# A Fog Based Approach for Hazards Differentiation in an IIoT Scenario

Azin Moradbeikie
Faculty of Computer Engineering
University of Isfahan
Isfahan, Iran
e-mail: azin.Moradbeikie@eng.ui.ac.ir

Kamal Jamshidi
Faculty of Computer Engineering
University of Isfahan
Isfahan, Iran
e-mail: jamshidi@eng.ui.ac.ir

Ali Bohlooli
Faculty of Computer Engineering
University of Isfahan
Isfahan, Iran
e-mail: bohlooli@eng.ui.ac.ir

Jordi Garcia
Advanced Network Architectures Lab (CRAAX)
UPC BarcelonaTech
Vilanova, Spain
e-mail: jordig@ac.upc.edu

Xavi Masip-Bruin
Advanced Network Architectures Lab (CRAAX)
UPC BarcelonaTech
Vilanova, Spain
e-mail: xmasip@ac.upc.edu

***Abstract*—Industrial control systems (ICS) are applied in many critical infrastructures. Reducing reconfiguration time after hazard leads to safety improvement, so it is one of the most important objectives in these systems. Hazards can be due to the "system failure" or "cyber-attacks" factors. One of the procedures that can reduce the reconfiguration time is determining as soon as possible the cause of hazards based on the above mentioned factors. Differentiation of attack from failure without redundant data in addition to data from the system sensors is not possible. With advent of the IoT as IIoT, a condition is developed to provide the required redundant data; however, by increasing the number of IIoT devices within a factory, the generated data volume becomes too large. In this paper we describe a fog-based approach applied in a factory to deal with such increasing complexity. We compare the proposed method with a traditional cloud-based solution. According to the results, the proposed method leads to a reduction of 60% lost time in the recovery reconfiguration step of the system.**

***Keywords-Industrial control systems (ICS); industrial internet of things (IIOT); fog computing; fault and attack detection***

## I. INTRODUCTION

Industrial Control Systems (ICS), which are usually applied in critical infrastructures, are often categorized as safety critical systems. Failures of these systems can lead to human harm and damage to property and the environment, so their security and safe operations are very important [1]. Providing safety and security in ICS stipulates the need for effective and efficient management of hazards in the system. A hazard management system in ICS is composed of hazard detection, hazard analysis, and system reconfiguration. In the physical infrastructure, organized from sensors and actuators, ICS is susceptible to cyber-attacks and physical destruction [2],[3].

A hazard in the sensor can be caused by attack or failure. In these cases, a physical real value is manipulated by the attacker or generated in the faulty sensor and sent to the controller. So a hazard (either fault or attack) is always reflected in the form of change in the received information. In most scenarios, the functionality of the system in presence of a failure or an attack is similar. Consequently, it is difficult to differentiate between these two issues [4], while it is essential for the analysis component and adoption of appropriate actions in the reconfiguration component, because different kind of attacks and failures can have different propagation level and occurrence probability [5]. This differentiation is necessary to select the appropriate action in the reconfiguration components. Although in many cases when the system is object to attacks or failures the functionality is similar, tacking appropriate measures in dealing with each of these two cases can be different. On this basis, lack of proper identification of the cause of the hazards leads to wrong estimation of the likelihood of occurrence and the level of propagation in the system, thus taking wrong control commands in the reconfiguration components. This wrong control commands can lead to hazard recurrence in the system or, in many cases, transferring the system into a more critical situation. This phenomenon will increase the system reconfiguration time and eventually the cost to recover from the hazard. Due to strict real-time limitations in

ICS, reducing recovery time is essential in order to reduce serious system safety harms in critical infrastructure, becoming a vital measure.

Differentiation of attack from failure is not possible without redundant data, in addition to the data from the system sensor. With the advent of the Internet of Things (IoT) in the ICS context, known as the Industrial Internet of Things (IIoT), a condition is developed to provide the required redundant data which allows the application of ad-hoc sensor data fusion, thus reducing the dependency on sensors. This makes it possible to identify the hazards in the system and differentiate them based on attack and failures.

Emerging of IoT technologies for the ICS in industry has played an important role in the next-generation industry. In IoT, anything that has a chip in it can be used for data collection. IoT offers a smart factory environment where all the objects around us are connected to the internet and communicate with each other. Therefore, IoT can be used to gather broader and more accurate information about our surroundings [6]. So enormous number of IoT devices spread in factories can be utilized for different monitoring applications.

By increasing the numbers of IoT devices within a factory, several challenges arise [7]. The volume of the generated data will be too large to be stored in a dataset for further processing, so the amount of data being generated by IoT devices and collected could easily saturate network and storage infrastructures [8]. Industry moves to assume cloud computing as a platform to solve these problems. Cloud computing provides a mechanism for storing, computing and processing data at reasonable costs. However, the centralized nature of the cloud introduces significant limitations due to communication bandwidths and latency. Limited latency and real time computing are critical in ICS.

To eliminating latency and communication bandwidths, there is a shift in the computing landscape towards distributed computing [9]. Fog computing [10] emerges as a computing paradigm to mitigate the need for transferring and processing data in the cloud [10]; instead, data are collected and processed much closer to its source, taking advantage of features such as locality and cost-efficiency. The fog layer is composed of geo distributed fog servers which are deployed at the edge of architecture. This acts as an intermediate layer between IoT devices and the cloud, so the fog server communicates directly with the IoT devices and, on the other hand, the fog servers later communicate with the cloud. As a result, fog can provide the real-time and low latency interaction with IoT devices, and its communication with cloud can prepare the integration of data that require the interplay and cooperation between the other fog servers and the cloud.

According to the above, a risk management system should differentiate hazards after detection based on attack and failure and in reconfiguration component, adopting the most appropriate manner that should be run in according. Providing required redundant information to do this, based on IoT spread out, has become possible. Due to the real-time processing requirements and favoring a cost-efficiency strategy, in this paper a fog-cloud combination architecture is proposed.

The remainder of this paper is organized as follows. The literate review is presented in Section 2. Section 3 describes a traditional system considered as a reference, and the proposed fog based architecture is described in Section 4. In Section 5, the simulation and analysis of the proposed method are discussed. Finally, in Section 6, the final conclusions of the paper are presented.

## II. Related Work

There exist a great number of articles on assessing the detection and even anticipation and isolation of sensor failures [5]. In [11] a fault detection and isolation system under real time working conditions has been developed which can be trained during the operating of system and it can detect new unknown faults. Attempts are made in [12] to provide a fault-tolerance method capable of providing tools for attack-resilience. For efficient application of these methods, first, it is necessary to consider the different nature of these two categories, next, to provide a method for their correct differentiation for proper and effective treatment. Attack on the physical layer in different parts of the communication path among the sensor, actuator and the controller is possible. In many articles, system modeling is run in order to detect attacks on the physical layer due to the physical laws prevail in nature. These modeling measure the normal operation of the system, while the attacks to this layer are detected. Authors in [13][14] explore the stuxnet attack due to the confused values received from the sensors. Different methods are proposed in [2][15][16] to detect different attacks on the system based on the values of sensors and control signals sent to the sensor. Attempt is made in [17] to differentiate the identified hazards into two general categories of transient failures and attacks by applying specific sensors in the system, where the features specified in the sensor are applied for this purpose. In the factory environment, this method is possible using IoT. By increasing numbers of IoT devices within a factory, various problems will be presented [7]. Cloud computing provides a mechanism for storing, computing and processing data [18]. Fog based IoT approaches are suggested to solve some challenges including slow processing, handling big data, and presence of too much heterogeneous data [19], [20].

## III. Traditional System

### A. Risk Management Control System

A general feedback control system to manage hazards in sensors, which could be caused by attack or failure, is shown in Figure 1 [4],[ 21]. The sensors in the physical layer first receive information from the environment and send it to the control layer ($y_i(t)$). And next, the control layer processes the received information from the environment and obtains an estimate of the system state ($x_i(t)$). Based on the estimated system condition, the required commands are sent to the operators by the control layer ($u_i(t)$). Actuators in the physical layer effect the environment based on commands. Physical real values can be manipulated by an attacker or

faulty sensor. Data injection attacks operate based on information of the attacker gained from the system. These attacks with $T_a$ duration modify the original data over time and collect the sensors data after adding with arbitrary value, as shown in equation 1.

$$y_i^a(t) = \alpha_i(t) + y_i(t) \quad (1)$$

Where $y_i^a(t)$ is the new value generated by the attacker for the sensor $i$ at time $t$, and $\alpha_i(t)$ represents the volume added to the sensor by the attacker.

Risk management consists of three major components, named risk detection, risk analysis, and system reconfiguration. The general idea to detect sensor hazards is the use of an estimator. The estimator compares the predicted values with the new values from the sensor. If the difference between them is greater than the specified value, it is determined as a hazard in the system. As to risk analysis, the probability of risk incident and the damage level thereof is computed according to the risk propagation level in the system. Then, the risk damage level is compared with the tolerable threshold of risk in the system. To reduce the harmful effects of risk, the necessary actions are taken in the system reconfiguration component. In the following subsection a cloud based system architecture is presented, which will be used as a reference for comparison in this paper.

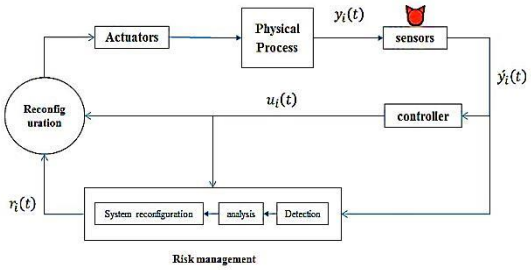


Figure 1. General feedback control system.

### B. Cloud Based System Architecture

In [17], for each sensor $i$ in the system, a transient failure model as $(e_i, w_i)$ is determined. This model specifies that the sensor $i$ has a maximum threshold transient failure of $e_i$ at time window $w_i$.

$$if\ (\alpha_i(t) > 0)\ then\ F(t) = 1$$
$$\left(\sum_{T_f - w_i}^{T_f} F(t)\right) < e_i$$

Where $T_f$ is the failure time and $\alpha_i(t)$ is the volume added to the correct value by the sensor $i$ at time $t$. In order to enable the system in hazard differentiation to adopt the best practice in dealing with them, the false alarm rate in the system should be in accordance with the following equation to be acceptable in the system:

$$acceptable\ false\ alarm\ rate = \left(\frac{e_i}{w_i}\right)$$

In order to reduce false alarm rate to acceptable range, a risk management approach is proposed using fuzzy clustering, timed automata and IoT. The proposed method consists of three components: 1) the hazard detection component, which employs the combination of fuzzy clustering, timed automata, and IIoT sensor data integration applied to detect hazards in the system, 2) the hazard analysis component, which categorizes the identified hazards into two categories, and 3) the reconfiguration component, which adopts the most appropriate manners based on the identified hazard causation. In smart factories, with increasing amount of IIoT devices, more accurate information about their surroundings can be achieved. With such growth of IIoT devices, the volume of data will increase significantly. In this case, real-time processing restrictions raise serious problems in the traditional cloud based system. It is crucial to improve the computing efficiency as well as reducing the data transfer latency and network traffic.

## IV. Fog Based Approach

A factory can be composed from different buildings and, in each building, different devices are working together in order to produce a particular product. Devices in ICS require quick response and undesired delays may result even in catastrophic hazards. Hazard differentiation requires deploying sensors in order to sense the environment and products, so IIoT becomes a viable solution. In an IIoT environment, the data obtained from the smart devices are collected and analyzed to generate valuable information about factory operations. In this paper, we propose a fog based architecture with three tiers. The proposed architecture is framed in figure 2. At the first tier, IIoT devices provide comprehensive information about the environment with an application that records sensor data and transfers to the fog layer. The IIoT devices are spread along the different buildings of the factory, and devices in a building communicate with the fog node at that building. In the second tier, the risk management process is implemented. The fog node at each building collects and processes its corresponding IIoT sensor data. Risk management detects and differentiates between the identified hazards by using sensor data fusion [22]. Thus, hazard differentiation can be processed locally for immediate tasks and operations. Fog prepares the integration of data that require the interplay and cooperation between the other fog servers and send it to the cloud as third layer of the architecture. In this tier, further processes for global system management are provided at cloud premises.

In the proposed architecture, a hieratical connection between different tiers is provided. Based on the proposed architecture, delay is decreased by network usage reduction caused by fog computing.

The advantages of using a fog-based architecture are numerous. The main advantage is having data available immediately because fog nodes are much closer to the IIoT devices than a cloud infrastructure. This reduces latency and, therefore, facilitates a real time data processing and hazards detection. Secondly, the volume of data that has to be transferred to the cloud can dramatically be reduced as long as only data that require interplay and cooperation will be moved to the cloud. In addition, data can be aggregated before transferring to the cloud, thus further reducing the

network usage. And finally, all these savings will enhance the system efficiency and energy savings.

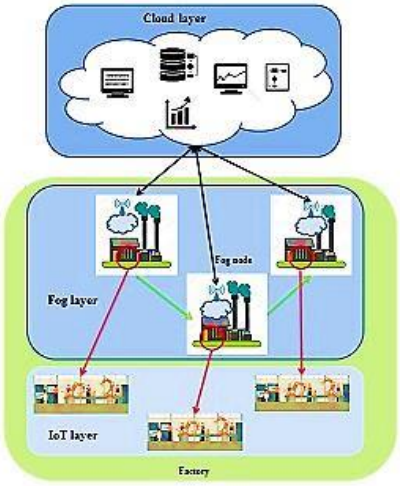


Figure 2. Proposed fog-based architecture.

## V. ANALYSIS

To assess this proposed method, a factory based scenario is considered. The factory has an area of 25 square kilometers composed of 10 buildings with area of 1 square kilometers each. In each building, 10 different devices are working together. The factory has 2,000 employees and the number of IIoT devices considered for sensing is from 2,000 up to 3,000 nodes. Each IIoT device sends a packet of 28 byte every 5 seconds. Therefore, the number of fog nodes and cloud are 100 and 1, respectively. IIoT nodes are associated with the fog node which has the shortest distance (i.e. has the smallest propagation delay). The communication between the IIoT node and its corresponding fog/cloud node is assumed to be through IEEE 802.11 a/g, and the transmission rate is 6 Mbps.

To evaluation, the system and simplified data presented in [23] are applied as a device in a building. The data set is the result of an ICS implementation to a liquid tank volume control system. The volume of the liquid inside the subjected tank is adjusted within 2,000 and 8,000 liters range. When the volume of the tank reaches its lowest range, a pump at the end of the tank will become activated. An evacuation hole is located at the bottom of the tank so that when the volume of the liquid in the tank exceeds the highest range, the pump is turned off and the access is discharged through the evacuation hole. An ultrasound sensor is applied to control and keep this volume within the determined range. In this system, the measured volume through this sensor is considered as the input and the command issued to the pump and the evacuation hole are considered as the outputs. Each one of these component are connected to a computer through a PLC controller. The liquid volume measured by the sensor is considered as $y_i(t)$ and the command issued by the system to the pump and the evacuation hole are considered as $u_i(t)$. The collected data reveal the normal system operation to last 7,000 seconds, as shown in Figure 3.

As stated in this paper, differentiation between hazards based on their causation is necessary to select the appropriate action in reconfiguration component. To illustrate this issue, the lost time oscillator due to the deficiency in proper differentiation of the attack from the failure of 100 different samples of the anomaly indicated in the system is shown in Figure 4, where the deficiency may lead to wrong action that would increase the reconfiguration time in the system; otherwise leading to a significant reduction in the system's reconfiguration time, thus, a very important tact in ICSs. According to the results, correct differentiation of hazards based on attack and failure leads to a reduction of 60% lost time in the recovery reconfiguration step of the system.

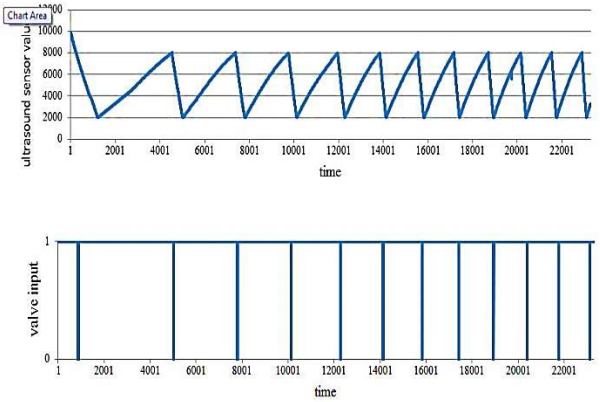


Figure 3. Sensor data and control commands in system normal operation.

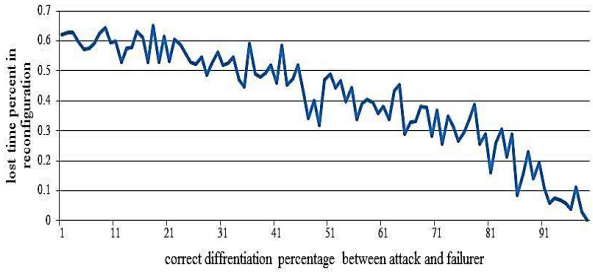


Figure 4. Time impact of hazard differentiation.

As observed, differentiation of hazard based on attack and failure, based on hard real-time restrictions of ICS, is necessary and differentiation of attack from failure without IIoT is not possible.

As observed, differentiation of hazard based on attack and failure, based on hard real-time restrictions of ICS, is necessary and differentiation of attack from failure without IIoT is not possible.

The red line indicates IIoT-Cloud and the blue line indicates IIoT-Fog-Cloud. As observed in the figure, time delay in the cloud increases with the number of service requests. Similarly, in each second, the network usage is increased based on the growth of the number of IIoT nodes, as shown in figure 6.

## VI. CONCLUSION

A new method for safety improvement is proposed here by differentiation of identified hazards based on attacks and failures in ICS. To accomplish this objective, a fog-based

sensor data fusion approach by considering IIoT sensor data is presented. In this system, a new three tier architecture for ICS in factory for data handling is provided. Hazard differentiation leads to take the best action in system reconfiguration component and reduces system reconfiguration time. This architecture due to the applying fog technology reduces the network delay and network data usage. The simulation results indicate that applying this method leads to reasonable delay reduction.

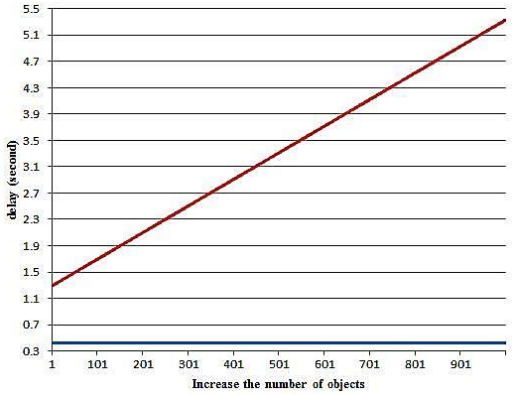


Figure 5. Network time delay comparison for two workflow.

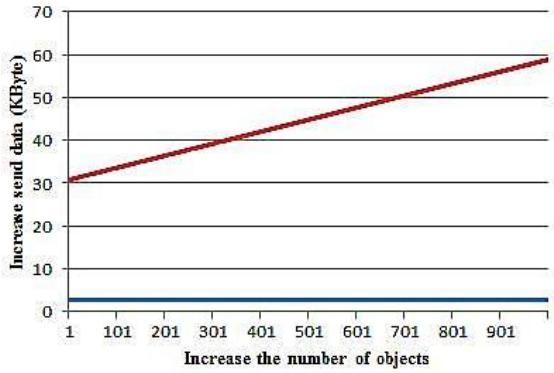


Figure 6. Network data usage comparison for two workflow.

## REFERENCES


[1] A. Humayed, J. Lin, F. Li, and B. Luo, Cyber-Physical Systems Security A Survey, IEEE Internet Things J., vol. 4,no. 6, pp. 18021831, 2017.

[2] Y. Liu, P. Ning, and M. K. Reiter, False Data Injection Attacks Against State Estimation in Electric Power Grids, in Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009, pp. 2132.

[3] R. Tan, V. Badrinath Krishna, D. K. Y. Yau, and Z. Kalbarczyk, Impact of Integrity Attacks on Real-time Pricing in Smart Grids, in Proceedings of the 2013 ACM SIGSAC Conference on Computer 38; Communications Security, 2013, pp. 439450.

[4] J. Giraldo et al., A Survey of Physics-Based Attack Detection in Cyber-Physical Systems, ACM Comput. Surv., vol. 51, no. 4, p. 76:1–76:36, Jul. 2018.

[5] F. Salfner, M. Lenk, and M. Malek, A Survey of Online Failure Prediction Methods, ACM Comput. Surv., vol. 42, no. 3, p. 10:1–10:42, Mar. 2010.

[6] M. S. Hossain and G. Muhammad, Cloud-assisted Industrial Internet of Things ( IIoT ) Enabled framework for health monitoring, vol. 0, pp. 111, 2016.

[7] D. W. Mckee, S. J. Clement, J. Almutairi, and J. Xu, Massive-Scale Automation in Cyber-Physical Systems: Vision & Challenges, pp. 511, 2017.

[8] G. Peralta, M. Iglesias-urkia, M. Barcelo, R. Gomez, A. Moran, and J. Bilbao, Fog Computing Based Efficient IoT Scheme for the Industry 4 . 0.

[9] M. Aazam, S. Member, S. Zeadally, K. A. Harras, and S. Member, Deploying Fog Computing in Industrial Internet of, vol. 3203, no. c, pp. 19, 2018.

[10] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, Fog Computing and Its Role in the Internet of Things Characterization of Fog Computing, pp. 1315, 2012.

[11] Dehestani, D., Eftekhari, F., Guo, Y., Ling, S. S., Su, S., & Nguyen, H. T. (2011). Online support vector machine application for model based fault detection and isolation of HVAC system. *International Journal of Machine Learning and Computing*.

[12] Z. Gao, C. Cecati, and steven x. Ding, A Survey of Fault Diagnosis and Fault-Tolerant TechniquesPart II: Fault Diagnosis With Knowledge-Based and Hybrid/Active Approaches, IEEE Trans. Ind. Electron., vol. 62, no. 6, pp. 37683774, 2015.

[13] R. Langner, Stuxnet: Dissecting a cyberwarfare weapon, IEEE Security and Privacy, vol. 9, no. 3, pp. 4951, 2011.

[14] N. Falliere, L. Murchu, and E. Chien, W32. Stuxnet dossier, White Pap. Symantec Corp., Secur. Response, vol. 5, no. 6, p. 29, 2011.

[15] A. A. Crdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, Attacks Against Process Control Systems: Risk Assessment, Detection, and Response, in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, 2011, pp. 355366.

[16] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, PyCRA: Physical Challenge-Response Authentication For Active Sensors Under Spoofing Attacks, in Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security, 2015, pp. 10041015.

[17] J. Park, R. Ivanov, J. Weimer, M. Pajic, and I. Lee, Sensor Attack Detection in the Presence of Transient Faults, in Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems, 2015, pp. 110.

[18] Mohamaddiah, M. H., Abdullah, A., Subramaniam, S., & Hussin, M. (2014). A survey on resource allocation and monitoring in cloud computing. *International Journal of Machine Learning and Computing*, *4*(1), 31.

[19] A. Sajid, H. Abbas, and K. Saleem, Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges, vol. 4, 2016.

[20] Donassolo, B., Fajjari, I., Legrand, A., & Mertikopoulos, P. (2019, January). Fog Based Framework for IoT Service Orchestration. In *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (pp. 1-2). IEEE.

[21] K. Paridari, N. OMahony, A. E.-D. Mady, R. Chabukswar, M. Boubekeur, and H. Sandberg, A Framework for Attack- Resilient Industrial Control Systems: Attack Detection and Controller Reconfiguration, Proc. IEEE, vol. 106, no. 1, pp. 113128, 2017.

[22] L. Xiao, S. Boyd, and S. Lall, A scheme for robust distributed sensor fusion based on average consensus, in IPSN 2005. Fourth International Symposium on Information Processing in Sensor Networks, 2005, pp. 6370.

[23] ] P. M. Laso, D. Brosset, and J. Puentes, Data in Brief Dataset of anomalies and malicious acts in a cyber-physical subsystem, Data Br., vol. 54, pp. 38, 2017. 22