Letters

Diffusion of Radiated Side-Channel Noise Intrusion in PLL-Dependent Cascaded Solid-State Transformers

Mateo D. Roig Greidanus, *Graduate Student Member, IEEE*, Shantanu Gupta, *Graduate Student Member, IEEE*, Debotrinya Sur, *Graduate Student Member, IEEE*, and Sudip K. Mazumder, *Fellow, IEEE*

***Abstract*—Solid-state transformers (SSTs) rely on adequately functioning the closed-loop control and measurement feedback variables. Due to physical coupling, a network of SSTs is vulnerable to the diffusion of cyberattacks and their impact on the system's stability. AC–AC-type SSTs, in particular, rely heavily on control synchronization, and any fluctuations can quickly lead to system instability. In this letter, we explore the impact of radiated side-channel noise intrusion (SNI) diffusion on cascaded SSTs when such an attack is tuned to affect the fundamental coupling frequency. Experimental results, supported by analytical discussion, describe the effects and impact of radiated SNI on the stability of the phase-locked loop control and the overall system. Furthermore, we propose an intrusion detection strategy that responds rapidly to attacks in such circumstances.**

***Index Terms*—Cyberattack, diffusion, intrusion detection, phase-locked loop (PLL), radiated electromagnetic (EM) interference.**

I. Introduction

THE impact and mechanism of electromagnetic side-channel noise intrusion (EM-SNI) have been recently discussed in [1] as a threat to the closed-loop performance of solid-state transformer (SST) systems. SST converters are known for their modularity, allowing voltage and current scalability [2]. However, there is a concern that as these modules are scaled up, cyberattacks may spread between them. This is because if the signals responsible for synchronization and voltage balancing are tampered with within a discrete module, it could impact the entire SST's performance. The impact of side-channel noise intrusion (SNI)-type attacks [1] in a network of SSTs is still an open-ended issue that requires further attention.

In [3], the effects of false data injection attacks on modular multilevel converters were examined. It demonstrated that such cyberattacks have the potential to spread through the physical layer, resulting in an unstable operation, even with distributed control strategies. The effects of SNI on a converter network motivated a discussion in [4] on the possible ramifications of tampering with measurement feedback with regard to the closed-loop performance of self-synchronizing inverters. In the latter, the implemented control strategy resonates with a 60-Hz limit cycle to ensure synchronism while rejecting disturbances apart from it. Similarly, this letter considers a network of cascaded SST modules with a 60-Hz resonant compensation for voltage balancing control to reject sub- and super-60-Hz alias disturbances presented in [1]. While studying the effect of SNI diffusion in cascaded SSTs, the authors of this letter identified that amplitude modulation (AM)-based SNI attacks, targeting the bandwidth of phase-locked loop (PLL) lock-in frequency, can result in instability and chaotic impact on the cascaded operation waveforms. An analytical discussion on the impact of the AM-radiated SNI cyberattack on the frequency spectrum and the stability of the PLL is provided in Sections II and III, respectively. Section IV introduces a novel intrusion detection system (IDS) methodology, which uses amplified noise quantification to quickly identify the adverse effects of AM-based SNI attacks on the experimental setup. Finally, in Section V, we document the observed impact and diffusion of these attacks on cascaded SSTs, as in a configuration outlined in Fig. 1. These results are accompanied by a validation of the proposed IDS in such an attack scenario.

II. AM of the Radiated SNI

Herein, we delve into the cyber-physical attack mechanism comprising an AM-radiated SNI that affects the voltage measurement feedback of the SST. Consider the time-domain representation of a voltage sensor feedback described by $v(t) = V \sin(2\pi f_n t)$, where V refers to the amplitude of the measurement feedback and f_n denotes the fundamental frequency $(60\,\text{Hz})$ of the converter. This voltage feedback is distorted by a radiated electromagnetic (EM) source of noise represented by $\rho(t)$, such that the resulting feedback signal is represented by $v'(t) = v(t) + \rho(t)$. The SNI mechanism for noise coupling to the printed circuit board analog signal circuitry is thoroughly discussed in [5]. This SNI

Manuscript received 13 June 2024; revised 10 July 2024; accepted 28 July 2024. Date of publication 2 August 2024; date of current version 11 September 2024. This work was supported in part by the U.S. Department of Energy under Grant DE-CR0000019 and in part by U.S. National Science Foundation under Grant 2219734. The work of Sudip K. Mazumder was suported by the University of Illinois Chicago. *(Corresponding author: Sudip K. Mazumder.)*

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

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TPEL.2024.3437233.

Digital Object Identifier 10.1109/TPEL.2024.3437233

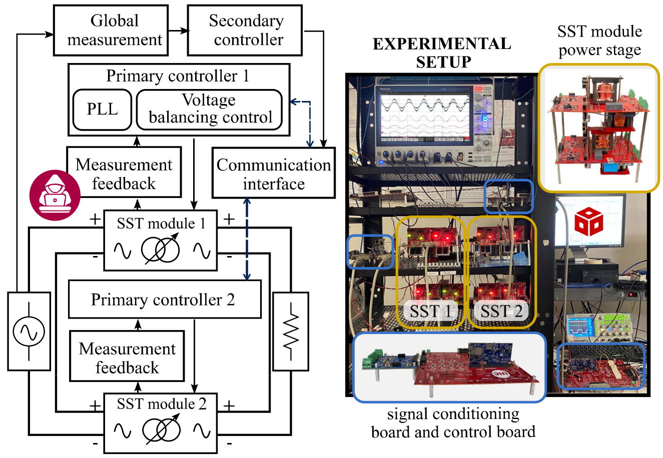


Fig. 1. Architecture of cascaded SSTs under the radiated SNI cyberattack.

is amplitude modulated with a radio frequency (RF) carrier and a low-frequency modulation component such that $\rho(t) = (1+\cos(2\pi f_m t))\cdot A_c\sin(2\pi f_c t)$, where A_c represents the amplitude of the carrier signal, and f_m and f_c are the frequencies of the modulator and the RF carrier, respectively. From Nyquist's theorem, aliasing occurs when the carrier frequency of $\rho(t)$ surpasses half the sampling frequency (f_s) rate. Should the voltage feedback signal experience aliasing due to undersampling, its resultant spectrum will be derived from the spectral folding of the sampled and the modulated signal spectrum. Let the discrete-time representation of the sampled feedback signal be $v'[n] = V\sin(2\pi f_n n/f_s) + (1+\cos(2\pi f_m n/f_s))\cdot A_c\sin(2\pi f_a n/f_s)$; its discrete-time Fourier transform (DFT) can be derived as

$$V'[k] = \underbrace{V\sum_{n=0}^{N-1}\sin\left(\frac{2\pi f_n n}{f_s}\right)e^{-\frac{j2\pi kn}{N}}}_{V[k]} + \underbrace{A_c\sum_{n=0}^{N-1}\left(1+\cos\left(\frac{2\pi f_m n}{f_s}\right)\right)\cdot\sin\left(\frac{2\pi f_a n}{f_s}\right)e^{-\frac{j2\pi kn}{N}}}_{\mathrm{P}[k]} \tag{1}$$

where $V[k]$ and $\mathrm{P}[k]$ are the DFTs of normal and radiated SNI feedbacks, respectively. Parameter f_a denotes the aliased carrier frequency such that $f_a = |f_c - k\cdot f_s|$, where k is an integer such that f_a lies within the range of $f_s/2$ to $f_s/2$. Note that $\mathrm{P}[k]$ can be represented as a convolution of the modulation term $m[n]$ and the aliased carrier $c[n]$ being

$$\mathrm{P}[k] = A_c\sum_{n=0}^{N-1} m[n]\cdot c[n]\,e^{-\frac{j2\pi kn}{N}} = M[k] * C[k] \tag{2}$$

where $*$ refers to the convolution operator and $M[k]$ and $C[k]$ are the DFTs of the modulation and aliased carrier terms, respectively.

The results depicted in Fig. 2 demonstrate that an intruder can manipulate the amplitude of radiated SNI to affect specific frequencies selectively. The frequency spectrums presented in the figure were obtained from the voltage feedback of a discrete-module SST. Apart from the aliases from the high-frequency sampled spectrum, the results suggest that an intruder can manipulate the noise source signal and target low-order harmonic frequencies without relying on aliasing effects to yield sub- and super-60-Hz harmonic damaging effects on the converter. In ac–ac and cascade SST systems, intrusion at frequencies near 60 Hz poses a critical threat due to the required module-to-module synchronization. As discussed in [1], radiated noise can propagate through the analog signal circuitry of the measurement board. As such, an attack of this type can impact both the PLL feedback for synchronism and the voltage-balancing control.

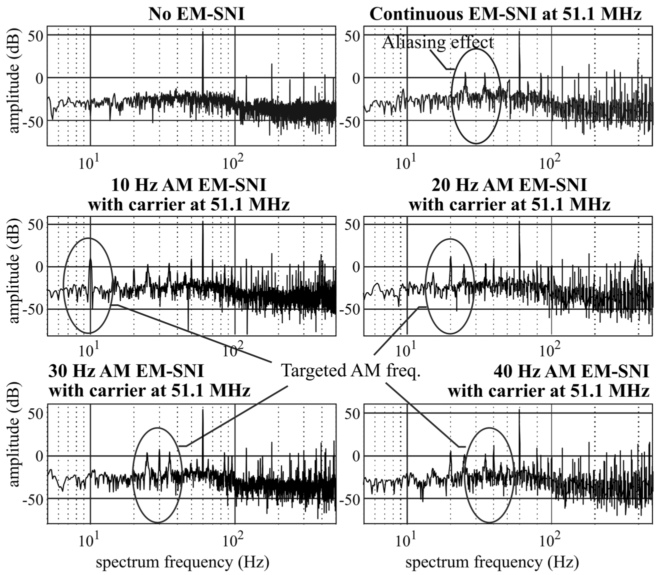


Fig. 2. Voltage feedback spectrum under normal conditions, subject to continuous and AM EM-SNI.

III. AM-Radiated SNI and the PLL Lock-In Performance

When the radiated SNI is amplitude modulated at a frequency in proximity to f_n, such that it distorts the measurement feedback of the SST primary voltage waveform, it can lead to a loss of synchronism among the cascaded SST modules. Under such circumstances, the following discourse analyzes the stability of the PLL to substantiate the experimental outcomes discussed in the subsequent section.

A. PLL Model

Consider the closed-loop model representation of the PLL, including synchronization and phase correction stages [6], as illustrated in Fig. 3. The mathematical description of the input and output signals is given by

$$f(\omega_1(t), t, \theta_1(t)) = A_1\sin(\omega_1(t)t + \theta_1(t)) \tag{3a}$$

$$h(\omega_2(t), t, \theta_2(t)) = A_2\cos(\omega_2(t)t + \theta_2(t)) \tag{3b}$$

where $f(\cdot)$ and $h(\cdot)$ are functions of the time-dependent frequencies $\omega_1(t)$ and $\omega_2(t)$, their independent phases $\theta_1(t)$ and $\theta_1(t)$, and amplitudes A_1 and A_2, respectively.

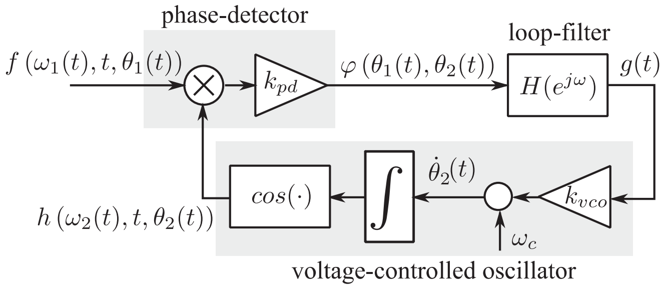

phase-detector
$f\left(\omega_1(t), t, \theta_1(t)\right)$
k_{pd}
$\varphi\left(\theta_1(t), \theta_2(t)\right)$
loop-filter
$H(e^{j\omega})$
$g(t)$
$\cos(\cdot)$
$\int$
$\dot{\theta}_2(t)$
k_{vco}
ω_c
$h\left(\omega_2(t), t, \theta_2(t)\right)$
voltage-controlled oscillator

Fig. 3. Basic PLL closed-loop diagram.

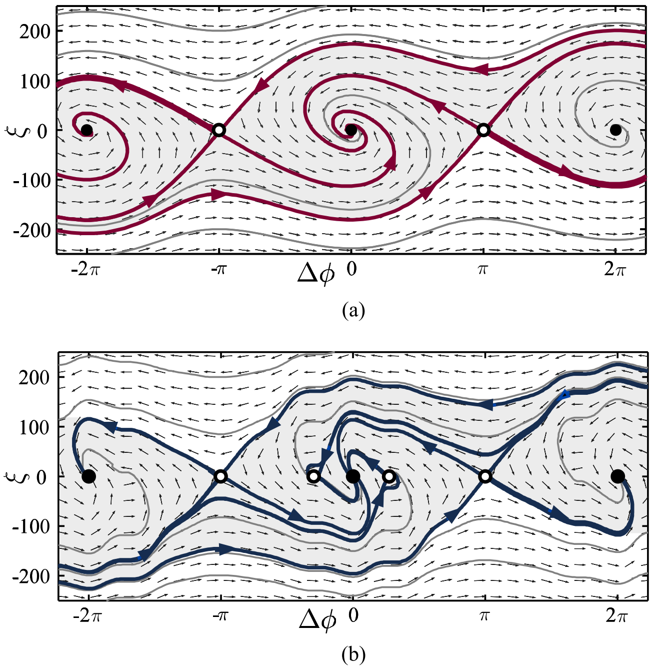
Equations (3a) and (3b) consider the PLL model design's premise that the voltage-controlled oscillator should generate a signal in quadrature with the input one. As such, from trigonometric identities, the phase detector error is given by

$$f\left(\omega_1\left(t\right), t, \theta_1\left(t\right)\right) \times h\left(\omega_2\left(t\right), t, \theta_2\left(t\right)\right) =$$
$$\frac{A_1 A_2}{2}\left[\begin{array}{c}\underbrace{\sin\left(\left(\omega_1\left(t\right) - \omega_2\left(t\right)\right) t + \left(\theta_1\left(t\right) - \theta_2\left(t\right)\right)\right)}_{\text{low-frequency term}} \\ + \underbrace{\sin\left(\left(\omega_1\left(t\right) + \omega_2\left(t\right)\right) t + \left(\theta_1\left(t\right) + \theta_2\left(t\right)\right)\right)}_{\text{high-frequency term}}\end{array}\right]. \tag{4}$$

Note that the high-frequency terms, apart from the natural frequency input, will be filtered out by the low-pass filter stage and can be, thereafter, suppressed for the analysis, as they do not influence the synchronization of the loop. Given the nonlinearity of the phase detector, the lock frequency range is herein considered, assuming that the feedforward frequency term ω_c is tuned so $\omega_1(t) \approx \omega_2(t)$ such that $f(\cdot) \times h(\cdot) \approx (A_1 A_2)/2 \sin(\theta_1(t) - \theta_2(t))$ in a small signal linearized approximation. It can also be verified that in the steady-state condition $(\omega_1(t) \approx 2\pi f_n)$, the existence of the voltage feedback frequency-derived state condition $\dot{\theta}_1(t) = \omega_1$ and the phase-locked state $\dot{\theta}_2(t) = \omega_c + k_{\text{vco}}\, g(t)$ hold. The PLL phase tracking dynamics depend mainly on the loop filter (LF) response. For analysis purposes, the LF will be represented as a proportional–integrative (PI) compensator with low-pass behavior. A linear approximation of the state-space equations of the PLL, considering its inner dynamics, is described by the set of equations as follows:

$$\dot{\xi} = k_{\text{pd}}\, \tilde{\varphi}\left(\theta_1\left(t\right), \theta_2\left(t\right)\right) \tag{5a}$$
$$g\left(t\right) = k_p \left(k_{\text{pd}}\, \tilde{\varphi}\left(\theta_1\left(t\right), \theta_2\left(t\right)\right)\right) + k_i \xi \tag{5b}$$

where $k_{\text{pd}} = (A_1 A_2)/2$ are the phase detector gain, and k_p and k_i are the PI controller's proportional and integral terms, respectively. The function $\tilde{\varphi}\left(\theta_1(t), \theta_2(t)\right) = \sin(\Delta\theta)$ refers to the linearized approximation of $f(\cdot) \times h(\cdot)$. The lock-in PLL synchronization can be defined as the phase displacement between the external signal phase $(\theta_1(t))$ and the internal oscillator closed-loop generated phase $(\theta_2(t))$. A complete description of the PLL synchronization dynamics will consider this phase displacement as a system state given by $\Delta\dot{\theta} = \dot{\theta}_1(t) - \dot{\theta}_2(t) = \Delta\omega - k_{\text{vco}}\, g(t)$, where $\Delta\omega$ equals $(\omega_1 - \omega_c)$ and results in the nonlinear state-space approximation of the PLL dynamics with the model



(a)

(b)

Fig. 4. Phase portrait representation of PLL state trajectories from (7) when (a) the PLL operates in normal measurement feedback conditions and (b) the PLL operates under AM SNI-distorted feedback conditions.

$$\dot{\xi} = k_{\text{pd}}\, \sin\left(\Delta\theta\right) \tag{6a}$$
$$\Delta\,\dot{\theta} = \left(\omega_1 - \omega_c\right) - k_{\text{vco}}\left(k_p\left(k_{\text{pd}} \sin\left(\Delta\theta\right)\right) + k_i \xi\right). \tag{6b}$$

B. AM-Radiated SNI and Its Impact on the PLL Stability

By linearizing the closed-loop nonlinear representation of the PLL from (6b) near the lock-in condition $(\Delta\,\dot{\theta} = 0,\ \dot{\xi} = 0)$, it can be verified that $k_{\text{pd}} \sin(\overline{\Delta\theta}) = (\Delta\omega/k_{\text{vco}} - k_i \bar{\xi})/k_p$, which, applied to (6a), provides the solutions that guarantee the equilibrium points to be found whenever $(\bar{\xi}, \overline{\Delta\theta}) = (\Delta\omega/(k_{\text{vco}} k_i), \pm n\ \pi)\ \forall n \in \mathbb{N}$. The stability of these equilibria can be resolved by evaluating the eigenvalues (λ) of the pair $(\xi, \Delta\theta)$ linearized at the aforementioned equilibrium point. The Jacobian linearization matrix results in

$$\Xi = \begin{bmatrix} 0 & k_{\text{pd}} \cos\left(\pm n\ \pi\right) \\ -k_{\text{vco}} k_i & -k_{\text{vco}}\left(k_p k_{\text{pd}} \cos\left(\pm n\ \pi\right)\right) \end{bmatrix} \tag{7}$$

such that its trace $\operatorname{tr}\left(\Xi\right) = -k_{\text{vco}}\left(k_p k_{\text{pd}} \cos(\pm n\ \pi)\right)$ and determinant $\det(\Xi) = k_{\text{vco}}\left(k_i k_{\text{pd}} \cos(\pm n\ \pi)\right)$. Note that the trace and determinant of Ξ are of opposite signs such that for odd values of n, $\det(\Xi) < 0$ and $\operatorname{tr}(\Xi) > 0$ indicating the existence of an unstable saddle point, while for even values of n, $\det(\Xi) > 0$ and $\operatorname{tr}(\Xi) < 0$ resulting in a stable node of convergence. The simulated phase portrait in Fig. 4(a) illustrates the zone of convergence (in gray) of a single PLL for variable phase displacement error and LF initial internal state under normal operating conditions. In the simulation, the LF parameters are chosen such that $k_{\text{vco}} = 0.01,\ k_p = k_i = 1$, and $k_{pd} = 50$. Note

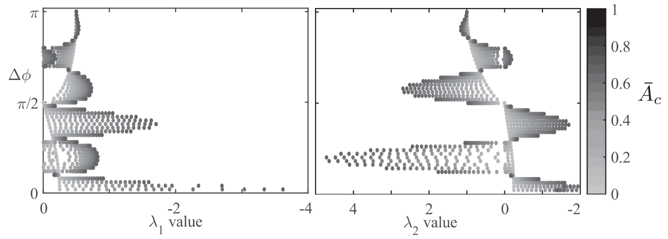


Fig. 5. $\overline{A_c}$ amplitude-dependent real eigenvalues location of the linearized PLL model for radiated SNI conditions.

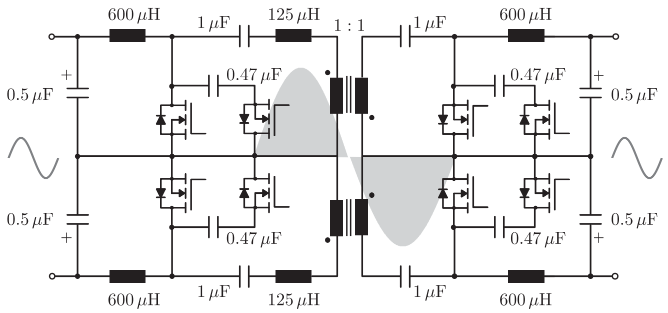


Fig. 6. Top-level architecture of a single-module SST. The modulation strategy and design of the differential-mode AC–AC converter are thoroughly discussed in [9].

that stable nodes (black-filled circles) with spiral convergence are located at every $\pm 2n\pi\ \forall n \in \mathbb{N}$, while unstable saddle equilibria (white-filled circles) are placed at $\pm(2n+1)\pi, \forall\, n \in \mathbb{N}$, as indicated analytically.

Differently, under distorted feedback conditions, other equilibrium states may appear. Consider a continuous time representation of sampled voltage feedback $v'[n]$ as a function of the frequencies of the sampled and modulated folded spectrum such that $\tilde{\varphi}(\cdot)$ is altered to be $\tilde{\varphi}'(\cdot) = \sin(\Delta\theta) + (1 + \cos(f_m/f_n \Delta\theta)) \cdot \overline{A_c} \sin(f_a/f_n \Delta\theta)$, where $\overline{A_c}$ is the normalized amplitude of the AM-radiated SNI. Under such attack conditions, the phase portrait in Fig. 4(b) indicates the existence of unstable equilibria in phase locations other than those under normal operation constraints. The existence of the saddle states is $\overline{A_c}$ amplitude dependent as depicted by the real part of complex eigenvalues versus $\overline{A_c}$ sweep in Fig. 5. In the latter, whether the eigenvalues λ_1 and λ_2 are of opposite sign indicates the existence of saddle states. Conversely, when both the eigenvalues are negative, a stable convergence is verified.

IV. Noise-Quantification-Based IDS

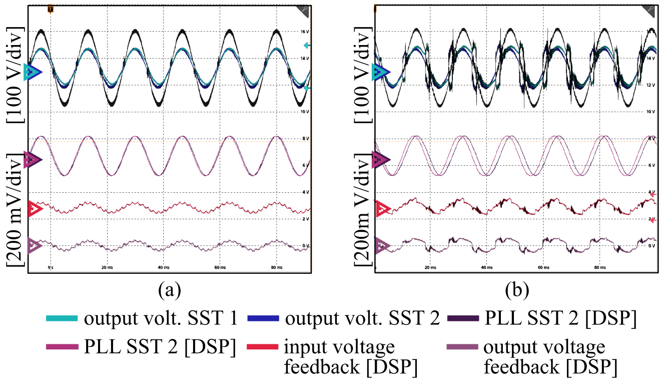
Considering the adverse effects of radiated SNI, it is critical to incorporate a rapid detection mechanism for such intrusions directly into the local controller. The details regarding its implementation are described in Algorithm 1, which will be herein referred to. A novel IDS methodology is proposed to gauge the impact of an intrusion by analyzing the noise it introduces, using the real-time assessment of the signal-to-noise ratio (SNR). The amplification of the noise on the signal feedback $v'[n]$ can be used to spot deviations compared to an internal signal reference. Consider here this internal reference to be $r\,[n] = \sin(\theta_2 n/f_s) = h(\omega_2(t), t, \theta_2(t) + \pi/2)$, where θ_2 is the locked-in frequency of the PLL. To amplify noise effects, a discrete derivative (lines 2 and 3) is utilized by an estimate as the finite difference between adjacent measurements over the discrete-time position, such that $\dot{v}'[n] = (v'[n] - v'[n-2]) \cdot f_s/2$. Under normal conditions, the computation of the real-time discrete derivative will generate a signal y with zero-mean Gaussian noise η with unknown but constant variance σ^2 [7]. A signal distorted by radiated SNI, however, will have measurable nonzero noise power, which can be quantified in finite measurement windows N, by the standard deviation σ of the noisy signal to the signal reference (lines 4–8), given by $S_N = \overline{P_R} - 10\log_{10}\sqrt{\frac{1}{N}\sum_{n=1}^{N}(\dot{v}'[n] - r[n])^2}$, where $\overline{P_R}$ is the average power of the reference signal $r[n]$ in dB. The window length is defined as the closest integer of $N = f_s/f_n$ to capture distortions and/or phase deviations to the fundamental frequency cycle. To identify radiated SNI interference at the local controller level of an SST module, the SNR is compared against a preset static threshold α (lines 9–13). The detectability index employed is derived from the *Rose criterion* [8]—a benchmark typically applied in imaging systems concerning signal detectability—which states that an SNR of 5 dB or more is needed to distinguish a signal from incident noise. A deviation in voltage feedback that falls within this threshold promptly triggers the IDS flag.

Algorithm 1. SNR-Based IDS.

```
 1: function IDS($v'[n], r[n]$)
        ▷ Calculation of $v'_n$ discrete-time derivative
 2:     $\dot{v}'[n] \leftarrow \frac{(v'[n]-v'[n-2])}{2}$
 3:     $v'[n-2] \leftarrow v'[n-1]$; $v'[n-1] \leftarrow v'[n]$
        ▷ Computation of derivative $v'[n]$ to reference $r[n]$ deviation and capture it in a sliding window of size $N$
 4:     $\vec{\varepsilon}[n] \leftarrow$ buffer.fill $(\dot{v}'[n] - r[n])$
        ▷ Cumulative summation of $\vec{\varepsilon}$ during the fundamental frequency cycle
 5:     for $(i : 1$ to $N)$ do
 6:         $\varepsilon_\Sigma \leftarrow \varepsilon_\Sigma + \|\vec{\varepsilon}[i]\|_2^2$
 7:     end for
 8:     $S_N \leftarrow \left\|\overline{P_R} - 10 \cdot \log_{10}\left(\sqrt{\varepsilon_\Sigma}\right)\right\|$
        ▷ Compare quantified noise to a threshold $\alpha$
 9:     if $S_N \leq \alpha$ then
10:         $\text{IDS}_{\text{flag}} \leftarrow 1$
11:     else
12:         $\text{IDS}_{\text{flag}} \leftarrow 0$
13:     end if
14:     return $\text{IDS}_{\text{flag}}$
15: end function
```

V. Experimental Validation

To investigate the diffusion of radiated SNI on cascaded SSTs, we utilized an experimental setup consisting of two 1-kW isolated differential-mode Ćuk-based ac–ac direct power conversion [9] SST modules. The SSTs were connected in



(a) (b)

Fig. 7. Experimental results on the impact of SNI on cascaded SSTs, when the radiated SNI (a) is a continuous 51.1-MHz sinusoidal noise intrusion and (b) is AM with a carrier of 51.1-MHz sinusoidal noise and modulation frequency of 59 Hz.

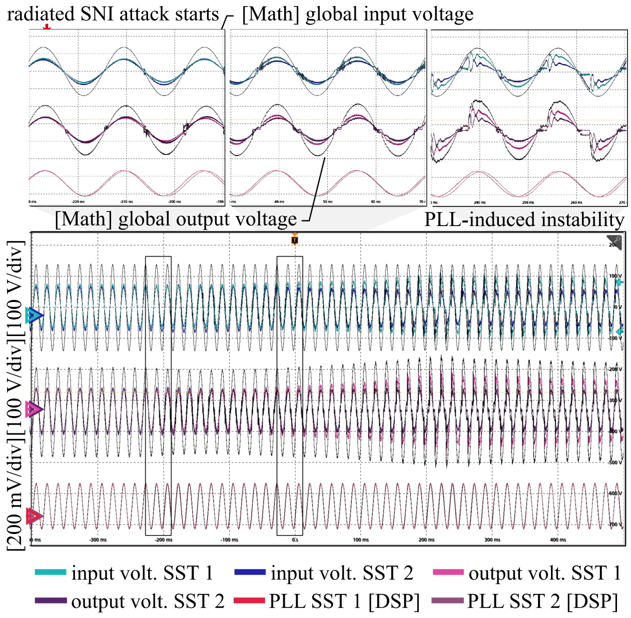


Fig. 8. Experimental results on the impact of the AM-radiated SNI in the closed-loop voltage balancing and synchronization of cascaded SSTs. The SNI conditions are of a sinusoidal SNI with an AM frequency of 59 Hz and a carrier of 51.1 MHz.

series, as depicted in Fig. 1, with an input voltage of 120 $\mathrm{V_{RMS}}$ and a constant switching frequency of 40 kHz. The topology and relevant parameters are displayed in Fig. 6. Similarly to the work in [1], this work explores a scenario in which an attacker targets the low-voltage sensing circuitry by disrupting its performance with an external EM source. To showcase how the attack diffuses throughout cascaded SST modules, a small transmitting antenna couples with the analog control feedback of a single module, hereinafter referred to as SST 2, affecting the overall system's performance. The antenna sources RF-radiated EM noise overwritten by a low-frequency AM wave, with a frequency near the synchronous reference of 60 Hz.

A. AM-Radiated SNI Diffusion in Cascaded SSTs

The following experimental results demonstrate the effects of radiated SNI under two scenarios—continuous SNI and AM SNI. From Fig. 7(a), we can observe that the impact of continuous noise intrusion is minimal on the output waveforms of the system as long as aliasing effects do not interfere with the controller's resonance frequency and synchronism in a band near 60 Hz. However, when the SNI is modulated, as shown in Fig. 7(b), it yields a swing in the synchronism—note the variation in phase displacement of the PLL-generated sine waves—and, consequently, voltage balancing instability.

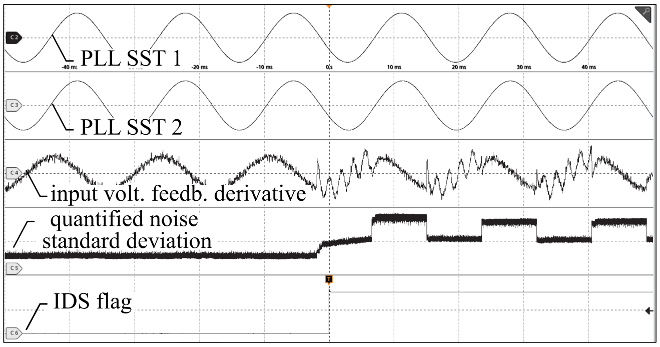


Fig. 9. Experimental results on the performance of the noise-quantification-based IDS. The SNI conditions are of a sinusoidal SNI with an AM frequency of 57 Hz and a carrier of 51.1 MHz.

Fig. 8 illustrates the impact of the radiated SNI diffusion in the cascaded SSTs. The onset of the attack causes a swing in the synchronism between the lock-in state and the phase of the saddle-node equilibria. This results in chaotic behavior on the output voltage balancing of the cascade system. Although the converter system waveforms immediately reflect the attack, within a few milliseconds, the instability becomes more pronounced. The controllers' high gain within a limited bandwidth toward frequency deviations further contributes to the cascaded SST's instability. Our empirical findings show that the proximity of the SNI noise's AM frequency to the fundamental frequency exerts a significant impact on the SST power stage voltage waveforms, especially within a ±3-Hz bandwidth around 60 Hz.

B. SNR-Based IDS Performance

The experimental results in Fig. 9 demonstrate that the proposed IDS yields promising results in detecting intrusions caused by AM-radiated SNI targeting SST module 2. The input voltage feedback, responsible for synchronization, receives a distorted signal, as described in Section II. It is worth noting that the PLL prevents the propagation of aliases due to its LF and 60 Hz-tuned oscillator. However, such an attack produces a phase deviation, altering the SNR and, thus, significantly impacting the quantified noise standard deviation.

Fig. 10 shows the discrete probability distribution obtained from experimental data on intrusion detection time for different SNI AM frequencies, with a noise SNR marginally below 5 dB in steady state at its higher level. The "rugs" in the figure represent the discrete positions of the detection time on the time axis, while the central red lines indicate the mean detection value—which ranges from 2.75 to 3.4 ms— for each dataset. Notably, for a radiated SNI at a modulation frequency of 60 Hz, the average

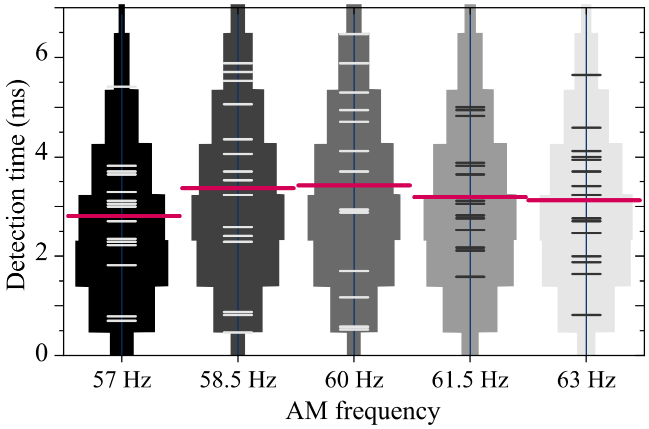


Fig. 10. Poisson discrete distribution of experimental intrusion detection times for different AM frequencies with a radiated SNI carrier of 50 MHz.

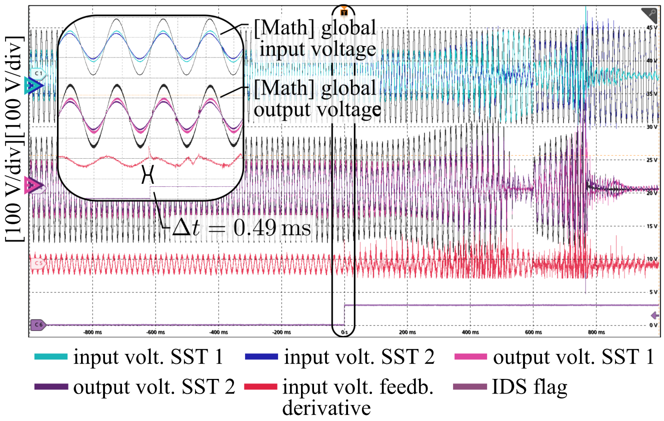


Fig. 11. Chaotic response and irreversible recovery of cascaded SSTs after AM-radiated SNI diffusion. The SNI conditions are of a sinusoidal SNI with an AM frequency of 58.5 Hz and a carrier of 50 MHz.

detection time is higher. This is due to the increased influence of the incident wave phase, while the dissimilarity between the intrusion signal modulated frequency (f_m) and the PLL's fundamental frequency (f_n) has a stronger influence in the PLL instability in the scenarios apart from 60 Hz.

Let $\overline{A_c}$ of the AM-radiated SNI be such that the PLL is unable to timely recover synchronization. Experimental results in Fig. 11 indicate that one of the cascaded SST modules begins to process a progressively larger portion of the input power, eventually causing the other module's power processing to cease. The loss of voltage balance, due to the sustained impact of the radiated SNI, causes one module to overtake the global input voltage. In this scenario, the cascaded control system reaches an irreversible state where it can no longer regulate the input-to-output voltage, resulting in both modules' secondary side to collapse with output voltages dropping to zero. The results depicted in the figure further illustrate the efficacy of intrusion detection mechanisms in the early stages of diffusion. The IDS promptly triggers an alert for noise detection as soon as the SNR falls below the predetermined threshold, as discussed in the previous section.

VI. Conclusion

The diffusion of radiated SNI in multimodule SSTs poses a significant threat to modern power grids. This letter shows that, due to the physical coupling and synchronization loop dependency, cyberattacks in discrete SST modules can cause a domino instability effect in cascaded systems. Moreover, it illustrates that the impact of SNI attacks can be amplified depending on the sampled SNI spectrum. The experimental results obtained in this study were restricted to isolated differential-mode Ćuk-based ac–ac direct power conversion SST topology. However, as the attack diffusion mechanism stems from radiated SNI impact on the PLL stability, it can be inferred that the impact analysis conducted in this study and similar results would presumably be verified in other SST topologies in a cascaded configuration. Hence, the impact analysis is constrained to cascaded physical connections and grid synchronism dependence, in which, the latter is a basic requirement for networking modular ac–ac SST converters.

The easy deployment of radiated SNI cyberattacks with such harmful effects emphasizes the need for research on resilient control environments that combat the growing threat of cyberattacks on power converters. Should the attack impact the PLL stability, as showcased in this work, advanced synchronization strategies would be required to improve the systems' stability. For instance, adaptive [10] and self-learning [11] techniques with sub- and supersynchronous harmonic rejection for disturbance rejection could be employed after thorough stability and dynamic performance verification. Alternatively, global synchronization strategies based on the mutual consensus [12] of the SST modules' PLL nodes may aid in mitigating the local phase displacement deviation, provided that not all distributed modules are affected by the EM source. However, such a solution would necessitate high-speed minimal time-delay peer-to-peer local phase communication between the SST modules.

References

[1] M. D. R. Greidanus, S. D'Silva, S. Gupta, D. Sur, S. K. Mazumder, and M. B. Shadmand, "Electromagnetic side-channel noise intrusion on solid-state transformer," *IEEE Trans. Power Electron.*, vol. 39, no. 8, pp. 9244–9256, Aug. 2024, doi: 10.1109/TPEL.2024.3391217.

[2] Y. Pan et al., "A cascaded modular isolated back-to-back solid state transformer scheme for AC/DC/AC interconnection with improved performance and simple control," *IEEE Trans. Power Electron.*, vol. 38, no. 9, pp. 11050–11068, Sep. 2023, doi: 10.1109/TPEL.2023.3285545.

[3] C. Burgos-Mellado et al., "Cyber-attacks in modular multilevel converters," *IEEE Trans. Power Electron.*, vol. 37, no. 7, pp. 8488–8501, Jul. 2022, doi: 10.1109/TPEL.2022.3147466.

[4] S. K. Mazumder, M. D. R. Greidanus, J. Liu, and H. A. Mantooth, "Vulnerability of a VOC-based inverter due to noise injection and its mitigation," *IEEE Trans. Power Electron.*, vol. 38, no. 2, pp. 1445–1450, Feb. 2023, doi: 10.1109/TPEL.2022.3214835.

[5] 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.

[6] G. A. Leonov, N. V. Kuznetsov, M. V. Yuldashev, and R. V. Yuldashev, "Hold-in, pull-in, and lock-in ranges of PLL circuits: Rigorous mathematical definitions and limitations of classical theory," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 10, pp. 2454–2464, Oct. 2015, doi: 10.1109/TCSI.2015.2476295.

[7] F. Van Breugel, J. N. Kutz, and B. W. Brunton, “Numerical differentiation of noisy data: A unifying multi-objective optimization framework,” *IEEE Access*, vol. 8, pp. 196865–196877, 2020, doi: 10.1109/ACCESS.2020.3034077.

[8] A. E. Burgess, “The rose model, revisited,” *J. Opt. Soc. Amer. A*, vol. 16, no. 3, 1999, Art. no. 633, doi: 10.1364/JOSAA.16.000633.

[9] 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.

[10] H. X. Nguyen, T. N.-C. Tran, J. W. Park, and J. W. Jeon, “An adaptive linear-neuron-based third-order PLL to improve the accuracy of absolute magnetic encoders,” *IEEE Trans. Ind. Electron.*, vol. 66, no. 6, pp. 4639–4649, Jun. 2019, doi: 10.1109/TIE.2018.2866088.

[11] M. Tang, S. Bifaretti, S. Pipolo, S. Odhano, and P. Zanchetta, “A novel repetitive controller assisted phase-locked loop with self-learning disturbance rejection capability for three-phase grids,” *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 8, no. 2, pp. 1870–1879, Jun. 2020, doi: 10.1109/JESTPE.2019.2941835.

[12] C. Hoyer, J. Wagner, and F. Ellinger, “Phase noise in networks of mutual synchronized spatially distributed 24-GHz PLLs,” *IEEE Trans. Microw. Theory Techn.*, vol. 72, no. 2, pp. 1312–1325, Feb. 2024, doi: 10.1109/TMTT.2023.3300180.