The 49th Annual Conference of the
IEEE Industrial Electronics Society
October 16-19, 2023, Marina Bay Sands Expo and Convention Centre
Singapore

IECON 2023 Tutorial Proposal Form

Title of the Proposal: Cyber Physical System Security and Resilience in Electric Vehicle Charging Systems

- Presenter(s):
Prof Milos Manic (corresponding)
Affiliation: Virginia Commonwealth University, Richmond, USA
Address: 601 West Main Street, Box 843068, Richmond, VA 23284-3068
Email: mmanic@vcu.edu

Timothy Pennington
Senior Research Engineer in the Energy Storage & Advanced Transportation
Affiliation: Idaho National Laboratory, Idaho, USA
Address: 1955 N. Fremont Ave., Idaho Falls, ID 83415 USA
Email: Timothy.Pennington@inl.gov

Benny J. Varghese
Research Engineer in the Energy Storage & Advanced Transportation
Affiliation: Idaho National Laboratory, Idaho, USA
Address: 1955 N. Fremont Ave., Idaho Falls, ID 83415 USA
Email: Benny.Varghese@inl.gov

Victor Cobilean
Affiliation: Virginia Commonwealth University, Richmond, USA
Address: 601 West Main Street, Box 843068, Richmond, VA 23284-3068
Email: cobileanv@vcu.edu

Harindra S. Mavikumbure
Affiliation: Virginia Commonwealth University, Richmond, USA
Address: 601 West Main Street, Box 843068, Richmond, VA 23284-3068
Email: mavikumbureh@vcu.edu

- Brief description:
Electric Vehicles (EVs) are becoming a primary component in Intelligent Transportation Systems (ITSs) as it decreases fossil fuel consumption and greenhouse gas emissions, reducing negative environmental impact. In recent years, there has been a rapid growth in EV infrastructure, expanding to various areas, including EV manufacturing, charging stations, battery advancements, electric vehicle supply equipment, and other roadside infrastructures.
In the following ten years, it's anticipated that there will be 120 million electric vehicles on the road. There are currently 290,000 electric vehicles on the road in the United States alone, a 69% increase from the previous year. Similar to gas stations, the charging equipment, often referred to as Electric Vehicle Supply Equipment (EVSE) or charging stations, offers safe and secure charging to electric vehicles.

Cyber-physical systems (CPS) are designed systems that are constructed through the secure and seamless integration of physical components, computation (sensing, computing, and networking) and communication. The foundations of this CPS integration are used by smart systems technologies such as smart charging infrastructures, smart transportation, smart grid. Existing EVSEs have several computing and communication components that are used to both manage and control the operation of power equipment. Emerging smart grid technologies additionally aim to facilitate a two-way power exchange between Plug-in Electric Vehicles (PEV) and the grid via EVSE, particularly fast chargers. Moreover, both personal and financial information are exchanged during smart charging as part of the authentication process. As the complexity and the interconnectivities of the EVSE increases, it has become vulnerable to cyber and physical attacks. The potential impact of attacks on these systems stretches from localized, relatively minor effects to long-term national disruptions. Therefore, cyber-physical security of electric vehicle (EV) charging infrastructure is critical to protect EV users, the EV charging network, and the grid.

Anomaly detection refers to the problem of finding patterns in data that do not conform to expected behavior. Anomalies are a strong indicator of a decrease in system performance which can lead to instabilities and failure. Often, the causes of anomalies are unknown effects within complex systems. Hence, the capability of understanding and detecting these underlying effects with the aid of data is the key to ensuring the desired outcome and resilience of complex CI such as electric vehicle charging systems.

Trustworthy AI is a widely discussed topic when applying NNs for mission-critical infrastructures. Despite the performance benefits of NNs, people hesitate to trust these systems. The main reason for this is the difficulty of understanding the decision-making process of the AI models, making these systems black-box models. It is crucial to address these trust-related issues to build trust between humans and these AI systems. One main component of Trustworthy AI is the Explainability or Interpretability of AI systems (XAI). XAI aims to provide an understanding of black-box models, enabling users to question and challenge the outcomes of AI systems.

Requirements: Participants will access Google Collaboratory resources using their gmail accounts. A laptop with an Internet browser and a stable Internet connection is mandatory.

- Duration: 3.5 hours

No	Topics
1	Importance of security of EV charging systems
2	Vulnerabilities in distributed EV charging systems ● Cyber (CAN protocol explanation) ● Physical
3	Anomaly/Intrusion detection ● What is anomaly detection ● Anomaly detection in EV charging systems
4	ML algorithms for Anomaly detection

5	Trustworthy AI for AD in EV charging ● Adversarial AI ● Explainability
6	Hands on session on Anomaly detection ● Benchmark dataset related to electric vehicles ● Using ML Algorithms ○ Autoencoder ○ OCSVM

- Motivation and Focus:
It is anticipated this tutorial will be beneficial to academics, research students, and industry practitioners alike in developing and advancing their skills and knowledge in cyber and physical security of electric vehicle charging systems. This tutorial is supported by the Technical Committee on Technology Ethics and Society of the IEEE Industrial Electronics Society.

-Brief CV:

Milos Manic (SM'06-M'04-StM'96) is a Professor with the Computer Science Department and Director of VCU Cybersecurity Center at Virginia Commonwealth University, He completed over 40 research grants in AI/ML in cyber and energy and intelligent controls. He authored over 200 refereed articles, holds several U.S. patents and has won 2018 R\&D 100 Award for Autonomic Intelligent Cyber Sensor (AICS).

He is a Fellow of IEEE, President Elect of IEEE IES, Fellow of Commonwealth Cyber Initiative, Inductee of National Academy of Inventors, recipient of IEEE IES 2019 Anthony J.Hornfeck Service Award, 2012 J. David Irwin Early Career Award, 2017 IEM Best Paper Award, an associate editor of Transactions on Industrial Informatics, Open Journal of Industrial Electronics Society, IES Officer and Senior AdCom member. He served as AE of Trans. on Industrial Electronics, was a founding chair of IEEE IES Technical Committee on Resilience and Security in Industry, and a general chair of IEEE IECON 2018, IEEE HSI 2019.

Timothy Pennington is a Senior Research Engineer in the Energy Storage & Advanced Transportation department of Idaho National Lab. Tim serves as the Principle Investigator for Department of Energy – Vehicle Technology Office funded projects and leads a team developing research tools to investigate Electric Vehicles' (EV) interactions with the electric grid and charging infrastructure. He also conducts research on charging hardware to enable future EV charging capabilities including extreme fast charging, high power wireless charging, and heavy duty vehicle charging. Tim holds a B.S. from the Massachusetts Institute of Technology and a MSc from the University of Southampton (UK), and previously led Department of Defense research and technology demonstration projects.

- Relevant publications:

[1] Wickramasinghe CS, Marino DL, Mavikumbure HS, Cobilean V, Pennington TD, Varghese BJ, Rieger C, Manic M. RX-ADS: Interpretable Anomaly Detection using Adversarial ML for Electric Vehicle CAN data. arXiv preprint arXiv:2209.02052. 2022 Sep 5.

[2] Harindra S Mavikumbure, Chathurika S Wickramasinghe, Daniel L Marino, Victor Cobilean, and Milos Manic. Anomaly detection in critical-infrastructures using autoencoders: A survey. In IECON 2022-48th Annual Conference of the IEEE Industrial Electronics Society. IEEE, 2022.

[3] D. L. Marino, C. S. Wickramasinghe, B. Tsouvalas, C. Rieger and M. Manic, "Data-Driven Correlation of Cyber and Physical Anomalies for Holistic System Health Monitoring," in *IEEE Access*, vol. 9, pp. 163138-163150, 2021, doi: 10.1109/ACCESS.2021.3131274.

[4] C. S. Wickramasinghe, K. Amarasinghe, D. L. Marino, C. Rieger and M. Manic, "Explainable Unsupervised Machine Learning for Cyber-Physical Systems," in *IEEE Access*, vol. 9, pp. 131824-131843, 2021, doi: 10.1109/ACCESS.2021.3112397.

[5] C. S. Wickramasinghe, D. L. Marino, J. Grandio and M. Manic, "Trustworthy AI Development Guidelines for Human System Interaction," *2020 13th International Conference on Human System Interaction (HSI)*, 2020, pp. 130-136, doi: 10.1109/HSI49210.2020.9142644.

[6] C. S. Wickramasinghe, D. L. Marino, K. Amarasinghe and M. Manic, "Generalization of Deep Learning for Cyber-Physical System Security: A Survey," *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 745-751, doi: 10.1109/IECON.2018.8591773.

[7] D. L. Marino, C. S. Wickramasinghe and M. Manic, "An Adversarial Approach for Explainable AI in Intrusion Detection Systems," *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 3237-3243, doi: 10.1109/IECON.2018.8591457.

[8] T. Vollmer, M. Manic and O. Linda, "Autonomic Intelligent Cyber-Sensor to Support Industrial Control Network Awareness," in *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1647-1658, May 2014, doi: 10.1109/TII.2013.2270373.