UNIVERSITY OF MARYLAND

WORKSHOP AND SHORT COURSE

CALL FOR PAPERS

Cyber and Digital Information in Railway Engineering and Operations

MARCH 7TH-8TH, 2024

University of Maryland
Kim Building, College Park

March 7th: Short Course on Cyber Rail - 9:00am-3:00pm

March 7th: 5:00pm-7:00pm - Reception

March 8th: 8:30am-4:30pm - Workshop

ABOUT

The past decade has witnessed rapid advancements in digital and cyber technologies. Key drivers of this trend include the so-called Big Data revolution, coupled with recent breakthroughs in artificial intelligence and the sub-field of machine learning. These breakthroughs continue to generate much value across different domains of railway engineering and operations. At the same time, major challenges have arisen with regard to data storage, data sharing, privacy, and other cyber related concerns. Railway transportation will contribute greatly to mobility in the future, and digitalization, cybersecurity, and artificial intelligence are key to higher capacity and passenger satisfaction. Rail cybersecurity is a fundamental requirement for smooth and safe operations. The increased connectivity and digitalization of rail systems and the heavy dependence on new technologies, such as the Internet of Things (IoT), sensors, and other tools have created cyber vulnerabilities in rail systems and operations, leading to the possibility of cyber attacks. Railway operations involve a range of scheduling activities, from operational train dispatching to provisional timetables. Incorrect decisions can have a major influence on operations and safety. Quantum computing in railway engineering and operations is relatively new, and its formulation and analysis is at an early stage. The future use of digital twins in railway track engineering is very promising. A digital twin provides a computational model (or set of couples) that evolves over time to persistently represent the railway structure, components, systems, and processes. Digital twins underpin intelligent automation by supporting data-driven decision-making and enabling asset-specific analysis and system behavior. Within the context of railway systems, digital twins represent the flow of information among connected platforms and the central clearinghouse for data and visualization. As railway agencies convert to digital twin capabilities, they must migrate towards continuous real-time railway data models and calibrate by pairing data from real-time sensors, meters, and weather.

Suggested Topics

- Data Sharing and Railway Maintenance and Operations
- Theory-Guided Machine Learning
- Digital Twins in Railway Track Engineering
- Quantum Computing and Information in Railway Operations
- Blockchain Applications
- Detecting Cyber-attacks in Railway Systems
- Implementing Digital Safety in Rail Systems
- Adapting Cybersecurity to Rail Environments
- Applications

IMPORTANT DATES:

SUBMISSION OF ABSTRACT

January 15th, 2024

NOTIFICATION OF ACCEPTANCE

February 1st, 2024

COURSE ON CYBER RAIL

March 7th: 9:00AM-3:00PM

March 7th: Reception 7:00pm-8:00pm

WORKSHOP DATE

March 8th, 2024: 8:30am-4:30pm

Papers must be clearly presented clearly in English. Electronically submit papers to niiokine@umd.edu

Questions? Contact Prof. Nii Attoh-Okine niiokine@umd.edu

Call for Sponsors:

The University of Maryland **Digital and Cyber Center for Railway Engineering and Operations** workshop is soliciting sponsorships for the conference in order to help fund scholarships and travel stipends for participating students and to cover other workshop expenses. Reception sponsors are also sought. Sponsorships are available in the following categories.

Short Course on Cyber Rail

Course Overview: This course presents an overview of cybersecurity applications in railway engineering and operations. It is designed to equip railway professionals and decision-makers with the expertise needed to identify and take action against cyber threats, including threats targeting train control systems, signaling systems, data storage, passenger information systems, and track station infrastructure. No prior knowledge of cybersecurity is required.

Audience: This course is designed for all practitioners and decision-makers with professional interests in railway engineering and operations.

Course Outline:

- Railway Digital Tecnology
    - Machine Learning and Artificial Intelligence
- Cyber Security Fundamentals
- Railway Cybersecurity: Challenges and Threat Vectors
- Requirements and Standards for Rail Transportation Cybersecurity
- Examples of Cyberattacks

Sponsors:

[Platinum] at $2,000

[Gold] at $1,000

[Silver] at $750

Technical Research and Industry Contributions

- Full paper: Completed research results (6 pages)
- Short paper: Work in progress/fresh development (3 pages)
- Invitations will be extended to the authors of selected full papers for submission to an ASCE/IEEE journal special issue.