© thamerpic I istock

Communication System Enables Grid Integration of E-Mobility

AUTHOR

Ursel Willrett, Dipl.-Ing. (BA) is Technical Consultant Infrastructure Systems E-Mobility Fuel Cell & Electrification at IAV GmbH in Sindelfingen (Germany).

There are many challenges to ensure a proper cooperation of the energy and vehicle world. This includes the standards and standards to be further developed and validated for testing and validating the systems, ensuring network stability and dynamic loading, as well as uniform communication models and IT security in the direction of a significantly improved user friendliness. IAV has built up know-how here.

CHALLENGES

The charging interface between grid and electric vehicles is new. Energy and automotive industry have to cooperate for a successful introduction of E-mobility. There are plenty of challenges to provide a proper cooperation of these "two worlds", **FIGURE 1**. From the view of the energy provider integration of E-mobility into smart grid is important, which includes effective dynamic load management and the use of the HV-batteries in the vehicles to store and feedback energy. The user expects sufficient and reliable charging points to recharge his electric vehicle everywhere and at any time. Keys for an infrastructure accepted by users are easy to use and secure data transfer of personal data. Important challenges for introduction of E-mobility are communication procedures and data security in the whole system. The standard ISO 15118 specifies the communication between electric vehicle and charging station. It also includes data security methods with encryption and handling of certificates and signatures.

For communication from charging station to further parties in the backend respective protocols and interfaces are used (i.e. OCPP). Some data (i.e. certificates, tariff tables) are transferred between electric vehicle and an entity in the backend.

For integration into a consistent system concept adequate processes have to be specified, agreed and supported by all parties (automotive industry, energy providers, charging station manufacturers and users).

An overall communication network between all parties supports all functions for proper grid integration. Process definition and assignment of the respective roles will enable business success of E-mobility. The components of an E-mobility system are connected via a communication network to exchange all necessary information to provide the desired functions, **TABLE 1**.

LOAD MANAGEMENT

Load management functions are performed to balance available energy and demand of energy by the users (smart grid). Charging requirements by the users are classified into three groups:

- Charging on demand (stochastic: the user expects to receive energy immediately)
- Controlled charging: the user expects fully charged battery at desired time (driven by financial reward)
- Dynamic load management: use of electric vehicles as electricity storage system. This option includes grid feedback facilities.

The grid is already overloaded from as few as 16 electric vehicles charging at the same time (3-phase 63 A, local grid 680 kVA).

To avoid overloading the grid by means of intelligent control it is required to provide a communication network with the appropriate control commands.

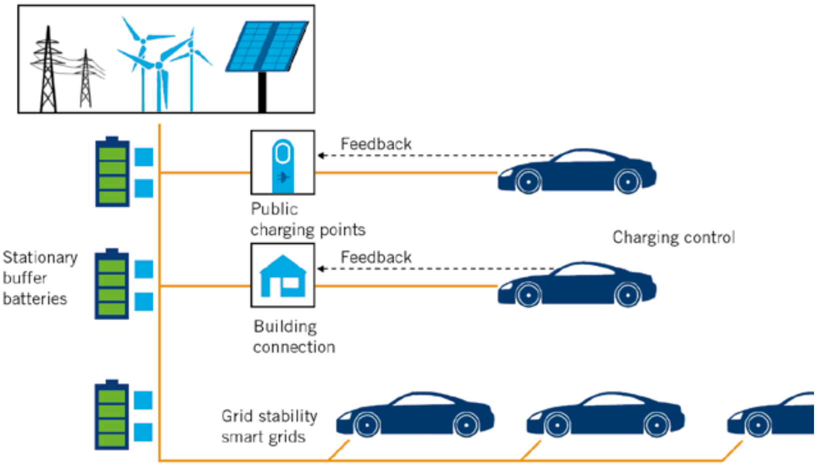


FIGURE 1 From the view of the energy provider integration of e-mobility into smart grid is important, which includes effective dynamic load management and the use of the HV-Batteries in the vehicles to store and feedback energy (© IAV)

REQUIREMENTS FOR COMMUNICATION

Users of electric vehicles want to charge vehicles everywhere (private, semi-public and public access) and at any time (24 hours per day, 7 days per week). After connecting a charging station, the user expects receiving energy from the network independent whether he has a contract with the energy provider delivering the energy for this charge point. The major requirements from the view of the user are:

- Location and time independent
- Transparent, includes similar access to all public charging stations
- Payment via account of home energy provider.

The business view has changed from local products (electric cars, charging stations) into a system product. Users are offered an E-mobility system product. This includes a communication network providing all necessary functions including E-roaming facilities.

Many existing charging stations are activated using an identification method by users (i.e. RF-ID, key card).

Group	Applications
Authorisation	– Authentication at any charging station consistently and independent of the operator of the infrastructure
Charging Control	– Charging controlled by voltage or current – Communication procedures independent on the current type (alternating current AC or direct current DC)
Grid stability	– Reduced noise and distortion caused by electric vehicles using adequate filters to comply with the standards – Robustness in electric vehicles to resist noise and distortion in the grid
Load Management	– Battery optimised charging (charging power, temperature, state of charge) and cost controlled charging (i.e. beneficial tariffs) – Avoidance overload in the grid – Smart-Grid options for optimised use of renewable energies – Fleet management with a huge number of electric vehicles (Drive & Charge)
Billing	– Automatic payment, access to all charging stations with one unique contract (e-roaming) – Calibrated metering – Data security using professional processes with signatures and certificates
Value added services	– Electric vehicle status information (i.e. state of charge, remaining charging time) – Time controlled charging (i.e. input of planned departure) – Access to services via internet, i.e. software updates, diagnostics

TABLE 1 Functions for integration into grid; the components of an e-mobility system are connected via a communication network to exchange all necessary information to provide the desired functions (© IAV)

User related data are stored on this card. This method is specified called external identification means (EIM). If the user intends to use a charging station from second provider another identification card may be required. The user needs to know in advance whether he owns the respective access card. Using “plug and charge” (PnC) the user just connects the charging plug. The identification process is maintained by the electric vehicle, charging station and backend automatically.

COMMUNICATION BETWEEN ELECTRIC VEHICLE, CHARGING STATION AND BACKEND

ISO 15118 is the specified protocol stack on Power Line Communication (PLC) between electric vehicles and charging stations [3] modulated on a basic pulse-width communication (PWM) [1]. In available charging stations and E-vehicles, the communication is implemented according to the standard DIN SPEC 70121 [5].

This standard is a derivate of the ISO 15118 with a reduced set of functions. It is used for DC-charging only to support especially charging control. Data security is not part of this standard. For data which are transferred between electric vehicles and the backend, the charging station acts as a gateway. Between charging station and the backend, adequate protocols are applicable (i.e. OCPP [4]). Several protocol stacks are currently used, a worldwide standard is actually developed.

ROLES IN THE COMMUNICATION SYSTEM

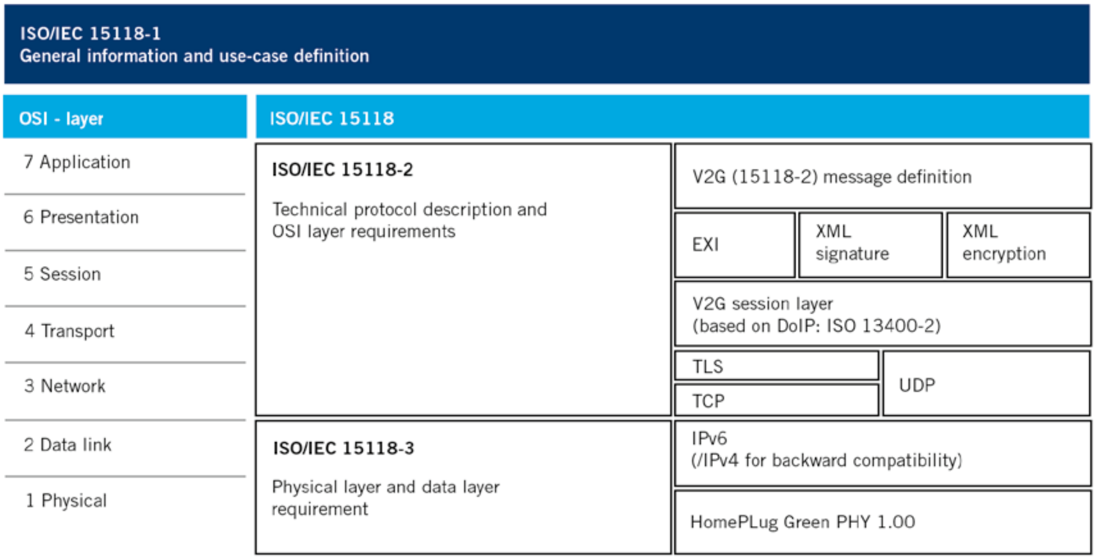
The system consists of many parties. The electric vehicles and charging stations are primary actors. All parties beyond the charging station from the view of the user of an electric vehicle are called “secondary actors”. Secondary actors are electricity providers, clearing house, E-mobility operator, meter operator, fleet operator, E-mobility operator clearing house, distribution system operator and original equipment manufacturer [2]. The communication between the primary actors (charging station, electric vehicle) is performed according to ISO 15118. The communication between charging station and secondary actors in the backend uses respective network protocols.

COMMUNICATION BETWEEN CHARGING STATION AND ELECTRIC VEHICLE (ISO 15118)

The communication between charging station and electric vehicle is performed according to ISO 15118 protocol stack. A protocol stack is in general the conceptual architecture of a set of communication protocols according to the OSI-Reference model (OSI – open system for interconnection). The protocols are sorted in seven layers starting from the physical layer (layer 1) to the application layer (layer 7), **FIGURE 2**. ISO 15118 describes all sequences, messages and parameters to provide the required functions. Data security methods are specified, i.e. encryption methods, format and contents of certificates. It provides controlled charging communication which includes connection and disconnection, authentication, selection of services, charging control, load management, data security methods and the support of value added service. The communication within a protocol is performed using specified messages and parameters. Each protocol includes the definition of syntax, semantics and timing constraints. Examples for important parameters are charging voltage, current, charging power, desired start or stop of charging process, tariff tables.

INTEROPERABILITY TEST

Manufacturers of charging stations and electric vehicles deploy products which include the communication modules. If the communication of one or both parties is not performed, according to the standard either charging is not even started or the process is interrupted before completion. It is required to prove interoperability before deployment. Potential problem areas may be:
- Pulse-width-modulated (PWM) signal may have quality or noise problems
- PLC signal quality not sufficient (noise level) PLC signal has attenuation beyond specified threshold of the standard



ISO/IEC 15118-1
General information and use-case definition

OSI - layer
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data link
1 Physical

ISO/IEC 15118

ISO/IEC 15118-2
Technical protocol description and OSI layer requirements

V2G (15118-2) message definition
EXI
XML signature
XML encryption
V2G session layer (based on DoIP: ISO 13400-2)
TLS
TCP
UDP

ISO/IEC 15118-3
Physical layer and data layer requirement

IPv6 (/IPv4 for backward compatibility)
HomePLug Green PHY 1.00

FIGURE 2 Protocol Stack of ISO 15118 [2, 3] (© IAV)

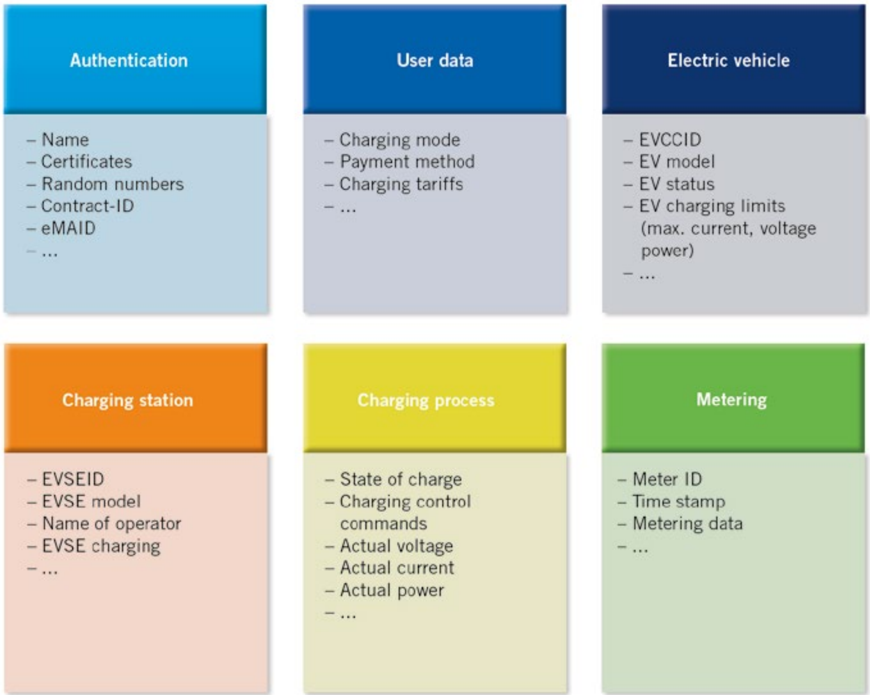


FIGURE 3 Data to be protected by unauthorised access (© IAV)

- PLC message contents is wrong
- PLC data contents is wrong
- PLC message timing fails time out values according to the standard
- Switch off procedures are not implemented properly.

To prove interoperability the communication modules of charging stations and electric vehicles are tested using a protocol test system. The test system acts as a charging station if an electric vehicle is tested. Therefore, a programmable power supply is required to support tests in the charging loop. The test system acts as an electric vehicle if a charging station is tested. In this case, an electrical load is part of the system.

All requirements specified in the ISO 15118 are tested using test cases. Using a test system which is capable to run the test cases in real time conditions electric vehicles and charging stations are tested separately. After successful test conformity of the standard has been proven. They will interact reliably with all other components which meet the standards. Electric vehicles can charge at all charging stations. There will be no problems caused by communication failures. Manufacturers of charging stations and electric vehicles can focus on their products only. Service requests by customers will decrease significantly.

DATA SECURITY

Data security covers three main properties:

- Authenticity: The communication parties are really those which they claim to be.
- confidentiality: The contents of a message can be read only by intended recipients, not by unauthorised third parties.
- Integrity: Unauthorised modification of the sent message must be avoided or at least detected.

DATA SECURITY METHODS STANDARDISED IN ISO 15118

The protocol stack of the ISO 15118 [3] provides encryption in two of the layers. In layer four, the transport layer security protocol (TLS) is specified. TLS supports encryption of the data between electric vehicle and charging station. In layer seven XML security is available with encryption of data between electric vehicle and secondary actors. Asymmetric and symmetric encryption algorithms are used for secure data transmission.

Encryption covers confidentiality of the two communication entities. It is a two-stage concept: lower layer encryption between electric vehicle and charging station and higher layer encryption between electric vehicle and secondary actor (end-to-end encryption). It is therefore not possible to read personal data in the charging station.

The methods for handling of certificates and signatures including the respective data formats are also described in ISO 15118. Creation and verification of digital XML based signatures is the method to cover authenticity and integrity. In the ISO 15118, seven types for certificates are specified used for different purposes which are handled by different instances: V2G root certificate, charge point operator certificate, mobility operator root certificate, contract certificate, OEM root certificate, OEM provisioning certificate, private operate root certificate [3].

According to ISO 15118 the chain for the certificates consists of at most three elements deviated by the root certificate. The lower layer certificates are signed by the higher layer certificate. For validation of authenticity of the certificates, private and public keys are used.

DATA TO BE PROTECTED BY UNAUTHORISED ACCESS

It seems to be a huge effort to provide data security. The data to be protected are personal data which the user does not want to be read by unauthorised persons. In addition further data (i.e. metering data) are transmitted which are used to create bills. They must not be read or manipulated by third parties. Otherwise, the confidence in E-mobility is lost. Data to be secured are sorted in groups including a few examples for sensitive data, **FIGURE 3**.

IMPLEMENTATION OF DATA SECURITY – STATUS AND CHALLENGES

Methods are available to provide secured data communication between electric vehicle, charging station and all secondary actors in the backend. In the ISO 15118, the communication between electric vehicle and charging station is specified including the description of the adequate encryption methods, handling of signatures and certificates. All specified methods comply with modern public key infrastructure systems.

The methods are specified, but the standards do not describe the process how to handle data security in the system. Because of the E-mobility system is built and maintained by several parties (i.e. automotive industry, charging station manufacturers, energy suppliers, providers, further secondary actors, root instances) the definition and establishment of a process is required with clearly defined roles. Some examples of topics to be specified are:

- World-wide standard of communication between charging station and backend
- Administration of various certificates (i.e. OEM, charge point operator CPO, provider)
- Encryption ley handling and updates, secured storage of private keys and certificates
- Administration of several contracts, E-roaming.

A reasonable specification, implementation and maintenance of secure communication is performed by IT specialists. Cooperation and agreement of all contributing parties of the E-mobility system is required.

REFERENCES

[1] IEC 61851-1 (2013): Electric vehicle conductive charging system – Part 1: General requirements

[2] ISO 15118 (2013): Road vehicles – Vehicle to grid communication interface Part 1: General Information and use case definition

[3] ISO 15118 (2013): Road vehicles – Vehicle to grid communication interface – Part 2: Network and application protocol requirements

[4] Open Charge Alliance (2014): Open Charge Point Protocol 2.0 – Interface description between Charge Point and Central System, URL: http://www.openchargealliance.org/sites/default/files/OCPP%202.0%20Release%20Candidate%202.pdf [Access 06.06.2017]

[5] DIN SPEC 70121:2014-12: Electromobility – Digital communication between a d.c. EV charging station and an electric vehicle for control of d.c. charging in the Combined Charging System