ISO/IEC 30144

Edition 1.0 2020-10

INTERNATIONAL STANDARD

colour inside

Internet of things (IOT) – Wireless sensor network system supporting electrical power substation

ISO/IEC 30144:2020-10(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

ISO/IEC 30144

Edition 1.0 2020-10

INTERNATIONAL STANDARD

Internet of things (IOT) – Wireless sensor network system supporting electrical power substation

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 29.240.10; 35.110

ISBN 978-2-8322-8941-9

CONTENTS

INTERNET OF THINGS (IOT) – WIRELESS SENSOR NETWORK SYSTEM SUPPORTING ELECTRICAL POWER SUBSTATION

FOREWORD

1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.
2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO National bodies.
3) IEC and ISO documents have the form of recommendations for international use and are accepted by IEC and ISO National bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC and ISO documents is accurate, IEC and ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC and ISO National bodies undertake to apply IEC and ISO documents transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC and ISO document and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC and ISO do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC and ISO marks of conformity. IEC and ISO are not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this document.
7) No liability shall attach to IEC and ISO or their directors, employees, servants or agents including individual experts and members of its technical committees and IEC and ISO National bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this ISO/IEC document or any other IEC and ISO documents.
8) Attention is drawn to the Normative references cited in this document. Use of the referenced publications is indispensable for the correct application of this document.
9) Attention is drawn to the possibility that some of the elements of this ISO/IEC document may be the subject of patent rights. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 30144 has been prepared by subcommittee 41: Internet of Things and related technologies, of ISO/IEC joint technical committee 1: Information technology.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
JTC1-SC41/163/FDIS	JTC1-SC41/176/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

The data collected from various types of electrical equipment is sparsely located, and on-line transmission of the data helps to collaboratively aggregate and analyse them in real-time. Transitioning to the smart electrical power substation using wireless communication among the sensor nodes – i.e. wireless sensor network (WSN) – requires systems architecture provisioning automated data collection from the electrical equipment, which allows collaborative data processing, sends automatic alerts, provides preventive actions, and potentially takes corrective actions for certain situations.

Electrical power substation communications should be designed to support scalability, interoperability, autonomous fault correction, and other key attributes. The intelligent wireless sensor network (iWSN) is inherently flexible and scalable in its capabilities and in operations including in the size of its converge areas; however, depending on the geographical (e.g. urban, suburban, remote location) and structural (both natural and man-made) situations, the installation architecture should ensure the fidelity of all sensor nodes' wireless connectivity. Furthermore, the WSNs can support either distributed or decentralized network architecture. The wired substation network typically uses high-availability seamless ring (HSR) and parallel redundancy protocol (PRP) protocols (see IEC 62439-3, IEC 61850-8-1 and IEC 61850-9-2) to provide seamless failover against failure of any network component. For the iWSN, it is also important to have the key iWSN network components (e.g. sensor nodes) from data communication failure. Therefore it is important to select wireless sensor network architecture for a substation which overcomes the potential issue of a single point of failure in the wireless sensor network, for example, by installation architecture, the use of PRP to improve packet loss and timing behaviour in wireless network, or a combination of these.

This document introduces iWSN as a system which helps to make the power substation smarter, which is compatible with IEC 61850. In the past, wireless communication was thought to be unreliable and ineffective over long distances. With the advancements in communication technologies in the last decade, the wireless communications have given rise not only to wireless meshed systems, multi-hop and self-healing networks, but also to various low-power protocols having high network/communication security standards. Additionally, different network topologies with effective wireless signal routing algorithms have improved range and reduced power consumption while minimizing frequency of communication channel error. These improvements can be leveraged to form a highly reliable communication network for the electrical power substation.

The existing applications of the WSNs in smart grid include, but are not limited to, automatic meter reading, remote system monitoring and control, equipment fault diagnostics, distribution automation, outage detection, line fault and electronic fault detection, underground cable system monitoring, towers and poles monitoring, conductor temperature and dynamic thermal rating. However, the realization of these existing and envisioned WSN-based smart grid applications is hindered by not having uniform sensing data formats, data interfaces, etc. Although some sensor communication systems are not compatible with the devices from different equipment manufacturers, most intelligent electronic devices used in electrical power substations are interoperable, through the use of standard protocols, for example, IEC 61850 GOOSE, TCP, UDP, etc., and standards related to the common information model (CIM) defined by IEC 61970 and IEC 61968. For cases where new types of sensors (either existing or newly developed) have not adopted IEC 61850, they may be used with an intelligent wireless sensor network (iWSN) system[1] [2] because the iWSN system interfaces can act as an adaptor for the sensors and the rest of the systems.

---

1 Wireless technology in general is not suitable for the transmission of mission critical data such as sampled measured values according to IEC 61850-9-2 or trip signals for circuit breakers due to the possible interference of electromagnetic radiation caused by arc-flashes (e.g. in case of an internal fault or switching operations inside a substation) with the radio signals of wireless sensors.

2 Any data commonly sent over layer 2 broadcast (e.g. GOOSE) are not suitable for transmission over wireless networks due to the unavailability of corresponding broadcast features.

The main purpose of wireless sensor network applications for electrical power substations is to improve the capability of acquiring, monitoring, processing, and maintaining the data and information from the power equipment. A wireless sensor network (WSN) is characterized by flexible deployment, device collaboration and low-cost implementation, and WSN realizes efficient monitoring of the smart grid systems and subsystems. By enabling the monitoring and controlling capabilities by installing wireless sensor nodes on critical power grid equipment, reliable and real-time online management of this equipment can be accomplished.

Electrical power substation is one of the most important building blocks of the smart grid. The monitoring and control systems in electrical power substations acquire current, voltage, status and other parameters from their primary equipment, and also data from their environment. The information from the measurement systems provides the basis for integrated applications, enabling the transformation of a conventional electrical power substation to a smart electrical power substation, especially when considering the use of the IEC 61850 series, iWSN and other information technologies. In addition to the substation equipment's (wired) connectivity, which is likely based on the IEC 61850 series, the iWSN system will provide additional benefits to collect, process, and transmit data/information about power substation equipment and its environment. An effective and efficient sensing system can be achieved by an iWSN system which takes the role of a data/information measurement and collection system. The concept of the iWSN system provides functions, such as automatic data collection and aggregation, collaborative information processing (e.g. data/information fusion), data analysis, and alarming, and other functional applications that enable the intelligence or smartness of the system that the iWSN system is monitoring.

The information collected in an electrical power substation about the equipment state and the flow of electricity provides the electricity providers with a clearer view and better control over the electrical power substation. Among the many add-values that the iWSN brings compared to the wired installation, one of them is the migration to the no-wire installation as all the sensor nodes are powered by batteries and the data is transmitted via the wireless communication links of the iWSN. A wireless sensor network that is able to communicate with the utility provider's control system by sharing the collected information with the existing networks becomes an attractive technology to deploy in an electrical power substation in order to collect required and critical information.

This document is built upon ISO/IEC 29182 (Sensor Network Reference Architecture) and ISO/IEC 30101 (sensor network and its interfaces for smart grid systems), IEC 61850 (communication networks and systems for power utility automation), and ETSI's and NIST's work in smart grid, and extends ISO/IEC 29182 and ISO/IEC 30101 to the application standard of the sensor network that supports the electrical power substations.

The iWSN system uses wireless sensor networks for power substations including substation, equipment, facility, environment, etc. The existing communication protocols specified in IEC 61850-8-1 and IEC 61850-9-2 can be used within power substation, or IEC 61850-8-2 can be used over public network. This document provides the iWSN system's infrastructure from System and Communications Views and also specifies the iWSN system's technical requirements to realize and support the smart electrical power substation. Electrical power substations with sensor networks use advanced information and communication technologies in order to improve the efficiency, reliability, and security of their components and services.

INTERNET OF THINGS (IOT) – WIRELESS SENSOR NETWORK SYSTEM SUPPORTING ELECTRICAL POWER SUBSTATION

1 Scope

This document specifies

– intelligent wireless sensor network (iWSN) from the perspectives of iWSN's system infrastructure and communications internal and external to the infrastructure, and

– technical requirements for iWSN to realize smart electrical power substations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61000-4-39, *Electromagnetic compatibility (EMC) – Part 4-39: Testing and measurement techniques – Radiated fields in close proximity – Immunity test*

IEC 61326-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 1: General requirements*

IEC 61850-3, *Communication networks and systems for power utility automation – Part 3: General requirements*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
control subsystem for sensor network
CSSN
platform together with all the sensor nodes communicated to it with networks, including the rules for control, for communication and for management among application processes of sensor network

[SOURCE: IEC 60050-732:2014, 732-10-02, modified – In the definition, "home network", "devices" and "attached to it" have been replaced by "platform", "sensor nodes" and "communicated to it with networks", respectively, and "of sensor network" has been added at the end.]

3.2
control subsystem for power substation
CSPS
infrastructure together with all the equipment attached to it, including the rules for control, for communication and for management among application processes of a power substation

[SOURCE: IEC 60050-732:2014, 732-10-02, modified – In the definition, "home network" and "devices" have been replaced by "infrastructure" and "equipment", respectively, and "of a power substation" has been added at the end.]

3.3
data acquisition functional subsystem
DAFS
subsystem for gathering required data from a group of sensors, and assembling them into messages for delivery to another component

[SOURCE: IEC 60050-721:1991, 721-18-64, modified – In the definition, "a facility", "small quantities of" and "a nominated group of addresses" have been replaced by "subsystem", "required" and "a group of sensors", respectively, and "a single message" and "nominated address" have been changed to "messages" and "component", respectively.]

3.4
intelligent wireless sensor network
iWSN
system of spatially distributed sensor nodes interacting with each other using wireless communication technology and, depending on applications, possibly with other infrastructure in order to acquire, process, transfer, and provide information extracted from its environment with a primary function of information gathering, analysing, fusing, and possible control capability to support the intelligent services based on the application scenarios and users

[SOURCE: ISO/IEC 29182-2:2013, 2.1.6, modified – In the definition, "using wireless communication technology" and "analysing, fusing," have been added, and "to support the intelligent services based on the application scenarios and users" has been added at the end.]

3.5
sensor network for electrical power substation
system of spatially distributed sensor nodes interacting with each other and, depending on electrical power substation applications, possibly with other infrastructure in order to acquire, process, transfer, and provide information extracted from electrical power substation's equipment and environment with a primary function of information gathering and possible control capability

[SOURCE: ISO/IEC 29182-2:2013, 2.1.6, modified – In the definition, "electrical power substation" has been added in front of applications, and "its environment" has been replaced by "electrical power substation's equipment and environment".]

3.6
smart electrical power substation
part of an electrical system, confined to a given area, mainly including ends of transmission or distribution lines, electrical switchgear and control gear, buildings and transformers, and generally including safety or control devices (for example protection), with the infrastructures and technologies of digital information, network communication and shared information to collect data, measure, detect and protect the electrical system, possibly support online analysis, decision-making, collaborative interaction, and real-time control

[SOURCE: IEC 60050-601:1985, 601-03-02, modified – "a" has been removed from the beginning, and "A. substation generally includes" is replaced by "and generally including". "network communication and shared information to collect data, measure, detect and protect the electrical system, possibly support online analysis, decision-making, collaborative interaction, and real-time control" is added in the end of the definition.]

3.7
reliability
ability to perform as required, without failure, for a given time interval, under given conditions

[SOURCE: IEC 60050-192:2015, 192-01-24]

3.8
availability
property of being accessible and usable on demand by an authorized entity

Note 1 to entry: IoT systems can include both human users and service components as "authorized entities".

[SOURCE: ISO/IEC 27000:2018, 3.7]

4 Symbols and abbreviated terms

ASD	Application and Service Domain
CAN	controller area network
CIP	collaborative information process
CSPS	control subsystem for power substation
CSSN	control subsystem for sensor network
CT	current transformer
DAFS	data acquisition functional subsystem
DER	distributed energy resource
EMF	electromagnetic field
GIS	gas isolated switchgear
GOOSE	generic object oriented substation event
HMI	human–machine interface
IED	intelligent electronic device
iWSN	intelligent wireless sensor network
LoRaWAN™	long range wide area network
OLTC	on load tap changer
MMS	manufacture message service
MTBF	mean time between failures
MTTF	mean operating time to failure
MTTFF	mean operating time to first failure
NB-IoT	narrow band Internet of Things
ONVIF	open network video interface forum
OTA	over the air
PD	partial discharge
PED	Physical Entity Domain

PSIA	Physical Security Interoperability Alliance
RTU	remote terminal unit
SCADA	supervisory control and data acquisition
SCD	Sensing and Controlling Domain
SF_6	sulfur hexafluoride
SNRA	Sensor Network Reference Architecture
SV	sample value
UD	User Domain
VT	voltage transformer
XML	extensible markup language

5 Intelligent wireless sensor network system supporting electrical power substation

5.1 System View

5.1.1 System overview

The iWSN system for electrical power substation is composed of subsystems which include sensor nodes, meters, cameras, and gateways, communication network, and control subsystem for sensor network (CSSN). The iWSN system collects data (system operation status, etc.) from electrical equipment and substation environment, and transmits the data wirelessly to be processed, aggregated and/or analysed for effective and efficient monitoring of the electrical power substation in real-time. The iWSN system contributes to the automation of the operation and management of the substation especially by feeding it with appropriate data, but also provides the electricity providers with a clearer operating picture of the substation and better automated control through supervisory control and data acquisition (SCADA). In addition, with consideration for sensor and actuator interoperable communication interfaces and common sensor and actuator data for sharing and exchanges between networks and systems, interoperability in electrical power substation operations should be achieved. Consequently, the application of the iWSN system results in a smart electrical power substation through interactive operations, self-healing, safer and securer environment, and so on. The system overview of the iWSN system supporting electrical power substation is depicted in Figure 1. In Figure 1, SCADA, control centre and control subsystem for power substation (CSPS) are only shown to provide the relationship with iWSN, but SCADA, control centre and CSPS are neither in the scope nor discussed in this document.

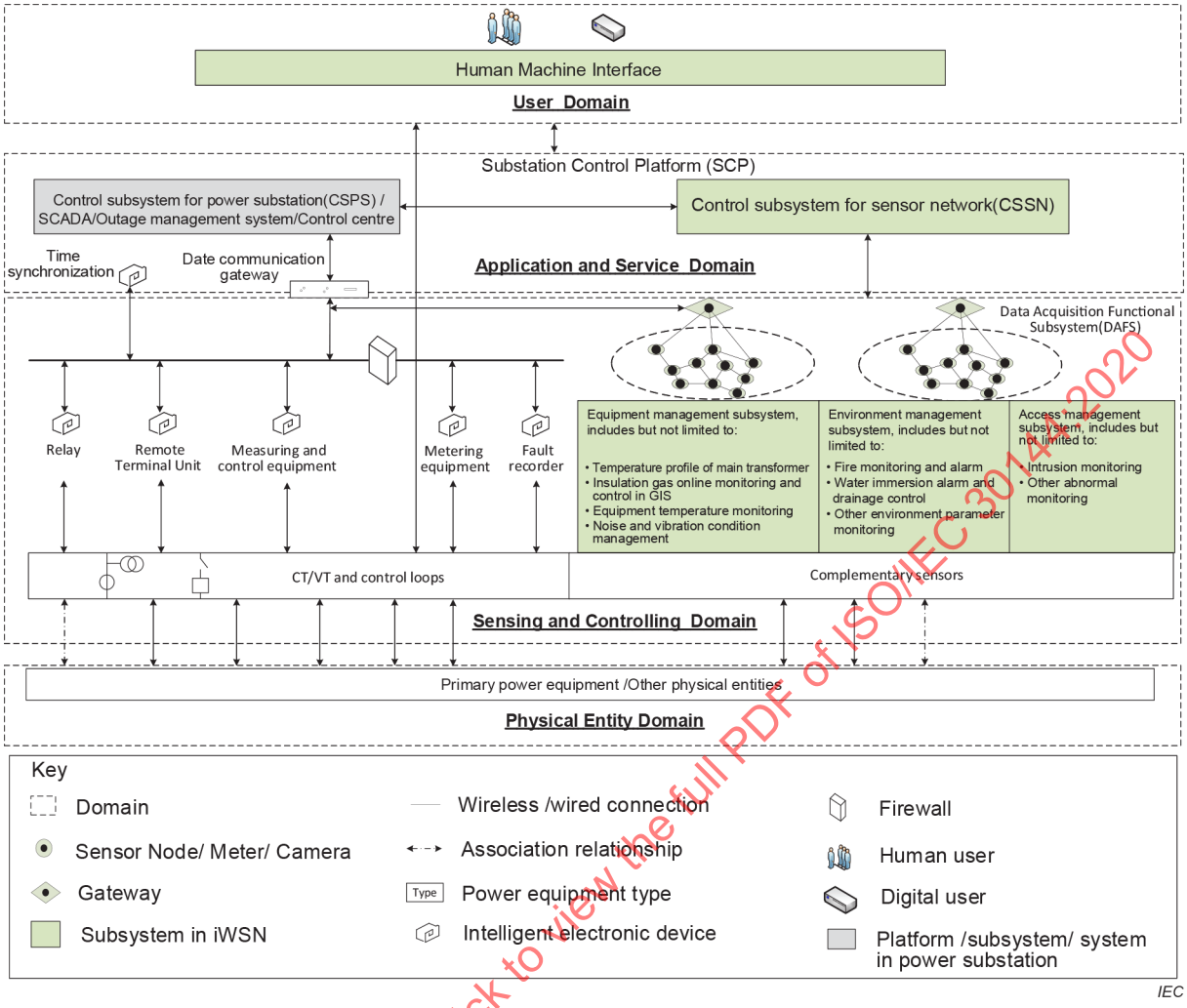


Figure 1 – System overview of the iWSN system supporting electrical power substation

As shown in Figure 1, in principle, the iWSN system's System View supporting electrical power substation follows the Sensor Network Reference Architecture (SNRA) described in ISO/IEC 29182. Figure 1 resulted from applying and tailoring the SNRA (see Figure A.1) supporting electrical power substation monitoring. Figure 1 shows the entire sensor network system that is used to improve the substation's intelligence and automated system performance. Sensor nodes (see Figure A.3) in Figure 1 are attached to power equipment or placed in the substation to monitor the equipment and environmental status. The sensor nodes with different type of sensors and communication modules are used for electrical power substations, and they are listed in this document. The entire functional models of the iWSN system comply with those of the SNRA (see Figure A.4). Interfaces of SNRA, layer focus model, sensor node physical reference architecture and functional models of the sensor network are shown in Annex A.

The iWSN systems are used for monitoring the electrical equipment, environment, access management, and other parameters in electrical power substations, and also provide numerous other services depending on the needs of specific users. An iWSN system consists of sensor nodes, gateways, and various types of the iWSN system's subsystems. It also includes a platform for managing the iWSN system that has a graphical user interface.

Since the iWSN system supporting electrical power substations is one of the application scenarios of Internet of Things, it also follows the Internet of Things Reference Architecture (IoT RA, ISO/IEC 30141). The mapping relationship between the entities in the iWSN system's System View (see Figure 1) and the domains of the IoT RA is shown in Table 1.

In Table 1, the four domains of the IoT Reference Architecture (see ISO/IEC 30141) are mapped and included in the iWSN system supporting electrical power substation. They are Physical Entity Domain (PED), Sensing and Controlling Domain (SCD), Application and Service Domain (ASD), and User Domain (UD). The main conception and functions for the domains are as follows.

Physical Entity Domain (PED): The PED mainly consists of sensed physical objects and controlled physical objects, which are related to IoT applications and are of interest to users. A sensed physical object is a physical entity from which information is acquired by sensors, while a controlled physical object is a physical entity which is subject to actions of actuators. electrical equipment, and the environment of the power substation are in the PED.

Sensing and Controlling Domain (SCD): In the SCD, the entities consist primarily of sensors, actuators, and IoT gateways. Sensors sense properties of physical entities while actuators change properties of physical entities. Sensors acquire information about a property of a physical entity (e.g. physical, chemical, biological properties). Actuators change properties of entities. Both sensors and actuators interact with physical entities independently or collaboratively. IoT gateways are devices which connect SCD with other domains. IoT gateways provide functions such as protocol conversion, address mapping, data processing, information fusion, certification, and equipment management. IoT gateways should be either independent equipment or integrated with other sensing and controlling devices. The IoT gateway should also perform security functions for constrained IoT devices using the gateway for connectivity to networks. The SCD might also contain local control systems which are used to run control services, i.e. components for local management of IoT gateway capabilities in scenarios where the IoT gateway is expected to work with or without upstream connectivity. DAFS is included in the SCD.

Application and Service Domain (ASD): The purpose of the ASD subsystem is to host the core functions, services and applications that deliver the IoT system functionality to the users (human and/or digital). The ASD subsystem will provide mainly basic services, including computing services such as data access, data processing, data fusion, data storage, identity resolution, geographic information service and user management, and inventory management. The ASD subsystem will also host business services and applications built on the generic services, as the ability to host applications will be one of the services provided by the IoT systems. CSSN is included in the ASD.

User Domain (UD): The UD contains both human users and digital users. Digital users are devices of some type and they interact directly with other entities in the IoT system via network interfaces or application programming interfaces. Human users interact using a user device which contains some form of human–machine interface (HMI). A HMI subsystem contains the devices and supporting software that allow human users to interact with the IoT system. Depending on user role, different aspects of the system will be presented for observation and/or control. Human users such as managers or operators of a power substation are included in the UD.

Table 1 – Mapping between the entities in the System View and the domains of the IoT RA

System View of the iWSN system supporting electrical power substation	Internet of Things Reference Architecture
DAFS	Sensing and Controlling Domain (SCD)
CSSN	Application and Service Domain (ASD)
Electrical equipment, and environment of the power substation	Physical Entity Domain (PED)
Managers or operators of power substation	User Domain (UD)

5.1.2 Subsystems and their relationships

In Figure 1, the substation control platform (SCP) contains two subsystems: (1) control subsystem for sensor network (CSSN); and (2) control subsystem for power substation (CSPS). These subsystems should be interconnected with the data acquisition functional subsystem (DAFS) which contains the sensor nodes, controller(s) and gateways deployed for the electrical power substations.

The existing substation system typically consists of the electrical equipment, intelligent electronic devices (IEDs), and CSPS of the substation control platform. The electrical equipment in the power substation mainly includes primary electrical equipment, current transformer / voltage transformer (CT/VT) and control loops, and other sensors such as (but not limited to) insulation, displacement, temperature, pressure, and humidity. IEDs include relays, remote terminal units (RTUs), measuring and control devices, metering equipment, fault recorders, engineer working stations and communication gateways, and these devices are connected by cable networks or fibre-optic networks in substations. A typical IEC 61850 based substation automation system architecture consists at least of a station bus and may use process bus to communicate with intelligent process equipment. Communication services like MMS (Manufacturing Message Specification), GOOSE (Generic Object Oriented Substation Event) or SV (Sampled Values) are applied onto the station bus and/or process bus in accordance with project requirements. The CSPS of the substation control platform is able to control, protect and monitor electrical equipment inside the substation and the connected electrical grid. Information security in substations is provided according project specific implementation plans following security assessments e.g. by implementing firewalls, white-listening, intrusion detection systems, etc.

The associated and connection relationship between the iWSN and the existing substation system is shown in Figure 1. With regard to the local communication connectivity between DAFS and the sensor information in the substation, as shown in Figure 1, the sensor information should be shared at the local level within the SCD or through the CSSN within ASD. However, the existing substation systems are neither within scope nor defined or discussed in this document. The iWSN system should provide the measurement information of inherent and additional measurements, but the strength of the iWSN system is in its flexibility in sensor node deployment in a substation and in sensing diversity, enabling to measure various kinds of parameters from equipment as well as from the substation's environment, for example temperature of the equipment or of one of its parts, SF_6 leakage, partial discharge, humidity, temperature, wind, water immersion, and fire. The measured parameters need to be associated to analytics either on a physical element (e.g. sensor node or sensing device), on the DAFS (e.g. gateway), on the CSSN, or on the CSPS (e.g. platform, cloud).

The iWSN system is composed of the DAFS and the CSSN, as shown in Figure 1. The DAFS includes, but is not limited to, the following examples of management subsystems.

a) Equipment management subsystem: This subsystem collects the parameters of the equipment such as transformer temperature, insulation gas (e.g. SF_6), partial discharge, solid insulation, temperature of the switch cabinet, other assisted parameter, etc. For example:

   1) Temperature profile of main transformer: Infrared thermal imager is used to monitor the overall temperature distribution of the main transformer. The temperature profile of the main transformer is analysed intelligently and alarmed if it is out of the normal ranges.

   2) Insulation gas (e.g. SF_6) online monitoring and control in gas isolated switchgear (GIS): For example, a double infrared gas sensor is used to detect the insulation gas leakage. If the leakage is detected, the alarm signal is sent to initiate the automatic exhaust ventilation.

3) Equipment temperature monitoring: The wireless sensor node for measuring temperature is used to monitor the operating temperature of some part of the high-voltage electrical equipment such as the joint, sleeve and capacitor cell, and transmit the data through wireless communication technologies to perform data report and analysis. By fusing and comparing the temperature differences between different phases of the same equipment, comparing the differences among the similar equipment, and also comparing with the temperature of the environment, flexible equipment operation temperature management is realized, and the accurate alarm for the equipment fault is achieved.

4) Noise and vibration condition management: The wireless sensor nodes for noise and vibration condition management and measurement are added to manage and measure the condition of the devices for equipment management subsystem.

b) Environment management subsystem: This subsystem collects the data of temperature, wind, lighting, water immersion, fire and other information in the environment. The potential iWSN system application model examples are defined in condition monitoring (see IEC 61850-7-4 and IEC TR 61850-90-3) and in environment monitoring (see IEC TR 61850-90-6), etc.

NOTE Additional information on sensor models already in IEC 61850 is given in Annex B.

For example:

1) Fire monitoring and alarm: Data from video surveillance cameras, infrared thermal image detector and smoke alarm is collected and aggregated to achieve the fire monitoring and alarming with high reliability.

2) Water immersion alarm and drainage control: The wireless sensor node for water immersion is deployed in the plant and on the cable to detect the water leakage and water immersion, and transmit the data through wireless communication technologies to perform data report and analysis, so as to realize on-line monitoring and automatic drainage control for substation.

3) Other environment parameter monitoring: Wireless sensor nodes for temperature, humidity and other environment parameters are used to monitor the environment of key areas in the substation, such as the indoor and terminal box, and transmit the data through wireless communication technologies to perform a comprehensive analysis, judgment and alarm. Sensor nodes for ozone measurement should be added to detect the ozone in the room for environment management subsystem. Furthermore, the environmental information is aggregated with information of flooding and video surveillance to achieve highly credible alarm for the status in the substation.

c) Access management subsystem: This subsystem detects the intrusion of the enclosure, door and windows in the building, other abnormal entrance, etc. For example, Intrusion monitoring: Infrared device, cameras, and other types of sensor nodes are used to collect information of electronic fence, infrared radiation, wall vibration and video surveillance. All of the information is aggregated and analysed to prevent outside intrusion and alarmed if the intrusion is detected.

The management subsystems described above contain different sensors, sensor nodes, communication protocols, and gateways based on the separate functions. The sensor and sensor nodes are deployed on or in the electrical equipment, and closely associated with that equipment depending on the acquisition information and characteristics. Sensor nodes and gateways, which are the physical entities for the functional subsystems, are described in 5.2.

The CSSN is connected with the CSPS and integrated in the substation control platform (SCP). The CSSN shall realize the following functions:

– collect the data from individual DAFS;

– perform data processing, analysis and fusion. A cloud system including database, servers and applications for analysis may be used as a part of the CSSN, in which data analysis will produce information about quality, efficiency and availability of the power substation performance;

– provide the connectivity to the CSPS;

– present the integrated fusion information from the DAFS;

– provide the complete functions for the iWSN system, such as monitoring the operating temperature of the equipment, temperature and humidity of the environment, leakage of SF_6, intrusion detection, and fire detection, which provide corrective, timely controls and maintain the substation in good operating conditions.

5.2 Communications View

5.2.1 Communications overview

Communications View is essential for a sensor network deployed in electrical power substation. It gives guidelines to set up wirelessly connected sensor networks for electrical power substations. The wireless communication architecture should be in line with the global reference architecture depicted in IEC TR 62357-1.

Communications View is depicted by physical entities with communication units and the communication interfaces between the physical entities as shown in Figure 2. For the iWSN system supporting the electrical power substation, the physical entities include, but are not limited to, sensors, controllers, gateways, and servers for comprehensive functions. Communication interfaces include communication links and communication protocols to enable the data transmission and reception. The detailed description of physical entities and communication interfaces is given in 5.2.

The information from sensor nodes already considered by the IEC 61850 semantic data models will be modelled according to IEC 61850. The usage of the data models of sensor nodes refers to IEC 61850-7-4 and IEC 61850-90-3.

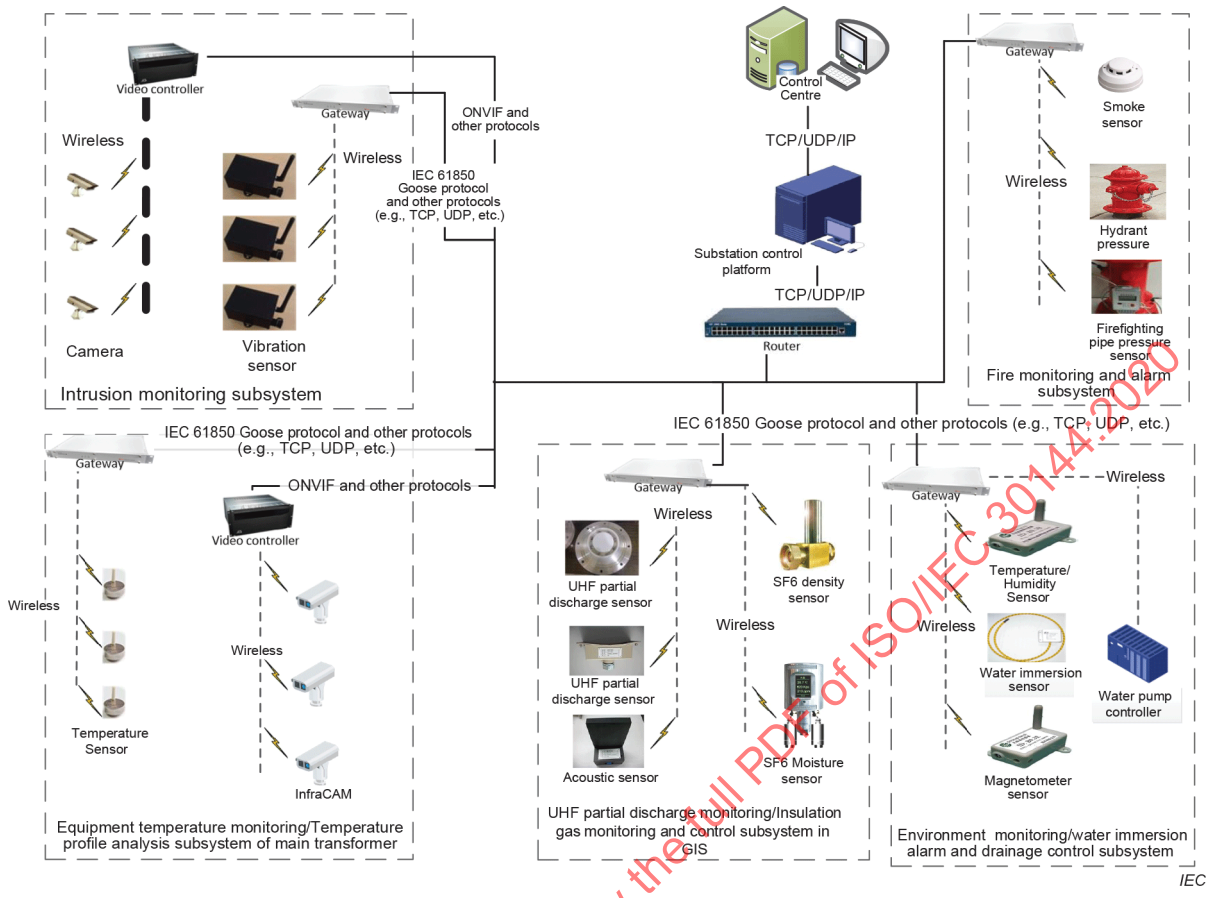


Figure 2 – Communications overview of the iWSN system supporting electrical power substation

5.2.2 Sensor nodes

Sensor nodes of the iWSN system used in electrical power substation can be divided into two groups.

1) Sensor nodes installed on power equipment

   Sensor nodes installed on power equipment can be usedt to monitor electrical and non-electrical parameters including voltage, current, discharge, electrical distance, arrester leakage current, leakage current of transformer core, current transformer (CT) leakage current, etc. In the installation of the iWSN system, each sensor node shall be placed on equipment without affecting its operation and safety of that equipment. The user of this document shall refer to the relevant standard for the equipment, for example IEC 62271 for high-voltage switchgear, to know the exact operational and safety requirements applying to the concerned power equipment. Here the typical sensor nodes installed on the power equipment include but are not limited to the following.

   – Sensor node on GIS: A gas insulated switchgear (GIS) is power equipment for disconnecting the power equipment from the power lines when the electrical fault or maintenance of power lines occurs. Sensor node on GIS is for monitoring the insulating medium, such as SF_6 or other insulated gas mixture in GIS.

   – Sensor node on transformer: Various types of sensors are installed to monitor the parameters of power transformer which include infrared temperature sensor, cooling oil quality sensor, acoustic sensor to detect potential damage on the transformer, dissolved gas and moisture in the oil, partial discharge (PD), temperature monitoring, solid insulation, bubbling temperature, bussing, cooling, and other assisted monitoring, etc.

– Sensor node for on-load tap-changer (OLTC): Sensors need to be installed to monitor the OLTC condition status, such as operation property, operational counting, contact abrasion, oil temperature of OLTC, and operation of oil filter unit, etc.

2) Sensor nodes installed on plant field

Sensor nodes installed on plant field, especially in the important locations and fences to monitor the environment, fire, and plant security, include the following types according to the characteristics.

– Sensor nodes for environment monitoring: Sensor nodes monitor the environmental information, such as temperature, humidity, atmospheric pressure, and rainfall, heating, cooling, wind velocity, wind direction, electromagnetic field (EMF) and pollution monitoring, etc. IEC 61850-3 may be used to set thresholds for the environmental sensor data to provide alarms and warnings either at the sensor node level or at the iWSN system level.

– Sensor nodes for fire monitoring and controlling: Sensor nodes monitor the fire, smoke, fire-fighting pipe pressure, water immersion, water level, and drainage, etc., and send the data to the CSSN, control centre, and/or CSPS for issuing warning and response messages if any abnormality is detected (see 6.1.5).

– Sensor nodes for monitoring the security of the enclosure: Sensor nodes monitor via video, vibration, and infrared radiation of the enclosure, etc.

5.2.3 Gateways

Gateways perform two functions for the sensor networks connecting to the substation control platform. One is data format transformation from the various sensor data to the unified data format, and the other is communication protocol transformation. The gateways are integrated with the substation communication network especially for some critical information such as the key information for main transformer. With the infrastructure-based networks, NB-IoT, 5G, LoRaWAN™[3], etc., the gateways can also be integrated with or collocated at a server or at the network/Web service providers.

The information security and network security of the gateways shall be performed, such as device access authentication and the network security protocols.

Cryptography shall be used to ensure the integrity, confidentiality and non-repudiation of the information transmitted between sensor nodes and the gateways.

Data format transformation refers to the standards of the unified description of sensors such as XML on sensors, or tailors and leverages the existing standards, for example, IEC TR 61850-90-2.

Communication protocol transformation performs the following protocol transformations.

– Communication protocols for gateway and sensor node: Wireless communication protocols are Zigbee®[4], Bluetooth®[5], LoRaWAN, NB-IoT, 5G, etc.

---

[3] LoRaWAN is a trademark of the LoRa Alliance. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC.

[4] ZigBee is a registered trademark of ZigBee Alliance. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC.

[5] Bluetooth is a registered trademark of Bluetooth SIG, Inc. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC.

– Communication protocols for cameras and video controller for sensor network: open network video interface forum (ONVIF®[6]), Physical Security Interoperability Alliance (PSIA), etc.

– Communication protocols for gateway and CSSN: IEC 61850 series, IEC TR 61850-90-12 for wide area communication network, TCP/IP, and UDP can be used.

5.2.4 Communication interfaces in the iWSN system

Subclause 5.2.4 describes the wireless interfaces for functional subsystem of iWSN system, and Table 2 describes each interface in iWSN. Certain cases, such as the location of equipment causing wireless signal blockage due to the structure and/or material surrounding it, may require a wired connection to the sensor node on the equipment.

Table 2 – Interface for functional subsystem of sensor networks

Functional subsystem	Entity 1 (Various types of sensors in the iWSN's functional subsystem)	Entity 2 (Gateway or video controller in the iWSN's functional subsystem)	Interface descriptions
Temperature profile analysis subsystem of main transformer	Infrared camera	Video controller	Wireless communication protocols
Intrusion monitoring subsystem	Camera	Video controller	Wireless communication protocols
	Vibration sensor	Gateway	Wireless communication protocols
Fire monitoring and alarm subsystem	Smoke sensor	Gateway	Wireless communication protocols
	Hydrant pressure sensor	Gateway	
	Firefighting pipe pressure sensor	Gateway	
Water immersion alarm and drainage control subsystem	Water immersion sensor	Gateway	Wireless communication protocols
	Water pump controller	Gateway	Wireless communication protocols
Insulation gas monitoring and control subsystem in GIS	SF_6 density sensor	Gateway	Wireless communication protocols
	SF_6 moisture sensor	Gateway	Wireless communication protocols
	Ultra high frequency (UHF) partial discharge sensor	Gateway	Wireless communication protocols
	Acoustic sensor	Gateway	
Equipment temperature monitoring subsystem	Temperature sensor	Gateway	Wireless communication protocols
	Infrared camera	Video controller	Wireless communication protocols
Environment monitoring subsystem	Temperature/humidity sensor	Gateway	Wireless communication protocols
	Water immersion sensor	Gateway	
	Magnetometer sensor	Gateway	

6 ONVIF is a registered trademark of Onvif, Inc. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC.

6 Technical requirements for the iWSN system supporting electrical power substations

6.1 System functional requirements

6.1.1 Information acquisition and collection

The iWSN collects the appropriate set of data coming from the sensor nodes connected to the entities in and around power substation, for example, environment and equipment. Identity authentication shall be used when collecting information from the sensor nodes; for example, uniform address coding rules for different sensor nodes.

– Sensor node collects the data from its connected sensor(s).
– Gateway collects the data from its connected sensor node(s) and transmits them to CSSN.
– CSSN obtains data from sensor nodes and gateways.

6.1.2 Device management

Device management and maintenance for four types of devices in the substations shall be provided:

– monitoring device including sensor nodes and transmission device, etc.;
– electrical equipment under monitoring including main transformer, circuit breaker, and electrical cable, and auxiliary device including fire protection device, water supply and drainage device, etc.;
– integrated type of device, which is the smart device combined with the electrical device and monitoring unit by itself;
– gateways or controllers in the subsystems.

6.1.3 Data analysis

The collected data shall be analysed not only with the model of monitored equipment, but also with the equipment's context of use and mission profile along with the equipment's operating history and statistics in order to determine the state of the equipment or system based on the following:

– the position of the given sensor within its context;
– the real-time history and statistical information of the equipment state and working environment, such as equipment temperature, electrical parameter, water immersion, etc.;
– the equipment's context of use and mission profile, which is used for assisting decision, alarm, system collaborative control, etc.

6.1.4 Data display

The collected data from DAFS may be displayed. The display data may include information like temperature, humidity, key equipment operational status and parameters, ventilation-drainage-hydrant status and video monitoring stream.

The data display can be centralized and real-time, based on the layout of the substation and equipment distribution map of auxiliary control system. The display may use trend diagrams, two-dimension tables, and statistical analysis charts. The type of the HMI and the technology applied is depending on project requirements and out of scope of the standard.

6.1.5 Warning and response

The warning data comes from two origins: one is directly from the DAFS, and another is from CSSN, based on the processed and analysed data received from DAFS.

The warning data should be classified and shown in the control centre dynamically based on various emergencies. Analysed and response data would be produced to reset or to send back the command according to the specific situation. All the warning and response data should be recorded for history query and analysis.

The availability and timeliness of the warning and response information for some subsystems are essential according to the requirements of the substation management and should be guaranteed by other special standards, for example the fire monitoring and alarm subsystem.

6.1.6 Network communication

The network communication shall be required for the sensor nodes, gateways and CSSN. See 5.2 for the detailed description.

6.1.7 System privilege management

System privilege management is to manage the personnel and their authorities in the organization, and it shall be done for the operation security in the substation. System privilege management may refer to IEC 62351. System privilege management includes personnel management and authority management.

Personnel management shall be responsible for the basic information and authorities of the personnel in the organization.

Authority management is to configure the different rights to access data and operate in terms of the type of user. The personnel in the organization should be authorized to be a certain type of user.

6.1.8 Collaborative information process (CIP) and decision support

CIP can be used to support decision making. Functions that rely on CIP, include but are not limited to, the following.

– Enclosure security monitoring: Data of wall vibration, electronic enclosure, and video of the region is used in CIP to judge if a person breaks in illegally. If this happens, the control subsystem shall alarm or take action.
– Fire monitoring: Data of smoke, location, temperature, and video of the region is used in CIP to judge if there is a fire. If there is a fire in the location, the control subsystem shall alarm and/or start a hydrant system, or any other type of fire-fighting system.
– Water immersion monitoring: Data of water immersion, water level and video of the region is used in CIP to judge if the equipment is soaked in water. If it is, the control subsystem shall alarm or start water drainage.

6.2 System performance requirements

6.2.1 Performance requirements of sensor node

6.2.1.1 Working conditions

The working conditions of sensors used in the power field shall comply with the operation conditions defined in IEC 60721-3-3 (for stationary use at weather protected locations) and IEC 60721-3-4 (for stationary use at non-weather protected locations). If these standards are not applicable for a certain sensor or sensor node, a study shall be carried out to determine the appropriate operational conditions for it.

In certain cases, where the study cannot be performed, the sensor nodes should operate as specified in the following general environmental conditions.

– Temperature: −25 °C and +70 °C.
– Atmospheric pressure: 70 kPa to 106 kPa.
– Relative humidity: 0 % to 93 %, without condensation.

6.2.1.2 Enclosure protection

Enclosure protection should comply with the IP65 of IEC 60529 for outdoor use when sensor node is exposed to severe conditions and if the characteristic is measured with accuracy.

Enclosure protection should comply with the IP54 of IEC 60529 for indoor use when sensor node is exposed to severe conditions.

6.2.1.3 Working mode and working period

Sensor nodes are preferred to use wireless radio communication technology to communicate with others. Sensor nodes should be powered by batteries in normal situation or use renewable energy source if they are deployed outdoors, working in the mode of periodic sleeping and waking-up to save the electric power. The working period of a sensor node including the period sleeping and wake-up shall be less than the observing interval of the object which is being monitored.

6.2.1.4 Data accuracy level

The data accuracy defines the accuracy of the data measured by wireless sensor node for power substation. Data accuracy performance should be specified with several classifications.

– Class A: the data accuracy of sensor nodes which collect data is equal to or greater than 99 % and less than 100 % of the true value (i.e. less than 1 % measurement error).
– Class B: the data accuracy of sensor nodes which collect data is equal to or greater than 98 % and less than 99 % of the true value (i.e. between 1 % and 2 % measurement error).
– Class C: the data accuracy of sensor nodes which collect data is equal to or greater than 95 % and less than 98 % of the true value (i.e. between 2 % and 5 % measurement error).
– Class D: the data accuracy of sensor nodes which collect data is less than 95 % of the true value (i.e. greater than 5 % measurement error).

6.2.1.5 Working lifetime

The durability of the sensor node depends on the ability to withstand the environmental and operating conditions before a limiting state such as a failure, a wear-out failure, or a deviation of measured signal.

The durability of the sensor node shall be demonstrated under defined environmental and operating conditions. In addition, for the sensor node the theoretical value of power consumption, battery capacity and the self-discharge rate shall be considered.

Durability of the sensor node without maintenance cycle shall be defined. If the maximum durability of the sensor node requires maintenance cycle(s), the number of maintenance cycle(s) shall be specified.

6.2.1.6 Wireless communication frequency

The wireless communication frequency range shall support the communication protocols of sensor network. Wireless communication frequency shall comply with each national regulation. Examples of communication protocols include Zigbee, Bluetooth, LoRaWAN, NB-IoT, 5G, etc. The wireless communication frequency is used to comply with the wireless communication protocols of sensor network. The communication protocol of the wireless sensor networks and gateway should comply with the standard industrial communication protocols and have its own algorithm for data quality and integrity for the high-voltage substation environment.

6.2.1.7 Availability

The concept of availability is the property of being accessible and usable on demand by an authorized entity. IoT systems can include both human users and service components as "authorized entities". In the IoT systems, availability can be considered as a characteristic of devices, data, and services.

Availability requirements for sensor nodes (i.e. IoT devices) are to ensure that the devices are accessible and usable, including reliability, recoverability, and maintainability for the sensor nodes, which vary significantly especially if redundancy is involved.

The reliability of the sensor node shall be demonstrated under defined environmental and operating conditions. The reliability shall be a total time operated or a number of measurements made by a device at which a certain percentage of sensors has reached a limiting or inoperable state (e.g. time by which accumulated 5 % or 10 % of a population will fail for B5 or B10 life, respectively). However, other reliability assessments such as mean operating time to failure (MTTF), mean operating time to first failure (MTTFF) and mean operating time between failures (MTBF) are also used. MTBF, at the minimum, shall be greater than the maximum device maintenance interval in substations.

NOTE MTTF, MTTFF and MTBF are the measures of constant risk; therefore, they do not represent the expected time to failure. In the case of a non-repairable product, MTTFF equals MTTF. For products with an exponential distribution of operating times to failure (i.e. a constant failure rate), MTTF is numerically equal to the reciprocal of the failure rate. Mean operating time between failures is only applied to repairable products.

Maintainability: All devices or subsystems shall be repairable or recoverable within a specified time (which differs depending on the device or system) after any system-generated warning message is received prior to the actual failure. The repair or recovery shall not affect the substation's normal operations. For the critical devices and subsystems which affect the normal operations, the system shall have redundancies and substitutes for the critical devices and subsystems upon the failure without warning messages.

6.2.1.8 Electromagnetic compatibility (EMC)

The sensor nodes, other iWSN system components and their communications devices shall comply with IEC 61326-1 and IEC 61000-4-39 dealing with EMC immunity and emission, in order not to interfere with the existing equipment of the power substations and not to be disturbed by that equipment of the power substations.

6.2.1.9 Data communication latency

The wireless communication between various components shall meet commonly acceptable latency requirements for different types of traffic. The network design should comply with the network design considerations as described in IEC TR 61850-90-4. If the DAFS's subsystems important for safety are to be included, additional requirements on timeliness will arise.

6.2.1.10 Other requirements

General security requirements of the sensor nodes shall comply with IEC 61010-1 for electrical equipment for measurement, control and use.

When sensors or sensor nodes are placed on or in equipment, they shall comply with the environment defined for the equipment. For example, the sensors on a switchgear shall comply with the environmental conditions which are defined in IEC 62271-304.

Other requirements of sensor nodes not mentioned in this document are given in IEC 61850-3.

6.2.2 Performance requirements of gateway

6.2.2.1 Working conditions

The working conditions of gateways used in the power field shall comply with the operation conditions defined in IEC 60721-3-3 (for stationary use at weather protected locations) and IEC 60721-3-4 (for stationary use at non-weather protected locations). If these standards are not applicable, a study shall be carried out to determine the appropriate operational conditions for it.

In certain cases, where the study cannot be performed, the gateways should operate as specified in the following general environmental conditions.

– Temperature: −25 °C and +70 °C.
– Atmospheric pressure: 70 kPa to 106 kPa.
– Relative humidity: 0 % to 93 %, without condensation.

6.2.2.2 Enclosure protection

Enclosure protection shall comply with the IP65 of IEC 60529 for outdoor use when gateway is exposed to severe conditions and if the characteristic can be measured with accuracy.

Enclosure protection shall comply with the IP54 of IEC 60529 for indoor use when gateway is exposed to severe conditions.

6.2.2.3 Synchronization

The gateway shall synchronize with the CSSN by a command message. The accuracy of clock synchronization depends on the classes of the time accuracy requirements in the whole system, which shall refer to the standard IED synchronizing for control and protection events or instrument transformers in IEC 61850-5.

6.2.2.4 Data relevant requirement

The gateway shall be qualified for these functions:

– data processing, data storage, data transformation, and data response (see IEC TR 62357-1);
– communicating with sensor nodes or control subsystem.

6.2.2.5 Power supply

The gateway is powered by alternating current or direct current. When de-energized, the gateway shall be able to operate for five days. Renewable energy may be used.

6.2.2.6 Communication protocols

The following communication protocols may be used in communication for gateways:

– Downlink: Zigbee, Bluetooth, WiFi, LoRaWAN, NB-IoT, and other appropriate wireless communication protocols;

– Uplink: RS-485, CAN, Ethernet, and equivalent communication protocols or, if any, wireless secured communication protocols.

6.2.2.7 Availability

The concept of availability is the property of being accessible and usable on demand by an authorized entity. IoT systems can include both human users and service components as "authorized entities". In the IoT systems, availability can be considered as a characteristic of devices, data, and services.

Availability requirements for gateways (i.e. IoT devices) are to ensure that the devices are accessible and usable, including reliability, recoverability, and maintainability for the gateways, which vary significantly especially if redundancy is involved.

The reliability of the gateway shall be demonstrated under defined environmental and operating conditions.

The reliability shall be a time at which a certain percentage of the gateway has reached a limiting state (e.g. time by which accumulated 5 % or 10 % of a population will fail for B5 or B10 life, respectively). However, other reliability assessments such as mean operating time to failure (MTTF), mean operating time to first failure (MTTFF) and mean operating time between failures (MTBF) are also used.

NOTE MTTF, MTTFF and MTBF are measures of constant risk; therefore, they do not give the expected time to failure. In the case of a non-repairable product, MTTFF equals MTTF. For products with an exponential distribution of operating times to failure (i.e. a constant failure rate), MTTF is numerically equal to the reciprocal of the failure rate. Mean operating time between failures is only applied to repairable products.

Maintainability: All devices or subsystems shall be repairable or recoverable within a specified time (which differs depending on the device or system) after any system-generated warning message is received prior to the actual failure. The repair or recovery shall not affect the substation's normal operations. For the critical devices and subsystems which affect the normal operations, the system shall have redundancies and substitutes for the critical devices and subsystems upon the failure without warning messages.

6.2.2.8 Working lifetime

The durability depends on the ability of the gateway to withstand the environmental and operating conditions before a limiting state such as a failure, a wear-out failure, or a deviation of measured signal.

The durability of the gateway shall be demonstrated under defined environmental and operating conditions. In addition, for the gateway the theoretical value of power consumption, battery capacity and the self-discharge rate shall be considered to achieve the five days in operation when de-energized.

Durability of the gateway without maintenance cycle shall be defined. If the maximum durability of the gateway requires maintenance cycle(s), the number of maintenance cycles shall be specified.

6.2.2.9 Electromagnetic compatibility (EMC)

The gateway shall comply with IEC 61326-1 and IEC 61000-4-39 dealing with EMC immunity and emission, in order not to interfere with the existing equipment of the power substations and not to be disturbed by that equipment of the power substations.

6.2.2.10 Other requirements

Other requirements of the gateway not mentioned in this document are given IEC 61850-3.

6.2.3 Performance requirements of control subsystem for sensor network

6.2.3.1 Hardware

– The hardware of the control subsystem should be equipped with servers, special communication equipment, storage equipment and uninterruptible power supplies, and it is appropriate to be portable for mobile workstations operation.

– When alternating current power is cut-out, the normal working time of uninterrupted power supply shall be no less than 30 min.

6.2.3.2 Software

The software qualifications shall include safe and reliable operating system, multiple threads and multiple process working mode, and high concurrent processing ability.

6.2.3.3 Database

– An appropriate size of relational database or other non-relational database shall be selected based on the iWSN system requirements.

– Standardized interface in accordance with IEC 61360, ISO 13584-42 and IEC 62271-3 shall be provided to connect the database with other systems.

6.2.3.4 Data management

Data management capabilities shall support different types of data operations, including the following.

– Perform on-line monitoring data processing, off-line data analysis, database management, and user authority management.

– Perform data statistics, analyse, evaluate, output and display.

– Generate alerts based on alarm data, such as sound (aural) and light (visual).

6.2.3.5 Data storage

The large amount of monitoring and controlling data shall be stored in the database specified in 6.2.3.3.

6.2.3.6 Data protection and backups

Data protection and backups shall provide the following.

– The equipment shall have a protection function to prevent data loss in case of power failure.

– Database and application service programs shall be backed up periodically.

– The data being stored in storage devices shall be encrypted with a standard and/or approved encryption technique for data security prior to storing or when being stored.

6.2.3.7 Security protection

Security protections shall be quantified based on the risk of the specific deployment. This will typically involve a risk assessment or threat model. This activity will result in the identification of the necessary controls to be deployed including session encryption, authentication and access controls. It may also include capabilities such as over the air (OTA) updates to ensure that they follow a strict set of checks prior to flashing a device component in-field.

Security controls shall ensure all communications are secure and authenticated.

A security standard, for example, IEC 62351, should be used as reference in implementing the security protection for the iWSN system.

6.2.3.8 Availability

Availability is represented by availability ratio value (ARV). ARV is the percentage from mean time between failures (MTBF) divided by the sum of MTBF and MTTR (mean time to repair). MTBF, at the minimum, shall be greater than the maximum device maintenance interval of the CSSN in substations.

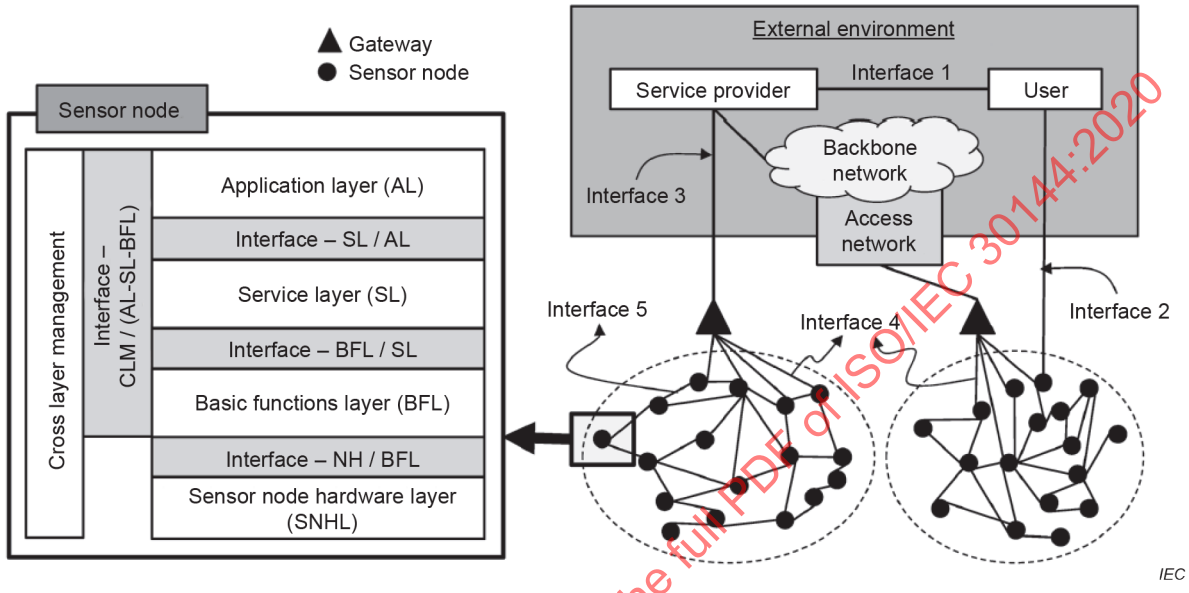
6.2.3.9 Accuracy of clock synchronization

The accuracy of clock synchronization depends on the classes of the time accuracy requirements in the whole system, which shall refer to the standard IED synchronizing for control and protection events or instrument transformers in IEC 61850-5.

Annex A
(informative)

Sensor network reference architecture from ISO/IEC 29182-3

A.1 Overview of sensor network interfaces



SOURCE: Figure 2 of ISO/IEC 29182-3:2014

Figure A.1 – Overview of sensor network interfaces in a sensor node, sensor node to sensor node, and sensor node to the external environment

Figure A.1 describes the sensor network reference architecture by identifying the main entities of sensor networks, and the interfaces between the main entities which make up a sensor network.

Sensor nodes and gateway have the same layers:

– hardware layer (SNHL);
– basic functions layer (BFL);
– service layer (SL);
– application layer (AL); and
– cross layer management (CLM).

External environment through access network and backbone network can connect to service providers and users.

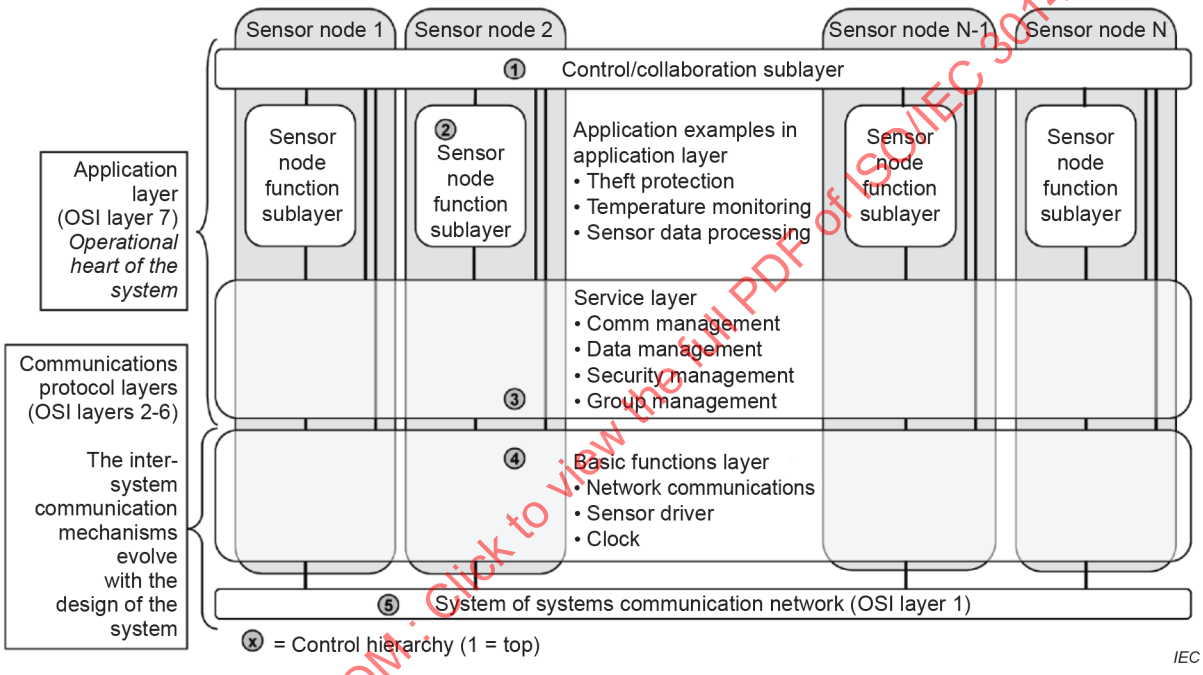
The interfaces between these main entities are illustrated by the lines indicated by Interfaces 1 through 5 in Figure A.1.

a) The interfaces within a sensor node are:
   - interface between sensor node hardware layer and basic functions layer (SNHL / BFL);
   - interface between basic functions layer and service layer (BFL / SL);
   - interface between service layer and application layer (SL / AL);
   - interfaces between cross layer management and applications layer, service layer, and basic functions layer (CLM / AL-SL-BFL).

d) Interface between a sensor node and a sensor node within a sensor network.

e) Interface between sensor network gateway node and other networks (ISO/IEC 29182-1).

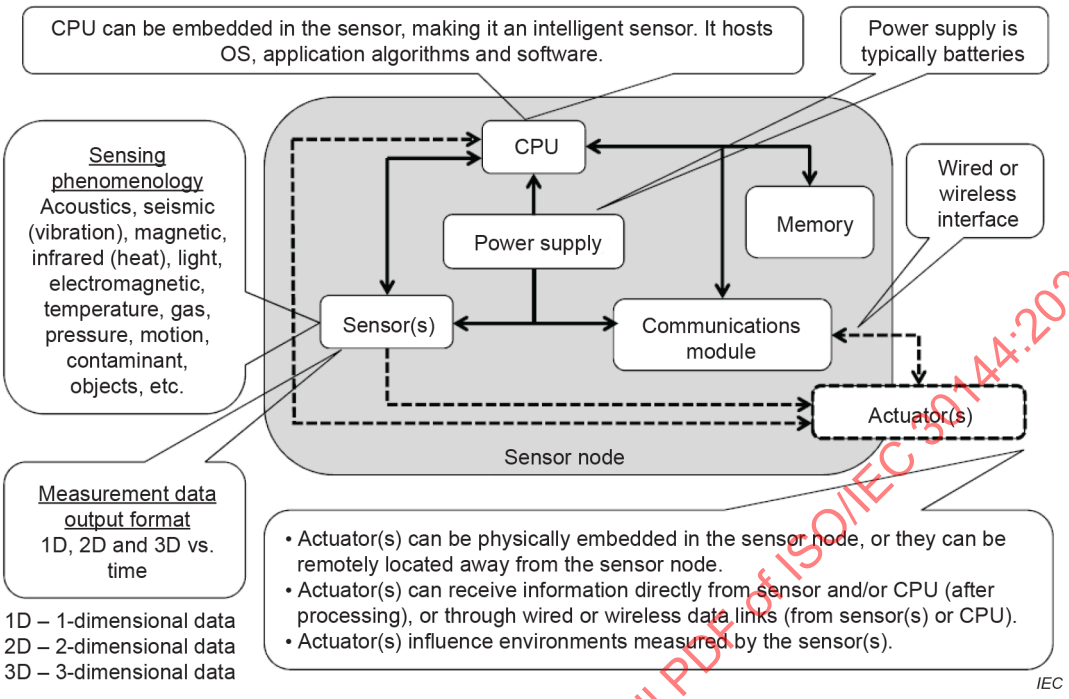
The layers in Figure A.1 can be linked to the OSI model in Figure A.2.



SOURCE: Figure 10 of ISO/IEC 29182-3:2014

Figure A.2 – Sensor networks system architecture – Layer focused

A.2 Sensor node physical reference architecture



SOURCE: Figure 3 of ISO/IEC 29182-3:2014

Figure A.3 – Sensor node physical reference architecture

Figure A.3 describes the physical architecture of a sensor node (ISO/IEC 29182), which can be mapped to a sensor node.

Hardware depicted in Figure A.2 represents the sensor node physical reference architecture. The sensor node physical reference architecture includes the following.

– Computer processing unit (CPU): A CPU embedded in a sensor node enables the node to become intelligent. It hosts an operating system (OS), application algorithms, and other software. A CPU could be located outside of a sensor node and a sensor node transmits its measurements to the CPU for processing.

– Storage: A storage device is a memory unit which can be embedded in a sensor node or can be located outside of the node. The memory unit stores various event data experienced by the node; for example, measurements, processed data if an on-the-node processing is performed, and other event data.

– Sensor: Sensor or sensing element is a measuring device of external environment of a certain phenomenology. Typically, this device converts raw measurements into a stream of measurable electrical signal. Depending on the type of a sensing device, the device can measure acoustics, seismic or vibration, magnetic, various light spectra (e.g. visual, infrared, etc.), electromagnetic (e.g. radio frequencies), temperature, gas, pressure, motion, contaminants, objects, etc. Depending on the complexity and technology implemented in the sensor, the sensor can measure 1-dimensional, 2-dimensional and 3-dimensional signals along with time tagging.

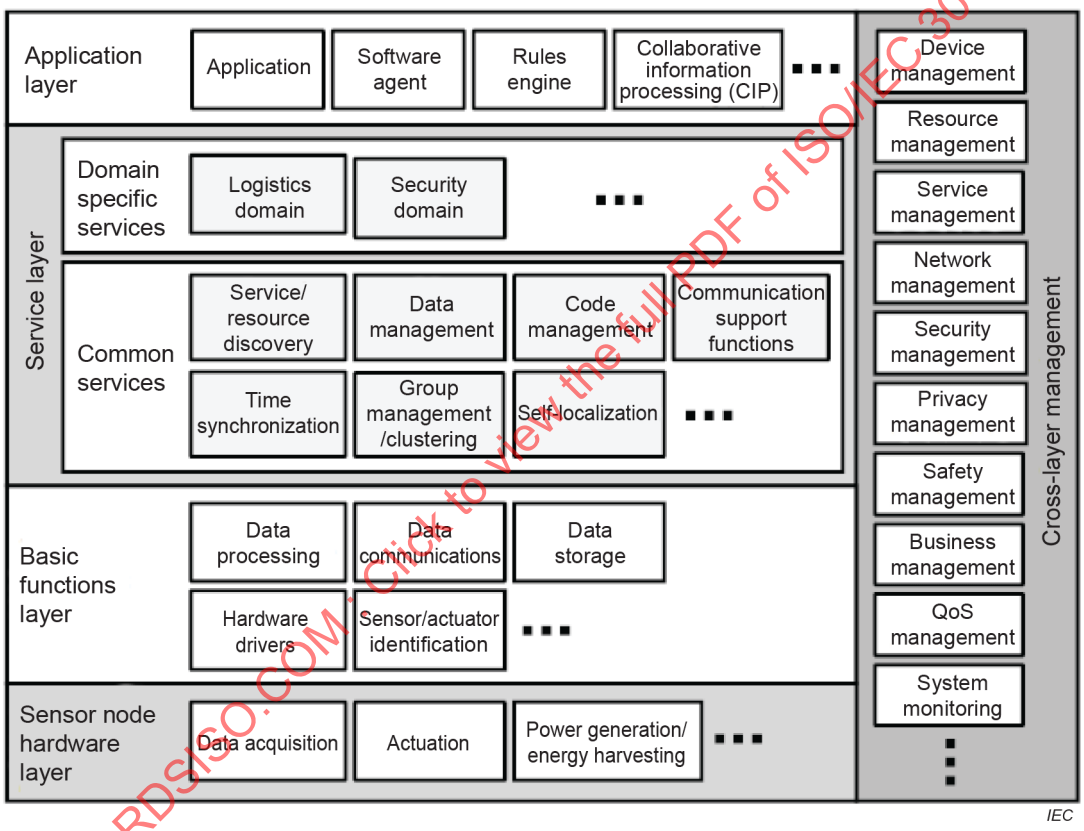
– Communication unit: A communication unit is an essential component of a sensor node. This communication unit provides either wired or wireless data link which is used to transmit the data collected by the sensor or sensing element and any processed data if available in real-time or in non-real-time. For the case of non-real-time data transmission, a type of storage device is required.

– Actuator(s): An actuator may reside in a sensor node or outside of the sensor node. Actuators are means to interact with physical environments, for example, automatic temperature control. Actuator(s) can receive information (e.g. command) directly from a sensor after data processing through wired or wireless data link.

– Power supply: A sensor node will require a power supply. If a sensor node is physically connected via a wire, such sensor node typically does not require on-board power supply, for example, batteries. In case of a wireless sensor node, a battery is required. Power management for a sensor node is a critical matter, and a power management utility firmware may be hosted in the CPU, especially for the sensor nodes remotely located wirelessly.

A.3 Functional model of the sensor network

See Figure A.4.



SOURCE: Figure 7 of ISO/IEC 29182-3:2014

Figure A.4 – Functional model of the sensor network