Cyber-attacks in modular multilevel converters

Claudio Burgos-Mellado, *Member, IEEE*, Felipe Donoso, *Member, IEEE*, Tomislav Dragičević, *Senior Member, IEEE*, Roberto Cárdenas-Dobson, *Senior Member, IEEE*, Patrick Wheeler, *Senior Member, IEEE*, Jon Clare, *Senior Member, IEEE*, Alan Watson, *Senior Member, IEEE*

***Abstract*—Distributed control of modular multilevel converter (MMC) submodules (SMs) offers several potential benefits such as flexibility, scalability and modularity. In this approach, low-level control tasks, such as capacitor voltage balancing, can be distributed amongst controllers placed in the SMs. This decreases the computational burden for the central control system that performs high-level control tasks; also, a single point of failure is avoided. Distributed control architecture requires a cyber-physical network (CFN) through which local controllers share all the information necessary to perform their respective control loops. To date, none of the reported works in this field have paid attention to potential imperfections in the CFN. Indeed, previous works are based on the assumption that the network always provides correct information to the local controllers. However, erroneous measurements in the CFN may degrade the distributed control scheme operation, leading to suboptimal or even unstable operation. These events can occur in the presence of cyber-attacks, for example, which can be created through illegitimate data intrusion into the distributed control architectures. This paper is the first to investigate the impacts of cyber-attacks on distributed control schemes used in MMCs. The effects of a specific cyber-attack, named false data injection attack (FDIA), on a consensus-based distributed control strategy are studied in this work. Additionally, a method for detecting FDIAs is proposed, along with a countermeasure strategy, to ensure the safe operation of the MMC whilst the attack is cleared. The proposals reported in this paper are validated using simulation and experimental results.**

***Index Terms*—Modular multilevel converters, Distributed control, Cyber-attacks, False data injection attack, Consensus theory, Kalman filter.**

I. Introduction

THE modular multilevel converter (MMC) is a solution for medium to high-voltage, high-power conversion applications, such as high voltage direct current (HVDC) transmission systems, offshore wind farms, and static synchronous compensators (STATCOMs) [1]. The main features of this converter are: (i) modular construction, (ii) voltage and power scalability, (iii) high efficiency, (iv) low harmonic distortion, and (v) the use of low-cost, low-voltage semiconductor technology [1].

The MMC comprises several building blocks named submodules (SMs), as shown in Fig. 2. The SM can be a range of different power converter circuits such as the half-bridge (HBSM), full-bridge (FBSM), flying capacitor (FCSM), and neutral-point clamped (NPCSM) circuit.

The MMC control scheme involves several objectives: output current control, circulating current control, and SMs capacitor voltage control. The latter can be divided into three control objectives [2]: (i) leg voltage control, (ii) upper and lower arm capacitor voltage control, and (iii) balancing the SM capacitor voltage inside each arm. Typically, these objectives are fulfilled using a centralised control approach; i.e. a single central controller is controlling the whole MMC. This central controller also generates the PWM signals for all of the switches [2], [3]. The main disadvantage of this approach is that the central controller needs an extensive processing capability and multiple digital outputs and communication channels for the switching signals, increasing the implementation complexity [2], [3]. This situation is especially critical for the MMC which has a high number of submodules, since the execution time might not be sufficient to perform all of the control tasks in each control cycle [4]. Moreover, the central controller represents a single point of failure. Thus, the centralised control approach limits the modularity, flexibility and expandability of an MMC with many SMs, in terms of software development. In recent years, the use of the distributed control approach for controlling modular multilevel topologies has received increased attention from researchers (see Table I). In this strategy, local controllers in the SMs (working in a distributed architecture) perform low-level control tasks such as the capacitor voltage balancing and PWM generation. A central controller still performs the high-level control tasks. This approach results in a more reliable and modularised system, with fewer signal wires, since the computational burden can be distributed among the local controllers placed in the submodules. [5].

The reported works in this area can be categorised as shown in Fig. 1. In these approaches, low-level control tasks are distributed among local controllers placed in the SMs. This is done by follower controllers in the leader/follower architecture, by distributed control schemes in the hybrid architecture, and by a distributed control scheme based on the consensus theory [6] in the consensus-based architecture. It should be pointed out that, different from the standard approaches (such as leader/follower and hybrid), the consensus-based method only needs sparse communication among the neighbouring sub-modules [6], [7].

The distributed architectures displayed in Fig. 1 have been proposed for several multilevel converter topologies, such

This work was supported in part by "Agencia Nacional Investigacion y Desarrollo" (ANID) under Grant: ANID/FONDECYT de Iniciación/11220989

C. Burgos-Mellado is with the Institute of Engineering Sciences, Universidad de O'Higgins, Rancagua, Chile (email: claudio.burgos@uoh.cl)

F. Donoso, P. Wheeler, J. Clare and A. Watson are with the Power Electronics, Machines and Control Group, University of Nottingham, Nottingham NG72RD, U.K. (emails: felipe.donoso2@nottingham.ac.uk; pat.wheeler@nottingham.ac.uk; jon.clare@nottingham.ac.uk; alan.watson@nottingham.ac.uk)

R. Cárdenas-Dobson is with the Department of Electrical Engineering, Faculty of Physical and Mathematical Sciences, University of Chile, Santiago 8370451, Chile (email: rcd@ieee.org)

T. Dragičević is with the Electrical Engineering Department of Technical University of Denmark, Copenhagen, Denmark (email: tomdr@elektro.dtu.dk)

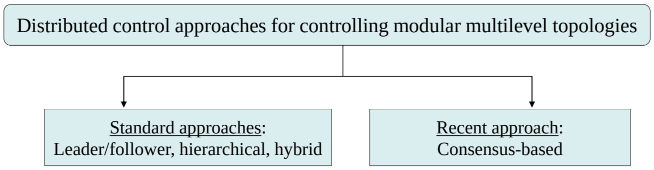

Distributed control approaches for controlling modular multilevel topologies
Standard approaches:
Leader/follower, hierarchical, hybrid
Recent approach:
Consensus-based

Fig. 1. Distributed control architectures used for controlling modular multilevel topologies.

TABLE I
REPORTED WORKS PROPOSING DISTRIBUTED CONTROL SCHEMES FOR MODULAR MULTILEVEL TOPOLOGIES

	CHB	MMC	M3C
Standard approaches	[5], [8], [9]	[4], [10]–[21]	[22], [23]
Consensus-based approach	[7], [24]–[26]	[27]	—

as the cascaded H-bridge (CHB) multilevel converter, MMC and M3C. Table I, summarises the reported papers proposing distributed control schemes for these topologies, classified following the categorisation presented in Fig. 1.

It is worth noting that all the papers reported in Table I assume a reliable CFN that reports true measurements. As already mentioned, erroneous measurements can occur in the presence of cyber-attacks [28], which can be created through illegitimate data intrusion into the CFN. Examples of cyber-attacks are: (i) false data injection attacks (FDIAs) [29] and (ii) replay attacks [30]. Additionally, there are other types, such as denial of service attacks, for example [29]. It is interesting to note that cyber-attack issues are intensively investigated in other electrical systems such as microgrids [28], modern power systems [31], and electric vehicle charging infrastructure [32]. Regarding cyber-attack issues in the MMC (and multilevel converters in general), the recent letter [33] is the only work reported in this area so far. That paper shows (via simulations) that an FDIA in the sensors of an MMC can affect the stability of its centralised control system. However, to the best of the authors' knowledge, there are no published papers addressing cyber attack issues on distributed control schemes used with MMCs. Thus, several open research questions need to be addressed, such as a study of the impacts of cyber-attacks on distributed control schemes, designing methods for their detection, and implementing countermeasures to deal with them.

To fill the research gaps identified above, this paper demonstrates that cyber-attacks affect the performance and operability of distributed control schemes used for MMCs. In particular, this article focuses on investigating the effects of FDIAs on the performance of a consensus-based distributed control scheme for an MMC. Secondly, a method, based on the Kalman filter (KF), to detect FDIAs is proposed along with countermeasures to ensure safe operation of the MMC while the attacks are cleared. The contributions of this paper are:

1) This is the first paper to investigate the impact of FDIAs, as the most common type of cyber-attack, on MMC converters whose submodules are controlled in a distributed way. It is found that cyber-attacks can affect the normal operation of the control system of the MMC, leading to power quality issues and operability issues.
2) A Kalman filter-based method to detect FDIAs is proposed. This method is implemented in each local controller of the SMs and operates in a distributed manner. Thus, only scalar mathematical operations are required for its implementation. Based on the information provided for the proposed KF, a countermeasure is proposed to ensure safe operation of the MMC during cyber-attacks. Both proposals are validated through simulations and experimental results.

II. DISTRIBUTED CONTROL STRATEGY FOR MMC

Fig. 2 shows the three-phase MMC considered in this work composed of two arms (positive and negative) in each phase. Each arm has N half-bridge-based SMs connected in series and an arm inductor L_{arm}. The converter is controlled by the control architecture shown in Fig. 3. In this scheme, control of the output current, the circulating currents, the arm balance, the total energy and the DC-link voltage are performed by the central controller, implemented in the $\Sigma\Delta\alpha\beta0$ reference frame, discussed in [34]. The consensus-based distributed control scheme shown in Fig. 3 is based on [26], [27], and is in charge of the capacitor voltage balancing control. For the sake of completeness, the following section summarises the main aspects of the consensus theory applied to control the capacitor voltages of each SM within an MMC. More information about this theory can be found in [6].

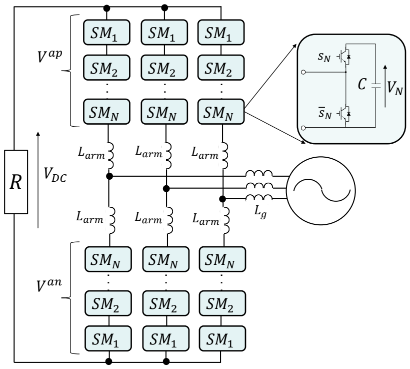
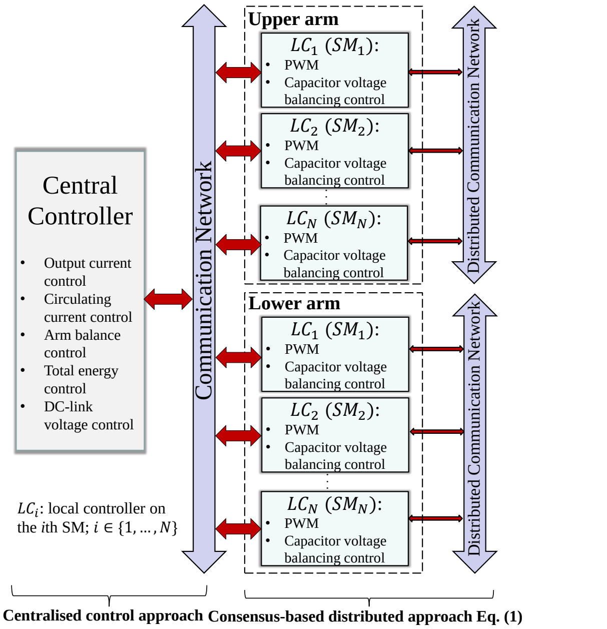


Fig. 2. Circuit topology of the three-phase MMC considered in this work.

A. Consensus-based distributed control approach for MMC

Note that in Fig. 3, the consensus-based distributed control scheme operates separately in each MMC arm. Therefore, the mathematical analysis performed in this section only considers one arm of the MMC; for the other arms, the procedure is identical.

Fig. 4 shows the upper arm in one of the three phases of the MMC displayed in Fig. 2. In this case, a consensus-based control scheme for balancing the capacitor voltages in that arm is implemented as follows: let us consider that the distributed communication network displayed in Fig. 4 corresponds to a bidirectional network modelled as an undirected cyber graph $\mathbb{G} = (\mathfrak{N}, \xi, B)$ among the SMs $\mathfrak{N} = \{1, ..., N\}$, where ξ is the set of communication links and B is a non-negative $N \times N$ weighted adjacency matrix [6]. The elements of B are $b_{ij} = b_{ji} \geq 0$, with $b_{ij} \geq 0$ if and only if $\{i, j\} \in \xi$. Also, let us assume that each SM corresponds to a node of the graph $\mathbb{G}$ with a scalar first-order single-integrator dynamics.


Upper arm
LC_1 (SM_1):
PWM
Capacitor voltage balancing control
LC_2 (SM_2):
PWM
Capacitor voltage balancing control
LC_N (SM_N):
PWM
Capacitor voltage balancing control
Distributed Communication Network
Central Controller
Output current control
Circulating current control
Arm balance control
Total energy control
DC-link voltage control
Communication Network
Lower arm
LC_1 (SM_1):
PWM
Capacitor voltage balancing control
LC_2 (SM_2):
PWM
Capacitor voltage balancing control
LC_N (SM_N):
PWM
Capacitor voltage balancing control
Distributed Communication Network
LC_i: local controller on the ith SM; $i \in \{1, \ldots, N\}$
Centralised control approach
Consensus-based distributed approach Eq. (1)

(*) Voltage measurements are interchanged between the LCs through the distributed communication network

Fig. 3. Scheme of the control system for the MMC used in this work: a central control is in charge of the high-level tasks, whereas a distributed control scheme is in charge of balancing the capacitor voltage in each SM. (Two arms are shown).

Under this framework, it can be said that the capacitor voltages which belong to the cyber graph $\mathbb{G}$ (see Fig. 4) achieve consensus if $[V_i(t) - V_j(t)] \rightarrow 0$ as $t \rightarrow \infty$ [26], [27]. In this situation, the consensus can be achieved via a feedback loop by applying the protocol u_i given by (1) (known as a local voting protocol [6]). This control is distributed, i.e. it only depends on the immediate neighbours $j \in \mathfrak{N}(i)$ of node i in the graph topology.

In (1), terms b_{ij} represent the entries of the adjacency matrix, meaning that V_j is shared with the ith SM if b_{ij} is not zero. The gain k_i modifies the transient behaviour of the controller: it depends on the current through that arm (I) (see Fig. 4). [26], [27]

$$u_i = -\frac{1}{k_i} \sum_{j \in \mathfrak{N}(i)} b_{ij} \cdot (V_i - V_j) \,. \tag{1}$$

By using this approach on the control architecture shown in Fig. 3, the overall control action ($U_i^{overall}$) for the ith SM, which is sent to the modulation stage, is composed of two parts, as shown in (2). In this equation, U_i is generated by the central controller to regulate the high-level control tasks (N is the number of SMs per arm), whereas u_i is generated by the consensus-based distributed control scheme for achieving the capacitor voltage balancing control amongst the SMs. (See Fig. 8 for more details)

$$U_i^{overall} = U_i/N + u_i \tag{2}$$

III. Definitions and Impacts of FDI Attacks in MMC

The previous section introduced the basis of the consensus theory applied to regulate the SM capacitor voltages of an MMC. However, in that approach, the occurrence of cyber-attacks was not considered. Such attacks should be considered since they could cause destabilisation of the MMC or discreetly penetrate the control system. The attacker could use the latter tactic to collect sensitive data of the system for a posterior coordinated attack [28] and provoke a shutdown of the MMC. It is worth remembering that there are several types of cyber-attacks. This paper considers the *false data injection attack* (FDIA) since it is regarded as a prominent attack methodology in other electrical systems such as DC microgrids and smart grids [28], [31]. Fig. 4 shows an FDIA being executed on the voltage sensor of the SM_1 placed in one of the upper arms of the MMC. Note that in this figure the FDIA will be propagated to the other SMs through the distributed communication network, affecting the distributed control scheme in that arm and the whole operation of the MMC.

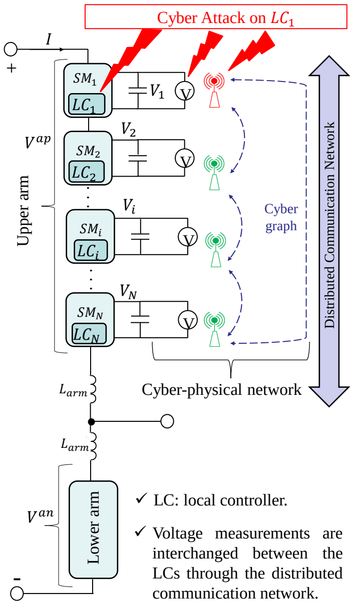


Fig. 4. Example of SMs in an MMC operating in a distributed control scheme.

Let us consider that the MMC converter is regulating the capacitor voltages in its cells via the consensus-based distributed control scheme shown in Fig. 3, as discussed in the previous section. This consensus algorithm is based on voltage measurements; thus, FDIAs, like that shown in Fig. 4, can occur on the voltage sensors of the SMs. In this case, an FDI attack in the ith SM of the MMC is modelled as follows:

$$Sensor \quad attack: \quad V_i^f(t) = V_i(t) + \kappa V_i^a(t) \tag{3}$$

where κ=1 denotes the presence of an attack sequence $V_i^a(t)$ in the voltage measurement $V_i(t)$ in the ith SM, otherwise κ=0. Note that the sensor attack can be conducted by hijacking the local controllers as shown in Fig. 4, meaning that the attacked controllers send erroneous voltage measurements to their neighbours [35].

A case study is developed to investigate the impact of the FDIAs given by (3) on the control system of the MMC shown in Fig. 3. To this end, the MMC converter illustrated in Fig. 2 is simulated using PLECS software with the parameters listed in Table II and Table III. The MMC is controlled using the control scheme shown in Fig. 3, where the central controller is implemented in the $\Sigma\Delta\alpha\beta 0$ reference frame (see [34]), and the distributed control scheme corresponds to that discussed in Section II-A.

In this test, the sequence attack (4) is used to emulate an FDIA. Here, V_i^a represents the attack sequence introduced into the voltage sensor measurement of the ith SM located in the upper arm shown in Fig. 4, t_i^{attack} is the time instant at which the attack on the ith SM starts and v_i^a corresponds to the attack element on that SM.

$$V_i^a(t) = \begin{cases} 0 & if \quad 0 \leq t < t_i^{attack} \\ v_i^a & if \quad t \geq t_i^{attack} \end{cases} \tag{4}$$

In this test, the voltage sensors associated with SM 1 and SM 2 (Fig. 4) are attacked by an FDIA at $t_1^{attack} = t_2^{attack} = 1s$ which persists, with the attack elements $v_1^a = -0.3$ p.u., and $v_2^a = -0.5$ p.u., respectively (the base is v_C^*, see Table II). Later on, another attack element $v_{15}^a = 0.4$ p.u., is introduced on the voltage sensor of SM 15, at $t_{15}^{attack} = 2s$.

Fig. 5(a), shows the real capacitor voltages on the attacked arm during the whole test. As shown, the capacitor voltage balancing in that arm is lost when the FDIAs of a given magnitude are introduced. In this case, the capacitor voltage in some SMs increase while others decrease, depending on the magnitude and sign of the attack element introduced. This behaviour potentially leads to the shutdown of the MMC since some capacitor voltages may reach the over-voltage and/or under-voltage threshold, activating the protection system of the MMC. In the case illustrated in Fig. 5(a), the voltage at SM$_1$ and SM$_2$ may activate the over-voltage protection; whereas the voltage at SM$_{15}$ may activate the under-voltage protection.

It is worth noting that the capacitor voltages depicted in Fig. 5(a) correspond to the real ones (those measured directly across the capacitor of each SM) before and after the occurrence of the FDIA. However, from the control system point of view, these voltages look different because of the inclusion of the FDIAs. To exemplify this, Fig. 5(b) shows the capacitor voltages seen by the local controllers on the attacked arm during the whole test (the central controller sees these voltages as well). From this figure, it is concluded that the local controllers reach a consensus point between the capacitor voltages before and after the FDIA. In particular, when the FDIAs start at $t = 1s$ and $t = 2s$, respectively, the consensus-based control scheme interprets the FDIA as a new operating point of the system (the same for the central controller). However, in reality, the reference operating point of the system has not changed, and the voltage variation on the attacked SMs are due to the FDIA. In this situation, everything looks fine for the control system; however, in reality, the normal operation of the MMC is affected, which might produce a critical failure of the MMC.

Fig. 6 shows the grid current before and after the first FDI attack considered in this test. As seen in Fig. 6(a), the grid current is balanced and with a low THD before the attack. In contrast, when the first attacks start, the grid current becomes unbalanced and its distortion increases as shown in Fig. 6(b). Therefore, the FDIA also affects the power quality of the MMC.

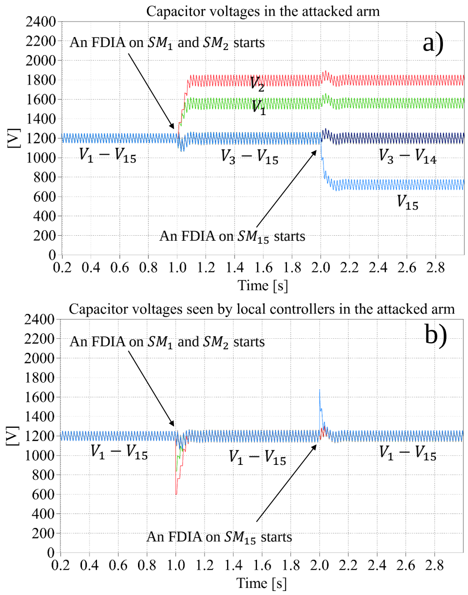


Fig. 5. (a) Real capacitor voltages on the attacked arm, (b) Capacitor voltages seen by the local controllers in the attacked arm.

From the results discussed in this section, it can be concluded that the control system of the MMC cannot distinguish if changes in voltage measurements are due to a change in the reference operating point of the MMC or due to an FDI attack. Also, it was shown that the FDIA affects the voltage balancing in the MMC and its power quality, and may lead to possible operability issues. Thus, methods for its detection and countermeasures to deal with it are needed.

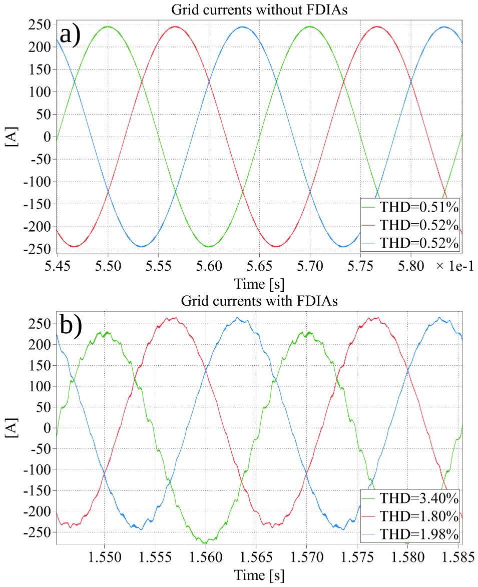


Fig. 6. (a) Grid current without FDI attacks, (b) Grid current when SM_1 and SM_2 of the arm shown in Fig. 4 is being attacked.

Finally, it must be recalled that in this work, FDIAs on voltages sensors measurements are studied as the distributed control scheme used for controlling the MMC is based on those measurements (see equations (1)-(2) in section II-A).

A. Practical aspects of cyber-attacks targeting MMCs

To begin with, it is essential to state the difference between cyber-attacks and communications errors affecting the communication network of the MMC control system (see Fig. 3). In this sense, communications errors correspond to random, and not persistent failures such as communication delays and communication link failures [36]. In contrast, cyber-attacks correspond to malicious attacks perpetrated by one or more attackers [37], aiming to destabilise the operation of the attacked system.

In the context of cyber-attacks targeting MMCs, it is worth recalling that the FDIA considered in this work is modelled by (3). It corresponds to the principal FDIA studied in other electrical systems such as microgrids and modern power systems [28], [31]. Based on that, and considering that there is very little literature on cyber-attacks for MMC [33], the selection of the FDIA (3) is a sensible starting point to provide the first steps to address for research into cyber-attacks in MMC. From here, more elaborate FDIA can be studied in future research efforts.

Even though the FDIA (3) could be considered as a basic cyber-attack, it represents a real threat to systems. This is evidenced by its use in the following real cases:

1) In [38], [39], it is argued that an FDIA similar to the one considered in this paper (see (3)) can counterfeit the value of the state of charge (SoC) measurements of the battery management system (BMS) in lithium-ion battery banks. Indeed, counterfeit battery bank parameters can make the battery work in an unsafe operating zone. This happened in 2019 in Korea, resulting in fire and damage to the battery bank [38].
2) In [40], a security researcher hacked an Apple MacBook battery introducing an FDIA to deceive the battery state of charge (SoC) estimator into reporting a low charge. This generated the activation of the charging circuit of the battery producing an overcharging of it, and as a consequence, the device was bricked.
3) An FDIA related to energy theft affected energy companies [41] in the USA, generating economic losses to these companies. In these attacks, FDIAs affected smart meters by sending false energy measurements to the utility company [41].

In addition, in the following works have been discussed that FDIAs are a plausible threat for the following real systems:

1) In [42], it is argued that in the cyber-attack that affected the Ukraine power grid in 2015, all the conditions to apply an FDIA were fulfilled. That paper concluded that the circumstances of the Ukraine blackout are enough to mount a successful FDIA on an electric power system.
2) In [43], it is argued that an FDIA affecting the measurements of power flow through the lines of a power system can cause overloading of one or more lines. This can result in cascading failure as that occurred in the 2003 northeast blackout [43].

Considering the events described above, it can be concluded that FDIAs can be regarded as real threats to real systems; therefore, they must be studied. Now, focusing on the MMC, particularly its use for HVDC applications, it must be considered that this converter is placed in a substation along with other electrical systems, as shown in Fig. 7. As observed, all the devices of the substation are coordinated and monitored by the supervisory control, data acquisition (SCADA) system. The SCADA system is usually hosted on communication infrastructure comprising wide area networks (WAN), field area networks (FAN), local area networks (LAN), among others [44], which is susceptible to cyber-attacks [37], [44].

In the context described above, a potential cyber-attack might penetrate into the SCADA system via any computer placed in the control center [37]. And from there, it can be propagated to the MMC via the communication network (see Fig. 7). Note that cyber-attacks targeting SCADA systems have been reported several times in real systems; examples of this are: (i) the attack targeting the SCADA system of the sewage control system in Maroochy Shire in Australia [45], (ii) the cyber-attacks that targeted the SCADA system of the Ukrainian power grid, causing a power outage that affected approximately 225,000 customers [42], (iii) the cyber-attack that affected the electrical power grid of Israel in 2016 [41]. Therefore, cybersecurity concerning the SCADA system and to the devices in the substation (see Fig. 7) is of vital importance.

Based on the above, and considering that the MMC is a promising solution to transfer power over long distances, with several commercial projects based on it (Trans Bay Cable, Dolwin2, Nano3-terminal DC grid, etc. [46], [47]), it can be concluded that cyber-attacks on the MMC seem to be likely and therefore, they must be considered for future projects based on this converter. In particular, this work starts this research area considering the FDIA (3), and from here, more investigation in this incipient area could be performed.

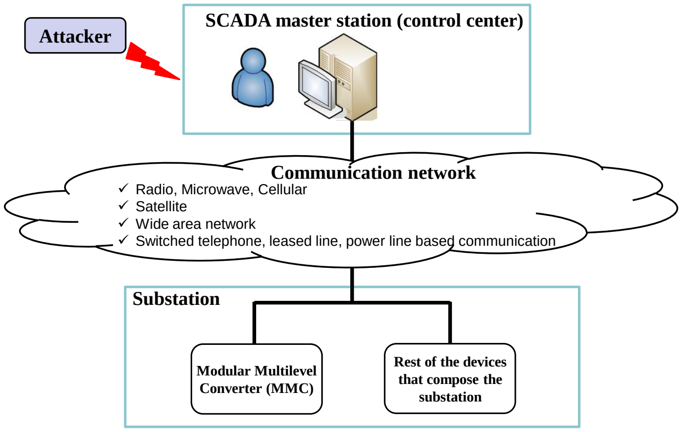

Attacker
SCADA master station (control center)
Communication network
✓ Radio, Microwave, Cellular
✓ Satellite
✓ Wide area network
✓ Switched telephone, leased line, power line based communication
Substation
Modular Multilevel Converter (MMC)
Rest of the devices that compose the substation

Fig. 7. Implementation of an MMC in a substation: All the devices of the substation are monitored by a SCADA system located in the control center.

IV. Proposed Kalman Filter-Based Method for Detecting FDIAs and Countermeasures

As concluded in the previous section, local controllers cannot identify if a variation in their voltage measurements are due to a change in the operating point of the MMC, or due to an FDIA. In the latter case, the FDIAs will affect the control system performance, produce power quality issues, and eventually produce operability issues. To avoid this critical situation, it is paramount to implement methods to detect the FDIA and countermeasures in the local controllers of the SMs to mitigate such an attack.

In this sense, Fig. 8 shows the scheme of the proposed distributed detection method along with the proposed countermeasures to deal with FDIAs. In this figure, the local controller related to the ith SM is displayed. As seen, the proposed FDIA detection method aims to complement each SM with an observer that estimates the SM voltage and then compares it with the measured voltage. Based on these voltages, the following magnitudes are calculated locally by the ith local controller (see Fig. 8 and Algorithm 1): (i) the residual index $r_i(k)$, (ii) the reliability index $\psi_i(k)$, and the compensation gain $G_i(k)$. Then, if $r_i(k)$ surpasses a predefined threshold, it means that the SM is being attacked, and its voltage reading $V_i(k)$ is not trustworthy. In this case, the reliability $\psi_i(k)$ is set at 1, and the compensation gain $G_i(k)$ is different from zero. The gain $G_i(k)$ is used to compensate for the attacked voltage measurements, allowing safe operation of the MMC while the FDIAs are neutralised. The latter can be done either by injecting corrective action in the attacked sensors or replacing the whole attacked SMs with redundant SMs typically available in MMCs. [1]

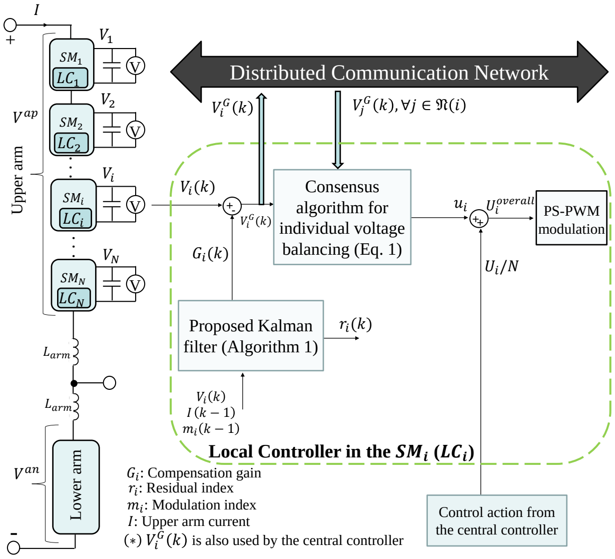


Fig. 8. Proposed scheme for detecting FDIA and countermeasures to deal with those attacks: Implementation on the LC_i local controller.

As observed in Fig. 8, a Kalman filter-based FDIA detection method is proposed. This filter is a well-known algorithm extensively used in many fields. References [48], [49] provide more information about this method. Focusing on MMCs, there are recent works [49]–[51] proposing centralised KF-based observers for implementing sensorless control schemes. In their implementation, they perform operations among matrices, increasing the computational burden for the central controller. Indeed, as discussed in [52], the algorithm complexity of the KF proposed in [49]–[51] is $O(m^{2.376} + n^2)$, where m is the observation dimension, and n the number of states, which makes its implementation in MMCs with high number of SMs difficult. Thus, distributed KF-based observers can be an effective solution to overcome this issue. In this paper, an FDIA detector based on a distributed KF-based observer is proposed. This observer can be easily implemented in the local controllers of the SMs since its implementation requires only scalar mathematical operations. It is discussed below.

Let us consider the ith SM in the upper arm shown in Fig. 8. The dynamics of the ith SM (in discrete-time), are given by (5) [50], [51]. In this equation, T is the sampling time, $m_i(k-1)$ is the modulation index at the time instant $k-1$, $I(k-1)$ is the arm current (see Fig. 8), C_i is the capacitance of the ith SM, and $w_i(k)$ is the process noise with covariance Q_i. Note that in (5) $w_i(k)$ quantifies the error in the modeling process [48].

$$V_i(k) = V_i(k-1) + \frac{T \cdot m_i(k-1) \cdot I(k-1)}{C_i} + w_i(k) \quad (5)$$

To implement the proposed KF-based observer, equation (5) is considered the state equation of the system, while (6) is considered as the observation equation. In this latter equation, $V_i(k)$ corresponds the the capacitor voltage in the ith SM, and v_i corresponds to the measurement noise, characterised by a covariance R_i.

$$y_i(k) = V_i(k) + v_i(k). \quad (6)$$

Using (5) as the state equation, and (6) as the observation equation, the ith SM could estimate its capacitor voltage running the well-known KF. However, in the context of FDI attacks, additional consideration needs to be taken into account. Indeed, since the KF uses the capacitor voltage $V_i(k)$ to update the state, and considering that this voltage is affected by an FDIA, the SM voltage estimation will be affected (it will follow the attacked voltage and not the real one) [53], [54]. Thus, the FDIA detection cannot be made. With this consideration in mind, in this paper, an FDIA detection method is proposed based on a modified KF able to work with FDIA in their measurements: it is shown in Algorithm 1. This algorithm considers that it is being run in the local controller placed on the ith SM in the arm shown in Fig. 8. The rest of the local controllers follow the same procedure.

In Algorithm 1, stages 1-3 correspond to the Kalman Filter implementation [48]. This implementation is augmented by adding the proposed stage 4, where an analysis of the measurement reliability is performed. In this stage, the voltage $V_i^{trust}(k)$ is defined, and is used for updating the Kalman filter (see stage 5 in Algorithm 1). This voltage is equal to the measured one $V_i(k)$ if the ith SM is not being attacked. Otherwise, this voltage is considered not trustworthy, and it is compensated by the gain $G_i(k)$. (See step 4)

In stage 4, an FDI attack is detected based on the index $g_i(k)$. It is defined as the difference between the voltage measured $V_i(k)$, and that estimated $\hat{V}_i(k/k-1)$ by the KF in stage 3, with the information in $k-1$. If the absolute value of $g_i(k)$ is above a pre-specified threshold c, it indicates that an FDIA is attacking the voltage sensor that measures $V_i(k)$, at the time instant k. In this case, the reliability index $\psi_i(k)$ is set at 1, the compensation gain $G_i(k)$ is calculated at the beginning of the attack as shown in Algorithm 1 (step

4), and the voltage $V_i^{trust}(k)$ is calculated as: $V_i^{trust}(k) = V_i(k) - G_i(k)$. Note that the pre-specified threshold "c" is determined heuristically based on the data of healthy operation (operation without any cyber-attack) and not healthy operation (operation with FDIAs) of the MMC (this data can get from numerical simulations and/or Hardware in the Loop studies [35], [55]). Based on this information, it is possible to set the threshold "c" to discriminate between the system with an FDIA and without an FDIA. Finally, the outputs of Algorithm 1, at each time instant, are the compensation gain $G_i(k)$ and the residual index $r_i(k)$. The first is used to compensate $V_i(k)$ in the case of an FDIA on the ith SM (see Fig. 8), whereas $r_i(k)$ allows monitoring if an FDIA is attacking the ith SM.

Algorithm 1 Pseudo-code of the proposed KF-based method for the detection of FDIAs: solution for the ith SM in the upper arm shown in Fig. 4

```
1: Inputs :
     Measurements: $V_i(k), I(k-1)$
     Internal variables: $m_i(k-1)$
2: Initialization :
     Initiate $P_i(0), R_i, Q_i, V_i(0)$
3: Kalman Filter Projection Stage:
     $\hat{V}_i(k/k-1) = \hat{V}_i(k-1/k-1) + \frac{1}{C_i} \cdot T \cdot m_i(k-1) \cdot I(k-1)$
     $P_i(k/k-1) = P_i(k-1/k-1) + Q_i$
4: Measurements Reliability Analysis:
     Define $V_i^{trust}(k)$ as the reliable measurement used for updating the Kalman filter
     Define: $g_i(k) = V_i(k) - \hat{V}_i(k/k-1)$
     Define: $\psi_i(k)$ as the reliability index

       $if$ $(|g_i(k)| > c)$ (An FDIA in the $ith$ SM is detected)
     {
     In this case, the measure $V_i(k)$ is not trustworthy.
     $\psi_i(k) = 1$
         $if$ $(|\psi(k-1) - \psi(k)| = 1)$ (The start of the attack is detected)
           {
             $G_i(k) = g_i(k)$ (The compensation gain $G_i(k)$ is calculated)
           }
     $\psi_i(k-1) = \psi_i(k)$
     $V_i^{trust}(k) = V_i(k) - G_i(k)$
     }
       $else$ (there is not an FDIA in the $ith$ SM)
     {
     The measure $V_i(k)$ is trustworthy, i.e.:
     $V_i^{trust}(k) = V_i(k)$
     $\psi_i(k) = 0$
     $G_i(k) = 0$
     $\psi_i(k-1) = \psi_i(k)$
     }
     $end$

5: Kalman Filter Update Stage:
     $K_i(k) = P_i(k/k-1) \cdot [P_i(k/k-1) + R_i]^{-1}$
     $P_i(k) = [1 - K_i(k)] \cdot P_i(k/k-1)$
     $\hat{V}_i(k) = \hat{V}_i(k/k-1) + K_i(k) \cdot [V_i^{trust}(k) - \hat{V}_i(k/k-1)]$
6: Outputs:
     $G_i(k)$ (compensation gain)
     $r_i(k) = \frac{|V_i(k) - \hat{V}_i(k)|}{V_N^*}$ (residual index)
```

V. Simulation Results

In this section, the proposed KF-based method for detecting FDI attacks and the proposed countermeasures to cope with these attacks are numerically validated. To this end, the MMC shown in Fig. 2 is simulated, using PLECS software, with the parameters listed in Table II. The MMC is controlled with the control system shown in Fig. 3: The central controller is implemented in the $\Sigma\Delta\alpha\beta0$ reference frame [34], whereas each local controller is implemented with the control scheme illustrated in Fig. 3. The parameters used for implementing the consensus algorithm (1) and those used for implementing the FDIA detection method are shown in Table III. Note that the cyber graph considered in this test is a fully-connected one, meaning that all the SM that belong to a given arm receive information from all the SMs of that arm.

TABLE II
MMC parameters used for simulation and experimental validation

Description	Simulated MMC	Experimental MMC
Grid inductance (L_g)	1mH	0.8mH
Arm inductance (L_{arm})	2.2mH	4.15mH
SM capacitance (C)	2.5mF	3.3mF
Number of SM per arm (N)	15 (90 SMs in total)	3 (18 SMs in total)
Carrier frequency (PS-PWM modulation)	1kHz	8kHz
Grid frequency (f_g)	50Hz	50Hz
Grid voltage (V_g)	$10kV_{RMS}$	$60V_{RMS}$
Power (P_n)	3MW	1.5kW
SM voltage reference (v_C^*)	1200V	70V
DC-link voltage (V_{DC})	18kV	182V
Resistive load (R)	108Ω	22.5Ω

To evaluate the effectiveness of the proposal, the test discussed in Section III and illustrated in Fig. 5 is repeated. It is worth remembering that in this test, an FDIA occurs in SM_1 and SM_2 at 1s, and another FDIA is applied to SM_{15} at 2s. In this case, the FDIA detection method is being run in each SM along with the proposed countermeasures. (See Fig. 8)

The FDIAs are effectively detected by the proposed detection method, as shown in Fig. 9. In this figure, the index $r_i(k)$ of the 15 SMs that belong to the attacked arm are plotted. It is concluded that the indices associated with SMs 1, 2 and 15 exceed the predefined threshold when those SMs start to be attacked, meaning that an FDIA is being executed on the associated SM. On the other hand, Fig. 10 shows the real capacitor voltages of the fifteen SMs that belong to the attacked arm during this test. By comparing Fig. 5(a) with Fig. 10, it can be concluded that the proposed detection scheme and countermeasures mitigate the FDIAs, ensuring safe operation of the MMC while those attacks are cleared. Indeed, without any detection method and countermeasures, FDIAs produce over-voltage (V_1 and V_2) and under-voltage (V_{15}) in the attacked SMs, as shown in Fig. 5(a). These adverse effects of the FDIAs are neutralised by the proposed method (see Fig. 8) as shown in Fig. 10.

Finally, Fig. 11 shows that the proposed detection scheme and countermeasures mitigate the current-quality issues produced by the FDIAs on the grid currents illustrated in Fig. 6(b). These results have shown the effectiveness of the FDIA detection method along with the countermeasures. Experimental validation of these proposals is provided in the next section.

A. Performance of the proposed FDIA detection method considering transient operation of the MMC

In this section, the performance of the proposed detection method in scenarios that produce a transient operation of the MMC is studied. This will provide information about how immune is the proposal to false positives. To this end, the

TABLE III
PARAMETERS OF BOTH CONSENSUS ALGORITHM AND KF-BASED DETECTION METHOD

Description	Simulated MMC	Experimental MMC
Consensus gain (k_i)	5	3
Covariance of the process noise (Q_{ii})	0.01	0.01
Covariance of the measurement noise (R_i)	0.5	0.5
Initial state ($V_i(0)$)	1200	70
Initial P ($P_i(0)$)	0.5	0.5
Threshold (c)	$0.1v_C^*$	$0.1v_C^*$

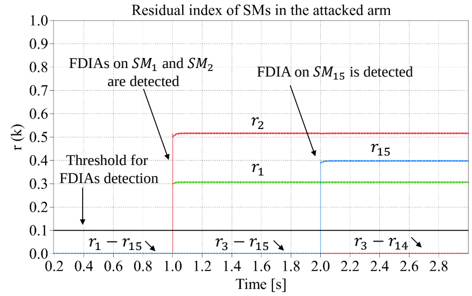


Fig. 9. Residual index provided by the proposed detection scheme.

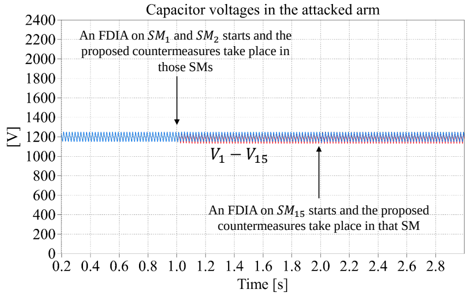


Fig. 10. Real capacitor voltages on the SMs of the attacked arm when the proposed detection method and countermeasures are working.

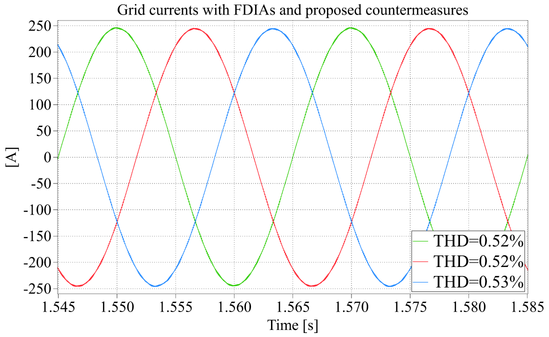


Fig. 11. Grid current when SM_1 and SM_2 of the arm shown in Fig. 4 is being attacked and the proposed countermeasures are working.

following operating conditions for the MMC were considered: (i) load change in the DC side of the MMC, (ii) change in the DC-link reference voltage, and (iii) balanced voltage drop in the grid voltage.

The test considered in this section is composed of four steps. In step 1 ($t < 1s$), the MMC operation is similar to the test presented in this previous section before 1s. Then, at the beginning of step 2 ($t = 1s$) and onwards, the resistive load shown in Fig. 2 is changed from 108Ω to 72Ω (increasing the power required by the load). In step 3 ($t = 2s$) and onwards, the DC-link voltage reference of the MMC is increased at $1.1V_{DC}$ (see Table II). Finally, in step 4 ($t = 3s$) and onwards, a balanced voltage drop in the AC grid is generated. The voltage drop corresponds to 30% of the nominal voltage of the grid (see Table II). To evaluate if the proposed FDIA method creates false positives, FDIAs are not applied to the MMC during the whole test. Thus, if the residual indexes generated by the proposed detector are close to zero during the entire test, it means that the FDIA detector does not cause false positives for operation modes considered in this test.

Fig. 12 illustrates the results associated with this test. As seen, a transient operation of the MMC is generated at the beginning of each step (at 1s, 2s and 3s, respectively). Fig. 12(a)-(c) shows the main variables related to the operating conditions described in the paragraph above. Fig. 12(d), shows the 90 residual indexes (one per each SM) generated by the proposed detection method. As observed in this figure, at any time, the threshold for FDIA detection is never surpassed, meaning that the proposed FDIA detection method does not present false positives for the cases considered in this test. This result shows the immunity of the proposed FDIA detection method against the operation modes (considered in this test) that generate transient states in the MMC.

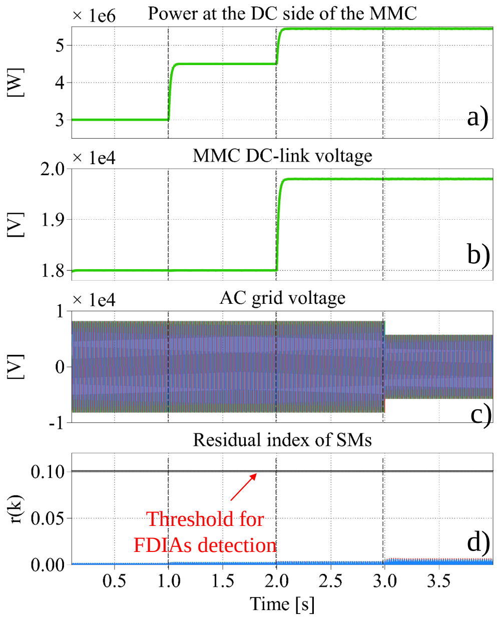


Fig. 12. (a) MMC DC-port output power, (b) MMC DC-link voltage, (c) Three-phase AC grid voltage, (d) Residual indexes provided by the proposed detection scheme: 90 indexes are shown (one per each SM of the MMC).

VI. EXPERIMENTAL RESULTS

To validate the proposed method for detecting FDIAs and the countermeasures to deal with such attacks, an experimental three-phase MMC prototype composed of 18 half-bridge-based SMs was constructed: it is shown in Fig. 13. This MMC converter has three SMs per arm. For the sake of clarity, FDIAs in the upper arm of phase "a" are studied. In this arm, the voltage sensors in each SM are named as (from top to bottom): v_{Ca1}^U, v_{Ca2}^U, and v_{Ca3}^U. The main parameters of the prototype are listed in Table II, and those used for implementing the proposal are shown in Table III. The control platform comprises a DSP Texas Instrument model TMS320C6713 augmented by 3 FPGA (Actel) boards. These boards are used to interface the A/D converters, to implement the hardware protection system (over-currents and over-voltages), and to generate the pulse-width modulation (PWM) signals of each cell. In this work, the phase-shift PWM technique is used. The grid is emulated using a Chroma 61511 programmable supply and the load is composed of resistors connected to the dc-port side of the MMC. It is worth remembering that the control system used for driving the MMC is shown in Fig. 3. The central controller is implemented in the $\Sigma\Delta\alpha\beta0$ reference frame discussed in [34], whereas the capacitor voltage balancing control is performed by the consensus-based distributed control scheme discussed in section II-A. This latter scheme was implemented in the control platform shown in Fig. 13, where its distributed nature is represented by the adjacency matrix B (see section II-A). In particular, for the experimental validation, it is considered that there is full communication among the SMs in the same arm.

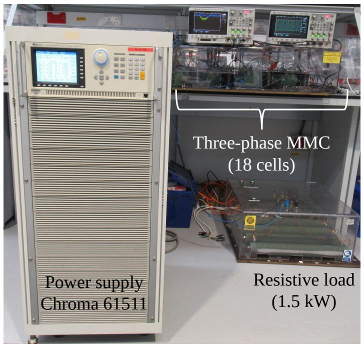


Fig. 13. Experimental rig used for the experimental validation.

Each SM of the experimental MMC (see Fig. 13) is implemented with the proposed FDIA detection method given by Algorithm 1, and with the countermeasures illustrated in Fig. 8). The performance of the MMC considering FDIAs in the SM voltage sensors is evaluated for the following cases: (i) Effects of FDIAs in the control system of the MMC, (ii) Experimental validation of the proposed method for FDIAs identification, and (iii) Experimental validation of the proposed countermeasures to mitigate the effect of FDIAs.

A. Experimental validation: Effects of FDIAs on the performance of the MMC

It must be pointed out that the intent of FDIAs could be either to look for an immediate destabilisation of the MMC or to deceive the system operator by discreetly penetrating the control system. In this sense, Fig. 14 shows an example of a destabilisation attack causing an immediate shutdown of the MMC. In that example, the measured voltage related to v_{Ca1}^{U} is attacked, at t_1, by an FDIA as follows: $v_{Ca1}^{U} = v_{Ca1}^{U} - 0.6v_{C}^{*}$ (see Table II). Thus, both the central and distributed controllers run with this attacked voltage measurement. As seen in Fig. 14, this simple attack produces an increase in the capacitor voltage of the attacked SM, producing a trip of the over-voltage hardware protection associated with that SM. Because of that, the identification and countermeasures to mitigate FDIAs should be studied for MMC.

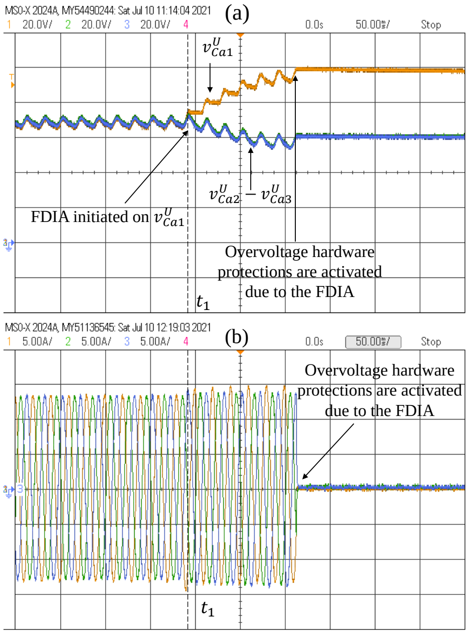


Fig. 14. Example of a destabilization attack: (a) real capacitor voltages of the attacked arm (directly measured across the capacitors), and (b) grid currents.

B. Experimental validation of the method for detecting FDIAs

In this test, the voltage sensors v_{Ca1}^{U} and v_{Ca2}^{U} are attacked at t_1 and $t_2{=}t_1{+}400ms$ respectively. The capacitor voltages v_{Cai}^{U} with $i{\in}\{1,2,3\}$ along with the grid currents are shown in Fig. 15(a)-(b) respectively. Initially, the capacitor voltages are balanced around v_{C}^{*}. At t_1, the voltage sensor of v_{Ca1}^{U} is attacked by adding 60% of v_{C}^{*}, in this case, the consensus algorithm is trying to ensure the local balance among v_{Cai}^{U} with $i{\in}\{1,2,3\}$, however due to the cyber-attack, the real value of this cell capacitor voltage decreases to $\approx$25 V. Despite the attack, the cell voltages v_{Ca2}^{U} and v_{Ca3}^{U} are still balanced. At t_2, the voltage sensor of cell v_{Ca2}^{U} is attacked by adding 40% of v_{C}^{*}. After this attack, the 3 cells within the upper arm of phase a have different voltages in steady-state, in particular, $v_{Ca1}^{U}{\rightarrow}27$ V, $v_{Ca2}^{U}{\rightarrow}42$ V, and $v_{Ca3}^{U}{\rightarrow}69$ V as shown in Fig. 15(a). Note that capacitor voltages displayed in Fig. 15(a) were directly measured across the capacitors in the attacked arm. The control system does not see these voltages due to the FDIAs. Fig. 16(b) shows the SM capacitor voltages seen by the control system. Initially the control platform sees a peak in the measured voltage due to the attack and then the consensus algorithm tries to balance the SMs using the attacked measurements. As a consequence, the control regulates the attacked voltages and it achieves a consensus point. However, the real capacitor voltages are not balanced as shown in Fig. 15(a)

In the situation described above, both FDIAs are effectively detected by the proposed detection method, as shown in Fig. 16(a). This figure shows the r index of each cell used to identify and quantify the magnitude of the attack. At t_1, an attack is detected and its magnitude is 0.6, afterwards at t_2 the second cell is attacked and as a consequence r_2 is equal to 0.4. Finally, by comparing the real capacitor voltages (see Fig. 15(a)) with those estimated by the proposed KF (see Fig. 16(c)), it is concluded the proposed strategy, can estimate the actual SM capacitor voltage.

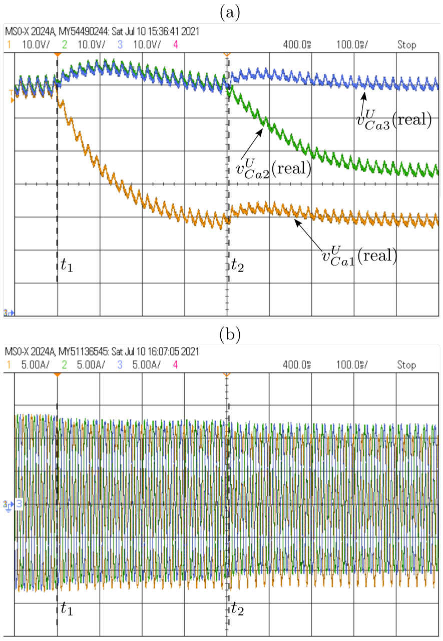


Fig. 15. Identification of 2 cyber-attacks: (a) real capacitor voltages of the upper arm of phase a (directly measured across the terminals of the capacitors), and (b) grid currents.

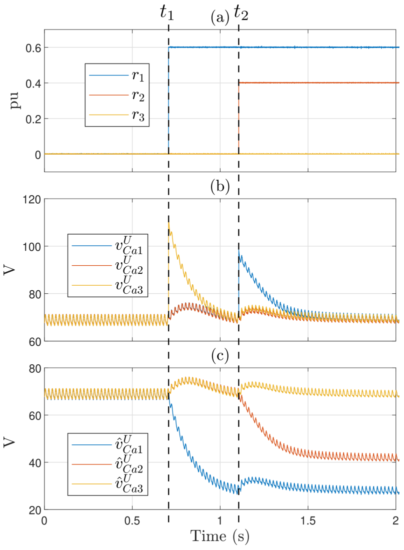


Fig. 16. (a) r-index for the cell capacitor voltages v^U_{Cai} with $i \in \{1, 2, 3\}$, (b) cell capacitor voltages v^U_{Cai} with $i \in \{1, 2, 3\}$ seen by the control platform, and (c) real capacitor voltages on the attacked arm (estimated by the proposed KF).

Finally, a zoomed view of the grid currents displayed in Fig. 15(b) is shown in Fig. 17(a)-(c). The grid current in regular operation, without any attack, is depicted in Fig. 17(a) and it has a THD=3.4%. After each attack, the harmonic distortion of the grid current increases; i.e. after the first and second attack the total harmonic distortion of the grid currents is THD=5.1% and THD=17.3% respectively. Finally, note that in this test, the proposed countermeasures were not activated.

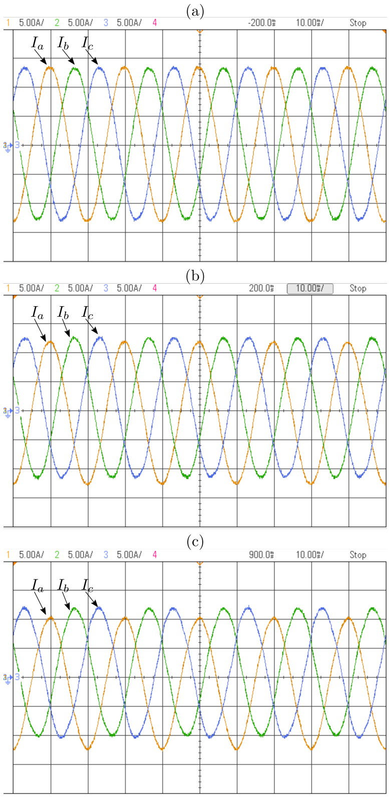


Fig. 17. Grid currents in different scenarios: (a) normal operation (without FDIAs), (b) FDIA in v^U_{Ca1} at t_1, and (c) FDIA in v^U_{Ca2} at t_2.

C. Experimental validation of the proposed countermeasures

In this test, the voltage sensors v^U_{Ca1} and v^U_{Ca2} are simultaneously attacked at t_1 by the following FDIAs: (i) $v^U_{Ca1} = v^U_{Ca1} + 0.2v^*_C$, and (ii) $v^U_{Ca2} = v^U_{Ca2} + 0.3v^*_C$. Then, at $t_2 = t_1 + 800ms$, the proposed countermeasures shown in Fig. 8 to mitigate such attacks are activated. In this case, for the attacked SMs, both the centralised and distributed control systems use the compensated voltage measurements to run their respective control strategies.

Fig. 18(a) and Fig. 18(b) show respectively the real capacitor voltages in the attacked arm, and the grid current during this test. These figures show that the capacitor voltages are balanced before the FDIAs ($t < t_1$). The same occurs with the grid currents. Then, at t_1, when the FDIAs are initiated, both the capacitor voltage balancing and current quality are affected. Finally, at t_2 (and onward), these issues are corrected by the proposed countermeasures.

Finally, some internal variables of the control algorithm are recorded, in particular, the r index, the cell capacitor voltages seen by the control and the cell capacitor voltage estimated by the proposed Kalman filter are shown in Fig. 19(a)-(c) respectively. From Fig. 19(a), it is concluded that the proposed method for detecting FDIAs effectively detects the cyber attacks emulated in this test. Note that the r index still indicates the presence of FDIAs after the activation of the countermeasures ($t > t_2$). This is because the attacks are still present in the system and need to be cleared.

Comparing Fig. 18(a) with Fig. 19(c), it is concluded that the proposed KF follows the real voltage during the whole test, showing its effectiveness.

Finally, Fig. 19(b) shows the capacitor voltages seen by the control system of the MMC. From t_1 to t_2 the control system runs with the attacked voltage measurements, whereas at $t = t_2$, these attacked measurements are compensated by the proposed countermeasures (see Fig. 8), noticeably improving the operation of the MMC as shown in Fig. 18 after $t = t_2$.

The experimental results presented in this section have shown the effectiveness of the proposed method for detecting FDIAs along with the proposed countermeasures to deal with them.

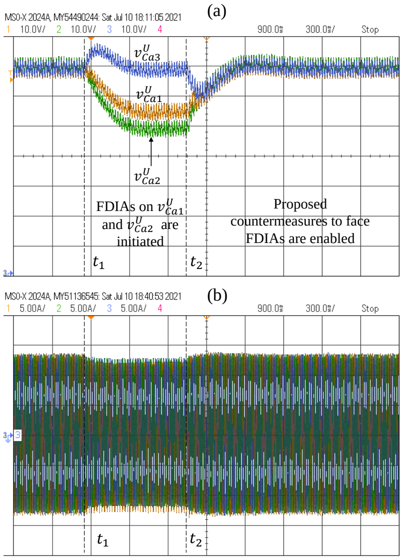


Fig. 18. Proposed countermeasures to mitigate FDIAs: (a) real capacitor voltages of the attacked arm (directly measured across the terminals of the capacitors), and (b) grid currents.

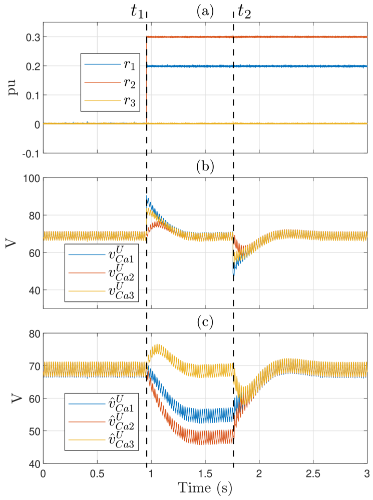


Fig. 19. (a) r-index for the cell capacitor voltages v^U_{Cai} with $i\in\{1,2,3\}$, (b) cell capacitor voltages v^U_{Cai} with $i\in\{1,2,3\}$ seen by the control platform, (c) real capacitor voltages on the attacked arm (estimated by the novel KF).

VII. Conclusions

This paper has studied the effects of FDIAs on control schemes used for controlling MMC. It was found that FDIAs produce power quality issues and eventually can lead to a shutdown of the MMC due to the activation of its protection system. Also, a method for detecting FDIAs was proposed and validated via simulations and experimental tests. This method can easily be implemented in the local controllers placed in the SMs of the MMC, and it does not require a high computational burden as it performs only scalar mathematical operations. In addition, countermeasures to mitigate FDIAs were proposed and validated through simulations and experimental results. These results show the effectiveness of the proposed method to overcome the adverse effects on the normal operation of the MMC produced by FDIAs. Finally, this paper provides the foundation for research into cyber-attacks on MMC type circuits, as so far, there is very little information in the literature on this topic. It is worth remembering that the MMC is deemed to be a prominent solution for medium to high-voltage and high-power applications. Indeed, it is a critical link in modern power systems (such as wind-farms interfacing, HVDC systems). Therefore it is a potential target for cyberattacks, and the result could be very significant. For this reason, it is necessary to explore this area of research.

As future work, the following tasks can be studied further: (i) the extension of the proposal to consider cyber-attack issues targeting the central controller (see (see Fig. 3)), (ii) to study FDIAs on measurements associated with current sensors, (iii) the study of more sophisticated FDIAs and methods for their detection, and (iv) to study methods for detecting FDIAs that considers fault conditions of the MMC.

References

[1] S. Du, A. Dekka, B. Wu, and N. Zargari, *Modular multilevel converters: analysis, control, and applications*. John Wiley & Sons, 2017.

[2] A. Dekka, B. Wu, R. L. Fuentes, M. Perez, and N. R. Zargari, "Evolution of topologies, modeling, control schemes, and applications of modular multilevel converters," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 5, no. 4, pp. 1631–1656, 2017.

[3] P. Poblete, J. Pereda, F. Nuñez, and R. P. Aguilera, "Distributed current control of cascaded multilevel inverters," in *2019 IEEE International Conference on Industrial Technology (ICIT)*. IEEE, 2019, pp. 1509–1514.

[4] S. Yang, S. Liu, J. Huang, H. Su, and H. Wang, "Control conflict suppressing and stability improving for an mmc distributed control system," *IEEE Transactions on Power Electronics*, vol. 35, no. 12, pp. 13 735–13 747, 2020.

[5] H. Geng, S. Li, C. Zhang, G. Yang, L. Dong, and B. Nahid-Mobarakeh, "Hybrid communication topology and protocol for distributed-controlled cascaded h-bridge multilevel statcom," *IEEE Transactions on Industry Applications*, vol. 53, no. 1, pp. 576–584, 2016.

[6] F. L. Lewis, H. Zhang, K. Hengster-Movric, and A. Das, *Cooperative control of multi-agent systems: optimal and adaptive design approaches*. Springer Science & Business Media, 2013.

[7] B. Xu, H. Tu, Y. Du, H. Yu, H. Liang, and S. Lukic, "A distributed control architecture for cascaded h-bridge converter with integrated battery energy storage," *IEEE Transactions on Industry Applications*, vol. 57, no. 1, pp. 845–856, 2020.

[8] P.-H. Wu, Y.-C. Su, J.-L. Shie, and P.-T. Cheng, "A distributed control technique for the multilevel cascaded converter," *IEEE Transactions on Industry Applications*, vol. 55, no. 2, pp. 1649–1657, 2018.

[9] B. P. McGrath, D. G. Holmes, and W. Y. Kong, "A decentralized controller architecture for a cascaded h-bridge multilevel converter," *IEEE transactions on industrial electronics*, vol. 61, no. 3, pp. 1169–1178, 2013.

[10] L. Mathe, P. D. Burlacu, and R. Teodorescu, "Control of a modular multilevel converter with reduced internal data exchange," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 248–257, 2016.

[11] Y. Zhou, D. Jiang, P. Hu, J. Guo, Y. Liang, and Z. Lin, "A prototype of modular multilevel converters," *IEEE Transactions on Power Electronics*, vol. 29, no. 7, pp. 3267–3278, 2013.

[12] B. Xia, Y. Li, Z. Li, G. Konstantinou, F. Xu, F. Gao, and P. Wang, "Decentralized control method for modular multilevel converters," *IEEE Transactions on Power Electronics*, vol. 34, no. 6, pp. 5117–5130, 2018.

[13] Y. Luo, Z. Li, Y. Li, and P. Wang, "A distributed control method for power module voltage balancing of modular multilevel converters," in *2016 IEEE Energy Conversion Congress and Exposition (ECCE)*. IEEE, 2016, pp. 1–5.

[14] B. Xia, Y. Li, Z. Li, F. Xu, and P. Wang, "A distributed voltage balancing method for modular multilevel converter," in *2017 IEEE 3rd International Future Energy Electronics Conference and ECCE Asia (IFEEC 2017-ECCE Asia)*. IEEE, 2017, pp. 1944–1948.

[15] S. Huang, R. Teodorescu, and L. Mathe, "Analysis of communication based distributed control of mmc for hvdc," in *2013 15th European Conference on Power Electronics and Applications (EPE)*. IEEE, 2013, pp. 1–10.

[16] Y. Koyama and T. Isobe, "Current control of modular multilevel converters using a daisy-chained distributed control system with communication path redundancy," in *IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society*, vol. 1. IEEE, 2019, pp. 6108–6113.

[17] A. The, C. Bruening, and S. Dieckerhoff, "Can-based distributed control of a mmc optimized for low number of submodules," in *2015 IEEE Energy Conversion Congress and Exposition (ECCE)*. IEEE, 2015, pp. 1590–1594.

[18] S. Yang, Y. Tang, and P. Wang, "Seamless fault-tolerant operation of a modular multilevel converter with switch open-circuit fault diagnosis in a distributed control architecture," *IEEE Transactions on Power Electronics*, vol. 33, no. 8, pp. 7058–7070, 2017.

[19] S. yang, Y. Tang, and P. Wang, "Distributed control for a modular multilevel converter," *IEEE Transactions on power Electronics*, vol. 33, no. 7, pp. 5578–5591, 2017.

[20] S. Yang, Y. Tang, M. Zagrodnik, G. Amit, and P. Wang, "A novel distributed control strategy for modular multilevel converters," in *2017 IEEE Applied Power Electronics Conference and Exposition (APEC)*. IEEE, 2017, pp. 3234–3240.

[21] H. Wang, S. Yang, H. Chen, X. Feng, and F. Blaabjerg, "Synchronization for an mmc distributed control system considering disturbances introduced by submodule asynchrony," *IEEE Transactions on Power Electronics*, vol. 35, no. 12, pp. 12 834–12 845, 2020.

[22] W. Yao, J. Liu, and Z. Lu, "Distributed control for the modular multilevel matrix converter," *IEEE Transactions on Power Electronics*, vol. 34, no. 4, pp. 3775–3788, 2018.

[23] J. Liu, W. Yao, Z. Lu, and J. Ma, "Design and implementation of a distributed control structure for modular multilevel matrix converter," in *2018 IEEE Applied Power Electronics Conference and Exposition (APEC)*. IEEE, 2018, pp. 1934–1939.

[24] S. Neira, P. Poblete, J. Pereda, and F. Nuñez, "Consensus-based distributed control of a multilevel battery energy storage system," in *2020 IEEE 21st Workshop on Control and Modeling for Power Electronics (COMPEL)*. IEEE, 2020, pp. 1–7.

[25] B. Xu, H. Tu, Y. Du, H. Yu, H. Liang, and S. Lukic, "A distributed control architecture for cascaded h-bridge converter," in *2019 IEEE Applied Power Electronics Conference and Exposition (APEC)*. IEEE, 2019, pp. 3032–3038.

[26] C. Burgos-Mellado, J. Gutierrez, C. Pineda, F. Donoso, A. Watson, M. Sumner, R. Cardenas, and A. Mora, "Distributed control strategy based on a consensus algorithm for the inter-cell and inter-cluster voltage balancing of a cascaded h-bridge based statcom," in *2020 IEEE 21st Workshop on Control and Modeling for Power Electronics (COMPEL)*. IEEE, 2020, pp. 1–8.

[27] S. Song and J. Liu, "Interpreting the individual capacitor voltage regulation control of psc-pwm mmc via consensus theory," *IEEE Access*, vol. 7, pp. 66 807–66 820, 2019.

[28] S. Sahoo, J. C.-H. Peng, A. Devakumar, S. Mishra, and T. Dragičević, "On detection of false data in cooperative dc microgrids—a discordant element approach," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 6562–6571, 2019.

[29] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[30] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE transactions on automatic control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[31] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.

[32] S. Mousavian, M. Erol-Kantarci, L. Wu, and T. Ortmeyer, "A risk-based optimization model for electric vehicle infrastructure response to cyber attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6160–6169, 2017.

[33] T. Ding, Z. Zeng, B. Qin, J. Zhao, Y. Yang, F. Blaabjerg, and Z. Dong, "Quantifying cyber attacks on industrial mmc-hvdc control system using structured pseudospectrum," *IEEE Transactions on Power Electronics*, vol. 36, no. 5, pp. 4915–4920, 2020.

[34] F. Donoso, R. Cardenas, M. Espinoza, J. Clare, A. Mora, and A. Watson, "Experimental validation of a nested control system for the balance of the cell capacitor voltages in a hybrid mmc," *IEEE Access*, 2021.

[35] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2018.

[36] A. Navas-Fonseca, C. Burgos-Mellado, J. S. Gómez, F. Donoso, L. Tarisciotti, D. Sáez, R. Cárdenas, and M. Sumner, "Distributed predictive secondary control for imbalance sharing in ac microgrids," *IEEE Transactions on Smart Grid*, 2021.

[37] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Power system reliability evaluation with scada cybersecurity considerations," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1707–1721, 2015.

[38] T. Kim, J. Ochoa, T. Faika, A. Mantooth, J. Di, Q. Li, and Y. Lee, "An overview of cyber-physical security of battery management systems and adoption of blockchain technology," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2020.

[39] S. Kumbhar, T. Faika, D. Makwana, T. Kim, and Y. Lee, "Cybersecurity for battery management systems in cyber-physical environments," in *2018 IEEE Transportation Electrification Conference and Expo (ITEC)*. IEEE, 2018, pp. 934–938.

[40] P. Zhuang and H. Liang, "False data injection attacks against state-of-charge estimation of battery energy storage systems in smart distribution networks," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2566–2577, 2020.

[41] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Transactions on Power Systems*, vol. 34, no. 2, pp. 1513–1523, 2018.

[42] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2016.

[43] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3864–3872, 2015.

[44] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[45] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2016.

[46] Q. Tu and Z. Xu, "Impact of sampling frequency on harmonic distortion for modular multilevel converter," *IEEE Transactions on Power Delivery*, vol. 26, no. 1, pp. 298–306, 2010.

[47] G. Liu, F. Xu, Z. Xu, Z. Zhang, and G. Tang, "Assembly hvdc breaker for hvdc grids with modular multilevel converters," *IEEE Transactions on Power Electronics*, vol. 32, no. 2, pp. 931–941, 2016.

[48] C. Burgos, D. Saez, M. E. Orchard, and R. Cárdenas, "Fuzzy modelling for the state-of-charge estimation of lead-acid batteries," *Journal of Power Sources*, vol. 274, pp. 355–366, 2015.

[49] M. D. Islam, R. Razzaghi, and B. Bahrani, "Arm-sensorless sub-module voltage estimation and balancing of modular multilevel converters," *IEEE Transactions on Power Delivery*, vol. 35, no. 2, pp. 957–967, 2019.

[50] O. S. M. Abushafa, M. S. Dahidah, S. M. Gadoue, and D. J. Atkinson, "Submodule voltage estimation scheme in modular multilevel converters with reduced voltage sensors based on kalman filter approach," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 9, pp. 7025–7035, 2018.

[51] O. S. M. Abushafa, S. M. Gadoue, M. S. Dahidah, D. J. Atkinson, and P. Missailidis, "Capacitor voltage estimation scheme with reduced number of sensors for modular multilevel converters," *IEEE Journal of*

Emerging and Selected Topics in Power Electronics, vol. 6, no. 4, pp. 2086–2097, 2018.

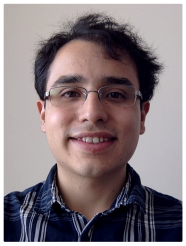
[52] Z. Wang and L. Peng, "Grouping capacitor voltage estimation and fault diagnosis with capacitance self-updating in modular multilevel converters," *IEEE Transactions on Power Electronics*, vol. 36, no. 2, pp. 1532–1543, 2020.

[53] Q. Yang, L. Chang, and W. Yu, "On false data injection attacks against kalman filtering in power system dynamic state estimation," *Security and Communication Networks*, vol. 9, no. 9, pp. 833–849, 2016.

[54] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE transactions on control of network systems*, vol. 1, no. 4, pp. 370–379, 2014.

[55] S. Zuo and D. Yue, "Resilient containment of multi-group systems against unknown unbounded fdi attacks," *IEEE Transactions on Industrial Electronics*, 2021.

Claudio Burgos-Mellado (S'17–M'19) was born in Cunco, Chile. He received the B.Sc. and M.Sc. degrees in electrical engineering from the University of Chile, Santiago, Chile, in 2012 and 2013, respectively, and the dual Ph.D. degree in electrical and electronic engineering from the University of Nottingham, U.K., and in electrical engineering from the University of Chile, Santiago, Chile in 2019. From 2019 to 2021, he was a Research Fellow in the Power Electronics, Machines and Control Group (PEMC group) at the University of Nottingham, United Kingdom. Currently, he is an Assistant Professor with the Institute of Engineering Sciences, Universidad de O'Higgins, Rancagua, Chile. His current interests include battery energy storage systems, electrical vehicle technologies, power electronics, microgrids, power quality issues and modular multilevel converters. In 2021, he received the best PhD thesis award in the category of Exact Science from the Chilean Academy of Sciences.



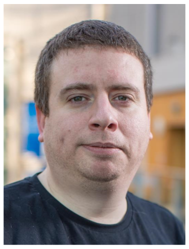
Felipe Donoso (S'17) was born in Santiago, Chile. He received the B.Sc and M.Sc. degrees in electrical engineering from the University of Chile in 2014 and 2016, respectively. He received the double degree PhD in Power Electronics at the University of Chile and the University of Nottingham in 2021. In 2019, he received the IEEE Transactions on Industrial Electronics Best Paper Awards. Currently, he is a research fellow at the PEMC group at the University of Nottingham. His research interests include control systems for power converters, resonant converters, modular multilevel converters and renewable energy systems.

Tomislav Dragičević (S'09-M'13-SM'17) received the M.Sc. and the industrial Ph.D. degrees in Electrical Engineering from the Faculty of Electrical Engineering, University of Zagreb, Croatia, in 2009 and 2013, respectively. From 2013 until 2016 he has been a Postdoctoral researcher at Aalborg University, Denmark. From 2016 until 2020 he was an Associate Professor at Aalborg University, Denmark. Currently, he is a Professor at the Technical University of Denmark. He made a guest professor stay at Nottingham University, UK during spring/summer of 2018. His research interest is application of advanced control, optimization and artificial intelligence inspired techniques to provide innovative and effective solutions to emerging challenges in design, control and diagnostics of power electronics intensive electrical distributions systems and microgrids. He has authored and co-authored more than 330 technical publications (more than 150 of them are published in international journals, mostly in IEEE), 10 book chapters and a book in this field, as well as filed for several patents. He serves as an Associate Editor in the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, in IEEE TRANSACTIONS ON POWER ELECTRONICS, in IEEE Emerging and Selected Topics in Power Electronics and in IEEE Industrial Electronics Magazine. Prof. Dragičević is a recipient of the Končar prize for the best industrial PhD thesis in Croatia, a Robert Mayer Energy Conservation award, and he is a winner of an Alexander von Humboldt fellowship for experienced researchers.

Roberto Cárdenas (S'95 M'97 SM'07) was born in Punta Arenas, Chile. He received his B.S. degree from the University of Magallanes, Chile, in 1988 and his Msc. and Ph.D degrees from the University of Nottingham in 1992 and 1996 respectively. From 1989-1991 and 1996-2008 he was a lecturer in the University of Magallanes Chile. From 1991 to 1996 he was with the Power Electronics Machines and Control Group (PEMC group), University of Nottingham, United Kingdom. He is currently a full professor of power electronics and drives in the Electrical Engineering Department, University of Chile, Chile. Prof. Cardenas was a recipient of the 2019 Third Prize Paper Award from the IAS Industrial Power Converter Committee. He was also the recipient of the IEEE Transactions on Industrial Electronics Best Paper Awards in 2005 and 2019. From 2014 to 2021, Prof. Cardenas was an Associated Editor for the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS.

Patrick Wheeler (M'90–SM'04) received his BEng [Hons] degree in 1990 from the University of Bristol, UK. He received his PhD degree in Electrical Engineering for his work on Matrix Converters from the University of Bristol, UK in 1994. In 1993 he moved to the University of Nottingham and worked as a research assistant in the Department of Electrical and Electronic Engineering. In 1996 he became a Lecturer in the Power Electronics, Machines and Control Group at the University of Nottingham, UK. Since January 2008 he has been a Full Professor in the same research group. He was Head of the Department of Electrical and Electronic Engineering at the University of Nottingham from 2015 to 2018. He is currently the Head of the Power Electronics, Machines and Control Research Group, Global Director of the University of Nottingham's Institute of Aerosapce Technology and was the Li Dak Sum Chair Professor in Electrical and Aerospace Engineering. He is a member of the IEEE PELs AdCom and is currently IEEE PELS Vice-President for Technical Operations. He has published over 750 academic publications in leading international conferences and journals.

Jon Clare (M'90–SM'04) was born in Bristol, UK, in 1957. He received the BSc and PhD. degrees in electrical engineering from the University of Bristol, UK, in 1979 and 1990, respectively. From 1984 to 1990, he was a Research Assistant and Lecturer with the University of Bristol, where he was involved in teaching and research on power electronic systems. Since 1990, he has been with the Faculty of Engineering at the University of Nottingham, UK. He is currently Professor of Power Electronics and is the Head of the Electrical and Electronic Engineering Department. He is a member of the Power Electronics, Machines and Control Research Group at Nottingham. His research interests are in power-electronic converters and their applications and control. Jon Clare is the recipient of a Royal Society Wolfson Research Merit Award.



Alan Watson (S'03-M'08-SM'21) received the M.Eng. (Hons.) degree in electronic engineering from the University of Nottingham, UK in 2004, and a PhD, also from the University of Nottingham in 2008. In 2009, he became a Research Fellow with the Power Electronics Machines and Control Group, University of Nottingham. Since 2009, he has been involved in various projects in high-power electronics including resonant converters, high voltage power supplies, and multilevel converters for grid connected applications such as HVDC and Flexible AC Transmission Systems. In 2012, he was promoted to Senior Research Fellow before becoming an Assistant Professor in High Power Electronics in 2013. As of 2022 he is an Associate Professor in High Power Electronics. His current research interests include the development and control of advanced high-power conversion topologies for industrial applications, grid connected converters and HVDC Transmission.