Original scientific paper

Implementation of the SCADA based Infrastructure for Distributed PV Systems Controlling

Ivan Vujović, Mladen Koprivica, and Željko Đurišić

Abstract — **Different types and different size photovoltaic (PV) systems are in use. Assuming that these systems are equipped with some of the: internet of things (IoT) devices, intelligent electronic devices (IED), phasor measurement units (PMUs) and that they are properly communicated with control center, or that inverters in the PV systems contain network interface cards (NICs) which are connected to the control center through network, a solution for infrastructure of the monitoring and management (M&M) system is proposed. The main parts of the system are cloud infrastructure on which supervisory control and data acquisition (SCADA) system is implemented, network that connects all parts of cloud together and enables connections, through proprietary links or service providers networks, to the distributed devices as well as to the inverters at PV sites. Time synchronization between the central part of the SCADA system and devices at PV systems sites enables obtaining precise moments of the events occurrence and timely response. All parts of the SCADA system and network must be secured from the inside and outside threats.**

Keywords — **PV system, SCADA, network, time synchronization, security.**

I. Introduction

THERE are more and more PV systems connected to the power grid at distribution and transmission voltage levels. From small, distributed PV systems, to the huge PV power plants, it is desirable to enable controlling for all of them. Possibility to monitor and management of PV systems is important for maintaining of the power system (PS) stability in certain situations, or when overload and malfunctions on PS parts occurs [1]. Generated electrical energy from PV panels is a function of sun irradiation, sun position relative to the panel, ambient temperature and panel efficiency. Direct current (DC) electrical energy at the PV panel output goes to the charge controller and inverter inputs. These devices use maximum power point tracking (MPPT) algorithm to extract maximum power from the PV system. Inverter output is alternating current (AC) connection to the grid. Besides production of active power, inverter can compensate or produce reactive power also [2].

Measurement and communication devices at PV systems locations (distributed devices) are the basic elements of the M&M system distributed network. Sensors and other devices connected to these devices continuously send information about parameters values. These data must be modified to the formats of Transmission Control Protocol/Internet Protocol (TCP/IP) architecture that are suitable for transmission over computer network. Connection between distributed devices and M&M center can be implemented using fiber optical infrastructure, wireless links, satellite links or power line communication (PLC). Depending on PV system installed power and significance for the PS, communication resources are different. Timestamps in the network time protocol (NTP) headers enable time synchronization between central part of the SCADA system and distributed devices, through network, while global navigation satellite system (GNSS) provide timing and location information for every distributed device in the system, using satellite communications.

The paper is organized as follows. Chapter two refers to the SCADA system infrastructure and functionalities. Design of the core network for the central part of the SCADA system as well as time synchronization system are presented in chapter three. Communication protocols used between devices at central and distributed locations, as well as between these devices and network devices are described in chapter four. In chapter five are considered security aspects of the SCADA system and network. Finally, the conclusion summarizes proposed designs and refers to the future work.

II. Design and Functionalities of the SCADA System

All SCADAs are industrial systems that monitor and control distributed devices from central site. In this paper, SCADA that incorporates wide area monitoring system (WAMS) will be analyzed [3]. One part of this system are PMUs on high voltage levels [4] and micro PMUs on medium and low voltage levels [5]. Key difference between

Paper received December 25, 2024; accepted December 27, 2024. Date of publication December 31, 2024. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Zoran Čiča.

This paper is revised and expanded version of the paper presented at the 32nd Telecommunications Forum TELFOR 2024 [22].

This work was financially supported by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia under contract number: 451-03-65/2024-03/200103.

Ivan Vujović is PhD student at Department of Power Systems School of Electrical Engineering, University of Belgrade, Belgrade, Serbia.
Mladen Koprivica is with Department of Telecommunications School of Electrical Engineering, University of Belgrade, Belgrade, Serbia.
Željko Đurišić is with Department of Power Systems School of Electrical Engineering, University of Belgrade, Belgrade, Serbia.

PMUs and remote terminal units (RTUs) that are part of the original SCADA system, is that in addition to magnitude of the voltage, or current, phase values are measured also. Measurement resolution is significantly higher when PMUs or micro PMUs are in use.

The central part of the SCADA system is presented in Fig. 1. It is a system installed on IaaS Cloud [6]. All information and commands pass through core network. Cloud switches are layer 3 devices in the TCP/IP stack which connects all parts of the cloud system together in one big, logical part, while SCADA switches, that are also layer 3 devices, connect internal components of the central part of the SCADA system. Three most important virtual machines for SCADA system that works using hardware and software resources of multiple redundant nodes (servers), are: master terminal unit (MTU), human machine interface (HMI) and database (DB). Virtual platform is connected with SCADA switches through which pass all traffic related to M&M system. Data exchange with storage system is realized through fiber channel (FC) switches. Processed information are sent to the storage, for future use. At the same time, these data are real time visualized and available for monitoring [7]. All connections between devices are established using optical fibers.

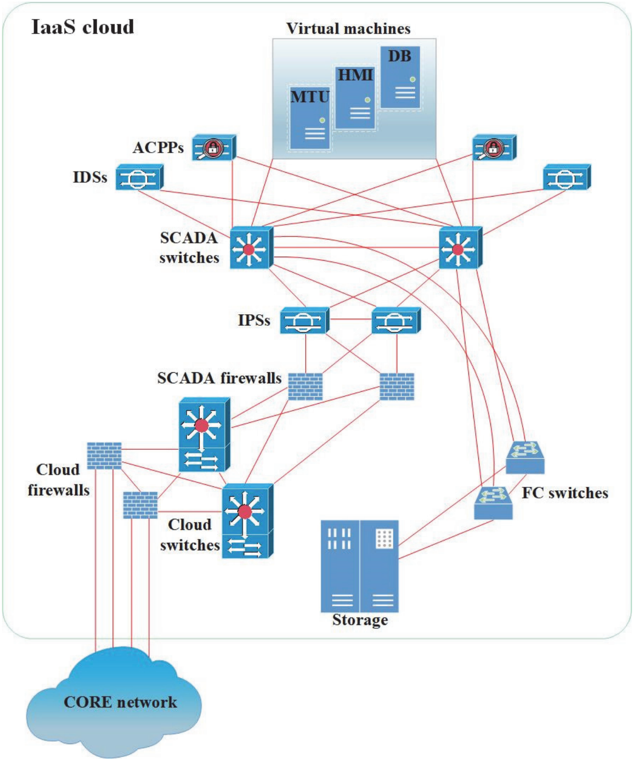

Fig. 1. Central part of the SCADA system

Functionalities of the SCADA system for distributed PV systems are presented in the Fig. 2. Data from the field devices (mostly sensors, relays and measurement transformers) and inverters are sent, through acquisition process, to the IoTs, IEDs and micro PMUs that collect information and communicate with central part of the SCADA system [8].

Data goes further, through acquisition interface, towards MTU, and, when it is necessary to present information directly from the field, through presentation interface, towards HMI. Data are processed on the MTU and sent to the DB and DB storage (historical DB) and to HMI for live presentation. Communication between MTU and: HMI, DB, DB storage must be enabled in both directions, because MTU sometimes needs information from these devices for the purpose of further processing. The HMI can directly take data from DB and DB storage and present information at any time.

As a central device for control of the SCADA system functionality, MTU sends commands to distributed control devices in the system (IoTs and IEDs). Communication goes through control interface to these devices. Further commands flow goes to the field devices (mostly actuators and relays) and inverters. If inverter has NIC and adequate software, communication between PV system and MTU can be established directly, based on TCP/IP architecture. Inverter sent information directly to MTU and execute commands received directly from MTU.

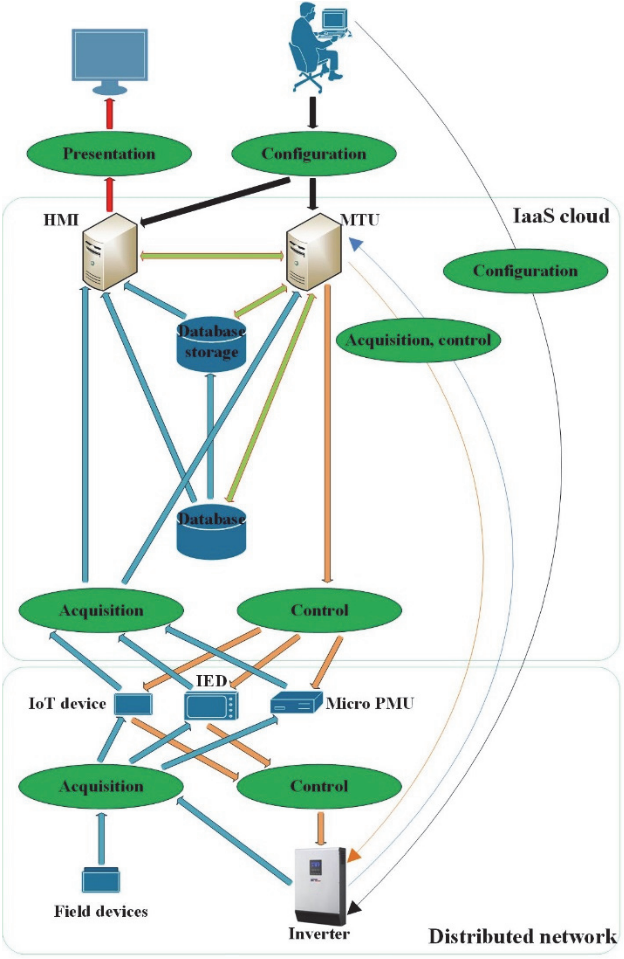

Fig. 2. SCADA functionalities for distributed PV systems.

The control of the inverter enables the whole PV system to be put in the desirable operation mode (active or reactive power production or compensation) and to adjust MPPT algorithm so that the PV system generates as much power as is needed at that moment and that is, generally, less then maximum.

At any moment it is suitable that all devices can be accessed from the central location of the SCADA system. The point from which that can be done is, usually, MTU. It is desirable to enable direct access to HMI also. Inverter can be accessed also directly, through configuration interface.

III. Design and Functionalities of the SCADA Core Network and Time Synchronization System

In Fig. 3 is presented solution for SCADA core network. Fast, network layer, multiprotocol label switching (MPLS), core switches, connect SCADA system IaaS cloud to the other parts of the network, while core switches for communication with external networks connects services providers and disaster recovery site (DRS) with SCADA system IaaS cloud, through switches, gateways (routers) and firewalls. There are redundant firewalls for both connections (with service providers networks and DRS network). Because connections to the distributed sites are realized using service providers networks, gateways are in use, while routers are in use for communication with DRS because connection to DRS is established using links that are proprietary. In normal conditions, links between DRS and service providers are inactive. They are in function only when central part of the SCADA system doesn't work. Monitoring and control devices in distributed network are connected to the SCADA system IaaS cloud through access switches for communication with service providers, while DRS links are connected to the switches for communication with DRS.

To ensure services continuity, central part of the SCADA system must be implemented on DRS also [9]. It is necessary to replicate DB, in the live time, between central location and DRS because, all data that are collected from the distributed devices and processed on MTU may be very important at any time.

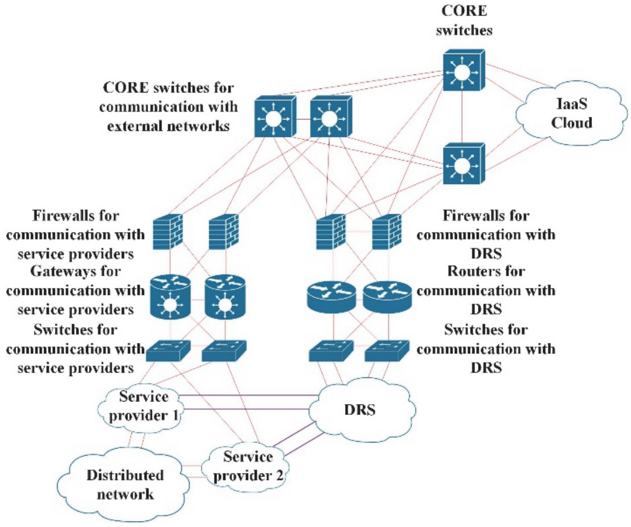
CORE
switches
CORE switches for communication with external networks
IaaS Cloud
Firewalls for communication with service providers
Gateways for communication with service providers
Switches for communication with service providers
Firewalls for communication with DRS
Routers for communication with DRS
Switches for communication with DRS
Service provider 1
DRS
Service provider 2
Distributed network

Fig. 3. Design of the SCADA core network.

Traffic in the SCADA network can be unicast or multicast. Unicast communication is in use when devices send data to MTU, or receive commands to perform some actions from MTU, or other devices. When a large number of devices, and, especially, large number of inverters must take some actions at once, it is preferable to use multicast communication. Basic communication scheme for time synchronization is presented on Fig. 4.

There are a few ways to achieve time synchronization [10]. Using NTP and one or more of the GNSS systems are most often. In the NTP hierarchy, root servers on the Internet are sources of the clock. Stratum of the server indicates the distance of the server from its original clock source [11]. In order to make the distribution of time in the SCADA system as accurate as possible, NTP appliances are implemented in Data center and on DRS. The clock sources for these appliances are Internet root servers with which connection is realized through networks and physical source (atomic clock, optical clock etc.) with which connection is realized using one of the GNSS systems [12]. These appliances are stratum 1.

All distributed devices have their own clock but accuracy of that clock is not satisfactory. Because of that, outside clock source is necessary for time correction when error is too high. Clock is sent to the distributed devices from NTP appliances, through SCADA network. If communication between central SCADA system and distributed devices doesn't functioning, synchronization of the distributed devices is achieved using GNSS system.

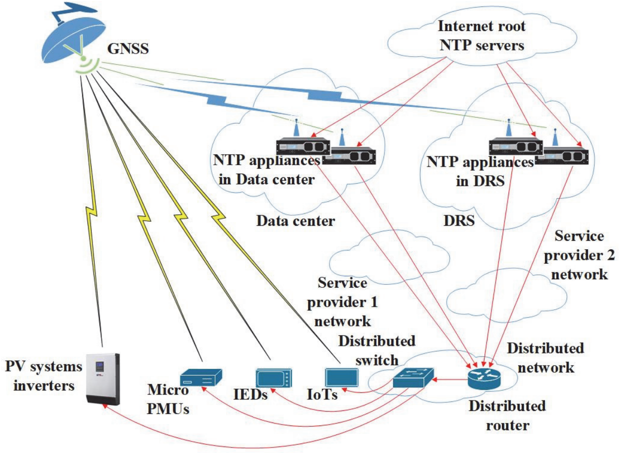

Fig. 4. Time synchronization system

IV. Communication Between SCADA Core, Network Devices and Distributed Devices

When field devices send data or receive commands from distributed devices, or when distributed devices send data to the SCADA system, or receive commands from the SCADA system, it is necessary to use communication standards and protocols. In Fig. 5 are presented most important standards and protocols that SCADA uses for the PV systems M&M. With L1-L4 on the right side of the figure are labeled layers in the TCP/IP architecture. On the bottom of the figure are layers: L1-L3 that represent SCADA system layers [13].

Standards and protocols are:

- Power line communication (PLC) is IEEE.901 standard that defines data transmission over AC power lines at the same time that current flow through conductors.
- 10 gigabit symmetric passive optical network (XGS-PON) is ITU-T G.9807.1 standard that defines 10 Gb/s symmetric communication through optical fibers.
- Dense wavelength-division multiplexing (DWDM) is technology for backbone communication over optical networks using frequencies defined in ITU-T G.694.1 standard.
- New radio (NR) is 5G, 3rd Generation Partnership Project (3GPP), radio access technology that uses gNodeB as an interface to the cellular network.

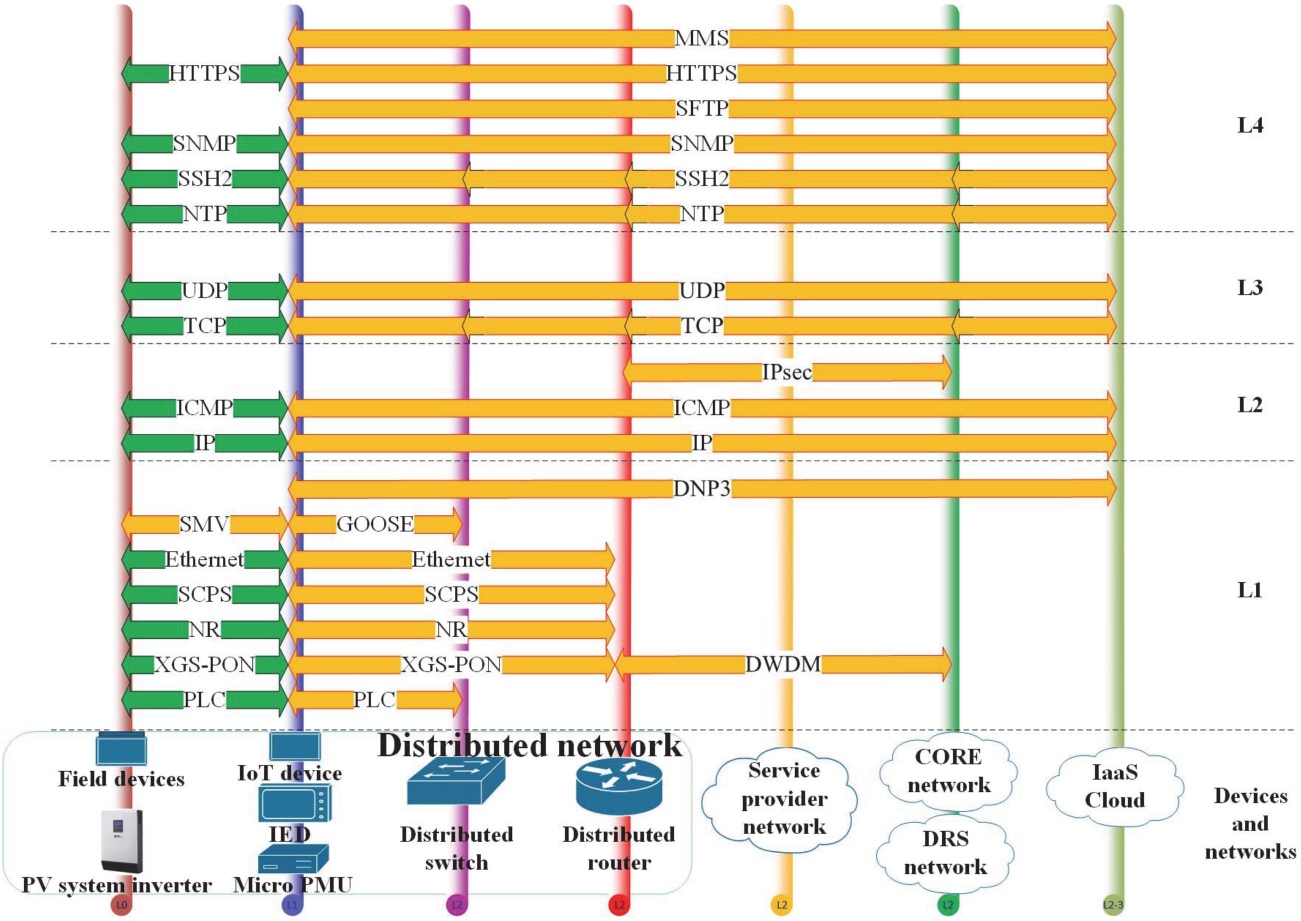

Fig. 5. Protocols in SCADA system and network

- Space communications protocol specifications (SCPS) is described in ISO 15893 standard and represent set of the protocols for space and satellite IP communication.
- Ethernet covers group of IEEEs standards which define communication on network access layer in the TCP/IP architecture.
- Sampled measured values (SMV) protocol is defined in the IEC 61850-9-2 standard and refers to digitalization of the measured values from field devices. Values of current and voltage phasors, temperature, humidity etc. as analog parameters are constantly measured and sent to the distributed monitoring devices. Digital values are relays signals, switch breaker position etc. These status information are sent when changes occurs. All data are sent as multicast traffic.
- The generic object-oriented substation event (GOOSE) protocol is defined in the IEC 61850-8-1 standard and describe fast transmission of important, real time, signals between IEDs or IoT control devices within one substation which includes multiple PV systems. Information are sent as multicast traffic.
- Distributed network protocol version 3 (DNP3) is defined in IEEE P1815 standard. This protocol defines communication between MTU and distributed control devices. Standard IEEE P1815.2 is extension of previous standard to distributed energy resources (in this case PV systems). Usually, MTU send commands or messages to IED and IoT devices, or to inverters in PV systems and they respond according to the requests.
- Network and transport layer protocols: IP, TCP and user datagram protocol (UDP) serve as a base for all application protocols and there is no need to explain how they work.
- Internet control message protocol (ICMP) is defined in IETF RFC 792. The main purpose of this protocol is to continuously check communication availability of distributed devices and PV systems invertors in the discrete periods of time.
- Internet protocol security (IPsec) is defined in IETF RFC 4301. This protocol specifies encrypted and authenticated communication between two network devices that use IP (in this case between SCADA core network and network devices at distributed sites).
- Network time protocol (NTP) defined in IETF RFC 5905 and precision time protocol (PTP) defined in IEEE 1588-2019 provides all devices time synchronization over the network. While NTP uses unicast and multicast mode, PTP uses only multicast.
- Secure shell version 2 (SSH2) defined in IETF RFC 4254, Remote authentication dial-in user service (RADIUS) defined in IETF RFC 2865 and 2866, Terminal access controller access-control system plus (TACACS+) defined in IETF RFC 8907 are in use for secure access from dedicated server in SCADA core network to the network devices, SCADA distributed devices and PV systems invertors.
- Simple network management protocol version 3 (SNMP 3) is defined in IETF RFC 3411-3418. This protocol

describes processes of collecting and organizing data about network devices, distributed devices and PV systems invertors status. To interpret messages, protocol use management information base (MIB) specified in IETF RFC 2578.

- Secure file transfer protocol (SFTP) provides file access, transfer and management in a secure manner, using SSH2 protocol. Files can be device operating software, software patches, configurations, etc.
- Hypertext transfer protocol secure (HTTPS) defined in IETF RFC 2660 enables access to the network devices, distributed devices and PV systems inverters using browser in secure manner.
- Manufacturing message specification (MMS) defined in ISO 9506-1 standard provides a mechanism that allows distributed devices and PV systems invertors to send reports, logs and files to the MTU or HMI.

V. Security of the SCADA System and Network

Cloud system and network can be target for many potential malicious attacks and different mitigation techniques can be used to suppress those attacks [14]. There are four primary vulnerability factors that cloud based SCADA systems facing: connectivity with cloud services, shared infrastructure, malicious insiders, and security of the SCADA protocols [15]. Traditional SCADA systems were quite isolated from the other services and communication networks. By moving SCADA systems to public cloud, the system become more vulnerable to everything that can affect all other services in the cloud. Nobody can guarantee that resources in the cloud will not be shared with other services. Persons with privileged access to any part of the cloud, locally or remote, can cause malicious attack on the system or can delete data by mistake. Some protocols that are in use for communication in the SCADA system (IEC 61850 standard protocols and DNP3) don't use encryption and authentication techniques. The solution for named vulnerabilities is private SCADA cloud.

Because high security demands related to cloud infrastructure, internal cloud firewalls are implemented between core network and cloud switches as presented in Fig. 1. To ensure that SCADA system functioning securely, separated from other services in the cloud, SCADA firewalls are implemented between central part of the SCADA system and the rest of the cloud. Full traffic inspection to and from virtual machines and storage system is accomplished by adding intrusion prevention system (IPS) and intrusion detection system (IDS) [16]. For inspection of the access to the network devices, access control policy platforms (ACPPs) are implemented [17]. In the [18]-[20] are described solutions to achieve cyber security for distributed devices (IoT, IED and PMU respectively), while [21] describes solution to achieve cyber security for inverters in the distributed energy resources (DERs) which include PV systems.

Logical segmentation of the network can be achieved using virtual local area network (VLAN) technologies. Software components of devices in the network must be regular update and upgrade. All communication between devices in the cloud and distributed devices must be authenticated and encrypted. Access to the internal resources from the Internet must be authenticated and encrypted also. All events, on any device in the cloud, distributed devices or network devices, as well as access attempts to the SCADA system must be recorded, in the form of logs, on central location and DRS. Communication with service providers and other outside entities must be established using virtual private network (VPN) tunnels.

VI. Conclusion

Distributed PV systems are increasingly present in the power system, with different installed powers, on different voltage levels, and on wide geographic area. It is very useful to have the possibility for monitoring and control all these systems from one or two locations. This can be achieved by implementing SCADA solution for distributed PV systems.

There are three main parts of the SCADA system as described in [22]. Central part is cloud in which are located: MTU that is main controller for all processing and operations in the system, HMI whose role is to present information gathered from distributed devices or from MTU in real time and DB which stores processed data. Field devices send measured values of specified parameters to distributed devices while PV system inverters can send data through distributed devices or directly to MTU. Distributed devices convert data in the IP format and send them to the MTU and HMI. Control commands go in opposite direction. From MTU to distributed devices and then to field devices, or PV systems invertors. Commands can also be sent directly from MTU to inverters.

Fast and secure transport of IP packets in the SCADA system is task for the network. Network is segmented and segments are independently protected. Besides the central part of the network and distributed network, DRS network is in use also. All parts of the SCADA system must be time synchronized. Protocols of communication between devices in the cloud and distributed devices, or PV system inverters are strictly defined. Security mechanisms to protect distributed devices, PV systems inverters, communication process, SCADA cloud and the network itself should be widely applied.

By getting measurement values more often i.e. with higher resolution, additional useful data can be collected and processed. By using obtained data and additional data from outside of the SCADA system, especially from PS SCADAs and meteorological center, neural network algorithms can predict most of the unwanted events that enables preventive actions.

References

[1] I. Vujović, M. Koprivica, Ž. Đurišić, “Centralized controling of the distributed PV systems using cloud and IoT technologies,” *Telfor Journal*, vol. 15(2), pp. 38–43, December 2023.

[2] F. L. Albuquerque, A. J. Moraes, G. C. Guimaraes, S. M. R. Sanhueza, A. R. Vaz, “Photovoltaic solar system connected to the electric power grid operating as active power generator and reactive power compensator,” *8th Latin-American congress on electricity generation and transmission – CLAGTEE*, pp. 1–6, Ubatuba, Brazil, December 2009.

[3] D. Kato, H. Horii, T. Kawahara, “Next-generation SCADA/EMS designed for large penetration of renewable energy,” *Hitachi Review*, vol. 63(4) , pp. 151–155, September 2014

[4] A. G. Phadke, T. BI, “Phasor measurement units, WAMS, and their applications in protection and control of power systems,” *Journal of Modern Power Systems and Clear Energy*, vol. 6, pp. 619–629, July 2018.

[5] E. Dusabimana, S-G Yoon, “A Survey on the micro-phasor measurement unit in distribution networks,” *Electronics 2020*, vol. 9(2), 305, Februray 2020.

[6] N. Serrano, G. Gallardo, J. Hernantes, “Infrastructure as a Service and cloud technologies,” *IEEE Software*, vol. 32(2), pp. 30–36, March 2015.

[7] G. Yadav, K. Paul, “Architecture and security of SCADA systems: A review,” *International Journal of Critical Infrastructure Protection*, vol. 34, 100443, pp. 1–26, September 2021.

[8] S. Hopkins, E. Kalaimannan, “Towards establishing a security engineered SCADA framework,” *Journal of Cyber Security Technology*, vol. 3(1), pp. 47–59, March 2019.

[9] N. Dhanujati, A. S. Girsang, “Data Center-Disaster recovery center (DC-DRC) for high availability IT service,” *International Conference on Information Management and Technology (ICIMTech)*, pp. 1–9, Jakarta, Indonesia, September 2018.

[10] Z. Idress, J. Granados, Y. Sun, S. Latif, L. Gong, Z. Zou, L. Zheng, “IEEE 1588 for Clock Synchronization in Industrial IoT and Related Application: A Review on Contributing Technologies, Protocols and Enhancement Methodologies,” *IEEE access*, vol. 8, pp. 155660–155678, August 2020.

[11] T. Rytilahti, D. Tatang, J. Kopper, T. Holz, “Masters of Time: An Overview of the NTP Ecosystem,” 3rd IEEE European Symposium on Security and Privacy, pp. 122–136, London, United Kingdom, April 2018.

[12] S. Jin, Q. Wang, G. Dardanelli, “A Review on Multi-GNSS for Earth Observation and Emerging Applications,” Remote Sens. 2022 vol. 14(16), 3930, August 2022.

[13] M. D. Stojanović, S. V. B. Rakas, J. D. M. Petrović, “SCADA systems in the cloud and fog environments: Migration scenarios and security issues,” *Facta Universitatis, series: Electronics and Energetics*, vol. 32(3), pp. 345–358, September 2019.

[14] N. Amara, H. Zhiqui, A. Ali, “Cloud computing security threats and attacks with their mitigation techniques,” *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 244–251, Nanjing, China, October 2017.

[15] A. Wali, F. Alshehry, “A Survey of Security Challenges in Cloud-Based SCADA Systems,” *Computers*, vol. 13(4), 97, pp. 1–19, April 2024.

[16] S. Alam, M. Shuaib, A. Samad, “A Collaborative Study of Intrusion Detection and Prevention Techniques in Cloud Computing,” *International Conference on Innovative Computing and Communications (ICICC), Lecture Notes in Networks and Systems*, vol. 55, pp. 231–240, New Delhi, India, May 2019.

[17] M. Penelova, “Access control models,” *Bulgarian academy of sciences, Cybernetics and information technologies*, Vol. 21(4), pp. 77–104, Sofia, Bulgaria, September 2021.

[18] K. Kimani, V. Oduol, K. Langat, “Cyber security challenges for IoT-based smart grid networks,” *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36–49, June 2019.

[19] J. Wang, D. Shi, “Cyber-Attacks Related to Intelligent Electronic Devices and Their Countermeasures: A Review,” *53rd International Universities Power Engineering Conference (UPEC)*, pp. 1–6, Glasgow, United Kingdom, September 2018.

[20] A. Sundararajan, T. Khan, A. Moghadasi, A. I. Sarwat, “Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies,” *Journal of Modern Power Systems and Clean Energy*, vol. 7(3), pp. 449–467, May 2019.

[21] N. D. Tuyen, N. S. Quan, V. B. Linh, V. V. Tuyen, A. G. Fujita, “A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy,” *IEEE Access*, vol. 10, pp. 35846–35875, April 2022.

[22] I. Vujović, M. Koprivica, Ž. Đurišić, “Infrastructure for distributed PV systems monitoring and management using SCADA,” In Proceedings of the *32nd Telecommunications Forum (TELFOR)*, Belgrade, Serbia, November 2024