Vulnerability Studies under EMP: Impedance and PCI Testing of the Grid Control Devices

Wei Qiu[1], Liang Zhang[1], He Yin[1], Lawrence C Markel[2]
[1]*Department of Electrical Engineering & Computer Science*
The University of Tennessee, Knoxville, TN, USA
qwei4@utk.edu, liangzhangswpu@gmail.com, hyin8@utk.edu

Dahan Liao[2], Ben W Mcconnell[2], Yilu Liu[1, 2]
[2]*Oak Ridge National Laboratory, ORNL, TN, USA*
markellc@ornl.gov, liaod@ornl.gov,
bwmcconnell@me.com, liu@utk.edu

***Abstract*—Control devices such as inverters and generator controllers are critical for the stable operation of the power grid, especially for power stability control and power dispatch. However, the Electromagnetic Pulse (EMP) is a potential threat to electronic devices in modern power grids, therefore decreasing the power grid resilience and bringing unrecoverable damages to the devices. To reveal the impact mechanism of the EMP, impedance and Pulse Current Injection (PCI) testing is established to study the vulnerability of the grid control devices. The impedance of the grid control devices is accurately measured using impedance analyzers with different frequency ranges. Then the voltage and current responses are tested based on the PCI testing. The vulnerability experiments based on two grid control devices are carried out. And the comparison results reveal that most ports would be damaged under EC8, and some ports can survive under EC5 according to the calculated PCI response and cumulative energy. The results can provide a reference for the future design of control devices and the strategic resilience of power grids.**

***Index Terms*—Grid control devices, Vulnerability study, Pulse Current Injection (PCI), Electromagnetic Pulse (EMP)**

I. Introduction

As the basic infrastructure of the power grid, the safety and reliability of the control devices are crucial to the stability and protection of the power system [1], [2]. However, the Electromagnetic pulse (EMP), a set of bursts of a powerful electromagnetic field with a wide frequency ranging from zero Hz to gigahertz, would directly damage or destroy electronic devices, especially for high-attitude EMP [3]. The E1 EMP is a brief and intense electromagnetic field that can easily cause field strength up to 10^5 volts per metre. It would induce very high voltages in power electronic components. Instead, limited studies have paid attention to the resilience of control devices under EMP. The electromagnetic radiation exposed by EMP can be easily coupled to the control devices through signal lines or transmission lines [4], causing irreversible damage. An effective vulnerability assessment method is necessary for revealing the impact mechanism of EMP and improving the protection ability.

To explore EMP impact on the power grid, the radiative test is developed, and this technology can be categorized into two classes, including the Electromagnetic Environments Simulator (EMES) and Pulsed Current Injection (PCI) test.

The EMES aims to construct a radar electromagnetic environment to achieve the conducted and radiated tests [5]. For example, a bounded wave simulator is established to measure the multigap loop antenna in [6]. And [7] tests the component and system vulnerability of the electric grid using Sandia's EMES. However, the primary limitation of the EMES is that it is high-cost and time-consuming to finish all the vulnerability studies for each component of devices.

Therefore, PCI technology is developed to test the vulnerability of electric/electronic equipment due to its convenience and effectiveness. In [8], a PCI setup involving the pulse generator is modeled with adjustable parameters. And the specific load impedance is a prerequisite for accurate EMP evaluation. Similarly, the kA-level PCI is implemented based on the MIL-STD-188-125-2 [9], where the coupling and decoupling efficiency is solved. Taking the benefits of PCI tests, the vulnerability can be well revealed.

To explore the vulnerability of the grid control devices, the impedance with a wide frequency is measured, and PCI testing is conducted to evaluate its immunity to EMP. The contributions of the paper are summarized as

1) First, to achieve the vulnerability analysis under EMP, the accurate impedance is measured by the three devices to overcome the limited frequency range of the instrument. Both the Differential Mode (DM) and Common Mode (CM) are collected to give a complete observation.
2) To investigate the response of the EMP under different immunity test levels, the PCI testing is established based on the measured impedance. Two immunity test levels including EC5 and EC8, are conducted. Based on the voltage and current responses, the cumulative energy and its spectrum are analyzed to reveal the sensitive frequency area.
3) Two control devices including the Automatic Genset Controller (AGC) and Load Sharing and Speed Control (LSSC) are utilized to verify the effectiveness of the proposed impedance measurement and PCI testing methods. The vulnerabilities of immunity test levels, frequency response, and tolerances are studied.

This work is supported in part by the DOE Grid Modernization Lab Call (GMLC) Project: Vulnerability of Power Generation Critical Systems Against Electromagnetic Threats under Agreement #36129, and also in part by CURENT Industry Partnership Program.

II. IMPEDANCE MEASUREMENT

To achieve the immunity study, impedance is required for accurate measurement. However, the frequency range of different impedance analyzers varies. For example, the resolution of MFIA from Zurich Instruments is 1 mHz to 500 kHz. Considering that the spectrum of the E1 HEMP ranges from about one megahertz to several hundred megahertz [10], impedance measurement devices with wide frequencies are preferred.

This research uses three impedance measurement devices, including the MCR-5200 [11], HP 4395A, and Planar TR1300/1 [12]. The frequency range of the LCR meter MCR-5200 locates between 40Hz and 200kHz. The frequency range of the impedance analyzer HP 4395A is 10Hz to 500MHz, and the vector network analyzer Planar TR1300/1 is 300kHz to 1.3GHz.

To give a consistent measurement, the following steps are performed

(i) The impedance analyzers warm up for an hour to make the measurement precise. Then the parameter of different devices is set to the same, e.g., the output voltages are set to 0.1V and the output power is set to -7dBm.

(ii) Then the impedance calibration is executed based on three-term calibration (open/short/load) to eliminate the line measurement error.

(iii) The impedance is measured by connecting the fixture, where the DM and CM cases are tested.

(iv) The de-embedding is modeled using the open-short and short-open techniques [13]. The non-uniform transmission line model is established to simulate the dynamic characteristics of the fixture.

According to the impedance measurement results, there are some overlaps in the frequency band. Based on this characteristic, the measured impedance can be cross-referenced to quickly discard the invalid measurements. Last, the spline interpolation technology is implemented to fuse the three measurements into one curve, which the impedance and phase can be denoted as $[Z_k,\ \phi_k]$.

III. PCI TESTING UNDER EC5 AND EC8

A. PCI testing

To study the port response under EMP, the PCI model is established, where the simplified circuit diagram is shown in Fig. 1 based on IEC 61000-4-25. Output waveforms are damped sinusoids and double exponential for EC5 and EC8, respectively.

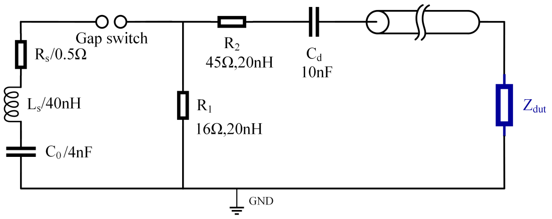


Fig. 1. Circuit diagram of PCI testing under EC8.

Circuit parameters illustrated in Fig. 1 ensure that the output waveform meets the requirements of the IEC standard. The output of the generator is connected to impedance Z_{dut} through a 50 Ω coaxial cable. Z_{dut} represents the measured port impedance of the device under test. A pulsed voltage will be applied to the circuit when the switch is triggered. As Z_{dut} is measured up to 1.3 GHz, voltage and current waveform on Z_{dut} are calculated in discrete points of 40Hz 1.3GHz's frequency range. As many as $n = 500 \times 10^3$ points are adopted by interpolation and Z_{dut} is expressed as $Z_{dut}(\omega) = \sum_{k=1}^{n} |Z_k| e^{j\phi_k}$, where $k = 1, 2..., n$ denotes the frequency point, ϕ_k is the phase.

Then voltage and current of each branch circuit can be calculated. Results on Z_{dut} can be obtained as follows

$$\left\{\begin{array}{l} U_{\text{dut}}(t) = \frac{2}{n}\sum_{k=1}^{n} |U_k| \cos\left(\omega_k + \phi_{k,U}\right) \\ I_{\text{dut}}(t) = \frac{2}{n}\sum_{k=1}^{n} |I_k| \cos\left(\omega_k + \phi_{k,I}\right) \end{array}\right. \tag{1}$$

where U_k is the magnitude of each frequency component, U_{dut} and I_{dut} denote voltage and current in the frequency domain, respectively. ω_k denotes the radian frequency. Then time domain waveform can be obtained through the inverse Fourier transform of U_{dut} and I_{dut}.

For the EC5 level, there are three oscillation frequency components with the following values: 3MHz, 10MHz, and 30MHz. Its short current is 40 A and the open voltage is 2 kV. Similarly, the short current is 160 A and the open voltage is 8 kV for EC8. All parameters meet the requirements of the IEC standards.

Afterwards, the cumulative energy and spectrum of the inducted voltage and current are calculated, where the spectrum can be refereed to [14]. The cumulative energy denotes the peak energy location with special frequency, indicating the value port vulnerability frequency points. Besides, the vulnerability and tolerances of the power grid control devices can be evaluated by comparing the design manual and EMP standard.

IV. EXPERIMENTS

To verify and evaluate the port vulnerability, two power grid control devices are tested including the AGC-4 produced by DEIF [15] and Woodward 2301E Digital LSSC for engines [16], as shown in Fig. 2. The AGC can be used as a single genset controller, and it can be seen that it contains rich interfaces. The LSSC is designed for driving a diesel or gaseous engines. Accordingly, the above control devices are critical for ensuring the power stability of the power system. During the testing, the DM and CM are tested.

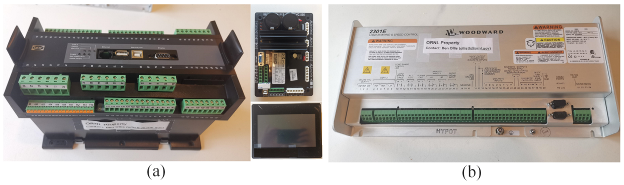


Fig. 2. Tested control devices, (a) automatic genset controller AGC-4 and display, (b) 2301E digital load sharing and speed control for engines.

A. Impedance measurement results of AGC

This section presents four pairs of the measured impedance and phase results for AGC, as demonstrated in Fig. 3. These four pairs of ports are selected as examples since they have different amplitudes and variation characteristics.

As depicted in Fig. 3 (a) and (c), the impedance results agree with each other when the frequency is higher than 1MHz. When the frequency is lower than 1MHz, the measurement trend of the HP 4395A is different from that LCR meter, the reason is that the impedance of the port exceeds the measurement range for HP 4395A. Thereafter, the measurement result of HP 4395A can be discarded if the impedance is higher than $10^5\Omega$. For Fig. 3 (b) and (d), all the measurements agree with each other, indicating the accuracy of the measurement results.

Besides, Fig. 3 (a) and (c) illustrate the capacitive impedance when the frequency is lower than 500MHz, indicating the open circuit. Conversely, the phases of Fig. 3 (b) and (d) change drastically, indicating many inductive and capacitive components existed in the circuit.

B. Results of pulsed current injection response under EC5

The PCI response under EC5 is presented in this section. The voltage and current responses of different pairs of ports for AGC and LSSC are demonstrated in Fig. 4 and 5, respectively. As can be seen from Fig. 4 (a), the current response of transistor outputs between ports 66 and 67 is higher than the rest of the ports. According to Fig. 3 (b), it has a minimum impedance value lower than 10000 Ohm. The maximum value of current and voltage for transistor outputs 4-5, display, and ground are lower than 10 A and 2500 V, respectively. The PCI responses of ground 2-3 and transistor output 4-5 are consistent because they have similar impedance and phase results from Fig. 3 (a) and (c). Compared with the DM and CM results, CM (ground 2 to port 3) shows the same trend as DM (transistor output 4-5).

For the results of LSSC shown in Fig. 5, the ETH and COM 10 denote the Ethernet port and communication interface, respectively. All the current responses are lower than 50A and the voltage is lower than 2300V. Interestingly, it can be found that the response of the Ethernet port includes high-frequency oscillation, especially when the time locates between 0 and 150 ns. This phenomenon might be caused by the high-frequency resonant circuit between ports 1 and 6.

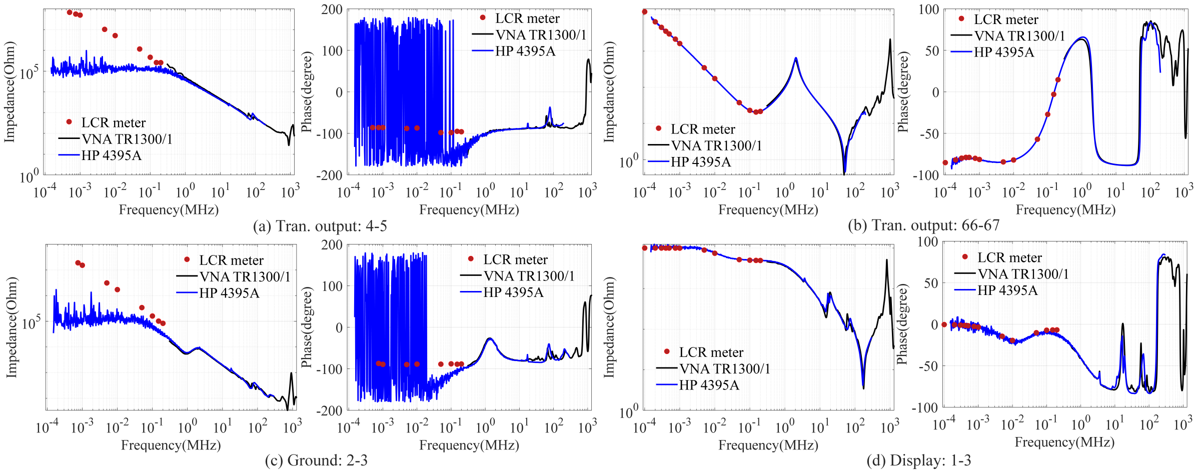
C. Results of pulsed current injection response under EC8

Meanwhile, the EC8 tends to have higher transient energy. Thus, the circuit will exhibit vulnerability. The PCI response of AGC under EC8 is demonstrated in Fig. 6. The current and voltage of the transistor outputs between 66 and 67 are as high as 200A and 10kV, respectively, due to a low port impedance. The results of Fig. 6 show similar results to Fig. 4, where the difference is that the response level is approximately four times higher. According to the immunity test levels defined in IEC 61000-4-25 [14], the voltage levels of EC5 and EC8 are 2000V and 8000V, respectively, indicating their consistency with the PCI response.

As illustrated in Fig. 7, the voltage of VGA ports between 13 and 14 decreases to -2500V in 8ns, and the current increases to nearly 200A in 8ns, indicating its high transient characteristics. For the Ethernet port 1-6, an oscillatory component is superimposed on its exponential pulse time history. Compared with PCT results under EC5 in Fig. 5, this oscillation is easier to excite, indicating that it is more sensitive to high-frequency energy. Based on the PCI responses, the maximum voltage and current can be referred to as the indicator of vulnerability assessment.

D. Comparison of cumulative energy and spectrum

To further evaluate the vulnerability of control devices, the cumulative energy and spectrum are calculated. Fig. 8 and Fig. 9 demonstrate the results under EC5 and EC8, respectively. The cumulative energy result reveals that the voltage and current energies are concentrated at 10MHz. This energy result is in line with the spectrum as shown in Fig. 8 (c), where the peak value is located near 10MHz. Besides, compared with Fig. 8 (b) and (d), some part of the energy is dispersed to 10-100MHz because it still contains rich spectrum components



(a) Tran. output: 4-5

(b) Tran. output: 66-67

(c) Ground: 2-3

(d) Display: 1-3

Fig. 3. Measurement impedance and phase of four pairs of ports for AGC under both differential mode and common mode. (a) DM: transistor outputs between 4 and 5, (b) DM: transistor outputs between 66 and 67, (c) transistor output (3) CM: to ground 2 and port 3, (d) DM: display port 1 and 3.

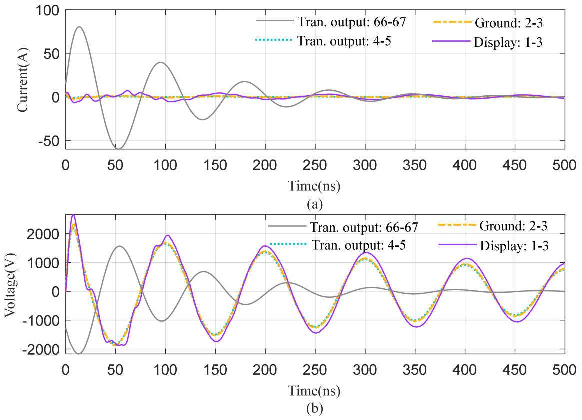


Fig. 4. Voltage and current responses under EC5-based PCI testing for AGC.

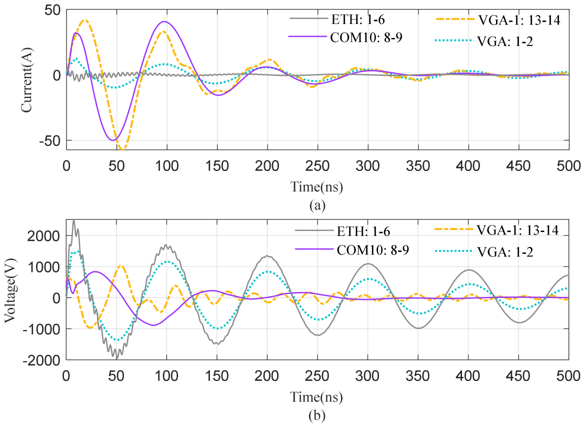


Fig. 5. Voltage and current responses under EC5-based PCI testing for LSSC. The VGA denotes the video graphics array.

near 10-100MHz. Overall, the results consist of the injected pulse with a 10MHz waveform.

Different from EC5, the energy distribution of EC8 is wider and located between 1MHz to 20MHz for the voltage response. The primary reason is that the frequency of burst EMP ranges from zero Hz to very upper limited frequency, as can be seen from Fig. 9 (c). Meanwhile, the maximum cumulative energy from Fig. 9 (b) indicates that the difference of the spectrum peaks leads to a change in the cumulative energy curves.

Additionally, the voltage energy and its spectrum of LSSC are demonstrated in Fig. 10. The cumulative energy has the same profile as Fig. 9(a). Instead, the oscillation with 239MHz frequency is depicted in Fig. 10(b). This phenomenon is consistent with Fig. 7 (b).

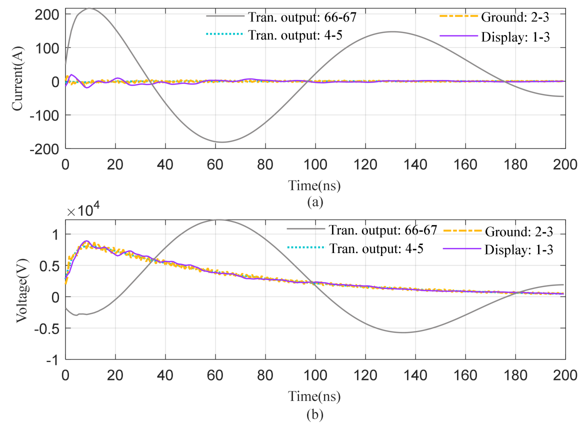


Fig. 6. Voltage and current responses under EC8-based PCI testing for AGC.

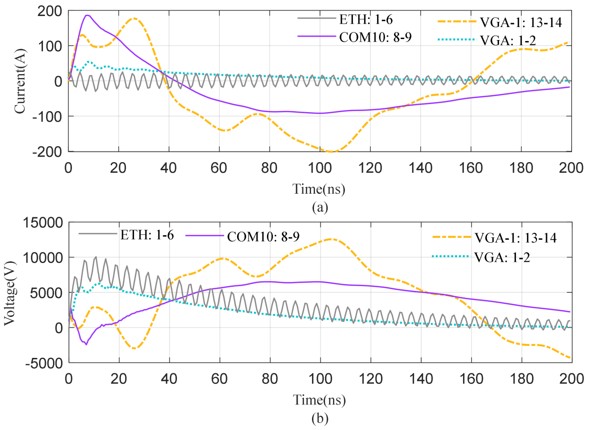


Fig. 7. Voltage and current responses under EC8-based PCI testing for LSSC.

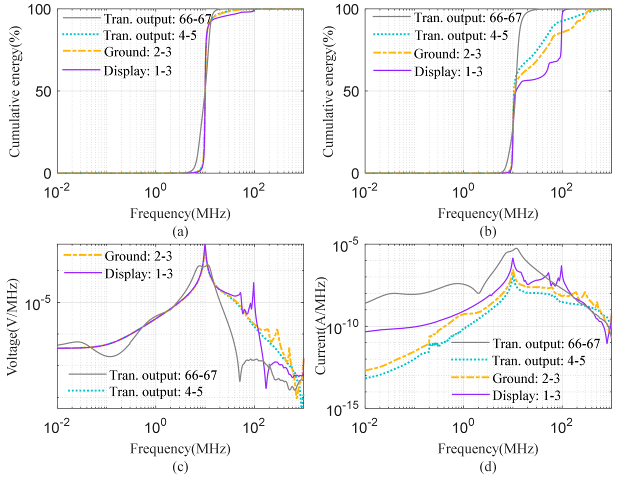


Fig. 8. Cumulative energy of voltage and current and its corresponding spectrum EC5-based PCI testing for AGC. (a) and (c) voltage, (b) and (d) current.

Overall, the above cumulative energy and spectrum analysis demonstrate that the port vulnerability can be improved by adjusting the location of the impedance and frequency response.

E. Discussion about the vulnerability study of AGC and LSSC

To study the vulnerability of the grid control devices, the standards for product design and E1 HEMP are used for comparison. The standards for AGC and LSSC design are listed in Table I, which is summarized based on their data sheets. It can be found that the maximum peak voltages of AGC are 4kV and 2kV for the Electrical Fast Transient (EFT) and damped oscillatory, respectively. Based on the PCT testing results shown in Fig. 4 and Fig. 6, the voltages are higher than 8kV and 2kV for some ports. Indicating that the control device AGC would fail under EC8 and only some ports can survive under EC5.

The maximum immunity level of LSSC is 1kV to 2kV for all types of ports, as listed in Table I. Based on the PCI testing results depicted in Fig. 5 and 7, two pairs of ports can survive, including the communication ports 8-9 and VGA ports 13-14.

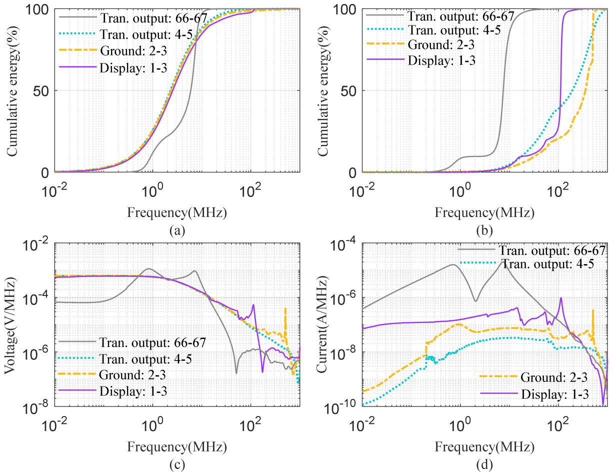


Fig. 9. Cumulative energy of voltage and current and its corresponding spectrum EC8-based PCI testing for AGC. (a) and (c) voltage, (b) and (d) current.

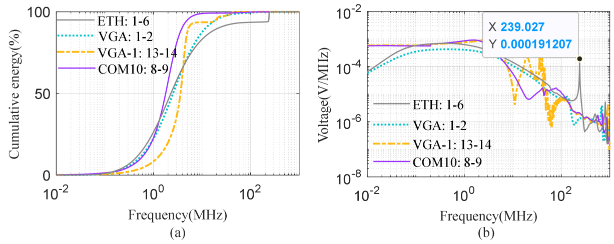


Fig. 10. Cumulative energy of voltage its corresponding spectrum EC8-based PCI testing for LSSC.

Obviously, the ports would be destroyed if there were no extra surge protection devices.

TABLE I
IMMUNITY PROTECTION REFERENCE STANDARD FOR CONTROL DEVICES.

Devices	Design Criteria and Values	
	Standard	Reference value
AGC	EN 61000-6-2 [17]	Signal/control/network ports
	EN 61000-6-4 [18]	Damped oscillatory: 2kV (peak)
	and	EFT/Burst: 4kV (peak), 5/50ns
	IEC 60255-26 [19]	Earth port: 4kV (peak), 5/50ns
LSSC	IEC 61000-4-5 [20]	Surge ±1kV I/O CM
	and	DC Power DM/CM±1kV
	EN 61000-6-2	AC Power DM/CM±1-2kV
	EN 61000-4-4 [21]	EFT ±2kV Power & I/O

DM/CM denotes the Differential mode/Common mode

V. CONCLUSION

To study the vulnerability of the critical power grid control devices, the impedance, as well as the PCI testing, are proposed under E1 EMP. The DM/CM port impedance of the control devices is first measured by using three impedance analyzers. The impedance measurements of four pairs of ports demonstrate the consistency of results. Then the PCI model is established and the PCI response can be inferred. Taking the AGC and LSSC as the tested objectives, their PCI responses are estimated under two immunity test levels including EC5 and EC8. PCI testing results indicate that the maximum voltage can reach 12kV due to its low impedance. The concentrated energy reveals the vulnerability frequency area of the control devices. Finally, the vulnerability study of AGC and LSSC demonstrates that only small parts of ports can survive under immunity test level EC5.

REFERENCES

[1] S. An, W. Qiu, Q. Pu, and et al., "Power system wideband oscillation estimation, localization, and mitigation," *IET Generation, Transmission & Distribution*, 2023.

[2] K. Sun and et al., "Wams-based hvdc damping control for cyber attack defense," *IEEE Transactions on Power Systems*, vol. 38, no. 1, pp. 702–713, 2023.

[3] D. Wang, Y. Li, P. Dehghanian, and S. Wang, "Power grid resilience to electromagnetic pulse (emp) disturbances: A literature review," in *2019 North American Power Symposium (NAPS)*.

[4] L. Zhang and et al., "Immunity study Port impedance measurement of pmu and pci testing under emp," in *2022 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia)*, 2022, pp. 800–805.

[5] "Ornl, high-voltage modeling and testing of transformer, line interface devices, and bulk system components under electromagnetic pulse, geomagnetic disturbance, and other abnormal transients," *Oak Ridge National Laboratory*, 2019.

[6] X. Kong, Y.-Z. Xie, Q. Li, and Y.-H. Hu, "A multigap loop antenna and norm detector-based nano-second-level transient magnetic-field sensor," *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 10, pp. 8393–8400, 2020.

[7] "Sandia report, electromagnetic pulse - resilient electric grid for national security: Research program executive summary," *SAND2020-11227*, 2020.

[8] Z. Cui, F. Grassi, and S. A. Pignari, "Circuit modeling of the test setup for pulsed current injection," in *2016 AsiaPacific International Symposium on Electromagnetic Compatibility (APEMC)*, vol. 01, 2016, pp. 726–728.

[9] Z. Cui and et al., "A coupling and decoupling device for pulsed current injection in mil-std-188-125-2," in *2019 IEEE International Symposium on Radio-Frequency Integration Technology (RFIT)*, 2019, pp. 1–3.

[10] D. E. Sanabria, T. Bowman, R. Guttromson, M. Halligan, K. Le, and J. Lehr, "Early-time (e1) high-altitude electromagnetic pulse effects on trip coils." [Online]. Available: https://www.osti.gov/biblio/1714422

[11] Eleshop, "Matrix mcr-5200 lcr precision meter, [online] avaliable at: https://eleshop.eu/mcr-5200.html," vol. n/a, no. n/a, 2023.

[12] Copper Mountain Technologies, "Tr1300/1 2-port 1.3 ghz analyzer, [online] avaliable at: https://coppermountaintech.com/vna/tr1300-1-2-port-1-3-ghz-analyzer/," vol. n/a, no. n/a, 2023.

[13] A. Mangan and et al., "De-embedding transmission line measurements for accurate modeling of ic designs," *IEEE Transactions on Electron Devices*, vol. 53, no. 2, pp. 235–241, 2006.

[14] IEC:61000-4-25, "Electromagnetic compatibility (emc), part 4-25: Testing and measurement techniques – hemp immunity test methods for equipment and systems," 2019.

[15] DEIF, "Agc-4," in *[Online] available at: https://pdf.directindustry.com/pdf/deif/agc-4/20890-438373.html*, 2023.

[16] Woodward, "2301e lssc, 24vdc, standard loc," in *[Online] available at: https://www.woodward.com/en/shop/woodward44-industrial-engines/8273-1011*, 2023.

[17] IEC 61000-6-2: 2016, "Electromagnetic compatibility (emc) - part 6-2: Generic standards - immunity standard for industrial environments," 2016.

[18] IEC 61000-6-4:2018 , "Electromagnetic compatibility (emc) - part 6-4: Generic standards - emission standard for industrial environments," 2018.

[19] IEC 60255-26: 2023, "Measuring relays and protection equipment - part 26: Electromagnetic compatibility requirements," 2023.

[20] I. .-.-. 2014, "Electromagnetic compatibility (emc) - part 4-5: Testing and measurement techniques - surge immunity test," 2014.

[21] IEC:61000-4-4, "Electromagnetic compatibility (emc) – part 4-4: Testing and measurement techniques – electrical fast transient/burst immunity test," 2004.