International Journal of Future Generation Communication and Networking
Vol. 9, No. 5 (2016), pp. 33-42
http://dx.doi.org/10.14257/ijfgcn.2016.9.5.04

Network Isolation in Electrical Vehicle Charging Station

Zhan Xiong[1], Liu Jian[2], Liang Xiao[1], Zhao Ting[1], Tian Wei[2],
Rao Xue[2] and Ru Yeqi[2]

[1]*Information & Communication Dept. State Grid Smart Grid Research Institute, Beijing, P.R. China*
[2] *School of Electrical Engineering, Wuhan University, Wuhan, P.R China*

Abstract

Network isolation system (NIS) can help electrical vehicle charging station (EVCS) to exchange messages with different systems (such as central monitor system, battery package and electrical vehicle (EV)) in a secure and efficient way. This paper focuses on the structure of EVCS, and then analyzes the boundaries of the trusted and the untrusted areas. On the top boundary, EVCS can communicate with the central monitor system. On bottom boundary, EVCS can communicate with EVs or battery packages. Based on this demarcation, this paper proposes the NIS architecture for EVCS. The new architecture can limit the top/bottom boundary of EVCS to enhance the securities. Finally, the proposed architecture is analyzed, which shows the feasibility.

Keywords*: Isolation System; Electrical Vehicle Charging Station; Architecture; the Trusted/Untrusted Area*

1. Introduction

Wide spread use of electrical vehicle (EV) is promising to reduce fossil fuels dependence and greenhouse gases emissions, which will help to alleviate air pollution in metropolis. As EVs are used in larger scale every single day, electrical vehicle charging stations (EVCSs) have become wide spread in China. Unlike other electrical devices, the information system in EVCS usually locates in more open space. Especially, some Internet and wireless service may be involved. Thus, more cyber attacks may occur.

Some researchers have realized the significance of the potential security issues in EVCS. IEC TS 62351-1[1] and IEC TS 62351-3[2] have been employed to exchange the messages and guarantee the security level for electrical management. Zhao *et. al.*, [3] proposes a key pool technology to simplify the encryption software, improve the efficiency and increase the attack difficulty during the interactions. Li *et. al.*, [4] propose the radio frequency identification (RFID) based information management system for EVCS. In such an open and attacked prone system, it is reasonable to separate cyber attacks from the creditable network. Because the sensitive information in the creditable network is leakage free in network isolation system (NIS), secure information exchange can be easily achieved under the above isolation circumstance [5].

Typically, NIS consists of three parts, *i.e.*, the inner unit, the private exchanging unit (PEU) and the outer unit [6]. Due to the Internet/wireless communications, it is natural that the outer unit exists in EVCS. Meanwhile, the EVCS monitoring management system handles the sensitive financial and charging data, which can form the natural boundary for the inner unit. So it is a good choice for EVCS to achieve the secure data exchange via NIS.

Based on the typical EVCS structure, this paper demarcates the trusted and the untrusted areas for EVCS, and then combines NIS and EVCS to realize a secure architecture, *i.e.*, NIS-EVCS. With the top and the bottom boundaries supported, the proposed architecture divides EVCS into two areas, i.e. the trusted area and the untrusted

ISSN: 2233-7857 IJFGCN

area. Then, many security requirements can be satisfied. Finally, the effects of the proposed system are discussed.

2. EVCS and NIS Architecture

2.1. EVCS Architecture

May be charged by AC, DC or battery charging [6]. Modern public and private transportation has become the main resort for people's daily commute, which leads to the high usage frequency of EVCS [7]. Due to the appearance of the new power source (such as photovoltaic), some new architectures have been introduced for EVCS. However, their communication management systems differ little, and multi-layer NIS structure is preferred [9]. A typical EVCS architecture is illustrated as Figure 1.

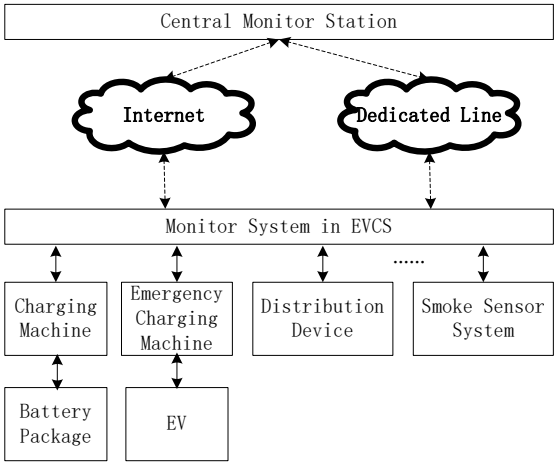

Figure 1. EVCS Structure and Management Framework

In Figure 1 described with the dashed line, the monitor system in EVCS can communicate with the central monitor system via the dedicated line or the Internet. In case of the dedicated line, it is easier to implement physical isolation. Then, security threat can be better defended. But this resort suffers from expensive construction and complex maintenance. Only some limited EVCSs can adopt this resolution. In case of the Internet, information may attract kinds of attacks, but it is more convenient to use.

In a specific EVCS, charging machine can charge the battery for quick battery exchange while emergency charging machine can be used to charge EV. Super charging station from Tesla can charge models to 50% electricity capacity in 30 minutes, and Tesla promises to shorten the charging time to 5~10 minutes in the near future. Currently, wireless and RFID technologies together with CAN bus systems are widely applied in EVCS, which leads to the complicated environment and makes adversaries easily launch attacks.

In general, EVCSs and EVs are still at an initial stage. Comparing to fueled vehicles and petrol stations, the number of EVs and EVCSs is much smaller. The related management framework is also not mature. Then, hackers will not take too much attention in attacking EVs and EVCSs. However, with the rapid development of EVs and EVCSs, the market size will swell at an incredible pace. Then, owing to the huge financial benefits, EVCS will become a rising primary target for cyber attackers. Thus, designing enough security measures is important at this stage.

As mentioned above, two distinctive boundaries have been naturally formed in EVCSs. The top boundary is the Internet via which EVCSs can communicate with the central monitor station. The bottom boundary is the wireless, RFID or CAN stretching from

EVCSs to end users (either battery packages or EVs). Because these demarcations have clearly denoted the trusted (top) and the untrusted (bottom) areas, respectively, NIS will play an important role in the information security of EVCSs.

2.2. NIS Architecture

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

Currently, firewall is the main security measure in practice. However, as firewall builds on the operation system, hackers can utilize system flaws to compromise firewalls, which is hard to defend in practice.

As analyzed in the previous section, there exist two boundaries. On the top boundary, EVCS connects to the central monitor system via Internet, which is typically realized by optical fiber. On the bottom boundary, EVCS connects to end users via RFID or other channels, such as ZigBee. Apparently, different strategies and technologies should be adopted to satisfy different security requirements.

2.2.1. Top Boundary NIS Architecture Design

As depicted in Figure 1, the top boundary is a typical network to network connection. So a standard NIS architecture can be used to solve the problem, as Figure 2 described.

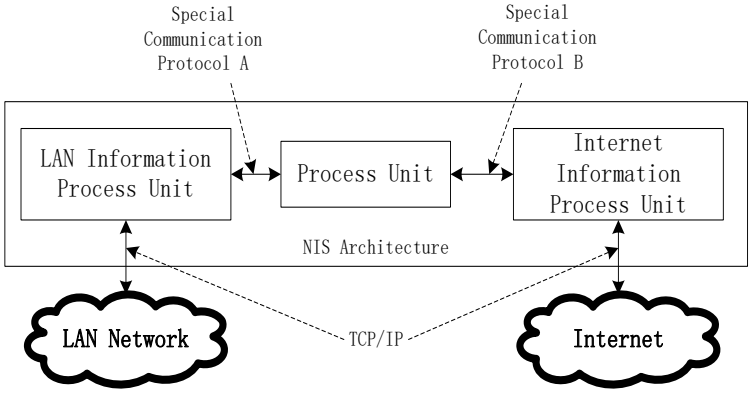

Figure 2. NIS for Top Boundary

In this trusted area, the communication consists of several parts, *i.e.*, LAN information process unit, process unit and Internet information process unit. Process unit is the secure communication channel. It can ensure that all the information is verified during the message interactions between the LAN network and the Internet.

All the involved units use the security-enhanced operation system. On one hand, they are independent to each other. This means that the LAN network is isolated from the Internet. On the other hand, they cooperate to accomplish the reliable and efficient communication between the LAN network and the Internet.

On the top boundary, topology between EVCSs and the central monitor system is relatively static. Quality of service (QoS) can be guaranteed through route optimization and adjustment. So the security issues can be solved in a relatively stationary way.

2.2.2. Bottom Boundary NIS Architecture Design

Comparing to the top boundary, the bottom boundary must face more complex situation. The mingled technologies exist, such as wire or wireless, LAN or industrial technologies, and then multiple protocols might be involved. However, the security issues are similar to the top boundary, which contains access control, identity authentication and data security.

In a sense, battery packages and EVs are volatile terminals. They usually need to communicate with EVCS through some special embedded devices. Some researchers have developed such encryption and decryption devices for secure communication through ARM S3C6410 or AT mega 128[10, 11]. Whatever, we only consider software design in this paper while hardware design is out of scope.

Currently, in software design, secure terminals mostly focus on the protocol and the key discussion. Some rules of thumb are summarized as follows.

Avoid interactive security protocols.

Avoid data segmentation transmission.

Support network scope information.

Support high error tolerance.

The top and the bottom boundaries are managed by an independent system. We will design the system's framework in the next section.

3. NIS Implementation

In this section, we discuss the system implementation of NIS in EVCS, *i.e.*, NIS-EVCS and give the detailed description of NIS-EVCS.

3.1. Management System Architecture

This system consists of control module and user interface, as shown in Figure 3. These two layers are closely coupled and integrated into the whole monitor system of EVCS. In the system, some actions are directly triggered by end users or terminals while some actions are triggered by events or specialist knowledge standards. Log data and statistical results are returned to the administrator of EVCS or the central monitor system. Particularly, the bottom communication is limited between terminals and the user interface while the top is limited between EVCS and the central monitor system [12, 13].

Ahead, several data flows should be pointed out.

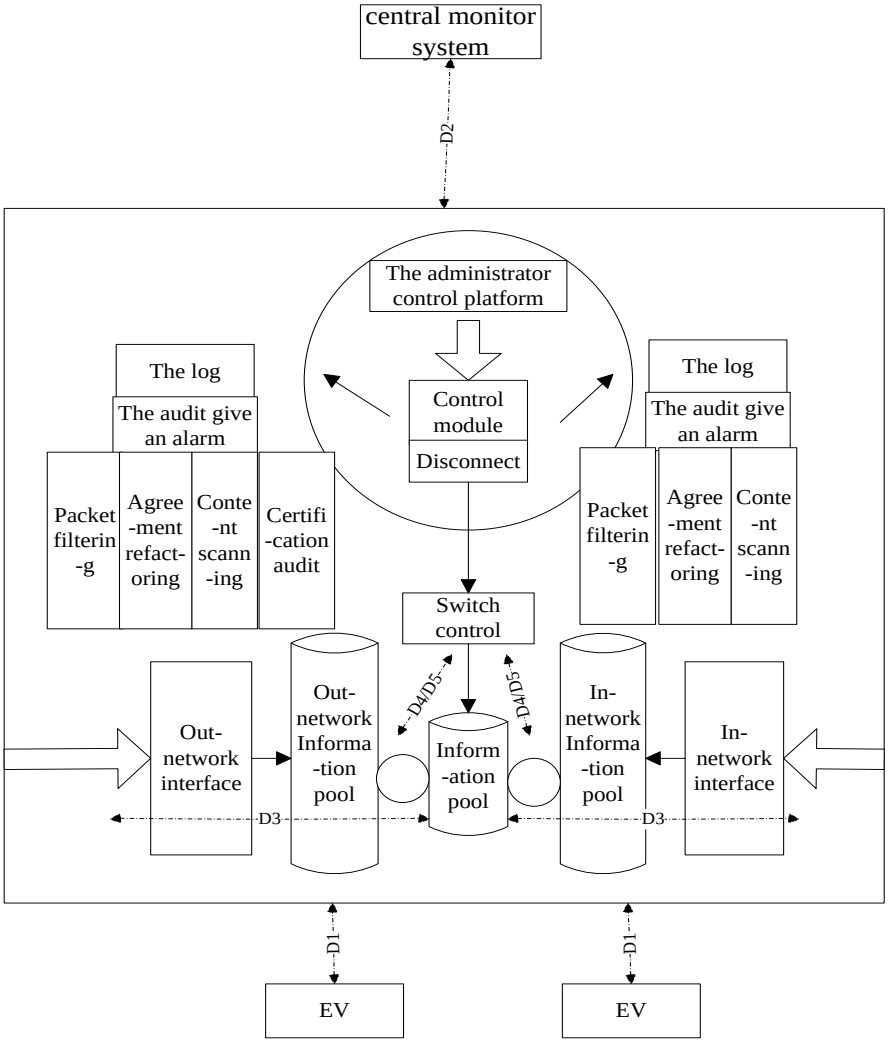

Figure 3. NIS-EVCS Architecture

- D1: This data flow belongs to the bottom boundary in EVCS. This data flow indicates the communication between devices, such as charging pile, EVs and the administrator control platform. After the data converts to the standard TCP/IP format and the primary packet filtering, the data is deposited in the information pool.
- D2: This data flow belongs to the top boundary. This data flow denotes the communication between EVCSs and the central monitor system. As the data on the top boundary is usually in TCP/IP format, packet filtering is carried out without data transformation required.
- D3: This data flow is used for content scanning and auditing in the information pool. For the data from outside network, this information pool should filter the data with malicious purposes, such as injection attacks code. For the data from inside network, sensitive data should not be spread out of the secure area, such as the user identity used to pay for the charging bill.
- D4 and D5 are the counterparts of D1 and D2 in the secure area, respectively.

3.2. System Functions

As NIS copes with data flows, it is important to take a look at them in EVCS, which would help to design better NIS.

According to the NIS-EVCS architecture in Figure 3, the related module functions are described as follows.

(1) Management and Control Module (MCM)

MCM is responsible for configuration management and surveillance. It is managed in the administrator control platform. Through modular control, all the configuration descriptions of various system functions can be accomplished. The legitimacy of different commands can be checked, and then function configuration files for this system can be generated according to the related descriptions. Meanwhile, the volume status of the information pool is monitored by this module. Logs are regularly checked and back up. In addition, by this module, global variables are managed, and dynamic settings and controls are accomplished.

In EVCS, MCM is responsible for the surveillance of both the top and the bottom boundaries. Charging pile and monitor workstations in EVCS are under the control of MCM.

(2) Physical Isolation Module (PIM)

PIM is controlled and coordinated by the control module. It handles the data in (In/Out) network information pool from In/Out-network. The data diode mode is adopted to ensure that the inner and the outer network will not be linked at the same time. That is to say, when the inner network is lined to the data pool, the outer network should keep unlinked. The link number of the data pool must be less than or equal to 1.

PIMs locate both on the top and the bottom boundaries. On the top boundary, it performs almost the same function of common PIM. On the bottom boundary, PIMs are often oriented by the related protocol. This means that one PIM tackles a specific protocol. In technical terms, it is possible to integrate all the protocols in one PIM. But for modular design and implementation, it is rational to adopt this kind of scheme.

For example, EVCS may communicate with the charging pile using CAN or ZigBee. Then, different PIMs should be deployed according to the electrical and the geographical restraints. It would also help to make full use of the current asset, which is enormous. Besides, this will encourage hybrid design to adapt different situations for EVCS.

(3) Protocol Reconfiguration Module (PRM)

PRM can accept those packets filtered by the filtering module, which can leads to executing the protocol stripping. This means that the data inside the packets and the information in the original header fields are repacked here. The data structure can be described as a two-tuple, RD=<D, P>, where D represents the application data, P represents the protocol information of the original header field. RD packets are repacked by using non-routable private protocols, and then are stored in the information pool. Then, these data are extracted to reconfigure protocols. That is to say, after the P element is taken, the related packet is restored back to accord with common protocols.

Note that many different protocols exist in EVCS, such as ZigBee, RFID, CAN or other industrial field bus. In order to enhance message process efficiency, it is important to transform these messages into the uniform format.

(4) Packet Filter Module (PFM)

In PFM, according to the security policies, these packets in and out are dynamically checked and processed with the matching rules. Each rule in the security policy table can be described as a six-tuple, AP=<SI, Sp, DI, Dp, If, Action>. SI:Sp represents source address and source port number; DI:Dp represents destination address and destination port number; If represents the distinction number of the distinguishing streams; Action represents the processing actions. When a packet enters this module, both the attribute (such as <SI, Sp, DI, Dp, If>) and the stream distinction number will be extracted to

match these policies by the system. If there is a match term, the corresponding process (such as pass permission or discarding) will be executed on the packet according to the matching actions.

If the state filtering technology is adopted further, the application protocol and the data type will be searched in the filtering strategy table, and then the filtering operation will be done. Each rule in the filtering strategy table can be described as a trituple, DEP=<A, Dt, Pro>, where A represents the application protocol type, Dt represents the data stream type, Pro represents the rule priority. The filter strategy table is modified based on the dynamic information, and the elements of the filtering rule can also be added or deleted according to the security requirements.

In EVCS, PFM is based on PRM conversion result. As all the data has been changed to TCP/IP format, it is relatively simple.

(5) Content Scanning, Audit and Log Module (CSALM)

Contents are scanned and filtered by filter algorithm, and then the results can be abandoned, dumped, *etc*. This module is linked to audit and log modules. It not only discards data, but also leaves the electronic evidence to ensure safety.

(6) Certification Examination Module (CEM)

In this module, the certification examination is asymmetrical. That is to say, this module is necessary when information is transmitted from outer network to inner network. This can control and authenticate the legal operations of the remote access in order to protect the inner network hosts from illegal invasion.

On the top boundary, it is important to implement CEM. Sensitive data such as D4 should be carefully verified to guarantee the integrity of the data and the security of the transaction record. However, on the bottom boundary, it depends on the employed technology. As some technologies such as RFID have restricted the resource for CEM, other credential methods should be performed, or multiple-sources information could be cross-checked. For example, to identify a vehicle, we can cross-check the plate, RFID information and two-dimensional code.

4. Analysis

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

In this section, we analyze NIS-EVCS of which the security features can be seen in Table 1.

Table 1. The Features Of NIS-EVCS

Characteristic	Function description
Network isolation	The top and the bottom boundaries are separated.
Access control	In/out netowork users have different rights to access resources.
Log audit	Secure behaviors are required through log audit.
Confidentiality and integrity	All the data are protected by the related rules.

(1) NIS-EVCS separates the top and the bottom boundaries. The outside attacker cannot invade the inner system through network connection while the inner information can be protected from leakage. Besides, each terminal cannot use the inner and outside network at the same time. Thus, network isolation can be achieved.

(2) NIS-EVCS provides access acceptance/rejection for isolated resources. Through the top and the bottom limitation, only the legal user has the rights to get access the related data by authentication. This means that the outside user can't connect the inner network. Then, sensitive information can be securely transmitted.

(3) NIS-EVCS audits the log for secure behaviors. Through CSALM, NIS-EVCS can scans and filters the system operations. Then, the system is monitored. Any illegal activity can be recorded and detected, and then the related responsible party can be traced, which can ensure the system security.

(4) NIS-EVCS can satisfy data confidentiality and integrity. In the top and bottom communications, the stored data and the filter policies will not be consulted without authorization. This means all the data are protected by the security rules. Then, data confidentiality and integrity can be achieved.

According to the above analysis, we can see that NIS-EVCS can achieve the kinds of security features, which is feasible for isolation requirements.

5. Conclusions

This paper researches on the security problem of EVCS. On demarcation of EVCS, the whole system is divided into three parts, and according boundaries is discerned. This paper proposes a management infrastructure, NIS-EVCS, by combining NIS and EVCS. It can satisfy kinds of security features, such as network isolation, access control, data confidentiality and integrity, *etc*. The analysis shows the feasibility of the proposed architecture.

Acknowledgements

This paper is sponsored by the National High Technology Research and Development Program ("863"Program) of China with number 2012AA050804.

References

[1] "IEC TS 62351-1", Power System Management and associated information exchange.
[2] "IEC TS 62351-3", Power System Management and associated information exchange.
[3] X. Zhao, Z. H. Liu and Q. M. Chen, "Data Communication Security Strategy for Electrical Vehicle Charging Station", Automation of Electrical Power Systems, vol. 35, no. 12, **(2011)**, pp. 92-94.
[4] J. P. Li, X. Jiang and J. S. Sui, "Intelligent Information Management System with RFID for Electric Vehicle Charging Station", Process Automation Instrumentation, vol. 34, no. 11, **(2013)**, pp. 62-65.
[5] H. Y. Wu, C. X. Tan and H. N. Wang, "Building a High-performance Communication Framework for Network Isolation System", ICNSC, **(2008)**, pp. 1086-1091.
[6] H. Yan, G. Y. Li and L. Zhao, "Development of Supervisory Control System for Electric Vehicle Charging Station", Power System Technology, vol. 33, no. 12, **(2009)**, pp. 15-19
[7] G. Ivana, K. Vedran and S. Srdjan, "The development of charging stations for electric vehicles: a solution or a problem?", MIPRO, Opatija, Croatia, **(2013)**, pp. 1226-1230.
[8] M. A. Abella and F. Chenlo, "Photovoltaic Charging Station for Electrical Vehicles", Photovoltaic Energy Conversion, Proceedings of 3rd World Conference, **(2013)**, pp. 2280-2283.
[9] J. Brassil, "Physical Layer Network Isolation in Multi-tenant Clouds", ICDCSW, Genova, Italy, **(2010)**, pp. 77-81.
[10] "S3C6410 USE'S MANUAL REV1.10", Samsung Electronics, **(2008)** .
[11] N. S. Liu and D. H. Guo, "Security Analysis of Public-key Encryption Scheme", Based on Neural Networks and Its Implementing International Conference on Computational Intelligence and Security, **(2006)**, pp. 1327-1330.
[12] P. S. Zhang, "Studying Safety and the Data Exchange of Based on Physical Isolation", China Date Communications, vol. 4, no. 5, **(2002)**, pp. 19-22.

[13] P. Zhao, H. H. Wang and C. X. Tan, "Design and Implementation of Network Isolation Security Audit System Based on Firewall Log", Application Research of Computers, vol. 24, no. 7, **(2007)**, pp. 114-116.

Authors

Zhan Xiong, he works at State Grid Smart Grid Research Institute. Zhan graduate from Fudan University in 2000. He is the director of active defense and controllable security technical office.

Liu Jian, he received M.S. from Wuhan University (WHU) in electrical and electronic engineering and Ph.D. degree in computer architecture from Huazhong University of Science &Technology, Wuhan, China, in 2001 and 2006, respectively.

Currently, he is associate professor at School of Electrical Engineering at the School of Electrical Engineering at WHU. His main research interests are related to distribution network risk evaluation and reliability and Life-Cycle Cost. He is the correspondence author of the paper.