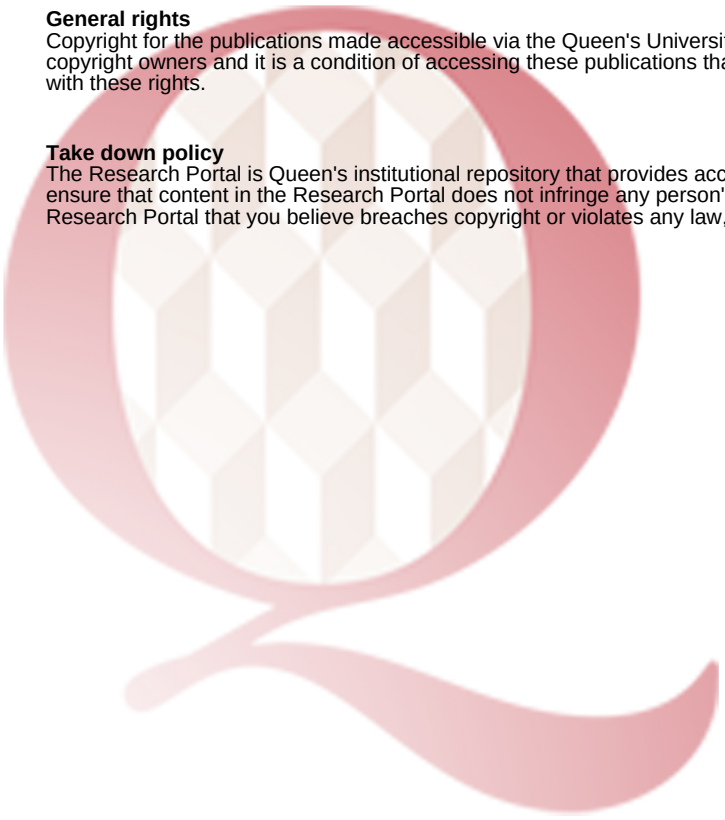
A Cyber-Physical Security Analysis of Synchronous-Islanded Microgrid Operation

Friedberg, I., Laverty, D., McLaughlin, K., & Smith, P. (2015). A Cyber-Physical Security Analysis of Synchronous-Islanded Microgrid Operation. In Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research 2015. (pp. 52-62). BCS Learning & Development Ltd. DOI: 10.14236/ewic/ICS2015.6

Published in:
Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research 2015

Document Version:
Peer reviewed version



A Cyber-Physical Security Analysis of Synchronous-Islanded Microgrid Operation

Ivo Friedberg
Queen's University Belfast
AIT Austrian Institute of Technology
ifriedberg01@qub.ac.uk

David Laverty, Kieran McLaughlin
Queen's University Belfast
{david.laverty, kieran.mclaughlin}@qub.ac.uk

Paul Smith
AIT Austrian Institute of Technology
paul.smith@ait.ac.at

Cyber-security research in the field of smart grids is often performed with a focus on either the power and control domain or the Information and Communications Technology (ICT) domain. The characteristics of the power equipment or ICT domain are commonly not collectively considered. This work provides an analysis of the physical effects of cyber-attacks on microgrids – a smart grid construct that allows continued power supply when disconnected from a main grid. Different types of microgrid operations are explained (connected, islanded and synchronous-islanding) and potential cyber-attacks and their physical effects are analyzed. A testbed that is based on physical power and ICT equipment is presented to validate the results in both the physical and ICT domain.

Testbed, Microgrid, Smart Grid, Cyber Security, Vulnerability, Synchronous Islanded Generation

1. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems are widely used in industrial control systems to collect information on the system state and issue control commands to remote actuators. Incidents like the attack on a German steel mill (Lee et al. 2014) show the ability of successful cyber-attacks to cause physical damage. A close relationship between Information and Communication Technologies (ICT) and the physical domain needs to be established to effectively counter these attacks. Models of Intrusion Detection Systems (IDS) can be enhanced with the constraints of the physical system. The same holds for control loops in the physical domain which can benefit from knowledge about the state of the ICT domain. Current research on SCADA system security is often based on an analysis of ICT protocols or network layouts, and is therefore strongly biased by cyber-security research in the ICT domain. The benefits that come from an understanding of the physical system that is under control are often ignored: Intrusion Detection Systems (IDS) as well as mitigation strategies for Industrial Control Systems (ICS) can leverage the laws of physics; they should be developed based on concrete domains and use cases to bridge the gap between the ICT and physical domains more effectively.

The development of current power grids into a smart grid revolves around a change from a centralized, uni-directional communication and power transmission layout, towards a meshed infrastructure as highlighted by Farhangi (2010). Considine et al. (2012) motivates a dynamic grid structure that is based on interconnected *microgrids*. This allows for an effective integration of renewable energy sources, but introduces new requirements for the tighter integration of ICT resources. Microgrids can be operated in two ways: *(i)* connected to the main grid, they can draw or supply power from it; and *(ii)* islanded – disconnected from the main grid – they supply local loads with local generation. Often, islanded operation is only possible for a limited amount of time. This calls for the capability to dynamically connect and disconnect power islands from the main grid; a transitional state that is highly dependent on ICT infrastructure while the grid is vulnerable to physical equipment damage due to power dynamics.

This paper presents a cyber-security analysis of the operational modes of microgrids. Special focus is given to synchronous-islanded operation: a mode of operation that controls the critical transitional state. Required for this operation are Phasor Measurement Units (PMUs), which are devices that allow the

measurement and communication of power dynamics. Currently, PMUs are primarily used as recording devices for post-fault analysis, but they have received increased attention for security and control applications. Our cyber-security analysis is based on a physical testbed that is designed to represent an islanded microgrid, which can be operated in an islanded, synchronous-islanded or connected (to the main grid) fashion. The main findings of this analysis are that attacks on the integrity of measurement and control communication can cause the most severe physical impact on microgrids. While attacks against communication availability require less attack capabilities, they can only cause critical physical effects under specific conditions out of the attacker's control. Attacks on confidentiality can cause no direct physical impact but can be used during the reconnaissance phase of an attack. Synchronous-islanded operation is most vulnerable to physical damage – even direct equipment damage – caused by cyber-attacks.

2. PRELIMINARIES

Dynamic connection and disconnection of microgrids is important for future smart grid operation. Power dynamics need to be controlled to prevent equipment damage and to ensure human safety. This section gives an overview of the challenges involved with synchronous-islanded operation of microgrids and what it can be used for.

2.1. Synchronous-Islanded Operation

For most types of microgrids, independent operation is only possible for a limited amount of time. To prevent blackouts in the microgrid during reconnection, it has to be possible for microgrids to be dynamically added and removed from the main grid during operation. Synchronous-islanded operation of microgrids is seen as one way to tackle this challenge. Even in islanding mode, the power metrics – *voltage magnitudes* (X_m), *frequency* (ω) and *phase angle* (ϕ) – are kept synchronized with the main grid. When these power metrics are matched between the islanded microgrid and the main grid, circuit breaker re-closure (see Sect. 2.2) is safe.

Microgrid internal controls can also take over completely when the main grid experiences severe stability problems. Military microgrids are an example where unstable environments are common and this feature is required. If synchronization is not guaranteed, re-closure of circuit breakers has to be prohibited.

Synchronous-islanded operation enforces strict transmission delay constraints on the underlying communication network. Control logic is used to control the difference in frequency between the systems taking the current phase angle difference into account. A detailed controller example is given in Sect. 3.

2.2. Circuit Breaker Re-closure

Connection of two independent and running power systems involves a set of risks, including out-of-sync closure. Two independent systems run potentially with different frequency and shifted phase angle. At the moment of connection three variables in the two systems have to be matched as closely as possible. These are the *voltage magnitude* (X_m), the *frequency* (ω) and the *phase angle* (ϕ). Limitations on the acceptable difference between the systems depend on the equipment in use. At the moment of connection the two systems are forced to synchronize. Depending on the synchronization quality at the time of connection, this might cause a strong immediate power flow on the circuit breaker. During this process also generator equipment is affected. The two phase angles are immediately forced to align, causing critical physical stress on equipment like generators.

2.3. The Phasor

A phasor – first described by Charles Proteus Steinmetz – is defined by the C37.118 standard (IEEE Power & Energy Society 2011) as a representation of the sinusoidal waveform defined in Eq. 1 with X_m describing the amplitude of the wave, ω the angular frequency and ϕ the phase angle of the waveform at time $t = 0$.

$$x(t) = X_m \cos(\omega t + \phi) \tag{1}$$

Using the transformation shown in Eq. 2 the phasor can use the representation of an imaginary number where the subscripts r and i signify real and imaginary part respectively.

$$\begin{aligned} X &= (X_m/\sqrt{2})e^{j\phi} \\ &= (X_m/\sqrt{2})(\cos\phi + j\sin\phi) \\ &= X_r + jX_i \end{aligned} \tag{2}$$

Phasors are commonly used in AC power analytics. The optimal assumption is a waveform with a constant frequency of 50 Hz and a voltage amplitude of 230 V for most of Europe and Asia. In this model, the waveform $x(t)$ is sufficiently defined by one phasor at time $t = 0$ for any future time t. Real power systems cannot fulfill this optimal model. Standards define the acceptable ranges of power quality for frequency and voltage. By allowing the frequency to change, the phase angle ϕ measured at time $t = 0$ is not sufficient to define the waveform at time t_1

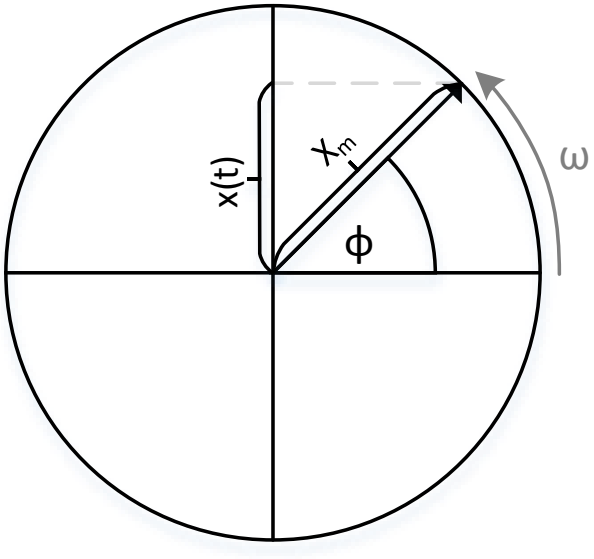


Figure 1: *Graphical description of phasor definition.*

(given ω and X_m at time t_1 are known). Successive measurements are needed to update the knowledge about the waveform.

Figure 1 shows a graphical interpretation of a phasor as a rotating vector. The magnitude X_m of the vector equals the amplitude of the waveform. The frequency ω describes the speed the vector rotates in. The phase angle ϕ is the angle between the vector and the base line. It becomes immediately clear, that the only parameter really depending on the time t is ϕ. We get the waveform by moving the source of the vector along the x-axis (in this case time) with constant speed. The projection of the vector on the y-axis is then the value of $x(t)$.

It has been possible to measure frequency and amplitude for a long time, but more recently Phasor Measurement Units (PMUs) have allowed operators to measure the phase angle remotely. PMUs allow the comparison of phasors of synchronous systems by assuming a reference waveform of nominal frequency. Phase Angle measurements are only comparable when taken at the same time. Precision requirements on time synchronization for comparable phase angle measurements are given by the C37.118 standard (IEEE Power & Energy Society 2011) with $\pm 3\mu s$. These measurements enable a set of new control capabilities but also open up new attack vectors as we will discuss in Sect. 4.

3. SYNCHONOUS-ISLANDING TESTBED

This section describes the current implementation of the synchronous islanding testbed at Queen's University Belfast. Section 3.1 gives an overview of the current testbed architecture. It highlights the physical components and describes their role in the testbed. Section 3.2 describes the controller functionality in more detail followed by a description of the used communication protocol in Sect. 3.3.

3.1. Architecture

Figure 2 gives an overview of the testbed's current implementation. It is designed to operate a DC machine synchronous with the main grid while in islanded mode.

DC Machine. The DC machine is a DC Motor / Alternator set. The DC motor is supplied from a 'Eurotherm 590+' digital DC drive; it offers analogue inputs to control the set points on the drive. The alternator is a 1000 rpm, 6 pole construction rated for 5kVA with a 0.8 power factor. Socket terminals on the laboratory work bench offer connection to the three phases, their neutrals and the alternator field winding over 4mm 'banana' plugs.

Phasor Measurement Units (PMUs). As PMU technology, equipment from the OpenPMU project (see Sect. 5) is used. PMUs are deployed at the main grid and within the power island. The collected power metrics are then transmitted to the controller.

Load Bank. A 3-phase resistive load bank is deployed within the power island. It can be used to evaluate the behaviour of the controlled island under shifting loads.

Controller. The controller collects the measurements from the PMUs and adapts the set points of the generator set. The controller in the testbed is implemented by a Python script running on a Raspberry Pi. The Serial Peripheral Interface (SPI) is used in combination with a transducer to transmit the set points to the analogue input of the digital DC drive. Figure 3 gives a schematic view on the modular software architecture of the controller. Network packets are received and then handled by separate worker threads to increase throughput. The worker thread logic decodes the network packet and is therefore protocol dependent. The decoded measurement points are then synchronized between the worker threads and measurements from the two PMUs are matched in the time domain. Once two measurements with the same timestamp are received, phase angle and frequency are extracted and sent to the controller. The controller block implements the logic described in Sect. 3.2. A generic Proportional-Integral-Derivative (PID) controller is used in combination with some additional logic to calculate the error value. The calculated update value is then transferred to a generator set specific communication module. It calculates an adequate set of set points as feedback for the internal controller of the generator set.

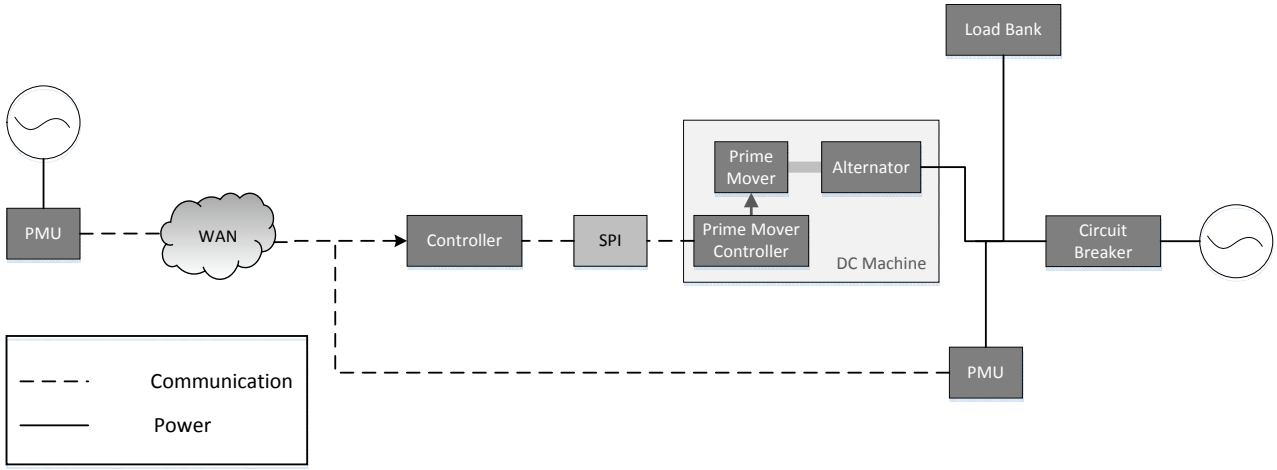


Figure 2: *Overview on the testbed architecture. A DC Machine is operated synchronous with the main grid while in islanding mode. A PMU at a remote, secure location in the main grid communicates with a local controller. A second PMU measures the power metrics in the island. The controller compares the measurements from the two PMUs and controls the generator.*

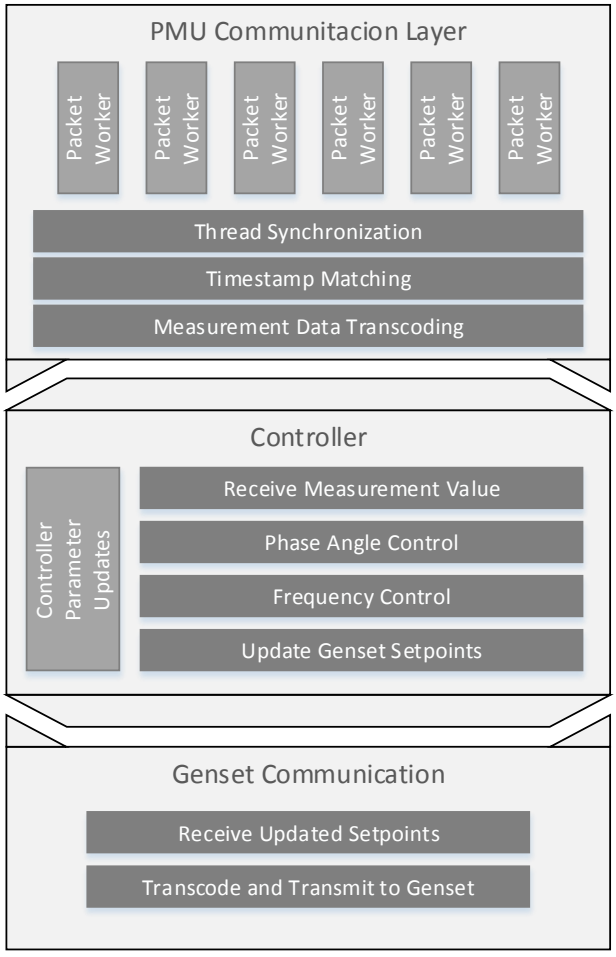


Figure 3: *Schematic view on modular controller software architecture*

3.2. Controller Strategy

A PID controller is a feedback-based control loop mechanism. It relies solely on the measured variables

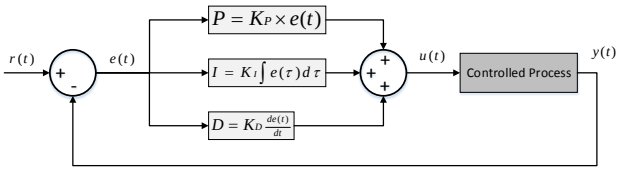


Figure 4: *Standard model of a PID controller.*

of the process under control and not on knowledge about the underlying processes. This makes the mechanism widely applicable without the need for adaptation. Figure 4 gives an overview of the general functionality of a PID controller.

The controlled process continuously emits measured process variables ($y(t)$). The PID controller tries to minimize the error ($e(t)$) between the process variables and given reference set points ($r(t)$). While $y(t)$ is measured on the running process that is controlled, $r(t)$ is controlled by the operator; both can change over time. An update signal ($u(t)$) is transmitted by the controller to the process to update the operation with the goal to minimize $e(t)$. The update signal comprises three weighted terms – the proportional term P depends on the current error, the integral term I depends on past errors and the derivative term D predicts future errors. The weights of each term (K_P, K_I, K_D) are used to tune the controller to a specific process.

For synchronous-islanded operation, two process values need to be controlled: phase ϕ and frequency ω. The internal controller in the generator set only accepts one feedback signal. Figure 5 shows the adaption of a general PID controller to the use case. The analogue set point at the generator is used to control the frequency. The classical PID control loop

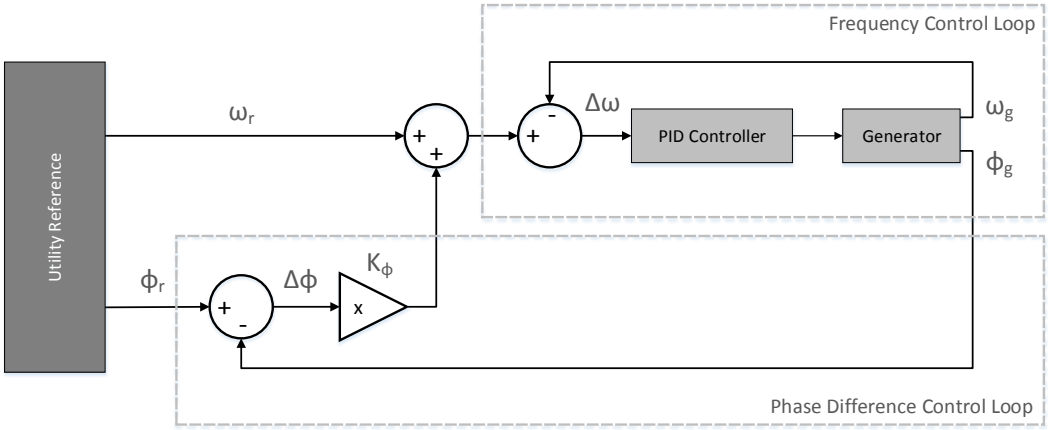


Figure 5: *The control logic for synchronous islanded generation.*

uses the current frequency of the power island (ω_g) as a feedback parameter and calculates the error given the controller's set point. The reference value for the frequency (ω_r) is received from the main grid. But it cannot be used as is. A *Phase Difference Control Loop* first calculates the error between the feedback phase angle in the island and the phase angle reference (see Eq. 3).

$$\Delta\phi = \phi_r - \phi_g \tag{3}$$

The *Phase Difference Control Loop* introduces a new tuning parameter K_ϕ that weighs the phase angle error. The weighted phase angle error is then added to ω_r to adapt the reference. As a result, the island will intentionally run with lower frequency than the main grid if its phase angle is ahead (the weighted phase angle error will be negative) and with higher frequency if the phase angle is behind. The complete calculation of the set-point for the PID controller $\Delta\omega$ is shown in Eq. 4.

$$\Delta\omega = K_\phi \Delta\phi + \omega_r - \omega_g \tag{4}$$

A known problem with PID controllers is integral windup. A large change in set-points can cause the integral part to accumulate a large error. This error causes the feedback to overshoot; the update from the controller further increases although the proportional error was already resolved and now points in the opposite direction. To resolve the issue, the accumulation in the integral term is blocked, while the update value from the controller is at the limits.

3.3. Protocol

The OpenPMU currently supports transmission of measurement values using the User Datagram Protocol (UDP) over the Internet Protocol (IP). Packets are transmitted to a statically defined IP address with a sampling rate of 10 measurements per second. UDP is a suitable transport layer protocol. Randomly dropped packets are obsolete by the time they would have been detected and requested again.

The payload of the packets contains text-based comma-separated values in the form of: *$<PMU ID>,<Time in UTC>,<Voltage>,<Frequency>,<Phase>**. This protocol is sufficient for the basic usage of PMUs and to operate a synchronous-islanded generator. This protocol is sufficient for the basic usage of PMUs and to operate a synchronous-islanded generator. Even though traditional industrial protocols like C37.118 do not offer more in terms of security, the lack of message integrity and message confidentiality limits the suitability of the protocol for security research. It has to be noted that a wide range of standardized protocols (like C37.118) do not offer more in terms of security. Only IEC 61850-90-5 comes with specifications of signature-based message integrity specified as part of the standard. While it is possible that integrity protection features receive more attention as PMUs are increasingly used for control tasks, standards leave vendors a lot of freedom when it comes to concrete implementations. Often security features are in place, but checks are disabled for simplicity or usability reasons. Thus, the potential impact of cyber-attacks that can circumvent integrity protection features remains relevant.

4. CYBER-SECURITY ANALYSIS

This section provides a detailed cyber-security analysis of different operation modes of microgrids using PMUs for active control. Figure 6 shows an extended version of the testbed, including *(i)* a bump-in-the-wire solution for IEC61850-90-5 support and *(ii)* a virtual office and SCADA network to allow multi-stage attacks.

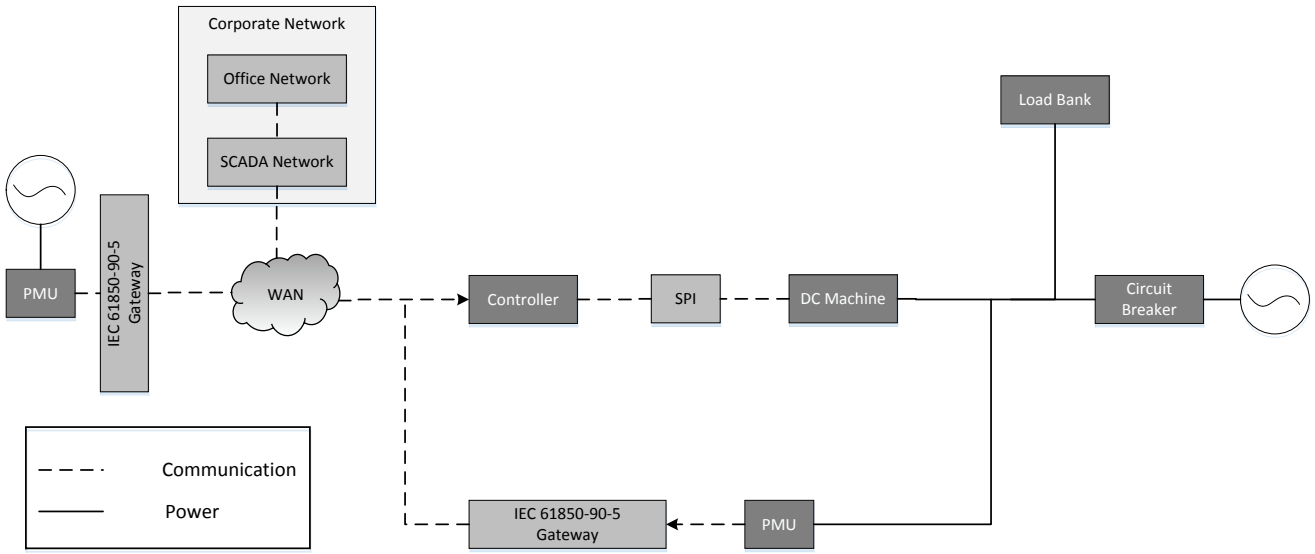


Figure 6: *Planned testbed layout including* (i) *a bump-in-the-wire solution for IEC61850-90-5 support and* (ii) *a virtual office and SCADA network to allow multi-stage attacks in addition to the testbed presented in Fig. 2*

The microgrid can be operated in three different modes. *Connected* to the main grid, *Islanded* from the main grid or *In Transition* between those two. Synchronous-islanded operation will be the use case for the transitional state as described in Sect. 2. Attacks can aim to compromise one of three security objectives: *Availability*, *Integrity* or *Confidentiality*. In the following, we focus on attacks on the communication infrastructure. Possible cyber-attacks to devices and physical attacks to the system are out of scope of this work. We give a general overview of the limitations given by current power control setups, describe attack types grouped by the three security objectives and analyze possible physical effects of each attack type in each of the operation modes. The analysis is supported with related work in Sect. 5.

4.1. Power Grid Operation

The physical prerequisites and the current state-of-the-art in power system control impose a set of limitations on potential cyber-attackers. Inflicting physical damage to power equipment by means of cyber-attacks is difficult. Each input parameter for power equipment is checked by an internal control algorithm against a range of acceptable values. This range assures safe operation of the device to prevent physical damage. Protective devices throughout the grid continuously check for unacceptable conditions and automatically isolate electrical faults. This does not prevent an attacker from achieving an unacceptable condition in the grid, but limits possibilities to propagate the fault. Further, protective relays are hard-wired to the power lines and, as such, cannot be attacked from the cyber domain. Governments standardize the metrics for power quality; namely the intended frequency and voltage levels in the grid, including acceptable ranges of deviation ($230V \pm 10\%$ for voltage at any time and $50Hz \pm 10mHz$ for the average frequency over a period of one day for Central Europe). Setpoints for frequency and voltage can again be limited to these acceptable ranges, in order to prevent accidental or malicious power quality violations. Cyber-attacks in the power domain can require detailed knowledge about the system under attack and the possibilities to inflict physical damage to power equipment are limited.

For microgrids three operational modes are identified that have further implications on the possibilities of cyber-attacks.

Connected Mode. A microgrid is operated connected to the main grid. Manual synchronization of phase and frequency are not needed. To manage the voltage on the distribution lines – to prevent over- or undervoltage situations – the main grid can control the active and reactive power that is fed into the distribution system by the microgrid. This is controlled by changing the *set-points for active and reactive power*, which are the commands that can be manipulated by an attacker in this stage.

Islanded Mode. The microgrid operates disconnected from the main grid. Local loads are supplied by local generation. Synchronization with the main grid is not needed. An internal controller has to take responsibility for the power quality within the microgrid. It has to ensure that the voltage and frequency levels in the microgrid fulfill the power quality requirements. These are fixed standardized references and as such not possible to attack from the cyber domain. Availability and integrity attacks are possible on *data from local measurement devices* that

are sent to the controller. In case the local demand in a islanded microgrid exceeds the possible local generation, three possibilities exist: *(i)* the microgrid can gracefully shut down, resulting in a local blackout; *(ii)* load can be shed to maintain stable operation; or *(iii)* the microgrid can attempt to reconnect to the main grid.

Transitional State. Disconnection and reconnection are the two most volatile states for a microgrid. Before disconnecting it has to be ensured that the local generation can supply the local demand to prevent a blackout in the microgrid. During reconnection syncrhonous-islanded operation is one way to align phasor and frequency in the main grid and in the island. In this state, both, the *reference from the main grid* as well as *local measurements* are sent over ICT networks and are, as such, open to attacks. In particular, reference measurements from the main grid have to potentially perform multiple hops to reach the local controller, each of which is a potential attack vector. Additional risk is imposed at this stage by measurement data from the phasor. For voltage and frequency, fixed power quality set-points are known. A high deviation from these set-points at the reference point in the main grid is very unlikely and indicates faulty measurements or an attack. For phasor measurement data, every potential value is valid at certain points in time. It is the deviation between the reference point and the local measurements that has to be minimized.

4.2. Attack Types

The proposed use case contains two communication links that can potentially be targeted by a cyber attack: the ICT network and the GPS communication used by the PMUs for clock synchronization. For both, attacks on all three security requirements are possible.

Availability. Communication in power systems is often time critical. Control commands and measurements are only valid for a given time window. Therefore, Denial-of-Service (DoS) attacks can either aim to block traffic completely or delay a message for long enough to shift the arrival time out of the accepted time window. DoS attacks can happen on different levels of the communication stack. On the *Physical Layer*, wireless communication technologies are vulnerable to cyber-attacks. In the given use case, this can include both the ICT network and the GPS signals. First, the communication between the PMUs and the controller can include wireless connections. This is especially true if the controlled island is in a geographically isolated area. Second, the PMUs rely on GPS for time synchronization. The *Data Link Layer* is responsible for a reliable point-to-point communication. In the proposed testbed, communication between PMUs and the controller is based on UDP/IP over Ethernet. With MAC address spoofing, an attacker can masquerade as another device. This is a potential threat to both availability and integrity. On the *Network and Transport Layer* resource exhaustion attacks can be especially effective on power equipment, as resources are very limited. These can also be performed on the *Application Layer*, where computationally expensive requests can be sent to devices.

Integrity. There are two main types of integrity attacks: *(i)* existing messages can be intercepted and altered or *(ii)* additional valid messages can be injected into a communication flow. The first type is also a potential threat to availability. Successful integrity attacks are potentially more dangerous than DoS attacks, because they can lead to unexpected control decisions. Two different aspects of the system need to be targeted. First, the integrity of a message needs to be compromised. Then the message needs to be manipulated in a way that results in the intended effect in the controlled physical domain. Integrity attacks are possible on GPS signals and on the ICT network. On the ICT network, the following measurements and control commands are at risk: in connected mode the *set-points for active and reactive power*, in islanded mode the *local measurements of frequency and voltage* and in synchronous-islanding mode all *measurements at the reference point of the main grid as well as local measurements of phase, frequency and voltage*. The potential effects of integrity attacks on this information are further discussed in Sect. 4.3.

Confidentiality. Attacks on confidentiality are the least critical for power grid operation. But a lack of message confidentiality can help attackers during reconnaissance. The network layout, the type of protocols in use, network addresses of potentially vulnerable devices and the current status of the power system are just a small sample of interesting information that can be gathered on the network.

	Availab.	Integrity	Confident.
Physical	◐	○	○
Data Link	◐	●	◐
Transport/ Network	◐	◐	◐
Application	◐	●	●

Table 1: *Overview of the attack capabilities required on the different communication layers to target each security objective. Full circles indicate, that an attack capability on the specific layer is required, half circles indicate that an attack on the layer is either sufficient but not required, or can be used to extend the attack capabilities.*

Table 1 shows the attack capabilities that are needed on each network in order to perform a specific type of attack. It can be seen that attacks on availability can be performed on each network layer independently.

They have a large attack surface. Integrity and confidentiality attacks, on the other hand, have strict requirements on the application layer. Especially on the security features in place like signatures and encryption.

4.3. Physical Effects

We have identified five types of physical impacts that a cyber-attack can have in the described microgrid use case. These include: *(i)* a local blackout in the microgrid with no imminent threat to the rest of the grid; *(ii)* instabilities on the main grid (these include cases in which protective relays isolate electrical faults); *(iii)* violations of the power quality in the microgrid; *(iv)* physical damage to power equipment; and *(v)* danger for human safety. Table 2 gives an overview of the potential physical effects of cyber-attacks in the different operation modes of the microgrid. We differentiate three attack types: *(i)* attacks on the availability and integrity of the GPS-based clock synchronization of PMUs; *(ii)* attacks on the availability of the ICT network; and *(iii)* integrity attacks on the messages in the ICT network. Attacks on availability and integrity of GPS are categorized together because the physical effects that can be caused are very similar. Only the effectiveness of the attack can be higher if an integrity attack is used to intelligently manipulate the time synchronization, instead of introducing an arbitrary error. Confidentiality attacks are not shown, as they cannot directly introduce physical effects.

It is assumed that the attacker can only gain control of the ICT network in the microgrid. Therefore, attacks on all messages sent from and to the microgrid by a central SCADA control center can be attacked. Messages to other devices or substations in the main grid cannot be affected. In the following, we will discuss the table for each operation mode.

Connected. In connected mode the attacker's capabilities to cause physical damage are the most limited. Measurements from the PMUs are not required for safe operation. Only messages controlling active and reactive power emission can be affected. The potential impact of a manipulation of these set-points depends on the significance of the attacked microgrid's size in comparison to the main grid or a certain section in the distribution network. Depending on the significance, blocking or manipulating these set-points can cause local grid instability and subsequently local blackouts. Additional redundancies in the distribution network can limit the possible damage. Further, protective devices are in place to isolate electrical faults and prevent propagation.

Islanded. In islanded mode, cyber-attacks cannot influence the main grid. The microgrid, on the other hand, is more vulnerable. One reason for this that is specific to the proposed use case is that PMUs are the only sensor in the proposed microgrid. Attacks on the GPS signal have limited effect on the grid, because control over frequency and voltage does not require phasor orientation in islanded mode. The lack of ICT communication as well as intelligent integrity attacks on the other hand can cause serious physical effects. By manipulating the local measurements of frequency and voltage, control over power quality is lost which can result in a violation of power quality metrics as well as a shutdown of the microgrid.

Synchronous-Islanding. Synchronous-islanding is the most volatile operation mode where the most critical physical damage can be achieved: damage to equipment and risk of human safety. The critical moment for equipment is the moment of circuit breaker re-closure. Significant differences of phase angle, frequency or voltage magnitude between the main grid and the island can damage the circuit breaker as well as local synchronous generators. This situation can be achieved by manipulating the feedback loop in charge of synchronization. DoS attacks on the ICT network can easily be detected and re-closure can be prohibited. The effects of limited precision in clock synchronization between the PMUs is harder to detect and therefore more critical. Most damage can be done using integrity attacks on the ICT network. Manipulation of the local measurements or measurements from the reference point trick the controller into making incorrect assumptions about the system state. This can be used to maximize the phase angle difference. The local controller has no way of verifying the correctness of the data. It will assume synchronization is achieved while the control decisions potentially led to a maximization of the phase angle difference. While frequency and voltage levels can be compared to the static set-points from the power quality metrics, the same cannot be done for phase angle information. This leaves the controller vulnerable to integrity attacks without the ability to detect them.

5. RELATED WORK

One approach for safe circuit-breaker re-closure is synchronous-islanded operation of power islands; a universally applicable method is presented by Best et al. (2008). The authors describe general requirements and possible limitations caused by time-delay introduced when transmitting the reference signal. Challenges like islanding detection and control initiation are covered as well as issues with power quality and security mechanisms in the case of a communication loss. Laverty et al. (2008) performs a detailed analysis on the effect of the time delay introduced by wide-area telecommunications. In their work, the authors show the response of an alternator operated by an Internet-based phase

		Local Blackout	Mains Instability	Violation of Power Quality	Equipment Damage	Human Danger
Connected	Avail. or Int. GPS	○	○	○	○	○
	Availability ICT	○	◐	○	○	○
	Integrity ICT	◐	◐	○	○	○
Islanded	Avail. or Int. GPS	◐	○	○	○	○
	Availability ICT	●	○	○	○	○
	Integrity ICT	●	○	●	○	○
Sync-Islanded	Avail. or Int. GPS	●	○	○	◐	◐
	Availability ICT	◐	○	◐	○	○
	Integrity ICT	●	○	●	●	●

Table 2: *Overview on physical effects of different types of cyber attacks in the three operation modes of a microgrid. Half circles indicate that control algorithms without knowledge of the ICT system can potentially mitigate the physical effect. Full circles indicate that additional control algorithms will be needed that bridge the gap between the physical and the cyber domain to detect and mitigate the threat.*

difference controller to local load acceptances. They were able to show that control is effective when it is operated on a telecommunication link with variable time delay such as the Internet. Caldon et al. (2004) evaluates the effects of synchronous and inverter-interfaced generators on the stability of power islands. The authors show, that inverter-interfaced generators increase the stability of frequency and phase angle difference. Synchronous-islanded operation highly depends on Phasor Measurement Units (PMUs).

Research on the potential effects of cyber-attacks on physical infrastructures in cyber-physical systems is often performed from either an ICT or a physical and control engineering perspective. In the ICT domain, Dondossola et al. (2008) analyze potential cyber-attacks on power substation control systems. Their research focus lies on the potential threats of cyber-attacks to the ICT communication capabilities. Potential physical effects are highlighted but no critical physical effects are achieved in the experiments. Wang and Lu (2013) highlight potential cyber-attacks on availability, integrity and confidentiality, and their potential effects on different use cases. They also present potential mitigation strategies. Signatures and encryption are presented as cryptographic countermeasures, and the difficulties that arise from limited computing power and strict time constraints are explained. Network-based countermeasures are presented and grouped by the targeted communication layers. Availability attacks on GPS signals by GPS jamming are presented by Hu and Wei (2009). The authors also elaborate on countermeasures against GPS jamming in modern GPS receivers. Zhang et al. (2013) presents an integrity attack on GPS signals with respect to time synchronization. The authors show how the injection of targeted GPS signals increases the effect of the attack in comparison to the arbitrary error introduced by availability attacks. In the control domain, work by Sandberg et al. (2010) and Dán and Sandberg (2010) focuses on risks associated with bad data injection – an attack against state estimation where the monitored system state is manipulated in order to remain undetected. The authors develop security indices for nodes in the grid that produce measurement data. These indices are used to define how critical measurements from a certain node are to the overall state estimation. This knowledge can be used to introduce security features step-by-step, starting with the most critical nodes in the system. Kundur et al. (2011) presents a first step towards a graph-based framework for modeling the physical impact of cyber-attacks on smart grids. Two case studies show the application of the framework in a Matlab environment based on two modified models of the IEEE 13 node distribution system. One case study shows that a successful cyber-attack can cause a severe under-frequency situation that ultimately results in a local blackout. Iowa State University (ISU) have developed the *PowerCyber testbed* in 2013 (Hahn et al. 2013). Real physical components are used to implement substations. Substation communication is performed using IEC 61850 GOOSE messages. The Internet-Scale Event and Attack Generation Environment (ISEAGE) project – also developed by ISU – is used to emulate wide-area networks. SCADA-specific hardware is used to emulate a control centre. The physical setup is integrated with a real-time digital simulator and a PowerFactory based offline simulator for bigger power grid instances. Of special interest is the use of IEC 61850 as well as the scalable approach of combining physical devices with power grid simulation. The authors further perform an analysis of the cyber and physical impact of cyber-attacks on three use cases of the system. The first use case shows the effect of a malicious breaker trip in a three generator set. It is shown that isolation of one generator can cause the remaining two synchronous generators to become unsynchronized. The second use case highlights the effects of DoS attacks on state

estimation algorithms. The third use case presents a coordinated multi-stage attack on a Remedial Action Scheme (RAS) that could cause load-shedding, as well as frequency instability.

6. CONCLUSION AND FUTURE WORK

In this paper, we have performed a cyber-security analysis of different operational states of microgrids, with a particular focus on synchronous-islanded operation. To control these operational states, an increased integration of power systems with ICT communication is needed. Our analysis, which is based on a testbed that includes both power equipment and ICT components, has considered the physical limitations imposed by real power equipment and the potential capabilities of an attacker in the cyber domain. We have indicated that a cyber-attack can cause physical damage to power equipment and endanger human safety. These findings motivate the need for new solutions for cyber-physical resilience in microgrids. These solutions need to tightly integrate efforts from ICT and power domain to detect and mitigate cyber-attacks accurately and ensure safe operation. Future work will include further development of the presented testbed. The described attacks will be implemented and evaluated in this cyber-physical environment. A more formal security analysis will be conducted using the Systems Theoretic Process Analysis (STPA) method, as proposed by Levenson (2011). Our goal is the realisation of a resilience framework that ensures the safe operation of microgrids during cyber-attacks.

Acknowledgements. This work was partly funded by the EU FP7 SPARKS project (Contract No. 608224) and the EPSRC CAPRICA (Contract No. EP/M002837/1) project.

REFERENCES

Best, R., Morrow, D., Laverty, D., and Crossley, P. (2008). Universal application of synchronous islanded operation.

Caldon, R., Rossetto, F., and Turri, R. (2004). Temporary islanded operation of dispersed generation on distribution networks. In *39th International Universities Power Engineering Conference, 2004. UPEC 2004*, volume 3, pages 987–991 vol. 2.

Considine, T., Cox, W., and Cazalet, E. G. (2012). Understanding microgrids as the essential architecture of smart energy. In *Grid Inerop Forum, Texas*.

Dán, G. and Sandberg, H. (2010). Stealth Attacks and Protection Schemes for State Estimators in Power Systems. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 214–219.

Dondossola, G., Szanto, J., Masera, M., and Nai Fovino, I. (2008). Effects of intentional threats to power substation control systems. *International journal of critical infrastructures*, 4(1):129–143.

Farhangi, H. (2010). The Path of the Smart Grid. *Power and Energy Magazine, IEEE*, 8(1):18–28.

Hahn, A., Ashok, A., Sridhar, S., and Govindarasu, M. (2013). Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid. *IEEE Transactions on Smart Grid*, 4(2):847–855.

Hu, H. and Wei, N. (2009). A study of GPS jamming and anti-jamming. In *Power Electronics and Intelligent Transportation System (PEITS), 2009 2nd International Conference on*, volume 1, pages 388–391.

IEEE Power & Energy Society (2011). IEEE Standard for Synchrophasors for Power Systems. In *IEEE Std C37.118.1-2011 (Revision of IEEE Std C37.118-2005)*.

Kundur, D., Feng, X., Mashayekh, S., Liu, S., Zourntos, T., and Butler-Purry, K. L. (2011). Towards modelling the impact of cyber attacks on a smart grid. *International Journal of Security and Networks*, 6(1):2–13.

Laverty, D. M., Morrow, D. J., Best, R., and Crossley, P. A. (2008). Internet based phasor measurement system for phase control of synchronous islands. In *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, pages 1–6. IEEE.

Lee, R., Assante, M., and Connway, T. (2014). ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack. Technical report, SANS ICS.

Levenson, N. G. (2011). Engineering a safer world. *Systems Thinking Applied to Safety, The MIT Press, Cambridge, MA, USA*.

Sandberg, H., Teixeira, A., and Johansson, K. H. (2010). On security indices for state estimators in power networks. In *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010, Stockholm, Sweden*.

Wang, W. and Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, 57(5):1344–1371.

Zhang, Z., Gong, S., Dimitrovski, A. D., and Li, H. (2013). Time Synchronization Attack in Smart Grid: Impact and Analysis. *Smart Grid, IEEE Transactions on*, 4(1):87–98.