



# **D6.1 CONCEPTUAL MODEL OF DATA STREAMS, DETECTION AND VERIFICATION REQUIREMENTS**

VERSION 1

Nils Müller

Kai Heussen

Zeeshan Afzal

Mathias Ekstedt

**31 March 2021**

ERA-Net Smart Energy Systems

This project has received funding in the framework of the joint programming initiative ERA-Net Smart Energy Systems, with support from the European Union's Horizon 2020 research and innovation programme.



## INTERNAL REFERENCE

<b>Deliverable No.:</b>	D 6.1 (2021)
<b>Deliverable Name:</b>	Conceptual model of data streams, detection and verification requirements
<b>Lead Participant:</b>	Nils Müller
<b>Work Package No.:</b>	WP6
<b>Task No. &amp; Name:</b>	T 6.1
<b>Document (File):</b>	210327_NM_D6-1_conceptual_model_of_data_streams_and_monitoring_requirements
<b>Issue (Save) Date:</b>	2024-10-12

## DOCUMENT STATUS

	Date	Person(s)	Organisation
<b>Author(s)</b>	2021-03-16	Nils Müller	Technical University of Denmark (DTU)
	2021-03-22	Kai Heussen	Technical University of Denmark (DTU)
	2021-03-29	Nils Müller	Technical University of Denmark (DTU)
<b>Verification by</b>			
<b>Approval by</b>			
<b>Approval by</b>			

## DOCUMENT SENSITIVITY

- ☒ **Not Sensitive** Contains only factual or background information; contains no new or additional analysis, recommendations or policy-relevant
- ☐ **Moderately Sensitive** Contains some analysis or interpretation of results; contains no recommendations or policy-relevant statements
- ☐ **Sensitive** Contains analysis or interpretation of results with policy-relevance and/or recommendations or policy-relevant statements
- ☐ **Highly Sensitive Confidential** 1. Contains significant analysis or interpretation of results with major policy-relevance or implications, contains extensive recommendations or policy-relevant statements, and/or contain policy-prescriptive statements. This sensitivity requires SB decision.

## 1. CONTENTS

<b>1</b>	<b>INTRODUCTION .....</b>	<b>5</b>
1.1	Objective.....	5
1.2	Scope .....	5
1.3	Approach and structure.....	6
<b>2</b>	<b>REVIEW OF RECENT TOPICS FOR MONITORING AND EVENT DETECTION IN CYBER-PHYSICAL POWER SYSTEMS .....</b>	<b>7</b>
2.1	Overview.....	7
2.2	Description .....	8
2.3	Conclusion .....	14
<b>3</b>	<b>HONOR TECHNICAL ARCHITECTURE.....</b>	<b>14</b>
3.1	General description .....	15
3.2	Actors and zones.....	18
3.3	Data streams of the HONOR technical architecture .....	24
<b>4</b>	<b>CONCEPTUAL MODEL OF THE MONITORING REQUIREMENTS IN CYBER-PHYSICAL SYSTEMS – ON THE EXAMPLE OF A DSO .....</b>	<b>24</b>
4.1	Model structure and components .....	25
4.2	Description of the monitoring requirements .....	29
4.3	Conclusion and Perspectives.....	34
<b>5</b>	<b>REFERENCES .....</b>	<b>36</b>
<b>6</b>	<b>APPENDIX.....</b>	<b>39</b>

### Disclaimer

The content and views expressed in this material are those of the authors and do not necessarily reflect the views or opinion of the ERA-Net SES initiative. Any reference given does not necessarily imply the endorsement by ERA-Net SES.

### About ERA-Net Smart Energy Systems

ERA-Net Smart Energy Systems (ERA-Net SES) is a transnational joint programming platform of 30 national and regional funding partners for initiating co-creation and promoting energy system innovation. The network of owners and managers of national and regional public funding programs along the innovation chain provides

a sustainable and service oriented joint programming platform to finance projects in thematic areas like Smart Power Grids, Regional and Local Energy Systems, Heating and Cooling Networks, Digital Energy and Smart Services, etc.

Co-creating with partners that help to understand the needs of relevant stakeholders, we team up with intermediaries to provide an innovation eco-system supporting consortia for research, innovation, technical development, piloting and demonstration activities. These co-operations pave the way towards implementation in real-life environments and market introduction.

Beyond that, ERA-Net SES provides a Knowledge Community, involving key demo projects and experts from all over Europe, to facilitate learning between projects and programs from the local level up to the European level.

[www.eranet-smartenergysystems.eu](http://www.eranet-smartenergysystems.eu)

## LIST OF ABBREVIATIONS

Abbreviation	Definition
<b>AMI</b>	Advanced metering infrastructure
<b>BRP</b>	Balance Responsible Party
<b>CDMA</b>	Code division multiple access
<b>D</b>	Deliverable
<b>DER</b>	Distributed energy resource
<b>DoS</b>	Denial-of-Service
<b>DMS</b>	Distribution management system
<b>DMZ</b>	Demilitarized zone
<b>DSO</b>	Distribution System Operator
<b>EMS</b>	Energy management system
<b>EV</b>	Electric vehicle
<b>GPRS</b>	General packet radio service
<b>HMI</b>	Human-machine interface
<b>ICT</b>	Information and communication technology
<b>IT</b>	Information technology
<b>IED</b>	Intelligent electronic device
<b>ISR</b>	Imbalancement Settlement Responsible
<b>LAN</b>	Local area network
<b>LoRaWAN</b>	Long range wide area network
<b>LTE</b>	Long term evolution
<b>LV</b>	Low voltage
<b>OT</b>	Operation technology
<b>PV</b>	Photovoltaic
<b>PMU</b>	Phasor measurement unit
<b>PLC</b>	Progamable logic controller
<b>PL-C</b>	Power line communication
<b>RTU</b>	Remote terminal unit
<b>SCADA</b>	Supervisory control and data acquisition

<b>TSO</b>	Transmission System Operator
<b>WP</b>	Work package

## 1 INTRODUCTION

### 1.1 Objective

The HONOR project aims at development and evaluation of a trans-regional flexibility market mechanism, integrating cross-sectoral energy flexibility at a community-wide level. A cornerstone of this work is the development of models and procedures to observe the cyber-physical systems of flexibility markets and detect incoherent and anomalous events. Potential applications are seen in state estimation, flexibility activation monitoring and verification as well as cyber-physical security monitoring of systems and devices. The present work aims at paving the way for the development of monitoring and event detection methods for applications in cyber-physical systems of flexibility markets, such as those mentioned above. Outcome of this work is a systematic representation and connection of monitoring requirements and information streams, supporting the identification and definition of use cases for monitoring and event detection methods in the cyber-physical systems of flexibility markets.

### 1.2 Scope

Cyber-physical systems are integrations of cyber components (computation and communication) and physical components (e.g. machinery or physical infrastructures) that are connected via sensors and actuators [1]. Computers and networks monitor and control the physical components, usually based on feedback loops and possibility for human intervention, interaction and utilization [2]. In a cyber-physical system the cyber part of the system (in the following referred to as the cyber system) affects the physical part of the system (referred to as the physical system) and vice versa: while a cyber attack may adversely influence the physical system, failures of physical equipment may lead to incomplete data or delays in computing and command delivery and thus negatively impact the performance of the cyber system. In a cyber-physical power system the traditional power system with physical equipment as a core element is more integrated with information and communication technology (ICT) what allows two-way flows of electricity and information for enabling smart grid technologies. While used for recording, communicating and processing physical measurement data, the cyber system adds metadata as an additional layer of data to the cyber-physical system. Metadata can be defined as the “data about data” [3]. Examples for metadata are the data packet length or latency. Even though the increasing application of ICT introduces a new era of monitoring and controlling the electric power system it also creates new vulnerabilities such as cyber security issues. Metadata provides information about the state of the cyber system and is therefore used for cyber system monitoring. Thus, metadata can be considered the equivalent of physical measurements for the cyber system. However, the strong interconnection of the cyber and physical system might also have as consequence that information about states and events in the

cyber system can also be found in the data of the physical system and vice versa. This situation raises two fundamental questions:

1. Can data from the physical system provide valuable information for monitoring of the cyber system and vice versa?
2. Can additional information about events or system states be revealed by correlating physical measurements and metadata for monitoring of systems and devices in cyber-physical systems?

This report is focused on the review of methods and conceptual modelling of the above described problem domain. Out of scope are detailed cyber-physical system models of specific applications and use cases. For HONOR use cases refer to D3.1 and for HONOR system architecture to D3.2. Specific cyber-physical analyses on the HONOR technical architecture will be reported in D7.1 and applications of monitoring solutions are reported in D6.2 and D6.3.

### **1.3 Approach and structure**

This work consists of three main parts: in Section 2 recent research topics for monitoring and event detection in cyber-physical power systems are reported based on a literature review. To be able to localise and analyse data streams within the HONOR system architecture [4], Section 3 presents a detailed technical representation of the ICT systems of stakeholders associated with the HONOR system architecture. Section 4 combines the results of Section 2 and Section 3 to contextualize monitoring requirements of the cyber-physical systems within the HONOR system architecture in form of a new generic multi-domain architecture model for monitoring of cyber-physical systems. The model is illustrated on the example of a Distribution System Operator (DSO).

## 2 REVIEW OF RECENT TOPICS FOR MONITORING AND EVENT DETECTION IN CYBER-PHYSICAL POWER SYSTEMS

In this Section current research topics for monitoring and event detection in cyber-physical power systems are presented. As in the HONOR project a local flexibility market concept is considered, the focus of this review is on distribution grids. The review covers topics concerned with either the physical system or the cyber system, topics that are relevant for both systems as well as topics that specifically address the interaction between the systems. The identification of current research topics is based on a screening of literature reviews which have been published between 2010 and 2021 on related topics such as state estimation, intrusion detection, fault detection, cyber-physical security and big data issues in smart grids.

### 2.1 Overview

In Figure 1 a categorization of the identified topics according to the underlying task is depicted. The topics have been separated into three main categories: monitoring, event detection and data processing. Many topics combine different categories, which is represented by the intersection zones. In Figure 2 the topics are assigned to either the physical or the cyber system. The intersection of both circles represents topics that specifically address correlation of information from the cyber and physical system as well as general data processing issues that concern both systems. The graphical overviews in Figure 1 and Figure 2 are not supposed to provide a strict categorization but rather a sense for the current research landscape in the field of monitoring and event detection in cyber-physical power systems.

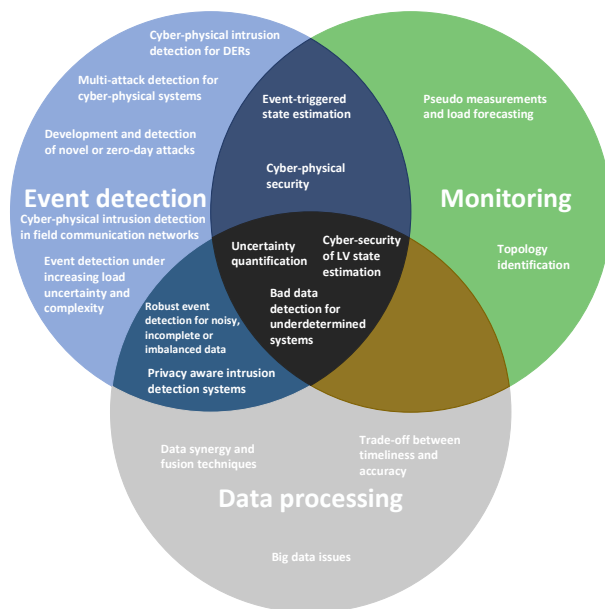


Figure 1 Task-oriented categorization of current research topics for monitoring and event detection in cyber-physical power systems.

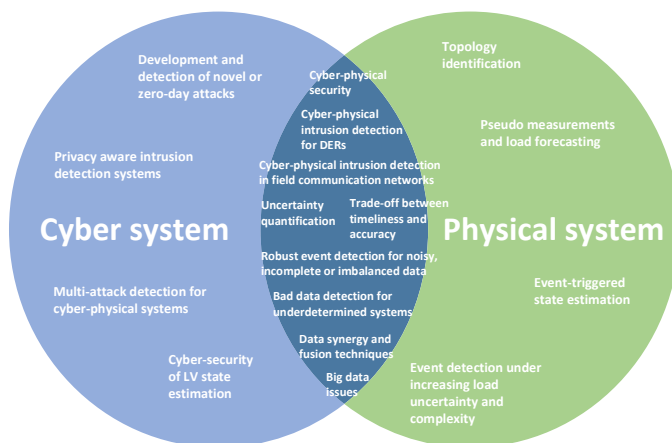


Figure 2 System-oriented categorization of current research topics for monitoring and event detection in cyber-physical power systems.

## 2.2 Description

In this Section the recent research topics for monitoring and event detection in cyber-physical power systems that are depicted and categorized in Figure 1 and Figure 2 are described.



### 2.2.1 Cyber-physical security

A more general direction for further research is seen in cyber-physical security [1,5]. According to [5] cyber-physical security aims at considering and correlating aspects and information from both the physical and cyber system. The motivation for taking into account both systems is given by the incompleteness of system and event models when considering either only the cyber or physical system. A physical attack can hardly be detected by only considering the cyber system (e.g. shunt connectors for bypassing smart meters), while crucial information about the cause of wrong physical measurements can often only be derived by monitoring the cyber system as well. Although the authors of [5] refer to attack detection when discussing cyber-physical security the approach can be transferred to event detection in general. Modeling both the cyber and physical system generally increases the awareness about the context in which an event takes place. On the one hand, a better understanding of the context helps in deciding whether an event of interest is actually present. On the other hand, additional insights into the nature of an event might be revealed.

### 2.2.2 Cyber-physical intrusion detection for DERs

A concrete application of the cyber-physical security approach is the cyber-physical intrusion detection for DERs. Unwanted changes in DERs data and control signals can lead to damages of DERs or electric infrastructure. Corrupted meter data can lead to wrong state estimations in the distribution management system (DMS) of a DSO or the energy management system (EMS) of a TSO. In order to better detect new or well-hidden intrusions as well as quickly classify and distinguish between different events or anomalies the use of various data sources from DER communication (e.g. packet length and polling frequency) and physical measurement equipment (e.g. voltage and current) is proposed [6,7]. In this context, processing large and heterogenous amounts of data can be particular challenging due to the limited computing power of DER.

### 2.2.3 Cyber-physical intrusion detection in field communication networks

Most literature on cyber-physical intrusion detection do not fully reveal the considered trust model [8]. However, the communication between field devices is conducted through different channels than the communication between local controllers (e.g. RTUs or PLCs) or between local controllers and the control center. By considering network packets for intrusion detection from within the control center network, it is assumed that the local controller is trustworthy. In the Stuxnet attack [9], a PLC was compromised to send manipulated control signals to a field device. While the actuators sent back the true measurements to the PLC, the compromised PLC reported false measurements to the control center. By considering only the communication between the compromised PLC and the control center, it is not possible to detect compromised local controllers unless it is possible to correlate information from other trusted PLCs. Given the increasing number of coordinated and distributed cyber attacks as well as the low measurement redundancy in distribution grids, monitoring of field communication networks can be considered as a bottleneck in current power systems. Liu et al. [10] showed, Deliverable No. 6.1 | Conceptual model of data streams, detection and verification requirements

it is possible for an attacker to create false sensor signals that will not raise an alarm by only monitoring network packets. A need for more research is therefore seen in combining and correlating information from the cyber system and physical system for monitoring of measurements and control signals in the field communication networks [1,8,11–13].

#### 2.2.4 Event detection under increasing load uncertainty and complexity

The uncertainty of loads in active distribution grids will increase due to increasing shares of volatile or hardly predictable DERs (e.g. PV and EV) as well as their continuous control for participating in power markets. A demand for more research is seen in the investigation of methods that are robust against uncertainty in system parameters, modelling and measurements [14,15]. One potential approach is seen in combining different data sources such as weather data, electricity price data, and net load data to increase the predictability of the normal behavior [16,17]. The increasing number of DERs and topology changes also increase the number of system states and frequency of system state changes. For this reason, another research field is seen in the development of context-aware event detection systems that can cope with the dynamic nature of smart grids [14,18]. Moreover, a lack of event detection methods that can work in general distribution network with multiple types of DERs is identified in the literature, as most proposed methods are tailored to specific scenarios and DERs [17].

#### 2.2.5 Multi-attack detection for cyber-physical systems

Most attack detection methods assume the presence of a single attack [11]. However, cyber-physical systems in the future may be exposed to multiple attacks instead of only single attacks. A cyber-physical system could be attacked by multiple intruders at the same time or an intruder could be capable of launching multiple attacks simultaneously on the networks or sensors. For example, a system may be subjected to replay attacks and covert attacks simultaneously. In such cases existing detection methods and defense strategies tailored to single attacks are not sufficient to ensure the security of cyber-physical systems. An important object for future research is therefore seen in multi-attack detection for cyber-physical systems [11,19].

#### 2.2.6 Development and detection of novel or zero-day attacks

Most of the existing works on intrusion or anomaly detection focus on improving the detection performance on known attack types [11,20]. This reveals two potential research directions: on the one hand more and ongoing research demand is seen on detecting new or zero-day attacks since new attack tactics are continuously discovered and existing ones evolved [18]. On the other hand, a barely addressed topic is the security and robustness of the detection algorithms [20]. Recently, it could be shown that many machine learning detection algorithms are very vulnerable to be by-passed by new adversarial techniques [21,22]. For that reason, a need for more research is seen in developing novel attacks targeting detection systems and especially the corresponding countermeasures.

### 2.2.7 Robust methods for noisy, incomplete or imbalanced data

One of the universal challenges for the application of data-driven methods is the robustness against noisy, incomplete or imbalanced data [23]. While the amount of data in active distribution grids is increasing, the occurrence of specific events (e.g. faults) in power systems can be very low. Event detection problems such as fault detection often poses an unbalanced data problem with only few available data, describing the power system under influence of the event. Important research fields are therefore seen in the investigation of advanced methods for artificial generation or simulation of minority class data [23] as well as methods for monitoring and event detection that can cope with small training and test datasets [6,24].

### 2.2.8 Privacy aware intrusion detection systems

The foundation for appropriate data-driven intrusion detection is accurate and sufficient data for model development. In most works on intrusion detection the use of fine-grain data is assumed [6]. Therefore, an open research question is seen in addressing privacy preservation in the context of intrusion or anomaly detection to achieve a trade-off between accuracy and privacy [1,6,16,20].

### 2.2.9 Pseudo measurements & load forecasting

One of the central issues for LV state estimation is the low observability of distribution systems. Since economic constraints in many cases avoid an extensive equipment of distribution grids with meter instruments much research is conducted on load forecasting and pseudo measurements based on historical data. However, for optimal power management and decision making under limited distribution system observability a need for more research on improved load forecast and pseudo measurement techniques is identified by various reviews [25,26].

### 2.2.10 Topology identification

The topology identification problem includes two separate subproblems: 1) system configuration identification and 2) topology learning. For the system configuration identification problem, it is assumed that the basic grid topology is known. However, due to local events (e.g. switching events) the topology will change over time. As the topology directly influences the results and applicability of LV state estimation methods, these changes need to be detected in order to avoid topology errors. Similar to LV state estimation the accuracy and validity of fault detection and analysis methods depends on the knowledge of the grid topology since every topology change is a challenge to fault detection and location techniques. Since the number of switching operation in distribution grids will increase due to the increasing active management, methods that are robust to topology changes need further investigation [24,27]. The topology learning problem deals with the identification of the basic grid topology and is based on the assumption that the operator has no or very limited knowledge of the basic topology. Topology identification as basis for LV state estimation is considered as important future research field by various reviews [25,28–30]. Three main challenges are identified: 1) topology identification under reduced observability due to meter and communication failures (e.g. after extreme weather events) [28]. 2) Integration of topology identification into LV state estimation. 3) Integration of topology identification into LV state estimation requirements.

estimation for continuously updating of the state estimator in a closed-loop approach [31]. 3) Overcome the trade-off between accurate and computational efficient topology identification [25].

#### 2.2.11 Event-triggered state estimation

The size and complexity of distribution systems as well as the increasing amount of data poses great challenges for online monitoring. To reduce the computation and communication burdens in LV state estimation most reviews see the necessity of more research in the field of event-triggered sensing, communicating and information processing for LV state estimation [25,26,29,31]. In an event-triggered approach, the state estimation functions could be carried out locally, only when the received measurements include sufficient novelty above a certain threshold value [25].

#### 2.2.12 Data synergy and fusion techniques

One of the most frequently proposed future research fields are data synergy and fusion techniques [25,26,29–36]. In the context of smart grid, the number of measuring devices and sensors in distribution systems (e.g. smart meters and PMUs) increases quickly. At the same time legacy data sources (e.g. SCADA) are still in use. The increasing amount of available data poses great opportunities for LV state estimation. However, legacy and new data sources differ in various aspects such as information source, data formats, data rate, accuracy, reliability, synchronicity, delay, and data privacy. For this reason, a need for more research in the field of exploiting large amounts of heterogeneous data is identified by almost every considered review. Main challenges are seen in the integration of smart meter data (data privacy issues, low data rate (15-60min), low reliability, lack of time synchronization) [31], PMU measurements [25,26], and logical measurements (e.g. switch/breaker statuses) [31] for accurate and robust monitoring and event detection. Besides the combination of physical measurements also the correlation of data from the cyber and physical system (see Section 2.2.1) can be considered a data synergy and fusion problem.

#### 2.2.13 Big data issues

An identified research field related to data synergy and fusion techniques is the extraction of informative features for monitoring and event detection from large raw data volumes. The development of smart grid leads to the generation of massive amounts of data. Such data is too large and complex to compute with traditional data analytics what makes it a big data challenge [37]. In their native form, such raw data signals can be noisy, redundant and heterogenous and require large amounts of memory to store. To handle these data sets, methods for extraction of informative features for meaningful and timely monitoring and event detection need to be further investigated [11,14,15,35]. This challenge is especially seen for DER intrusion detection systems due to comparatively strong limitations of the available computational power. For cyber-physical monitoring and event detection a real-time requirement may come with additional difficulty as part of the monitored

data might be affected by additional delay for instance because of cryptographic mechanisms [1].

#### 2.2.14 The trade-off between timeliness and accuracy

Reviews on existing literature on monitoring and event detection have revealed that proposed methods typically come either with high accuracy or speed. Therefore, need for more research on overcoming the trade-off between timely and accuracy was identified [17]. One approach is seen in the investigation of hybrid methods [36]. The basic idea of hybrid methods for event detection is to combine the strengths of individual methods while restraining shortcomings. However, the related decision-making process for output determination is seen as a big challenge for hybrid methods [24,38].

#### 2.2.15 Bad data detection for underdetermined systems

Bad data refers to data measurements that have considerable deviation from the underlying actual behavior, e.g. due to meter malfunction and communication noise. Missing data constitutes a special case of bad data. In transmission systems bad data detection is conducted by inspecting the normalized measurement residuals. However, this method requires sufficient measurement redundancy. In contrast to transmission systems, distribution systems lack redundant real-time measurements. This changes problems such as LV state estimation from an overdetermined to an underdetermined problem [28]. Since such underdetermined problems can be highly affected by the quality and availability of sensor data, a system for bad data detection and correcting is required. In traditional state estimation methods such as weighted least squares methods, bad data detection is conducted after the state estimation process, by reducing the weight of measurements with high residual during the estimation process so that the influence of bad data on the solution is minimized. Within the investigated literature, bad data detection for underdetermined systems that rely on pseudo measurements is identified as a field that need further research [29]. To cope with the scarcity of available measurements, data-driven methods can be applied to detect and correct bad data before the actual state estimation calculation.

#### 2.2.16 Cyber-security of LV state estimation

LV state estimation can be corrupted by different types of cyber-attacks such as false data injection, topology attacks, and eavesdropping [28]. As LV state estimation will constitute a central functionality of the monitoring and control of future active distribution system, corrupted LV state estimation poses a high risk for power system operation. Moreover, more research in the field of cyber-security of LV state estimation is seen due to the ongoing development of new attack strategies.

#### 2.2.17 Uncertainty quantification

Different sources of uncertainty exist for monitoring and event detection applications such as inherent noise of data or insufficient data for model development [39]. Moreover, due to the increasing share of highly volatile DERs and their continuous control the uncertainty of power production and consumption in

distribution systems rises. To cope with the volatile and hardly predictable nature of DERs, it is proposed to consider and express the prediction uncertainty of monitoring and event detection models as additional information output [25,29,40]. The determination of the prediction uncertainty improves the situational awareness of the grid operator and facilitates the interaction between decision support tools and operators domain-knowledge.

### 2.3 Conclusion

The overarching research question in all identified research topics is “how to benefit from the increasing amount of data streams in power systems?”. However, depending on the scientific background this question is considered from one of the following two different perspectives:

1. How can we process the increasing amount of data and maximise the information extraction to improve the operation of power systems?
2. How can we ensure trustworthiness of the data to avoid threats for power systems because of the increasing dependency on potentially wrong data streams?

Data fusion is seen as very promising approach in both perspectives. Data fusion within the physical or cyber system and across systems was discussed by almost every review article and is part of most of the identified research topics. However, the correlation of information across systems is rather rarely considered and in most cases only from a cyber security point of view (e.g. cyber-physical intrusion detection in communication networks). One of the barriers is seen in the difficulty of procuring appropriate cross-domain data sets for model development. Another reason could be the interdisciplinarity of the topic as combining physical and cyber information also joins different research fields. Nevertheless, promising research topics could exist in the combination of the different perspectives on monitoring and event detection in cyber-physical systems. Resulting concrete use cases for monitoring and event detection are discussed in Section 4.3.

## 3 HONOR TECHNICAL ARCHITECTURE

The HONOR system architecture presented in [4] is oriented towards overall use cases of flexibility management. In order to develop a detailed view for the

identification of relevant and feasible use cases for monitoring and event detection methods, an overview of data streams within the HONOR system architecture is required. The information a detailed overview of data stream provides is twofold and can be related to the two perspectives on monitoring and event detection in cyber-physical systems that were defined in Section 2.3:

- 1) Overview about possible information sources for monitoring and event detection applications. This information provides the basis for the first perspective defined in Section 2.3.
- 2) Information about data streams that need to be checked for confidentiality, integrity, availability, non-repudiation and authentication [2] in order to ensure trustworthiness of the data streams. This information provides the foundation for the second perspective defined in Section 2.3.

In order to identify all relevant data streams of the HONOR system architecture (presented in D3.2 [4]) the degree of detail of the system representation needs to be increased. For that purpose, a model of the underlying IT systems and network layer was developed which in the following is referred to as the HONOR technical architecture. Besides the use for identification and representation of data streams, the HONOR technical architecture will provide the basis for cyber security modelling and assessment in the HONOR project.

### **3.1 General description**

Starting point for modelling the technical architecture is the HONOR system architecture which was presented in D3.2 [4]. Based on the high-level overview of actors and communication paths within the HONOR system architecture, the various actors and communication paths were modelled in more detail. The modelling language as well as the representation of some actors of the system were derived from [41]. The resulting HONOR Technical Architecture is depicted in Figure 3. A description of the model components, representing the modelling language, can be found in Table 1.

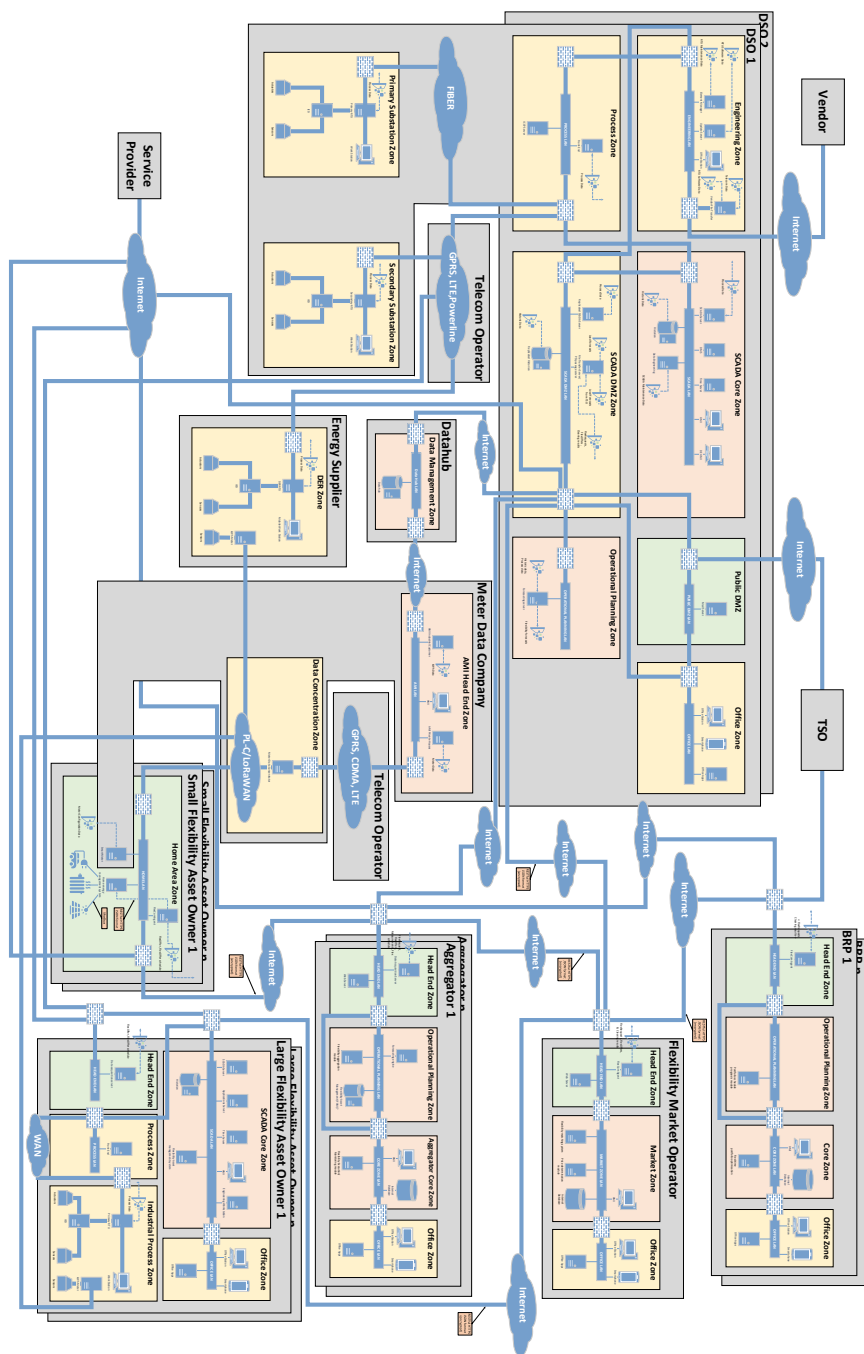

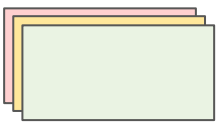



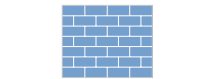


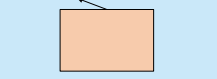


Figure 3 HONOR technical architecture.  
 Deliverable No. 6.1 | Conceptual model of data streams, detection and verification requirements  
 - 16 -



Table 1 Component description of the HONOR technical architecture.

Component	Description
	Boundary of the respective system actor. Multiple occurring actors are represented by stacked boxes.
	Network zones within the actors. The color coding represents the security level. Two network zones of the same color use a similar level of security rules and guidelines to protect the network. In practice, zones do not necessarily have a physical separation and can run on the same system.
	Functional components within the networks. For better readability the functionalities are depicted as physical components. However, in practice the functionalities are often hosted by the same system.
	Communication paths between different actors and network zones.
	Communication networks
	Firewalls or Gateways
	Local area networks (LAN) of the network zones
	Data streams
	Definition of protocols

## 3.2 Actors and zones

### 3.2.1 DSO

#### 3.2.1.1 SCADA Core Zone

The SCADA Core Zone is the central part of the architecture of the DSO. From the SCADA Core Zone operator commands are distributed to the process equipment such as the substations. The interaction of human operators with the SCADA system is conducted via the Human Machine Interface (HMI). Measurements, statuses, issued commands and other data are collected and stored in the Historian.

#### 3.2.1.2 SCADA DMZ Zone

The SCADA DMZ Zone is a “network between the networks”. It separates the OT or SCADA from less-trusted IT networks such as the Office Zone. Data from the SCADA Server and Historian are transferred to the replicated SCADA Server and replicated Historian, respectively, to allow the Office Zone access to the process data. Moreover, the SCADA DMZ Zone contains the File Transfer Server, which is responsible for collection of external data such as load forecast data, software updates and flexibility offers.

#### 3.2.1.3 Engineering Zone

Via the Element Manager of the Engineering Zone parameters of RTUs and IEDs are changed. Examples are allocation of signals to input board channels. The Vendor File Transfer Server collects software and firmware updates. From the Engineering Zones these updates are transferred to the SCADA Core Zone. The Engineering Zone is not concerned with real-time operation of the system.

#### 3.2.1.4 Office Zone

In the Office Zone tasks that are not directly related to power system operation are located such as statistics and status information (e.g. outages). Staff located in the Office Zone can access data from the Replicated Historian and Replicated SCADA Server.

#### 3.2.1.5 Public DMZ Zone

The Public DMZ Zone is responsible for regular communication of the office with the public internet e.g. via a mail server.

#### 3.2.1.6 Process Zone

The Process Zone is responsible for the communication between the SCADA Core Zone and the substations. By transferring data streams bidirectionally via the SCADA Front End, the Process Zone allows communication between the SCADA Core Zone and the Substations without a direct connection.

#### 3.2.1.7 DSO FIBER Network and Primary Substation

The DSO FIBER network is a communication channel that is hosted and managed by the DSO. The FIBER network is used to connect Primary Substations to the SCADA system. Which component a Primary Substation includes varies strongly from DSO to DSO. In many cases Primary Substations contain Remote Terminal Units (RTUs) which are either directly connected to the physical hardware or via Intelligent Electronic Devices (IEDs)

#### 3.2.1.8 Telecom Operator and Secondary Substation

The vast number of Secondary Substations makes a connection via FIBER networks unfeasible. If communication between Secondary Substations and the SCADA system exists it is realized by public networks of telecom operators.

#### 3.2.1.9 Operational Planning Zone

Within the Operational Planning Zone tasks concerned with daily planning of power system operation are conducted such as congestion management, Redispatch and day-ahead flexibility demand forecasting. The Operational Planning Zone is not concerned with real-time operation of the power system.

### 3.2.2 Aggregator

#### 3.2.2.1 Head End Zone

The Head End Zone of the Aggregator is hardware and software (Data Acquisition Server) that receives data from and sends data to external entities. Before making the data available to other zones of the Aggregator architecture or pushing data out of the system the Data Acquisition Server may perform a limited amount of data validation. The Head End Zone is separated from more critical system zones via security gateways.

#### 3.2.2.2 Operational Planning Zone

The Operational Planning Zone of the Aggregator hosts functionalities for planning and maintenance of the portfolio of small flexibility assets. The forecasting engine generates forecasts with respect to the consumption, production or storage of flexibility assets. The forecasts will be used by the flexibility aggregation module, to produce flexibility activation schedules as a response to a flexibility request. In this way incoming service requests are mapped to control domain signals. The Flexibility Asset Management System collects and evaluates data about the behaviour of individual Flexibility Assets. Data is analyzed to determine the performance of a client and the compliance with the contracted flexibility service [42]. Moreover, the Flexibility Asset Management System maintains an overview of the flexibility asset availability. Assets can be temporarily or permanently excluded. The Operational Planning Zone is not concerned with real-time management of the portfolio.

#### 3.2.2.3 Aggregator Core Zone

The Aggregator Core Zone can be compared to the SCADA Core Zone of the DSO. Via the Core Zone the operator can enter commands and monitor the flexibility

service activation via the HMI. The Flexibility Execution and Monitoring Module provides the control inputs for individual Flexibility Assets and monitors the flexibility service activation in real-time. The Aggregator Internal Database collects and stores process and contractual data such as flexibility asset measurements, control setpoints and market clearing results. The Aggregator Core Zone hosts service applications for the real-time operation and management of the flexibility portfolio.

#### 3.2.2.4 Office Zone

In the Office Zone tasks such as statistics and customer service that are not directly related to planning and operation of the portfolio are located. Staff located in the Office Zone can access data from the Aggregator Internal Database.

### 3.2.3 Small Flexibility Asset Owner

#### 3.2.3.1 Household Zone

The Household Zone hosts the Home LAN which facilitates communication among devices within close vicinity of a home. Smart devices such as network printers and mobile computers are connected to the Home LAN. Small Flexibility Assets such as electric vehicles, heating, ventilation and air condition systems or rooftop PV plants are connected to the Home LAN via the Home Energy Management System. The Home Energy Management System is responsible for controlling the smart devices of the household and thus for following a flexibility schedule to provide flexibility according to a contractual agreement. In some cases the Home Energy Management System is capable of generating flexibility forecasts that can be send to the Aggregator. If this is not the case measurements are transferred to the Aggregator. The communication between the Small Flexibility Asset and the Aggregator is conducted via the FlexCom Agent. Smart meters for recording of the energy consumption are also connected to the Home LAN. The energy consumption recordings are transferred to the Meter Data Company on a regular basis.

### 3.2.4 Large Flexibility Asset Owner

#### 3.2.4.1 SCADA Core Zone

As an example of a large flexibility asset an industrial process is considered. In most cases monitoring and control of industrial processes is conducted by a SCADA system. Thus, similar to the DSO the heart of the technical architecture of a Large Flexibility Asset Owner is a SCADA Core Zone. A description of the network components (e.g. HMI, Historian, SCADA server) can be found in Section 3.2.1.1. The Flexibility Asset Management System is responsible for providing flexibility offers based on process and external data as well as generating control commands (e.g. setpoints) for the process under control to provide flexibility according to the contractual agreement.

#### 3.2.4.2 Office Zone

In the Office Zone tasks that are not directly related to the operation of the industrial process are located such as statistics, quality control and factory planning and management. Staff located in the Office Zone can access data from the SCADA Historian.

#### 3.2.4.3 Process Zone

The Process Zone is responsible for the communication between the SCADA Core Zone and the Industrial Process Zone. By transferring data streams bidirectionally via the SCADA Front End, the Process Zone allows communication between the SCADA Core Zone and the process under control without a direct connection.

#### 3.2.4.4 Head End Zone

Similar to the Head End Zone of the Aggregator (Section 3.2.2.1) the Head End Zone of the Large Flexibility Asset Owner is hardware and software (Data Acquisition Server) that receives data from and sends data to external entities. An important example are emergency control signals from the DSO that are received by the Data Acquisition Server before transferring to the real-time operation zones.

#### 3.2.4.5 Industrial Process Zone

Similar to Substation networks of the DSO the Industrial Process Zone is assumed to contain a RTU as well as several IEDs. In many cases instead of RTUs programmable logic controllers (PLC) are implemented. The energy consumption of the factory is recorded by kWh meters and collected by the Meter Data Company.

### 3.2.5 Flexibility Market Operator

#### 3.2.5.1 Market Zone

The Market Zone hosts the modules that provide basic functionalities for operation of the flexibility market such as market clearing, price determination and settlement. The Flexibility Matching System realizes the market clearing based on the matching of flexibility requests and offers. In the Price Determination Module market prices for various flexibility services (e.g. congestion management) are determined. Flexibility requests, offers and market clearing results are stored in the Internal Database and presented to the human operator via the HMI.

#### 3.2.5.2 Head End Zone

The Head End Zone of the Flexibility Market Operator is responsible for collecting flexibility requests and offers of the market participants as well as sending out clearing results and settlements. Similar to the Head End Zone of other actors of the system the Head End Zone of the Flexibility Market Operator separates the data acquisition from the core functionalities (Market Zone).

### 3.2.5.3 Office Zone

In the Office Zone tasks that are not directly related to the operation of the flexibility market are located. Staff located in the Office Zone can access data from the Internal Database in the Market Zone.

## 3.2.6 Balance Responsible Party

### 3.2.6.1 Operational Planning Zone

The Operational Planning Zone of the Balance Responsible Party hosts portfolio management applications related to portfolio scheduling and prognosis. The Operational Planning Zone is not concerned with real-time management of the portfolio.

### 3.2.6.2 Core Zone

The Core Zone of the Balance Responsible Party is concerned with (near) real-time optimization of the portfolio. Real-time portfolio optimization also includes the decision about flexibility activation requests. Information related to portfolio management are stored in the Internal Database. Human operators can observe and control the portfolio management process via the HMI.

### 3.2.6.3 Office Zone

In the Office Zone tasks that are not directly related to the operation and planning tasks for portfolio management are located. Staff located in the Office Zone can access data from the Internal Database in the Core Zone.

### 3.2.6.4 Head End Zone

The Head End Zone of the Balance Responsible Party is responsible for information exchange with the TSO for portfolio management. Additional flexibility requests and offers are exchanged with the flexibility market via the data acquisition server in the Head End Zone. Similar to the Head End Zone of other actors of the system the Head End Zone of the Balance Responsible Party separates the data acquisition from the core functionalities (Portfolio management).

*At the time of finalizing this report, the role and functionalities of the BRP within the HONOR system architecture and market design was not finally defined. Deviations to later reports may occur.*

## 3.2.7 Energy Supplier

### 3.2.7.1 DER Zone

The DER Zone represents the local network of a DER which is hosted by an energy supplier. Similar to the Substations of the DSO the DER Zone contains systems for managing the power generation of the distributed energy resource. Although the DER is hosted by an energy supplier the DSO has ability to directly control the DER in emergency situations. The DER Zone also contains a kWh meter for recording

energy generation/consumption. The kWh meter data are collected by the Meter Data Company.

### 3.2.8 Meter Data Company

#### 3.2.8.1 Data Concentration Zone

The Data Concentration Zone hosts the Meter Data Concentrator which is responsible for collecting smart meter data from a cluster of private households and industrial customers. Remote handling requests (e.g. meter status query) from the Meter Data Company are distributed via the Meter Data Concentrator as well.

#### 3.2.8.2 AMI Head End Zone

The AMI Head End Zone hosts the systems that are in charge of managing all the metering information retrieved from smart meters. The Head-End Zone is also the target for commands to be delivered to smart meters, e.g. connection/disconnection of the customers to/from the network, change of settings, other commands and firmware upgrades. In some cases the AMI Head End Zone is equipped with a HMI that allows the Meter Data Company to look at Meter Data from AMI Private Houses, i.e. power quality data in profiles in the meter.

**Commented [NM1]:** This needs some input/revision from people with better understanding of AMI

### 3.2.9 Additional actors

Although a detailed architecture representation of some actors of the HONOR system architecture is out of scope of this work, the consideration of these actors in the developed technical architecture is necessary as their interaction with other actors results in relevant data streams that need to be included. Such actors are represented in the technical architecture as black box models. In this way, relevant data streams, resulting from the communication and data exchange between actors can be presented without a detailed representation of the architecture.

#### 3.2.9.1 TSO

Manifold interactions between the TSO and other actors exist. The TSO provides the DSO with load forecast data. Moreover, the TSO can participate on the flexibility market and procure flexibility services. In order to avoid conflicts between the local flexibility market and upstream markets (spot market, ancillary service market) the TSO monitors the market action and restricts the flexibility market in critical situations.

*At the time of finalizing this report, the role and functionalities of the TSO within the HONOR system architecture and market design was not finally defined. Deviations to later reports may occur.*

#### 3.2.9.2 Vendor

Vendors provide all actors of the HONOR system architecture with hardware and software updates. For the sake of readability, only the supply of the DSO with updates is represented in Figure 3.

### 3.2.9.3 Data Hub

The Data Hub stores all information about the electricity consumption of consumers. Besides storing data business processes such as changes of address or supplier are handled. The Data Hub receives the smart meter readings from the Meter Data Company and distributes them to the Data Hub users such as energy suppliers and DSOs.

### 3.2.9.4 Service Provider

Service provider such as weather stations provide various actors of the HONOR system architecture with critical data for operational planning and therefore must be considered in the Technical Architecture.

## 3.3 Data streams of the HONOR technical architecture

Given the background of the HONOR project, focus of the data stream overview is on data streams referring to the implementation of flexibility markets. In the overview process data, meter data, flexibility trading data, flexibility control data, historic data and maintenance data are considered. A large part of data streams in the presented HONOR technical architecture refers to maintenance of hardware and software components. To limit the size of the data stream overview data streams related to maintenance are exemplary described on the DSO. It is assumed that other actors will have similar maintenance data streams. The overview of data streams of the HONOR technical architecture is based on the extension of the data stream overview presented in [43] and can be found Table 3 in the Appendix.

## 4 CONCEPTUAL MODEL OF THE MONITORING REQUIREMENTS IN CYBER-PHYSICAL SYSTEMS – ON THE EXAMPLE OF A DSO

This Section is concerned with the presentation and contextualization of monitoring requirements of cyber-physical systems within the HONOR system architecture on the example of a DSO. For that purpose, a generic multi-domain security architecture model was developed. The developed security architecture consists of a system of monitoring requirements and interactions of underlying monitoring components and aims at defining an overall security system for holistic monitoring of cyber-physical systems. The security architecture is motivated by the cyber-physical security architecture approach of Ashibani et al. [2]. According to Ashibani et al. a security architecture for cyber-physical systems must consider cross-domain security measures in every layer of the system (see Section 4.1.1) as well as cooperation of individual security measures. However, Ashibani et al. define cyber-physical security solely as information and control security against cyber attacks. With the proposed generic multi-domain security architecture this approach is, on the one hand, extended beyond the boundaries of cyber security and, on the other hand, adapted to cyber-physical systems within the HONOR system architecture on the example of a DSO. For that purpose, the review of recent research topics for monitoring and event detection in cyber-physical power systems (Section 2) as well



as the identification of data streams, system components and networks of the HONOR system architecture in Section 3 was used as the basis. The fundamental concept of the proposed security architecture is the correlation of information from and about multiple domains as well as from multiple monitoring components according to Ashibani et al. [2]. By extending the traditional cyber security background of security architectures with monitoring of the physical domain and human factors the capability of detection and analysis of the cause of events as well as the monitoring of the state of the cyber-physical system are enhanced.

The long-term purpose of the developed security architecture model is twofold: in a first step the model is used to present and contextualize monitoring requirements of cyber-physical systems in a graphical manner. After defining the monitoring requirements, the model can be used to identify weakpoints in existing monitoring strategies and architectures of cyber-physical systems. Based on the identified weakpoints use cases for monitoring and event detection methods can be developed and formulated. Focus of this work is the presentation and contextualization of monitoring requirements on the example of the cyber-physical system of a DSO. Some derived use cases for monitoring and event detection methods are discussed in Section 4.3.

#### **4.1 Model structure and components**

##### **4.1.1 Cyber-physical system architecture**

To allow the application on various actors of the HONOR system architecture the generic security architecture is based on a typical architecture of cyber-physical systems [13,44–46]. Cyber-physical systems are based on the integration of computational systems, networking and physical processes. A common representation of such systems is depicted in Figure 4. The architecture of cyber-physical systems is typically divided into three main layers namely the application layer, network layer and physical layer. The physical layer consists of a physical infrastructure, which is the exogenous system under control as well as the sensors and actuators which enable measuring of the environment and delivering control actions. The network layer connects the application layer with the physical layer via data transmission in communication networks. Multiple and heterogenous communication networks can exist in one cyber-physical system. The communication networks are connected through gateways. The application layer is responsible for processing of the data which are collected in the physical layer and transmitted via the network layer as well as generating control commands. Functions for monitoring and remote control are implemented through specific software.

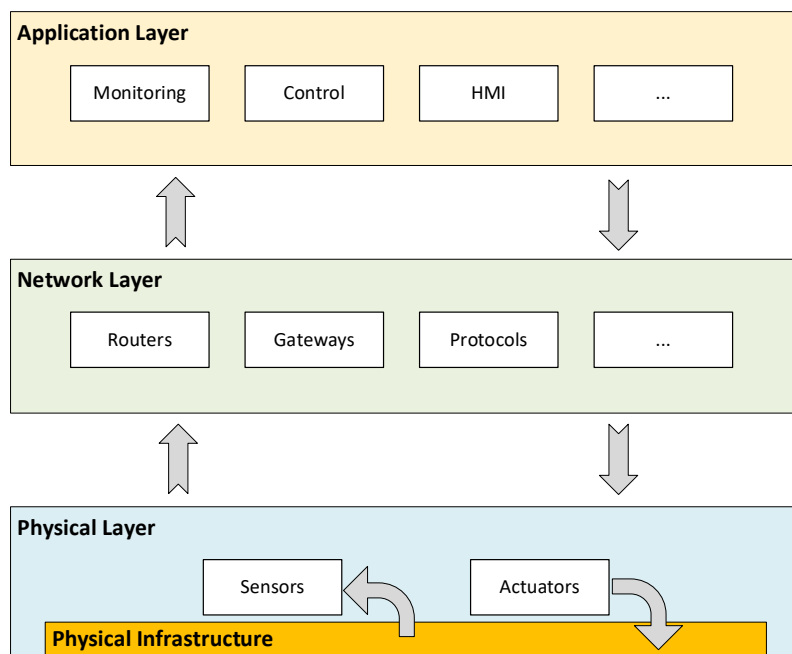
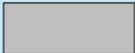




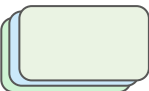





Figure 4 Architecture of a cyber-physical system.

#### 4.1.2 Component description

The developed generic multi-domain security architecture is based on various components that represent monitoring requirements, sub-systems, system components or data flows. In Table 2 an overview of the model components is given, including a short description of each component.

Table 2 Component description of the generic multi-domain security architecture model.

Component	Description
	Modeled actor of the HONOR Flexibility Market

	Security architecture zone
	Layers of the cyber-physical architecture
	Identified monitoring requirements
	System components or zones (e.g. database or substation)
	Data streams that are relevant for power system operation (e.g., control signals or measurements)
	Data streams that transmit the reports of individual monitoring components to the central and system-wide state and risk analysis component
	Data streams that are relevant for the various monitoring components
	Defines which domains (cyber, physical and/or human factors) are considered for the respective monitoring requirement

#### 4.1.3 Generic multi-domain security architecture model for holistic monitoring of cyber-physical systems

In Figure 5 the generic multi-domain security architecture model is depicted on the example of a DSO. As a foundation of the model the architecture of a cyber-physical systems (see Section 4.1.1) is used. For better differentiation of the monitoring requirements the application layer is further divided into a supervisory control layer and a decision support layer. The decision support layer comprises software-based automated functionalities for decision support to the human operator. The supervisory control layer represents the human interaction with the system from the control room. From the physical layer of Figure 4 only the sensors and actuators are considered in the model. To underline the focus on the sensors and actuators “perceptual execution layer” was chosen as the name of the associated layer. As in some countries the AMI is hosted by the DSOs, smart meters were considered as part of the perceptual execution layer. Please note, that in the HONOR technical architecture (Section 3) a separate Meter Data Company is considered. The communication of the DSO with other actors and entities constitutes a considerable share of the data flows of the cyber-physical system of the DSO. Moreover, the implementation of the HONOR system architecture would increase the number

communication paths to external actors such as Aggregators and Flexibility Market Operators. To emphasize the increasing communication and corresponding data flows, the interacting actors and entities are included into the security architecture model of the DSO.

The operation of the cyber-physical system of the DSO relies on a variety of system components (e.g. measurement devices, software and databases), human interaction with the system (e.g. field crew or operator) and process relevant data streams (e.g. measurements and control devices) which will further be summarized as the operational system. The physical and human components of the operational system are marked in blue. The data streams of the operational system are represented as red arrows. The proposed multi-domain security architecture represents the monitoring requirements and interaction of monitoring components for supervising the operational system of the DSO. The monitoring requirements are considered within the security architecture model as colored boxes. A categorization of the monitoring requirements is given by the color coding. Equal monitoring requirements are represented in the same color. A detailed description of the monitoring requirements follows in Section 4.2. The location of the monitoring requirements within the architecture is determined by the system component that the monitoring requirement is referring to. The location of the physical counterpart of a monitoring requirement is not defined within the presented security architecture. As an example, the requirement of smart meter data integrity checking is located in the perceptual execution layer, since smart meter belongs to the sensors of the cyber-physical system of the DSO. However, the software that conducts the data integrity check is not necessarily located on a smart meter. Data integrity checking could also be realized in a centralized approach, where various data streams are monitored at a central location in the cyber-physical system. The operational system of the DSO consists of components from various domains, namely a physical domain (e.g. workstations, transformers or remote terminal units), cyber domain (e.g. communication networks and software updates) and human factors (e.g. field crew activity and operator control action). Given the multi-domain nature of the cyber-physical system of the DSO, the monitoring requirements cover the concerned domains as well. The domains concerned by a specific monitoring requirement are indicated by the signs within the monitoring requirements (see also description in Table 2). The yellow arrows represent status reports of the monitoring components that fulfil the defined monitoring requirements. For the sake of legibility the monitoring reports are originating from the monitoring requirements. In this way additional representation of monitoring components could be avoided. The monitoring reports are collected from a central component for system-wide state and risk analysis. A detailed description of the multi-domain system-wide state and risk analysis can be found in Section 4.2.3.3.

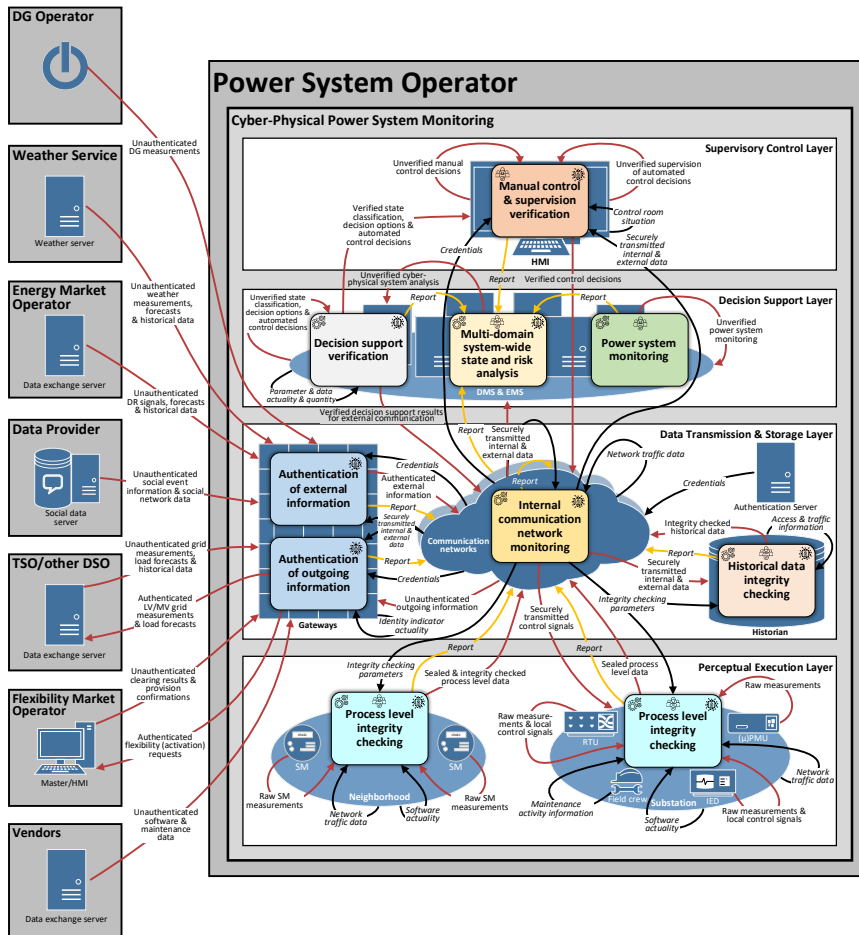


Figure 5 Generic multi-domain security architecture model on the example of a DSO.

## 4.2 Description of the monitoring requirements

### 4.2.1 Perceptual Execution Layer

#### 4.2.1.1 Process level integrity checking

Sensors and actuators may collect anomalous or even wrong measurements or execute wrong control commands, respectively, due to various reasons such as natural causes, human errors, device errors, and cyber attacks. Existing security monitoring in the perceptual execution layer comprises to some extent detection and flagging of anomalous data, that deviates from statistical normal behavior. However, in most cases resulting log files are manually investigated after transmission to the control center. Devices (e.g. RTUs) with a suspect behavior are disabled and their functionality is taken over by redundant devices. If a device error

Deliverable No. 6.1 | Conceptual model of data streams, detection and verification requirements

cannot be solved by rebooting the device, it will be replaced with a new one. Although this approach might be sufficient for the present situation of distribution grid monitoring and control, shortcomings exist with a view to recent developments in the smart grid era. 1) Increasing monitoring and control requirements in distribution grids will require more measurement devices e.g. in secondary substations. Although decreasing costs for measurement devices may allow a roll out of measurement devices in distribution grids, economic concerns will negatively impact measurement redundancy. Thus, it can not be assumed that data integrity checking in the process level can in principle be avoided by redundant measurements. 2) The increasing number and versatility of cyber threats questions redundancy as a probate mean. Attacks can be adapted to the regular operation and protection mechanisms to hide the attack behavior. Moreover, distributed and coordinated attacks might affect multiple devices simultaneously. 3) The increasing collection of data makes the already very time consuming and difficult task of manual evaluation of log files impracticable. A requirement for monitoring in the perceptual execution layer is therefore seen in the automated indication of erroneous behavior or lack of data integrity, including the identification of the error source. To account for the increasing variety of threats (especially from a cyber security perspective) and allow for fast and reliable identification of the error source, information from multiple domains should be correlated (see Sections 2.2.1 and 2.2.3).

#### 4.2.2 Data Transmission and Storage Layer

##### 4.2.2.1 Authentication of incoming and outgoing information

As monitoring, operation and control of future distribution grids will extensively rely on external information (e.g. state of neighboring power systems, flexibility offers or weather data), verification of external information is of crucial importance. Power system communication comes with some specific requirements: in power system communication networks reliability, security, and real-time message delivery have higher priorities than providing high throughput. Therefore, unlike to many other communication systems, for power systems timely authentication of up to a few seconds is required. At the same time power system communication is characterized by millions of interacting devices, which sets high requirements on the authentication performance. Moreover, connecting legacy but operation-critical systems, initially not designed for cyber security (e.g. SCADA), to new communication networks, such as internet, considerably increases security and privacy threats. In [47] key requirements for authentication in the smart grid environment are defined:

- Low execution and protocol delay
- Low computational and storage cost
- Low communication and computation overhead
- Resistance to attacks and failures
- Trust among SG entities

- Buffer management
- Confidentiality and privacy

Saxena et al. [47] have shown that existing solutions cannot meet all key objectives, which justifies the demand for further investigation on secure and efficient authentication protocols. For risk monitoring purposes (see Section 4.2.3.3), bi-directional authentication metadata such as the actuality of identity indicators and information about unauthorized access attempts should be monitored and integrated into the analysis.

#### 4.2.2.2 Internal communication network monitoring

As a central entity of the data transmission and storage layer communication networks connect the information sensing and control execution within the perceptual execution layer with the operation and control functions located at the higher layers. Critical data for real-time operation as well as sensitive data are transmitted through a variety of heterogeneous communication networks. A disruption of the data transmission might result from natural causes, device errors or cyber attacks and can provoke inadequate control actions that damage the power system. Beside the disruption of data transmission, cyber-attacks can observe, hide, create, or even change critical and sensitive data. Data transmission is protected by several security measures such as firewalls, authentication, and encryption [48]. However, these technologies cannot guarantee cyber security as e.g. insider attacks and connections from trusted sources are not detected by firewalls. To isolate the compromised sub-system and initiate adequate counteractions, intrusions or anomalous events, resulting from physical or cyber events need to be detected, located, and classified in real-time. This requires advanced intrusion detection methods as existing methods (e.g. network-based intrusion detection that uses network traffic data to detect intrusions) cannot cope with new emerging challenges for network monitoring. New security challenges arise from the data exchange between different heterogeneous networks, increasing dependency on public networks (e.g. internet), the integration of legacy and new communication networks, increasing network traffic [49], the variety of network access points, the strict availability requirements and hidden or insider attacks. As an example, existing methods may miss some malicious network behaviors such as replay attacks. Moreover, normal network delay as a result of high network traffic could be identified as a denial of service (DoS) attack [50].

#### 4.2.2.3 Historical data integrity checking

With the deployment of data-driven techniques for operation, monitoring and control of power systems, historical process data will play an increasingly important role [51]. Historical records of power system operation and events can be evaluated for the development of data-driven models for a variety of critical applications such as state estimation, fault detection and load forecasting. However, model development based on compromised data will misdirect the algorithm and thus result in wrong results. Historical data integrity checking thus will become an even more important requirement for secure power system operation in the future [51].

Today, historical data typically is not checked for integrity, after being stored. The integrity of historical data can be affected through human errors, transfer errors, compromised hardware, and attacks. Cloud storage and computing may expose power systems to further threats in the future.

### 4.2.3 Decision Support Layer

#### 4.2.3.1 Power system monitoring

Power system monitoring comprises existing functionalities such as topology identification, state estimation and fault detection. Especially for distribution grids for some of these functionalities there was no need in the past due to the uni-directional power flow and low dynamics. However, due to increasing integration of volatile and continuous controlled DERs also DSOs have to increase the observability of distribution grids. Challenges and requirements for power system monitoring of distribution grids such as event-triggered state estimation, cyber security of low-voltage state estimation and fault detection under increasing load uncertainty can be taken from Section 2.

#### 4.2.3.2 Decision support tools verification

Decision support applications for automated operation, monitoring and control may generate misleading results due reasons such as outdated model parameters and unknown system states, resulting from the fast transition of distribution grids (increased amount of DERs and topology changes) as well as cyber attacks. Cyber attacks on decision support tools include among others malicious code, buffer overflow and control command forgery attacks [2]. Misleading decision support can result in unobservability of the system as well as inadequate control actions that might lead to damage of the physical system components. The implementation of data-driven black-box applications will bring additional requirements and challenges for the verification of decision support tools. A major barrier for the application of complex machine learning methods, such as neural networks, in power systems is their low transparency [12]. While big data and an increasing model complexity allow for higher model accuracy, the interpretability generally decreases. However, in order to verify decision support applications, the process must be traceable for the operator. Recent works have shown that several machine learning models, despite their high prediction accuracy on unseen test data, can predict incorrect answers with high confidence due to small input perturbation what results in a non-robust performance [22]. Venzke et al. have developed a framework for verification of neural networks to obtain a provable performance guarantee for power system applications [52]. The proposed methods enable evaluating the robustness and improve interpretability of neural networks, which might set the foundation for regularly verification of data-driven decision support applications and their performance.

#### 4.2.3.3 Multi-domain system-wide state and risk analysis

Power systems are increasingly becoming distributed and complex systems for several reasons: Increasing dependency between cyber and physical domain;



distribution and automation of control functions (e.g. substation automation and demand response) and distribution of power generation due to installation of DERs. This increases not only the space to be monitored but also complicates monitoring and interpretation of the system state. Cyber attacks and other events might not be detectable and traceable by monitoring of individual system components and domains [2]. One example are distributed attacks which become increasingly common [53]. Thus, another monitoring requirement is seen in the aggregation and correlation of the monitoring results of individual monitoring components in a holistic system-wide state analysis. A system-wide state analysis should also include risk analysis. Additional to the state analysis ("what is currently happening?") risk analysis could provide an answer to the question "what is likely to happen?". A better understanding of what could happen would allow the DSO a better preparation to react fast and adequate on critical events. Current power system risk analysis methods are based on centralized computation and N-1 contingencies [54]. While these risks should still be taken into account, results from the power system state analysis should be associated with external information (e.g. weather data, availability of flexibility on the flexibility market and state of neighboring energy systems) to enable holistic power system risk analysis. In [55] a system-wide cyber-physical intrusion detection system was presented. The proposed intrusion detection system architecture consists of two main parts: 1) analysis of individual system components (DER, power system and cyber-security) and 2) a joint analysis of the cyber-physical system. In [56] the authors propose a framework for risk assessment for transmission system operation that extends the existing N-1 analysis by taken into account a variety of threats from multiple domains such as natural disasters, human errors, cyber attacks and device failures. With this approach the existing static risk analysis approach could be shifted towards a dynamic system-wide risk analysis which would improve the operators awareness of the system state.

#### 4.2.4 Supervisory Control Layer

##### 4.2.4.1 Manual control and supervision verification

Research efforts on the security of cyber-physical systems often focus solely on technological aspects of security and ignore the human contributions to risk and resilience. However, the human factor in many systems is seen as the greatest uncertainty and threat [1,53,57]. Although power system operation and control will become increasingly automated, human operator will not disappear from control rooms in the foreseeable future [58]. As humans by fault or on purpose can initiate or overlook malicious control actions verification of control actions is desirable [1]. Lin et al. [59] use contingency analysis to predict the consequences of control commands. Using set theory, they show it is possible to determine the set of safe states, the set of reachable states, and invariant sets. The risks in the supervisory control layer include unauthorized accessing, outdated passwords, presence of externals, social engineering, new or disgruntled employees as well as the out-of-the-loop syndrome. The verification of manual control and supervision includes authentication and authorization of the operator as well as verification of taken

control decisions. Control decisions that are not consistent with the decision support results should be identified. However, for highly automated power systems a general problem exists: manual decisions will mainly be necessary in extreme situations where decision support applications fail, e.g. due to lack of representative training data. In such situations, information for verification of control decision are also not available.

### 4.3 Conclusion and Perspectives

The systematic representation of monitoring requirements for the cyber-physical systems within the HONOR system architecture is based on the recent research topics for monitoring and event detection in cyber-physical systems (Section 2) and the overview of data streams in Section 3. Contrary to many other security architectures, in the presented multi-domain security architecture “security” is considered beyond the cyber system. In this way, the generic multi-domain security architecture provides an holistic and concise overview about monitoring requirements that need to be considered for cross-domain security of cyber-physical systems in the HONOR system architecture. By mapping the current research topics for monitoring and event detection in cyber-physical power systems on the multi-domain security architecture, promising research fields could be derived that provide potential use cases for the following work on the development of monitoring and event detection methods in the HONOR project:

One research topic is seen in multi-domain event detection in lower system levels, such as substation RTUs and flexibility assets or HEMS, respectively. Successful attacks on local controllers (e.g. Stuxnet [9]) have shown that centralized event detection approaches are not able to detect these kind of attacks what can result in devastating situations for power systems. In a similar way flexibility markets could be manipulated e.g. via fake flexibility offers, resulting from manipulated HEMS. The connection to public networks makes HEMS a comparatively easy target for attackers. Centrallized event detection applications at the Aggregator or flexibility market level would not able to detect such fake flexibility offers from individual flexibility assets. Besides cyber security concerns also physical events such as device failures or wrong control behavior of individual devices needs to be detected. The challenge for event detection on lower system levels is the limited computational and financial capabilities what complicates the implementation of sophisticated security software. A multi-domain detection scheme could overcome these barriers. By correlating physical and cyber information events could be detected without sophisticated monitoring of network data. Existing models of the physical behaviour of a flexibility asset (e.g. for flexibility asset control or flexibility prognosis) could be incorporated into event detection schemes to improve detection performance with minimal additional computational effort. By exploiting existing resources multi-

domain event detection could overcome the trade-off between computational effort and accuracy, facilitating lightweight event detection and classification in lower system levels. For secondary substation RTUs another approach is seen in physical event-triggered intrusion detection systems that make use of existing physical measurements to reduce the computational burden of intrusion detection systems. Only if physical measurements show anomalous behavior the local host would be extensively scanned for cyber threats.

In contrast to the distributed detection in lower system levels flexibility offers could be pre-qualified in a top-down approach by the Flexibility Market Operator by means of data fusion. Previous offers of the respective Aggregator could be correlated with exogenous data such as weather forecasts to prove trustworthiness of flexibility offers. In this way, fake flexibility offers, infiltrated by attackers that by-passed the authentication process of the flexibility market, could be detected. Integrated with an authentication or intrusion detection system a cyber-physical flexibility offer pre-qualification procedure could be developed.

Another unexplored topic is seen in the real-time detection of flexibility service activations in aggregated load data. Given a flexibility market design considering other market participants than DSOs (e.g. BRPs and TSOs) a DSO is not always aware of flexibility service activations in his distribution grid. Real-time detection of flexibility service activations would increase the observability of the distribution grid and thus improve the situational awareness of the DSO. For that purpose, information from historic load data could be combined with exogenous data such as solar irradiation and temperature.

Regardless of the specific application data-driven monitoring and event detection methods often suffer from bad explainability. As a consequence decision support verification was identified as one of the monitoring requirements in the cyber-physical system of a DSO (see Figure 5). An alternative to explainability that places no constraints on the complexity of the underlying algorithm is uncertainty. By providing information about the confidence of a prediction trust into the decision support tool can be achieved without taking the reasoning into account, facilitating the adoption of new data-driven techniques. For that reason, uncertainty quantification should be considered for development of monitoring and event detection methods within the HONOR project.

## FUNDING



This document was created as part of the ERA-Net Smart Energy Systems project XXXX, funded from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 646039 (SG+) / no. 775970 (RegSys).

## 5 REFERENCES

- [1] Humayed A, Lin J, Li F, Luo B. Cyber-Physical Systems Security—A Survey. *IEEE Internet Things J.* 2017;4(6):1802–31.
- [2] Ashibani Y, Mahmoud QH. Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security* 2017;68:81–97.
- [3] Greenberg J. Understanding Metadata and Metadata Schemes. *Cataloging & Classification Quarterly* 2005;40(3-4):17–36.
- [4] Kraft O, Pohl O, Rewald F. System Architecture: Deliverable 3.2 of the HONOR project; 2021.
- [5] Mo Y, Kim TH-J, Brancik K, Dickinson D, Lee H, Perrig A et al. Cyber-Physical Security of a Smart Grid Infrastructure. *Proc. IEEE* 2012;100(1):195–209.
- [6] Himeur Y, Alsalemi A, Bensaali F, Amira A. Anomaly detection of energy consumption in buildings: A review, current trends and new perspectives; 2020.
- [7] Hybrid Intrusion Detection System Design for Distributed Energy Resources.
- [8] Giraldo J, Urbina D, Cardenas A, Valente J, Faisal M, Ruths J et al. A Survey of Physics-Based Attack Detection in Cyber-Physical Systems. *ACM Comput. Surv.* 2018;51.
- [9] Farwell JP, Rohozinski R. Stuxnet and the Future of Cyber War. *Survival* 2011;53(1):23–40.
- [10] Liu, Y., Ning, P., & Reiter, M. K. (ed.). False Data Injection Attacks against State Estimation in Electric Power Grids; 2011.
- [11] Tan S, Guerrero JM, Xie P, Han R, Vasquez JC. Brief Survey on Attack Detection Methods for Cyber-Physical Systems. *IEEE Systems Journal* 2020;14(4):5329–39.
- [12] Luo Y, Xiao Y, Cheng L, Peng G, Yao DD. Deep Learning-Based Anomaly Detection in Cyber-Physical Systems: Progress and Opportunities; 2020.
- [13] Han S, Xie M, Chen H-H, Ling Y. Intrusion Detection in Cyber-Physical Systems: Techniques and Challenges. *IEEE Systems Journal* 2014;8(4):1052–62.
- [14] Musleh AS, Chen G, Dong ZY. A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids. *IEEE Trans. Smart Grid* 2020;11(3):2218–34.
- [15] Aoufi S, Derhab A, Guerroumi M. Survey of false data injection in smart power grid: Attacks, countermeasures and challenges. *Journal of Information Security and Applications* 2020;54:102518.
- [16] Wang Y, Chen Q, Hong T, Kang C. Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges. *IEEE Trans. Smart Grid* 2019;10(3):3125–48.

- [17] Kumar R, Saxena D. A Literature Review on Methodologies of Fault Location in the Distribution System with Distributed Generation. *Energy Technol.* 2020;8(3):1901093.
- [18] Gunduz MZ, Das R. Cyber-security on smart grid: Threats and potential solutions. *Computer Networks* 2020;169:107094.
- [19] Cao L, Jiang X, Zhao Y, Wang S, You D, Xu X. A Survey of Network Attacks on Cyber-Physical Systems. *IEEE Access* 2020;8:44219–27.
- [20] Cui L, Qu Y, Gao L, Xie G, Yu S. Detecting false data attacks using machine learning techniques in smart grid: A survey. *Journal of Network and Computer Applications* 2020;170:102808.
- [21] Yize Chen, Yushi Tan, Deepjyoti Deka. *Is Machine Learning in Power Systems Vulnerable?* Piscataway, NJ: IEEE; 2018.
- [22] Goodfellow IJ, Shlens J, Szegedy C. Explaining and Harnessing Adversarial Examples; 2014.
- [23] Koziel S, Hilber P, Ichise R. A review of data-driven and probabilistic algorithms for detection purposes in local power systems. In: 2020 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS): IEEE; 2020 - 2020, p. 1–6.
- [24] Shafiullah M, Abido MA. A Review on Distribution Grid Fault Location Techniques. *Electric Power Components and Systems* 2017;45(8):807–24.
- [25] Ahmad F, Rasool A, Ozsoy E, Sekar R, Sabanovic A, Elitaş M. Distribution system state estimation-A step towards smart grid. *Renewable and Sustainable Energy Reviews* 2018;81:2659–71.
- [26] Huang Y-F, Werner S, Huang J, Kashyap N, Gupta V. State Estimation in Electric Power Grids: Meeting New Challenges Presented by the Requirements of the Future Grid. *IEEE Signal Process. Mag.* 2012;29(5):33–43.
- [27] Gholami M, Abbaspour A, Moeini-Aghaie M, Fotuhi-Firuzabad M, Lehtonen M. Detecting the Location of Short-Circuit Faults in Active Distribution Network Using PMU-Based State Estimation. *IEEE Trans. Smart Grid* 2020;11(2):1396–406.
- [28] Dehghanpour K, Wang Z, Wang J, Yuan Y, Bu F. A Survey on State Estimation Techniques and Challenges in Smart Distribution Systems. *IEEE Trans. Smart Grid* 2019;10(2):2312–22.
- [29] Primadianto A, Lu C-N. A Review on Distribution System State Estimation. *IEEE Trans. Power Syst.* 2017;32(5):3875–83.
- [30] Saldaña-González AE, Sumper A, Aragüés-Peñalba M, Smolnikar M. Advanced Distribution Measurement Technologies and Data Applications for Smart Grids: A Review. *Energies* 2020;13(14):3730.
- [31] Hayes B, Prodanovic M. State Estimation Techniques for Electric Power Distribution Systems. In: 2014 European Modelling Symposium: IEEE; 2014 - 2014, p. 303–308.
- [32] Prasad, S., Kumar. *Distribution System State Estimation: A Bibliographical Survey.* Piscataway, NJ, USA: IEEE; 2017.
- [33] Chen J, Dong Y, Zhang H. Distribution system state estimation: A survey of some relevant work. In: 2016 35th Chinese Control Conference (CCC): IEEE; 2016 - 2016, p. 9985–9989.
- [34] Tu C, He X, Shuai Z, Jiang F. Big data issues in smart grid – A review. *Renewable and Sustainable Energy Reviews* 2017;79:1099–107.

- [35] Labrador Rivas AE, Abrão T. Faults in smart grid systems: Monitoring, detection and classification. *Electric Power Systems Research* 2020;189:106602.
- [36] Zhang D, Wang Q-G, Feng G, Shi Y, Vasilakos AV. A survey on attack detection, estimation and control of industrial cyber-physical systems. *ISA transactions* 2021.
- [37] Phan SK, Chen C. Big Data and Monitoring the Grid. In: *The Power Grid*: Elsevier; 2017, p. 253–285.
- [38] Tong Z, Jianchang L, Lanxiang S, Haibin Y. Fault Analysis and Fault Diagnosis Method Review on Active Distribution Network. In: Xhafa F, Patnaik S, Zomaya AY, editors. *Advances in intelligent systems and interactive applications: Proceedings of the 2nd International Conference on Intelligent and Interactive Systems and Applications (IISA 2017)*. Cham, Switzerland: Springer; 2018, p. 628–633.
- [39] Zhu L, Laptev N. Deep and Confident Prediction for Time Series at Uber 2017:103–10.
- [40] Zufferey T, Renggli S, Hug G. Probabilistic State Forecasting and Optimal Voltage Control in Distribution Grids under Uncertainty. *Electric Power Systems Research* 2020;188:106562.
- [41] Vernotte A, Vålja M, Korman M, Björkman G, Ekstedt M, Lagerström R. Load balancing of renewable energy: a cyber security analysis. *Energy Inform* 2018;1(1).
- [42] Bondy, D. E. M., Heussen, K., Gehrke, O., & Thavlov, A. (ed.). *A Functional Reference Architecture for Aggregators*; 2015.
- [43] Vernotte A, Vålja M, Fransen F, Ekstedt M, Björkman G. SEGRID detailed reference model use case 2 scenario 2.
- [44] Lu T, Lin J, Zhao L, Li Y, Peng Y. A Security Architecture in Cyber-Physical Systems: Security Theories, Analysis, Simulation and Application Fields. *IJSIA* 2015;9(7):1–16.
- [45] ZHANG L, WANG Q, TIAN B. Security threats and measures for the cyber-physical systems. *The Journal of China Universities of Posts and Telecommunications* 2013;20:25–9.
- [46] Januario F, Cardoso A, Gil P. A Distributed Multi-Agent Framework for Resilience Enhancement in Cyber-Physical Systems. *IEEE Access* 2019;7:31342–57.
- [47] Saxena N, Choi B. State of the Art Authentication, Access Control, and Secure Integration in Smart Grid. *Energies* 2015;8(10):11883–915.
- [48] Xie J, Stefanov A, Liu C-C. Physical and cyber security in a smart grid environment. *WIREs Energy Environ* 2016;5(5):519–42.
- [49] Suaboot J, Fahad A, Tari Z, Grundy J, Mahmood AN, Almalawi A et al. A Taxonomy of Supervised Learning for IDSs in SCADA Environments. *ACM Comput. Surv.* 2020;53(2):1–37.
- [50] Liu J, Zhang W, Ma T, Tang Z, Xie Y, Gui W et al. Toward security monitoring of industrial Cyber-Physical systems via hierarchically distributed intrusion detection. *Expert Systems with Applications* 2020;158:113578.
- [51] Tan S, De D, Song W-Z, Yang J, Das SK. Survey of Security Advances in Smart Grid: A Data Driven Approach. *IEEE Commun. Surv. Tutorials* 2017;19(1):397–422.
- [52] Venzke A, Chatzivasileiadis S. Verification of Neural Network Behaviour: Formal Guarantees for Power System Applications. *IEEE Trans. Smart Grid* 2020:1.
- [53] Ahram T. *Advances in Artificial Intelligence, Software and Systems Engineering*. Cham: Springer International Publishing; 2021.

- [54] Rasmussen TB, Yang G, Nielsen AH, Dong Z. A review of cyber-physical energy system security assessment. In: 2017 IEEE Manchester PowerTech: IEEE; 2017 - 2017, p. 1–6.
- [55] Kosek AM, Gehrke O. Ensemble regression model-based anomaly detection for cyber-physical intrusion detection in smart grids. In: 2016 IEEE Electrical Power and Energy Conference (EPEC): 12-14 Oct. 2016. [Piscataway, New Jersey]: IEEE; 2016?, p. 1–7.
- [56] Perkin S, Bjornsson G, Baldursdottir I, Palsson M, Kristjansson R, Stefansson H et al. Framework for Threat Based Failure Rates in Transmission System Operation. In: Frenkel IB, Lisnianski A, SMRLO, editors. Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management - SMRLO 2016: 15-18 February 2016, Beer Sheva, Israel proceedings. Piscataway, NJ: IEEE; 2016, p. 150–158.
- [57] Ding D, Han Q-L, Xiang Y, Ge X, Zhang X-M. A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing 2018;275:1674–83.
- [58] Prostejovsky AM, Brosinsky C, Heussen K, Westermann D, Kreusel J, Marinelli M. The future role of human operators in highly automated electric power systems. Electric Power Systems Research 2019;175:105883.
- [59] Lin H, Slagell A, Kalbarczyk Z, Sauer PW, Iyer RK. Semantic security analysis of SCADA networks to detect malicious control commands in power grids. In: Defend B, editor. Proceedings of the first ACM workshop on Smart energy grid security. New York, NY: ACM; 2013, p. 29–34.

## 6 APPENDIX

Table 3 Overview of data streams within the HONOR system architecture.

#	Name	From	To
<b>DSO</b>			
1	Primary substation measurements	IEDs	Primary RTU
2	Primary substation control signals	Primary RTUs	IEDs
3	Primary substation process data (bidirectional)	Primary RTUs	SCADA Front End
4	Primary RTU&IED maintenance data	DSO Element Manager	Primary RTUs

5	Remote primary substation login	Office Station	Primary substation workstation
6	Secondary substation measurements	IED	Primary RTU
7	Secondary substation control signals	Secondary RTU	IED
8	Secondary substation process data (bidirectional)	Secondary RTU	SCADA Front End
9	Secondary RTU&IED maintenance data	DSO Element Manager	Secondary RTUs
10	Remote secondary substation login	Office Station	Secondary substation workstation
11	DERs process data (bidirectional) (measurements and emergency control commands)	DER RTUs	SCADA Front End
12	Primary substation, secondary substation and DER process data	SCADA Front End	SCADA Server
13	Process data (commands and set points) to primary substation, secondary substation and DER	SCADA Server	SCADA Front End
14	Primary substation, secondary substation and DER process data	SCADA Server	HMI
15	Process data (commands and setpoints)	HMI	SCADA Server
16	Primary substation, secondary substation and DER process data	SCADA Server	Replicated SCADA Server
17	Primary substation, secondary substation and DER process data	Replicated SCADA Server	Replicated HMI



18	Time synchronization data	SCADA Time Server	SCADA Server
19	Time synchronization data	SCADA Time Server	SCADA Front End
20	Time synchronization data	SCADA Front End	Primary RTUs
21	Time synchronization data	SCADA Front End	Secondary RTUs
22	Time synchronization data	SCADA Front End	DER RTU
23	Load forecast data	TSO	DSO File Transfer Server (DMZ)
24	Load forecast data	DSO File Transfer Server (DMZ)	SCADA Server
25	Historic Data	SCADA Server	Historian
26	Historic Data	Historian	HMI
27	External service data (e.g. weather forecasts)	Service Provider	DSO File Transfer Server (DMZ)
28	External service data	DSO File Transfer Server (DMZ)	SCADA Server
29	External service data	SCADA Server	DMS
30	External service data	SCADA Server	HMI
31	Historic external service data	SCADA Server	Historian

32	Smart Meter Data	Data Hub	DSO File Transfer Server (DMZ)
33	Smart Meter Data	DSO File Transfer Server (DMZ)	SCADA Server
34	Historic Smart Meter Data	SCADA Server	Historian
35	Historic Data	Historian	Replicated Historian
36	Process data	SCADA Server	DMS
37	Process Data	Replicated SCADA Server	Forecasting Server
38	Historic Data	Historian	DMS
39	Replicated Historic Data	Replicated Historian	Forecasting Server
40	External service data	DSO File Transfer Server (DMZ)	Forecasting server
41	(Near) real-time flexibility demand	DMS	DSO File Transfer Server (DMZ)
42	Flexibility demand forecast	Forecasting Server	DSO File Transfer Server (DMZ)
43	Flexibility Request	DSO File Transfer Server (DMZ)	Flexibility Market Data Acquisition Server
44	Flexibility Market clearing results	Flexibility Market Data Acquisition Server	DSO File Transfer Server (DMZ)
45	Flexibility portfolio activation request	DSO File Transfer Server (DMZ)	Aggregator Data Acquisition Server

46	Flexibility portfolio activation confirmation	Aggregator Data Acquisition Server	DSO File Transfer Server (DMZ)
47	Large Flexibility Asset activation request	DSO File Transfer Server (DMZ)	Flexibility Asset Data Acquisition Server
48	Large Flexibility Asset activation confirmation	Aggregator Data Acquisition Server	DSO File Transfer Server (DMZ)
49	Large Flexibility Asset emergency control command	SCADA Server	DSO File Transfer Server (DMZ)
50	Large Flexibility Asset emergency control command	DSO File Transfer Server (DMZ)	Flexibility Asset Data Acquisition Server
51	Settlement	Flexibility Market Data Acquisition Server	DSO File Transfer Server (DMZ)
52	SCADA Maintenance data	DE HMI	Data Engineering
53	SCADA Maintenance data	Data Engineering	SCADA Server
54	RTU&IED Software	Vendor Server	DSO File Transfer Server (DMZ)
55	SCADA Software	Vendor Server	DSO File Transfer Server (DMZ)
56	RTU&IED Software	DSO File Transfer Server (DMZ)	DSO Update server
57	RTU&IED Software	DSO Update server	Primary RTU
58	RTU&IED Software	DSO Update server	Secondary RTU
59	SCADA Software	DSO File Transfer Server (DMZ)	SCADA Server

60	Primary RTU&IED Maintenance data	Primary Substation workstation	Primary RTUs
61	Secondary RTU&IED Maintenance data	Secondary Substation mobile workstation	Secondary RTUs
62	Primary RTU&IED Software data	Primary Substation workstation	Primary RTUs
63	Secondary RTU&IED Software data	Secondary Substation mobile workstation	Secondary RTUs
64	SCADA Front End Maintenance Data	SCADA Server	SCADA Front End
65	Historic Data	Replicated Historian	Office station
66	Primary substation, secondary substation and DER process data	Replicated SCADA HMI	Office station
67	Process Data (commands)	Office station	Replicated SCADA HMI
68	Internet Data	Office station	Public Internet
<b>Flexibility Market Operator</b>			
69	Flexibility Request	BRP Data acquisition server	Flexibility Market Operator Data acquisition server
70	Flexibility Offer	Aggregator Data Acquisition Server	Flexibility Market Operator Data acquisition server
71	Flexibility Request	Flexibility Market Operator Data acquisition server	Flexibility matching system
72	Flexibility Offer	Flexibility Market Operator Data acquisition server	Flexibility matching system

73	Flexibility Request	Flexibility Market Operator Data acquisition server	Flexibility Market Operator HMI
74	Flexibility Offer	Flexibility Market Operator Data acquisition server	Flexibility Market Operator HMI
75	Flexibility Request	Flexibility Market Operator Data acquisition server	Flexibility Market Operator Internal Database
76	Flexibility Offer	Flexibility Market Operator Data acquisition server	Flexibility Market Operator Internal Database
77	Flexibility Market clearing results	Flexibility matching system	Flexibility Market Operator HMI
78	Flexibility Market clearing results	Flexibility matching system	Flexibility Market Operator Internal Database
79	Flexibility Market clearing results	Flexibility matching system	Flexibility Market Operator Data acquisition server
80	Flexibility Market clearing results	Flexibility Market Operator Data acquisition server	BRP Data acquisition server
<b>Aggregator</b>			
81	External service data (e.g. weather forecasts)	Service Provider	Aggregator Data Acquisition Server
82	Flexibility Request	Flexibility Market Data Acquisition server	Aggregator Data Acquisition Server
83	Flexibility Request	Aggregator Data Acquisition Server	Flexibility aggregation module
84	Small Flexibility Asset availability status request	Flexibility aggregation module	Aggregator Data Acquisition Server
85	Small Flexibility Asset availability status request	Aggregator Data Acquisition Server	Small Flexibility Asset Owner FlexCom Agent

86	Small Flexibility Asset availability status	Small Flexibility Asset Owner FlexCom Agent	Aggregator Data Acquisition Server
87	Small Flexibility forecast data request	Flexibility aggregation module	Aggregator Data Acquisition Server
88	Small Flexibility forecast data request	Aggregator Data Acquisition Server	Small Flexibility Asset Owner FlexCom Agent
89	Small Flexibility forecast data	Small Flexibility Asset Owner FlexCom Agent	Aggregator Data Acquisition Server
90	Small Flexibility Asset measurement data request	Flexibility aggregation module	Aggregator Data Acquisition Server
91	Small Flexibility Asset measurement data request	Aggregator Data Acquisition Server	Small Flexibility Asset Owner FlexCom Agent
92	Small Flexibility Asset measurement	Small Flexibility Asset Owner FlexCom Agent	Aggregator Data Acquisition Server
93	Small Flexibility Asset measurement	Aggregator Data Acquisition Server	Forecasting engine
94	Flexibility Forecast Data	Forecasting engine	Flexibility aggregation module
95	Small Flexibility forecast data	Aggregator Data Acquisition Server	Flexibility aggregation module
96	Flexibility activation schedules	Flexibility aggregation module	Aggregator Data Acquisition Server
97	Flexibility activation schedules	Aggregator Data Acquisition Server	Small Flexibility Asset Owner FlexCom Agent
98	Flexibility activation schedules	Flexibility aggregation module	Flexibility Execution & Monitoring module
99	Small Flexibility Asset control commands and setpoints	Flexibility Execution & Monitoring module	Aggregator Data Acquisition Server

100	Small Flexibility Asset control commands and setpoints	Aggregator Data Acquisition Server	Small Flexibility Asset Owner FlexCom Agent
101	Small Flexibility Asset activation confirmation	Small Flexibility Asset Owner FlexCom Agent	Aggregator Data Acquisition Server
102	Small Flexibility Asset activation confirmation	Aggregator Data Acquisition Server	Flexibility Execution & Monitoring module
103	Small Flexibility Asset activation confirmation	Aggregator Data Acquisition Server	Aggregator HMI
104	Small Flexibility Asset activation confirmation	Aggregator Data Acquisition Server	Aggregator Internal Database
105	Portfolio activation confirmation	Flexibility Execution & Monitoring module	Aggregator Data Acquisition Server
106	Portfolio activation confirmation	Aggregator Data Acquisition Server	Flexibility Market Data Acquisition server
107	Portfolio activation confirmation	Aggregator Data Acquisition Server	DSO File Transfer Server (DMZ)
108	Small Flexibility Asset measurement	Aggregator Data Acquisition Server	Flexibility Execution & Monitoring module
109	Small Flexibility Asset measurement	Aggregator Data Acquisition Server	Aggregator Internal Database
110	Small Flexibility Asset control commands and setpoints	Flexibility Execution & Monitoring module	Aggregator Internal Database
111	Flexibility activation schedules	Flexibility aggregation module	Aggregator Internal Database
112	Portfolio monitoring data	Flexibility Execution & Monitoring module	Aggregator HMI
113	Flexibility Offer	Flexibility aggregation module	Aggregator Data Acquisition Server

114	Flexibility Offer	Flexibility aggregation module	Aggregator HMI
115	Flexibility Offer	Flexibility aggregation module	Aggregator Internal Database
116	Flexibility Market Clearing Results	Flexibility Market Data Acquisition server	Aggregator Data Acquisition Server
117	Flexibility Market Clearing Results	Aggregator Data Acquisition Server	Aggregator HMI
118	Flexibility Market Clearing Results	Aggregator Data Acquisition Server	Aggregator Internal Database
119	Settlement	Flexibility Market Data Acquisition server	Aggregator Data Acquisition Server
120	Settlement	Aggregator Data Acquisition Server	Aggregator HMI
121	Settlement	Aggregator Data Acquisition Server	Aggregator Internal Database
<b>Small Flexibility Asset Owner</b>			
122	External service data (e.g. weather forecasts)	Service Provider	Small Flexibility Asset Owner FlexCom Agent
123	External service data (e.g. weather forecasts)	Small Flexibility Asset Owner FlexCom Agent	
124	Small Flexibility Asset availability status request	Small Flexibility Asset Owner FlexCom Agent	Home energy management system
125	Individual Small Flexibility forecast data request	Small Flexibility Asset Owner FlexCom Agent	Home energy management system
126	Asset measurement data request	Small Flexibility Asset Owner FlexCom Agent	Home energy management system



127	Small Flexibility Asset availability status	Home energy management system	Small Flexibility Asset Owner FlexCom Agent
128	Individual Small Flexibility forecast data	Home energy management system	Small Flexibility Asset Owner FlexCom Agent
129	Asset measurement data	Home energy management system	Small Flexibility Asset Owner FlexCom Agent
130	Flexibility activation schedules	Small Flexibility Asset Owner FlexCom Agent	Home energy management system
131	Small Flexibility Asset control commands and setpoints	Small Flexibility Asset Owner FlexCom Agent	Home energy management system
132	Small Flexibility Asset activation confirmation	Home energy management system	Small Flexibility Asset Owner FlexCom Agent
<b>Large Flexibility Asset Owner</b>			
133	External service data (e.g. weather forecasts)	Service Provider	Large Flexibility Asset Owner Data acquisition server
134	External service data (e.g. weather forecasts)	Large Flexibility Asset Owner Data acquisition server	Large Flexibility Asset Owner SCADA Server
135	External service data (e.g. weather forecasts)	Large Flexibility Asset Owner SCADA Server	Flexibility Asset Management System
136	External service data (e.g. weather forecasts)	Large Flexibility Asset Owner SCADA Server	Large Flexibility Asset Owner Historian
137	Flexibility Request	Flexibility Market Data Acquisition server	Large Flexibility Asset Owner Data acquisition server
138	Flexibility Request	Large Flexibility Asset Owner Data acquisition server	Large Flexibility Asset Owner SCADA Server
139	Flexibility Request	Large Flexibility Asset Owner SCADA Server	Flexibility Asset Management System

140	Historic Data	Large Flexibility Asset Owner Historian	Flexibility Asset Management System
141	Flexibility offer	Flexibility Asset Management System	Large Flexibility Asset Owner SCADA Server
142	Flexibility offer	Large Flexibility Asset Owner SCADA Server	Large Flexibility Asset Owner HMI
143	Flexibility offer	Large Flexibility Asset Owner SCADA Server	Large Flexibility Asset Owner Historian
144	Flexibility offer	Large Flexibility Asset Owner SCADA Server	Large Flexibility Asset Owner Data acquisition server
145	Flexibility offer	Large Flexibility Asset Owner Data acquisition server	Flexibility Market Data Acquisition server
146	Flexibility clearing results	Flexibility Market Data Acquisition server	Large Flexibility Asset Owner Data acquisition server
147	Flexibility clearing results	Large Flexibility Asset Owner Data acquisition server	Large Flexibility Asset Owner SCADA Server
148	Flexibility clearing results	Large Flexibility Asset Owner SCADA Server	Flexibility Asset Management System
149	Flexibility clearing results	Large Flexibility Asset Owner SCADA Server	Large Flexibility Asset Owner HMI
150	Flexibility clearing results	Large Flexibility Asset Owner SCADA Server	Large Flexibility Asset Owner Historian
151	Flexibility activation request	Large Flexibility Asset Owner Data acquisition server	Large Flexibility Asset Owner SCADA Server
152	Flexibility activation request	Large Flexibility Asset Owner SCADA Server	Flexibility Asset Management System
153	Process Data (commands and setpoints for flexibility activation)	Flexibility Asset Management System	Large Flexibility Asset Owner SCADA Server

154	Process Data (commands and setpoints for flexibility activation)	Large Flexibility Asset Owner SCADA Server	Large Flexibility Asset Owner Front End
155	Process Data (commands and setpoints for flexibility activation)	Large Flexibility Asset Owner Front End	Large Flexibility Asset Owner Primary RTU
156	Process Data (commands and setpoints for flexibility activation)	Large Flexibility Asset Owner Primary RTU	Large Flexibility Asset Owner IEDs
157	Process Data (measurements)	Large Flexibility Asset Owner IEDs	Large Flexibility Asset Owner Primary RTU
158	Process Data (measurements)	Large Flexibility Asset Owner Primary RTU	Large Flexibility Asset Owner Front End
159	Process Data (measurements)	Large Flexibility Asset Owner Front End	Large Flexibility Asset Owner SCADA Server
160	Process Data (measurements)	Large Flexibility Asset Owner SCADA Server	Large Flexibility Asset Owner HMI
161	Process Data (measurements)	Large Flexibility Asset Owner SCADA Server	Large Flexibility Asset Owner Historian
162	Process Data (measurements)	Large Flexibility Asset Owner SCADA Server	Flexibility Asset Management System
163	Flexibility activation confirmation	Large Flexibility Asset Owner SCADA Server	Large Flexibility Asset Owner Data acquisition server
164	Flexibility activation confirmation	Large Flexibility Asset Owner Data acquisition server	DSO File Transfer Server (DMZ)
165	Settlement	Large Flexibility Asset Owner Data acquisition server	Large Flexibility Asset Owner SCADA Server
<b>Energy Supplier</b>			
166	Process Data (measurements and emergency control) (bidirectional)	DER RTU	DER IEDs
<b>Meter Data Company</b>			

167	Private House Meter Data	Smart Meter	Meter Data Concentrator
168	Concentrated Private Houses Meter Data	Meter Data Concentrator	AMI Private Houses
169	DER kWh Meter Data	DER kWh Meter	Meter Data Concentrator
170	Large Flexibility Asset kWh Meter Data	Large Flexibility Asset kWh Meter	Meter Data Concentrator
171	Concentrated DER/Large Flexibility Asset Meter Data	Meter Data Concentrator	AMI Industrial Customers
172	Private House Meter Data	AMI Private Houses	AMI HMI
173	Private House Meter Data	AMI Private Houses	Data Hub
174	Large Flexibility Asset kWh Meter Data	AMI Industrial Customers	Data Hub
175	Smart Meter Data	Data Hub	DSO File Transfer Server (DMZ)