Resilient Access to Heterogeneous Measurement Data for Grid Observability

Nostro, Nicola ; Shahid, Kamal; Bondavalli, Andrea; Schwefel, Hans-Peter Christian

Published in:
Proceedings - 2019 15th European Dependable Computing Conference, EDCC 2019

DOI (link to publication from Publisher):
10.1109/EDCC.2019.00043

Publication date:
2019

Document Version
Accepted author manuscript, peer reviewed version

Resilient Access to Heterogeneous Measurement Data for Grid Observability

Nicola Nostro*, Kamal Shahid†, Andrea Bondavalli‡* and Hans-Peter Schwefel§†
*ResilTech s.r.l., Pontedera, Italy
Email: nicola.nostro@resiltech.com
†Dept. of Electronic Systems, Aalborg University, Denmark
Email: ksh@es.aau.dk
‡Dept. of Mathematics and Informatics, University of Florence, Italy
Email: andrea.bondavalli@unifi.it
§GridData GmbH, Germany
Email: schwefel@griddata.eu

***Abstract*—The ability to fuse data from heterogeneous sources (such as Smart Meters etc.) in the low-voltage grid highly depends on the communication and data management infrastructure that allows an exchange of information between different grid assets. Failure or any attempt to attack this data fusion solution can lead to inefficient grid operation and in worst case even blackouts. Therefore, this paper describes methodologies to cope with threats and faults in a low-voltage grid scenario to provide resilient access to the heterogeneous measurement data.**

***Keywords*-Grid Observability; Resilient data access; Smart Grid Data Integration; HAZOP; Threat Analysis**

I. Introduction

The evolving decentralized power system has led to a huge penetration of renewable energy sources such as wind and photovoltaic generation. Such energy resources are distributed across medium voltage and low voltage (LV) grids and have volatile power production. This brings new challenges for Distribution System Operators (DSOs) for grid efficiency and voltage quality [1]. However, grid-connected systems use inverters that provide opportunities including provision of new measurement points that to a large extent are already connected to Internet portals of the inverter vendors. Moreover, the massive deployment of Smart Meters (SM) provides opportunities for DSOs to obtain valuable information about the LV grid.

In order to achieve observability of LV grids, the data from the SMs, inverters and other measurement devices need to be correlated to the LV grid topology. However, fusing heterogeneous data provides multiple challenges [2], including vulnerabilities associated with the use of existing communication networks and information systems that may be exploited for financial or political motivation to delay, block, alter process related information (with fraudulent information) or even direct cyber-attacks against the power system. In either case, this will affect the integrity, confidentiality or availability of the ICT system [3], which can lead to an inefficient grid operation and in worst case to blackouts. Therefore, algorithmic solutions as well as connectivity and security from an ICT perspective need to be designed carefully and strategies should be defined to cope with potential associated risks.

The control and security of power systems using existing communication networks for control purposes has been tackled in several works. Authors of [4] analyze end-to-end security of the communication between DSO substation and distributed energy resources over heterogeneous networks through TLS encryption and authentication compliant to IEC 62351-3. [5] describes a solution to use standardized technologies to allow secure communications for ancillary services with minimal configuration by corporate networks administrators. Similarly, [3] focuses on medium voltage grids characterized by a high level penetration of renewable generation plants and examines the risks associated with communication malfunctions of an ICT architecture implementing the voltage control function.

This paper summarizes a data fusion architecture developed for LV grid observability applications, presents an analysis of threats and hazards applied to the ICT architecture as case study and selected analysis results, together with directions to follow up in research and system design as consequence.

II. Grid Observability - System Architecture

Data fusion from different heterogeneous data sources (e.g., SMs, inverters) in LV grids can add value to the DSOs in terms of increased grid observability, which allows for voltage quality enhancement and loss minimization in the LV grid. A middleware-based architecture has been, shown in Fig. 1, has been proposed in [2] and used in this work as reference case study. The ICT Gateway (middleware-layer) provides a uniform application platform for domain-oriented applications by abstracting specific details about provider subsystem interface into a normalized/harmonized data model and by taking care of issues related to reliability and security.

In Fig. 1, grid observability applications are shown on the top, which use measurements and grid topology information from existing DSO subsystems (shown at the bottom) in order to calculate and visualize derived metrics such as location of faults. Since the applications only interact with measurement and actuation subsystems via the ICT Gateway (ICT GW), these can be implemented independent of the used subsystems. The detailed description of complete system architecture is out

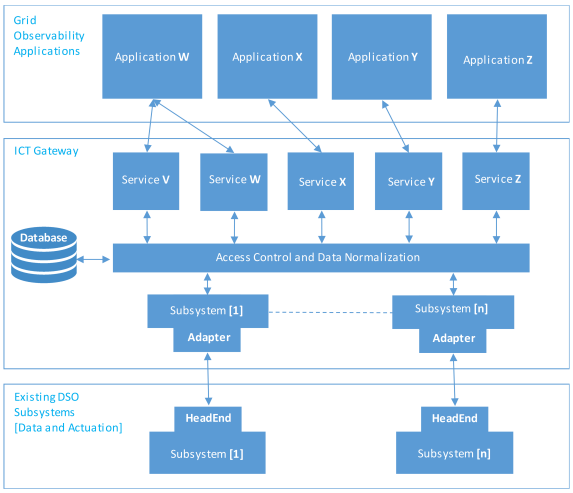

Fig. 1: System Architecture for data fusion, adapted from [2]

of the scope of this paper and can be found in [2], while this work aims at providing an analysis of the ICT GW with respect to accidental faults and cyber-security.

III. Threat and Fault Analysis to the ICT Gateway

The identification of potential operability problems is one of the approaches used when dealing with safety-critical systems. All the approaches have a common factor, namely the identification of hazards, which is a real or potential condition that, when activated, can lead to a series of interrelated events that result in damage to equipment or property or injury to people. Fault Modes and Effects Analysis (FMEA) [6], Fault Tree Analysis (FTA) [7], Hazard and Operability Studies (HAZOP) [8] are the most used techniques available for the identification of hazards.

Although these techniques are usually applied to evaluate the impact of accidental faults to the system's safety, this work aims at applying the HAZOP approach in an unusual way to analyze in combination both faults and cyber-security aspects of the ICT GW, which can have impact on the smart grid operation, through implementation of erroneous actions, or which can be originated by the HeadEnds of the grid.

A. The Methodology

In order to follow a systematic approach, leading to cover all potential threats and hazards to the system, the analysis is based on two aspects: the functions the ICT Gateway has to perform and the interfaces between DSO's subsystems with the ICT Gateway in order to consider the data exchanged.

The threat and hazard identification is based on a HAZOP approach conducted through the application of selected guidewords to both functions and interfaces. The application of guidewords allows systematically identifying potential deviations from the expected behavior of the system under analysis. The sets of guidewords for functions and interfaces are respectively: {NOT, OTHER THAN, REPETITION} and {NOT, CORRUPTION, DELAY, MISROUTE, EAVESDROP, SCAN, SPOOF}. Each function and interface of the system is inspected in turn by applying the guidewords to identify possible deviations from the normal behavior, thus potential causes of both accidental faults and intentional acts. The analysis is recorded and maintained through specific worksheets.

B. Threat and Hazard Risk Evaluation

Once threats and hazards have been identified along with detailed, the risk is evaluated. In order to check the acceptability of dangerous events, the approach considers the combination of the severity of the harmful event with its probability. A threat having serious consequences but whose probability of occurrence is very weak can be accepted, while a less serious but more frequent event cannot be accepted. This comparison is presented through a criticality matrix.

The probability and severity have been assigned on expert judgment, in a conservative and protective way, thus considering the worst case, while the probability has to be re-assigned after identification of proper countermeasures able to reduce the risk to an acceptable level.

Once the threats have been identified and according to the results of the Risk analysis, The methodology follows two different ways based on the risk obtained through the combination of probability and severity: i) if the risk of the hazardous event is evaluated as "Negligible" or "Tolerable" then no other actions are required; ii) if the risk is evaluated as "Intolerable", countermeasures useful to prevent the occurrence of the event or to reduce its probability of occurrence must be identified. Countermeasures identify long-term strategies that may include planning, procedures, maintenance activities, utilization of specific components, equipment, and other technological solutions able to counteract the undesired event.

C. Analysis Results

The analysis and risk assessment led to identify hazardous events that need to be addressed to avoid or to prevent system failure. In the following, relevant results from the analysis are reported, while the full analysis can be found in [9].

Measurement data for grid observability is a relevant asset to be safeguarded with respect to faults and cyber-attacks. Fig.2 shows an extract of the analysis of hazardous events identified by the application of guidewords *corruption* and *delay* to the measurements from a generic HeadEnd to the ICT GW. Consequences of these events are that problems occurring in the electrical grid are not promptly addressed (in case of *delay*, even worse useless activities of maintenance or setting of the grid are performed in case of *corruption* of data, leading to degradation, instability of the grid, customers' dissatisfaction, loss of money. Causes identified range from ICT faults (e.g., HW faults, Network congestion/disconnection) to intentional attacks to the communications (e.g., Man in the Middle, Interference). The Risk Classification pre-mitigation is *Intolerable*, based on Probability and Severity before the identification of mitigations; while introducing proper mitigations, to lower the probability of occurrence of the threat, leads to reduce the risk to a *Tolerable* level, thus bringing the threat status from Open to Solved and, after implementation, to Closed.

IV. Conclusion and Related Research Directions

This work discussed the relevance of accessing measurement data from heterogeneous field devices for grid observability and provided as example a set of analysis results obtained through the application of a threat and hazard analysis to the ICT Gateway characterizing the overall system.

In addition to classic mitigations, such as use of firewalls, anti-viruses, authentication, encryption protocols, security policies, the performed threat and hazard analysis reveals meaningful research directions that deserve to be further investigated, as described in the following.

Information freshness in real-time observability applications: The analysis, as well as other researches in critical domains [10], highlights the importance for applications that work in real-time to deal with reliable data from the point of view of updating. Handling grid scenarios with outdated or incomplete data could have different impacts. While there are several quantitative metrics and calculation models to quantify the impact of communication and information access delays, existing studies [11], [12] look at probabilistic delay distributions, without linking those to different root causes; the results of the hazard analysis enable a top-down identification of relevant scenarios and root causes.

The approaches in [13] link information age to value errors in the retrieved data. Value errors however can be caused by multiple other reasons including: measurement noise, time alignment errors for measurement intervals that are caused by imperfect clock deviations [14], faults in the measurement device or in other components in the measurement subsystems, malicious attacks on the communication networks. A quantitative investigation of the joint impact of relevant causes of value errors is interesting future work that can use the hazard analysis as the starting point to identify the relevant causes.

Anomaly Detection Methods: The analysis draw attention to corruption of measurement, in particular to the difficulty to distinguish malicious intentional modifications from measurement errors due to subsystems failures. Several anomaly detection approaches exist focusing on power consumption anomalies [15], [16], which anyway do not distinguish between the causes (either accidental or intentional) of the deviation from normal expectation.

An interesting direction in order to follow the way of cybersecurity is the joint monitoring of both electrical measurements and ICT aspects, such as resource usages (e.g., CPU percentage usage, memory percentage usage) and communications between network devices (e.g., number of packets sent/received), which are usually a symptom of security violations.

Acknowledgment

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 774145 for the Net2DG Project.

References

[1] H.-P. Schwefel, W. Schaffer, and R. Damböck, "Ict and data-management for dependability of electricity distribution grids: Opportunities and barriers," in *2017 13th European Dependable Computing Conference (EDCC)*. United States: IEEE, 9 2017, pp. 8 – 9.

[2] Net2DG, "Deliverable d1.2 - initial baseline architecture," 2018.

[3] G. Dondossola and R. Terruggia, "Security of communications in voltage control for grids connecting der - impact analysis and anomalous behaviours," August 2014.

[4] R. Terruggia and G. Dondossola, *Cyber Security Analysis of Smart Grid Communications with a Network Simulator*. Cham: Springer International Publishing, 2015, pp. 153–164.

[5] M. Krebs, S. Röthlisberger, and P. Gysel, *Secure Communications for Ancillary Services*. Springer International Publishing, 2015.

[6] *BS 5760-5 Reliability of systems, equipment and components. Guide to failure modes, effects and criticality analysis (FMEA and FMECA).* British Standards Document, 1991.

[7] *IEC61025 - Fault tree analysis (FTA).*, 2nd ed. IEC, 2006.

[8] IEC, *Hazard and operability studies (HAZOP studies): application guide.*, 2001.

[9] Net2DG, "Deliverable d3.1 - ict analysis and gateway design," 2018.

[10] A. Ceccarelli, F. Brancati, B. Frömel, and O. Höftberger, *Time and Resilient Master Clocks in Cyber-Physical Systems*. Cham: Springer International Publishing, 2016, pp. 165–185.

[11] T. Kristensen, R. Olsen, J. Rasmussen, and H.-P. Schwefel, "Information access for event-driven smart grid controllers," *Sustainable Energy, Grids and Networks*, vol. 13, pp. 78–92, 2018.

[12] M. Kemal, R. Olsen, and H.-P. Schwefel, "Optimized scheduling of smart meter data access: A parametric study," in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. US: IEEE, 10 2018.

[13] M. Bøgsted, R. Olsen, and H.-P. Schwefel, "Probabilistic models for access strategies to dynamic information elements," *Performance Evaluation*, vol. 67, no. 1, pp. 43–60, 2010.

[14] H.-P. Schwefel, I. Antonios, and L. Lipsky, "Impact of time interval alignment on data quality in electricity grids," in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. US: IEEE, 10 2018.

[15] L. Mookiah, C. Dean, and W. Eberle, "Graph-based anomaly detection on smart grid data," 2017. [Online]. Available: https://aaai.org/ocs/index.php/FLAIRS/FLAIRS17/paper/view/15443

[16] X. Liu, N. Iftikhar, P. S. Nielsen, and A. Heller, "Online anomaly energy consumption detection using lambda architecture," in *Big Data Analytics and Knowledge Discovery*, S. Madria and T. Hara, Eds. Cham: Springer International Publishing, 2016, pp. 193–209.

Source	Destination	Data flow/Information	Guideword	Threat/Hazard Description	Consequence	Cause	Probability (Pre-Mitigation)	Severity (Pre-Mitigation)	Risk Classification (Pre-Mitigation)	Mitigation/Countermeasure	Probability (Post-mitigation)	Severity (Post-mitigation)	Risk Classification (Post-mitigation)
HeadEnd	ICT GW	Measurements from the field	CORRUPTION	Message is corrupted: - the message is not accepted - the message is acceptable but wrong	- ICT GW does not reply to registration. - ICT GW addresses wrong data and event thinking they are correct.	- Environmental condition - Interference - Interruption of data transmission - Cable disconnection - SW bug - HW fault - Malware - Data Injection - Man in the Middle	Highly Probable	Catastrophic	Intolerable	- Authentication techniques - Security Policies - Maintenance procedures - Encryption schema (TLS) - Error and corruption detection mechanisms - Anomaly detection - Intrusion detection	Remote	Catastrophic	Tolerable
HeadEnd	ICT GW	Measurements from the field	DELAY	Message is delayed during transmission	- ICT GW cannot promptly react to events or address fresh data.	- SW bug - Huge amount of Data - Network Congestion - Network Disconnection - Malicious code installed	Highly Probable	Catastrophic	Intolerable	- Timestamping - Authentication - Anomaly detection	Highly Probable	Serious	Tolerable

Fig. 2: Extract of the analysis from [9]