2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) | 978-1-6654-1502-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/SMARTGRIDCOMM51999.2021.9632

Securing SCADA networks for smart grids via a distributed evaluation of local sensor data

Verena Menzel
University of Twente,
the Netherlands
v.m.menzel@utwente.nl

Johann L. Hurink
University of Twente,
the Netherlands
j.l.hurink@utwente.nl

Anne Remke
Westfälische Wilhelms-Universität
Münster, Germany
anne.remke@uni-muenster.de

***Abstract*—Within smart grids the safe and dependable distribution of electric power highly depends on the security of Supervisory Control and Data Acquisition (SCADA) systems and their underlying communication protocols. Existing network-based intrusion detection systems for Industrial Control Systems (ICS) are usually centrally applied at the SCADA server and do not take the underlying physical process into account. A recent line of work proposes an additional layer of security via a process-aware approach applied locally at the field stations. This paper broadens the scope of process-aware monitoring by considering the interaction between neighboring field stations, which facilitates upcoming trends of decentralized energy management (DEM). Local security monitoring is lifted to monitoring neighborhoods of field stations, therefore achieving a broader grid coverage w.r.t. security. We provide a distributed monitoring algorithm of the generated sensory readings for this extended setting. The feasibility of the approach is shown via a prototype simulation testbed and a scenario with two subgrids.**

I. Introduction

The ongoing energy transition leads to a replacement of fossil fuels by renewable energy. Hereby, the sources for this renewable energy production are quite heterogeneous. Compared to the production with fossil fuels, the availability of these renewable sources is often unpredictable and more dispersed across the power grid geographically. Because of the reduced control over the amount of energy produced (e.g. by PV panels), but also the increased loads resulting from the electrification of transport (electric vehicles) and heating (heat-pumps), the grid becomes more volatile and as a consequence unstable, often asking for quick, automated and local load balancing. Therefore, for the management and control of electrical grids new and decentralized approaches are developed instead of the previously used central approach.

Next to the changes in load and generation, also the growing inter-connectivity between different grid components and their connection to the internet influences the way of managing the grids. The grid operator is now able to quickly adapt to local load imbalances by e.g. adjusting the tap position in a transformer. This is possible trough smart devices that can be operated remotely and (partially) automated. However, this direct remote access and the usage of common yet unsafe network protocols between devices of different manufactures also make the grid more vulnerable to (terrorist) attacks. Incidents like in Iran in 2010 and Ukraine in 2015 show how devastating such attacks against electrical grid infrastructure are and how hard it is to fight their impacts [1], [2].

To enhance the security of SCADA networks different approaches from classical IT security exist. To detect illegitimate commands, behaviour-based approaches (e.g. [3], [4]), anomaly-based approaches (e.g. [5]) and specification based approaches (e.g. [6]) are researched. To detect legitimate commands send by an intruder in the context of SCADA networks, packet inspection, package order and protocol safety is investigated by e.g. [7]–[10], Nonetheless, these approaches rarely take the physical dimension of the underlying electrical grid into account. Notable exceptions are, e.g., [11], [12], which include generated sensory data of the physical process. Another class of related work also takes into account the topology of the network and the related risk because of random failures and direct attacks (see e.g. [13]). State estimation is widely used to secure electrical grids, where the state of the complete grid is evaluated centrally and supervised based on the measurements received over the SCADA network (see e.g. [14], [15]). However, in case of an attack the state estimation is likely to be affected too, as it receives manipulated messages.

To mitigate this problem, a recent line of work by Chromik et al. proposes a local and process-aware approach of monitoring SCADA systems for distribution grids [16]–[20]. The process-aware intrusion-detection system (IDS) takes into account the underlying physical process of power distribution. It utilizes sensor data of the grid model to verify that the data is feasible and issued control actions keep the grid in a safe state. However, the above research focuses on a single substation and its internal processes but does not take into account the relation between neighbouring substations. In this work, the conceptual model for local substations is widened to cover (a part) of a distribution grid. The distribution grid is partitioned into multiple smaller units, i.e. subgrids. Hereby, the topological relation between the subgrids is taken into account to exchange and combine their knowledge on shared components, e.g. a cable connecting two field stations. This combination of knowledge enables a distributed evaluation of the subsystems to detect possible attacks or manipulations within the sensory

This research is conducted as part of the ISoLATE project (CS.016) funded by NWO.

data received from different components within the grid. Combined with the work of Chromik et al. this leads to an IDS which is able to check physical and safety-related requirements in a distributed way for different levels of grid hierarchy. This approach not only secures each individual subgrid and checks the plausibility of sensory readings and incoming commands, but also ensures that both the readings and commands are reasonable regarding the neighboring substations. In this way the presented approach aims to prevent the cascading effects from one substation to its neighbours in case of an attack. To test the feasibility of the presented approach a small test case with four different attack scenarios is evaluated in an extended version of the intrusion detection testbed by Chromik [16], [19].

The paper is organized as follows. First, Section II explains the considered setting and constraints for this paper w.r.t. both, power grids and SCADA networks. Section III builds a decentralized and hierarchical monitoring approach, extending the theoretical model from [19]. Furthermore, Section IV shows the evaluation of the proposed approach using a co-simulation framework, while Section V discusses the result gained from the testbed. Section VI concludes the paper.

II. Background

This section provides background on SCADA networks for electrical grids (Section II-A) and sketches the attack model considered in our approach (Section II-B).

A. SCADA networks

Electrical grids are controlled, among others, by SCADA networks. The central entity of a (centralized) SCADA network is the *control room*. The control room hosts first of all the Human Machine Interface (HMI) which allows the operator to either operate the network automatically or, if necessary manually. For a SCADA network operating an electrical grid, the control room is likely to host additional systems to operate the *Energy Management System* (EMS). Furthermore, there is a *data acquisition server* to collect the data from *field stations* over different communication channels. The control room generally has diverse security mechanisms, like a firewall to prevent malicious command over communication channels. The field stations host the actual physical process and the matching components. Historically speaking, a security paradigm used for SCADA networks and especially for the used communication protocols was ”security through obscurity” (used until the early 2000s) [21], [22]. Consequently, searching for faults in those protocols was not an option for most adversaries. With the opening of SCADA networks to the internet and the standardization of protocols, however, this became a major problem and SCADA infrastructure became vulnerable to cyber-attacks [23]. Furthermore, this problem is expected to increase as soon as vulnerabilities in commonly used protocols are discovered [24]. Such vulnerabilities within the communication protocol enable attackers to intercept or manipulate messages sent from Remote Terminal Units (RTUs) to the EMS, creating a distorted image of the system. This does not only lead to wrongly issued commands, either by humans or automation, back to the field stations, but further circumvents a correct state estimation by the (central) EMS. Furthermore, it should not be neglected that also security breaches in e.g. Windows or other more common software used within the SCADA network may lead to critical problems in the infrastructure [22]. Finally, social attacks and attacks against the physical layer also have to be taken into account.

This paper takes into account the (potentially) insecure communication within the SCADA network and focuses on the evaluation of local data within field stations by comparison with the surrounding context via additional communication channels. Hence, small manipulations targeting the devices within the distribution grid can be detected quickly, without relying e.g. on state estimation.

B. Attack Model

Potential attacks performed by an intruder against the system are summarized in the following. Known vulnerabilities in the employed protocols can enable an attacker to eavesdrop on sent network traffic. Note, that *secure* versions of commonly used network protocols (like Modbus) are often not used [25]. Hence, an intruder may analyse the eavesdropped traffic and can, along with protocol specification and commonly used architecture solutions, gain knowledge about the underlying topology. Furthermore, an intruder may also successfully register legitimate entity (spoofing) and re-send historically captured and slightly manipulated data sets.

This paper focuses on attacks via small manipulations of locally measured data (e.g., at a single sensor) or wrongly issuing commands to individual actors. We also consider an attacker that exchanges all readings with the same time stamp at one field station with historical ones. Both attack types result in a wrong state image at the human machine interface (HMI) and may lead to wrongly issued commands in the (central) EMS. Resulting failures at one field station, e.g. an open switch which causes a local overload and therefore a power outage, then quickly affect neighbouring field stations, possibly triggering a cascading effects.

III. Methodology

This section extends the theoretical model of the IDS, presented in [18], [19]. We consider a division of the distribution grid in so-called *subgrids*, which form connected and to some extend self-contained units within the electrical grid. The region connecting two subgrids with power lines is called a *border region*. The formal definition of the extended model is given in III-A. The physical- and safety requirements used to evaluate a given system state of the model are discussed in III-B. Finally, Section III-C illustrates how the division into subgrids helps to securely supervise with the presented evaluation algorithm.

A. Formal model description

The formal model represents the structure of an electrical grid Ω and its evolution over time. It consists of both *static* and

variable parts, where *static* properties describe the *topology* of the system, i.e, its architecture, and *dynamic* parts describe the current *state* of the system. An instance of the model Ω consists of different physical components, like e.g. power lines and meters. Physical components also have *static* properties describing their topology and *variable* properties describing their current state (e.g. the measured current). Formally, an electrical grid Ω is defined as:

$$\Omega = (\mathcal{P}, \mathcal{B}, \mathcal{T}, \mathcal{L}, \mathcal{S}, \mathcal{M}, \mathcal{F}, \mathcal{R}, \mathcal{K}),$$

where $\mathcal{P} = \mathcal{P}^C \cup \mathcal{P}^G$ is the union of the set of power consumers ($\mathcal{P}^C$) and the set of power generators ($\mathcal{P}^G$), $\mathcal{B}$ the set of buses, $\mathcal{T}$ the set of transformers, and $\mathcal{L}$ the set of power lines. Furthermore, $\mathcal{S}$ is the set of switches, $\mathcal{M}$ the set of meters, $\mathcal{F}$ the set of fuses and $\mathcal{R}$ the set of protective relays. Finally, $\mathcal{K}$ is the set of interlocks present in the electrical grid Ω. Note that not every instance of Ω necessarily needs to contain each of these component types. For instance, there may be electrical grid without any transformers.

Following this structure, a subgrid Ω_i of Ω can be defined by the tuple: $\Omega_i = (\mathcal{P}_i, \mathcal{B}_i, \mathcal{T}_i, \mathcal{L}_i, \mathcal{S}_i, \mathcal{M}_i, \mathcal{F}_i, \mathcal{R}_i, \mathcal{K}_i)$, where, $\mathcal{P}_i \subset \mathcal{P}$, $\mathcal{B}_i \subset \mathcal{B}$, $\mathcal{T}_i \subset \mathcal{T}$, $\mathcal{L}_i \subset \mathcal{L}$, $\mathcal{S}_i \subset \mathcal{S}$, $\mathcal{M}_i \subset \mathcal{M}$, $\mathcal{F}_i \subset \mathcal{F}$, $\mathcal{R}_i \subset \mathcal{R}$, and $\mathcal{K}_i \subset \mathcal{K}$.

In the following calligraphic capital letters denote the set of components in the complete electrical grid, and an additional index refers to the subset of components belonning to a subgrid. A specific element of a subset is indicated by the capital letter, which corresponds to the identifyer of the subset, equipped with an index, e.g., $B_i \in \mathcal{B}$. We collect all component types except power lines as $\mathcal{E} = \{\mathcal{P}, \mathcal{B}, \mathcal{T}, \mathcal{S}, \mathcal{M}, \mathcal{F}, \mathcal{R}, \mathcal{K}\}$, and refer to a general component of the set $\mathcal{E}$ as E or E_i.

For two different subgrids Ω_i and Ω_j of Ω, with i $\neq$ j it must hold that the following subsets are disjoint:

$$\mathcal{E}_i \cap \mathcal{E}_j = \emptyset.$$

Noticeably this does not hold for power lines $\mathcal{L}$, as they may connect two subgrids. For example, a power line $L \in \mathcal{L}$ may connect subgrid Ω_i and Ω_j, and therefore $L \in \mathcal{L}_i \wedge L \in L_j$.

We define a *border region* B_{ij} between two subgrids Ω_i and Ω_j, as a tuple $\mathsf{B}_{ij} = (\mathcal{L}^{\mathsf{B}}_{ij}, \mathcal{S}^{\mathsf{B}}_{ij}, \mathcal{M}^{\mathsf{B}}_{ij}, \mathcal{F}^{\mathsf{B}}_{ij}, \mathcal{R}^{\mathsf{B}}_{ij})$. The power lines connecting both subgrids are collected in $\mathcal{L}^{\mathsf{B}}_{ij} = \mathcal{L}_i \cap \mathcal{L}_j$. Furthermore, the components that are directly attached to one of the connecting power lines are collected componentwise in the following respective sets: set of connected switches ($\mathcal{S}^{\mathsf{B}}_{ij}$), set of connected meters ($\mathcal{M}^{\mathsf{B}}_{ij}$), set of connected fuses ($\mathcal{F}^{\mathsf{B}}_{ij}$), and set of connected protective relays ($\mathcal{R}^{\mathsf{B}}_{ij}$). In contrast to the connecting power line itself, these components are always assigned to either of the two involved subgrids.

Figure 1 illustrates an exemplary *border region* B_{01} between two subgrids Ω_0 and Ω_1. In this topology, Ω_0 consists of the power lines $\mathcal{L}_0 = \{L_1, L_2, L_4, L_5\}$, the meters $\mathcal{M}_0 = \{M_1, M_2, M_4\}$, the switch $\mathcal{S}_0 = \{S_1\}$ and fuse $\mathcal{F}_0 = \{F_1\}$, and bus $\mathcal{B}_0 = \{B_1\}$. Ω_0 only has one RTU, located at B_1. Ω_1 consists of the power lines $\mathcal{L}_1 = \{L_2, L_3, L_5, L_6\}$, the meters $\mathcal{M}_1 = \{M_3, M_5\}$, the switch $\mathcal{S}_1 = \{S_2\}$ and fuse $\mathcal{F}_1 = \{F_2\}$ and buses $\mathcal{B}_1 = \{B_2, B_3\}$. Ω_1 has two RTUs, one located at B_2 and one at B_3. The *border region* B_{01} consists of the power lines $\mathcal{L}^{\mathsf{B}}_{01} = \{L_2, L_5\}$, the meters $\mathcal{M}^{\mathsf{B}}_{01} = \{M_2, M_3, M_4, M_5\}$, and the switch $\mathcal{S}^{\mathsf{B}}_{01} = \{S_1\}$.

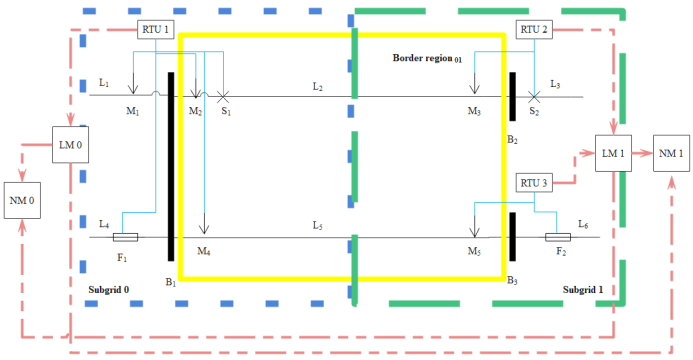

Fig. 1: An exemplary topology for two subgrids, Ω_0 (blue) and Ω_1 (green) and their connecting border region B_{01} (yellow).

For every component type we define the additional *static* property *origin*, which indicates to which subgrid Ω_i said component belongs. More formally, except for power lines $\mathcal{L}$, the *origin* of an element E of component type $\mathcal{E}$ which belongs to subgrid Ω_i is defined as $E.or = i$.

Power lines require a more elaborate definition of origin. For this, we first repeat their definition (c.f. [18]). Power lines connect different components of the grid, i.e. power consumer and producer with buses, transformers and with each other, i.e.:

$$\mathcal{L} \subseteq ((\mathcal{P} \times \mathcal{B}) \cup (\mathcal{T} \times \mathcal{B}) \cup (\mathcal{B} \times \mathcal{B}) \cup (\mathcal{B} \times \mathcal{T}) \cup (\mathcal{B} \times \mathcal{P})).$$

As power lines can connect components that belong to two different subgrids, power lines itself can belong to either one or two subgrids, but not to more. Therefore, the *static* property *origin* $L_i.or$ of a power line L_i which connects a component F_j with a component F_k with $F \in \{\mathcal{P}, \mathcal{B}, \mathcal{T}\}$, is a tuple containing the origin of its two connecting components:

$$L_i.\text{or} = (F_j.\text{or}, F_k.\text{or}).$$

Each power line has a maximum current $L_i.I_{\text{max}}$ and a reference voltage $L_i.V_{\text{ref}}$, which indicate the maximum current that can be endured without damage, and the allowed voltage boundaries. The component descriptions follow [18], [19], extended by the *origin* property, and include further *dynamic* properties like the state of a switch (*open* or *closed*) and *static* properties like attachment of switches to power lines.

Note that the size of subgrids is flexible and subgrids may be formed to match the scope of specific security requirements. Similar to the complete grid, also the subgrids do not need to contain a component of every type. In this paper we focus on the combination of around four field stations and their controlled components into one subgrid. This eases the definition of the physical- and safety requirements in the next section, which mainly focus on the RTU and its components.

B. Physical- and safety requirements

To decide whether a given state of a subgrid Ω_i can be considered as safe, it is checked against pre-defined physical and safety-related requirements. While the physical requirements ensure that the measured data is consistent with physical laws like e.g. the power formula P = V·I, the safety requirements ensure that softer limits, like e.g. desired safety threshold are met. We follow the requirements as defined in [18]–[20] and summarized in Table I. Using the proposed design,

ID	Ensured property of the electrical grid
P1	incoming current matches outgoing current at a bus
P2	all voltages reported at one bus are equal
P3	there is no current on a power line with an open switch
P4	measured values (voltage and current) remain the same over the length of a power line
P5	P = V·I holds for every power producer and consumer
P6	measured outgoing values (voltage and current) at transformers are consistent with the transformation rate and the incoming values
S7	safety threshold regarding current is met at every meter
S8	safety threshold regarding voltage is met at every meter
S9	all fuses and protective relays are functional
S10	maximum current is not met at any fuse or protective relay
S11	currently set transformation rate in every transformer meets the reference voltage
S12	every consumer is connected to the grid and receives positive voltage
S13	power generated in the grid equals the power consumed
S14	operator-defined threshold is met for all meters
S15	all interlocks are not violated by the switches states

TABLE I: (P)hysical and (S)afety requirements (c.f. [18]–[20]).

these requirements can easily be extended, e.g. to include new standards from the European Committee for Electronically Standardisation.

In contrast to the work by Chromik et al., which only considers the information available locally at one RTU and therefore only evaluates requirements that do not require further information, we propose to exchange information with neighbouring field stations. Thus, the requirements need to be classified depending on the level of information needed for their evaluation. Exemplary, requirements which affect components that are part of a border region need to be adapted as both subgrids might be affected by them. This classification is further discussed in the following section.

C. Knowledge scopes and algorithm outline

This section presents the concept of knowledge scopes for the defined physical- and safety requirements and proposes an algorithm for automated evaluation of requirements by the IDS, as illustrated in Figure 2. We distinguish three different knowledge scopes for evaluating the physical- and safety requirements for different ranges of information:

1) *local*: evaluation with the information of a individual subgrid possible
2) *neighbourhood*: evaluation requiring a data exchange between two subgrids sharing a border region
3) *global*: evaluation which is only possible with global knowledge

To minimize the amount of exchanged data beyond the subgrid level (which takes place via dedicated communication channels, as illustrated as red dashed lines in Figure 1), knowledge scopes are defined. These communication channels have to be implemented outside the existing SCADA network and sre assumed to ensure dependable and secure communication.

Every requirement that can be evaluated *locally* at the subgrid, is evaluated via the *local* subgrid monitor (LM). In this case, data is communicated only within the subgrid, i.e. from the local RTUs to the corresponding LM. If the LM detects a violation of a requirement, an alert can be send directly to the grid management or the grid operator. If all requirements are met, the LMs already marks the respective subgrids as safe and secure w.r.t. the requirements of the *local* scope. All LMs evaluate *local* requirements in parallel and independently on their respective data.

Subsequently, the LMs exchange data between subgrids sharing a border region to enable the neighbourhood monitors (NM) to evaluate the *neighbourhood* scope. Note that for the neighbourhood scope not the complete subgrid data needs to be exchanged but only the data concerning the components in the border region. After all NMs received the relevant data from each border region in which they participate, they can evaluate the *neighbourhood* requirements. Note that each border region is supervised by a NM on each side, which introduces further redundancy in the security design.

For the *global* scope, data is collected at a global monitor (GM) which evaluates the *global* requirements. Our proposed approach to use LMs aims to minimize the requirements that need to be evaluated globally as this induces a larger computational load and more secure communication channels. In the setting proposed above, only requirement S13 requires global evaluation.

To illustrate the classification of requirements into the three knowledge scopes, in the following requirement P3 is discussed: Requirement P3 has to ensure that there is no current on a power line with an open switch. It may target power lines that are either located within a subgrid (*inner power line*) or part of a border region (*shared power line*). For inner power lines requirement P3 can be evaluated locally,

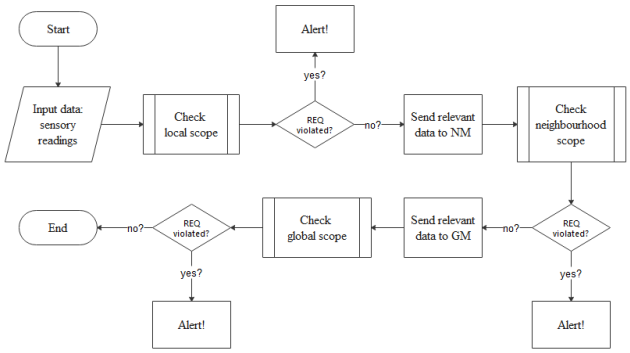

Fig. 2: The outline of the monitoring algorithm as a flowchart.

as all meters and switches attached to the power line always belong to the same subgrid. The local version of P3 formulates as follows:

$$\textbf{REQ P3 L: } \forall\ L_i \in \mathcal{L}_a \wedge L_i.\text{or} = (\text{a,a}) \ \exists\ S_j \in L_i.\text{S}: \\ S_j = 0 \rightarrow \forall\ M_k \in L_i.\text{M} : M_k.\text{I} = 0.$$

For shared power lines however, not all meters and switches attached to the power line are necessarily part of the same subgrid. In contrast, at least one meter is likely attached to both sides of the border region. Hence, for a shared power line within the border region B_{ab} between subgrids Ω_a and Ω_b requirement P3 is written as follows:

$$\textbf{REQ P3 N: } \forall\ L_i \in \mathcal{L}^{\mathsf{B}}_{ab}\ \exists\ S_j \in L_i.\text{S}: \\ S_j = 0 \rightarrow \forall\ M_k \in L_i.\text{M} : M_k.\text{I} = 0.$$

Currently, all requirements belong to the local scope except for P3 and P4, which both have a local and a neighbourhood version. Furthermore, S13 is evaluated globally. Note that, the above requirements serve as a starting point to demonstrate to design of the distributed IDS and can easily be extended.

In contrast to a sequential evaluation of all three scopes, as explained above, a parallel evaluation would further improve the real-time capabilities of the proposed design. In this case, the local subgrids first communicate all necessary information to every monitor and then every monitor evaluates their requirements simultaneously. One advantage of the sequential evaluation is that no unnecessary data is communicated as each manipulation is caught at the lowest possible scope.

IV. Testbed prototype

This section explores the capabilities and limitations of the proposed approach. As it is hard or even impossible to directly test the feasibility of the proposed IDS in a real environment, we resort to a simulation testbed. This simulation models part of a distribution grid and allows to manipulate components to simulate attacks within the testbed. We do not require a full network simulation, as the scope of the proposed approach is local, while taking into account information from two neighbouring substations. We build a model of the electrical grid with two designated subgrids and their shared *border region* in the co-simulation framework Mosaik [26], which simulates electrical grids. The resulting simulation testbed is available via gitlab [1] and builds on the previously presented RTU simulator (c.f. [18]). In that testbed[2] the RTU supervises part of the simulated electrical grid and serves as Modbus/TCP server presenting the sensory data of the supervised part. Note that the simulated environment in these implementations is based on the Mosaik demo scenario[3], which represents a small neighbourhood of houses with a residual load and photovoltaic panels producing additional energy, both simulated randomly.

This paper considers two subgrids (Ω_0 and Ω_1) within the simulated electrical grid each with a few power lines, buses, houses and photovoltaic-panels. Both subgrids share a *border region* and Ω_1 is furthermore connected to the rest of the simulated electrical grid. Figure 3 shows the topology used within the prototype testbed. In this topology each bus is equipped with an RTU, however they are not included in this overview. Both subgrids have a Modbus/TCP server created by the RTU simulator to communicate the data to their (local) monitors. Next to extending the testbed, we also added local and neighborhood monitors to it. Both monitor types receive an appropriate representation of their part of the subgrid topology and take the sensory data produced by the testbed as input. The monitors evaluate the input data with respect to the requirements of their matching scope and test if requirements are violated by the given input. For both subgrids, one instance of a local monitor and one neighbourhood monitor has been created. Thus, both neighbourhood monitors evaluate the border region between the two subgrids from the view point of their respective subgrid. In addition, a monitor has been developed to manage the information exchange between the testbed and the local monitors and between the local and the neighbourhood monitors.

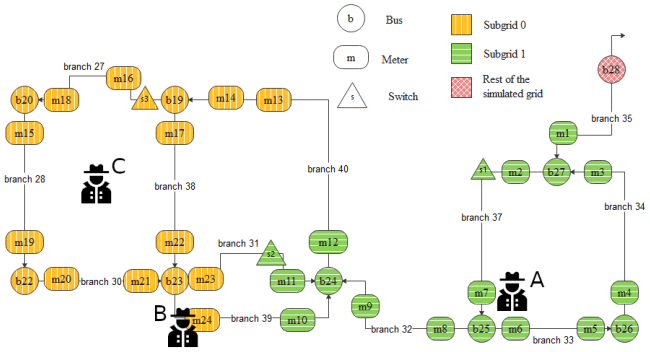

Fig. 3: The grid topology with two subgrids in the proposed testbed. b28 indicates the connection to the rest of the simulated grid. Furthermore three attack points within the electrical grid are denoted with A, B, and C.

V. Evaluation

In this section an evaluation of the proposed approach and testbed is given. Section V-A presents four different scenarios, which were applied to the testbed, together with their respective tool output. Section V-B discusses the types of manipulations that the proposed IDS can detect within the electrical grid.

A. Test scenarios

To explore the feasibility and capability of the proposed model within the testbed, four scenarios are presented, which contain different types of attacks as small manipulations either to switch positions or measured voltage and current. We discuss whether the proposed IDS is able to detect the performed manipulations, which are summarized per attack scenario in Table II. Each row represents an individual attack, which corresponds to the scenario indicated in the first column.

[1] https://gitlab.utwente.nl/vmenzel/distributed_ids_prototype
[2] https://github.com/jjchromik/mosaik-cosim
[3] https://gitlab.com/mosaik/mosaik-demo

1) Scenario 1: Normal grid operation
Attack: No attack happens in this scenario.
Tool output: The proposed prototype triggered no unexpected alerts in Scenario 1. Note that similar to [17], sometimes delays were observed caused by the handovers in the simulation framework, leading to inaccuracies in the communicated measurements. This may lead to false positives.

2) Scenario 2: Violations within the local scope
Attack: Manipulation of individual readings of components from within a subgrid.
Tool output: The prototype is able to detect *all* manipulations from the input data within the local scope, without exchanging any data. This attack corresponds to an attacker who either is physically present at the component or can manipulate only small parts of the data packages sent by the RTU, to cause small disturbances within the grid management.

3) Scenario 3: Violations in local and neighbourhood scope
Attack: Manipulation of individual readings, targeting components from the border region between both subgrids.
Tool output: The prototype IDS is able to detect *all* manipulation that target components from within the border region between the two subgrids. The implemented neighbourhood monitors which correspond to the border region both reported the alerts. Note, that some manipulations in this scenario also caused violations within *local* requirements and therefore trigger alerts before information was exchanged.

4) Scenario 4: Violations within the neighborhood scope
Attack: Manipulation of individual readings of components from within both subgrids and the border region. Replay of a complete historical data set. Manipulations are coordinated by the attacker, so that they do not cause requirement violations in the local scope.
Tool output: The prototype was able to detect *all* performed manipulations. This scenario considers more elaborate attacks, where the attacker is able to manipulate multiple components at the same time. Manipulations target one side of the *border region* and *inner* components of the corresponding subgrids. The manipulations could not be detected by the local monitors, as they were designed to match within a subgrid. However, the proposed design allows to detect these manipulations via the *border regions*: The values reported at both sides of the border region do not match, which the neighborhood monitor picks up and issues an alert.

Scenario	Subgrid	Performed manipulation
1	Ω_0, Ω_1	-
2	Ω_0	Altering the voltage value of m_{17}
2	Ω_0	Altering the current value of m_{23}
2	Ω_0	Changing the switch value of s_3 from true to false
2	Ω_1	Altering the voltage value of m_5
2	Ω_1	Altering the current value of m_6
2	Ω_1	Changing the switch value of s_1 from true to false
3	Ω_0	Altering the voltage value of m_{13}
3	Ω_1	Altering the voltage value of m_{10}
3	Ω_1	Changing the switch value of s_2 from true to false
4	Ω_0	Altering the voltage value of $m_{21}, m_{22}, m_{23}, m_{24}$
4	Ω_0	Replay of a complete historical data set
4	Ω_1	Changing the switch value of s_2 from true to false and the voltage value of m_{11} to 0.0

TABLE II: Manipulation in the different attack scenarios.

B. Detectable attack types

We summarize three attack types (A, B, C), as illustrated in Figure 3. The proposed monitoring system is able to detect all the manipulations presented to it in the above four scenarios. The tool output is available in the gitlab repository of our testbed.

1) A: Manipulation of components within a subgrid
This attack restricts to inner components of a subgrid, as they can already be detected by the local monitoring approach. Here, the attacker can manipulate single readings, either within the communication traffic or while being physically close to the actual component. This could for example manipulate a sensory reading or the position of a switch. Such manipulation, if undetected, may lead to wrongly issued commands and can result in physical damage to components.

2) B: Manipulation within the border region
Using the proposed approach, attacks which target components within the border region, can be detected. In a local approach without the exchange of information the supervision of the border region would not be possible. As an attack on the shared power line between two subgrids can partially detach one of the subgrids from the rest of the main grid, it is of utmost importance to supervise the border regions.

3) C: Manipulation visible in the border region only
As scenario 4 successfully demonstrated, there exist attacks on one subgrid which cannot be detected only within this subgrid. This includes e.g. the replay of historical data, either partially or for the complete subgrid, which does not lead to local alerts when evaluated. We assume that an intruder is able to exchange the complete data traffic within that substation or the data traffic communicated from the subgrid to the outside, e.g. the EMS. Such an attack can lead to distorted state estimations and wrongly issued commands. However, if the attacker is only able to exchange parts of the communicated data traffic within the electrical grid, the surrounding neighbourhood monitors are able to detect this attack, as the data from the both sides of the border region does not match. At the same time, it is unlikely that an attacker is able to exchange large parts of the communication traffic from different subgrids at the same time to make the manipulations consistent. The monitoring system itself is not able to decide which side of the border region is manipulated. However, the manipulations are detected quickly at every border region which has at least one field station that is not under attack.

VI. Conclusion and Future Work

This paper proposes the design of an intrusion detection system, which builds on information from the underlying physical process. It evaluates physical and safety requirements within a broader knowledge scope, connecting neighbouring subgrids. The proposed design enables an IDS to check various physical and safety-related requirements in a distributed way for different levels of hierarchy. By exchanging information

on shared components between neighbouring field station it is now possible to secure these components e.g. against, replay attacks, which could not be achieved by previous purely local approaches. We use a simulation prototype to show the feasibility of the proposed approach. The evaluation results clearly show that adding a broader knowledge scope, e.g. via border regions, to the IDS helps to identify also more intricate attacks. For example, in case of a replay attack to one subgrid, the IDS detects inconsistencies using data from the border region between the attacked stations and its neighbours and issues an alert to the operator.

The current proposal includes three limitations: A secure communication link is required between the local field stations to ensure a secure exchange of the sensory information. Note that, it is easier to achieve a secure link locally, than within the complete SCADA network. Future work will identify appropriate communication on a more technical level.

The testbed prototype simulation currently covers two subgrids, which we plan to extend to larger electrical grids, to also evaluate the global scope. Such an extension furthermore will be able to give additional insights regarding the scaling of the approach. Finally, the approach itself requires synchronization of time-stamps, to ensure that measurements between substations are compatible and do not lead to false positives due to time-shifts.

Future work will go into two directions: Further requirements covering the physical process in more detail, e.g., through reactive power, will be incorporated to further improve security. Especially when taking into account special hardware within a defined subgrid, e.g. a charging station for electric vehicles, meaningful requirements can be added. Additionally, grid topology will be taken into account when monitoring, e.g. the combination of subgrids as a ring. A specific topological structure then allows to introduce additional requirements and properties, which are evaluated by a specific topology monitor.

REFERENCES

[1] D. Kushner. (2013 (Last accessed on September 21, 2021)) The Real Story of Stuxnet. [Online]. Available: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[2] M. Assante. (2016 (Last accessed on September 21, 2021)) Confirmation of a Coordinated Attack on the Ukrainian Power Grid. [Online]. Available: https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/

[3] C. Zhou, S. Huang, N. Xiong, S. Yang, H. Li, Y. Qin, and X. Li, "Design and Analysis of Multimodel-Based Anomaly Intrusion Detection Systems in Industrial Process Automation," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 10, pp. 1345–1360, 2015.

[4] I. Ullah and Q. H. Mahmoud, "A hybrid model for anomaly-based intrusion detection in SCADA networks," in *IEEE Int. Conf. on Big Data (Big Data)*. IEEE, 2017, pp. 2160–2167.

[5] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, "Using Model-based Intrusion Detection for SCADA Networks," in *Proceedings of the SCADA Security Scientific Symposium*, Miami Beach, Florida, Jan. 2007.

[6] G. Koutsandria, V. Muthukumar, M. Parvania, S. Peisert, C. McParland, and A. Scaglione, "A hybrid network IDS for protective digital relays in the power transmission grid," in *2014 IEEE Int. Conf. on Smart Grid Communications (SmartGridComm)*. IEEE, 2014, pp. 908–913.

[7] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J. Tan, "An Intrusion Detection System for IEC61850 Automated Substations," *IEEE Transactions on Power Delivery*, vol. 25, no. 4, pp. 2376–2383, 2010.

[8] H. Lin, A. Slagell, C. Di Martino, Z. Kalbarczyk, and R. K. Iyer, "Adapting Bro into SCADA: Building a Specification-Based Intrusion Detection System for the DNP3 Protocol," in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*. Association for Computing Machinery, 2013.

[9] G. Ndonda and R. Sadre, "A Two-level Intrusion Detection System for Industrial Control System Networks using P4." ICS-CSR, 2018, pp. 31–40.

[10] M. Caselli, E. Zambon, and F. Kargl, "Sequence-Aware Intrusion Detection in Industrial Control Systems," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*. Association for Computing Machinery, 2015, p. 13–24.

[11] S. Pan, T. Morris, and U. Adhikari, "A specification-based intrusion detection framework for cyber-physical environment in electric power system," *International Journal of Network Security*, vol. 17, pp. 174–188, 2015.

[12] A. Valdes and S. Cheung, "Communication pattern anomaly detection in process control systems," in *IEEE Conference on Technologies for Homeland Security*. IEEE, 2009, pp. 22–29.

[13] P. Hines, S. Blumsack, E. C. Sanchez, and C. Barrows, "The Topological and Electrical Structure of Power Grids," in *43rd Hawaii Int. Conf. on System Sciences*. IEEE, 2010, pp. 1–10.

[14] Y.-F. Huang, S. Werner, J. Huang, N. Kashyap, and V. Gupta, "State Estimation in Electric Power Grids: Meeting New Challenges Presented by the Requirements of the Future Grid," *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 33–43, 2012.

[15] A. Monticelli, "Electric power system state estimation," *Proceedings of the IEEE*, vol. 88, no. 2, pp. 262–282, 2000.

[16] J. J. Chromik, A. Remke, and B. Haverkort, "Improving SCADA security of a local process with a power grid model," in *Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research*, 2016, pp. 114–123.

[17] J. J. Chromik, C. Pilch, P. Brackmann, C. Duhme, F. Everinghoff, A. Giberlein, T. Teodorowicz, J. Wieland, B. R. Haverkort, and A. Remke, "Context-aware local Intrusion Detection in SCADA systems: A testbed and two showcases," in *IEEE Int. Conf. on Smart Grid Communications (SmartGridComm)*. IEEE, 2017, pp. 467–472.

[18] J. J. Chromik, A. Remke, and B. Haverkort, "An integrated testbed for locally monitoring SCADA systems in smart grids," *Energy Informatics*, vol. 1, pp. 1–29, 2018.

[19] J. J. Chromik, "Process-aware SCADA traffic monitoring: A local approach," Ph.D. dissertation, University of Twente, Netherlands, 2019.

[20] R. Flosbach, J. J. Chromik, and A. Remke, "Architecture and Prototype Implementation for Process-Aware Intrusion Detection in Electrical Grids," in *38th Symp. on Reliable Distributed Systems (SRDS)*, 2019, pp. 42–51.

[21] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of Cyber-Warfare," *Computers Security*, vol. 31, no. 4, pp. 418–436, 2012.

[22] S. D. Antón, D. Fraunholz, C. Lipps, F. Pohl, M. Zimmermann, and H. D. Schotten, "Two decades of SCADA exploitation: A brief history," in *IEEE Conference on Application, Information and Network Security*. IEEE, 2017, pp. 98–104.

[23] B. Galloway and G. P. Hancke, "Introduction to industrial control networks," *IEEE Communications Surveys Tutorials*, vol. 15, no. 2, pp. 860–880, 2013.

[24] T. Sommestad, G. N. Ericsson, and J. Nordlander, "SCADA system cyber security — A comparison of standards," in *IEEE PES General Meeting*. IEEE, 2010, pp. 1–8.

[25] T. S. Irfan A. Siddavatam, Sachin Parekh and F. Kazi, "Testing and Validation of Modbus/TCP Protocol for Secure SCADA Communication in CPS using Formal Methods," *Scalable Computing: Practice and Experience*, vol. 18, no. 4, 2017.

[26] M. Büscher, A. Claassen, M. Kube, S. Lehnhoff, K. Piech, S. Rohjans, S. Scherfke, C. Steinbrink, J. Velasquez, F. Tempez, and Y. Bouzid, "Integrated Smart Grid simulations for generic automation architectures with RT-LAB and mosaik," in *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2014, pp. 194–199.