



Solving The Electric Vehicle
CYBERSECURITY DILEMMA

ABSTRACT

This paper is intended to give a technical overview of GuardKnox's EV ECU platform for electric vehicles and to explain why it is uniquely suited for providing cybersecurity for connected and autonomous electric vehicles (EVs).

The paper opens with the rapid growth of the EV market, the changing EV charging landscape, and the additional cyber risks faced by EVs that are connected to public charging stations and therefore the overall electric grid.

GuardKnox's patented cybersecurity solution is then explained, including its patented three-layer Communication Lockdown™ methodology and its Service-Oriented Architecture. The paper then examines the benefits of the GuardKnox EV solution and concludes with a look at the potential future applications of the solution in the wider EV charging ecosystem.

THE FUTURE OF TRANSPORTATION IS CLOSER THAN YOU THINK

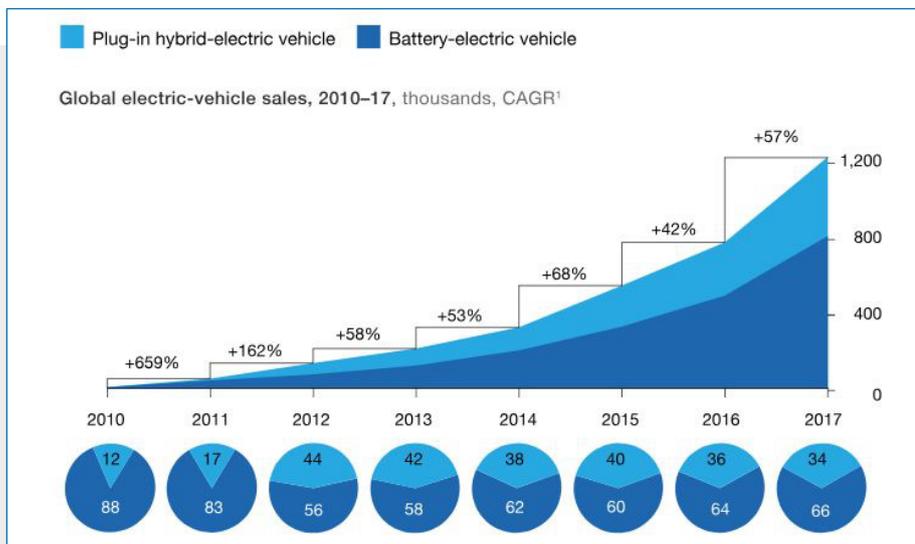
It's safe to say that the electric vehicle revolution is truly underway. In 2017 and 2018, the EV and energy manufacturer, Tesla, was the [highest-ranked American car brand](#) and eighth among all car brands in the USA. Selling more than 160,000 cars in 2018, the Tesla's Model 3 was [the USA's best-selling luxury vehicle](#) of any type (gasoline cars, EVs and even SUVs).

Tesla is just one indicator of the fundamental changes taking place. In 2017, global annual sales of battery-electric vehicles (BEVs) exceeded 1 million units, outselling plug-in hybrid electric vehicles (PHEVs) by a ratio of 2 to 1. At the end of 2017, there were 3 million battery-electric vehicles on the road, representing about [0.23% of the global vehicle population](#).

The sales of electric vehicles (EVs) are expected to quadruple to [4.5 million units](#) per year by 2020, influenced by a number of factors that are accelerating EV adoption:

- [Lower running costs](#) than combustion-engine vehicles
- [Increased battery range](#) that enables a full-day of electricity for most drivers
- The deployment of thousands of charging stations
- Efforts to reduce worldwide carbon emissions by 45% by 2030

By 2040, the sales of electric vehicles are expected to [comprise 54% of new car sales](#) worldwide.



Source: [McKinsey 2018](#)

Electric vehicles are just the first step on the way to autonomous vehicles, a seismic change equivalent to the migration from horse and buggies to the “horseless carriages” we now call “cars”. OEMs are investing huge sums to transform their businesses to produce electric and autonomous cars. Indeed Volkswagen is allocating \$50 billion over the next five years on this transition and expects [the era of the combustion car to fade away](#) after it rolls out its next-generation gasoline and diesel cars in 2026.

In regards to [the timeline](#) for deploying autonomous vehicles, [Ford and other OEMs](#) have conceded that they may have underestimated their time to market, but Volkswagen has recently started testing [Level-4 autonomous vehicles](#) in Hamburg on three kilometers (1.9 miles) of urban roads fitted with smart signals and other traffic management systems. Adding the equivalent of 15 laptops to each e-Golf test vehicle, up to [5 gigabytes of data](#) are processed each minute from the transportation digital ecosystem, the car’s 11 laser scanners, seven radars and 14 cameras.

While it may be hard for us to imagine that we could be the [last generation to own cars](#), our grandchildren may find our car ownership an anachronism - like owning a horse and buggy.

THE EV CHARGING LANDSCAPE

The ubiquitous deployment of EV charging stations and other electric vehicle supporting equipment (EVSEs) is critical for mainstream adoption of electric vehicles and overcoming “range anxiety”. According to a study by the US National Renewable Energy Laboratory, EVs will need to travel [650 km \(400 mi\) per charge](#) for a majority (55%) of potential buyers to consider purchasing them.

Today there are [three basic types](#) of EV charging:

- **Level 1** chargers are essentially adapters or extension cords that are used to plug an EV into a standard US 120V home outlet. Delivering 120-volt charging and 1.4 kW/h of power, Level 1 chargers take 17-25 hours to recharge a car for 160 km (100 mi) of driving. This type of charger comes standard with all BEVs.
- **Level 2** chargers are special adapters for home use that deliver 208-240 volts and 6.2-7.6 kW/h of power. Requiring a 240V outlet, these chargers take 4-5 hours to deliver 160 km (100 mi) worth of charge. This charger is often purchased with the electric vehicle, but it is usually an aftermarket item from Bosch or other companies that is sold separately.
- **Level 3** chargers are EV charging stations for public use and provide 20-50 kW/h and can recharge a vehicle in as little as 20 minutes, but not all vehicles can use Level 3 chargers.

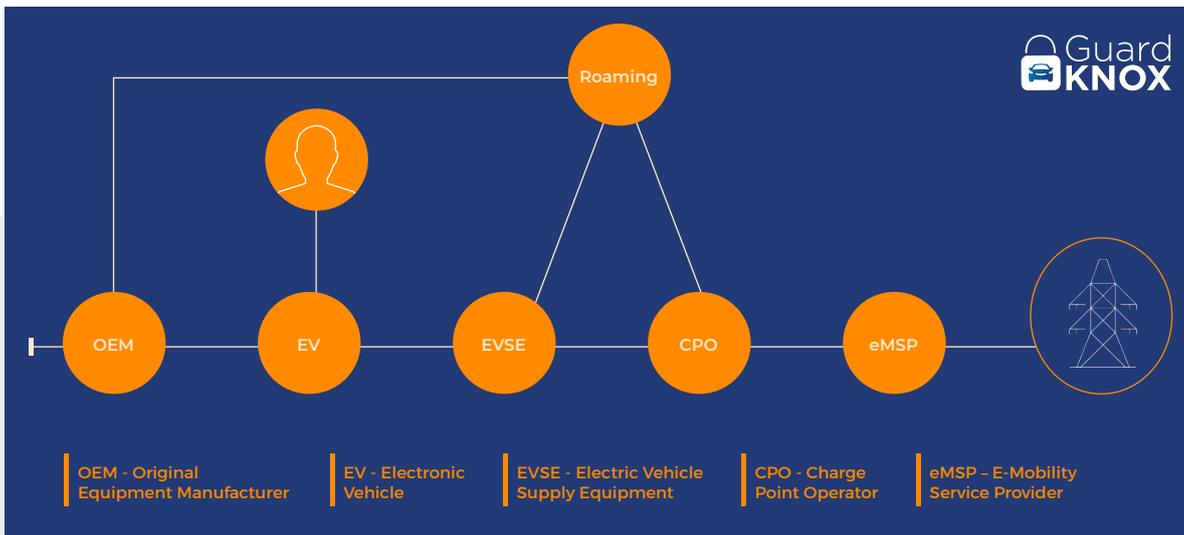
As electric vehicles become mainstream, they will be increasingly purchased by middle- and lower-class households that live in more dense urban environments, including multi-dwelling units (MDUs). Lacking the space required for Level 1, home-based EV charging stations, these EV owners will rely on Level 2 and Level 3 commercial public charging stations on streets and in parking garages.

By [2029, 10 million public chargers and 50 million private chargers](#) are expected to be installed, supported by large investments from the private sector and generous government incentives. In markets such as China, where individual homes are less common or even rare, public charging stations already serve as the primary form of EV charging.

Key Stakeholders in the EV Charging Process

There are a variety of stakeholders in the EV charging ecosystem. In addition to the energy providers to the grid and the OEMs, the ecosystem includes a variety of businesses and service providers:

- **Emobility Service Providers (EMSPs or EMPs)** offer EV charging services to EV drivers and enable access to a variety of charging points around a geographic area. EMSPs help EV drivers locate charging stations and pay for charging. EMSPs may direct drivers to their own charging stations or to stations owned by third-parties.
- **Charge Point Operators (CPOs)** or Charge Spot Operators (CSOs) operate and maintain a collection of charging points and connect smart charging devices to EMSPs. Charge Point Operators may own the infrastructure, merely provide connection to EMSPs, or may own the infrastructure and enable access to other charging station owners.
- **Charge Spot Infrastructure Operators (CSIO)** operate and maintain the infrastructure of charging stations, including the updating of firmware.





While some companies focus on specific areas of the ecosystem, such as owning the charging stations, others may perform multiple services such as EMSPs that provide services for locating a charging station, manage the payment, and own the EV charging stations.

ChargePoint operates more than 60,000 total charging spots and more than 1,000 Express DC fast spots (Level 3 charging stations). In addition to operating the EVSEs, the company designs, builds and supports all of its technology, from charging station hardware to energy management software to the mobile app. ChargePoint sells and leases a large variety of solutions for home users, high-density residences, parking lot operators, vehicle fleets, workplaces, and more. They also offer programs that help monetize the charging stations as well as offer charging-as-a-service.

Emerging Protocols and Standards

Typical with an emerging technology or market, there is not a single, unified standard that supports interoperability between vendors or across all countries. Charging stations may use one of a [variety of connectors](#) and EV users may need to subscribe to multiple EMSPs and phone apps to enable easy access to EV charging stations.

In many European countries, the EVSE communication and control protocol standards may not be identical with neighboring countries (with some exceptions) which makes EV roaming between different countries especially challenging.

Fortunately several EV ecosystem players are working together to create standard protocols for interoperability between various vendors that supply the infrastructure. ElaadNL, the smart charging infrastructure lab founded by Dutch grid operators has developed the IOTA Tangle Distributed Ledger Technology (DLT), an open-source protocol facilitating novel Machine-to-Machine (M2M) interactions, including secure data transfer and fee-less real-time micropayments. The solution has eliminated the need for a back office or communication protocol for operating the charging station and all transactions are exchanged directly without the use of a charge card or subscription.

Connector types	
	<p>Connector: Port J1772</p> <p>Level: 2</p> <p>Compatibility: 100% of electric cars</p> <p>Tesla: With adapter</p>
	<p>Connector: CHAdeMO</p> <p>Level: 3</p> <p>Compatibility: Check specifications of your EV</p> <p>Tesla: With adapter</p>
	<p>Connector: SAE Combo CCS</p> <p>Level: 3</p> <p>Compatibility: Check specifications of your EV</p> <p>Tesla: No</p>
	<p>Connector: Tesla HPWC</p> <p>Level: 2</p> <p>Compatibility: Only Tesla</p> <p>Tesla: Yes</p>
	<p>Connector: Tesla supercharger</p> <p>Level: 3</p> <p>Compatibility: Only Tesla</p> <p>Tesla: Yes</p>

Source: [ChargeHub](https://www.chargehub.org/)

In addition, Hubjet created an “eRoaming platform” that uses the Open InterCharge Protocol to enable EV owners to connect to a network of more than 90,000 charging points in 20 countries on three continents. The platform is designed to connect a variety of market players including Charge Point Operators (CPOs), Emobility Service Providers (EMSPs), energy suppliers, fleet operators, car-sharing companies and OEMs.

ISO 15118 is an international standard that defines vehicle-to-grid (V2G) communication for bi-directional charging and discharging of electric vehicles. It adds an element of control over the recharging process in order to match the grid’s capacity with the power demands of electric vehicles. The Plug & Charge feature of ISO 15118 enables EVs to be automatically identified by the EV charging station so the EV battery can be recharged without an RFID or the use of a mobile phone app. The authorization process is automatically initiated when a drive plugs the charging cable into the EV and/or charging station.

THE THREATS AND VULNERABILITIES OF THE EV CHARGING PROCESS

The cyberrisks of connected cars started to enter the public consciousness in 2015 with the cyber-hijacking of a Jeep by white hat hackers. In 2018, a rash of keyless Tesla thefts received wide coverage in mainstream print and TV media as well as the Internet. Today there is significant appreciation that the computer-driven conveniences of modern cars have turned them into computers-on-wheels with all the cyberrisks computer networks and smart phones.

But few realize that the EV recharging process opens a highway for unprotected messages between the electric vehicle and the charging station, potentially giving viruses and hackers unfettered access to the car's computer networks. These risks will increase as the deployment and use of public Level 3 charging stations grows. DDoS attacks, ransomware, trojan viruses, malware audio/video files, phishing, OTA file updates and app vulnerabilities can be used for the theft of personal and financial data or the theft and hijacking of goods - such as electricity or electric vehicles.

Whether performed by criminals, disgruntled employees, state-sponsored organizations or terrorists, there are many potential soft targets in the EV ecosystem including but not limited to:

- EV charging system hardware or physical interfaces
- EV charging system software
- Apps for locating charging stations and paying for services
- Wireless communication links
- Physical communication links

Risky Hardware and Physical Interfaces

The deployment of tens of thousands of charge points - which will grow to millions in the coming years - makes it [nearly impossible to physically secure](#) the system hardware or physical interfaces. This issue is compounded by basic security errors such as exterior USB connections which are equally convenient for charging phones and hacking a charging station. In addition, studies have shown that best practice for security are not used: with some charge points the Administrative password is never changed from the original settings and leading SCADA systems continue to use [hard-coded passwords](#) for access control.

Unsecure & Outdated EVSE Protocols

Most of the protocols used by EVSEs were developed, tested and deployed over large periods of time and reflect the challenges and threats as they were understood at the time of their development. In addition, they have not - and cannot - keep pace with the rapid developments in the hacking industry, leaving a large attack surface to be exploited. Relying on older technology, they lack the capacity to be updated over-the-air like mobile phones, connected vehicles or laptops with the Windows 8 operating system that are connected to a network.

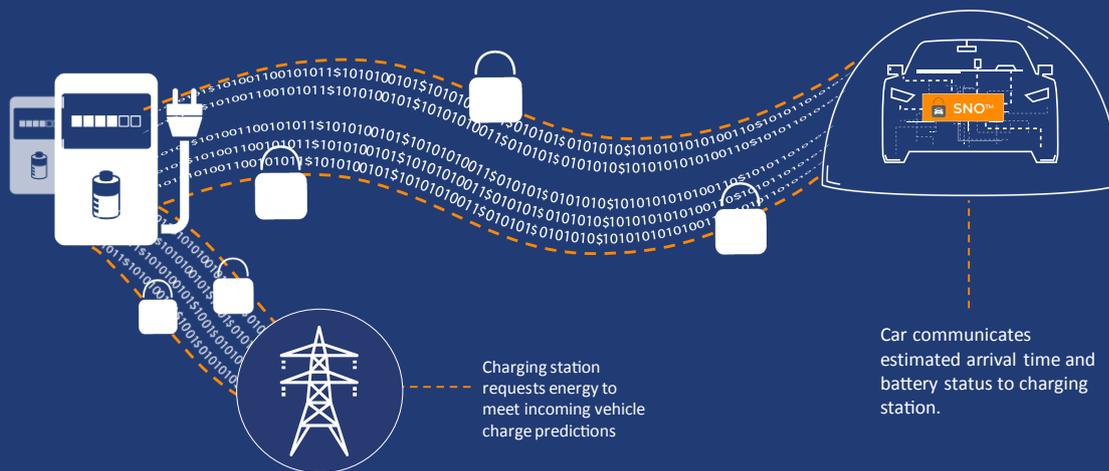


The EV charging process is guided by two standards for communication: [the Open Charge Point Protocol \(OCPP\)](#) that allows charging stations to communicate with backend systems and the [ISO 15118 standard](#) for bidirectional vehicle-to-grid (V2G) communications.

The V2G communications between the vehicle and EV charging networks, with its direct access to the vehicle network is a primary risk to electronic vehicles. In addition, it is composed of well-known protocol suites with equally well-known risks:

- The XML protocol is prone to denial-of-service (DoS) attacks, data theft and remote code execution (RCE)
- The TCP/IP protocol can be hacked through number spoofing, routing attacks, source address spoofing, and authentication attacks
- TLS ostensibly used to encrypt data has been proven to be easy to hack
- PLC (Power Line Communications) protocol can be physically intercepted and decrypted

A Typical Example of Securing the V2G



THE GUARDKNOX EV ECU PLATFORM FOR ELECTRIC VEHICLES

GuardKnox's [EV solution](#) is an EV [ECU](#) Platform that offers comprehensive cybersecurity protection against any type of known and unknown cyberattack, including EV charging threats. With a full software stack and hardware architecture, GuardKnox's patented technologies adhere to the most stringent security (ISO 15408) and safety (ISO 26262) standards.

The EV ECU is completely autonomous and eliminates the need for human intervention in the security mitigation process. It has high-performance data processing capabilities, does not require external connectivity, constant communication, cloud connectivity, or on-going updates.

Complying with GDPR (General Data Protection Regulation), the EV ECU provides holistic [automotive cybersecurity](#) that easily fits the automotive tiered value chain and can be used to offer cybersecurity for:

- Physical interfaces connecting vehicles to charging stations
- Wireless interfaces connecting vehicles to charging stations

The solution architecture is split into an external partition and an internal

partition. The external partition handles all external communication with the vehicle. Using GuardKnox's patented three-layer Communication Lockdown™ methodology, GuardKnox examines all messages on the routing layer, the content layer and the contextual layer.

Only allowed "legal" communication such as PLC, CAN or wireless communication is permitted to cross to the internal partition, while all unauthorized or improper communication is dropped, including communication from the EV charging network. GuardKnox, which is currently developing towards ISO 15118 compliance, can identify all "legal" V2G traffic between the charging station and the EV and mitigate the risks of DOS attacks, data exfiltration and remote code execution (RCE).

In addition, all protocol-related data is stripped out to prevent protocol-level attacks as GuardKnox mediates the data-stream between the external environment and the internal partition. Once data has crossed to the internal partition, GuardKnox examines the content and context of all communications for safety before passing the data to the internal vehicle network.

THE BENEFITS OF THE GUARDKNOX APPROACH

The Communication Lockdown™ Methodology for Holistic Cybersecurity

All GuardKnox products and solutions are distinguished by a [patented Communication Lockdown™ approach](#) for providing holistic vehicle cybersecurity. Using the vehicle's communications matrix and the OEM's specifications of the vehicle, GuardKnox builds a machine-state model that is used to inspect all communication activity on three layers:

- **Routing Layer** - verifying that messages originate on the appropriate network
- **Content Layer** - verifying that message content is permissible down to the bit level
- **Contextual Layer** - verifying that each message is legitimate within the context of the vehicle's specific functional state (e.g., opening the sunroof at 100 km/h (54 mi/h))

The three layers of inspection ensure that if the external vehicle network is compromised by a message from the vehicle's external ecosystem, the internal vehicle network remains fully protected from the propagation of malicious activity.

The [Communication Lockdown™ methodology](#) is completely agnostic to all types of known, unknown and future cyberattacks since the proper behavior of all messages has been fully defined by the GuardKnox communications schema and certified by the OEM. This also enables the EV ECU to become fully autonomous after installation and to operate deterministically without the need for frequent software or firmware updates - unlike Intrusion Detection/Intrusion Prevention Systems (IDS/IPS) or firewalls.

If the OEM changes the vehicle's Technical Specifications or its configuration, a new Communication Lockdown™ schema can be generated, certified and installed via secure OTA update or via the OBD-II port. In the context of a Service-Oriented Architecture design and the compartmentalization of specific functionality and services, changes to the Communication Lockdown schema would be limited in scope and would not have to affect hundreds of thousands of lines of code across multiple services or applications.

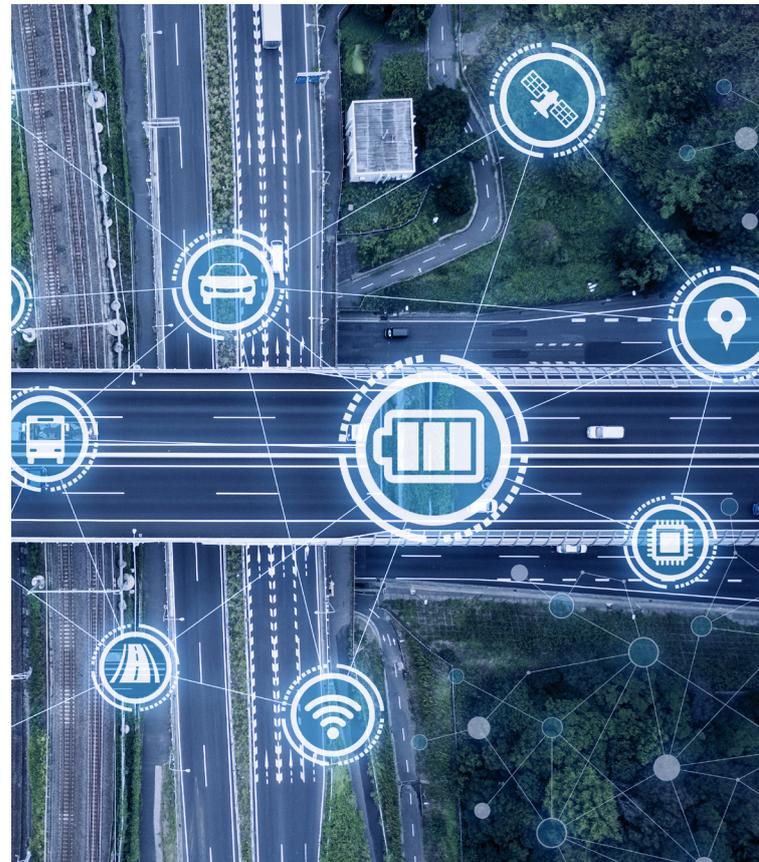
INTO THE FUTURE: CYBERSECURITY FOR THE EVSE ECOSYSTEM

The continued development and maturation of the EVSE ecosystem will bring new risks that will also require cybersecurity solutions. While one might think that supplying additional power for 30-50 million electric vehicles by 2030 poses a risk, the US Department of Energy's Pacific Northwest National Laboratory calculated that the US electric grid currently has [enough excess capacity](#) to support more than 150 million EVs.

Rather than posing a threat or challenge to the power grid, EVs could be the “killer app” of electrical utilities that will renew demand for electricity. Demand for electricity has [stagnated since 2007](#) from large customers generating their own power (often from renewables), more energy-efficient electronic devices, and ubiquitous [LED light bulbs](#) that use 85% less electricity than Edison's incandescent bulbs.

Electric vehicles and the EV charging ecosystem offer the power industry a real [opportunity for growth](#). EVs offer utilities the prospect not only to sell more electricity, but also to leverage smart meters, analytics, and a modernized infrastructure to:

- Develop rate plans that incentivize off-peak EV charging for households and fleets
- Offer separate home meters for EV charging
- Sell “green electricity” generated from renewable sources for charging EVs
- Incentivize EV charging stations to help balance the grid.



Balancing the Grid and Energy Storage

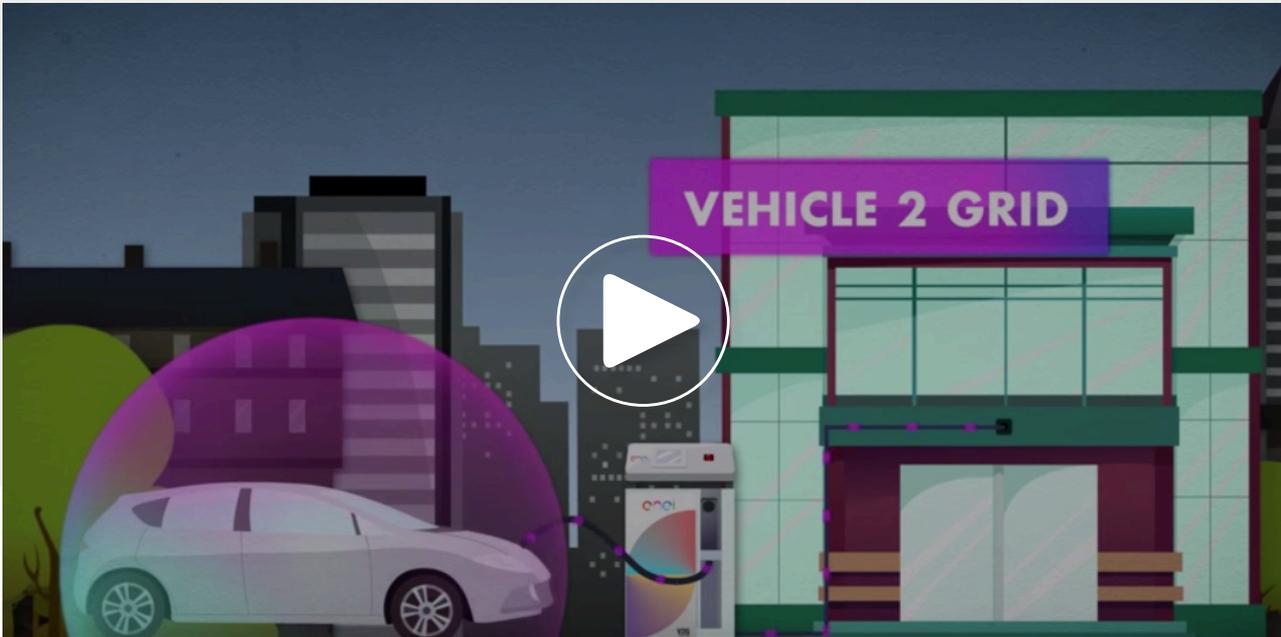
Balancing the grid is a critical function for ensuring that utilities can create and supply the right amount of electricity to meet demand. In recent years, the increased reliance on renewable wind and solar energies has made this [increasingly challenging](#) as a cloudy or windless day means that less electricity is generated and available for use. Electricity and utilities need to anticipate needs as well as shortfalls and increase power generation from conventional fossil-fuel power plants and decrease the flow of electricity.

In 2018, a proof-of-concept for [autonomous grid balancing](#) was successfully concluded in the Netherlands between ElaadNL and the Dutch grid operator, Enexis. Using data shared via the IOTA Tangle protocol, the EV charging stations could decide by themselves whether they wanted to help balance the grid load by charging EVs at slower speeds or charging at off-peak hours. To encourage load-balancing, EV charging stations earned a small fee in IOTA tokens each time they assisted in balancing the grid.

The Vehicle-To-Grid (V2G) Opportunity

But it's not just EV charging stations that could be used to balance the smart grid. EVs, with their lithium-ion batteries, could be also used for [energy storage with zero capital cost and zero operating costs](#). When the sun is strongest and solar fields are generating the most electricity, idle EVs could absorb excess electrical power that could be discharged to the grid during times of need. In addition, vehicles could serve as mobile battery packs or energy stations that could provide or supplement power to homes and places of work.





Vehicle-to-grid (V2G) systems that allow cars to discharge energy back into the electrical grid have already been tested in a year-long trial in Denmark. In the joint project between the Nissan Motor Co. and Enel SpA, Italy's largest utility, owners of Nissan eNV-200 vans [earned \\$1,520 \(€1,300\) a year](#) for selling their electricity back to the grid during times of need. Additional V2G projects have been run by The University of Delaware and a US Air Force base in Los Angeles. The 2014 Air Force program involved a fleet of nearly 30 vehicles for more than a year in which vehicles earned an average of [\\$41 per month](#) for selling their electricity to the utility Southern California Edison.

While the two-way V2G process is very promising, the hardware for discharging electricity from EVs to the grid is not yet available and utilities do not yet have a commercial program for buying-back electricity from EVs. For now, electronic vehicles only support one-way V1G communication with power being transferred only from the grid to the vehicle.

CONCLUSION

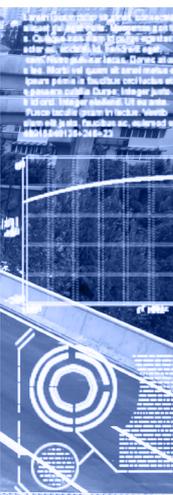
The EV ECU brings a new paradigm to cybersecurity of connected and autonomous EVs. It provides a high-performance platform that will:

- Secure the vehicle during charging/recharging process and prevent cyberattacks via compromised charging stations (EVSEs)
- Provide a cybersecurity core on which all vehicle internal and external communications are performed
- Enable autonomous cyber protection from all known and future unknown threats without software or firmware updates
- Offer the scalability to support existing services used by today's subsystems as well as support new services for Level 4 and Level 5 autonomous driving

Future development of the EVSE ecosystem and the continued protection of electric vehicles will require the development of additional cybersecurity solutions for:

- Physical interfaces connecting charging stations to the local electrical utility
- Wireless or physical communication links connecting charging stations to billing systems
- Wireless or physical communication links connecting charging stations to metering systems

Many aspects of the EV ECU may lend itself as the basis of such a future solution.



ABOUT GUARDKNOX

GuardKnox Cyber Technologies is a world-leading automotive cybersecurity coGuardKnox is a technology & engineering company specializing in E/E products and solutions for the automotive market. As the automotive industry's first Cybertech Tier supplier, GuardKnox gives OEMs, Tier 1 suppliers, and the aftermarket the freedom to evolve.

GuardKnox's secure, flexible & scalable solutions enable added connectivity, Zonal E/E Architecture, application hosting, high-speed routing, and vehicle personalization while offering the expertise, technologies, and solutions that allow the automotive industry to rapidly deliver revolutionary vehicle functionality on a cost-effective budget. Getting its start in the aviation industry, the GuardKnox team has already experienced the challenge of integrating full connectivity into advanced moving platforms by providing new and ultra-fast communication networks, fast data-based systems with a patented Service-Oriented Architecture (SOA), and high-performance computing—all with secure by design software and hardware development.

Founded in 2016, GuardKnox is collaborating with top OEMs and Tier 1 suppliers to support them in this challenging era. GuardKnox is based in Israel, with subsidiary locations in Stuttgart, Germany, and Detroit, Michigan.