









Port Impedance Measurement and Current Injection Response Analysis for PLCs

Wei Qiu , Member, IEEE, Liang Zhang , He Yin , Senior Member, IEEE, Kaiqi Sun , Member, IEEE, Lawrence C. Markel , Member, IEEE, DaHan Liao , Member, IEEE, Zhi Li , Member, IEEE, Ben W. McConnell, Senior Member, IEEE, and Yilu Liu , Fellow, IEEE

Abstract—Programmable logic controllers (PLCs) are used to control devices throughout the power system since they have fast control capabilities and can utilize multiple types of communication interfaces. Therefore, studying and mitigating their vulnerabilities to electromagnetic pulse is important for the reliability of PLC operations. In this article, an effective impedance measurement scheme is proposed and demonstrated for three PLCs to estimate their susceptibility to an electromagnetic pulse. The equivalent nonuniform transmission line model is established to eliminate the impact of the fixture in the de-embedding process. Then, different parameters of the impedance measurement setup are explored. Based on the measured impedance, the equivalent circuit is established to calculate the response of the device when subjected to the electromagnetic pulse. The voltage and current responses of different interfaces are compared utilizing the developed pulsed current injection (CI) method. Finally, the impedance measurement scheme is verified through testing using three measuring instruments. And the CI simulation experiments reveal the characteristics and susceptibilities of different PLCs interfaces, indicating that some protection measures are required for the reliable operation of the PLC.

Index Terms—Electromagnetic pulse, impedance measurement, nonuniform transmission line, programmable logic controllers (PLCs), pulsed current injection (CI).

I. INTRODUCTION

THE normal operation of the power system requires the stable performance of key controllers and detectors.

Manuscript received 5 March 2022; revised 31 May 2022; accepted 2 August 2022. Date of publication 10 August 2022; date of current version 21 November 2022. Paper 2022-IACC-0277.R1, presented at the 2021 IEEE Industry Applications Society Annual Meeting (IAS), Vancouver, BC, Canada, Oct. 10–14, and approved for publication in IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS by the Industrial Automation and Control Committee of the IEEE Industry Applications Society. This work was supported in part by the DOE Grid Modernization Lab Call (GMLC) Project: Vulnerability of Power Generation Critical Systems Against Electromagnetic Threats under Grant 36129, and also in part by CURENT Industry Partnership Program. (Corresponding author: Liang Zhang.)

Wei Qiu, Liang Zhang, He Yin, and Kaiqi Sun are with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996 USA (e-mail: qwei4@utk.edu; liangzhangswpu@gmail.com; hyin8@utk.edu; ksun8@utk.edu).

Lawrence C. Markel, DaHan Liao, Zhi Li, and Ben W. McConnell are with the Oak Ridge National Laboratory, Oak Ridge, TN 37831 USA (e-mail: markellc@ornl.gov; liaod@ornl.gov; liz2@ornl.gov; bwmccconnell@me.com).

Yilu Liu is with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996 USA, and also with the Oak Ridge National Laboratory, Oak Ridge, TN 37831 USA (e-mail: liu@utk.edu).

Color versions of one or more figures in this article are available at <https://doi.org/10.1109/TIA.2022.3198039>.

Digital Object Identifier 10.1109/TIA.2022.3198039

Extreme conditions and events may challenge the reliability of the power system. Extreme electromagnetic pulses, especially high-altitude electromagnetic pulse (HEMP), pose a potential threat to the power system measurement, monitoring, and control [1], [2]. In addition to direct exposure, the electromagnetic pulse can couple to cables and antennas, and then, propagate to equipment [3]; thus critical equipment of the power system must take the threat of electromagnetic pulse into consideration [4].

Programmable logic controllers (PLCs) are a base for power system control, with varied applications such as microhydroelectric systems [5], wide area measurement system, and supervisory control and data acquisition system [6], [7], [8]. The advantages of PLCs are that they usually have enhanced network capabilities for data transmission and a high-speed counter for real-time control [9]. The reliability of PLCs depends on successful real-time delivery of control commands, the reception of status, etc. The transient voltage or current caused by HEMP may damage the input circuits, solid-state (transistor), and relay of the PLCs. However, research on the impact of HEMP on PLCs has not been comprehensive.

For example, in 2008 [10] and 2010 [2], the electromagnetic pulse attack is injected into PLCs and found the vulnerabilities of some components. However, high test costs make it difficult to test all the ports of the PLCs. The objective of this article is to measure the impedance of PLCs, and then, study the influence of HEMP on PLCs based on HEMP modeling. To this end, analysis of HEMP influence can be divided into two steps: the impedance test and immunity analysis under HEMP.

Impedance calculation directly affects the accuracy of the modeled HEMP response. The LCR meter is a commonly used impedance measurement device that can directly measure inductance (L), capacitance (C), resistance (R), and impedance. However, the frequency range is usually limited, which leads to incomplete measurement [11]. To solve this problem, an indirect measurement method is introduced in [12], where the impedance can be inferred from the S parameter. And in [13], four different types of measurement instruments are investigated by comparing their measurement results. The advantage of this method is that a model valid over a wider frequency range can be achieved.

The measured impedance usually contains the impedance component of the fixture, so the influence of the fixture needs to be removed. A de-embedding technology used in the field of IC design is proposed [14]. However, it requires symmetrical transmission line test structures, which limits its application.

Therefore, an S-parameter measurement-based method is proposed to perform accurate de-embedding up to 110 GHz [15]. Nevertheless, it is difficult to apply this method to some self-made fixtures due to the differences in size and material. Thereby, a flexible de-embedding solution is necessary for the PLC-based impedance measurement.

Although the electromagnetic environment simulator (EMES) is an effective way to generate the real electromagnetic environment. For example, the Sandia National Laboratory has developed the EMES to test the EMP effects on the photovoltaic system in [16]. However, the experimental equipment requires great economic cost, which limits its application. Based on the measured impedance of the load, the simulation methods based on PSCAD/EMTDC and MATLAB software provide another low-cost and convenient solution. In [17], a 2.1-MW wind farm, energy storage system, and load are simulated by PSCAD/EMTDC software to analyze its lightning transient effects.

Besides, some equivalent charging and discharging circuits can be used to simulate the effects of HEMP. One of the most common methods is pulse current injection (CI). The pulsed CI is a cost-effective method to test the vulnerability of PLC under HEMP. According to IEC 61000-4-25 [18], the simplified circuit diagram of the generator is provided. The electrical fast transient/burst can then be simulated in the pulsed CI testing. Actual experiments of fast electromagnetic disturbance are conducted based on the pulsed CI in wire pairs and antenna systems [19], [20]. The experiments have verified that the pulsed CI method is an effective analysis method for modeling the effects of electromagnetic pulses. Given the critical role of PLC in the SCADA, it is challenging to develop a rapid analysis method to verify its vulnerability under EMP.

To explore the influence of HEMP on PLCs, a PLC-based impedance measurement scheme and current injection response are proposed. Moreover, the vulnerabilities of the other key devices in the power system can also be analyzed using the proposed methods. The immunity levels of different components can be tested so that the corresponding protective measures can be taken [21]. Besides, this method can provide a rapid analysis way to verify the vulnerability of different devices to avoid establishing a high-cost experimental site.

And this article is an extension of the IAS conference paper in [22]. This article has improved the conference versions in the following parts: the sensitivity analysis of the measurement parameters as well as more literature reviews are added. Additionally, more PLCs and two types of immunity test levers are selected to enrich the results. The contributions of this article are summarized as follows.

- 1) An impedance measurement scheme is proposed for the impedance measurement based on three different measuring instruments. The measured data are integrated using interpolation and data averaging.
- 2) To eliminate the impact of the fixture, the nonuniform transmission line model is established in the de-embedding process. A seven-stage model is used to approximate the impedance of the fixture.
- 3) A pulse current injection method is proposed to simulate the response to electrical fast transient caused by HEMP.

TABLE I
FEATURES OF THREE IMPEDANCE MEASURING INSTRUMENTS

	LCR meter	Imp. Analyzer	VNA
Name	MCR-5200	HP 4395A	Planar TR1300/1
Adapter	-	HP 87512A	N1.1 Calibration Kit
Freq. range	40Hz-200kHz	10Hz-500MHz	300kHz-1.3GHz
Imp. range	0.1mΩ – 99.99MΩ	< 40kΩ	-
Accuracy	> 0.1%	3%-10%	0.5%-3%

To simulate the fragility of PLCs under two immunity test levers, where the EC5 and EC8 levels are selected from IEC 61000-4-25.

- 4) Different experiments based on three different PLCs are conducted to verify the effectiveness of the impedance measurement scheme and pulsed CI method. The results demonstrate that the impedance measurement results are consistent, and some protection measures can be taken to mitigate the effects of HEMP.

The rest of this article is organized as follows. Section II introduces the impedance measurement devices. De-embedding and data integration of impedance measurement results is presented in Section III. The CI method is introduced in Section IV. Different experiments are conducted in Section V. Finally, Section VI concludes this article.

II. PLC-BASED IMPEDANCE MEASUREMENT

To achieve the CI response of PLC, the tested impedance and phase can be obtained to establish the simulation circuit. Once the measurements are ready, the induced voltage and current of the PLCs to EMP can be calculated based on the electromagnetic theory. Considering that the electromagnetic pulses can occur in the electric or magnetic field of different strengths in different directions, they typically comprise a wide frequency range from a low value (hertz level) to a high value (gigahertz level). The impedance measurement devices should have a wide measurement interval. However, most measuring instruments can only provide a specific range of values. Therefore, three instruments are used together to obtain the actual impedance results for different frequency ranges.

The evaluation of these three instruments is listed in Fig. 1 and Table I. As can be seen from Table I, both the LCR meter and impedance analyzer can directly test the impedance. Based on the data-sheet of the tested devices, for the LCR meter, the accuracy of measurement up to 200 kHz is lower than 1% when the measured impedance is lower than 1 MΩ. For the TR1300/1, its accuracy is lower than 3% when the measured impedance is lower than 100 kΩ. And the HP 4395 A can provide 3% accuracy up to 100 MHz if the impedance is lower than 1 kΩ. Overall, 3% accuracy can be ensured for the higher frequency components. The vector network analyzers (VNAs) can test the reflection coefficient S_{11} using one-port measurement, then the impedance can be calculated from S_{11} based on the following equation [23]:

$$z_{\text{eff}} = \sqrt{\frac{(1 + S_{11})^2 - S_{21}^2}{(1 - S_{11})^2 - S_{21}^2}} \quad (1)$$

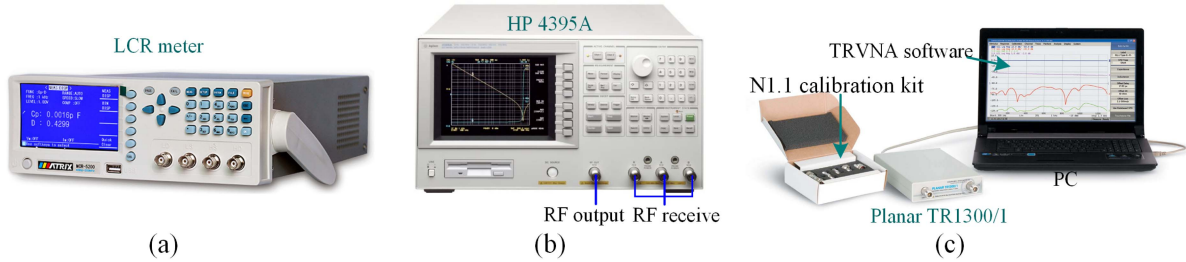


Fig. 1. Three impedance measurement instruments. (a) LCR meter: MCR-5200. (b) Impedance Analyzer: HP 4395 A. (c) VNA: Planar TR1300/1.

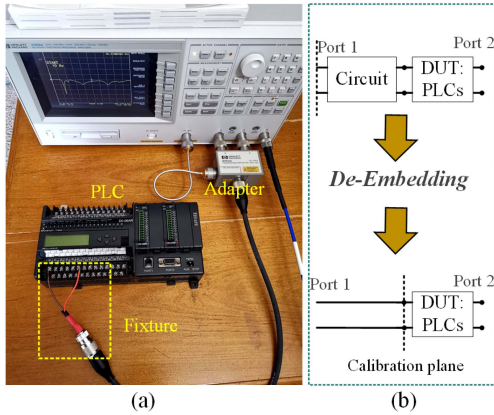


Fig. 2. Impedance measurement using the HP 4395 A. (a) Test platform. (b) De-embedding.

where S_{21} is the forward voltage gain, S_{21} can be safely set to zero if only one port is used in the VNA.

The impedance measurement test unit is shown in Fig. 1. For the LCR meter, the measurement value is based on the discrete data points, of which a total of 41 frequency points can be obtained from 40 Hz to 200 kHz. The impedance analyzer and VNA instruments have more measurement points, which can reach 805 and 16 001 points, respectively. This means that these instruments have a higher resolution compared to the LCR meter.

During the measurement process, two main parameters will affect the test results: the intermediate frequency (IF) bandwidth and the power level of the output signal. The IF bandwidth can affect resolution and detection speed, where a lower value means a higher resolution but a lower speed. The power level of the output signal would determine the measured impedance value, especially for some sensitive components. For example, high voltage may conduct current and reduce the impedance value for photodiodes. Therefore, a relatively low and stable voltage helps to obtain consistent detection results for PLCs.

An actual test setup is shown in Fig. 2. As shown in Fig. 2(a), the fixture is used to connect the PLC and RF line. The measurement results contain the impedance from both PLC and fixture. Therefore, the de-embedding process is necessary to remove the influence of the fixture.

III. DE-EMBEDDING FOR THE RAW MEASURING VALUES

To obtain the actual impedance of PLCs, the commonly used methods are the open-short and short-open de-embedding

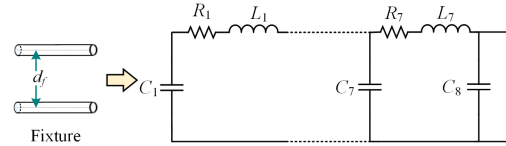


Fig. 3. Nonuniform transmission line model for de-embedding based on fixture.

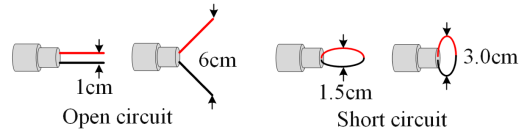


Fig. 4. Distance example of the fixture for open and short circuits.

methods [15]. It has an effective effect in the low-frequency part. However, it should be noted that the wires between the ground and signal also have resistance and inductance in the short pattern, leading to bias at high frequencies. In this section, a de-embedding method is established to eliminate the impact of fixtures based on the nonuniform transmission line model.

The seven-stage cascade of the transmission line model is proposed, as shown in Fig. 3, which is the equivalent circuit of the fixture. The results of lower stages, such as three or four stage, are not efficient as seven stage. Resistance, inductance, and capacitance are the three main parameters of the fixture. To obtain these parameters, the total parallel capacitance and serial inductance are estimated using the open and short methods based on the measured impedance. Usually, a small distance between two wires means smaller inductance and larger capacitance.

Seven different distances d_f are tested using the open method. The total capacitance can be calculated using $C_t = -1/(2\pi f X_c)$, where the f and X_c are the frequency (Hz) and the capacitive reactance (Ω), respectively. Similarly, the total serial inductance can be calculated as $L_t = X_l/(2\pi f)$ based on the short method, where X_l is the inductive reactance.

The distance of the short circuit cannot be adjusted flexibly limited by the lines, as shown in Fig. 4. It should be noted that the maximum $d_f = 3.0$ cm for short measurement. Considering that the distance can be adjusted flexibly from 1 to 9 cm when the lines are open for the fixture, as shown in Fig. 4, this means that more d_f values are measured first for C_t measurement.

The C_t and L_t with distances $d_f \in \{1 \text{ cm} - 9 \text{ cm}\}$ are tested and calculated, as shown in Fig. 5. As depicted in Fig. 5(a), the capacitance is changing with the distance between two wires.

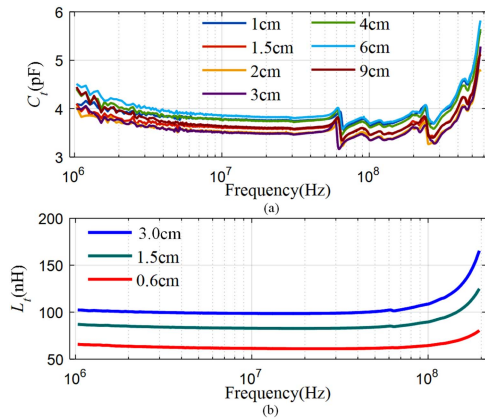


Fig. 5. Calculated total capacitance and inductance C_t and L_t in different d_f . (a) C_t . (b) L_t .

TABLE II
DISTRIBUTION OF CAPACITORS AND INDUCTORS IN THE SEVEN-STAGE
CASCADE OF TRANSMISSION LINE MODEL

Stage	1	2	3	4	5	6	7	8
C_n (pF)	1.8	0.7	0.5	0.25	0.15	0.1	0.09	0.07
l_n (nH)	7.4	9.5	12.3	12.3	12.3	12.3	12.3	-

The mean value can be obtained and is located from 3.48 to 3.83 pF. Considering that the distance between wires will not exceed 4 cm, an average capacitance C_t is set to 3.7 pF for the transmission line model. Meanwhile, the total serial inductance L_t is distributed in 60–100nH when f is lower than 100 MHz. The mean total serial inductance L_t is set to 80 nH. The resistance of the nonuniform transmission line model can be obtained from the short-circuit impedance.

The next step is to estimate the detailed capacitance and inductance value for each stage transmission line model. Generally, the capacitance and inductance of the transmission line model can be expressed as [24]

$$C_i = \frac{\pi \varepsilon}{\ln \frac{d_f}{2r}}$$

$$L_i = \frac{\mu_0}{4\pi} + \frac{\mu_0}{\pi} \left(\ln \frac{d_f - r}{r} \right) \quad (2)$$

where μ_0 denotes the vacuum permeability, r is the wire radius of the fixture, and ε is the relative permittivity, $i = 1, 2, \dots, 7$.

The motivation to estimate the C_i and L_i is to minimize the impedance errors between the measurement and the equivalent circuit. Based on the resonance points, the C_i and L_i are estimated, as listed in Table II. The d_f values for measuring C_t and L_t are different because the distance is different where the impedance is slightly different. To verify this difference, the calculated and measured open-circuit impedance is shown in Fig. 6 using the estimated C_t and L_t . It can be seen that there are some slight differences in the impedance and phase results under different distances, indicating the correction of the parameters.

After de-embedding is complete, the measured impedance needs to be further integrated since there are three sets of

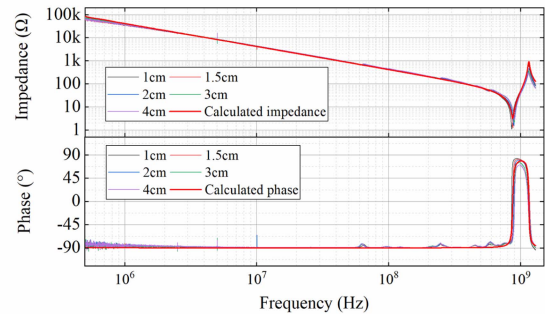


Fig. 6. Measured and calculated impedance and phase of the open circuit.

measurement results. Due to measurement errors of different instruments, the measured values at the intersection of frequencies may be different. Therefore, it is necessary to preprocess the data before the CI response analysis, which contains the following three steps.

- 1) The cubic spline interpolation is first performed on the result of the LCR meter since there are fewer measuring points.
- 2) For the area where the frequency overlaps, take the average of the measured values of the different instruments.
- 3) Perform cubic spline interpolation on the data from step 2, where the frequency is taken on a logarithmic scale to ensure the resolution at low frequencies.

A. Sensitivity Analysis of Measurement Parameters

After establishing the de-embedding model, the power level of the output signal is tested to verify the sensitivity of the parameters in this section. As described in [25], higher signal levels result in an electrical breakdown in the device under test (DUT), but also with less variability in measured values. Therefore, it is necessary to analyze the sensitivity of different test conditions.

Here, the LCR meter and VNA are used to verify the influence of the power level parameter. Different ports from the same PLC are tested, where its result is shown in Fig. 7. For Fig. 7(a), the low-frequency range (40 Hz–200 kHz) is verified on its expansion module. It should be noted that there exist some optocouplers in the expansion module. It can be seen that the power level has an impact on the tested result. An impedance value under the lower power level with 6.89 dBm is higher than $2M\Omega$. A higher power level with 13 dBm has a lower impedance, indicating that some electronic components in the circuit of the expansion module may have already started working.

In addition, the high-frequency range (300 kHz–1.3 GHz) result is shown in Fig. 7(b). It demonstrates that the impedance does not change significantly. However, if the power level is lower than 0.007 V, the results would start to fluctuate. The reason is that the low voltage causes an increase in the proportion of measurement noise.

Based on the aforementioned analysis, it is recommended to choose a fixed power level for the different instruments. Meanwhile, an intermediate voltage value (near 0.1 V and

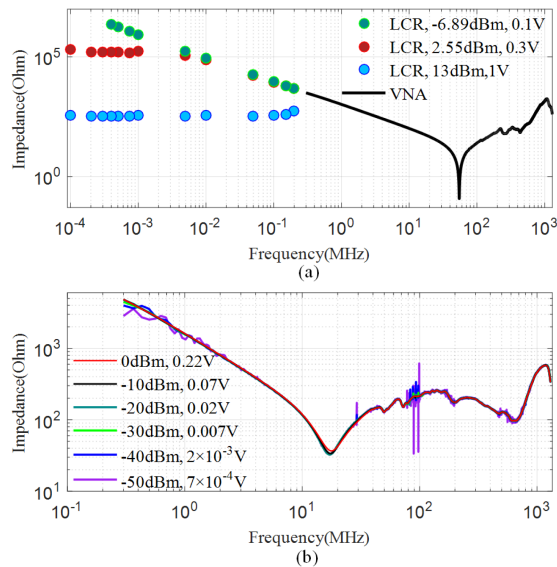


Fig. 7. Impedance. (a) Impedance for expansion module of PLC, power level of VNA is -10 dBm. (b) Impedance for communication port of PLC using the VNA.

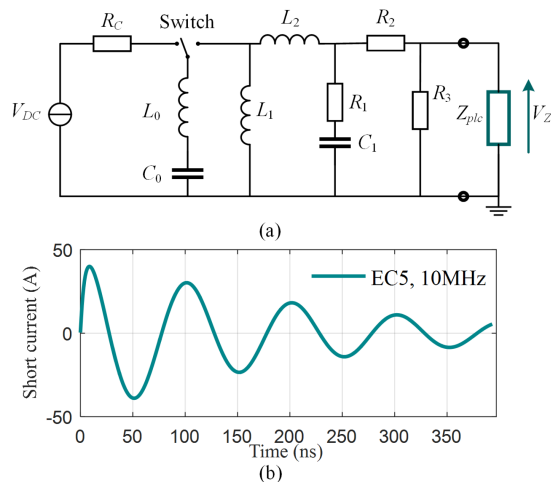


Fig. 8. Circuit diagram of pulsed CI. (a) Simplified circuit diagram of pulsed CI. (b) Pulse short current.

-0.689 dBm) is recommended to avoid starting electronic components and avoid introducing measurement noise. It should be noted that the low power level is safer to prevent components from working to get consistent results.

IV. PLC-BASED CURRENT INJECTION RESPONSE ANALYSIS

To explore the response of the PLCs under HEMP, the coupling mechanism has been proposed using the circuit network. For example, the probe is modeled as the transformer in [26]. And the current distributions are shown with reasonable accuracy. The advantages of pulsed CI are its simplicity, and it is easy of operation [27]. Therefore, the early-time (E1) HEMP coupling is emulated via the pulsed CI method.

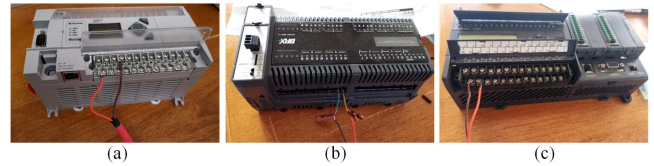


Fig. 9. Tested PLCs. (a) Allen Bradley 1766-L326BWA. (b) BX-DM1-36ER-D.

The simplified circuit diagram of pulsed CI is shown in Fig. 8. To obtain the current and voltage response of the PLC port, the pulsed CI uses two steps.

- 1) *Charging process*: It can be seen that the capacitance C_0 is charged by a high-voltage dc source when the high-voltage switch turns left. The $R_c = 100 \text{ k}\Omega$ is the series charging resistor. In an actual hardware setup, the portable generator PPG-E1-1200 / SPG-188-125-E1 can be used to generate the expected voltage.
- 2) *Discharge process*: As shown in Fig. 8(a), in this process, the high-voltage switch turns right. The capacitance C_0 is then connected to the subcircuit to discharge [28]. The L_0 and R_2 denote the matching inductance and source resistor, respectively. L_2 , R_1 , and C_1 represent the filter RLC harmonic oscillator, which is used to connect the capacitance and PLC. The L_1 denotes the oscillating circuit coil. The R_3 can be used as the voltage divider resistor, and it is optional. The short current is shown in Fig. 8(b).

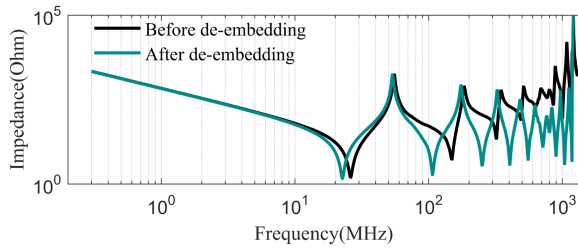
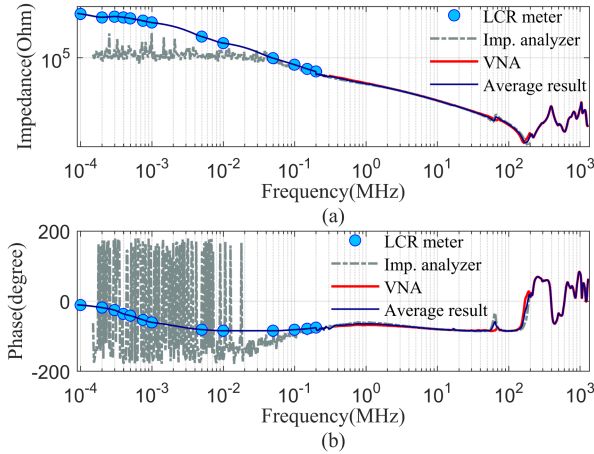
As depicted in Fig. 8(b), the damped oscillatory wave (40 A, EC5) is selected, where a 10-MHz frequency is used based on the definition in [18]. The circuit parameters of Fig. 8(a) are set to $C_0 = 1.5 \text{ nF}$, $L_0 = 50 \text{ nH}$, $L_1 = 120 \text{ nH}$, $L_2 = 200 \text{ nH}$, $R_1 = 1000\Omega$, $C_1 = 50 \text{ pF}$, $R_2 = 80\Omega$, and $R_3 = 100\Omega$. Based on the calculation method in [29], the V_Z and current can be calculated.

V. EXPERIMENTS

To verify the current and voltage response of PLCs under HEMP, three PLCs are used, including the Allen Bradley 1766-L326BWA (PLC₁), the BX-DM1-36ER-D (PLC₂), and Automation-direct DL06 Micro (PLC₃), as shown in Fig. 9. These PLCs contain multiple communication ports and I/O modules, and can be used for power system control and general industrial machinery applications. To obtain accurate and consistent results, the IF bandwidths are set to 30 Hz, and 20 kHz for HP 4395 A and TR1300/1. The power level of the output signal is set to 0.1 V (-6.89 dBm) for all the instruments. All instruments are warmed up for one hour before measurement. During the test, the rest of the ports are always left open.

A. Data Integration Verification

To verify the validity of the de-embedding process and data integration, the results before and after the de-embedding are presented, as shown in Fig. 10. It shows that the low-frequency


 Fig. 10. Impedance before and after de-embedding for PLC₁.

 Fig. 11. Integrated impedance of three measuring instruments for network interface TXD-RXD from PLC₃. (a) Impedance result. (b) Phase result.

component results are consistent, and the high-frequency component is calibrated.

The integrated impedance of three measuring instruments is depicted in Fig. 11. It shows that the measured impedance value of the LCR meter is higher than the impedance analyzer when the frequency is lower than 100 kHz. This reason is that the impedance has exceeded the maximum range of the instrument. Therefore, the LCR meter is treated as the benchmark when the impedance is higher than $2 \times 10^4 \Omega$. Meanwhile, for the frequency range between 300 kHz and 500 MHz, the impedance and phase calculation results agree with each other for the impedance analyzer and VNA. Moreover, the tested value of the LCR meter is consistent with the other two instruments when f is near 200 kHz, which evidences that the results are accurate. Overall, it shows that the average result can effectively smooth three sets of measurement data, indicating the effectiveness of interpolation and data integration.

B. Impedance Comparison of PLCs

In this section, the impedance of three PLCs is tested and compared. Considering that PLCs have many interfaces, one interface from general Input/Output (I/O), the power supply port, and the RXD-TXD port from RS232 communication are selected for analysis, as shown in Fig. 12.

Fig. 12 shows that the impedance of different PLCs interfaces is also different. In Fig. 12(a), there is a significant difference

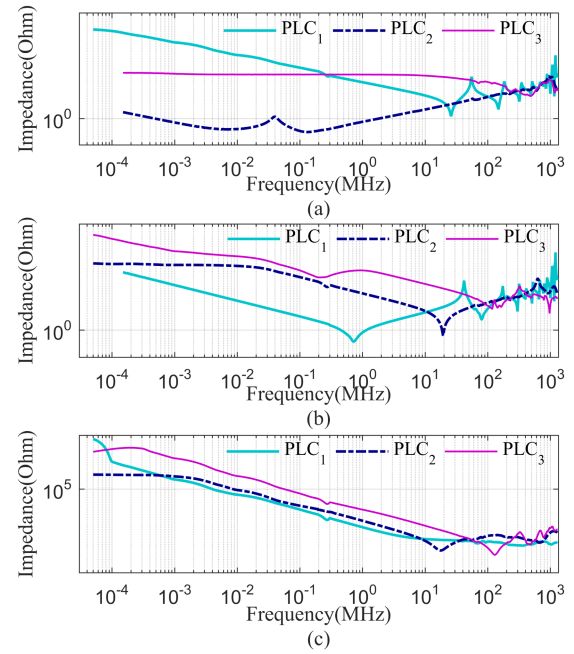


Fig. 12. Impedance results of three PLCs. (a) Impedance result of general I/O. (b) Impedance result of power supply port. (c) Impedance result of the RXD-TXD port from RS232.

among all the PLCs. This is because the circuit design structure and electronic components are different. The maximum impedance can reach $8.9 \times 10^6 \Omega$ for PLC₁ at 50 Hz, and the minimum impedance is about 0.09Ω for PLC₂ at 0.1 MHz. As for the power supply port, Fig. 12(b) shows that the impedance is smoother at low frequencies and has large fluctuations at high frequencies. In Fig. 12(c), the results from different PLCs have similar trends and close impedance values, where the impedance decreases as the frequency increases. This means that a similar circuit is designed for the same communication module.

Under the influence of an electrical fast transient, the multiple impedance results of different interfaces imply that the ability to withstand electromagnetic pulses is not static.

C. Result of Current Injection Response Under EC5

In IEC 61000-4-18 and IEC 61000-4-25 [18], [28], the immunity test levels range from EC1 to EC11, which can be classified into damped sinusoids (EC1-EC6) and double exponential (EC8-EC11) waveforms. To analyze current and voltage response under the HEMP, two immunity test levels are used to verify the vulnerability of PLCs including EC5 and EC8, considering that the PLCs may be installed inside or outside the box.

In this test, the damped sinusoidal current signal is tested on three pairs of ports under EC5, where the voltage and current are 2000 V and 40 A, respectively. The oscillation and damping parameters of the wave are set to 10 MHz and 10, respectively. The voltage and current results are shown in Figs. 13 and 14.

It can be seen from Fig. 13(a) that the maximum voltage value of the general I/O port is higher than 1000 V for PLC₁. And 500 V is obtained for PLC₂. HEMP has two potential

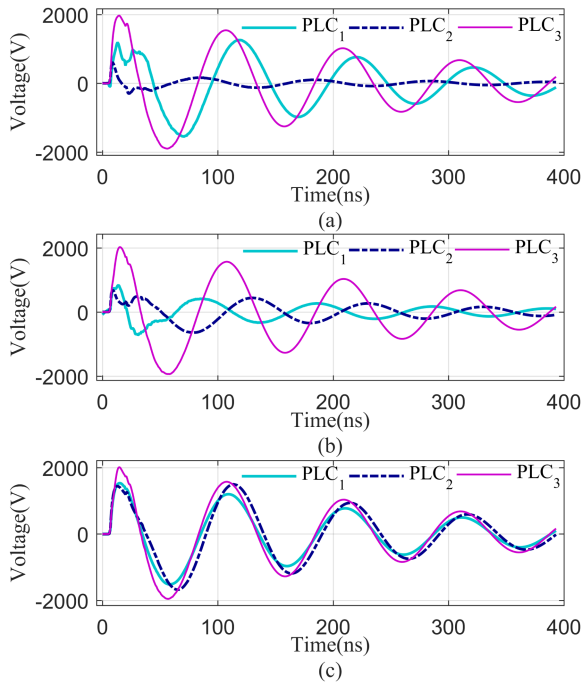


Fig. 13. Voltage response of three PLCs. (a) Voltage result of general I/O. (b) Voltage result of the power supply port. (c) Voltage result of the RXD-TXD port from RS232.

effects on PLCs, including upset and direct destruction. The upset means PLCs disruption since some ports may have the input overvoltage protection function. In this state, the manual intervention may be required to resume the PLCs' operation. According to the manual of PLCs [30], the I/O and power supply ports of PLC₁ can tolerate a voltage of 2 kV under the electronic fast transient. And the communication cable (RS-232 and RS-485) can tolerate a voltage of 1 kV. Therefore, the I/O and power supply ports of PLC₁ would survive under the EC5 level attack of HEMP. However, the voltage surge has exceeded the damage threshold of RS232, so the failure would occur for the interfaces of PLC under the EC5 level. According to the current results in Fig. 14(a), near 40-A current is reached and it would exceed the inrush current of 40 A (lasting for 4 ms) for PLC₁ if a higher test level is selected. Similar conclusions can be inferred based on the manual and experimental results for the rest of the PLCs.

Meanwhile, it can be derived from Fig. 13(c) that the voltage of the RXD-TXD port is similar for these three PLCs. The main reason is that they have the same level of impedance according to Fig. 12(c). However, the current result from Fig. 14(c) shows that the peak occurs at a different time due to the different phase angle. Fig. 14 demonstrates that there are some differences in current between different ports for the same PLC. For example, about 40-, 32-, and 10-A currents are generated for different interfaces of PLC₂ since the impedance is diverse.

For PLC₃, all the voltage and current levels are about 2000 V and less than 10 A, respectively. One reason is that the impedance of PLC₃ is higher than the other two PLCs, especially in the high frequency, which will get more voltage according to the Kirchhoff circuit laws. Based on its user manual, the metal

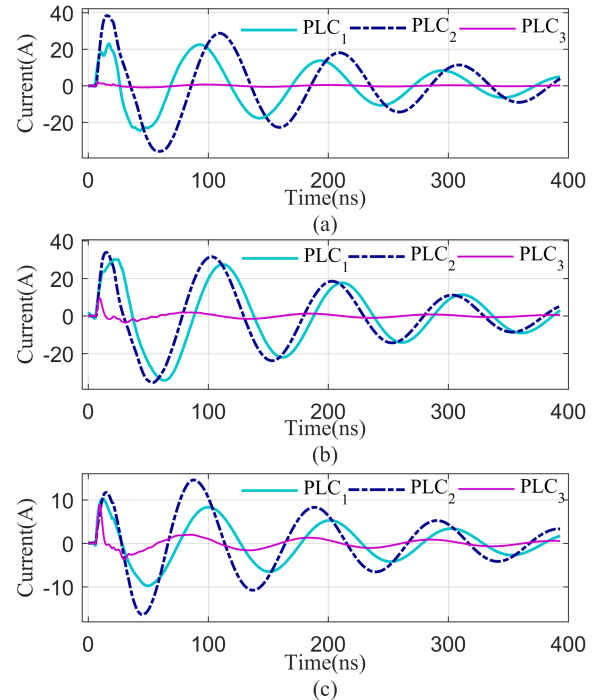


Fig. 14. Current response of three PLCs. (a) Current result of general I/O. (b) Current result of the power supply port. (c) Current result of the RXD-TXD port from RS232.

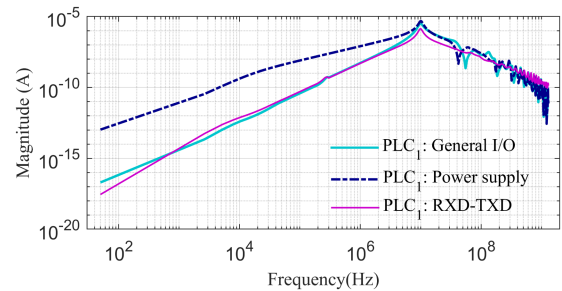


Fig. 15. Current spectrum of PLC₁ for different ports.

oxide varistors (MOV) or transient voltage suppression (TVS) diodes are recommended to be connected for best surge transient protection. However, the MOV and TVS also may not tolerate the transients when it has a higher level.

Besides, Fig. 14 shows that the voltage and current waveforms of PLC₁ do not have the smooth damped oscillation. The primary reason is caused by the difference in the frequency components. Fig. 15 shows the current spectrum of PLC₁ for different ports. It shows that there are oscillations near 10 MHz and a peak exists at 55.3 MHz. This means high-frequency oscillations exist in the current. In the time-domain waveform, it shows ups and downs between 0 and 50 ns. High-frequency components attenuate fast over time, so the curve return to smooth after 50 ns.

D. Result of Current Injection Response Under EC8

The key equipment of the power system is expected to resist HEMP with different strengths. In this section, the pulsed CI response under EC8 is also presented. Considering that most

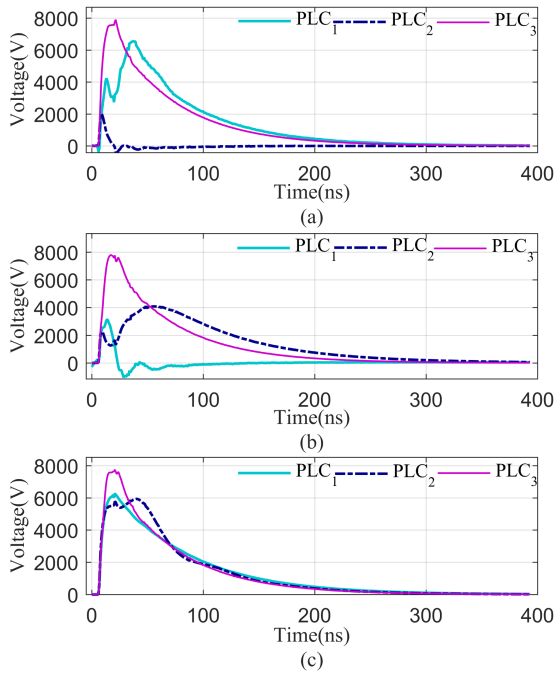


Fig. 16. Voltage response of three PLCs. (a) Voltage result of general I/O. (b) Voltage result of power supply port. (c) Voltage result of RXD-TXD port from RS232.

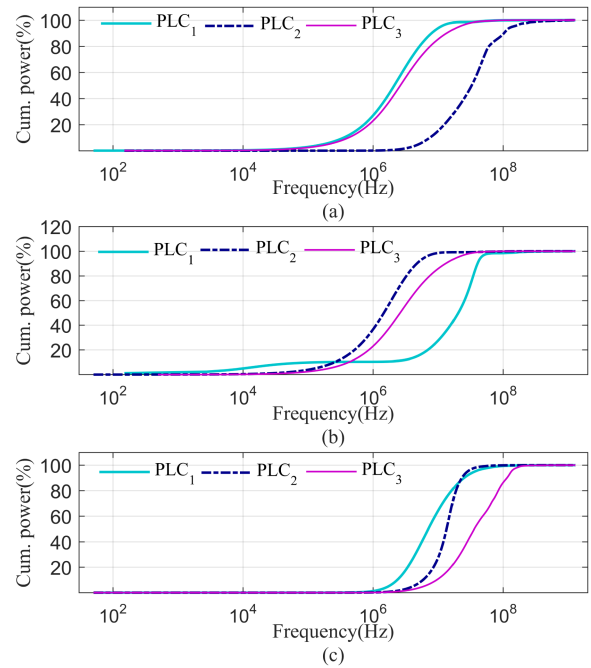


Fig. 18. Cumulative power of pulsed CI tests. (a) Cumulative power of general I/O. (b) Cumulative power of power supply port. (c) Cumulative power of the RXD-TXD port from RS232.

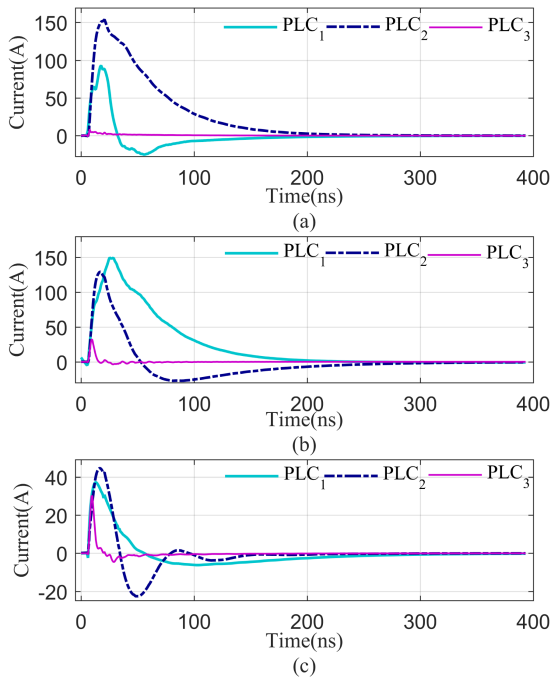


Fig. 17. Current response of three PLCs. (a) Current result of general I/O. (b) Current result of power supply port. (c) Current result of the RXD-TXD port from RS232.

of the ports may survive in the EC5, a higher immunity level is selected to verify its vulnerability. Instead of the damped sinusoidal current, the immunity test level EC8 uses the transient current, where the voltage and current are 8000 V and 160 A, respectively. The voltage and current results are shown in Figs. 16 and 17.

Fig. 16 shows the voltage response of three PLCs. It can be seen that voltage waveforms are quite different even for the same kind of ports. As can be seen from the general I/O ports in Fig. 16(a), voltage waveforms of PLC₁ and PLC₃ have high peak values and large pulsewidth. However, the peak value of PLC₂ is only 2 kV which is much smaller than PLC₁ and PLC₃. The pulsewidth of PLC₂ is also smaller because it disappears quickly. For power supply ports, peak value of voltage is 3.2, 4.1, and 7.8 kV for PLC₁, PLC₂, and PLC₃, respectively. Besides, the shapes of voltage waveforms are quite different. Pulse of PLC₁ is narrow and that of PLC₂ is much wider. For RXD-TXD ports from RS232, the difference in the waveforms is small compared with the other two kinds of ports. They have large peak values and pulsewidth. Overall, general I/O and RXD-TXD ports of PLC₁ can be damaged since only 2-kV voltage can be tolerated. Compared with EC5, the voltage of PLC₃ is always higher than that PLC₁ and PLC₂, indicating that the PLC₃ can be easier damaged in the same HEMP environment. This result also means that the EC8 poses a higher threat to the PLCs than that of EC5.

Fig. 17 shows the current response of three PLCs. It can be seen that the current waveforms are also quite different for the same kind of ports. Peak values in the current of PLC₃ are much smaller than those of PLC₁ and PLC₂. Besides, the peak value tends to be small when the peak value of voltage response is large for the general I/O port and power supply port.

Actually, voltage and current response are decided by impedance in a specific frequency range. The frequency range can be analyzed by the accumulated power of the response, as shown in Fig. 18. Averagely, 90% of the power locates in the frequency range of 1–30 MHz. For PLC₃, the weighted value of impedance in this frequency range is more than 1000Ω. Thus,

the amplitude of voltage in Fig. 16 is always close to 8000 V. For PLC₁ and PLC₂, the weighted value of impedance is between 10Ω and 200Ω, resulting in voltage amplitude of 3.2–6.6 kV.

To mitigate the potential effects of HEMP, some measures can be considered to improve the reliability of PLCs [31]. The first one is to add an enclosure constructed of sheet steel or conductive concrete for PLCs to suppress the strength of HEMP. The helical copper tape shielded cables provide stable performance for the control and signal cables. The second measure is to add some typical low-voltage surge protection devices, input choke, flyback diodes, and line filters to protect the devices.

VI. CONCLUSION

To explore the vulnerability and reliability of PLCs in power systems under HEMP, this article proposes an impedance measurement scheme with parameters derived by using three instruments. The sensitivity analysis results reveal the relationship between the impedance and different power levels. Then, the nonuniform transmission line model is established to eliminate the effects of the fixture. The results from the three instruments agree with each other for the measured impedance data. The impedance results also demonstrate that there are some differences in the impedance of different ports in PLCs. According to the standard signal EC5 and EC8 in IEC 61000-2-18, the pulsed CI method is further proposed and conducted to estimate the voltage and current response of PLCs, where the simulation results reveal that some key ports of the PLC can be damaged if there is no extra protective measure.

REFERENCES

- [1] S. Hyun et al., "Analysis of shielding effectiveness of reinforced concrete against high-altitude electromagnetic pulse," *IEEE Trans. Electromagn. Compat.*, vol. 56, no. 6, pp. 1488–1496, Dec. 2014.
- [2] E. Savage et al., "The early-time (E1) high-altitude electromagnetic pulse (HEMP) and its impact on the U. S. power grid," *Metatech Corporation*, Goleta, CA, USA, Tech. Rep. Meta-R-320, 2010.
- [3] R. G. Olsen and A. G. Tarditi, "EMP coupling to a straight conductor above ground: Transmission line formulation based on electromagnetic reciprocity," *IEEE Trans. Electromagn. Compat.*, vol. 61, no. 3, pp. 919–927, Jun. 2019.
- [4] L. Zhang, C. He, R. Guo, W. Yuan, and J. Li, "Research on effectiveness of lightning impulses with different parameters for detecting protrusion defects in GIS," *IEEE Trans. Dielectr. Electr. Insul.*, vol. 27, no. 4, pp. 1354–1362, Aug. 2020.
- [5] M. Kaban, D. Tamir, and P. Singh, "Electrical load controller for rural micro-hydroelectric systems using a programmable logic controller," in *Proc. IEEE Canada Int. Humanitarian Technol. Conf.*, 2015, pp. 1–4.
- [6] W. Qiu, Q. Tang, K. Zhu, W. Yao, J. Ma, and Y. Liu, "Cyber spoofing detection for grid distributed synchrophasor using dynamic dual-kernel SVM," *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 2732–2735, May 2021.
- [7] Wei-Jen Lee et al., "Development of a real time power system dynamic performance monitoring system," in *Proc. IAS Ind. Commercial Power Syst. Tech. Conf.*, 1996, pp. 161–166.
- [8] W. Qiu, Q. Tang, K. Zhu, W. Wang, Y. Liu, and W. Yao, "Detection of synchrophasor false data injection attack using feature interactive network," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 659–670, Jan. 2021.
- [9] J. C. Lorenzana-Gerardo, J. L. Díaz-Reséndiz, and E. A. Rivas-Araiza, "IoT based robust electrical energy monitoring system with programmable logic controller," in *Proc. IEEE Int. Conf. Automat./23rd Congr. Chilean Assoc. Autom. Control*, 2018, pp. 1–6.
- [10] J. John and S. Foster, "Report of the commission to assess the threat to the United States from electromagnetic pulse (EMP) attack?" 2008. [Online]. Available: http://www.empcommission.org/docs/empc_exec_rpt.pdf
- [11] R. Malarić et al., "Method for nonlinear fitting and impedance analysis with LCR meter," in *Proc. 23rd Int. Conf. Mixed Des. Integr. Circuits Syst.*, 2016, pp. 410–414.
- [12] X. Qing and Z. N. Chen, "Comments on 'comments on 'measuring the impedance of balanced antennas by an s-parameter method''," *IEEE Antennas Propag. Mag.*, vol. 52, no. 1, pp. 171–172, Feb. 2010.
- [13] M. Horibe, "Performance comparisons between impedance analyzers and vector network analyzers for impedance measurement below 100 MHz frequency," in *Proc. 89th ARFTG Microw. Meas. Conf.*, 2017, pp. 1–4.
- [14] A. M. Mangan, S. P. Voinigescu, Ming-Ta Yang, and M. Tazlauanu, "De-embedding transmission line measurements for accurate modeling of IC designs," *IEEE Trans. Electron Devices*, vol. 53, no. 2, pp. 235–241, Feb. 2006.
- [15] H. Ito and K. Masuy, "A simple through-only de-embedding method for on-wafer S-parameter measurements up to 110 GHz," in *Proc. IEEE MTT-S Int. Microw. Symp. Dig.*, 2008, pp. 383–386.
- [16] T. Bowman and J. D. Flicker, "High altitude electromagnetic pulse testing of photovoltaic modules," Sandia National Lab., Albuquerque, NM, USA, Tech. Rep. SAN D2020–3824, 2020.
- [17] Z. Mohammed, H. Hizam, and C. Gomes, "Analysis of lightning transient effects on hybrid renewable energy sources," in *Proc. 34th Int. Conf. Lightning Protection*, 2018, pp. 1–7.
- [18] *Electromagnetic Compatibility (EMC), Part 4-25: Testing and Measurement Techniques—HEMP Immunity Test Methods for Equipment and Systems*, IEC:61000-4-25, 2019.
- [19] Z. Cui, B. Wei, F. Grassi, and S. A. Pignari, "Experimental analysis and circuit modeling of pulsed current injection in wire pairs," in *Proc. IEEE Int. Symp. Electromagn. Compat./IEEE Asia-Pacific Symp. Electromagn. Compat.*, 2018, pp. 1109–1113.
- [20] X. Lu, G. Wei, X. Pan, X. Zhou, and L. Fan, "A pulsed differential-mode current injection method for electromagnetic pulse field susceptibility assessment of antenna systems," *IEEE Trans. Electromagn. Compat.*, vol. 57, no. 6, pp. 1435–1446, Dec. 2015.
- [21] "Jelectric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats," Jun. 2016. [Online]. Available: <https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20ResilienceEstablishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf>
- [22] W. Qiu, L. Zhang, and H. Yin, "PLC-based impedance measurement and current injection response analysis," in *Proc. IEEE Ind. Appl. Annu. Meeting*, Vancouver, BC, Canada, Oct. 2021, pp. 1–6.
- [23] Z. Szabó, G. Park, R. Hedge, and E. Li, "A unique extraction of metamaterial parameters based on Kramers-Kronig relationship," *IEEE Trans. Microw. Theory Techn.*, vol. 58, no. 10, pp. 2646–2653, Oct. 2010.
- [24] M. S. Sarto and A. Tamburrano, "Single-conductor transmission-line model of multiwall carbon nanotubes," *IEEE Trans. Nanotechnol.*, vol. 9, no. 1, pp. 82–92, Oct. 2010.
- [25] H. E. Corporation, *Impedance Measurement Handbook*, 1st ed., 2018. [Online]. Available: https://hiokiusa.com/wp-content/uploads/2017/07/A_UG_IM0004E01-3.pdf
- [26] M. Sultan, "Modeling of a bulk current injection setup for susceptibility threshold measurements," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, 1986, pp. 1–8.
- [27] Z. Cui et al., "Circuit modeling of the test setup for pulsed current injection," in *Proc. Asia-Pacific Int. Symp. Electromagn. Compat.*, 2016, vol. 01, pp. 726–728.
- [28] *Electromagnetic Compatibility (EMC), Part 4-18: Testing and Measurement Techniques—Damped Oscillatory Wave Immunity Test*, IEC:61000-4-18, 2019.
- [29] Z. Cui, F. Grassi, S. A. Pignari, and B. Wei, "Pulsed current injection setup and procedure to reproduce intense transient electromagnetic disturbances," *IEEE Trans. Electromagn. Compat.*, vol. 60, no. 6, pp. 2065–2068, Dec. 2018.
- [30] "Micrologix 1400 programmable controllers, installation instructions," Rockwell Automation. Accessed: Aug. 30, 2022. [Online]. Available: https://literature.rockwellautomation.com/idc/groups/literature/documents/in/1766-in001_-en-p.pdf
- [31] R. Horton et al., "High-altitude electromagnetic pulse and the bulk power system, potential impacts and mitigation strategies," Electric Power Research Institute (EPRI), Palo Alto, CA, USA, 2019, Art. no. 3002014979.