Potential Cybersecurity Issues of Fast Charging Stations with Quantitative Severity Analysis

Yongwan Park[1,2], Omer C. Onar[2], and Burak Ozpineci[2]

[1]Maryland Power Electronics Laboratory (MPEL), Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742 USA
[2]Power Electronics and Electric Machinery Group, Oak Ridge National Laboratory
National Transportation Research Center. Knoxville, TN 37932 USA
Email: ywpark@umd.edu, onaroc@ornl.gov, and burak@ornl.gov

***Abstract*—Potential issues of front-end converters of wireless power transfer system modules for extreme fast charging are discussed and analyzed in this study in order to provide some recommendations to defend against attacks on electric vehicles and charging systems. Compared to conventional low-power charging systems, the impact of a cyber-attack might be more detrimental in high-power / fast charging systems since the fault energy levels would be inherently higher both on the grid- and vehicle- side converters. In order to analyze the potential issues that might be a result of cyber-attacks, the negative scenarios are reviewed in this study which include interfering with the grid-side controllers, establishing fake communications between the vehicles and the charging stations, and interfering with the battery management system functionalities. A 100-kW stationary wireless power transfer system with a series-series resonant compensation network is used as a representative system in the analysis. Potential damages and the fault energy levels for selected fault scenarios are investigated. The system is simulated to verify the analysis results. On the basis of the discussed worst-case study, a set of hardware design-level solutions are recommended in this study to provide cyber protection.**

***Index Terms*—Extreme fast charging, security, hardware, design consideration, wireless power transfer system.**

I. Introduction

The significance of cybersecurity on power electronics systems has dramatically increased in recent years with the augmented electrification of transportation and introduction of the smart grid. Even though electricity-based power systems are continuously monitored by central energy management systems, the power systems are inherently vulnerable to cyberattacks because these systems are in contact with external devices that are relatively less secure. The bidirectional data communication between the system processors and the external devices exposes higher systems to the threats from the outside. For example, Ukrainian electric utilities were under attack in 2015 and 2016 that resulted in a few hours of black outs in the city of Kiev [1].

This manuscript has been authored by Oak Ridge National Laboratory, operated by UT-Battelle, LLC, under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. The Department of Energy will provide public access to these results of federally sponsored research in accordance with the *DOE Public* Access *Plan (http://energy.gov/downloads/doe-public-access-plan).*

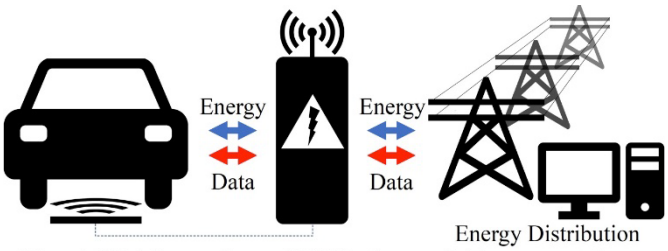


Fig. 1. Conceptual configuration of EV charging systems.

The problem also exists and is even more serious in fast charging systems for electric vehicles (EVs) due to their high accessibility and the large amount of the power flow to electric vehicles. The U.S. Department of Energy's Vehicle Technologies Office (VTO) recently launched a comprehensive research program on extreme fast charging (XFC) that deals with high power levels up to 350 kW and emphasized the vulnerability of the XFC systems [2]. Similar to DC fast chargers, XFC-level wireless power transfer systems also need external charging stations, shared with multiple EV owners. And, the start and stop of the charging process as well as the voltage, current, and power modulations are done through the communication between the vehicle-side sensors and the controller of the charging station as depicted in Fig. 1, based on the charging profile and real-time status of the battery. One possible attack scenario on the communication system might be an infection of the controller of the charging station and, eventually, the central management system with undesired viruses and malwares via the data communication buses. Or, the malicious codes can spread via the station, and the number of infected EVs can grow up exponentially. As a result, the attackers can gain the control of the charging stations and/or the vehicles [2], [3]. Both software- and hardware- level approaches have been investigated for this problem in references [4], and [5].

In addition to the high-level problems, local issues can occur at the front-end or grid interface part of the charging system. The outermost infrastructures can easily be disrupted by fake information or requests from the vehicle side. A representative case is that the external charging station for an XFC station supplies excessive power due to the fake request from the vehicle side, so the excessive current flow damages the vehicle-side power converters or the battery pack. This can be done by interfering with the battery current sensor or by manipulating the sensor data sent to the controller. Moreover, considering the

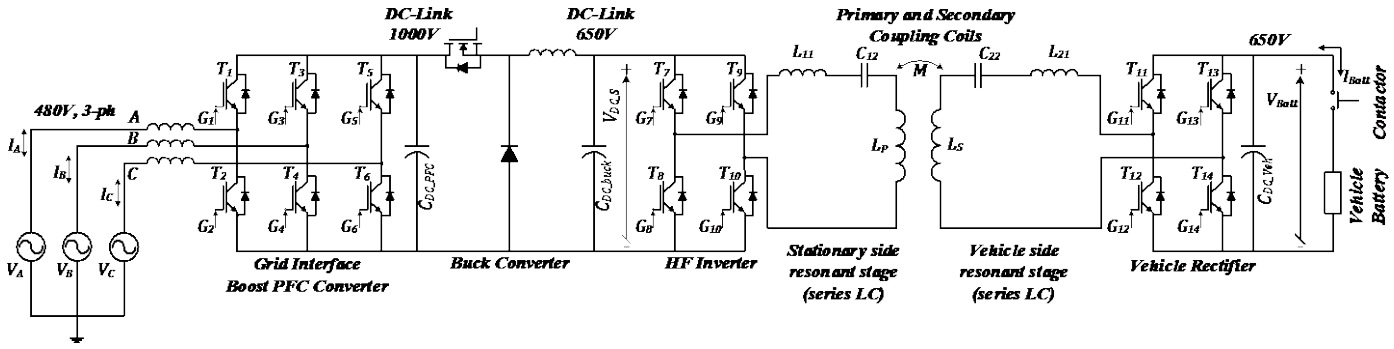


Fig. 2. System level schematic of simulated 100 kW wireless power transfer XFC module.

high power of XFC, the station-level issues can even lead to damage on the higher-level systems, from the charging station to the adjacent power supplies. To effectively defend against the local threats, the negative scenarios should be identified and evaluated first. Then, the estimated damage such as the amount of fault energy and potential damage to the dedicated components should be determined. Finally, solutions that prevent the possible issues can be built based on the analyses. This paper therefore aims at providing both qualitative and quantitative analysis of the potential issues of fast-charging wireless power transfer (WPT) system stations under a controller-level attack.

This paper is organized as follows. The XFC-level wireless power transfer system module is described in Section II. The potential amount of fault energy is discussed in Section III using simulation results. The possible solutions to prevent the identified problems on hardware design aspects are suggested in Section IV. Finally, this paper is concluded in Section V.

II. Analyzed Wireless Power Transfer System and Potential Issues

A simplified circuit schematic of the implemented 100 kW WPT system module is illustrated in Fig. 2 [6], [7]. The high-power wireless charger circuitry mainly consists of three stages. The grid interface boost PFC converter converts 480 V 3-phase AC grid voltage to 1 kV DC voltage with near-unity power factor, and the following buck converter is responsible for regulating the voltage for controlling the power while charging vehicles with different battery nominal voltages. In this particular setup, the buck converter steps-down the primary side DC-link voltage to 650 V for the resonant compensation network. The transferred voltage and current can be controlled by the DC link voltage and the frequency and duty cycle of the high-frequency (HF) inverter. Then, the required power is transferred to the output battery load through the vehicle-side full-bridge rectifier circuitry with capacitive filtering. In most systems, a battery management system (BMS) is utilized to monitor the battery voltage, current, temperature, and state-of-charge. BMS is also responsible to operate the charging/discharging enable relays of the battery pack. This battery status information is conveyed to the primary side for the grid-side controller to operate based on this information and the charging profile. The wireless power transfer system is designed to transfer power up to 100 kW at a switching frequency of 22 kHz, which is equal to the resonant frequency of the implemented resonant stage, and 50 kW operation under a coupling coefficient k of 0.44 is validated through experiments. Transistor switches and diodes of the WPT system module are implemented by CAS325M12HM2 1200 V – 325 A silicon carbide (SiC) MOSFET phase-leg modules.

Among many potential failures, the following issues are mainly discussed in this paper:

- Grid-interface converter short-circuit condition (phase-to-phase or three-phase faults),
- Primary-side DC-bus short-circuit condition (shoot-through)
- Sudden loss of the load (disabling battery charge enable relay)
- Faked electric vehicle presence (no secondary side physically available while primary runs at full power)

III. Estimation of Fault Energy & Damage

A. Short-Circuit Condition

Electrical short-circuit conditions can occur by either error in the control system or by interfering the control system software to command same phase-leg switches to turn on at the same time. In this section, two representative short-circuit conditions, DC-bus short-circuit condition and AC phase-to-phase short-circuit condition, are investigated with various considerations, from ideal transistor devices to realistic components.

1) DC-bus Short-Circuit Condition

The DC-bus short-circuit condition is caused by overlapping the turn-on of two switches in a transistor phase-leg. In the implemented WPT system module, the output DC-link capacitor of the PFC converter (C_{DC_PFC}) can be shorted by the three phase-leg modules of the PFC converter. And the two phase-leg modules in the HF inverter can short the output capacitor of the buck converter (C_{DC_buck}). Under the short-circuit condition, the drain-source current of the shorted devices surges up, resulting in high energy dissipation.

With ideal transistor devices, of which the drain-source current does not saturate, two loss mechanisms are dominant: discharge of DC-link capacitors and excessive current injection from adjacent converters. Figure 3 demonstrates time-transient simulation results in short-circuit condition of C_{DC_buck}. From the simulation results, it is seen that the current and the voltage across the short-circuit follow a typical RC-discharging process

in the beginning; therefore the current instantly rises to $V_{DC,t=0}/R_{on,leg}$. Since high-current SiC devices have a low on-resistance of few mΩ, that ideal short-circuit current is usually in orders of kilo-Amps, much higher than peak saturation drain current of real devices.

Maximum drain current of a real MOSFET device is lower than that of the ideal MOSFET model because the peak current is limited as saturation current during withstand time. And, electrical parameters under short-circuit condition highly depend on the type of devices. SiC MOSFETs, which have relatively high instantaneous power density and small thermal capacitance, have fast temperature rise and short withstand time. In addition, the peak saturation current (typically around 15 times higher than the nominal current [8]) is determined by the design of the channel; hence, low on-resistance of high-current SiC transistors results in high peak saturation current.

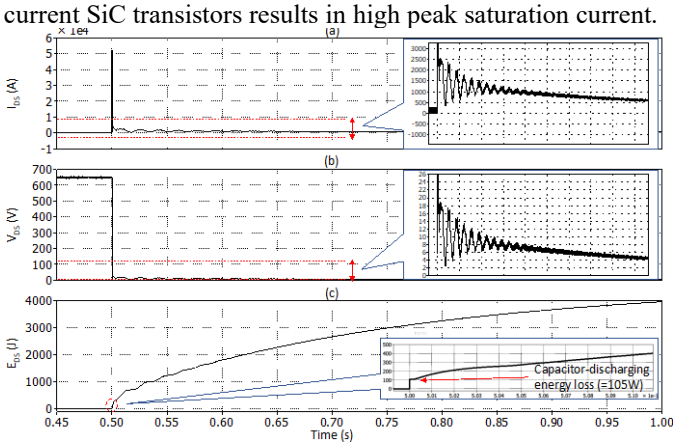


Fig. 3. Transient response of the ideal transistor in the DC-link capacitor short-circuit condition: (a) drain-source current, (b) voltage across C_{DC_buck}, (c) fault energy loss.

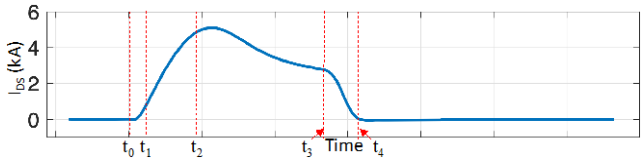


Fig. 4. Expected transient response of 1200 V – 300A phase-leg module in the short-circuit condition, protected by de-saturation protection circuitry.

Experimental data of Cree's 1200 V – 300 A phase-leg module is provided in [8] and [9]. As discussed in these references, the phase-leg module has about a 5 kA peak saturation current for 3.2 μs withstand time under $V_{DS} = 600$ V condition, so the critical energy of the switch module turns out to be 6.9 J. Two failure mechanisms are: 1) thermal runaway failure and 2) gate breakdown failure [8]. Because the failure mechanisms highly depend on temperature variation and worn-out of a device, repeated short-circuit pulses cause further reduced withstand time of transistor devices.

A widely used solution for short-circuit breakdown of switching devices is utilizing gate driver ICs that offer a de-saturation protection function, which senses V_{DS} during the operation and turns off the devices when overcurrent flows. Figure 4 depicts the current waveform of the short-circuit condition with the de-saturation protection-enabled gate driver IC, where:

- t_0: short-circuit event time
- t_1: over-current detection time
- $t_1 \sim t_2$: blanking time
- $t_2 \sim t_3$: response time
- $t_3 \sim t_4$: soft turn-off time

As illustrated in the expected current waveform, the short-circuit failure is prevented when the total response time of the protection circuitry is shorter than the withstand time. According to the investigation in [8], higher V_{DS} results in shorter withstand time, so the phase-leg module under V_{DS} of 800 V has about 1.9 μs withstand time. Design of fast-responding de-saturation protection circuitries, which ensure the prevented device failure, is challenging due to unique characteristics of high-current low-resistance SiC transistors [10], [11]. At higher power levels, required response time of the protection circuitry becomes even shorter due to the high current carrying capacity of switches. In addition to that, a tradeoff between providing high noise immunity and operating within the short-circuit withstand time, determined by passive components of the protection circuitry, makes it harder to meet the withstand time restrictions.

Once the device failure occurs, the drain-source current surges up with uncontrollable gate voltage; and then, slowly decreases to 0 A because the PFC converter is designed to maintain constant output voltage by modulating the amount of current. As a result, additional power is dissipated for a longer period of time. During the trip time of the current, the high current request from the buck converter also drops the voltage potential across C_{DC_PFC} to zero, so the input impedance of the grid-interface converter becomes purely inductive. Thus, high reactive power is induced in the grid input source.

Source-connected protection circuitries such as fuses can alleviate the high fault energy issue. For example, L50QS (500 V_{AC} - 200 A_{RMS} high-speed fuse from Littelfuse®) disconnects the grid power supply in 0.05 s after it senses an input current of 1 kA_{RMS}.

2) AC Grid Interface Converter Short-Circuit Condition

Another potential short-circuit condition can occur in the boost PFC converter stage when the switches between two or three phases are on simultaneously. The potentials at the nodes connected to the filter inductors become 0 V because the PFC converter still operates to maintain a constant output voltage while achieving unity power factor. Thus, the single-phase 277 V AC input voltage is solely applied across the filter inductors. This results in high current due to the small input impedance of the grid-interface converter. The implemented module has 750 μH inductance, so the current from each single-phase source becomes 980 A_{RMS}. Simulation results in Fig. 5 demonstrate that the AC-grid short-circuit condition results in 980 A_{RMS} at steady-state.

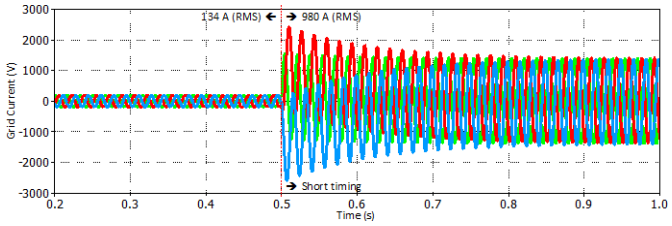


Fig. 5. Simulation result of the grid interface converter short-circuit condition: 3-phase grid current.

B. Improper Operation of the WPT Resonant Network

Operation of the HF inverter depends on the operating frequency of the inverter and the following resonant network. Furthermore, electrical parameters of the implemented series-series WPT system module are highly sensitive to the load variation as depicted in Fig. 6. Therefore, the charging station requires accurate information from the BMS, so that the charging station can achieve safe and robust operation for regulating the battery current or voltage.

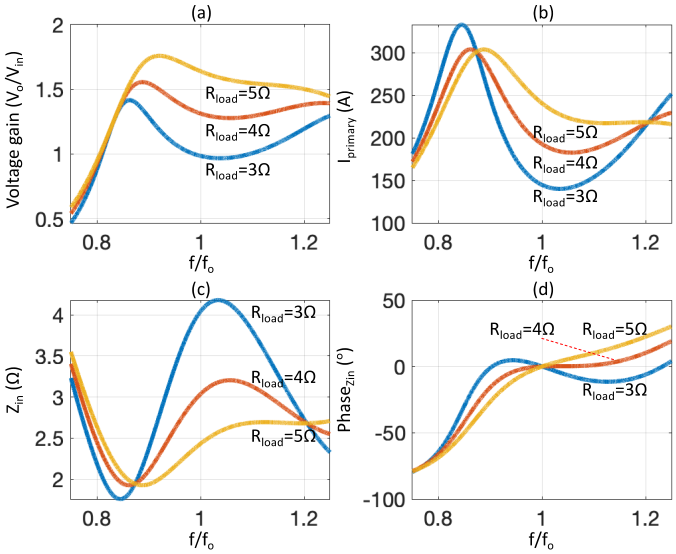


Fig. 6. Fundamental harmonic approximation of the implemented series-series resonant compensation network in normal conditions with variable load resistance (fixed coupling coefficient, $k = 0.44$): (a) voltage gain, (b) primary-side RMS current, (c) input impedance, (d) phase of input impedance.

Especially, once the battery is fully charged, a charging termination request is issued by the BMS. Following this comment, primary-side power converters are orderly turned off and the load is safely disconnected. The following steps are used to open the battery contactor [12]:

- BMS issues a STOP CHARGE message to the grid-side control system.
- The grid-side HF inverter stops operating, and the controller stops charging by turning off the converters.
- The battery contactor responds, and inrush current alleviation circuitry starts to operate within 2-4 ms until the contactor opens.

Because the steps are proceeded solely based on the communication between the BMS and the grid-side control system, the termination process has a high possibility of being interrupted by external intervention or timing mismatches.

For the implemented resonant converter-based WPT system module, the worst case happens when the battery contactor is opened before the grid-side control system turns off the converters. It is preferred to operate the resonant converter at a near-resonant frequency in normal operation in order to minimize power losses and the circulating current. Under the open load condition; however, the resonant frequency operation causes extremely high voltage gain and primary coil current would be as shown in Fig. 7. As depicted in the estimation, the voltage gain of the resonant converter with an ideal DC voltage source is higher than 400 V/V when the switching frequency is around the resonant frequency. This is because the peak voltage across the magnetizing inductance is directly transferred to the output low-pass filter capacitor. The result-in voltage level is too high for the main components to endure. The frequency, 1.1 times higher than the resonant frequency, can still cause a hazardous situation with a predicted voltage gain of 2.53 V/V.

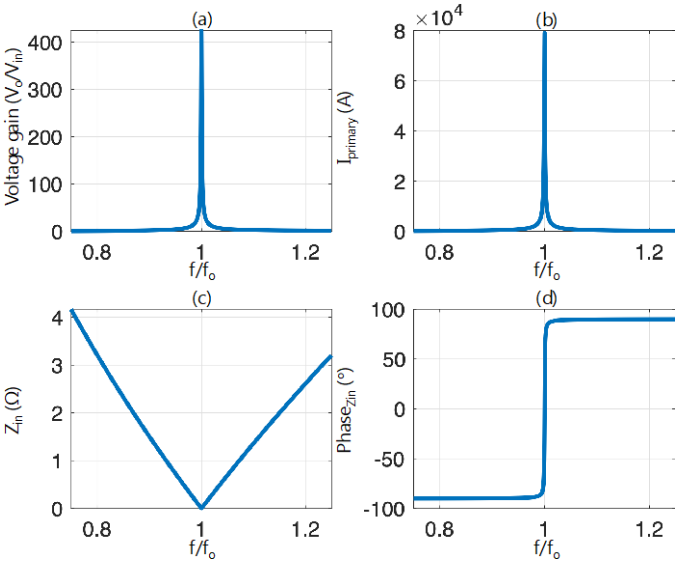


Fig. 7. Fundamental harmonic approximation of the implemented series-series resonant compensation network with open load condition: (a) voltage gain, (b) primary-side RMS current, (c) input impedance, (d) phase of input impedance.

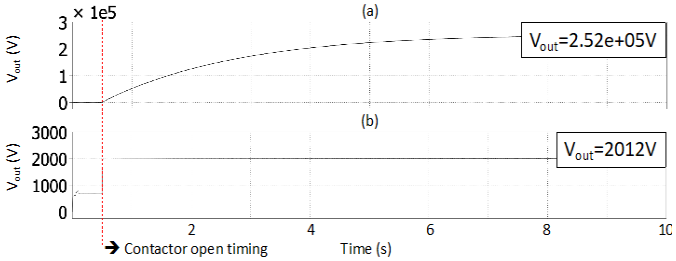


Fig. 8. Simulation results of the output voltage in open-contactor condition with different switching frequencies (ideal DC voltage input to the HF inverter, $V_{in} = 650\ V$, coupling coefficient $k = 0.44$): (a) 22.3 kHz, (b) 24.541 kHz.

Since all components are selected by considering normal operations with reasonable margins, these high voltages and currents may damage the components. To be specific, the

implemented WPT system module employs the SiC phase-leg module CAS325M12HM2 for the primary-side HF inverter and the secondary-side passive rectifier; and they are rated for up to 1200 V, assuming 800 V as the upper limit of the transistor devices in normal operations. Other main components such as capacitors and inductors may be damaged for the same reason.

Simulation results of the output voltage in aforementioned two switching frequencies (22.3 kHz and 24.541 kHz) are demonstrated in Fig. 8. An ideal input DC voltage source is used for the simulation, and the results fit the estimation. Note that the closer to the resonant frequency, the more accurate the result is, due to the fact that the estimation is based on the fundamental harmonic approximation (FHA).

For a more realistic estimation, entire module (boost PFC + buck DC-DC + WPT) is modeled and simulated in PLECS with appropriate closed loop controls, and time-transient simulation results are demonstrated in Fig. 9.

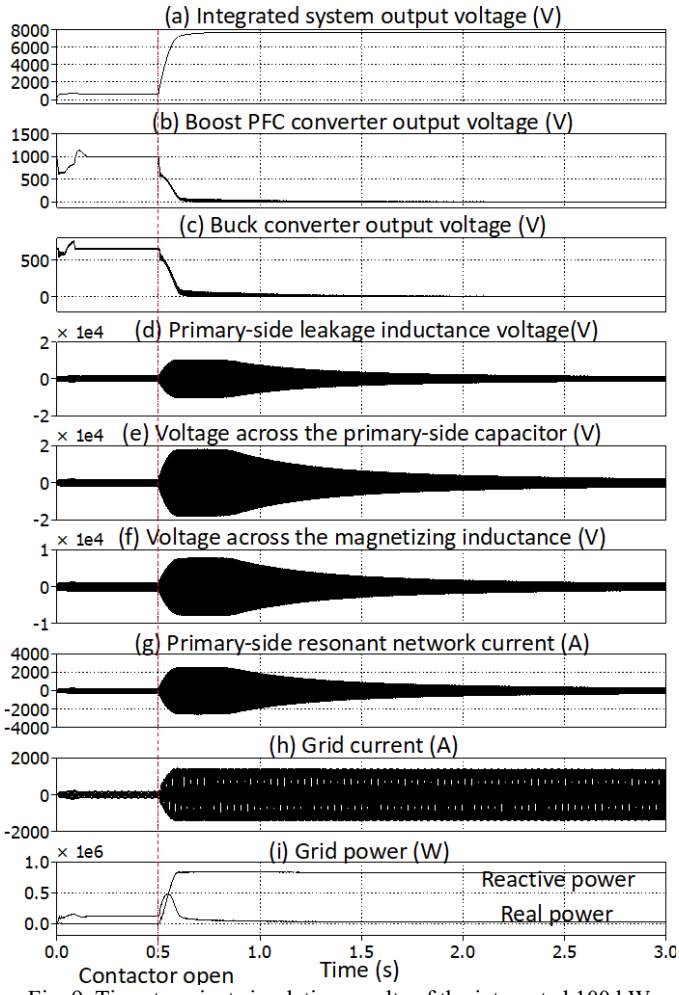


Fig. 9. Time-transient simulation results of the integrated 100 kW WPT system module with 22.3kHz switching frequency.

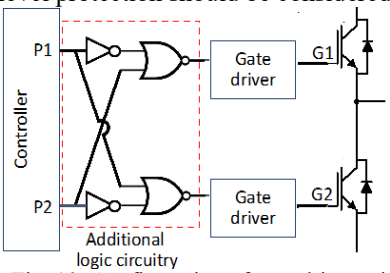
It is seen that the integrated system module has lower current and voltage levels than the case with an ideal DC voltage source. Because the maximum current that the boost PFC converter can supply is limited by the size of the filter inductance, the output voltage of the PFC converter drops to zero early when the extracted current is higher than the supply current limitation. Nevertheless, electrical parameters of main components are still excessively high; therefore, all components in the WPT system module are in danger in the worst case of the near-resonant frequency operation with the no-load condition. Note that the current from the grid gradually reaches 980 A_{RMS} as illustrated in Fig. 9 (h); hence, a total of 815 kVA ($= 3 \cdot 980\ A_{RMS} \cdot 277.1282\ V_{RMS}$) is circulating as reactive power until the implemented fuse trips. This high reactive power may affect adjacent grid connections, dropping the overall voltage of the grid. As a result, grid protection circuitries such as under-voltage protection circuitries may start to operate.

IV. Hardware Design Level Solutions

As discussed in Section I, many researchers have been investigating solutions to enhance the security of high-power fast charging systems. However, it is impossible to absolutely prevent all attack scenarios because attack methodologies have evolved together with protection schemes. Furthermore, real-time firmware update and real-time control of charging stations are significantly beneficial features to maximize benefits of the smart grid. Therefore, hardware design-level approaches can be effective solutions for some potential issues. Two main issues covered in this paper are the short-circuit condition and the unorderly turn-off process of the system. Example hardware design-level approaches to avoid those two cases are proposed, which require relatively less effort.

A. Prevention of the Short-circuit Condition

The switch pairs that cause the DC or AC short-circuit conditions should not be turned on simultaneously at any time. The de-saturation protection circuitry can be an effective solution for the DC short-circuit issue, but the protection has a definite limitation in high current SiC devices due to their short withstand time and high saturation current. Once the device failure happens, related components are usually burned out. Even if the short-circuit issue is prevented by a well-designed protection circuitry, high temperature rise during the withstand time results in shortened lifespan of the transistor devices due to thermal stress-wear out mechanism. For these reasons, lower-level protection should be considered in advance.



INPUT		OUTPUT	
P1	P2	G1	G2
LOW	LOW	LOW	LOW
LOW	HIGH	LOW	HIGH
HIGH	LOW	HIGH	LOW
HIGH	HIGH	LOW	LOW

Fig. 10. Configuration of gate driver with the simplest external non-overlapping circuitry and corresponding truth table.

Conventionally, non-overlapping switch operation is conducted by microcontrollers in software level. However, the microcontroller-level prevention of the short-circuit condition may not work if the controller is overtaken by attackers. Utilizing an external digital-logic circuitry between the

controller and gate driver ICs can be an appropriate solution. For example, the digital-logic circuitry in Fig. 10 consisting of only a few logic gates directly transfers gate signals for normal operations but filters out the signal pair that causes the short-circuit condition; therefore, the transistor leg turns off instead of shorting as shown in the truth table. Those additional digital logic circuitries can be implemented by μm scale transistor technology, which is considerably cost-effective and small, and can be integrated with gate driver ICs.

As a separate option, other existing non-overlapping circuit topologies for micro- or nano- scale integrated circuits can be considered for an effective solution. This hardware solution used to be the standard for designing gate drivers as a form of dead-time control feature. With more digitized controls, it was switched to a digital solution. For improved cybersecurity, hardware shoot-through prevention, independent of the digital control, is needed.

B. Prevention of the Safe Turn-off Process Violation

The issues from the unorderly turn-off process occur if the series-series compensation network operates with near-resonant switching frequency when the battery contactor is opened. Various compensation network topologies have been proposed, and each topology has unique advantages and disadvantages. The series-series tuned WPT system does not require additional inductors and it simply involves adding a series capacitor on primary and secondary sides. Therefore, the power density can be maximized. In addition, reduced number of components enables the topology to achieve considerably high efficiency in optimal operation by reducing realistic effects from intrinsic resistance.

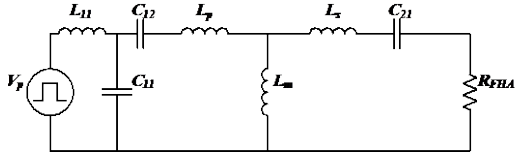


Fig. 11. Equivalent circuit of LCC-series resonant compensation network topology.

Recently, LCC-based compensation topologies such as LCC-LCC and LCC-series have been proposed and investigated as a promising solution for high-power WPT systems. Those primary-side LCC-tuned topologies have several advantages. For example, primary-side resonant tank current of LCC-tuned topologies is load-independent (independent of coupling coefficient k and load resistance) at resonant frequencies so that the topologies can operate with a characteristic of a constant current source [13], [14]. Among them, LCC-series compensation network in Fig. 11 has especially insensitive voltage and current variation around the resonant frequency as depicted in Fig. 12. This feature enables the WPT system to stay safe from the sudden no-load condition issues; therefore, implementing the LCC-series compensation network topology instead of the series-series topology can be an effective way to protect the converters that are vulnerable to the controller attacks.

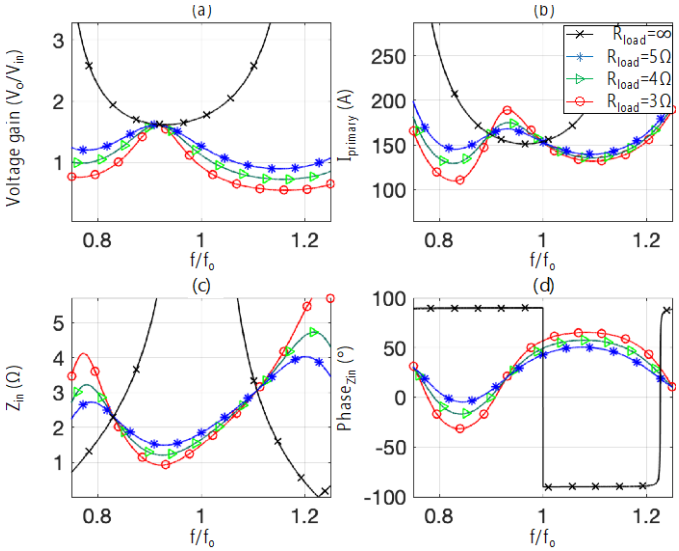


Fig. 12. Predicted behaviors of the LCC-series compensation network topology with variable load resistance with fixed $k = 0.44$: (a) voltage gain, (b) primary-side coil current, (c) input impedance, (d) phase of input impedance.

V. Conclusions

A severity analysis of high-power fast-charging wireless power transfer system modules with a series-series compensation network is conducted. Potential losses and damages in the worst case when the control of the charging stations and the vehicle-side BMSs is taken by attackers are investigated in this paper. Among many potential scenarios, two representative scenarios have been mainly discussed: DC and AC short-circuit conditions by an infected controller and faulty operation by manipulating request from the battery management system. The analysis is based on parameters of the implemented 100 kW WPT system module for extreme fast charging. Both theoretical approaches and simulation results of the module demonstrate that the fault energy losses are considerably high that the resulted damage can burn out the main components in charging stations and vehicles. Those scenarios should be considered in advance in the hardware design stage to absolutely eliminate the possibility of the worst cases.

References

[1] D. Goodin, "Hackers Trigger yet Another Power Outage in Ukraine," ArsTechnica, 2017.

[2] "Enabling Fast Charging: A Technology Gap Assessment," U.S. Department of Energy, October 2017.

[3] A. Bindra, "Securing the Power Grid: Protecting Smart Grids and Connected Power Systems from Cyberattacks," IEEE Power Electronics Magazine, pp. 20-27, September 2017.

[4] R. Deng, G. Xiao and R. Lu, "Defending Against False Data Injection Attacks on Power System State Estimation," IEEE Transactions on Industrial Informatics, vol. 13, no. 1, pp. 198-207, 2017.

[5] G. Guez, "Why Hardware-Based Design Security is Essential for Every Application," Maxim Integrated Products, White Paper, 2017.

[6] V. Galigekere, J. Pries, O. Onar, G.-j. Su, S. Anwar, R. Wiles, L. Seiber and J. Wilkins, "Design and Implementation of an Optimized 100 kW Stationary Wireless Charging System for EV Battery Recharging," in

2018 IEEE Energy Conversion Congress and Exposition (ECCE), Portland, OR, 2018.

[7] J. Pries, V. Galigekere, O. Onar, G.-J. Su, R. Wiles, L. Seiber, J. Wilkins, S. Anwar and S. Zou, "Coil Power Density Optimization and Trade-off Study for a 100kW Electric Vehicle IPT Wireless Charging System," in 2018 IEEE Energy Conversion Congress and Exposition (ECCE), Portland, OR, December 2018.

[8] P. Reigosa, F. Iannuzzo, H. Luo and F. Blaabjerg, "A Short-Circuit Safe Operation Area Identification Criterion for SiC MOSFET Power Modules," IEEE Transactions on Industry Applications, vol. 53, no. 3, pp. 2880-2887, May/June 2017.

[9] L. Ceccarelli, P. Reigosa, F. Iannuzzo, F. Blaabjerg, "A survey of SiC Power MOSFETs Short-Circuit Robustness and Failure Mode Analysis," Microelectronics Reliability, Elsevier, vol. 76-77, pp. 272-276, July 2017.

[10] C. Chen, D. Labrousse, S. Lefebvre, M. Petit, C. Buttay and H. Morel, "Study of Short-circuit Robustness of SiC MOSFETs, Analysis of the Failure Modes and Comparison with BJTs," Microelectronics Reliability, Elsevier, vol. 55, no. 9-10, pp. 1708-1713, August 2015.

[11] L. Gant, G. Sheh and X. Zhang, "All about circuits," 16 July 2018. [Online]. Available: https://www.allaboutcircuits.com/industry-articles/evaluating-the-robustness-of-1200v-sic-mosfets-under-short-circuit-conditio/. [Accessed 2 April 2019].

[12] J. M. Miller, "Wireless Plug-in Electric Vehicle (PEV) Charging," Invited presentation for 2012 U.S. DOE Hydrogen and Fuel Cells Program and Vehicle Technologies Program Annual Merit Review and Peer Evaluation Meeting, Oak Ridge National Laboratory, 15 May 2012.

[13] S. Zou, O. Onar, V. Galigekere, J. Pries, G.-j. Su and A. Khaligh, "Secondary Active Rectifier Control Scheme for a Wireless Power Transfer System with Double-Sided LCC Compensation Topology," in IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, Washington DC, 2018.

[14] V. Galigekere, O. Onar, J. Pries, S. Zou, Z. Wang and M. Chinthavali, "Sensitivity Analysis of Primary-Side LCC and Secondary-Side Series Compensated Wireless Charging System," in 2018 IEEE Transportation Electrification Conference and Expo (ITEC), Long Beach, CA, 2018.