A Methodology for Resilient Control and Monitoring in Smart Grids

Daniel Hauer*†, Denise Ratasich‡, Lukas Krammer* and Axel Jantsch†
*Corporate Technology, Siemens AG Österreich, Vienna, Austria,
† Institute of Computer Technology, TU Wien, Vienna, Austria,
‡ Institute of Computer Engineering, TU Wien, Vienna, Austria,
Email: *{daniel.hauer, lukas.krammer}@siemens.com, †‡{daniel.hauer, denise.ratasich, axel.jantsch}@tuwien.ac.at

***Abstract*—The increasing importance of decentralized and volatile energy sources causes huge challenges for future energy grids. Besides intelligent grid planning, real-time monitoring and control is necessary to guarantee reliable and sustainable grid operation. The basis for such applications is dependable monitoring of the grid. This paper introduces a methodology for resilient control and monitoring. A self-healing algorithm ensures that the system can operate even when monitoring devices or connections fail. Based on that, a model-free context-aware monitoring algorithm allows for detection of anomalies, drift and, in general, undesired conditions. These core components are embedded in a scaleable system architecture that allow for easy integration even in existing systems.**

***Index Terms*—fault-tolerance, smart grids, dependable systems, context-aware monitoring, internet of things**

I. Introduction

The increase of diversity of distributed energy producers and consumers poses a great challenge for the future grid and its management systems. The generation of renewable energy as well as e-mobility or demand-response applications require intelligent planning and management of low voltage grids. To efficiently facilitate the grid by preventing from overloads and outages, new control and protection concepts must be developed [1]. Due to the highly distributed nature of such systems, traditional measures of established automation systems do not suffice, but technologies developed in the context of "Industrial Internet of Things" (IIoT) are well suited, as they address dependable system behavior and decade-long life-cycles.

Thus, different kinds of technologies, levels of automation and sensor densities have evolved in the existing grid. Beside the ongoing smart meter roll-out, different kinds of IoT devices and smart sensors are integrated in all kinds of devices also including grid related consumers and producers (e.g., intelligent wall-box, smart substation monitoring systems). This trend results in a large number of sensors and actuators in the grid environment, generating an enormous amount of data, however, with varying and often unknown quality. In order to realize a resilient grid, it is necessary to have a guaranteed Quality of Service (QoS) for the sensory data and the communication network in the smart grid, ranging from power generation and distribution to customer applications [2].

The presented work is conducted in the "Trustworthy IoT for Cyber-Physical-Systems" (863129) project, funded and supported by the Austrian Research Promotion Agency (FFG).

To optimize the energy flow in smart grids, new concepts such as self-adaptation or self-aware control and monitoring are required [3]. Smart grids connected to the Internet further require to be resilient to system anomalies, including both faults and security vulnerabilities [4] which can be achieved by self-healing. These mechanisms are applied on top of a highly-scalable IIoT communication and computing architecture.

We therefore propose a novel methodology for resilient control and monitoring in the smart grid domain, by reusing existing infrastructure and applying novel approaches of data handling and monitoring with the following key objectives:

- A Build the architecture on top of the existing infrastructure.
- B Ensure safety and security in the event of faults or threats.
- C Guarantee functionality despite the diversity of IoT devices and their individual lack of reliability.
- D Ensure that the smart grid is future-proof for technological, functional and environmental changes in terms of maintainability and hardware/software life-cycle.

In order to achieve the goals, the proposed solution consists of (*) self-healing data collection, (*) context-aware data monitoring, (*) optimized control algorithms (e.g., faster overload prevention), (*) enhanced management support (e.g., efficient long-term grid expansion).

The system will be applicable to legacy systems by facilitating existing sensing and communication infrastructure. *Resilient control and monitoring* refers to *dependability* and *security* throughout the entire life cycle of a system [5], [6]. Our methodology focuses on increasing the *reliability*, *availability* and *integrity* of the collected sensor data by a self-healing data collection approach in combination with a context-aware data monitoring. This has a direct impact on monitoring applications and is a prerequisite for control applications. Although safety is implicitly improved by the proposed solution as reliability and availability are improved, explicit and application-specific safety measures are not addressed by this approach. Confidentiality is also tackled by some components of the methodology, but an overall security concept is out of scope of this work.

The rest of this paper is organized as follows: After a review of related work (section II) the proposed methodology is introduced in section III and further discussed in section IV by analyzing a comprehensive set of faults, failures and threats. Conclusions and an outlook are given in section V.

978-1-7281-5754-2/20/$31.00 ©2020 IEEE

II. Related Work

The need for a smarter grid and its possible realisations are extensively discussed in literature. [2], [4] and [7] provide an overview and highlight some of the most important enhancements needed to provide a future-proof smart grid. Key features such as dynamic demand response, self-healing structures, context-aware monitoring and intelligent bidirectional data and energy flow are discussed and theoretical implementation concepts are presented. Noteworthy research and development activities can be found on all these topics. [2] and [8] discuss different communication infrastructures and wireless networks in the smart grid. [3] and [9] develop semantic information models for smart grids to unify heterogeneous grid environments. [10] and [11] propose resilient architectures for specific use-cases in the smart grid domain (grid stability and load balancing) but therefore lack a generic system-wide approach.

Fault-tolerance and self-healing are extensively covered in literature, not just in the smart grid area but across multiple domains. In [12]–[14] an overview to fault-tolerance and self-healing is presented. However, typically the literature on dependability or resilience is split into fault prevention or predictive maintenance, fault detection and diagnosis and fault recovery or mitigation. A fault detection unit comprises a model of the expected (specification, cf. runtime verification [15] or anomaly detection [16]) or anomalous behavior (signature, cf. intrusion detection [17], [18]), or some redundancy [19] to compare against the actual behavior of a signal.

Our proposed methodology combines self-healing data collection and context-aware data monitoring. According to [20] context-awareness means that *"the system is aware of its context, which is its operational environment"*. The authors of this landscape paper claim that context-awareness together with self-awareness are part of the general property self-adaptiveness. Recent surveys about self-awareness and context-awareness can be found in [20] and [21]. Approaches based on deep learning and data mining could also form part of the solution, however, they require massive processing and memory resources [22], which is not available in IoT devices. Therefore solutions with a small footprint and without a extensive model building are favoured. Examples can be found in [23], [24] (medical monitoring) and [22] (health-monitoring of an AC-motor).

III. Methodology

Existing sensor and communication infrastructures in a grid typically provide heterogeneous data sets, e.g., in terms of redundancy, quality, quantity, and availability. New data sets can emerge, exiting ones can fail or change its characteristics during run-time. To enable resilient monitoring and control, we propose to add self-healing and context-awareness algorithms before the information is forwarded. The combination of the strengths of these two algorithms leads to a novel enhancement for resilient smart grid monitoring and control. Figure 1 shows the proposed methodology with its four planes: Physical, Network, Control and Monitoring & Management.

The self-healing unit monitors and (if necessary recovers) relevant information. Subsequently, a Context-Aware Monitoring (CAM) algorithm is used to enlarge the knowledge about the system under investigation. We propose two different levels of CAM. One level can detect the system's state and health and optimize this information for the control units (e.g., the system's reaction to control interventions can be observed and abstracted system information can be used to adapt the control algorithm). The second level of CAM is designed to provide relevant state and health conditions of the system for the management level. This information can be used to adapt or change control mechanisms (e.g., by recognizing recurring but sub-optimal reactions of the system to control decisions) or to optimize the infrastructure and plan long-term expansions.

The rest of this section describes the different planes and the self-healing and CAM algorithm of the proposed methodology.

- **Physical plane**
  The physical plane is the basis of an IoT system and represents the "Things". In IoT architectures sensors and actuators typically have very limited computing capabilities and they are connected to so-called edge devices [25]. Edge devices have higher computing capabilities to perform control applications. For realizing reliable real-time applications, hardware and software support is necessary. Since hardware and software have different life-cycles, one key feature of edge devices is the update-ability.
  Applied to a smart grid, which is a highly dynamic and massively distributed and heterogeneous automation system, the physical plane can basically be split into "behind-the-meter" and "in front of the meter". Behind the meter, there are the energy assets such as photovoltaic systems, battery storage or electric vehicle charging stations. These systems and the combination of them have almost unpredictable behavior. However, there are further limited means for controlling and monitoring them from systems in front of the meter. In front of the meter, there are components to monitor and control the grid. Monitoring in terms of measuring current, voltage and power over time is done in substations and at neuralgic points of the grid with so-called grid monitoring devices.
- **Network plane**
  The network plane is responsible for the connectivity in the whole system. In a typical IoT system, there are different types of connections: In a local network, sensors and actuators are connected to edge devices. In order to perform control applications, this connection fulfills dedicated quality-of-service requirements such as high reliability and real-time performance. As shown in Figure 1 the network plane is also responsible for collecting and forwarding network related data (network statistics) to the monitoring algorithms. In the smart grids domain, networking is a crucial topic. There, it is basically distinguished between technologies and components "behind the meter" and "in front of the meter". Behind the meter, mainly wired technologies based on Ethernet or twisted-

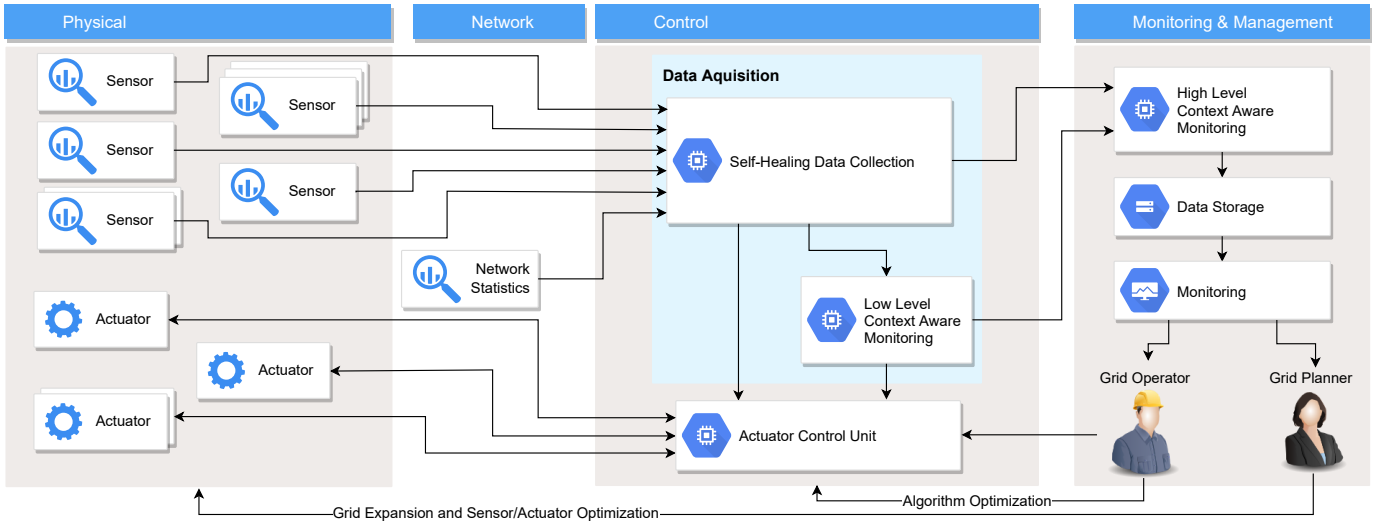

Fig. 1. Resilient methodology for monitoring and control in smart grids

pair media are used. For retrofitting applications even wireless technologies such as Bluetooth-LE or protocols based on IEEE 802.15.4 can be used. While technologies such as ZigBee or Bluetooth-LE are mainly used for consumer-grade applications, technologies like 6TISCH are used for real-time applications [26]. Time-sensitive networking (TSN) technologies [27] can be used for realizing dependable control applications. In front of the meter, various communication technologies are applied. Within a secondary substation, local systems are used to connected sensors and actuators with the automation station which represents the edge device. For connecting substations to the backend system of a grid operator (in the cloud or on-premise), wide-range communication technologies such as fibre optics connections, power-line communication or mobile communications (e.g., 4G, GPRS, etc.) are used. For connecting sensors at neuralgic points of the grid directly to the backend, technologies such as LoRaWAN or Narrowband-IoT can be used.

- **Control plane**
  The control plane is the heart of our proposed methodology. All collected data is processed by a self-healing algorithm to provide a constant and resilient set of information for the next levels even in terms of unforeseen changes in the physical and network plane. The healed information is then used to detect operating states and the health condition of the system with our so called ”Low Level CAM” algorithm. Such context-aware knowledge can then influence existing control units by providing additional information such as drifts, reoccurring states or suspicious behavior (both relevant for safety and security). For example, data sets from spatially separated distribution stations can be used to identify global effects of local control interventions and to optimize the control parameter. Both CAM and the self-healing algorithm will be explained in detail in the following sections.
- **Monitoring and Management plane**
  Complex automation and control systems require supervision and management. This plane can be basically distinguished in a functional and non-functional part.
  The non-functional part consists of system management functions that allow for keeping the software base systems as well as the applications on top up-to-date. In addition, it supports the update of applications if the system changes or a new functionality is added. Furthermore, the system management must allow for parameter updates of applications such as self-healing or CAM.
  From a functional point of view, the monitoring and management plane closes the loop of our proposed methodology. Long term data collection and context-aware monitoring is used to observe the systems state and health from a grid operator’s point of view. It is therefore an extension to existing systems like SCADA, which are more restricted to high voltage transmission networks only [2]. We propose a second ”High Level CAM” algorithm which is parameterized to detect global and long term events in the grid. This abstracted information can be used to change the underlying algorithms (control unit, self-healing, CAM), restructure parts of the grid (e.g., prevent overload through re-meshing) or to use the information to cost-effectively expand the current grid. For example, CAM can detect reoccurring malfunctions and therefore adapt the corresponding control strategy.

A. *Self-Healing by Structural Adaptation*

Faulty observation data used by subsequent units like controllers or monitors can lead to failures decreasing the system’s dependability. Traditional fault-tolerance is designed to overcome critical failures. Self-healing can be applied to react also to failures not specifically considered during design-time, e.g., faults caused by functional, environmental or technological changes or zero-day malware.

A component is designed to provide some information (e.g., a in Fig. 2). However, additional information ($a_1 \dots c_3$) often becomes available during runtime by connecting new subsystems to the network. For instance, the physical entities (CPS variables) observed (e.g., voltage, current, power on different power lines) can be related to each other, thus providing implicit information redundancy. Such redundancy can be used to detect faulty information by comparing it to related information [28], and to substitute failed information by spawning a substitute component advertising the failed information by consolidating related information, we refer to as *self-healing by structural adaptation* (SHSA) [29].

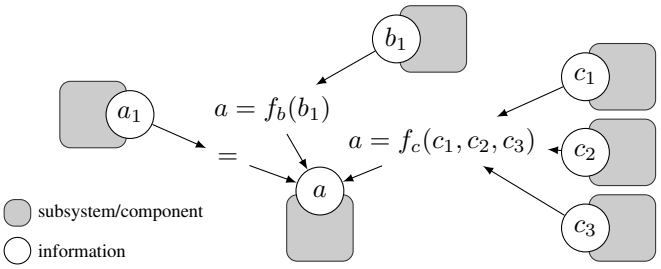

Fig. 2. Components providing related information through its interfaces (relations can be arbitrary functions, learned or defined by a domain expert).

The central part of SHSA (as it is self-healing and self-* in general) is a knowledge base. The SHSA knowledge base encodes the relations and the availability of the information, e.g., as a set of Prolog rules [28]. Given some CPS variable or signal under test, the knowledge base is searched to find related information for comparison or substitution. Furthermore, the knowledge base is adaptive, that is, the relations and availability of signals may change during runtime, in order to cope with various system changes. SHSA is implemented as an additional service acting on the communication network of a system (monitoring messages and substituting signals in messages). The SHSA service may run on a separate platform and connect to existing systems [30].

B. Context-Aware Monitoring

Context-Aware Monitoring (CAM) has originally been developed for the analysis of body signals for health monitoring [23], [24] and then extended to the monitoring of AC motors [22] and hydraulic systems [31]. An application of CAM in the analysis and observation of industry 4.0 manufacturing can be found in [32].

CAM is based on concepts of self-aware systems [21], [33] and assumes that, with comprehensive data collection and careful analysis, an abstract "understanding" of an observed object can be built dynamically and without pre-developed models (Figure 3). The CAM algorithm collects all available sensor data and continuously identifies new and already known patterns - called "states" - in the data streams. Initially all states are new, but with ongoing observation newly emerging states are unusual and, depending on the context and application, may be marked as an anomaly. CAM has the ability

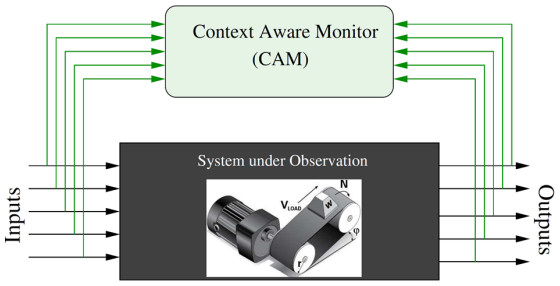

Fig. 3. Context-Aware monitoring system [22]

to recognize normal and unusual sequences of states, and creeping changes in sensor values assigned to a state are also recognized as drift symptoms.

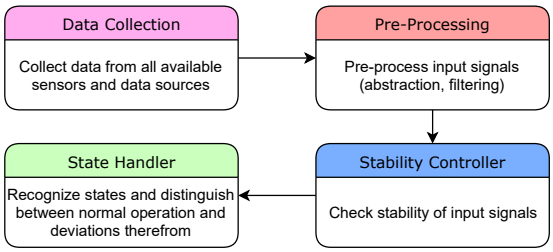

Fig. 4. Block Diagram of the Context-Aware monitoring system [22]

Figure 4 shows the CAM system consisting of data collection and three functional blocks [22]. The pre-processing block covers both abstraction and filtering (e.g., low-pass) of the signals. The pre-processed data is then checked for stability by using a sample history in the form of a sliding window. The subsequent state handler does the bulk of the work. It tries to recognize all states of normal operation, to be able to detect deviations from the normal operation. Detailed information about CAM can be found in [22]. The main advantages of CAM can be split in operation and installation benefits:

- Operation: CAM works without pre-developed models of the object under observation, is general and adaptive, and can distinguish the "normal" from the "unusual" without an explicit learning phase.
- Installation: CAM has a small footprint and can operate on top of existing systems without the need for major hardware changes [32]. Therefore it can easily be applied to a variety of existing IoT devices. A hierarchical agent-based toolbox (C++) is available [23].

According to figure 1, we propose a two level monitoring approach. The goal of the Low Level CAM algorithm is to detect states or drifts, that might lead to an failure or unhealthy state (e.g., overload along a power line) and immediately provide this information to the control units. For instance, it can detect the activation of various electric vehicle charging stations and can therefore suggest to limit the individual charging currents.

While Low Level CAM detects threats for immediate use at the control units, the High Level algorithm is designed to

detect global and long-term events. Furthermore the results are abstracted in such a way that they can be visualized for human operators. Hence, High Level CAM can detect recurring global effects of control interventions. For instance, if the grid is re-meshed due to an overload on one segment, this can lead to faults in the long run on other segments. Such a pattern can be detected and Low Level CAM or the corresponding control unit can be switched to an alternative failure handling.

IV. Discussion

Considering the smart grid and its IoT infrastructure, a resilient control and monitoring system has to handle different kinds of failures and threats to ensure the functionality. The system therefore has to detect and identify faulty, attacked or failed components during run-time and has to autonomously maintain resilience [6]. Table I gives an overview on possible failures and threats in the different planes of a smart grid.

TABLE I
FAILURES AND THREATS WITH RESPECT TO SMART GRID PLANES [6]

Plane	Dependability	Security	Long-term
Physical	Broken connector Uncertainties	Sensor hacking Physical damage	Material decay Physical stress
Network	Message collision Interference	Jamming/Flooding Routing ill-directing	Overload Protocol violation
Control	Input errors Deadline miss	Signal manipulation Illegal access	Upgrades/Updates New requirements
Monitoring & Manag.	Data corruption Unavailability	Data poisoning Eavesdropping	Infrastructure aging Staff turnover

To justify, that our novel approach ensures resilient control and monitoring for smart grids, in this section we want to discuss the threats and failures listed in Table I. In order to increase readability, similar points are grouped together.

A. Broken connector, Physical damage, Message collision

These failures all lead to one or more sensors or actuators failing and no longer transmitting data or performing control interventions. Broken sensors or communication channels are compensated by our self-healing data acquisition. As long as there is redundancy in the sensor network, the SHSA algorithm ensures the data collection and higher-level systems do not see any changes. If the failure affects an actuator, this fault is detected by state-of-the-art protective mechanisms on the one hand (in the worst case by triggering a fuse) and on the other hand its malfunction also causes a change in grid's behaviour. These changes can be detected by CAM.

B. Uncertainties, Material decay, Physical stress, Interference

Both material decay and physical stress cause sensor values to change their behavior over a longer period of time (drift) or to fail completely. Uncertainties and inferences lead to fluctuating measurement data over a short or longer period of time. In case of failures, the data can be replaced using our SHSA algorithm as described in the previous point. If the behavior changes over a long time, one of the strengths of CAM is that it can detect drifts. Affected sensors or communication paths can thus be replaced.

C. Sensor hacking, Jamming/Flooding, Routing ill-directing, Signal manipulation, Illegal access, Data poisoning

Similar to the already mentioned points, these kinds of security threats lead to a abnormal system behaviour an can be detected by CAM. Therefore CAM also uses additional data input such as data rates, network load or status updates from the sensor and communication networks. This improves CAM's ability to detect malicious interventions (e.g., changes in the network traffic). When detecting malicious behaviour (regardless if its an attack or malfunction), the grid can ignore the affected devices and the SHSA algorithm can ensure operational reliability (as long as redundancy is still given, otherwise an alarm can be raised). If an intentional attack is recognized (e.g., by detecting distinctive network traffic patterns) additional warnings can be sent to the grid operator beside the immediate fault actions.

D. Overload, Deadline miss, Protocol violation, Input errors

In contrast to e.g., material decay, these threats result in sudden changes in the behavior of the grid. Either sensor data cannot be transmitted correctly or successfully, or actuators receive incorrect control signals. Again SHSA compensates missing sensor data and CAM is able to detect sudden grid state changes and react accordingly (e.g., reconfigure communication network to avoid overload or fix protocol violations).

E. Upgrades/Updates, New requirements

Both SHSA and CAM have a knowledge base that needs to be updated with each grid update or system change. One strength of CAM is that changes in the grid operation due to unknown updates are also recognized as state changes. The High Level CAM processes the data and provides abstracted monitoring information for the grid operator and planner. In case of a planned update, the operator can then mark the changes as "healthy" and CAM's parameter can be adjusted.

F. Staff turnover

The High Level CAM is designed to provide abstracted grid health information and seamlessly integrate them into existing monitoring systems (e.g., SCADA). Grid operators therefore do not have to familiarise themselves with different and complex monitoring systems and their individual details. This simplifies staff turnover, saves time and maintenance costs, and reduces susceptibility for human errors.

G. Unavailability, Infrastructure aging, Eavesdropping, Data corruption

Data loss or corruption at the Monitoring and Management plane are not the focus of this work. Common data protection techniques can be used to ensure functionality of databases or servers. As safety measures are not explicitly addressed by this approach, a human operator is still needed to supervise safety-critical decisions (e.g., detect false positives). Also the detection of pure eavesdropping without influencing the grid operation is beyond the scope of our work.

V. Conclusion and Outlook

This paper proposes a novel methodology for resilient control and monitoring in the smart grid domain. Our approach is designed to operate on top of the existing grid infrastructure without requiring major hardware changes and can be applied with low investment costs due to its small footprint. First the self-healing data acquisition algorithm SHSA guarantees dependable data collection even in the advent of faults or threats. As long as SHSA sees enough redundancy in the infrastructure, it can guarantee functionality despite the diversity of IoT devices and their individual lack of reliability. Based on this reliable data and additional information, the context-aware CAM algorithm detects the grid's state and health and forwards the abstracted information to both the control units and the grid operators and planners on the management plane. CAM's output is then used to trigger and optimize control algorithms for a fast failure correction or failure prevention and for long-term infrastructure optimizations. With this methodology we ensure that the smart grid is future-proof for technological, functional and environmental changes.

To validate our proposed methodology, we addressed well-known failures and threats in the smart grid domain and discussed how our solution can solve these issues. However, extensive field tests will be necessary to optimize our methodology. In future work we will therefore implement such tests and evaluate the results. Furthermore, CAM is currently being extended so that the algorithm can include component models and use feedback information to perform self-adaptation without human intervention.

References

[1] P. Zhang, F. Li, and N. Bhatt, "Next-generation monitoring, analysis, and control for the future smart control center," *IEEE Transactions on Smart Grid*, vol. 1, no. 2, pp. 186–192, 2010.

[2] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE communications surveys & tutorials*, vol. 15, no. 1, pp. 5–20, 2012.

[3] D. Schachinger, W. Kastner, and S. Gaida, "Ontology-based abstraction layer for smart grid interaction in building energy management systems," in *2016 IEEE International Energy Conference (ENERGYCON)*, pp. 1–6, IEEE, 2016.

[4] H. Farhangi, "Smart grid," in *Encyclopedia of Sustainable Technologies* (M. A. Abraham, ed.), pp. 195 – 203, Oxford: Elsevier, 2017.

[5] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Trans. on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, 2004.

[6] D. Ratasich, F. Khalid, F. Geissler, R. Grosu, M. Shafique, and E. Bartocci, "A roadmap towards resilient internet of things for cyber-physical systems," *CoRR*, vol. abs/1810.06870, 2018.

[7] M. L. Tuballa and M. L. Abundo, "A review of the development of smart grid technologies," *Renewable and Sustainable Energy Reviews*, vol. 59, pp. 710–725, 2016.

[8] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renewable and Sustainable Energy Reviews*, vol. 57, pp. 302–318, 2016.

[9] Q. Zhou, S. Natarajan, Y. Simmhan, and V. Prasanna, "Semantic information modeling for emerging applications in smart grid," in *2012 Ninth International Conference on Information Technology-New Generations*, pp. 775–782, IEEE, 2012.

[10] J. Lopez, J. E. Rubio, and C. Alcaraz, "A resilient architecture for the smart grid," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3745–3753, 2018.

[11] Z. Wang and J. Wang, "A delay-adaptive control scheme for enhancing smart grid stability and resilience," *International Journal of Electrical Power & Energy Systems*, vol. 110, pp. 477–486, 2019.

[12] S. S. Sathya and K. S. Babu, "Survey of fault tolerant techniques for grid," *Computer Science Review*, vol. 4, no. 2, pp. 101 – 120, 2010.

[13] D. Ghosh, R. Sharman, H. Raghav Rao, and S. Upadhyaya, "Self-healing systems — survey and synthesis," *Decision Support Systems*, vol. 42, pp. 2164–2185, Jan. 2007.

[14] H. Psaier and S. Dustdar, "A survey on self-healing systems: Approaches and systems," *Computing*, vol. 91, pp. 43–73, Jan. 2011.

[15] E. Bartocci and Y. Falcone, eds., *Lectures on Runtime Verification: Introductory and Advanced Topics*. Programming and Software Engineering, Springer International Publishing, 2018.

[16] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," *ACM Comput. Surv.*, vol. 41, pp. 15:1–15:58, July 2009.

[17] I. Butun, S. D. Morgera, and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 266–282, First 2014.

[18] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1153–1176, Secondquarter 2016.

[19] H. Zhang, Q. Zhang, J. Liu, and H. Guo, "Fault Detection and Repairing for Intelligent Connected Vehicles Based on Dynamic Bayesian Network Model," *IEEE Internet of Things Journal*, vol. 5, pp. 2431–2440, Aug. 2018.

[20] M. Salehie and L. Tahvildari, "Self-adaptive software: Landscape and research challenges," *ACM transactions on autonomous and adaptive systems (TAAS)*, vol. 4, no. 2, p. 14, 2009.

[21] A. Jantsch, N. Dutt, and A. M. Rahmani, "Self-awareness in systems on chip—a survey," *IEEE Design & Test*, vol. 34, no. 6, pp. 8–26, 2017.

[22] M. Götzinger, N. TaheriNejad, H. A. Kholerdi, and A. Jantsch, "On the design of context-aware health monitoring without a priori knowledge; an ac-motor case-study," in *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp. 1–5, IEEE, 2017.

[23] M. Götzinger, N. Taherinejad, A. M. Rahmani, P. Liljeberg, A. Jantsch, and H. Tenhunen, "Enhancing the early warning score system using data confidence," in *International Conference on Wireless Mobile Communication and Healthcare*, pp. 91–99, Springer, 2016.

[24] A. Anzanpour, I. Azimi, M. Götzinger, A. M. Rahmani, N. TaheriNejad, P. Liljeberg, A. Jantsch, and N. Dutt, "Self-awareness in remote health monitoring systems using wearable electronics," in *Proceedings of the Conference on Design, Automation & Test in Europe*, pp. 1056–1061, European Design and Automation Association, 2017.

[25] A. Rahmani, P. Liljeberg, J.-S. Preden, and A. Jantsch, eds., *Fog Computing in the Internet of Things*. Springer, 2018.

[26] D. Dujovne, T. Watteyne, X. Vilajosana, and P. Thubert, "6tisch: deterministic ip-enabled industrial internet (of things)," *IEEE Communications Magazine*, vol. 52, pp. 36–41, December 2014.

[27] IEEE 802.1, "Time-Sensitive Networking (TSN) Task Group." https://1.ieee802.org/tsn/.

[28] D. Ratasich, M. Platzer, R. Grosu, and E. Bartocci, "Adaptive Fault Detection exploiting Redundancy with Uncertainties in Space and Time," *arXiv:1903.04326 [cs]*, Mar. 2019.

[29] D. Ratasich, T. Preindl, K. Selyunin, and R. Grosu, "Self-healing by property-guided structural adaptation," in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, pp. 199–205, May 2018.

[30] D. Ratasich, O. Höftberger, H. Isakovic, M. Shafique, and R. Grosu, "A Self-Healing Framework for Building Resilient Cyber-Physical Systems," in *2017 IEEE 20th International Symposium on Real-Time Distributed Computing (ISORC)*, pp. 133–140, May 2017.

[31] M. Gotzinger, E. Willegger, N. TaheriNejad, A. Jantsch, T. Sauter, T. Glatzl, and P. Lilieberg, "Applicability of context-aware health monitoring to hydraulic circuits," in *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*, pp. 4712–4719, IEEE, 2018.

[32] L. C. Siafara, H. A. Kholerdi, A. Bratukhin, N. TaheriNejad, A. Wendt, A. Jantsch, A. Treytl, and T. Sauter, "Samba: A self-aware health monitoring architecture for distributed industrial systems," in *IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society*, pp. 3512–3517, IEEE, 2017.

[33] N. TaheriNejad, A. Jantsch, and D. Pollreisz, "Comprehensive observation and its role in self-awareness; an emotion recognition system example.," in *FedCSIS Position Papers*, pp. 117–124, 2016.