Renewable Energy, Environment, and Power Quality Journal (REE&PQJ)
ISSN:3020-531X
Volume 26, July 2026

Detection of Cyber-Attacks on Grid-Connected Converter with Output LCL Filter

Viktor Valouch[1]
[1] Faculty of Electrical Engineering
Czech Technical University
Prague, Czech Republic
valouch@it.cas.cz

Martin Bejvl[2], Petr Šimek[2], Miroslav Chomát[2]
[2] Department of Electrotechnics and Electrophyzics
Insitute of Thermomechanics,
Czech Academy of Sciences
Dolejškova 1402/5, 18200, Praha 8.
bejvl@it.cas.cz, simek@it.cas.cz

Abstract. This paper presents the implementation of a cyber-attack detection system based on a watermarking strategy for a grid-connected power electronic converter equipped with an LCL filter. Mathematical models of the system are established to derive the detection equations. The proposed strategy was verified through both Matlab/Simulink simulations and laboratory experiments using a dSPACE-based control platform. The analysis focuses on voltage and current waveforms under both nominal operation and simulated scaling attacks on the sensors. The results demonstrate that the watermarking strategy is an effective tool for identifying compromised measurement data and ensuring the security of control systems in grid-connected converters.

Key words. cyber attack detection system, watermark strategy, power electronic converter, LCL grid filter, simulation, laboratory tests

Nomenclature

DES	Distributed energy sources
GPC	Generalized predictive control
GPCC	Generalized predictive current control
MPC	Model predictive control
PCC	Point of common coupling
PWM	Pulse width modulation
SRF^p	Synchronous reference frame rotating by ω_1
VAr	Unit of reactive power
VSC	Voltage source converter

1. Introduction

With the rapid development of multi-level control systems in distributed power grid suppliers and transmitters, cyber threats can have a devastating impact on grid management operations. Smart grid applications consisting of communication and transmission networks are vulnerable to numerous hacker attacks. The control systems can receive inaccurate signals, which may lead to the destruction of instruments or even entire controlled systems.

Consequently, cyber threats in power electronics based smart grid applications [1]-[6] are currently a subject of ever-growing interest among researchers and companies.

This contribution describes an attempt to implement a cyber attack detection system based on a "watermark strategy" in grid-connected converters. The principle of this strategy is based on injecting a watermark signal into the control signal of the converter and verifying whether a corresponding signal can be detected in some of the feedback signals produced by the sensors of the controlled object [7], [8]. Any discrepancy between the injected watermark signal and some sensor signal indicates the possible presence of a cyber attack.

The Model Predictive Control (MPC) has become popular also in control systems applied in power electronic applications [9]-[13].

A special type of the MPC is the Generalized Predictive Control (GPC), [14], which has recently been used for the control of power electronic converters.

The current control of a converter with an L grid filter using the Generalized Predictive Current Control (GPCC) was developed and tested in [15]-[17]. Power control based on the GPCC applied in the grid-connected converter with L filter was presented in [18].

However, the simplest L filter has low efficiency in suppressing of current harmonics. This is the main reason why a more efficient LCL filter is used.

The grid filter structure can be developed according to acceptable grid current spectrum defined by the IEEE 519-2014 standard in the USA and IEC/TR 61000-3-6:2008 in Europe.

An essential parameter is the ratio between the short circuit power at a PCC (Point of Common Coupling) and the nominal power of the converter connected to the PCC. In [19], a possible procedure for the LCL filter design was presented.

Considering the full LCL filter topology introduces certain difficulties in the design of current control circuitry. Various control and PWM (Pulse Width Modulation) strategies were presented, [20]-[23]. Among these, MPC theory has found its application here [24]-[26].

To date, the GPCC strategy applied to grid-connected converter with LCL filter has only been presented in [27]. A different design procedure for GPCC was previously presented in [18] for the grid-connected converter with the L filter. The same type of the GPCC is now applied to converter with the LCL filter now, in conjunction with the developed cyber attack detection system.

This contribution is organized as follows: Section II presents the block diagram and equations of the PWM converter connected to the grid via the LCL filter. Section III explains the principle of the watermark strategy and the corresponding equations used for detection of the cyber attacks. Section IV presents simulation results for selected cyber attack examples. Section V describes experimental setup and results. Section VI provides the conclusion.

2. Equations of power system

Figure 1 presents a simplified block diagram of a PWM converter connected to the grid via an LCL filter and with grid current ($\boldsymbol{i}_{\mathrm{G}}$) control. The current reference components i^{*}_{Gd} and i^{*}_{Gq}, calculated from reference active and reactive powers, are transformed to the $\alpha\beta$ static reference frame where the GPCC is implemented. The converter output voltage $\boldsymbol{v}_{\mathrm{C}}$ is generated using a PWM algorithm. The DC voltage (v_{DC}) controller is not included in the following analysis. The measured grid voltage is used in digital models of the system running in parallel with the real system to enable the detection of potential attacks.

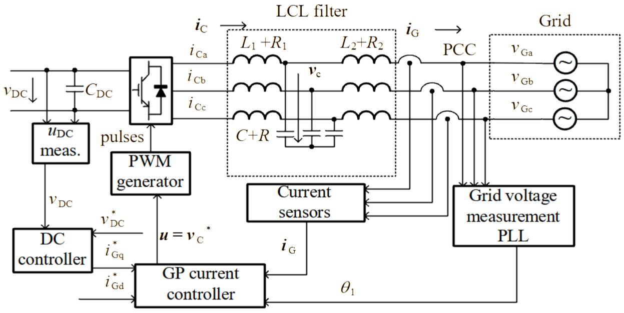

Fig. 1 Simplified block diagram of PWM converter connected to grid via LCL filter and with GPCC of $\boldsymbol{i}_{\mathrm{G}}$

The analysis begins with the LCL filter equations in the Laplace domain, which is subsequently transformed into the Z-domain using the backward Euler approximation.
The derivation of the Laplace-domain model may be divided into two steps: first, $\boldsymbol{i}_{\mathrm{G}}$ is calculated as an independent variable assuming $\boldsymbol{v}_{\mathrm{G}}$=0, $\boldsymbol{v}_{\mathrm{C}}$<>0; second $\boldsymbol{i}_{\mathrm{G}}$ is calculated as an independent variable assuming ($\boldsymbol{v}_{\mathrm{C}}$=0, $\boldsymbol{v}_{\mathrm{G}}$<>0). Both steps are next superposed, and the grid current $\boldsymbol{i}_{\mathrm{G}}(s)$ can be expressed as:

$$\boldsymbol{i}_{\mathrm{G}}(s)=\boldsymbol{v}_{\mathrm{C}}(s)\frac{B_{\mathrm{C}}(s)}{A_{\mathrm{C}}(s)}-\boldsymbol{v}_{\mathrm{G}}(s)\frac{B_{\mathrm{G}}(s)}{A_{\mathrm{G}}(s)}=$$
$$\boldsymbol{v}_{\mathrm{C}}(s)\frac{b_{2\mathrm{C}}s^{2}+b_{1\mathrm{C}}s+b_{0\mathrm{C}}}{a_{4\mathrm{C}}s^{4}+a_{3\mathrm{C}}s^{3}+a_{2\mathrm{C}}s^{2}+a_{1\mathrm{C}}s+a_{0\mathrm{C}}}$$
$$-\boldsymbol{v}_{\mathrm{G}}(s)\frac{b_{2\mathrm{G}}s^{2}+b_{1\mathrm{G}}s+b_{0\mathrm{G}}}{a_{3\mathrm{G}}s^{3}+a_{2\mathrm{G}}s^{2}+a_{1\mathrm{G}}s+a_{0\mathrm{G}}} \quad (1)$$

with input variables $\boldsymbol{v}_{\mathrm{C}}(s)$ and $\boldsymbol{v}_{\mathrm{G}}(s)$. Coefficients A, B, a, b are consisted of the LCL filter inductances and capacitances. The equations for the coefficients are in the Appendix.

To derive the GPCC control algorithm, a transition (1) to the Z-domain is required, for instance, by employing the backward Euler method.

$$s \triangleq \frac{1-z^{-1}}{T_{\mathrm{S}}} \quad (2)$$

Applying (2), the following equations are derived, where the coefficients in the numerators and denominators are determined from the corresponding parameters in (1)

$$\frac{\boldsymbol{i}_{\mathrm{G}}(z^{-1})}{\boldsymbol{v}_{\mathrm{C}}(z^{-1})}=\mathbf{Z}\left\{\frac{B_{\mathrm{C}}(s)}{A_{\mathrm{C}}(s)}\right\}=F_{\mathrm{C}}(z^{-1})=\frac{B_{\mathrm{C}}(z^{-1})}{A_{\mathrm{C}}(z^{-1})}=$$
$$\frac{B_{0\mathrm{C}}+B_{1\mathrm{C}}z^{-1}+B_{2\mathrm{C}}z^{-2}}{A_{0\mathrm{C}}+A_{1\mathrm{C}}z^{-1}+A_{2\mathrm{C}}z^{-2}+A_{3\mathrm{C}}z^{-3}+A_{4\mathrm{C}}z^{-4}} \quad (3)$$

and

$$\frac{\boldsymbol{i}_{\mathrm{G}}(z^{-1})}{\boldsymbol{v}_{\mathrm{G}}(z^{-1})}=\mathbf{Z}\left\{\frac{B_{\mathrm{G}}(s)}{A_{\mathrm{G}}(s)}\right\}=F_{\mathrm{G}}(z^{-1})=\frac{B_{\mathrm{G}}(z^{-1})}{A_{\mathrm{G}}(z^{-1})}=$$
$$\frac{B_{0\mathrm{G}}+B_{1\mathrm{G}}z^{-1}+B_{2\mathrm{G}}z^{-2}}{A_{0\mathrm{G}}+A_{1\mathrm{G}}z^{-1}+A_{2\mathrm{G}}z^{-2}+A_{3\mathrm{G}}z^{-3}} \quad (4)$$

Equations (3) and (4) elaborate on the intermediate superposition steps for $\boldsymbol{v}_{\mathrm{G}}=0$ and $\boldsymbol{v}_{\mathrm{C}}=0$ in greater detail than (1) and (2).

These equations (3), (4) serve as the basis for formulating the GPCC algorithm applied along both axes $\alpha\beta$ of the stationary reference frame.

This GPCC strategy, as applied to a grid-connected converter with an L filter, was detailed in [18].

3. Watermark Strategy

The watermark strategy is based on incorporating a watermark signal into the converter control signal and verifying its presence in the electrical or mechanical feedback signal generated by a system sensor, [7]-[8]. A mismatch between the injected and the feedback signal indicates a malfunction caused by an attacker.

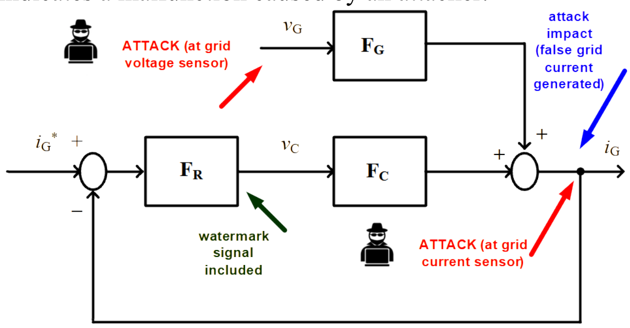

Fig. 2 Simplified block diagram of control system for grid-connected converter via LCL grid filter, indicating watermark injection points, potential attack locations, and attack detection points.

Figure 2 presents a simplified block diagram of the current control for a grid connected-converter. The symbols $\mathrm{F_G}/\mathrm{F_R}/\mathrm{F_C}$ mark transfer functions (4)/GPCC controller/(3). The objective is to control the current $\boldsymbol{i}_{\mathrm{G}}$, where the converter and grid are connected via an LCL filter. Only the current $\boldsymbol{i}_{\mathrm{G}}$ is measured. This current is influenced by two variables: the converter-generated voltage $\boldsymbol{v}_{\mathrm{C}}$ and the grid voltage $\boldsymbol{v}_{\mathrm{G}}$. The voltage $\boldsymbol{v}_{\mathrm{C}}$ is managed by the controller F_R which compares the reference and actual values of the current $\boldsymbol{i}_G$.

Figure 2 also highlights two potential locations where an attacker can manipulate the measured variables, thereby compromising the entire systems performance.

Based on (1), the system shown in Fig. 2 can be described by the following equations in the Laplace domain

$$\boldsymbol{i}_G(s) = F_C(s)\boldsymbol{v}_C(s) + F_G(s)\boldsymbol{v}_G(s) \quad (5)$$

$$\boldsymbol{v}_C(s) = F_R(s)\left[\boldsymbol{i}_G^*(s) - \boldsymbol{i}_G(s)\right] \quad (6)$$

Thus, the grid current $\boldsymbol{i}_G$ is expressed as

$$\boldsymbol{i}_G(s) = \frac{F_C F_R}{1+F_C F_R}\boldsymbol{i}_G^*(s) + \frac{F_G}{1+F_C F_R}\boldsymbol{v}_G(s) \quad (7)$$

By transforming this equation into the Z-domain, the following expression is obtained:

$$\boldsymbol{i}_G(k+1) = H_C \boldsymbol{i}_G^*(k) + H_G \boldsymbol{v}_G(k) \quad (8)$$

Where H_C and H_G are composed by F_C, F_R, F_G

If an additional watermark signal w(t)~N(0,σ_{W2}) with Gaussian distribution is injected by the power electronic converter, the equation (8) becomes

$$\boldsymbol{i}_{GW}(k+1) = H_C \boldsymbol{i}_G^*(k) + H_G \boldsymbol{v}_G(k) + H_W \boldsymbol{w}(k) \quad (9)$$

Equations (8) and (9) represent the mathematical models of the PWM converter connected to the grid via the LCL filter, without and with the watermark signal, respectively. These models run in real time alongside the converter controller.

Based on the procedure outlined in [7], [8] the following three test outputs are designed to detect potential attacks:

$$\text{TEST1: } \lim_{K\to\infty} \frac{1}{K}\sum_{k=1}^{K-1}\left[\boldsymbol{i}_{GM}(k+1) - \boldsymbol{i}_{GW}(k+1)\right]^2 \overset{?}{=} \sigma_S^2 \quad (10)$$

$$\text{TEST2: } \lim_{K\to\infty} \frac{1}{K}\sum_{k=1}^{K-1}\left[\boldsymbol{i}_{GM}(k+1) - \boldsymbol{i}_{G}(k+1)\right]^2 \overset{?}{=} \sigma_S^2 + H_W^2 \sigma_W^2 \quad (11)$$

$$\text{TEST3} = \text{TEST2} - \text{TEST1} = H_W^2 \sigma_W^2 \quad (12)$$

where $\boldsymbol{i}_{GW}$(k+1), $\boldsymbol{i}_G$(k+1) are the currents calculated by the models, and $\boldsymbol{i}_{GM}$(k+1) represents the measured grid current values, which may be affected by potential attacks and σ_S, which is the process noise variance. It is necessary to realize that the measured grid current $\boldsymbol{i}_{GM}$(k+1) without an attack is described also by (9).

During normal operation (without an attack), TEST1 reflects only the system noise variance, as the actual measurements and the model with a watermark generate nearly identical data. TEST2 yields the same noise plus watermark, because the measured values are compared with the model without the injected watermark.

However, if an attack occurs, the value of TEST1 increases due to higher difference between measured and modeled values of $\boldsymbol{i}_G$. Similarly, TEST2 exceeds the sum of the system noise and watermark variances.

4. Simulation Results

The system shown in Fig. 2 was simulated in Matlab/Simulink environment by incorporating cyber-attacks to obtain the measured current $\boldsymbol{i}_{GM}$(k+1). To evaluate TEST1-TEST3 (10)-(12), discrete attack-free models – both with and without the watermark signal (8), (9) – were implemented in parallel within the simulation.

The LCL filter parameters, which comply with the criteria summarized in [19], are listed in TABLE I along with the converter parameters and voltages used in the simulation.

TABLE 1 Parameters of LCL filter and converter.

Inductance L_1 of filter (H)	0.005
Resistance R_1 (Ω)	1
Inductance L_2 of the filter (H)	0.002
Resistance R_2	0.5
Capacitance C	20
Resistance R	10
Sampling frequency f_s	6000
Switching frequency f_{sw}	3000
Grid phase voltage V_{RMS}(V)	115
Converter dc bus voltage V_{dc}	400
Dead time $T_d = T_s$ (ms)	1/6

Fig. 3 shows the time responses of the grid phase currents i_{Ga}, i_{Gb}, i_{Gc}. The red curves represent the system model without the watermark signal, while the blue curves show the real grid current with both the watermark and an attack. The attack is simulated by doubling the current sensor output at t = 0.02s, returning to normal values at t = 0.06s. A similar manipulation is applied to the grid voltage sensor starting at t = 0.1s. It is evident that during the current sensor attack, the current magnitudes are half the reference values.

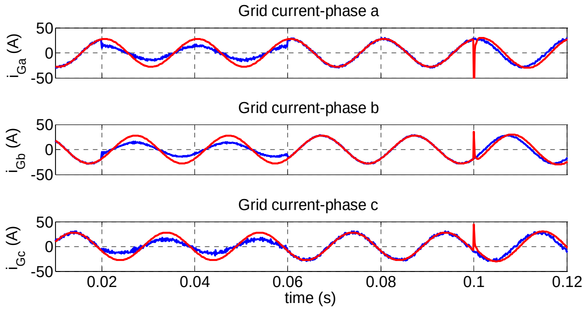

Fig.3. Time responses of grid phase currents i_{Ga}, i_{Gb}, i_{Gc} for system model without watermark signal (red) and grid current responses with watermark and attack (blue)

During the attack on the grid voltage sensor, only the magnitudes and phases of the currents calculated by the digital models (8), (9), running in parallel with the real process, are affected.

Fig. 4 shows the time responses of the converter phase voltages v_{Ca}, v_{Cb}, v_{Cc} for the exact system model without a watermark signal (red) and for the real converter voltage responses with the watermark and attack (blue) during the process shown in Fig. 3. Comparing Figs. 3 and 4 it is evident that an attack on the current sensor leads to errors in the real grid current, whereas an attack on the voltage sensor only results in errors in the calculated converter voltage, as the current controller does not utilize this voltage signal. Nevertheless, this attack is also detected as shown in Fig. 5.

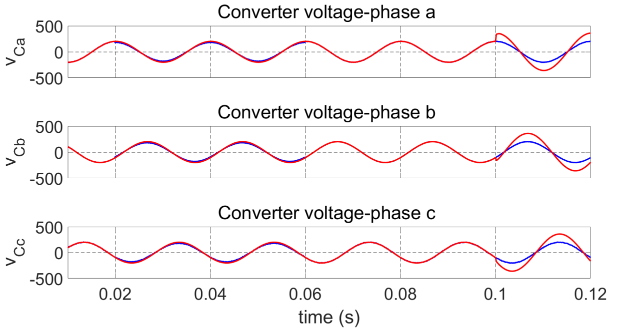

Fig. 4 Time responses of converter phase voltages v_{Ca}, v_{Cb}, v_{Cc} for the exact system model without watermark signal (red) and for real converter voltage responses with watermark and attack (blue)

Finally, Fig. 5 presents the results of TESTS 1, 2 and 3. The rapid changes in the values of TEST1 and TEST2 during the relevant time intervals indicate a cyber-attack. In laboratory experiments residual values of TEST1 and TEST2 can be expected even during attack-free periods. This is due to the presence of noise σ_S, parameter mismatches between the model and the experimental systems, and also due to some inaccuracies in all data acquisition and processing.

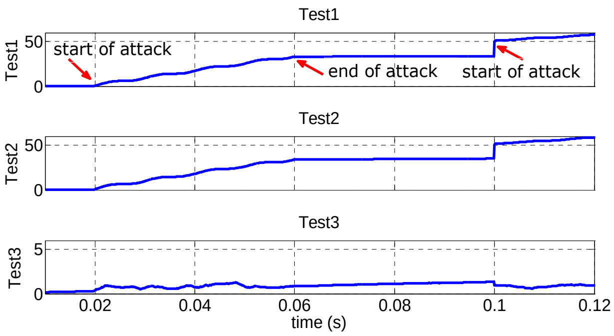

Fig. 5 Time responses of TEST1, TEST2, and TEST3 for processes shown in Figs. 3 and 4

Fig. 6 presents the time responses of the grid phase currents i_{Ga}, i_{Gb}, i_{Gc} for the system model without a watermark signal (red) and for the real grid current responses with the watermark and attack (blue). The attack consists of injecting fictitious 5th (25%) and 7th (15%) harmonics into the real grid current at t = 0.02s with the sensors returning to normal values at t = 0.06s. Similar 5th (15%) and 7th (9%) harmonics are applied to the grid voltage sensor starting at t = 0.1s. It is evident that an attack on the current sensor leads to the propagation of these harmonics into the real grid current, whereas an attack on the voltage sensor does not affect the current waveform. Nevertheless, this attack is also detected as shown in Fig. 7.

A series of simulations of attacks on the measured grid current or voltage for the inverter connected to the grid via an LCL filter was performed. The figures presented above show the waveforms of TEST1-TEST3 when the measured current or voltage is distorted by changing its magnitude or by adding fictive 5th and 7th. The simulations confirm the effectiveness of the watermark strategy for detecting cyber-attacks on the sensors of power electronic converters connected to electrical grids.

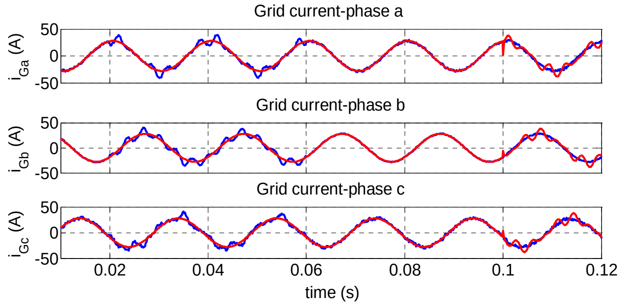

Fig. 6 Time responses of grid phase currents i_{Ga}, i_{Gb}, i_{Gc} for the system model without watermark signal (red) and real grid current responses with watermark and attack (blue)

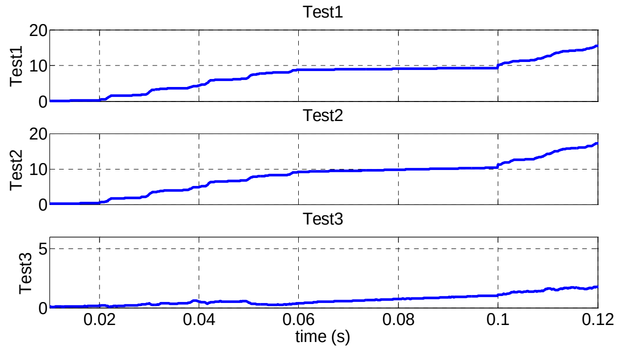

Fig. 7 Time responses of TEST1, TEST2, and TEST3 for processes shown in Fig. 6

5. Experimental Results

The proposed strategy was experimentally verified. The laboratory setup comprised a Chroma 61704 programmable voltage source, a digital control unit based on the dSPACE™ DS1005 system, and an Infineon Mipaq™ IGBT based converter. Both the developed GPCC and the watermark-based attack-identification algorithms were implemented in the dSPACE™ DS1005 control system.

All relevant responses were captured within the dSPACE™ system, transferred to a computer and subsequently visualized using MATLAB™ plotting functions.

Fig. 8 illustrates an example of the layout of the dSPACE™ control panel.

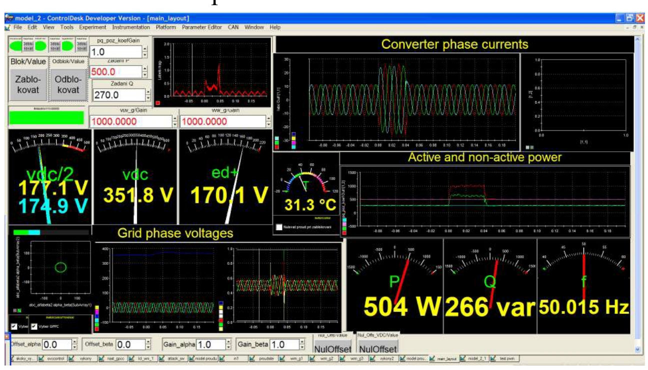

Fig. 8 Example of the dSPACE™ control panel layout

Fig. 9 presents the time responses of the measured grid phase currents i_{Ga}, i_{Gb}, i_{Gc}. The attack is simulated by halving the current sensor output at t = 0.0s, with the current sensor returning to its normal values at t = 0.04s. Consequently, the current magnitudes during the attack are twice as high as those under normal operation.

The responses for TEST1 and TEST2 are also provided in Fig. 9. Rapid change in these test values during the relevant time intervals indicate the presence of a cyber-attack. In laboratory experiments residual changes are observed in TEST1 and TEST2 even during attack-free periods. This is caused by noise σ_S parameter mismatches between the model and the experimental system, and by potential inaccuracies in data acquisition and processing.

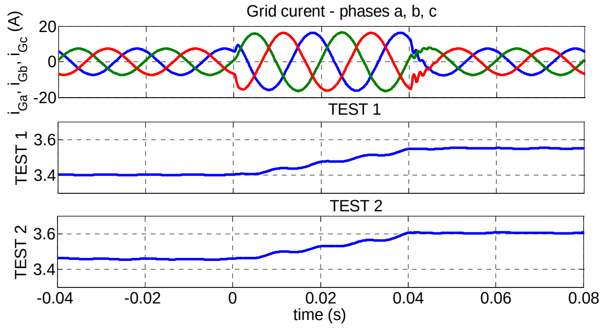

Fig. 9 Time responses of measured grid phase currents i_{Ga}, i_{Gb}, i_{Gc} and signals TEST1, TEST2. Attack is caused by halving i_{Ga}, i_{Gb}, i_{Gc} values.

Fig. 10 presents again the measured time responses of the grid phase currents i_{Ga}, i_{Gb}, i_{Gc} and the tests signals TEST1 and TEST2. The attack consists of the grid voltage sensor halving the actual voltage values at t = 0.0s and returning to real values at t = 0.04s. It is evident that the voltage sensor attack does not lead to errors in the actual grid currents, as the current controller does not utilize this voltage signal. Only small, rapid transients in the phase currents are detected at the beginning and end of the attack. Nevertheless, this attack is also detected by changes in the TEST1, and TEST2 values in relevant time intervals.

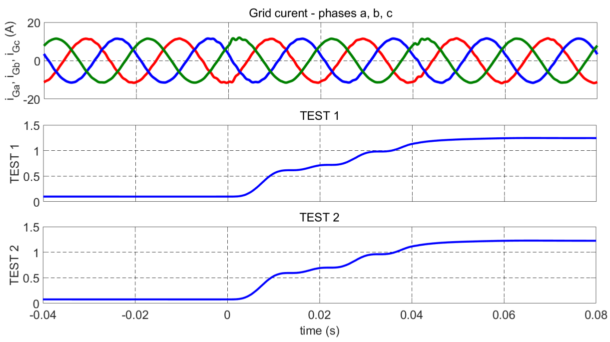

Fig. 10 Time responses of measured grid phase currents i_{Ga}, i_{Gb}, i_{Gc} and signals TEST1, TEST2. Attack is caused by halving v_{Ga}, v_{Gb}, v_{Gc} values.

6. Conclusion

This paper presents the implementation of a cyber attack detection strategy based on the watermark strategy for a grid-connected power electronic converter with an LCL filter. The same type of the GPCC, previously used for converters with L filters, is applied here for the converter with an LCL filter.

Simulation and experimental results are presented and discussed. The effectiveness of the proposed strategy under different types of the attacks on the current or voltage sensor is illustrated. The results confirm that the watermark strategy may be an effective tool for recognizing cyber-attacks on the control system.

7. Appendix

Parameters in equation (1):

$b_{2C}=RCL_2$
$b_{1C}=L_2+RR_2C$
$b_{0C}=R_2$

$a_{4C}=L_1L_2^2C$
$a_{3C}=L_1L_2CR_2+L_2[L_2CR_1+L_1C(R_2+R)+RC\,L_2]$
$a_{2C}=R_2[L_2CR_1+L_1C(R_2+R)+RCL_2]+L_2[R_1(R_2+R)C+L_1+L_2+RR_2C]$
$a_{1C}=L_2(R_1+R_2)+R_2[R_1(R_2+R)C+L_1+L_2+RR_2C]$
$a_{0C}=R_2(R_1+R_2)$

$b_{2G}=-L_1C$
$b_{1G}=-(R_1+R)C$
$b_{0G}=-1$

$a_{3G}=L_1L_2C$
$a_{2G}=L_1C(R_2+R)+(R1+R)L_2C$
$a_{1G}=(R_1+R)CR_2+RR_1C+L_1+L_2$
$a_{0G}=R_1+R_2$

Parameters in equations (3), (4):

$B_{0C}=(b_{2C}/T_s^2+b_{1C}/T_s)T_s+b_{0C}$
$B_{1C}=(-2b_{2C}/T_s^2-b_{1C}/T_s)T_s$
$B_{2C}=b_{2C}/T_s^2T_s$

$A_{0C}=(a_{4C}/T_s^4+a_{3C}/T_s^3+a_{2C}/T_s^2+a_{1C}/T_s)T_s+a_{0C}$
$A_{1C}=(-4a_{4C}/T_s^4-3a_{3C}/T_s^3-2a_{2C}/T_s^2-a_{1C}/T_s)T_s$
$A_{2C}=(6a_{4C}/T_s^4+3a_{3C}/T_s^3+a_{2C}/T_s^2)T_s$
$A_{3C}=(-4a_{4C}/T_s^4-a_{3C}/T_s^3)T_s$
$A_{4C}=a_{4C}/T_s^4T_s$

$B_{0G}=(b_{2G}/T_s^2+b_{1G}/T_s)T_s+b_{0G}$
$B_{1G}=(-2b_{2G}/T_s^2-b_{1G}/T_s)T_s$
$B_{2G}=(b_{2G}/T_s^2)T_s$

$A_{0G}=(a_{3G}/T_s^3+a_{2G}/T_s^2+a_{1G}/T_s)T_s+a_{0G}$
$A_{1G}=(-3a_{3G}/T_s^3-2a_{2G}/\,T_s^2-a_{1G}/T_s)T_s$
$A_{2G}=(3a_{3G}/T_s^3+a_{2G}/T_s^2)T_s$
$A_{3G}=(-a_{3G}/T_s^3)T_s$

Acknowledgement

The authors would like to acknowledge the support from the Institute of Thermomechanics of the Czech Academy of Sciences for its long-term conceptual development, RVO: 61388998, and the financial support of the Faculty of Electrical Engineering, CTU in Prague, research program Advanced SW for predictive management of energy consumption in decentralized energy systems, FW10010304, TA CR.

References:

[1] M. Kouki, B. Marinescu, and F. Xavier, “Exhaustive modal analysis of large-scale interconnected power systems with high power electronics penetration,” IEEE Trans. Power Syst., vol. 35, is. 4, pp. 2759-2768, Jul. 2020, **DOI:** 10.1109/TPWRS.2020.2969641.

[2] S. Musleh, G. Chen, and Z. Y. Dong, “A survey on the detection algorithms for false data injection attacks in smart grids,” IEEE Trans. Smart Grid, vol. 11, is. 3, pp. 2218-2234, May 2020, **DOI:** 10.1109/TSG.2019.2949998.

[3] E. Drayer and T. Routtenberg, “Detection of false data injection attacks in smart grids based on graph signal processing,” IEEE Syst. J., vol. 14, is. 2, pp. 1886-1896, Jun. 2020, **DOI:** 10.1109/JSYST.2019.2927469.

[4] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, and P. Dehghanian, “Electric power grid resilience to cyber adversaries: State of the art,” IEEE Access, vol. 8, pp. 87592-87608, May 2020, **DOI:** 10.1109/ACCESS.2020.2993233.

[5] F. Pasqualetti, F. Dorfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” IEEE Trans. Automatic Control., vol. 58, is. 11, pp. 2715–2729, Nov. 2013, **DOI:** 10.1109/TAC.2013.2266831

[6] M. Leng, S. Sahoo, F.Blaabjerg, “Stabilization of DC Microgrids Under Stealth Cyber Attacks-Optimal Design and Sensitivity Analysis.” Vol. 15, is. 1, is: pp: 113-123, Jan 2024, **DOI:** 10.1109/TSG.2023.3278094

[7] B. Satchidanandan and P. R. Kumar, “Dynamic watermarking: Active defense of networked cyber-physical systems,” Proceedings of the IEEE, Vol. 105, Is. 2, pp. 219-240, Feb. 2017, **DOI:** 10.1109/JPROC.2016.2575064.

[8] J. Kim, W.H. Ko and P. R. Kumar, “Cyber-security with dynamic watermarking for process control systems,” AIChE annual meeting 2019, No. 452a, Nov. 2019.

[9] Vasquez et al., J. I. Leon, L. G. Franquelo, J. Rodriguez, H. A. Young, A. Marquez “Model predictive control: A review of its applications in power electronics,” IEEE Ind. Electron. Mag., vol. 8, no. 1, pp. 16-31, March 2014, **DOI:** 10.1109/MIE.2013.2290138

[10] H. A. Young, M. A. Perez, J. Rodrigues, H. Abu-Rub, “Assesing finite-control-set model predictive control: A comparison with a linear current controller in two-level voltage source inverters,” IEEE Ind. Electron. Mag., vol. 8, no. 1, pp. 44-52, March 2014. **DOI:** 10.1109/MIE.2013.2294870

[11] T. Geyer and D. E. Quevedo, “Performance of multistep finite control set model predictive control for power electronics,”IEEE Trans. Power Electron., vol. 30, no. 3, pp. 1633–1644, Mar. 2015. **DOI:** 10.1109/TPEL.2014.2316173

[12] Z. Song, Y. Tian, W. Chen, Z. Zou, and Z. Chen, “Predictive duty cycle control of three-phase active-front-end rectifier,”IEEE Trans. Power Electron., vol. 31, no. 1, pp. 698–710, Jan. 2016. **DOI:** 10.1109/TPEL.2015.2398872

[13] S. Vazquez, J. Rodriguez, M. Rivera, L. G. Franquelo, and M. Norambuena, “Model Predictive Control for Power Converters and Drives: Advances and Trends,” IEEE Trans. Ind. Electron., vol. 64, no. 2, pp. 937, Feb. 2017. **DOI:** 10.1109/TIE.2016.2625238

[14] D. W. Clarke, C. Mohtadi, P. S. Tuffs, “Generalized predictive control–part I: The basic algorithm,” Automatica, vol. 23, no. 2, pp.137-148, 1987. DOI: 10.1016/0005-1098(87)90087-2

[15] S. Vazquez, C. Montero, C. Bordons, L. Franquelo, “Design and experimental validation of a model predictive control for a VSI with long prediction horizon,” Proc. 39th annual Conf. IEEE Ind. Electr. Society (IECON’13), pp. 5788-5793, Nov. 2013. **DOI:** 10.1109/IECON.2013.6700083

[16] M. G. Judewicz, S. A. Gonzalez, N. I. Echeveria, J. R. Fischer, D. O. Carrica,”Generalized predictive current control (GPCC) for grid-tie three-phase inverters,” IEEE Trans. Ind. Electron., vol. 63, no. 7, pp. 4475- 4484, July 2016. **DOI:** 10.1109/TIE.2015.2508934

[17] M. G. Judewicz, N. I. Echeverrıa, J. R. Fischer, S. A. Gonzalez and D. O. Carrica,” Generalized Predictive Control of Three-Level Boost Rectifiers,” XVII Workshop on Information Processing and Control (RPIC), Mar del Plata, Argentina, September 2017. **DOI:** 10.23919/RPIC.2017.8211626

[18] P. Simek, M. Bejvl, V. Valouch: Power Control for Grid-Connected Converter Based on Generalized Predictive Current Control. IEEE JOURNAL OF EMERGING AND SELECTED TOPICS IN POWER ELECTRONICS, VOL. 10, NO. 6, pp. 7072-7083, DECEMBER 2022, DOI: 10.1109/JESTPE.2022.3208777

[19] M. Bejvl, V. Valouch.: LCL Filter Design for Interconnection Inverter of Distributed Source to Utility Grids. In Proc. of the 17th Int. Sci. Conf. Electric Power Engineering 2016. Prague, Czech Republic, 16-18 May 2016, **ISBN:**978-1-5090-0909-1, DOI: 10.1109/EPE.2016.7521832

[20] R. Pena-Alzola, M. Lissere, F. Blaabjerg, R. Sebastian, J. Dannehl, F. W. Fuchs.: Analysis of the Passive Damping Losses in LCL-Filter-Based Grid Converters. IEEE TRANSACTIONS ON POWER ELECTRONICS, VOL. 28, NO. 6, JUNE 2013, pp. 2642-2646. **DOI:** 10.1109/TPEL.2012.2222931

[21] Z. Zou, Z. Wang, M. Cheng.: Modeling, Analysis, and Design of Multifunction Grid-Interfaced Inverters With Output LCL Filter. IEEE TRANSACTIONS ON POWER ELECTRONICS, VOL. 29, NO. 7, JULY 2014. pp. 3830-3839. **DOI:** 10.1109/TPEL.2013.2280724

[22] R. N. Beres, X. Wang, M. Liserre, F. Blaabjerg, and C. L. Bak, “A review of passive power filters for three-phase grid-connected voltage-source converters,”IEEE J. Emerg. Sel. Topics Power Electron., vol. 4, no. 1, pp. 54–69, Mar. 2016. **DOI:** 10.1109/JESTPE.2015.2507203

[23] Y. Wu, T. B. Soeiro, A. Shekhar, J. Xu and P. Bauer, “Virtual Resistor Active Damping with Selective Harmonics Control of LCL-Filtered VSCs,” 2021 IEEE 19th International Power Electronics and Motion Control Conference (PEMC), Gliwice, Poland, 2021, pp. 207-214, **DOI:** 10.1109/PEMC48073.2021.9432569.

[24] B. Hoff, “Cascaded Model Predictive Control of Grid Connected Converter with LCL Filter,” IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 2018, pp. 5277-5282, **DOI:** 10.1109/IECON.2018.8591137.

[25] T. Dragičević, C. Zheng, J. Rodriguez, and F. Blaabjerg, “Robust QuasiPredictive Control of LCL-Filtered Grid Converters,” in IEEE Transactions on Power Electronics, vol. 35, no. 2, pp. 1934-1946, Feb. 2020, **DOI:** 10.1109/TPEL.2019.2916604.

[26] T. Zhao, M. Zhang, C. Wang, and Q. Sun, “Model-Free Predictive Current Control of Three-Level Grid-Connected Inverters With LCL Filters Based on Kalman Filter,” in IEEE Access, vol. 11, pp. 21631-21640, 2023, **DOI:** 10.1109/ACCESS.2023.3251410

[27] M. G. Judewicz, S. A. González , J. R. Fischer , Juan F. Martínez, and D. O. Carrica,” Inverter-Side Current Control of Grid-Connected Voltage Source Inverters With LCL Filter Based on Generalized Predictive Control,” IEEE Journal of Emerging and Selected Topics in Power Electronics, Volume. 6, no. 4, December 2018, DOI: 10.1109/JESTPE.2018.2826365