Transportation electrification imposes special considerations and concerns for cybersecurity. These are in addition to widely discussed issues of connection security and vehicle-to-vehicle communication and control. The IEEE Transportation Electrification Community and the IEEE Standards Coordinating Committee on Transportation (SCC 42), with technical cooperation of the NSF Center for Power Optimization of Electro-Thermal Systems, the Information Trust Institute at the University of Illinois, Howard University, and the IEEE-USA Committee on Transportation and Aerospace Policy, will sponsor this special one-day workshop followed by a full-day meeting of IEEE SCC 42. The event will address cybersecurity issues directly associated with more-electric transportation, including propulsion system cyber vulnerabilities, cyber issues linked to human error and software bugs, vulnerabilities of active safety systems, the challenges of "always on" large battery packs, vehicle-to-grid aspects, and others. The overall goal is to characterize the cyber-security requirements for enabling transportation electrification, not including V2V and personal communications.

The workshop will include invited presentations and focused breakout discussion directed to the following objectives:

- **Identify and delineate key areas of concern in cybersecurity issues directed at transportation electrification.**
- **Identify relevant gap areas in which fundamental engineering research and development are needed for progress.**
- **Set up objectives to nucleate working groups on recommended practices and standards.**
- **Evaluate and identify specific topics in which there is urgent need for solutions.**
- **Identify existing practices and advances that can be applied in the near term to cybersecurity issues in electrified transportation.**

The outcomes of the discussion will provide immediate guidance and action items for IEEE SCC 42 and will lead to a published report providing guidance for near-term industry and government efforts directed at cybersecurity in transportation electrification.

Speakers and participants will address questions that include:

- How can extreme intentional operating modes be distinguished consistently from fault conditions or tampering?
- What are best design and validation practices to evaluate operational cybersecurity challenges in highly energy-dense systems?
- Are there strategies that lead to inherent safe modes in the event of security issues or vehicle damage?
- How do active safety systems in more-electric transportation, such as collision avoidance and positive train control, impact cybersecurity considerations?
- What are best practices for securing software and hardware update and repair processes?
- What policy and standards-related activities would be of benefit in cybersecurity issues specific to transportation electrification, including interaction of devices with power grids?

Participants are invited to this workshop, and to the subsequent SCC 42 meeting, that are designed to raise awareness of cyber-related security challenges now emerging with the growth of electric and hybrid vehicles and the trend toward more-electric energy in all forms of transportation. The workshop seeks to gather a group of experts in power electronics, systems engineering, machines and drives, and cybersecurity of devices and infrastructure.

Much of the past work on cybersecurity in transportation has emphasized vehicle-to-vehicle and vehicle-to-infrastructure communication links. Although these challenges are widely discussed and unresolved, the challenges to be addressed by this workshop are different. Issues linked to rapid energy exchange and to electric propulsion are introduced even in vehicles with minimal communication interfaces. The workshop intends to develop metrics related to key issues and develop a working plan toward policy and standards activities that could help overcome or avoid cyber-based vulnerabilities. The agenda will include invited talks by leading experts on cybersecurity in physical systems, open discussion sessions, and talks by industry participants summarizing best practices. This will be an interactive workshop.

Invited speakers include:

Prof. David Nicol, Director, Information Trust Institute, University of Illinois at Urbana-Champaign
Prof. Klara Narstadt, Director, Coordinated Science Laboratory, University of Illinois at Urbana-Champaign,
Prof. Charles Kim, Howard University
OTHERS TBA

Schedule: (Wed. Feb 24, 2016) *Workshop*

7:30am	Continental breakfast
8:00am	Welcome and introductions
8:15am	Invited talk
8:45am	Q&A
9:00am	Invited talk
9:30am	Q&A
9:45am	Coffee break
10:00am	Invited talk
10:30am	Begin morning breakout discussions
11:45am	Discussion reporting
12:00pm	Lunch and lunch presentation
1:15pm	Invited talk
1:45pm	Q&A
2:00pm	Invited talk
2:30pm	Q&A
2:45pm	Coffee break
3:00pm	Begin afternoon breakout discussion
4:15pm	Discussion reporting
4:30pm	Group discussion: action items and next steps
5:00pm	Adjourn

Schedule: (Thurs. Feb 25, 2016) *SCC 42 meeting* (workshop participants are welcome)

7:30am	Continental breakfast
8:00am	SCC 42 chair welcome and introductions
8:15am	Working groups WG2040, 2040.1, and 2040.2 joint meeting: Standards for connected, automated and intelligent vehicles
9:45am	Coffee break
10:00am	Continue working groups
11:15am	SCC42 task force TF1 meeting -- Cybersecurity in Transportation
12:15pm	Lunch
1:15pm	SCC42 task force TF2 meeting -- Road Electrification
2:15pm	SCC42 advisory group AG1 meeting -- Global Policy
3:15pm	Coffee break
3:30pm	SCC42 committee meeting
4:30pm	Adjourn

Registration

Advance registration is encouraged, one-day registration $150 if paid by February 15, 2016 (covers breakfast, lunch, and breaks, meeting room rental, and workshop materials), or both days for $250.
Student registration by February 15, 2016 is $50.
After February or onsite, registration is available at $300.
Register at http://tecworkshop.crosby.work/

Suggested hotel

Holiday Inn Central, 1501 Rhode Island Ave NW, Washington, DC 20005
http://www.inndc.com/location.php

Motivating issues of cybersecurity in electrified transportation

Transportation electrification imposes special considerations and concerns for cybersecurity. These are in addition to widely discussed issues of connection security and vehicle-to-vehicle communication and control in the broader context of transportation cybersecurity. Examples of the issues include (but are not limited to):

- Electrified vehicles will have "wire pedals" and are more likely to have other "x by wire" systems than more conventional vehicles. These have different vulnerabilities than mechanical units. There is a need to identify vulnerabilities such as acceleration and deceleration controls.
- Inverters and chargers in electrified vehicles have internal control settings and firmware. Some settings are relatively sensitive and major problems can be created with relatively stealthy changes. There is a need to define firmware and internal control setting sensitivity characteristics for inverters and chargers in electrified vehicles
- Energy levels are high and systems are extensive and complex. Electrification introduces propulsion-based entry points in all vehicle types, including aircraft, ships, construction vehicles, and trucks. There is a need to define implementation of traction control and stability and define entry point vulnerabilities for the propulsion systems under investigation.
- In some intentional operating modes (e.g. rapid acceleration), the operating conditions are difficult to distinguish from fault conditions, complicating safety and protection.
- In general, full torque capability is available across the spectrum of operation, from stopped and full forward speed to full reverse speed. Often software limits must have precedence over mechanical limits to maintain safe conditions.
- Batteries are always energized, vs. internal combustion vehicles being de-energized when parked. Battery management and charging circuits are active even in parked vehicles. There is a need to define battery management and its impacts on safety and security, issues of parked and on-road charging, safety issues associated with battery status, charger billing, and post-incident battery management.
- Vehicles with an active grid interface introduce vulnerabilities linked to known challenges in utility systems, and energy flows from the grid can be manipulated in harmful ways.
- Many cybersecurity issues in these contexts are linked to human error, software bugs, physical loss of communication and network links, or single-point failure modes in cyber-based hardware rather than malicious attacks. There is massive code complexity, unfamiliar operating modes, sophisticated grid interfaces, and associated opportunities for human error. There are established practices in aerospace but not necessarily across the broad transportation application space. There is a need to define mitigation strategies to overcome human error, software bugs, and internal communication and network link loss.
- Positive train control and other active safety enforcement approaches introduce new types of attack points and vulnerabilities. There is a need to define these vulnerabilities and human fail-safe modes.

This workshop will not give much emphasis to secure V2V and V2I communications, because these have been widely discussed and are being addressed within other IEEE groups. Not to imply they are resolved! But the special issues of internal cybersecurity, grid interaction, and safety management have had limited prior discussion.