Cybersecurity Overview of Wireless Power Transfer (WPT) for Electrified Transportation

Barney Carlson

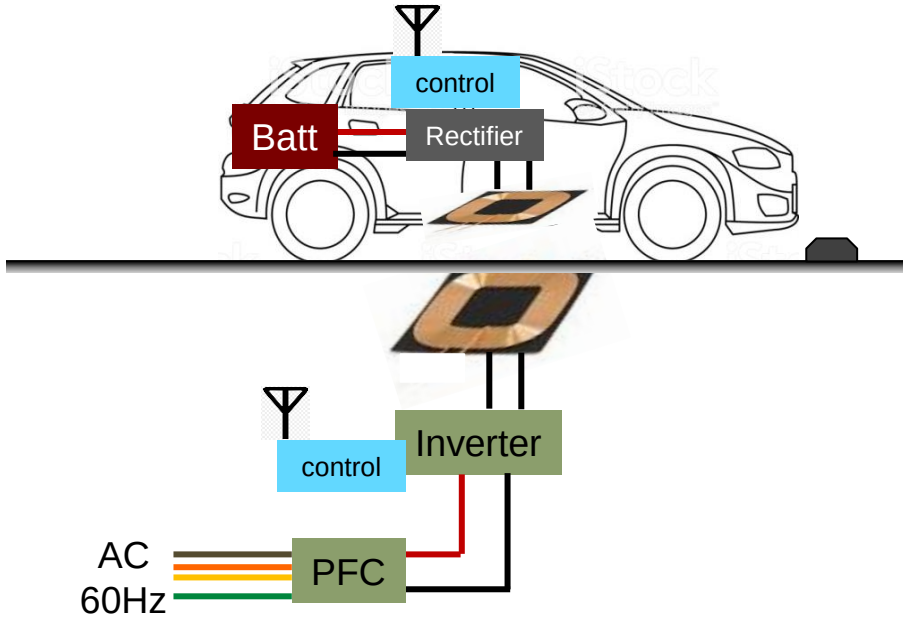
February 11, 2020

INL/CON-20-57233

Static WPT

Potential Vulnerabilities (additional to conductive DC charging)

- Wireless communication used for: authentication, charge event initiation, power transfer control, etc.
  - No physical connection required by malicious cyber actor
- WPT system interaction with autonomous parking systems (vehicle movement for coil alignment)
  - Potential for unintended vehicle movement
- EM-field safety systems (live object or foreign object detection)
  - Potential safety hazard



Dynamic WPT

- Vehicle-side WPT system: expected interoperable with static and dynamic WPT ground-side systems
  - Topology, tuning frequency, gap and power class interoperability, etc.
- Control system complexities often create additional potential vulnerabilities
  - Authentication, power control and tuning, lane alignment, etc.
- Control system speed and latency
  - Encryption and other security measures latency may require different approach for control system