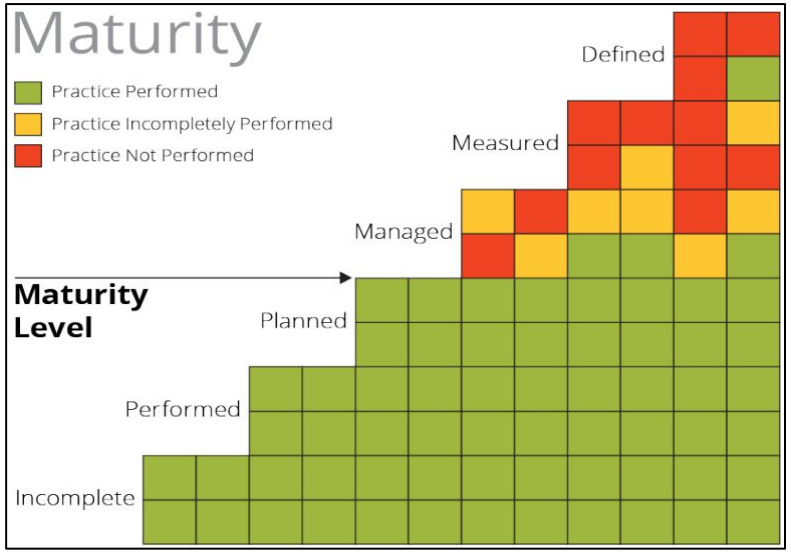
A maturity model for managing and improving operational resilience

- Defines maturity as driven by consistency, efficiency, and risk
- Enables assessment and measurement

Eight Core Principles:

- Mission Focused
- Risk Based
- Efficiency Oriented
- Standards and Regulation Neutral
- Requirements Driven
- Converged Approach
- Collaborative
- Process Maturity and Improvement Foundation

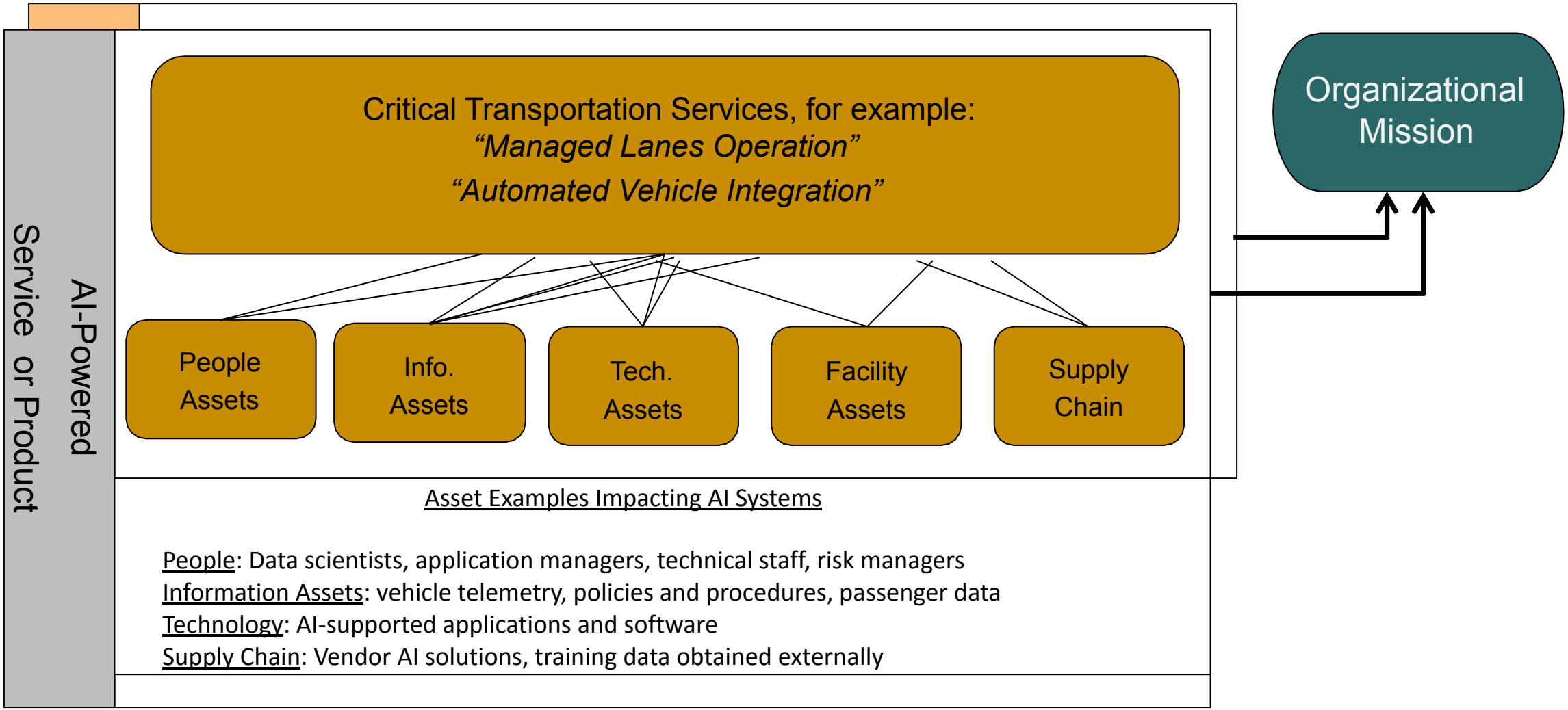




CERT-RMM combines best practices for cybersecurity from leading organizations and numerous standards and codes of practice.

Service-Asset Relationships and Asset Types

Principles for managing resilience and technology risk remain the same ….



AI Conditions, Threats, and Risks Impacting Critical Services

Threats

- Data leakage
- Data poisoning
- Application attacks
  - Prompt Injection
  - Adversarial data inputs
- Hallucinations
- Bias

Implementation Challenges

- Ill-defined problem statement
- Lack of expertise
- Model-system-data disconnection
- Data challenges
- Lack of explainability

Potential Risks:

- Reputational damage
- Legal or contractual claims
- Compliance problems
- Project delays
- Operational disruptions
- Information security breach

Better news … You probably already have processes to help manage AI related risks.

Concern	Organizational Capabilities	Recommended Action	Resource
Risk exceeding enterprise tolerance	Risk Management	• Update policies and procedures • Identify enterprise risk appetite and measures • Integrate AI concerns into existing governance routines • Evaluate data management standards and program	OCTAVE FORTE – Carnegie Mellon University NIST AI Risk Management Framework
Data leakage	Data Loss Prevention Access Management Web Controls	• Review existing controls: -Web filtering for public AI tools -Identify toxic combinations and entitlements -Inspecting web page traffic	NIST Publication 800-53 NIST Cyber Security Framework CERT Resilience Management Model
Application attacks	Software and application testing Application logging and monitoring Internet protections	• Expand the scope of application testing • Tune Web Application Firewalls • Log application activity based on risk	OWASP Top Ten for LLMs, https://genai.owasp.org/llm-top-10/
Data Poisoning	Integrity checks Segmentation Privileged identity management Multi-factor authentication	• Identify critical data supporting AI solutions and ensure existing information security controls provide coverage	NIST Publication 800-53 NIST Cyber Security Framework CERT Resilience Management Model
Supply Chain Risks	3rd party/vendor management	• Apply practices for external dependency and 3rd party risk management to AI solutions and data • Update due diligence questions and 3rd party monitoring, risk manage the findings • Understand and assess the risk of your data supply chain	

Artificial Intelligence in Support of Cybersecurity

Carnegie Mellon University
Software Engineering Institute

Machine Learning Dimensions*

Carnegie Mellon University
Software Engineering Institute

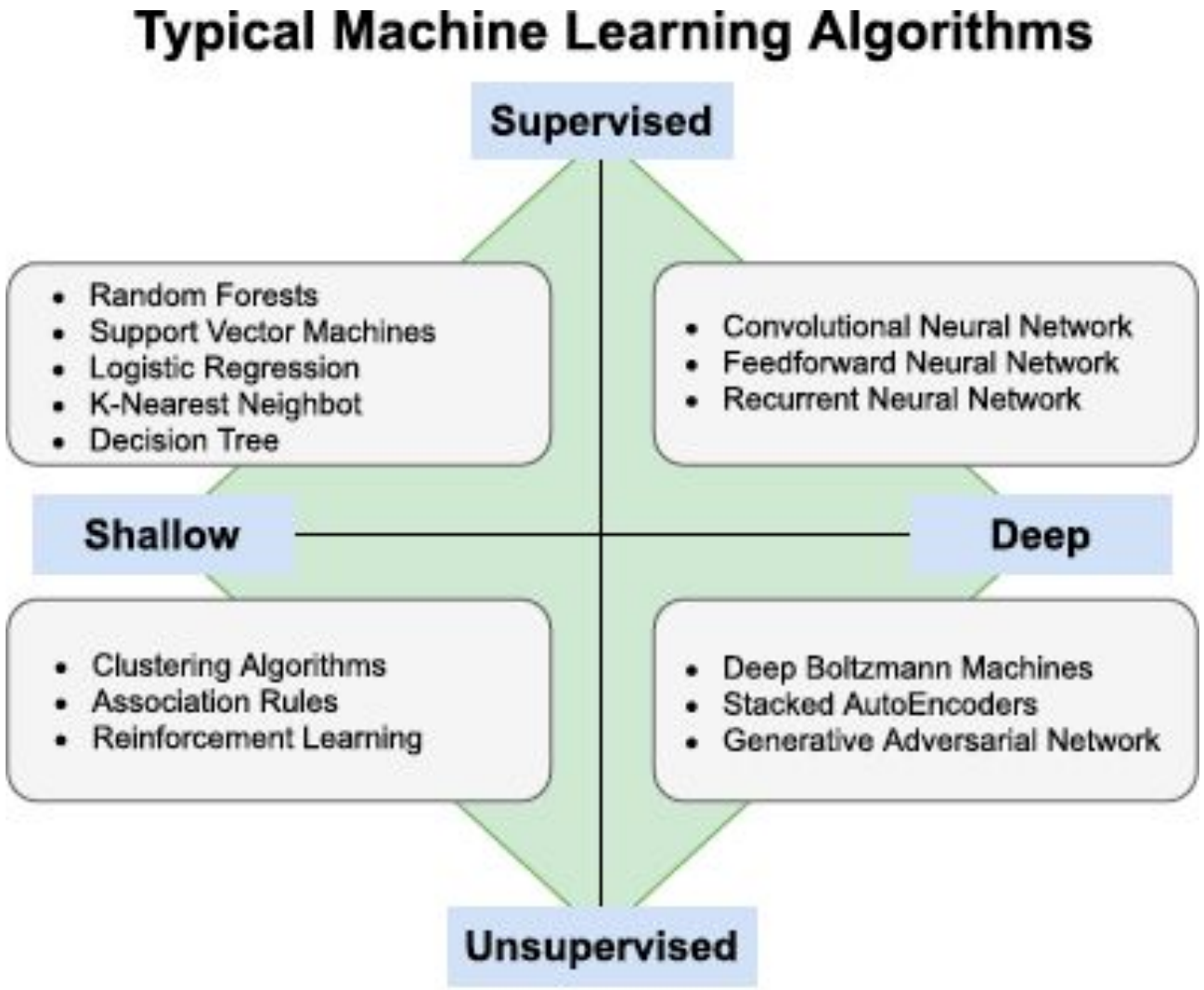


*Diagram from [APRUZZESE 2023]

Supervised Model: The model learns from datasets that have already been labelled

Unsupervised Model: There are labels assigned to the data and the model identifies relationships in the data

Deep Learning: Models that use neural networks.

Typical Uses of Machine Learning for Cybersecurity

Threat Detection

- Network Intrusion Detection
- Malware Detection (HIDS)

  Static – less effective against polymorphic malware even with machine learning techniques

  Dynamic – more effective against polymorphic malware and other evasion techniques
- Phishing Detection – supervised models focused on malicious webpages and emails

Additional and Emerging Use Cases

Alert Management
- Filtering
- Prioritization
- Fusion and analysis

Optimizing labels for supervised models Risk exposure assessment
- Penetration testing
- Identifying compromised hosts Cyber Threat Intelligence – quicker conversion of intelligence to IOCs Insider Threat Hunting

Fraud / AML

Summarizing open-source Intelligence

Interpretation of policies, standards, and procedures

Supporting policy and regulatory harmonization

Security consulting to organization

Incident ticketing and summarizing cases

Implementation Problems and Considerations

- Concept Drift – the original training data may become less relevant over time (based on use case).
- Adversarial Samples – threat actors use input data to compromise model predictions.
- Confidentiality – limits the ability to read and interpret training and operational data, both within networks and organizationally.

Commercial-off-the-Shelf (COTS) product limitations

- Limited scope- the training data may not be specific to the organization
- Lack of transparency – unknown levels of robustness and difficulties establishing explainability.

Threat Actor Use of Artificial Intelligence

Carnegie Mellon University
Software Engineering Institute

Snapshot and High-Level Summary

Carnegie Mellon University Software Engineering Institute

Threat Actor Use of Artificial Intelligence	Likely Impact	Recommendations
Attack automation and speed • Phishing emails • Malware • Reconnaissance New business models in the criminal ecosystem	Increasing velocity and scalability of attacks	• Consider more advanced anomalous activity monitoring • Consider more frequent control reviews • Review sources and analysis of threat intelligence
Use of Generative AI to support fraud scams • Reconnaissance • Business Email Compromise • Impersonation (using Deepfakes) • Various attacks on authentication	Increased likelihood and impact of successful fraud scams and attacks	• Review and test operational and business controls for design and operational effectiveness • Implement Multi-factor Authentication
Use of Generative AI to fabricate realistic-seeming content for various purposes	Potential increased reputational risk to organizations and governments	• Consider enhancing environmental scanning • Review crisis response and communication plans with stakeholders

Questions?

Carnegie Mellon University Software Engineering Institute

John Haller
Technical Manager – Cyber Assurance
CERT Division, Software Engineering Institute, Carnegie Mellon University
jhaller@cert.org
LinkedIn: www.linkedin.com/in/john-haller-pittsburgh/

Sources

[SEI 2016]

Software Engineering Institute. *CERT Resilience Management Model (CERT-RMM) Version 1.2.* Software Engineering Institute. 2016. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084

[SEI 2020]

Tucker, B.. A Risk Management Perspective for AI Engineering, Software Engineering Institute. 2020 https://insights.sei.cmu.edu/library/a-risk-management-perspective-for-ai-engineering/

[SEI 2020A]

Tucker, B. (2020, November 17). Advancing Risk Management Capability Using the OCTAVE FORTE Process. Retrieved March 25, 2025, from https://doi.org/10.1184/R1/13014266.v1.

[APRUZZESE 2023]

Giovanni Apruzzese, Pavel Laskov, EdgardoMontes de Oca,WissamMallouli, Luis Búrdalo Rapa, Athanasios Vasileios Grammatopoulos,

and Fabio Di Franco. 2023. The Role of Machine Learning in Cybersecurity. Digit. Threat.: Res. Pract. 4, 1, Article 8

(March 2023), 38 pages. https://doi.org/10.1145/3545574

[FS-ISAC 2024]

Financial Sector Information Sharing and Analysis Center, Building AI Into Cyber Defense, Retrieved March 24, 2025, from https://www.fsisac.com/knowledge/ai-risk

Today's Presenters

Urban Jonson
ujonson@serjon.com
Serjon, LLC

John Haller
jhaller@cert.org
The CERT Division, Carnegie Mellon University

Kaan Ozbay
kaan.ozbay@nyu.edu
New York University

Matt Miller
mmiller@camsys.com
Cambridge Systematics

Upcoming events for you

April 30, 2025

TRB Webinar: Implementation of Uncrewed Aerial Systems (UAS) into Transportation Infrastructure Inspection

May 27-29, 2025

TRB's Conference on Data and AI for Transportation Advancement

https://www.nationalacademies.org/trb/events

NATIONAL ACADEMIES Sciences Engineering Medicine

TRB TRANSPORTATION RESEARCH BOARD

Subscribe to *TRB Weekly*

If your agency, university, or organization perform transportation research, you and your colleagues need the *TRB Weekly* newsletter in your inboxes!

Each Tuesday, we announce the latest:

- RFPs
- TRB's many industry-focused webinars and events
- 3-5 new TRB reports each week
- Top research across the industry

Spread the word and subscribe!
https://bit.ly/ResubscribeTRBWeekly

NATIONAL ACADEMIES Sciences Engineering Medicine

TRB TRANSPORTATION RESEARCH BOARD

Discover new TRB Webinars weekly

Set your preferred topics to get the latest listed webinars and those coming up soon every Wednesday, curated especially for you!

https://mailchi.mp/nas.edu/trbwebinars

And follow #TRBwebinar on social media

@NASEMTRB
@NASEMTRB
Transportation Research Board

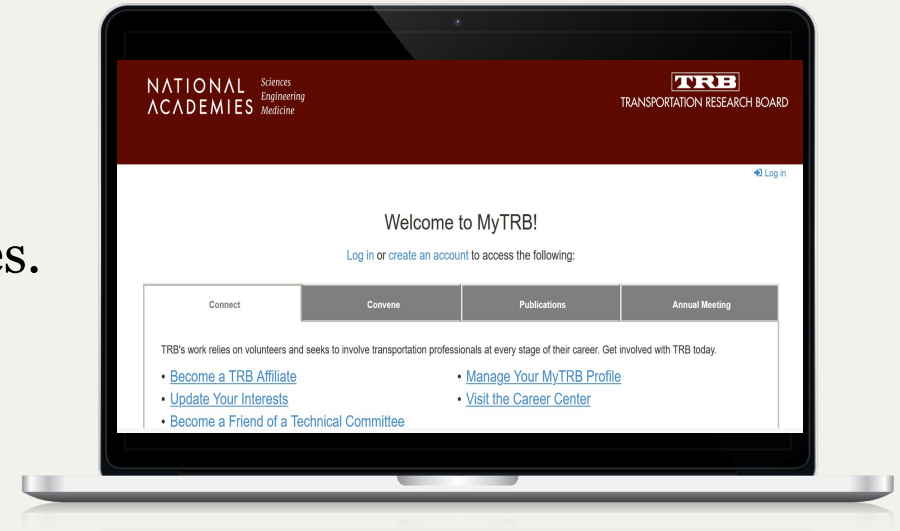
NATIONAL ACADEMIES Sciences Engineering Medicine
TRB TRANSPORTATION RESEARCH BOARD

Get involved

TRB mobilizes expertise, experience, and knowledge to anticipate and solve complex transportation-related challenges.

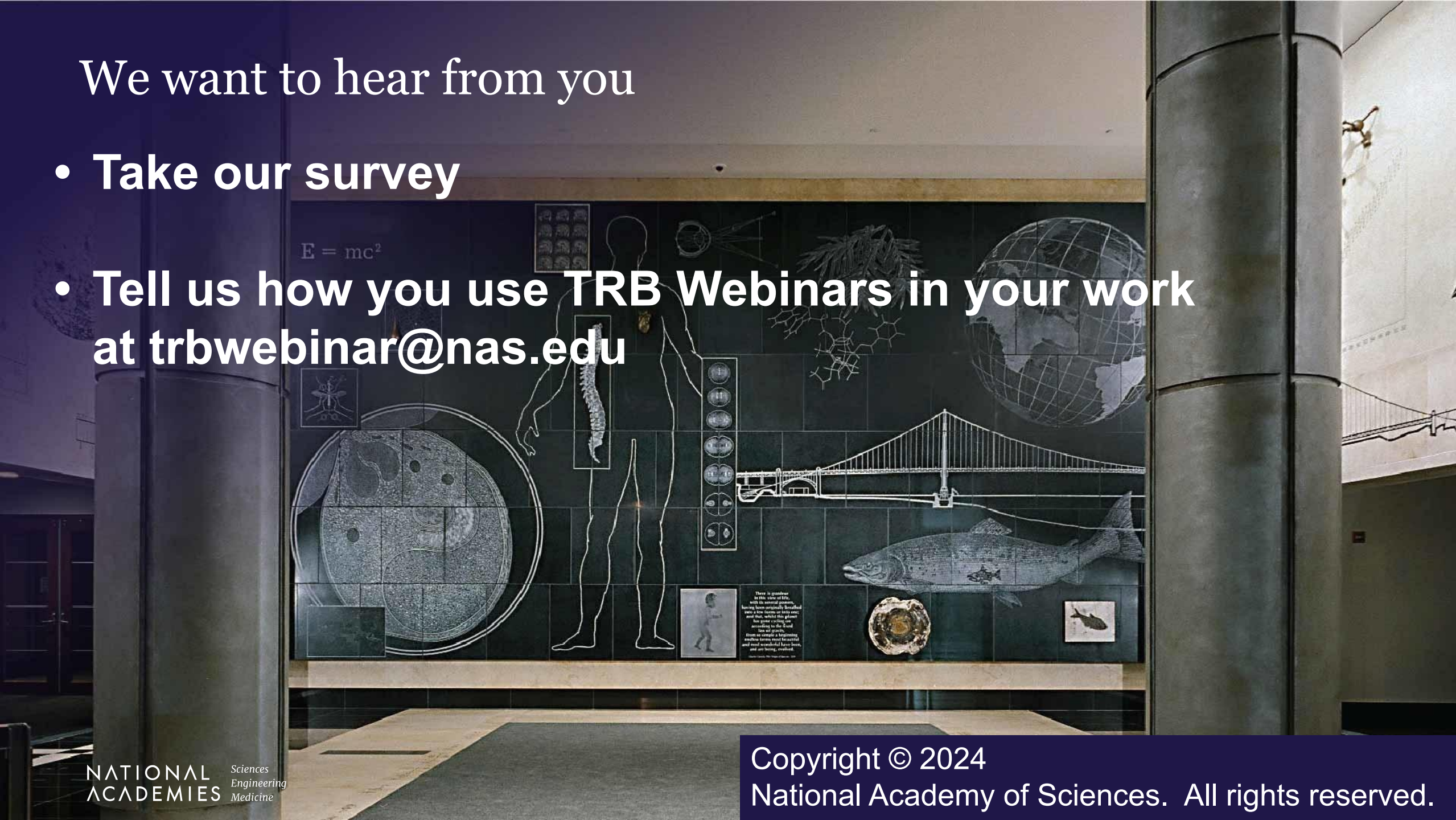
TRB's mission is accomplished through the hard work and dedication of more than **8,000 volunteers**.

https://www.nationalacademies.org/trb/get-involved



We want to hear from you

- **Take our survey**
- **Tell us how you use TRB Webinars in your work at trbwebinar@nas.edu**



NATIONAL ACADEMIES Sciences Engineering Medicine