# Electromagnetic Side-Channel Noise Intrusion on Solid-State Transformer

Mateo D. Roig Greidanus, *Graduate Student Member, IEEE*, Silvanus D'Silva, *Graduate Student Member, IEEE*, Shantanu Gupta, *Graduate Student Member, IEEE*, Debotrinya Sur, *Graduate Student Member, IEEE*, Sudip K. Mazumder, *Fellow, IEEE*, and Mohammad B. Shadmand, *Senior Member, IEEE*

***Abstract*—This article delves into the intricacies of electromagnetic side-channel noise intrusion (EM-SNI) and its impact on the voltage sensors of a solid-state transformer (SST). As described in this work, the EM-SNI attack can be easily deployed using a small antenna, and its effects spread without any electrical contact with the power-electronics hardware circuitry or measurement signal feedback. The cyber-physical attack is performed by injecting noise at very high frequencies (MHz range), and due to the aliasing effects of the analog-to-digital converter sampling, corrupt the feedback signal as sub- and super-60 Hz harmonic frequencies. Hence, this article details how the EM-SNI mechanism works and analytically discusses the aliasing effects on noise frequency injections that could potentially harm the SST system. Subsequently, a method to detect and mitigate the impact of EM-SNI on the SST system is proposed to counteract its effects. The method involves a cross-correlation-based intrusion detection and voltage feedback observation on the instantaneous power-transfer relationship for mitigation. Experimental results confirm the effectiveness of the proposed methodology and are presented throughout the article.**

***Index Terms*—Cyberattack, cyber resilient, electromagnetic interference, measurement feedback, solid-state transformer.**

## I. Introduction

CYBER-ATTACKS that corrupt the sensor data feedback can most immediately degrade the electrical variables of a power converter system. As demonstrated by [1] and [2], an intruder can intentionally disrupt embedded system components and sensors by placing high-power antennas, amplifiers, or thin electromagnetic actuators in close proximity to the devices. Such an attack mechanism, herein called electromagnetic side-channel noise injection (EM-SNI), presents the advantage of being nonintrusive, besides allowing for untethered propagation across multiple devices. In addition, the EM-SNI easily allows customization and fine-tuning [3] of the attack through an external agent, enabling diverse data corruption objectives [4].

Manuscript received 6 December 2023; revised 21 February 2024; accepted 12 April 2024. Date of publication 19 April 2024; date of current version 20 June 2024. The work of Sudip K. Mazumder at the University of Illinois Chicago was supported in part by the U.S. Department of Energy under Grant DE-CR0000019 and in part by the U.S. National Science Foundation under Grant 2219734. Recommended for publication by Associate Editor M. Liserre. *(Corresponding author: Sudip K. Mazumder.)*

The authors are with the Electrical and Computer Engineering Department, University of Illinois Chicago, Chicago, IL 60607 USA (e-mail: mgreid2@uic.edu; sdsilv2@uic.edu; sgupt57@uic.edu; dsur2@uic.edu; mazumder@uic.edu; shadmand@uic.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TPEL.2024.3391217.

Digital Object Identifier 10.1109/TPEL.2024.3391217

This work experimentally performs the EM-SNI-based intrusion mechanism and studies its effect on the direct-power conversion type solid-state transformer (SST) ac/ac converter [5]. Direct-power conversion (DPC) converters are particularly vulnerable to the effects of sensor feedback data manipulation. These single-stage type ac/ac converters are less exposed to potential software integrity breaches. However, due to minimal internal energy storage [6], such converters have low disturbance rejection capability, allowing for disturbance propagation in closed-loop operation.

The authors of this article previously explored the effects of a similar side-channel noise intrusion (SNI) in an inverter [7]; the cyber-attack conditions that differ this article from the previous work are as follows.

1) The nature of the side-channel attack coupling mechanism studied in this article—unlike previous work on conductive coupling by direct electrical contact with the printed-circuit board (PCB) trace, this work considers an inductive coupling between the intrusive radiated electromagnetic source and the PCB microstrips of the signal conditioning board. A radio-frequency (R.F.) designed helical antenna is used here to perform such an attack.
2) The intrusive electromagnetic noise propagates untethered between the analog signal circuitry, with a higher impact depending on the proximity between the nonintrusive source and sensor feedback.
3) The higher frequency nature of the intrusive noise source tuned for a radio-frequency oscillation rate in the range of tens of MHz.

When attacks cannot be avoided, a resilient power converter system must have an attack-tolerant control mechanism to counteract and maintain system operability at acceptable levels [8]. A cyber resilient mechanism, in general, can be designed using two distinct approaches as follows: 1) by either prioritizing the inherent robustness against external intrusions at the expense of optimal performance, or 2) by leveraging reactive methodologies to adapt the converter's dynamic operation to adverse conditions. To ensure near-optimal performance and restoration of operating conditions, a reactive intelligent mechanism must comprise at least two steps [9]. First, the intrusion must be detected in a limited time frame; then, the mitigation of the effects of such intrusions is required to prevent the propagation of impacts and any potential disruptions in the converter operation.

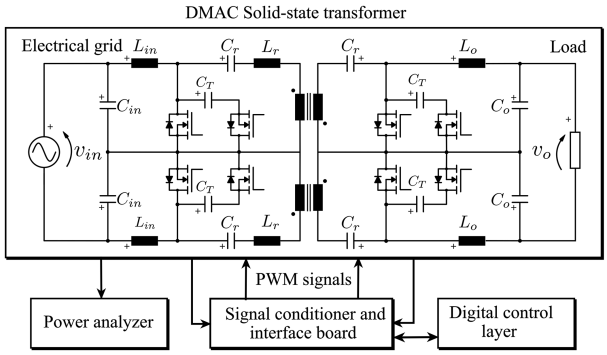



Fig. 1. Top-level architecture of an SST. The differential-mode ac/ac converter (DMAC) and its modulation strategy are thoroughly discussed in [5].

Hence, after looking into the adverse effect of EM-SNI based intrusion attack on the converter's performance degradation, this research ultimately discusses a strategy to promote its resilient operation.

The rest of this article is organized as follows. The explaination of the EM-SNI-type attack mechanism, its impact and propose a solution for the resilient operations of an SST is as follows. Section II briefly explains a DPC SST converter and describes its nominal operation baseline and control. The EM-SNI mechanism and the particularities of the inductive coupling of an antenna with the PCB microstrips are discussed in Section III. Next, supported by mathematical analysis and experimental results, Section IV explains how an intruder can exploit the aliasing factor on the finite rate sampling of the analog-to-digital conversion to attack the measurement feedback. Our findings indicate that such an attack can cause sub- and super-60 Hz distortions, even if the EM-SNI intrusion is in the MHz frequencies band. The resilience mechanisms for the control operation are described in the following sections. In Section V, a cross-correlation-based intrusion detection scheme (CC-IDS) is applied to identify whether a malicious intrusion is affecting the normal operation of the converter. An EM-SNI mitigation strategy is proposed in Section VI, which uses the power transfer characteristic of the converter described in Section II to estimate the affected measurement feedback and return the converter output to acceptable operating levels. Finally, Section VII concludes this article.

## II. The Nominal SST System

The semiconductor-based ac/ac SST is an active and compact alternative to the widely used bulkier low-frequency (60/50 Hz) passive low-frequency transformers (LFTs). Compared to LFTs, the SST has the potential to offer an economical, modular, and denser solution [10]. However, the cyber-physical architecture required from an SST system differs significantly from a monolithic LFT due to the large number of active components involved in its design. A modern SST architecture broadly entails an ac/ac power converter with semiconductor devices and passive components, sensors with a signal conditioning circuit, and a digital controller for feedback control, as depicted in Fig. 1.

TABLE I
PAC-Ćuk DMAC Prototype Designed Parameters

| Parameter(s) | Symbol(s) | Value(s) |
|---|---|---|
| RMS input and output voltages | $V_{in}, V_o$ | 120 V |
| Nominal load resistance | $R$ | 45 Ω |
| Input and output capacitance | $C_{in}, C_o$ | 0.5 $\mu$F |
| Equivalent blocking capacitance and auxiliary blocking capacitors | $C_r, C_T$ | 1 $\mu$F, 0.47 $\mu$F |
| Transformer leakage inductance | $L_r$ | 125 $\mu$H |
| Input and output inductors | $L_{in}, L_o$ | 600 $\mu$H |
| Sampling and switching frequency | $f_s$ | 40 $k$Hz |

Utilizing the high switching frequency capability of the semiconductor devices, the ac/ac power converter performs the galvanically isolated ac–ac conversion. An ac/ac converter can be categorized based on the number of power conversion stages and the presence of a dc link for power decoupling [11]. Among the various types of converters, a single-stage ac/ac converter with a DPC configuration offers a more straightforward, efficient, and economical solution than a multistage converter power-stage solution. This configuration performs direct power transmission between the input and output ports without significant energy storage, thereby, offering a dense and economical solution.

In this article, an isolated differential mode (D.M.) pulsewidth modulation active-clamp (PAC) Ćuk-based ac/ac converter (DMAC) is used to emulate a scaled-down SST system [5], [12]. The PAC-Ćuk DMAC converter topology boasts several noteworthy characteristics, such as continuous input and output currents, low total harmonic distortion (THD) of output voltage, and reduced size of input and output filter capacitors in comparison to other DPC topologies. The converter offers a wide soft-switching range, resulting in high-efficiency operation over a wide load and gain region. The relevant design parameters for the 1kW DMAC prototype utilized in this work, as outlined in [5], are summarized in Table I.

### A. The Instantaneous Power Transfer on the SST

The power transfer process in a lossless transmission line is usually described by $p_{12} = \frac{|v_1||v_2|}{X} \sin\delta$, wherein $p_{12}$ denotes the real power flow, $|v_1|$ and $|v_2|$ represents the line-to-line voltages at the two ends of the line, $X$ signifies the series reactance of the line, and $\delta$ stands for the phase displacement angle between $|v_1|$ and $|v_2|$. Analogously, a power transfer type ac/ac converter can regulate the secondary output voltage amplitude and exert control over the phase displacement between its primary and secondary voltage terminals. This characteristic of instantaneous power transfer is analytically described for different DPC ac/ac converter topologies in [13], [14], and [15]. The closed-form solution of the instantaneous output power $(p_o)$ for PAC-Ćuk DMAC converter as a function of the input voltage $(v_{in})$, output voltage $(v_o)$, and phase-shift displacement ratio $(\delta_\phi)$ between the primary-side and secondary-side SST switches, is given by [5].

$$p_o = \frac{8 v_{in} v_o}{Z_r \omega_r T_s} \cdot f\left(\delta_\phi, \omega_r, T_s\right); \tag{1}$$

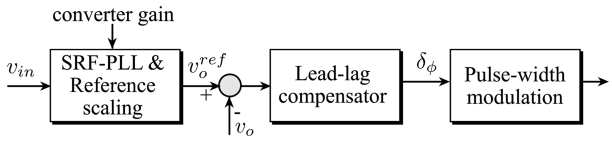



Fig. 2. Simplified control schematic implemented in the digital signal processing (DSP) unit.

$$f(\delta_\phi, \omega_r, T_s) = \left( \frac{\sin\left(\delta_\phi \frac{T_s\omega_r}{2}\right) \sin\left(\frac{T_s\omega_r}{4}\left(1 - \frac{\delta_\phi}{2}\right)\right)}{\cos\left(\frac{T_s\omega_r}{4}\right)} \right), \tag{2}$$

where $Z_r, \omega_r$, and $T_s$ stands for resonance impedance, resonance frequency, and switching frequency, respectively, which are the design parameters of the converter.

### B. The SST Control-Layer

Under normal operating conditions, it is necessary to maintain a regulated voltage on the secondary side of the DMAC SST. Given a continuous active power demand (constant resistive load $R_{load}$), the output voltage regulation must solely depend on the design parameters on $v_{in}$ and $\delta_\phi$. Hence, the regulated output voltage solution can be derived from (1).

$$v_o = \frac{8 v_{in} R_{load}}{Z_r \omega_r T_s} \cdot f\left(\delta_\phi, \omega_r, T_s\right). \tag{3}$$

In this work, the PAC-Ćuk SST converter employs a simple linear output voltage controller with lead-lag compensation to regulate its output voltage $v_o$. The regulation is achieved by comparing $v_o$ measurement feedback to an internally generated voltage reference ${v_o}^{ref}$, aided by a synchronous reference frame (SRF) phase-locked loop (PLL) [16] on the input voltage $v_{in}$ and normalized by the required input-to-output voltage gain. The block diagram in Fig. 2 portrays the overall output voltage control and modulation embedded in the digital control layer.

## III. EM-SNI Mechanism on an SST

Herein, we delve into the EM-SNI mechanism and discuss how intruders can use a small tunable R.F. antenna to disrupt the SST control feedback. The EM-SNI is described here to indicate how electromagnetic interference may spread over the analog circuitry and have a noticeable impact on the digital layer afterward. Please note that the authors do not intend to discuss the best or ideal PCB project design regarding electromagnetic compatibility (EMC). Instead, we aim to explain how an external source of malicious EM-SNI emission can exploit the characteristics of a signal conditioning and control stage of a converter that has already been designed.

The feedback sensor signal from the power stage of the SST undergoes signal conditioning in a chain of analog signal transmission, data translation, and analog-to-digital conversion (ADC) prior to the digital processing stage in a dedicated digital central processing unit (CPU). Throughout this process, various stages, such as amplification, high-frequency component filtering, and signal sampling, are critical to ensuring high-quality data is received by the microcontroller. Each stage is vulnerable to external interference, which can compromise the overall integrity of the feedback data. The malicious intrusion via radiated electromagnetic field intrusion occurs after analog signal conditioning and in the gateway of the digital signal processing (DSP) board, as illustrated in Figs. 3 and 5.

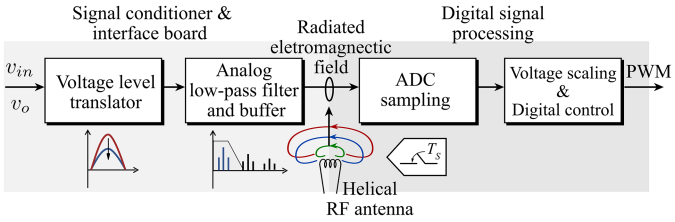



Fig. 3. Depiction of the EM-SNI cyber-attack mechanism on the SST control board.

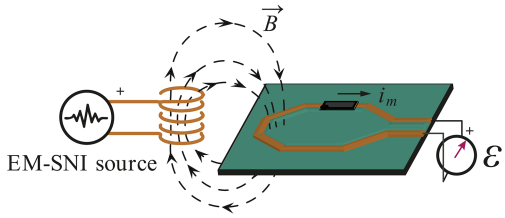



Fig. 4. Inductive coupling of the EM-SNI source-inducing circuit with the signal circuit.

The EM-SNI induces interference by taking advantage of the coupling between the intruder antenna and the PCB traces via air/free-space. As per Faraday's law of induction, the magnetic field oscillation generated by an EM-SNI source will induce an electromotive force (EMF) in a nearby conductor (i.e., the control board PCB traces), possibly disrupting or altering the signal passing through the conductor (PCB traces) as also shown in Fig. 4. In the figure, $\varepsilon$ represents the induced voltage as a result of a time-varying magnetic flux $\phi$, which is dependent only on magnetic flux density, $\vec{B}$. The magnitude of the induced voltage is dependent on both the physical angle of the antenna and the distance of the propagated signal to the center of the coil. For monofilar-designed antennas, such as the one used in this work, the radiation is linearly polarized parallel to the helix axis [17]. The proximity of the antenna's radiated field induces a magnetic field that opposes the voltage induced in the nearby PCB traces [18].

The inductive coupling between the circuit on the PCB and the antenna is depicted in Fig. 4. The EM-SNI source with the antenna introduces a time-varying magnetic field $\vec{B}$ which links with the PCB traces and induces a time-varying voltage in the trace. The high-frequency electromagnetic oscillation in the MHz range permits a malicious intruder to cause detrimental effects on the PCB signal transmission utilizing a small-size transmitting antenna to the feedback analog circuitry, as illustrated in Fig. 5.

## IV. EM-SNI Impact on the Converter Operation

This section discusses how intruders can exploit the aliasing effects of analog-to-digital signal conversion (ADC) to introduce

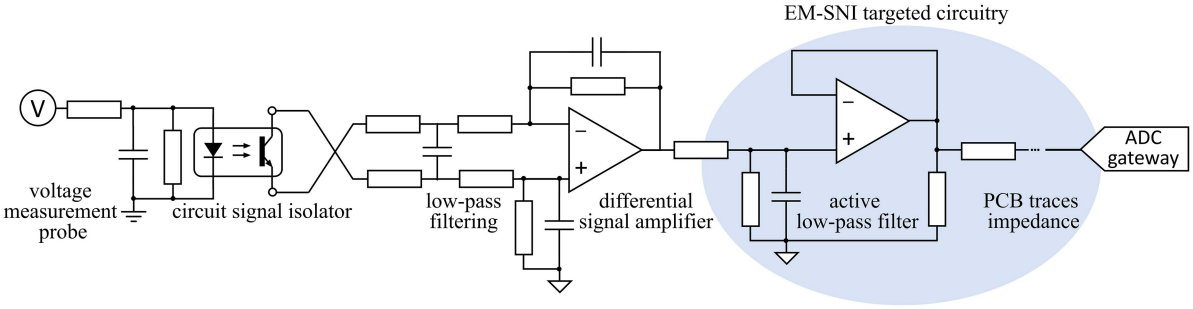



Fig. 5. Voltage measurement signal feedback analog circuitry with highlighted EM-SNI targeted region on the PCB traces.

sub- and super-60 Hz harmonic distortion in SST measurement feedback. Next, experimental results show the consequential effects of such cyber-attacks on the closed-loop performance of the SST converter, outlined in Section II.

### A. EM-SNI Intrusion Aliasing Effects on the Sensor's Feedback

A closer look into the mathematical fundamentals of signal processing and sampling theory reveals the impact that RF EM-SNI has on the dynamics of the SST, specifically in the low-frequency spectrum. An analytical investigation shows that a continuous voltage feedback signal sampled at a finite rate may not always be an accurate representation but rather a distorted version of the presampled actual input.

Consider here the output voltage SST voltage sensor feedback, represented as $v_o\ (t) = V_o\ \sin(\omega_m t)$ is corrupted by a sinusoidal noise intrusion signal represented as $\gamma_{\text{EM-SNI}}\ (t) = \Gamma_{\text{EM-SNI}}\ \sin(\omega_{\text{EM-SNI}}\, t)$, such that the combined continuous resulting signal can be represented by $v_o'(t) = v_o(t) + \gamma_{\text{EM-SNI}}(t)$. On the notation above, $\omega_m = 2\pi f_m$ and $\omega_{\text{EM-SNI}} = 2\pi f_{\text{EM-SNI}}$, where $f_m$ denotes the fundamental frequency (60 Hz) of the converter and $f_{\text{EM-SNI}}$ refers to the resulting intrusion EM-SNI resonance frequency. $V$ and $\Gamma_{\text{EM-SNI}}$ stand for the amplitude of the voltage sensor feedback signal and the amplitude of the induced EM-SNI voltage at the particular signal processing stage, respectively, as indicated in Fig. 3.

Now, assume here the relation between the $\omega_{EMS} \gg \omega_m$, such that the Fourier transform of $v_o'(t)$ is given by

$$V_o\,(\omega) \triangleq \int_{-\infty}^{\infty} v_o'(t) e^{-i\omega t}\mathrm{d}t = \int_{-\infty}^{\infty} v_o(t) e^{-i\omega_m t}\mathrm{d}t + \int_{-\infty}^{\infty} \gamma_{\text{EM-SNI}}\,(t) e^{-i\omega_{\text{EM-SNI}} t}\mathrm{d}t, \tag{4}$$

being $V_o(\omega)$ a band-limited $B$ frequency representation of $v_o'(t)$. Note here that the Fourier-transformed signal $V_o(\omega)$ will reflect the spectral characteristics of both $v(t)$ and the distortions introduced by $\gamma_{\text{EM-SNI}}\ (t)$ [19].

From the Poisson summation formula [20], the samples $v_o'(nT_s)$ of $V_o(\omega)$ are sufficient to create a period sum as follows:

$$V_{os}\,(\omega) \triangleq \sum_{k=-\infty}^{\infty} V_o\,(\omega - k f_s) = \sum_{n=-\infty}^{\infty} T_s \cdot v_o'\,(nT_s)\, e^{-i\omega n T_s}, \tag{5}$$

where $n$ and $k$ denote sampling instants. $f_s$ and $T_s$ refer to the sampling frequency (40 kHz for the ADC sampling frequency of the understudy system) and sampling period, respectively. For $v_o'(t) = v_o(t) + \gamma_{\text{EM-SNI}}\ (t)$, (5) can be expanded as

$$V_{os}\ (\omega) = \sum_{n=-\infty}^{\infty} T_s \begin{pmatrix} v_o\,(nT_s)\, e^{-i\omega_m n T_s} \\ +\ \gamma_{\text{EM-SNI}}\ (nT_s)\, e^{-i\omega_{\text{EM-SNI}}\, nT_s} \end{pmatrix}. \tag{6}$$

From (6), it can be verified that copies of $V_o(\omega)$ are combined by addition and displaced by multiples of the sampling rate $f_s$ ($\triangleq 1/T_s$). As per the summation operator, both voltage sensor feedback $v_o(t)$ and noise component $\gamma_{\text{EM-SNI}}\ (t)$ can be decoupled, allowing independent analysis of each. According to the Nyquist–Shannon sampling theorem [21], if $f_s$ is sufficiently large, the copies of a band-limited function can stay apart from one another. However, consecutive copies overlap if the Nyquist criterion is not met, making it virtually impossible to reconstruct $v_o'(t)$ from its sampled version $V_{os}(\omega)$. From the Nyquist criterion, as $f_m < \frac{f_s}{2}$, the voltage feedback fundamental frequency $v_o(t)$, and unfiltered harmonics, can be digitally reconstructed from the sum of sampled copies of $v_o(2\pi f_m - k f_s)$, with limited to no loss of information. Above $f_s/2$, where the sampled copies of the EM-SNI intrusion frequency $f_{EMS}$ are located, any resulting frequency component $f' = (2\pi f_{EM-SNI} - k f_s)$ is alike in amplitude to a lower-frequency component, known as an alias. Those aliases overwrite the sampled version of the normal voltage feedback signal, such that the digitally reconstructed signal takes the form

$$v_o'\,[n] = \underbrace{V_o \sin\left(2\pi f_m \frac{n}{f_s} + \varphi_1\right)}_{\text{normal feedback}} + \Gamma_{\text{EM-SNI}}\ \underbrace{\sin\left(2\pi f' \frac{n}{f_s} + \varphi_2\right)}_{\text{EM-SNI aliases}} \tag{7}$$

where $\varphi_1$and $\varphi_2$ denotes distinct phase displacements of the sampled version of $v_o(t)$ and $\gamma_{\text{EM-SNI}}\ (t)$ signals. Note, from Fig. 5, that the affected EM-SNI happens at the gateway of the

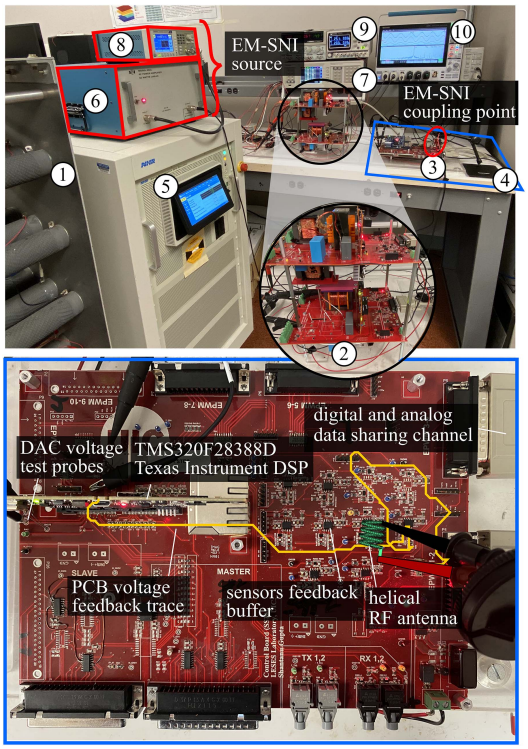



Fig. 6. Experimental setup for the study of EM-SNI impact on the SST. (1) Resistor load. (2) SST's power stage. (3) SST's control board (details in scaled version at the bottom of the picture). (4) EM-SNI intruder; R.F. antenna mechanical support. (5) Grid-simulator. (6) R.F. amplifier. (7) Power analyzer. (8) EM-SNI source function generator. (9) D.C. logic supplies. (10) Oscilloscope.

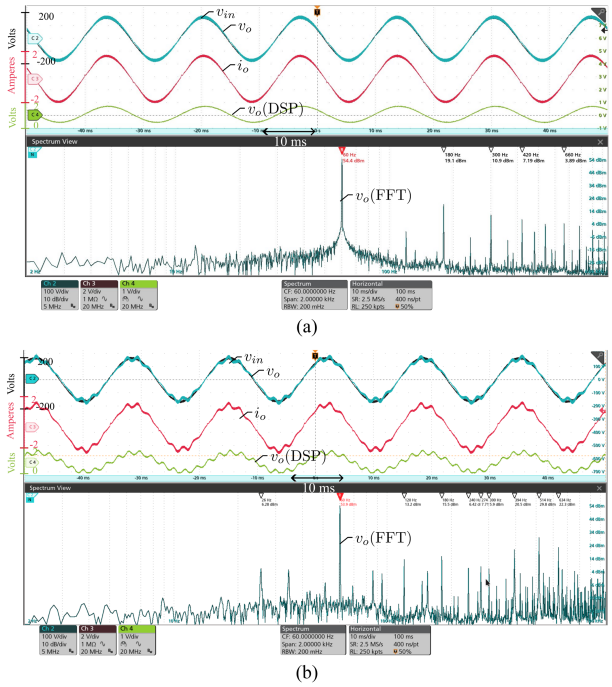



Fig. 7. Time domain and FFT results on the output voltage waveform (a) when no EM-SNI source is near the SST control board and (b) when 51.1 MHz EM-SNI source is close to the output voltage feedback of the control board.

DSP after the voltage-level translation stages, thus, reducing the energy necessary to transmit a significant level of disturbance to $v_o'[n]$, which will be digitally scaled up per the power-stage rated levels.

### B. Impact of the EM-SNI Aliasing on the SST Operation

The experimental configuration depicted in Fig. 6 was assembled to verify the impact of the discussed EM-SNI on SST performance, including the outcomes related to intrusion detection and mitigation, later discussed in Sections V and VI. The power stage entails a PAC-Ćuk DMAC SST featuring a rated power of 1 kW at an input voltage of 120 V. The converter's nominal input and output gain is unitary. Additional details of the SST experimental design are discussed in [5]. The experimental setup includes a decoupled PCB control board, which has the analog and digital signal processing stages previously discussed. The control board is highlighted at the bottom of Fig. 6. The configuration also includes a function generator, AFG1000 Function Generator, with 60 MHz bandwidth, and an ENI 550L R.F. power amplifier. This amplifier has 50 dB amplification for R.F. signals with a maximum amplitude of 1V and a bandwidth of 400 MHz. The amplifier excites the terminals of a W3100B-ND helical R.F. antenna with dimensions of 11 mm in height and 9.6 mm in width. Texas Instrument's TMS320F28379D is used as the DSP unit to digitally control, process, and generate the PWM signals for the DMAC.

The time and frequency-domain results depicted in Fig. 7 demonstrate the impact of EM-SNI on the output voltage feedback of the SST. The Figure compares the standard operational state in Fig. 7(a) to the scenario when an EM-SNI intruder source is brought into proximity with the feedback operational amplifier (OP-AMP) filtering buffer in Fig. 7(b). The time-domain waveform illustrated in green is the signal processed by digital signal processing, following a digital-to-analog conversion of the pertinent signal. The high-frequency components (MHz range) of the radiated side-channel attack are suppressed by the sampling, resulting in aliasing that overlaps the 60 Hz waveform of the fundamental feedback component. The aliasing effect is also discernible in the frequency spectrum, where amplitude peaks are identified at sub- and super-60 Hz harmonic frequencies not previously observed in nominal operating conditions.

The aliasing phenomena in the frequency domain are most relevant when analyzed through an EM-SNI frequency sweep side-by-side visualization, as depicted in Fig. 8. The heatmap highlights the peak amplitude outcomes resulting from the aliasing caused by the injection frequency variations, centered at 51.1 MHz and 50.1 MHz–50 Hz. Worth mentioning are two critical aspects regarding the results illustrated in the figure: first, the choice of the two frequencies of interest was heuristic, based on experimental visualization of the impact of EM-SNI aliasing on the output waveforms of the SST converter, while similar aliasing results can be observed at other relevant frequencies; then, the heatmap data has undergone filtering to exclude from the spectrum frequencies where the results display an amplitude

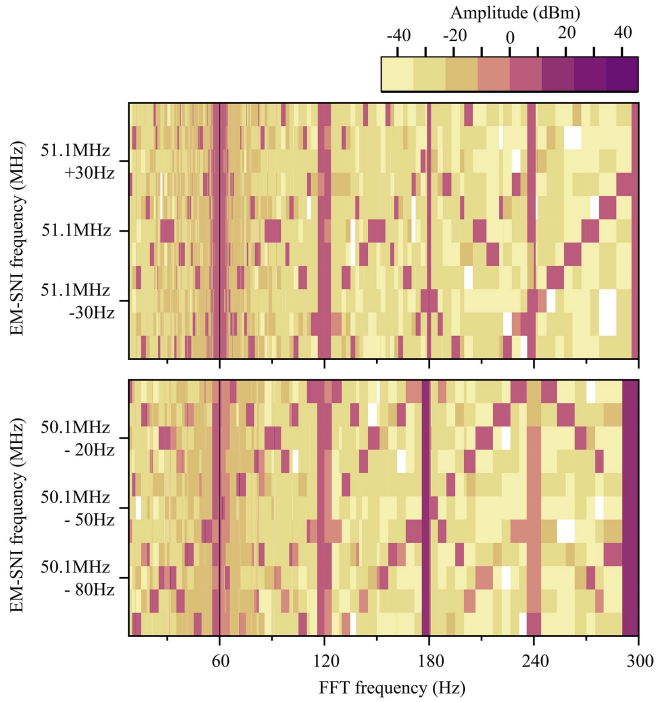



Fig. 8. Heatmap of the Fast Fourier Transform (FFT) experimental results for an EM-SNI noise frequency sweep centered into two targeted frequencies of 51.1 MHz (top plot) and 50.1 MHz–50 Hz (bottom plot).

of less than 0 dB, regardless of the EM-SNI frequency injected. The latter consideration does not affect the aliasing analysis but enhances the heatmap data visualization. The EM-SNI frequency heatmap shows darker points as aliases components in the linear displacement between the natural harmonics of the converter, which are the discernible constant lines at frequency multiples of 60 Hz. Another noteworthy observation is that the patterns are replicated as the frequency varies in a direct relationship with $f' = (2\pi f_{EM-SNI} - kf_s)$ .

A knowledgeable malicious intruder can potentially exploit the aliasing characteristics by selectively targeting frequencies of interest. The intruder can sweep the frequencies to impact the amplitude of specific natural harmonic components of the converter or to increase the THD of the ac/ac converter, leading to the failure of the SST performance during power quality assessments. The EM-SNI injection may also create load instability by amplifying the SST's input and output gain ratio. The impact of the EM-SNI on the THD and SST gain is illustrated in Fig. 9, where the EM-SNI frequency is modulated in increments of 1 MHz. In the worst-case scenario, the outcomes reveal that at an EM-SNI frequency of approximately 20 MHz, the output gain surpasses 120% of the input voltage while exhibiting a total output THD of roughly 5.5%. A reference line (in red) indicates the nominal input-output gain of the SST for this experiment, which operates with a verified total THD of 2%.

The reproducibility of the above results is contingent on several factors, including the susceptibility of energy transfer between the antenna and control board PCB traces and the maximum power transfer capability by the EM-SNI source. Thus, the impact peaks of the converter's input and output

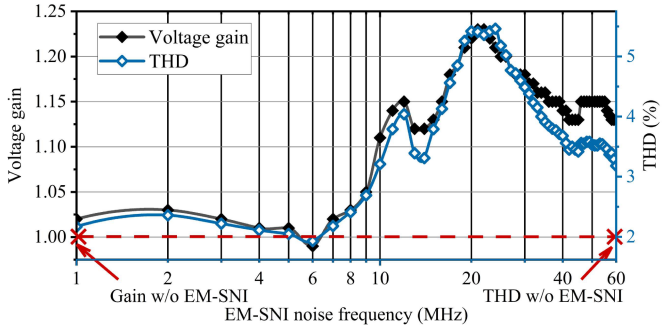



Fig. 9. Experimental results on the impact of the EM-SNI on steady-state SST performance.

gain ratio and resulting THD must be carefully considered case-by-case regarding the inherent characteristics of the devices in hand. Nevertheless, it is a matter of fact that the effects of aliasing can be verified and extrapolated to a myriad of sampling frequencies beyond the 40 kHz utilized in this study, and ultimately, the finding holds relevance across a range of applications and converters with a structure comparable to those examined herein. It is to be observed that existing antialiasing techniques are not effective in reducing the impact of irradiated EM-SNI. Despite active analog filtering being considered during the development of the SST prototype, as shown in Fig. 5, it was found to be ineffective in suppressing the high-frequency noise that propagates untethered between the measurement feedback in the signal processing board and the DSP. Digital antialiasing options, as described in [22], are limited by the CPU's maximum sampling frequency, typically in the range of a few MHz and below the EM-SNI RF bandwidth. Consequently, they are also unable to rectify the aliases-induced distortions neighboring sub- and super-60 Hz harmonics (vide Fig. 8) without affecting the SST power converter's natural frequency feedback.

## V. EM-SNI Intrusion Detection

The proposed approach for detecting intrusion via EM-SNI on the SST is based on the cross-correlation of measured signals and nominal references under normal operation. Cross-correlation measures the similarity of two signals as a function of one signal's displacement relative to the other [23]. Recently, the application of the cross-correlation method has been extended to cybersecurity analytics in cyber-physical energy systems [24], [25]. This article presents an extension of cross-correlation techniques for real-time intrusion detection in the SST system. Next, it alerts the primary controller of the SST if a signal anomaly is detected. This last step calls for an action of the mitigation algorithm, which will be discussed in Section VI. The CC-IDS formulation and functionality are explained below.

### *A. CC-IDS Background to Determine the Correlation Between Two Time-Domain Signals*

A rational approach to detecting signal anomalies is determining if (and where) they differ from normal conditions. In mathematical terms, this translates to calculating the cross-correlation between a subject signal and a baseline signal. This

baseline can be either a predefined reference signal or based on time-dispersed time-domain sampled data. The applied intrusion detection mechanism, based on cross-correlation, compares the captured sampled signal data $x'$ with a baseline $x^B$ by computing their cross-correlation coefficients. This comparison allows the detection scheme to determine the similarity between the two data sets and effectively identify potential EM-SNI intrusions. Here, $x$ may refer to either the output voltage $v_o$ or the output current $i_o$.

In this application, for the windowed output voltage measurement $\overrightarrow{x'}$ and its reference signal given by $\overrightarrow{x^B}$, their cross-correlation is given by $r_x$ as (8).

$$\overrightarrow{r_x}[l] = \sum_{n=1}^{N} \overrightarrow{x'}[n] \cdot \overrightarrow{x^B}[n-l]\,;\ l = 0, \pm 1, \pm 2, .. \tag{8}$$

Here, index '$l$' is the lag or shift in time, and $N$ is the size of the sliding buffer. Normalizing the cross-correlation of two signals helps in estimating their similarity. Thus, the normalized cross-correlation, which is termed the cross-correlation coefficient $\psi_x$ is obtained as follows:

$$\psi_x[l] = \frac{r_x[l]}{\sqrt{\overrightarrow{r_o}[0]\,\overrightarrow{r_o{}^B}[0]}} = \frac{1}{N-1}\sum_{n=1}^{N}\left[\left(\frac{\overrightarrow{x'}[n]-\mu_o}{\sigma_o}\right)\left(\frac{\overrightarrow{x^B}[n-l]-\mu_o{}^B}{\sigma_o{}^B}\right)\right]. \tag{9}$$

Here, $\overrightarrow{r_o}[0]$ and $\overrightarrow{r_o{}^B}[0]$ indicate the autocorrelation for $\overrightarrow{x'}$ and $\overrightarrow{x^{ref}}$, respectively, at zero lag. Also, $\mu_o$ and $\mu_o{}^B$ are arithmetic means while $\sigma_o$ and $\sigma_o{}^B$ are standard deviations of the captured voltage vectors $\overrightarrow{x'}$ and $\overrightarrow{x^B}$, respectively.

The cross-correlation coefficient $\psi_x$ satisfies the condition $-1 \leq \psi_x \leq 1$ and hence, provides a means to estimate the similarity of two signals, as discussed in [26]. If the measured voltage data for both the captured signals (being tested for similarity) are highly matched (strongly correlated), their cross-correlation coefficients $\psi_x$ will be 1 or close to 1 (peak at lag = 0). As the vectors become less similar (loosely correlated) and more statistically independent, the cross-correlation coefficient starts decreasing below 1 and approaching zero ($\psi_x \to 0$). In the proposed CC-IDS approach, as $\psi_x$ drops below the threshold $\xi$, it indicates a loss of correlation (similarity) between the measured voltage and the reference voltage. This deviation between $\psi_x$ and $\xi$ is used as an indicator of anomaly or presence of EM-SNI attack and is detected by using the comparison conditions in (10) as

$$\begin{aligned}(\psi_x[0] \geq \xi) &\Rightarrow \text{Normal operation}\\ (\psi_x[0] < \xi) &\Rightarrow \text{Intrusion.}\end{aligned} \tag{10}$$

The threshold $\xi$ is a system design parameter and offers a tradeoff between intrusion detection time and probability of false alarms and hence needs to be adjusted diligently. In this work, the threshold was set to 0.95 to minimize the CC-IDS's response time for almost instantaneous detection while also minimizing the occurrences of false alarms.

### B. CC-IDS Algorithm Execution Flow

The execution flow of the proposed CC-IDS algorithm is depicted in Algorithm 1. A one-line cycle of SST measured sampled signal data ($x'$) is captured using sliding window buffers. This captured voltage signal is fed to the proposed CC-IDS module along with one line-cycle of the baseline signal ($x^B$) corresponding to the SST's output side variable reference. Next, the cross-correlations and autocorrelations are estimated. Using these metrics and (9), the cross-correlation coefficients $\psi_x$ corresponding to the data measurement is estimated. These cross-correlation coefficients $\psi_x$ at the vector position zero ($l = 0$) is compared with the preset threshold '$\xi$' using the conditions in (10) to detect the presence of an EM-SNI intrusion. If the value of the computed cross-correlation coefficient $\psi_x$ decreases below the threshold $\xi$, the SST's measurement $x'$ is detected to be compromised/manipulated by an intruder. Accordingly, the CC-IDS module raises the alarm by switching its status output from a logic level low (0) to a logic level high (1). The EM-SNI mitigation strategy discussed in Section VI further utilizes this status output.

## VI. EM-SNI Mitigation

This section delves into mitigating the EM-SNI after intrusion detection. The proposed mitigation technique effectively remedies the adverse effects of EM-SNI, restoring the converter to acceptable operating levels. Meanwhile, the anomaly can be reported to higher control stages to eliminate the root cause of EM-SNI.

The proposed strategy leverages knowledge of the instantaneous power transfer characteristic of the ac/ac converter to dynamically estimate the control feedback. The estimated output voltage $\hat{v}_o[\mathrm{k}]$ is derived from a state observer that combines the feedback from the sampled output voltage $v_o'[k]$ with the control system's dynamic plant characteristics, described in (3). In the equation, the output voltage is a nonlinear function of the input voltage and the resistive load by the phase-shift displacement ratio, which is the control action that regulates the converter output. Thus, paying attention to the nonlinearities of the system, as well as the operating limits of the phase shift operator, the modified discrete version of the (3) takes the following form:

$$\hat{v}_o[\mathrm{k}] = \frac{8\,\hat{v}_{\mathrm{in}}[k]\,\hat{r}_{Load}[k]}{nZ_r\omega_r T_s} f(\delta_\varphi[k-1], T_s, \omega_r) + L(v_o[k] - \hat{v}_o[\mathrm{k}-1]). \tag{11}$$

Here, $L$ is the Luenberger observer [27] error feedback gain, and $f(\cdot)$ is a nonlinear function of the control output phase-shift operator $\delta_\phi$ computed at the instant $k-1$ and defined as

$$f(\delta_\varphi[k-1], T_s, \omega_r) = \frac{\sin\left(\delta_\varphi[k-1]\ \frac{T_s\omega_r}{2}\right)\sin\left(\frac{T_s\omega_r}{2}\ (0.5-\delta_\varphi[k-1])\right)}{\cos\left(\frac{T_s\omega_r}{4}\right)}. \tag{12}$$

**Algorithm 1:** CC-IDS Pseudo-Code.

**function** IDS $(x^B, x')$

/* capture data in a sliding window for the SST's sampled output voltage $v_o$ and the baseline reference $x^B$ */

$\left[\overrightarrow{x'}[k], \overrightarrow{x^B}[k]\right]$= **buffer.fill** $(x', x^B)$;

/* computation of the cross-correlation and autocorrelation coefficients from (8) and (9)*/

**for** $(l < N, l++)$ **do**

$\overrightarrow{r_x}[l] = \sum_{n=1}^{N} \overrightarrow{x'}[n] \cdot \overrightarrow{x^B}[n-l]$;

$\overrightarrow{r_o}[l] = \sum_{n=1}^{N} \overrightarrow{x'}[n] \cdot \overrightarrow{x'}[n-l]$;

$\overrightarrow{r_o{}^B}[l] = \sum_{n=1}^{N} \overrightarrow{x^B}[n] \cdot \overrightarrow{x^B}[n-l]$;

**end**

/* computation of the correlation coefficients from (9).*/

$$\psi_x[0] = \frac{r_x[0]}{\sqrt{\overrightarrow{r_o}[0]\overrightarrow{r_o{}^B}[0]}}$$

/* compare cross-correlation to threshold ($\xi$) */

**if** $(\psi_x[0] < \xi)$ **then**

IDS flag = 1;

**end**

/* activate the mitigation algorithm */

$\left[\hat{v}_o[k]\right]$= **mitigation** $\left(v_o[k], \hat{v}_{\text{in}}[k], \hat{r}_{Load}[k], \delta_\varphi[k-1]\right)$;

**end**

In (11), unlike its steady-state representation in (3), the converter's output resistance $\hat{r}_{Load}[k] = V_o/I_o$ is estimated in real-time based on the output voltage and current amplitudes to allow dynamic adaptation to load variations. The second-order generalized integrators (SOGI) 60 Hz filter with direct and quadrature components is leveraged [28] to extract the amplitude of the converter's output voltage $V_o$ and current $I_o$. Similarly, the input voltage $\hat{v}_{\text{in}}[k] = V_{in}\sin(\omega_m\, kT_s)$ is estimated from the peak detector and phase-locked digitally generated sinewave coming from the SRF-PLL. The real-time estimation of the input voltage provides an extra degree of noise [16] due to the untethered propagation of the EM-SNI between the different sensors on the printed circuit control board.

To avoid control-loop instability due to $k$-instant estimation of the output voltage, the control loop must be obtained as a prediction of $\hat{v}_o[k]$. The next-step prediction is attained from the Lagrange interpolation formula [29] such that

$$\hat{v}_o[k+1] = \sum_{i=0}^{n} (-1)^{n-l} \left(\frac{(n+1)!}{i!\,(i-l+1)!}\right) \hat{v}_o[k+i-n]\,. \tag{13}$$

Using $n = 2$, the linear prediction applied to the $\hat{v}_o$ leads to a next-step prediction

$$\hat{v}_o[k+1] = 3\hat{v}_o[k] - 3\hat{v}_o[k-1] + \hat{v}_o[k-2]\,. \tag{14}$$

Here, the compromised sensor readings of the output voltage feedback $v_o'$ are replaced by estimated sensor values in the control portrayed in Fig. 2 to temporarily mitigate the attack's impact and thus ensure attack-resilient operation.

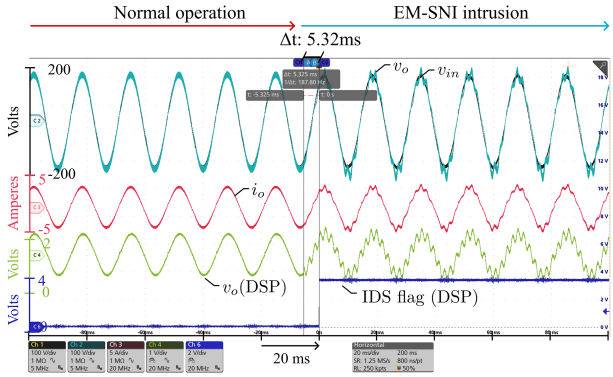



Fig. 10. Experimental results indicating the CC-IDS mechanism detecting intrusion for 51.1 MHz EM-SNI noise injection within 5.325 ms.

## VII. Experimental Results on the SST Resilient Operation

The experimental results described hereby concern the resilient operation of the SST given the proposed CC-IDS and mitigation strategies subject to EM-SNI interference, as described in Sections V and VI, respectively. The experimental results presented here were obtained using the same experimental prototype and operating conditions described in Section IV-B.

### A. Results on the CC-IDS Mechanism

Based on the findings of Section IV-B, it was empirically observed that the aliasing was dominant for some specific noise frequencies, namely 48.5 MHz, 49.1 MHz, 50.5 MHz, and 51.1 MHz, near the maximum bandwidth of the experimental function generator unit (60 MHz), for which the CC-IDS mechanism's ability to detect the EM-SNI intrusions timely is here discussed.

Fig. 10 presents the time-domain experimental results obtained for the SST's operation before and after injection of the EM noise. Fig. 10 displays the SST's voltages and currents for one of the aforementioned EM-SNI frequencies (51.1 MHz). The left half of the plot shows the normal operation of the SST, while the right half of the scope indicates the operation under EM-SNI. The light blue and black sinusoidal plots represent the SST's input/output voltages, while the pink plot represents the SST's output current. The green plot represents the voltage feedback distorted by the injected 51.1 MHz noise signal (as discussed in Section IV-B). Finally, the deep blue plot at the bottom represents the output of the CC-IDS mechanism (IDS flag). As observed, after the noise is injected in the voltage feedback, the CC-IDS mechanism detects this intrusion and changes the status of its IDS flag from logic low (0) to logic high (1) within 5.325 ms.

To investigate the reproducibility of the CC-IDS's intrusion detection, the above procedure was repeated for ten iterations of a few dominant EM-SNI frequencies with results described by the Weibull [30] probability plots in Fig. 11. The cumulative distribution function (CDF) can be interpreted as the

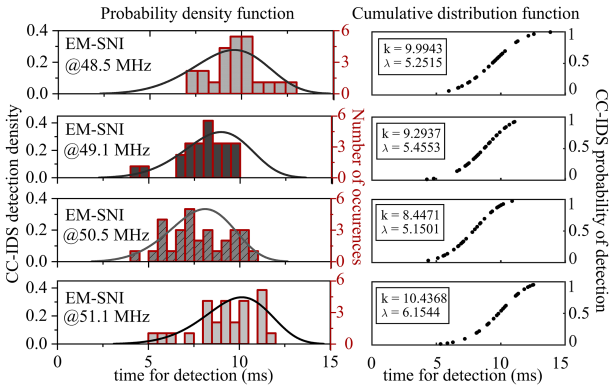



Fig. 11. CC-IDS mechanism's intrusion detection times probability of distribution and cumulative distribution functions from the number of detection occurrences when EM-SNI noise at 48.5, 49.1, 50.5, and 51.1 MHz is injected on the voltage feedback in the SST.

chance of successfully detecting alias noise at a given EM-SNI frequency after a certain time has elapsed since the intrusion. The function is computed from $f(i,k,\lambda) = 1 - e^{-(i/\lambda)^k}$, where $i$ is the sampled detection time with $k$ and $\lambda$ being the shape and scale parameters of the Weibull distribution, respectively. In all cases, the detection occurrence time was within 12 ms.

### B. Results of the EM-SNI Mitigation Strategy

Fig. 12 depicts the time-domain results of the proposed EM-SNI mitigation. Fig. 12(a) illustrates the introduction of an EM-SNI at a frequency of 51.1 MHz, close to the feedback buffers of the input and output voltage sensors of the ac/ac converter. With a similar mechanism, Fig. 12(b) illustrates the results of EM-SNI intrusion at 20.2 MHz. At this later frequency, as previously discussed in Fig. 9, the highest degree of energy transfer/coupling between the antenna traces and the PCB traces is verified. Similar to what is described in Section IV, the feedback signal $v_o[k]$ observed by the DSP is highlighted in green and persists with the effects of the EM-SNI even after the mitigation algorithm becomes active. Notably, the aliasing effects of EM-SNI distortions in the control feedback almost immediately impact the output voltage (in light blue) and the output current (in red). The CC-IDS algorithm successfully detects the intrusion, and following the processing of this information, the mitigation algorithm commences its action, as indicated by the rise of the logical level of the "mitigation flag". The feedback signal is then replaced by the filtered prediction of the output voltage obtained from the combination of (14) and (11). The slight difference in the input and output voltage regulation before and after the mitigation algorithm is active suggests that the converter remains under the influence of the intrusion and can be explained by an inaccurate estimate of the amplitude of the input voltage $\hat{v}_{\text{in}}[k]$. It is pertinent to mention that although there is no change in the intensity of the EM-SNI, the waveform is much cleaner, with the alias effects considerably attenuated.

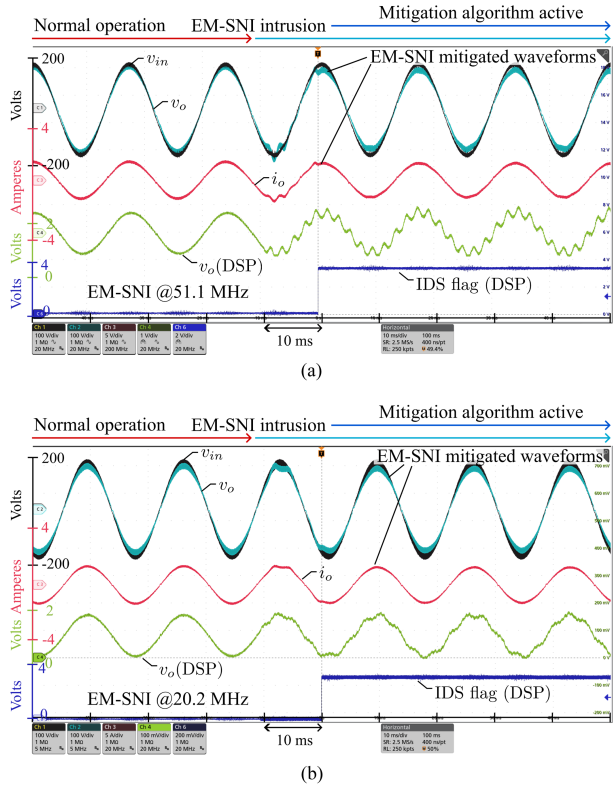



Fig. 12. Time-domain experimental verification effectiveness of the CC-IDS and mitigation strategy to compensate for deviations in the output voltage feedback for EM-SNI. (a) 51.1 MHz. (b) 20.2 MHz.

The spectral performance of the mitigation strategy for an EM-SNI intrusion frequency of 51.1 MHz and 20.2 MHz is depicted in Fig. 13. Under EM-SNI conditions and nominal control operation—the FFT amplitude trace in black—, sub-, and super-60 Hz harmonic components in close proximity to the fundamental frequency can be verified. In Fig. 13(a), the EM-SNI intrusion at 51.1 MHz results in stronger super-60 alias components whose impact is effectively damped with the proposed mitigation. In Fig. 13(b), lower frequency aliases are verified and effectually mitigated with EM-SNI of 20.2 MHz. Note that the DMAC converter exhibits odd harmonic components ($3^{\text{rd}}$, $5^{\text{th}}$, $7^{\text{th}}$, $9^{\text{th}}$, ...), which are still present after the mitigation strategy. Thus, it is observed that the proposed mitigation strategy effectively reduces the amplitude of alias frequencies introduced by EM-SNI while preserving the inherent signature of the DMAC SST converter.

### C. Performance of the Mitigation Strategy to Dynamic Variations on the Load

A step variation in the load (62–45 Ω) was implemented to ascertain the dynamic validity of the converter's output voltage predictions while an EM-SNI at 51.1 MHz, akin to the one depicted in Fig. 12, persisted without respite. The time-domain results, depicted in Fig. 14, show that the voltage is dynamically updated to the new load level, thereby preserving the ac/ac input to output voltage gain in a steady state. The inertia exhibited in updating the voltage to the new load level is due to variations in

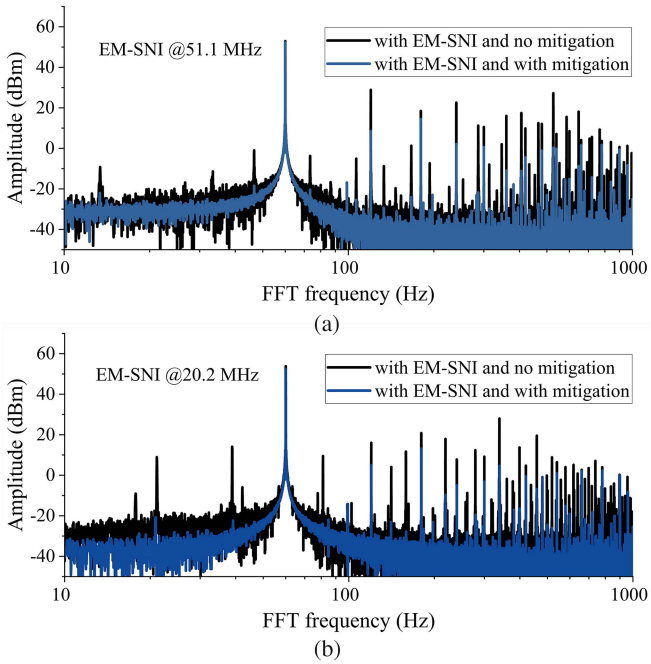



Fig. 13. Comparison of the frequency spectrum response for EM-SNI intrusion with and without the proposed mitigation strategy for EM-SNI intrusions. (a) 51.1 MHz. (b) 20.2 MHz.

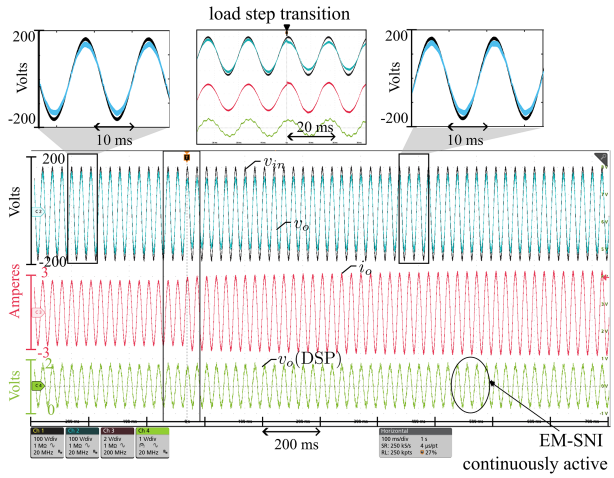



Fig. 14. Experimental verification of the proposed mitigation algorithm subject to EM-SNI interference and load transient conditions variation from 62 to 45 Ω.

constraints imposed on the $\hat{r}_{Load}[k]$ update in (11). The phase shift displacement to the output voltage relationship for both load levels whilst being subject to noise, is presented in the phase portrait of Fig. 15(a). Note that the phase displacement absorbs a fraction of the aliasing content of the EM-SNI intrusion. In contrast, the output voltage is regulated to a constant steady-state condition, irrespective of the load condition. Despite the EM-SNI intrusion, the input voltage to output voltage ratio remains steady, irrespective of the load, as evident in the phase portrait in Fig. 15(b).

The results presented above demonstrate the effectiveness of the mitigation strategy in both dynamic and steady-state scenarios, even when faced with varying resistive load conditions. However, it is important to note that the strategy's

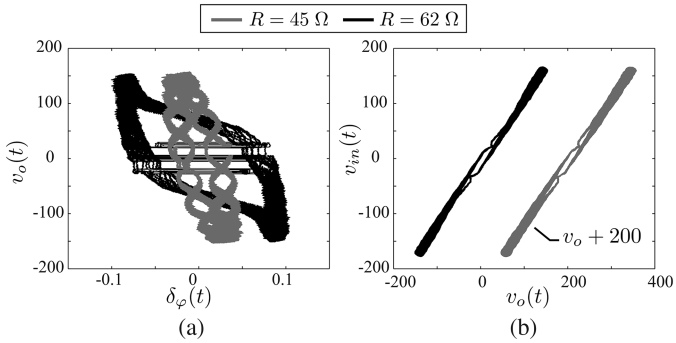



Fig. 15. (a) Phase-portrait on the steady-state performance of $v_o(t)$ to variations on $\delta_\varphi(t)$ and (b) phase-portrait on the steady-state performance of $v_{in}(t)$ by $v_o(t)$.

response to sudden changes in the SST output may be slower than typical feedback due to real-time load estimation. As such, it is recommended to revert to the control state prior to the intrusion condition once the EM-SNI is no longer detected.

## VIII. Conclusion

This study presents an empirical investigation into the adverse effects of electromagnetic radiated intrusion on the control feedback of an SST. The findings reveal that by exploiting the effects of aliasing, a malicious intruder can inject noise components into the converter's nominal feedback, potentially leading to catastrophic consequences in the SST output voltage regulation. Notably, the intrusion can be carried out using radio frequency wavelength in the MHz range, resulting in sub- and super-60 Hz harmonics in the output variables. To counter such threats, intrusion detection and mitigation solutions must leverage specific knowledge of the converter's behavior, emphasizing that a sufficiently accurate model must be dynamically evaluated to ensure resilient operation. The study concludes that the results obtained herein can also be verified for power converters of different natures and power ranges, albeit with due consideration to their dynamic characteristics.

Sections V and VI provided a solution to counteract and mitigate the adverse effects of EM-SNI on the SST performance. This is done by implementing a resilient mechanism in the cyber layer. Alternatively, physical layer solutions like EMC tools and filtering techniques could be considered to reduce the impact of EM-SNI. Nevertheless, several factors would need to be considered, such as the impedance of the PCB traces [31], the parasitic parameters of the components [32], and the high-frequency performance of the magnetic material [33], making this physical design-based alternative convoluted.

The experimental results in Section VII confirm the validity of the proposed SST's resilient operation against EM-SNI-type intrusions. It should be noted that the selection of cases and frequencies for validating intrusion detection and mitigation strategies were carefully chosen to underscore the efficacy of the proposed strategy. The dominant frequency components pointed out in Section VII were probed to result in evident low-frequency signatures of alias components from the $v(2\pi f_{\text{EM-SNI}} - kf_s)$ voltage measurement feedback. It is worth mentioning that numerous other frequencies of the EM-SNI could also have an

impact on the SST. The intrusion mechanism's proximity of the coupling channels (EM-SNI source antenna and PCB traces), antenna projection angle, and induced voltage magnitude are all pertinent factors that can induce milder or more severe effects on the physical variables of the SST. From the results discussed in Fig. 9 and empirical observation, it was verified that the EM-SNI produced a significant impact above the 10 MHz intrusion band, where we concentrated the analysis of this article.

Although physically-oriented *flight-by-light* photonically controlled solutions for electronics and semiconductor switching devices could hold significant potential for providing immunity against electromagnetic interference in power electronics systems [34], it is currently observed that cyber-oriented solutions, like the one presented in this work, are gaining more traction in academic discourse. Along those lines, active EMI noise cancellation solutions for power electronics systems also hold promise in interrupting the operation of EM-SNI. However, those approaches are currently limited to suppressing EMI in known band-limited frequency ranges and have only been applied to periodic and quasi-periodic disturbances thus far [35]. Our findings herein conclusively established that the CC-IDS is a highly efficient system capable of detecting and activating the mitigation algorithm within an average time of 5 to 6 ms, with a maximum limit of 15 ms. This enables the root cause of the intrusion to be effectively isolated and removed from operational units without any adverse impact on the performance of the SST. Provided that the experimental results on the resilient strategy account for linear load conditions, a brief discussion on the extension of the CC-IDS algorithm applied to nonlinear load conditions is presented in the Appendix.

## Appendix
## CC-IDS Under Nonlinear Load Conditions

The results presented above indicate the effectiveness of the detection strategy against EM-SNI intrusion in voltage feedback with resistive load. In this scenario, the CC-IDS compares the sampled signal data with a predefined internal reference signal by measuring the similarity between the two signals and computing their cross-correlation coefficients, given the expected linear behavior of the voltage forms at the output. Alternatively, the baseline signal can be compared with time-dispersed sample data to detect any EM-SNI-induced changes in SST behavior. This second alternative is especially interesting under highly nonlinear load conditions, where the load itself can induce natural distortions on the output voltage and current waveforms, such as illustrated in Fig. 16. Both voltage and current waveforms can be utilized to avoid false triggering, given that the EM-SNI effects as an intrusion on the voltage feedback must also be subsequently verified on the current waveform.

The proposed CC-IDS mechanism is then designed to work as follows: 1) data collection of voltage and/or current measurements from SST cells and DSP memory buffer of the captured data; 2) the baseline comparison defined—specifically, the cross-correlation between time-dispersed voltage and/or current measurements and most current sampled captured data; 3) next, the cross-correlation analysis is performed on the data collected in step 1, and 4) finally, potential anomalies can be detected

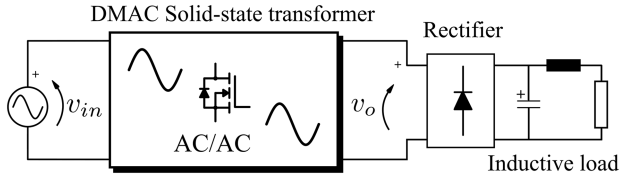



Fig. 16. Diagram of the DMAC SST with nonlinear inductive load.

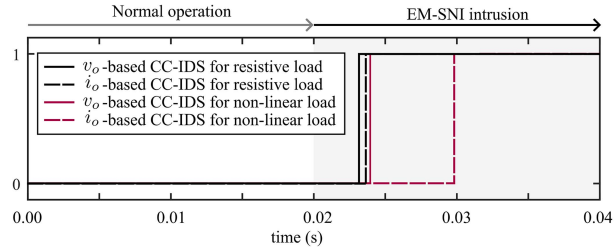



Fig. 17. Simulated comparison of the detection-time performance of the CC-IDS detection flag under nominal resistive load and nonlinear load conditions.

in this step, which is attained by comparison of the real-time cross-correlation results against predefined a threshold.

The simulation results in Fig. 17 demonstrate the efficacy of CC-IDS in detecting linear and nonlinear loads using two distinct techniques. The first method, for resistive load (with results in black), employs a predefined internal reference, while the second approach, considering a nonlinear load (with results in red), relies on time-dispersed sampled data. Note that the second method exhibits a longer detection time for nonlinear loads due to the time-dispersed baseline reference. These observations highlight the significance of selecting an appropriate detection method that accounts for the characteristics of the loads being monitored.

## References

[1] J. Selvaraj, G. Y. Dayanıklı, N. P. Gaunkar, D. Ware, R. M. Gerdes, and M. Mina, "Electromagnetic induction attacks against embedded systems," in *Proc. Asia Conf. Comput. Commun. Secur.*, 2018, pp. 499–510, doi: 10.1145/3196494.3196556.

[2] A. Barua and M. A. Al Faruque, "Special session: Noninvasive sensor-spoofing attacks on embedded and cyber-physical systems," in *Proc. IEEE 38th Int. Conf. Comput. Des.*, 2020, pp. 45–48, doi: 10.1109/ICCD50377.2020.00024.

[3] H.-W. Wu, H.-J. Chen, H.-F. Xu, R.-H. Fan, and Y. Li, "Tunable multiband directional electromagnetic scattering from spoof Mie resonant structure," *Sci Rep*, vol. 8, no. 1, Jun. 2018, Art. no. 8817, doi: 10.1038/s41598-018-27268-6.

[4] Y. Zhang and K. Rasmussen, "Detection of electromagnetic interference attacks on sensor systems," in *Proc. IEEE Symp. Secur. Privacy*, 2020, pp. 203–216, doi: 10.1109/SP40000.2020.00001.

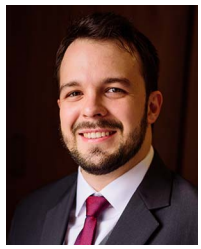
[5] S. Gupta and S. K. Mazumder, "A differential-mode isolated AC/AC converter," *IEEE Trans Power Electron*, vol. 38, no. 10, pp. 12846–12858, Oct. 2023, doi: 10.1109/TPEL.2023.3292983.

[6] P. Szcześniak, J. Kaniewski, and M. Jarnut, "A.C.–A.C. power electronic converters without D.C. energy storage: A review," *Energy Convers Manag*, vol. 92, pp. 483–497, Mar. 2015, doi: 10.1016/j.enconman.2014.12.073.

[7] N. Gajanur, M. D. R. Greidanus, S. K. Mazumder, and M. A. Abbaszada, "Impact and mitigation of high-frequency side-channel noise intrusion on the low-frequency performance of an inverter," *IEEE Trans Power Electron*, vol. 37, no. 10, pp. 11481–11485, Oct. 2022, doi: 10.1109/TPEL.2022.3170885.

[8] B. Ahn et al., "An overview of cyber-resilient smart inverters based on practical attack models," *IEEE Trans Power Electron*, pp. 1–18, Apr. 2024, doi: 10.1109/TPEL.2023.3342842.

[9] N. Mtukushe, A. K. Onaolapo, A. Aluko, and D. G. Dorrell, "Review of cyberattack implementation, detection, and mitigation methods in cyber-physical systems," *Energies (Basel)*, vol. 16, no. 13, Jul. 2023, Art. no. 5206, doi: 10.3390/en16135206.
[10] S. A. M. Saleh et al., "Solid-State transformers for Distribution Systems–Part I: Technology and construction," *IEEE Trans Ind Appl*, vol. 55, no. 5, pp. 4524–4535, Sep. 2019, doi: 10.1109/TIA.2019.2923163.
[11] M. A. Hannan et al., "State of the art of solid-State transformers: Advanced topologies, implementation issues, recent progress and improvements," *IEEE Access*, vol. 8, pp. 19113–19132, 2020, doi: 10.1109/ACCESS.2020.2967345.
[12] S. Gupta and S. K. Mazumder, "Analysis of resonant PWM active-clamp Ćuk DC/DC converter," in *Proc. IEEE Appl. Power Electron. Conf. Expo.*, 2023, pp. 2170–2176, doi: 10.1109/APEC43580.2023.10131318.
[13] B. K. Johnson and G. Venkataramanan, "A hybrid solid state phase shifter using PWM AC converters," *IEEE Trans. Power Del.*, vol. 13, no. 4, pp. 1316–1321, Oct. 1998, doi: 10.1109/61.714502.
[14] H. Qin and J. W. Kimball, "Solid-State transformer architecture using A.C.–AC dual-active-bridge converter," *IEEE Trans. Ind. Electron.*, vol. 60, no. 9, pp. 3720–3730, Sep. 2013, doi: 10.1109/TIE.2012.2204710.
[15] M. A. Tawfik, M. Ehab, A. Ahmed, and J.-H. Park, "Single-stage isolated AC/AC converter with phase-shifted controller," *IEEE J Emerg Sel Top Power Electron*, vol. 11, no. 2, pp. 1815–1826, Apr. 2023, doi: 10.1109/JESTPE.2022.3219023.
[16] S. Golestan and J. M. Guerrero, "Conventional synchronous reference frame phase-locked loop is an adaptive complex filter," *IEEE Trans. Ind. Electron.*, vol. 62, no. 3, pp. 1679–1682, Mar. 2015, doi: 10.1109/TIE.2014.2341594.
[17] H. Nakano, Y. Okabe, H. Mimaki, and J. Yamauchi, "A monofilar spiral antenna excited through a helical wire," *IEEE Trans Antennas Propag*, vol. 51, no. 3, pp. 661–664, Mar. 2003, doi: 10.1109/TAP.2003.809865.
[18] H. Shall, Z. Riah, and M. Kadi, "A novel approach for modeling near-field coupling with PCB traces," *IEEE Trans Electromagn Compat*, vol. 56, no. 5, pp. 1194–1201, Oct. 2014, doi: 10.1109/TEMC.2014.2304306.
[19] J. W. Kirchner, "Aliasing in 1/fαnoise spectra: Origins, consequences, and remedies," *Phys Rev E*, vol. 71, no. 6, Jun. 2005, Art. no. 066110, doi: 10.1103/PhysRevE.71.066110.
[20] A. Napolitano, "Almost-cyclostationary signal processing," in *Cyclostationary Processes and Time Series*, Amsterdam, The Netherlands: Elsevier, 2020, pp. 81–131, doi: 10.1016/B978-0-08-102708-0.00014-5.
[21] B. P. Lathi and R. Green, *Linear Systems and Signals*, 3rd ed. London, U.K.: Oxford Univ. Press, 2017.
[22] S. He, D. Zhou, X. Wang, Z. Zhao, and F. Blaabjerg, "A review of multisampling techniques in power electronics applications," *IEEE Trans Power Electron*, vol. 37, no. 9, pp. 10514–10533, Sep. 2022, doi: 10.1109/TPEL.2022.3169662.
[23] P. Tahmasebi, A. Hezarkhani, and M. Sahimi, "Multiple-point geostatistical modeling based on the cross-correlation functions," *Comput Geosci*, vol. 16, no. 3, pp. 779–797, Jun. 2012, doi: 10.1007/s10596-012-9287-1.
[24] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Trans Smart Grid*, vol. 6, no. 6, pp. 3104–3113, Nov. 2015, doi: 10.1109/TSG.2015.2409775.
[25] P. Haller and B. Genge, "Using sensitivity analysis and Cross-association for the design of intrusion detection systems in Industrial cyber-physical systems," *IEEE Access*, vol. 5, pp. 9336–9347, 2017, doi: 10.1109/ACCESS.2017.2703906.
[26] S. Gupta et al., "Cyber resiliency of a solid-state power substation," in *Proc. IEEE Appl. Power Electron. Conf. Expo.*, Long Beach, CA, USA, 2024.
[27] H. Gholami-Khesht, P. Davari, and F. Blaabjerg, "Adaptive control in power electronic systems," in *Control of Power Electronic Converters and Systems*, Amsterdam, The Netherlands: Elsevier, 2021, pp. 125–147, doi: 10.1016/B978-0-12-819432-4.00008-1.
[28] P. Rodriguez, A. Luna, I. Candela, R. Teodorescu, and F. Blaabjerg, "Grid synchronization of power converters using multiple second order generalized integrators," in *Proc. 34th Annu. Conf. IEEE Ind. Electron.*, 2008, pp. 755–760, doi: 10.1109/IECON.2008.4758048.
[29] O. Kukrer, "Discrete-time current control of voltage-fed three-phase PWM inverters," *IEEE Trans Power Electron*, vol. 11, no. 2, pp. 260–269, Mar. 1996, doi: 10.1109/63.486174.
[30] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes*, 4th ed. New York, NY, USA: McGraw-Hill Education, 2001.
[31] J. Yao, S. Wang, and Z. Luo, "Modeling, analysis, and reduction of radiated EMI due to the voltage across input and output cables in an automotive non-isolated power converter," *IEEE Trans Power Electron*, vol. 37, no. 5, pp. 5455–5465, May 2022, doi: 10.1109/TPEL.2021.3128628.
[32] S. Wang, J. D. van Wyk, and F. C. Lee, "Effects of interactions between filter parasitics and power interconnects on EMI filter performance," *IEEE Trans. Ind. Electron.*, vol. 54, no. 6, pp. 3344–3352, Dec. 2007, doi: 10.1109/TIE.2007.906126.
[33] S. Wang, F. C. Lee, and J. D. van Wyk, "Design of inductor winding capacitance cancellation for EMI suppression," *IEEE Trans Power Electron*, vol. 21, no. 6, pp. 1825–1832, Nov. 2006, doi: 10.1109/TPEL.2006.882898.
[34] S. K. Mazumder and T. Sarkar, "Optically-triggered power transistor (OTPT) for fly-by-light (FBL) and EMI-susceptible power electronics: Plenary paper," in *Proc. 37th IEEE Power Electron. Specialists Conf.*, 2006, pp. 1–8, doi: 10.1109/pesc.2006.1711731.
[35] A. Bendicks, T. Dorlemann, T. Osterburg, and S. Frei, "Active cancellation of periodic EMI of power electronic systems by injecting artificially synthesized signals," *IEEE Electromagn Compat Mag*, vol. 9, no. 3, pp. 63–72, Jul.–Sep. 2020, doi: 10.1109/MEMC.2020.9241554.



**Mateo D. Roig Greidanus** (Graduate Student Member, IEEE) received the B.E. and M.S. degree in electrical engineering from the Federal University of Santa Catarina (UFSC), Florianópolis, Brazil, in 2018 and 2020, respectively. He is currently working toward the Ph.D. degree in electrical and computer engineering with the Laboratory for Energy and Switching-Electronic Systems (LESES), University of Illinois Chicago (UIC), Chicago, IL, USA. His research interests include ac stability of power electronics systems, renewable energy integration, and cyber–physical security of power electronic-dominated grids.

**Silvanus D'Silva** (Graduate Student Member, IEEE) received the Bachelors degree in electronics and telecommunication engineering from University of Mumbai, Mumbai, India, he received the M.Sc. degree in electrical engineering from Kansas State University, Manhattan, KS, USA, in 2020. He is currently working toward the Ph.D. degree in electrical engineering with the University of Illinois Chicago (UIC), Chicago, IL, USA. UIC.

He was a Visiting Scholar with the TEES lab managed by the Smart Grid Centre in Texas A&M University, Ar Rayyan, Qatar, until August 2021. He joined the IPEG Research Group with the University of Illinois Chicago, IL, USA, in August 2021. He was the Financial Chair of the First Kansas Power and Energy Conference (KPEC20), K.S. He is the Local Organizing Chair of 50th Annual Conference of the IEEE Industrial Electronics Society (IECON 2024), Chicago, IL. USA.

**Shantanu Gupta** (Graduate Student Member, IEEE) received the B.Tech. degree in electrical engineering from Delhi Technological University, Delhi, India, in 2016. He is currently working toward the Ph.D. degree in electrical and computer engineering at the University of Illinois Chicago, Chicago, IL, USA.

From 2016 to 2019, he was a Research Engineer with TEX E.G., Japan. His work involved working on embedded and power electronics systems. Among the projects he worked on were the development of a semiconductor wafer alignment machine and a motor driver for a refrigerator compressor. His research interests include design, modeling, and control of high efficiency power electronics converters, solid-state transformers, and electric vehicle chargers.

Mr. Gupta is a reviewer for IEEE TRANSACTIONS ON POWER ELECCTRONICS IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS.

**Debotrinya Sur** (Graduate Student Member, IEEE) received the B.Tech. degree in electrical engineering from the Indian Institute of Engineering Science and Technology, Shibpur, India, in 2023.

He is currently working toward the Ph.D. degree in electrical and computer engineering with the University of Illinois Chicago, located in Chicago, IL, USA. His research interests include designing, modeling, and controlling power electronics converters.

**Sudip K. Mazumder** (Fellow, IEEE) received the Ph.D. degree in electrical and computer engineering from Virginia Tech, Virginia, Va, USA, in 2001.

He is an UIC Distinguished Professor and the Director of Laboratory for Energy and Switching-Electronic Systems (LESES) with the Department of Electrical and Computer Engineering, University of Illinois Chicago (UIC). He has over 30 years of professional experience and has held R&D and design positions in leading industrial organizations and he was a Technical Consultant for several industries. He is the President of NextWatt LLC.

Dr. Mazumder is the recipient of the 2023 IEEE Power & Energy Society's Ramakumar Family Renewable Energy Excellence Award, IEEE awards/honors, including IEEE TRANSACTIONS ON POWER ELECTRONICS Prize Paper Awards (2022, 2002) and Highlighted Papers (2023, 2022, 2018), Featured Article for IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING (2023), IEEE Conference Best Paper Award (2013), and IEEE International Future Energy Challenge Award (2005). He was a Fellow of the American Association for the Advancement of Science (AAAS), in 2020, a Fellow of the Institute of Electrical and Electronics Engineers (IEEE), in 2016, and a Fellow of the Asia-Pacific Artificial Intelligence Association (AAIA) in 2022. He is an Editor in Large for the IEEE TRANSACTIONS ON POWER ELECTRONICS (TPEL) since 2019 and He has been an Administrative Committee Member for IEEE PELS, since 2015. He has also been a Member-at-Large for IEEE PELS, since 2020. He was the Chair for the IEEE PELS Technical Committee on Sustainable Energy Systems, from 2015 to 2020. He was the General Chair for IEEE PEDG Conference in 2023 and the General Co-Chair for IEEE Energy Conversion Congress & Exposition (ECCE) in 2024.

**Mohammad B. Shadmand** (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Texas A&M University, College Station, TX, USA, in 2015.

Since 2020, he is an Assistant Professor with the University of Illinois, Chicago, IL, USA.

From 2017 to 2020, he was an Assistant Professor with the Department of Electrical and Computer Engineering, Kansas State University, Manhattan, KS, USA.

Dr. Shadmand was the recipient of the Michelle Munson Serban Simu Keystone Research Scholar, Kansas State University, in 2017 and the 2019 IEEE Myron Zucker Faculty-Student Research Grant. He has been the recipient of multiple best paper awards at different IEEE conferences. He is the General Chair of the 50th Annual Conference of the IEEE Industrial Electronics Society (IECON 2024), Chicago, IL, USA. He is an Associate Editor for IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, IEEE TRANSACTIONS ON INDUSTRY APPLICATION, and *IET Renewable Power Generation*.