Professor Osama Mohammed is a distinguished Professor of Electrical and Computer Engineering and the Director of the School of Electrical, Computer, and Enterprise Engineering. He is also the Director of the Energy Systems Research Laboratory with its Smart Grid Testbed Facility. He was Associate Dean for Research and Graduate Studies, 2016-2023.

Professor Mohammed is a Fellow of the National Academy of Inventors, a Fellow of IEEE, and a Fellow of the Applied Computational Electromagnetic Society. He received the Prestigious Cyril Veinott Electromechanical Energy Conversion Award from the IEEE Power and Energy Society 2010. Professor Mohammed has published nearly 900 journals and refereed conference articles. He holds more than 20 patents in his research areas. He has also published a book and several book chapters.

His research interests include renewable energy utilization, power systems, smart grids, and wide-area network applications. He is also interested in Electric machines and Drives, Fault-tolerant designs, diagnostics, and intelligent systems applications. He is interested in transportation electrification, shipboard power systems, and Lunar Habitat energy infrastructure. He is also interested in power electronics for integrated motor drives and DC distribution systems for renewable energy. He also has an interest in computational electromagnetics. Dr. Mohammed has successfully obtained many research contracts and grants from industries and Federal government agencies and has current active research programs in several areas.

He has been general chair and Technical Program Chair of more than 12 major IEEE international conferences, including IEEE/ISAP, IEEE/IEMDC, IEEE/CEFC, and COMPUMAG. He has been an editor of IEEE Transactions on Energy Conversion, IEEE Transactions on Smart Grid, IEEE Transactions on Magnetics, and IEEE Transactions on Industry Applications.

Distinguished Lecture 1:

New Challenges in Transportation Electrification, Powertrain Drives & New Power Electronics Architectures.

Abstract: Electrification of the transportation industry and large-scale integration of renewable energy sources into the power grid represent some of the most disruptive transformations of our time. This engineering field brings ideas from Computational electromagnetics, power and energy, electromechanics, IoT, and artificial intelligence. This enables the creation of efficient, reliable, safe, and environmentally friendly means of implementing these ideas in new applications.

In this talk, we will share our views on the future of these applications through a detailed discussion of the roles of computational modeling, Power electronics architectures, devices, the embedding of components, challenges of utilizing magnetics, and thermal management under higher operational frequencies, currents, and voltages. We will discuss packaging issues and describe some applications requiring increased power densities. This part of the presentation will identify the research areas that promise high impact and potential for achieving improved performance.

Distinguished Lecture 2

Operational Security and Control Challenges in Smart Energy Systems

Abstract: The development of innovative cybersecurity technologies, tools, and methodologies that advance the energy system's ability to survive cyber-attacks and incidents while sustaining critical functions is needed for the secure operation of utilities, industrial systems, smart homes, and transportation systems. It is essential to verify and validate the ability of the developed solutions and methodologies so that they can be effectively used in practice. Developing solutions to mitigate cyber vulnerabilities throughout the energy delivery system is essential to protect hardware assets. It will also make systems less susceptible to cyber threats and provide reliable delivery of electricity if a cyber incident occurs.

This talk will describe how the developed solution can protect the power grid, industrial systems, smart homes, transportation systems, and infrastructures from cyber-attacks and build cybersecurity protection into emerging power grid components and customer-based services. This includes microgrid and demand-side management components as well as protecting the network (substations and productivity lines) and data infrastructure to increase the resilience of the energy delivery systems against cyber-attacks.

Developing secure operation and cybersecurity capabilities in energy systems should span over multiple strategies in the near term, midterm, and long term. Continuous security state monitoring across cyber-physical domains is the goal in the near term. The development of continually defending interoperable components that continue operating in degraded conditions is required in the midterm. Developing methodologies to mitigate cyber incidents to return to normal operations quickly is necessary for all system components in the long term. We will discuss R&D efforts in these research areas centered on developing operational frameworks related to communication and interoperability, control, and protection in various platforms, including smart homes and electric vehicles.

One of the emerging research areas is the scalable cloud-based Multi-Agent System for controlling large-scale penetration of Electric Vehicles (EVs) and their infrastructure into the power grid. This is a system that can survive cyber-attacks while sustaining critical functions. This framework's network will be assessed by applying contingencies and identifying the resulting real-time signatures for detection. As a result, protective measures can be taken to address the dynamic threats in the foreseen grid-integrated EV parks where the developed system will have an automated response to a cyber-attack.

In distributed energy management systems, the protection system must be adaptive. It is assisted by communication networks to react to dynamic changes in the microgrid configurations. This presentation will also describe a newly developed protection scheme with extensive communication for power networks to monitor the microgrid during these dynamic changes. The robustness and availability of the communication infrastructure are required for the success of protection measures.

Distinguished Lecture 3

Digital Twins for Enhanced Power System Operation, Cyber-Physical Security and Resiliency

Abstract: The Power system infrastructure represents the backbone of regional and national economic activities. Resilient and secure grid operation is increasingly becoming important because a disruption or loss of function could negatively impact the whole infrastructure.

The multiterminal distributed microgrids infrastructure is the future of new energy systems implementing increased renewables and energy storage levels. For real-time control and security, there will be heavy reliance on digital communication and control with deep integration of information and physics. The latter makes the system vulnerable to cyberattacks. In communication networks, the packets of information are sent around the network and assembled at the destination. Delays and errors in time, either due to communication or cyber-attacks, can lead to errors in power and energy control and management, which may result in outages and increased levels of instability.

Innovative techniques that can offer appropriate real-time or faster-than-real-time decisions are needed to maintain resilient and reliable operations in addition to cyber-physical security. In this talk, we will discuss the implementation of the Digital Twins (DT) technology to deal with these complex and critical challenges. The DT is an integrated solution that can cover every asset and component. The digital twin model is continuously updated and synchronized from sources and provides near real-time status updates, working conditions, and operational challenges in the field. With advanced analytics such as machine learning and artificial intelligence, the DT provides simulation capabilities to predict, optimize, and estimate future states. This strategic solution can be a fully integrated situational-awareness platform for the system operator based on the digital twin shadow and the machine learning insights for physical faults and cyber threats events. The DT will introduce a virtual replica of the system for state estimation and prediction and the appropriate operation scenario after detecting such events to guarantee continued operation. We can then select the candidate optimal scenario of operation in real-time or even faster-than-real-time if high-performance computing is used, based on the what-if scenarios capability of the digital