

IEEE Power & Energy Society

May 2020

Final Version

TECHNICAL REPORT

PSCC-S6



Report: IoT for Connected Home – Communication and Cybersecurity Requirements

PREPARED BY THE
Technical Committee PSCC
Task Force S6

© IEEE 2019 The Institute of Electrical and Electronics Engineers, Inc.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

THIS PAGE LEFT BLANK INTENTIONALLY

PSCC-S6

IoT for Connected Home – Communication and Cybersecurity Requirements

Chair: Marc Lacroix
Vice-chair: James Formea

Members and Contributors

Raed Abdullah
Jay Anderson
Mike Dood
Didier Giarratano
Tim Godfrey
Shane Haveron
IEEE 802.24 TAG
Mario Jardim
Nicholas Kraemer
Steve Kunsman
Steve Mark
Ryan Newell
Nathan Wallace

KEYWORDS

Smart Grid, Smart Grid Model; Smart Homes; Business Use Cases; Demand Response; DER, IoT

CONTENTS

1. Introduction	1
2. References	1
3. Impact of Connected Homes on Power Systems	2
4. The Smart Grid Model.....	3
4.1 Smart grid architecture.....	3
4.2 Customer Domain Architecture	6
5. Utility Use Cases for Connected Homes.....	8
5.1 Business Use Cases.....	8
5.2 Performance Requirements	10
6. Communication technologies and protocols used by IoTs.....	11
6.1 Current Situation	11
6.2 Emerging Solutions	13
7. Connected home integration.....	14
7.1 High-level Architecture	14
7.2 Home Generic Architecture.....	15
7.3 Other Challenges for Domestic IoT Integration.....	17
8. Cybersecurity Architecture.....	17
9. Recommended Requirements for Connected Home Integration	19
9.1 Communications Utility.....	19
9.1.1 General requirements.....	19
9.1.2 Physical and link layers.....	19
9.1.3 Network Layer	19
9.1.4 Transport Layer.....	19
9.1.5 Application Layer.....	19
9.2 Cybersecurity	20
9.2.1 Level 1.....	20
9.2.2 Level 2.....	21
9.2.3 Level 3.....	21
9.3 Privacy	21
9.4 Time Synchronization.....	22
9.4.1 Time Synchronization Methods	22

9.5 IoT Lifecycle	23
9.5.1 Development (vendor).....	23
9.5.2 Engineering (Client).....	24
9.5.3 Manufacturing (Vendor).....	24
9.5.4 Procurement (Client)	24
9.5.5 Commissioning (Vendor and Client).....	24
9.5.6 Maintenance and Support (Vendor)	25
9.5.7 Maintenance and Operation (Client)	25
9.5.8 Decommissioning (Client)	25

THIS PAGE LEFT BLANK INTENTIONALLY

1. Introduction

Connected Homes are residential customer dwellings that can transact with the customer's energy provider for purposes of information exchange or, if a Smart Home, execution of load or energy management commands. A Smart Home is a Connected Home that contains any number or combination of generation devices, storage systems or flexible loads for the purpose of providing the customer capability for managing their load profile, cost or comfort. The Connected Smart Home is enabling grid edge transformation whereby the customer becomes a prosumer helping their energy provider uphold grid integrity (reliability & safety), better manage supply to demand (i.e., have demand follow supply), and possibly reallocate or defer system upgrades through management of the premise's load shape impact on the grid assets.

These transformations at the edge will also impact power system operations and control and affect existing load forecasting, generation dispatching, energy costing and power restoring functions. With ever more transformation, the complexity in executing these tasks will also become ever more complex; new tools will be needed to handle the many more variables, and energy providers will need to develop collaborative relationships with the customers who will transform into prosumers.

With the benefit of communication technology, energy data can be shared within a smart city, such as with the smart transportation system, to improve the communities' well-being. In spite of the advantages brought by technology, challenges exist that need solving and the most important one is cybersecurity. Millions of connected consumer grade IoT devices will require well defined cyber-security programs. A second important challenge is for the IoT devices to communicate at least with the relevant stakeholders in an interoperable manner. Different communications technologies and protocols are in use and are not interoperable across vendor platforms. Use of a standardized interoperability protocol (IEEE or IEC) will unlock full benefit from this new edge technology.

2. References

- IEC 62913-2-3 Generic Smart Grid Requirements - Part 2-3: Resources connected to the Grid Domain
- NIST special publication 1108r3
- IEC 63097: Smart Grid Roadmap
- ANSI/UL 2900-1 Software Cybersecurity
- UL 2900-2-2 Industrial Control Systems
- IEEE 2030.5 IEEE Standard For Smart Energy Profile Application Protocol

3. Impact of Connected Homes on Power Systems

New edge technology installed in homes can largely impact the service provider. Affordable green generation and storage will interest an increasing number of customers. Not only will the load pattern change at the grid edge, it will influence the pattern on the upstream assets through to the transmission nodes. Shown in Figure 1 is an example of high penetration solar generation impact on the California power system: the green curve represents the total demand, while the purple curve is the service provider delivered power. At the end-of-the-day, the utilities are challenged to rapidly connect more generators to the system to compensate for the decrease in solar generation (blue curve). The rate of these additions is unsustainable and costly.

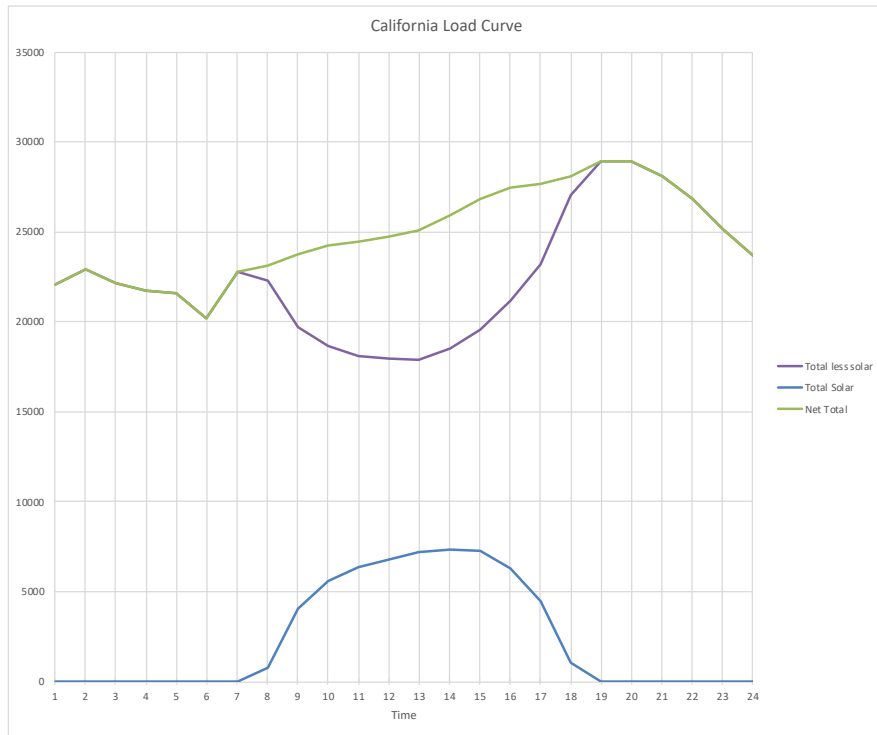


Fig. 1. Example of California’s daily load profile

With domestic generation and storage, the problem can be more severe if the utilities don’t implement load management programs in partnership with their residential customers by means of demand-response programs. This is where the utilities can take advantage of IoT that controls devices that use, generate, or store energy. IoTs allow customers to actively participate in the electricity market by interaction with the market based on signals (such as a price or marketing program’s signal).

The price signal approach to load control has demonstrated poor response from the customer. A more promising approach is the implementation of a program that includes a fully automated home energy management system combined with a customer incentive program. These systems must be easy to use, reliable, robust and they should not impact power system reliability.

4. The Smart Grid Model

The smart homes will be able to support the smart grid functions listed in the NIST special publication 1108r3:

- a) **Demand response and consumer energy efficiency:** Provide mechanisms and incentives to modify energy use during times of peak demand or when power reliability is at risk.
- b) **Wide-area situational awareness:** Utilizes monitoring and display of power-system components and performance across interconnections and over large geographic areas in near real time.
- c) **Distributed Energy Resources (DER):** Covers generation and/or electric storage systems that are interconnected with distribution systems, including devices that reside on a customer premise, “behind the meter.”
- d) **Energy Storage:** Means of storing energy, directly or indirectly.
- e) **Electric transportation:** Refers primarily to enabling large-scale integration of plug-in electric vehicles (PEVs).
- f) **Network communications:** Refers to a variety of public and private communication networks, both wired and wireless, that will be used for smart grid domains and subdomains.
- g) **Advanced metering infrastructure (AMI):** Provides near real-time monitoring of power usage.
- h) **Distribution grid management:** Focuses on maximizing performance of feeders, transformers, and other components of networked distribution systems and integrating them with transmission systems and customer operations.
- i) **Cybersecurity:** Encompasses measures to ensure the confidentiality, integrity, and availability of the electronic information communication systems and the control systems necessary for the management, operation, and protection of the smart grid’s energy, information technology, and telecommunications infrastructures

These use cases show that the smart homes can become a very critical actors in the energy sector that can impact smart grid integrity and security.

4.1 Smart grid architecture

This section describes how the connected homes are integrated in new smart grid architectures. The NIST smart grid model, developed by NIST in North America, and SGAM model, developed by CEN-CENELEC-ETSI SG-CG/RA working group in Europe, will be referenced.

Shown in figure 2 is the NIST general conceptual model that includes seven (7) different domains:

- a) **Customer:** the end user of electricity. Can be residential, commercial, industrial, institutional or agricultural, though the focus in this standard is residential. Customer can be strictly a “consumer” or user of electricity or a “prosumer” in the

evolved SG model as the consumer becomes a true participant in the grid as a user and provider.

- b) Markets: represents the operators and participants to the electricity trading venues. These can be wholesale, retail, or local trading markets
- c) Service providers: organizations that fulfil electricity user or service provider ecosystem needs to the customers or to the utilities. This includes the Curtailment Service Provider, or aggregator.
- d) System Operators: managers of energy flow (transmission or distribution)
- e) Generator: electricity source providers. Can also be energy storage. This domain covers both major power plants and DER.
- f) Transmission System: long-distance high or very high voltages carrier of electricity from large energy sources to end users. May also have large scale storage or generation directly connected to it.
- g) Distribution System: connects the transmission system to medium or low voltage served end user customers. This domain includes high voltage stations, substations and emanating circuits and feeders that connect the energy sources or loads

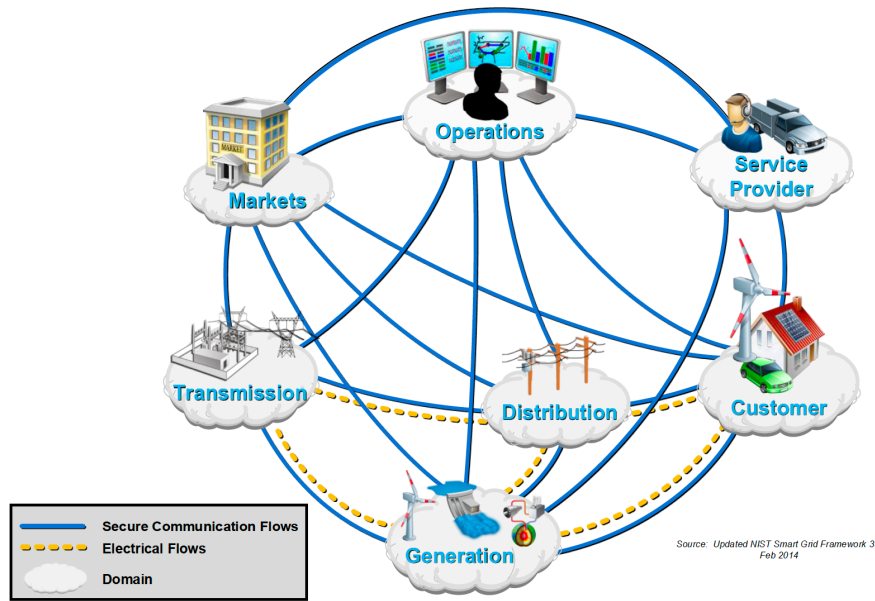


Fig. 2. High-level Smart Grid Conceptual Model

Communication links are essential for this model to work. We can also see in Figure 2 the flows of energy represented by dashed yellow lines. The customer domain can communicate with all the others except the transmission domain. This makes the customer an active participant to smart grid operation. Not shown in this figure are the regulators and law makers who have an important role in the conceptual model.

The SGAM model uses the same domains as in the NIST model except it adds the DER domain. DER is taking evermore a major part in the development /evolution of the smart grid, and thus needs its own domain. Figure 3 shows the smart grid plan with different domains representing the physical electrical installation: power plant, transmission system,

distribution system, DER and customers’ premises. The zones represent the hierarchical organization of the smart grid management. The process zone includes the primary equipment such as overhead lines, transformers, breakers, etc. The field zone comprises all the IEDs used for protection, automation and control of the primary equipment. The station zone is an aggregation level for field objects for process automation plus supervision, local SCADA, and data gateway. Operation zone is the level where we find the control center systems for the different domains such as distribution management systems (DMS), energy management systems (EMS) in generation and transmission systems, microgrid management systems, virtual power plant management systems (aggregating several DERs), and electric vehicle (EV) fleet charging management systems. Enterprise zone includes organizational processes, services and infrastructure such as asset management, logistics, human resources, billing, and customer relation management. Finally, Markets contains all the activities to trade including retail energy.

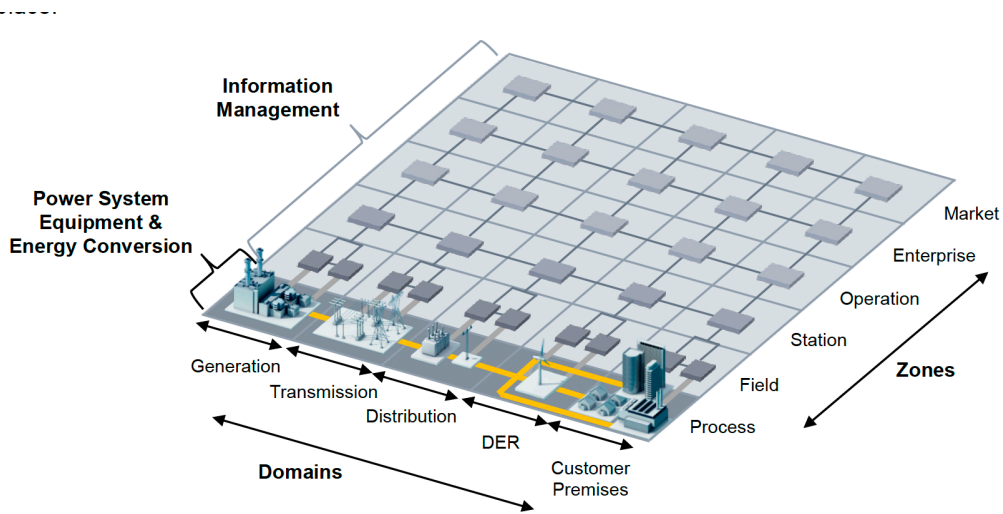


Fig. 3. Smart-Grid component layer (CEN-CENELEC-ETSI - Smart Grid Reference Architecture)

To allow more detailed information about the smart grid, the SGAM model represents the system with five different layers. Shown in Fig. 4 is that additional to the component layer described earlier, four other layers model detail the interoperability between entities and the relation between enterprise objectives, business functions, information technologies, communication systems and components.

For instance, we may have business objectives in terms of revenue that uses metering functions from the layer below. The metering needs data defined on the information layer. This data is obtained with the help of communication protocols and systems to obtain information from the component layer.

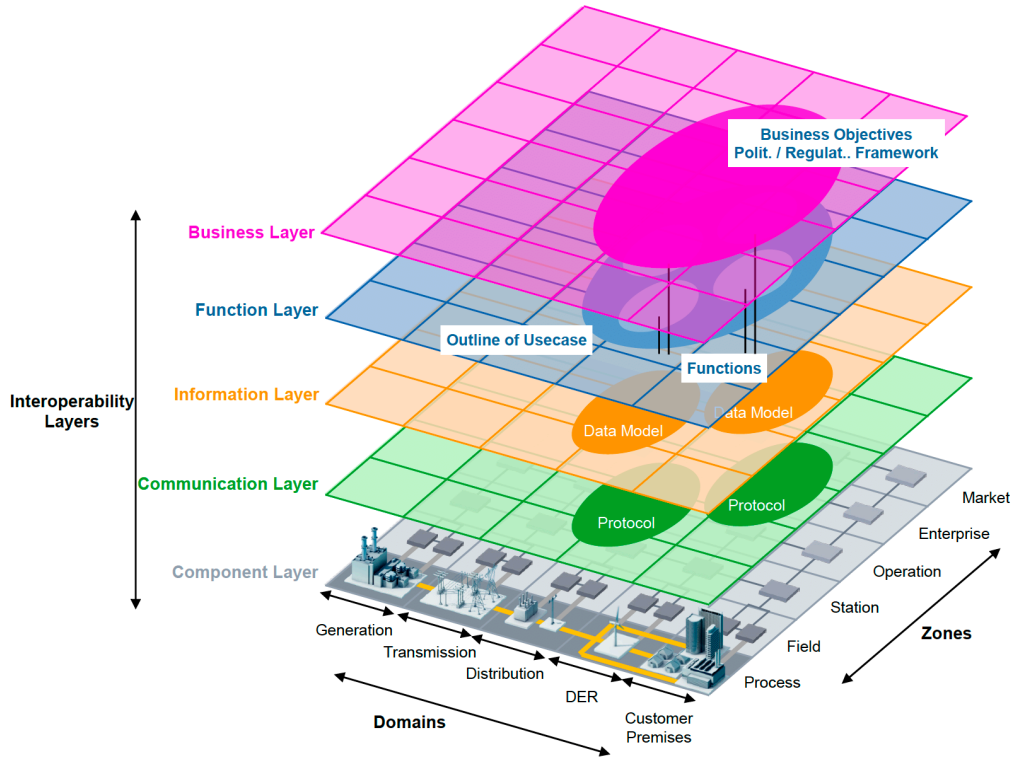


Fig. 4. Smart-Grid SGAM Model (CEN-CENELEC-ETSI - Smart Grid Reference Architecture)

4.2 Customer Domain Architecture

Since this report focuses the integration of IoT to the utilities, we look now in more detail at the architecture of Customer domains. Figure 5 shows the conceptual domain as defined by NIST in its 1108 report. This report introduces the three categories of customers: industrial, commercial and residential. Each of the three categories of customers can contain DER installations. For the residential sub-domain, we also have a set of devices that can communicate with each other. For each of the sub-domains, a gateway can be used as a point of connection with other domains.

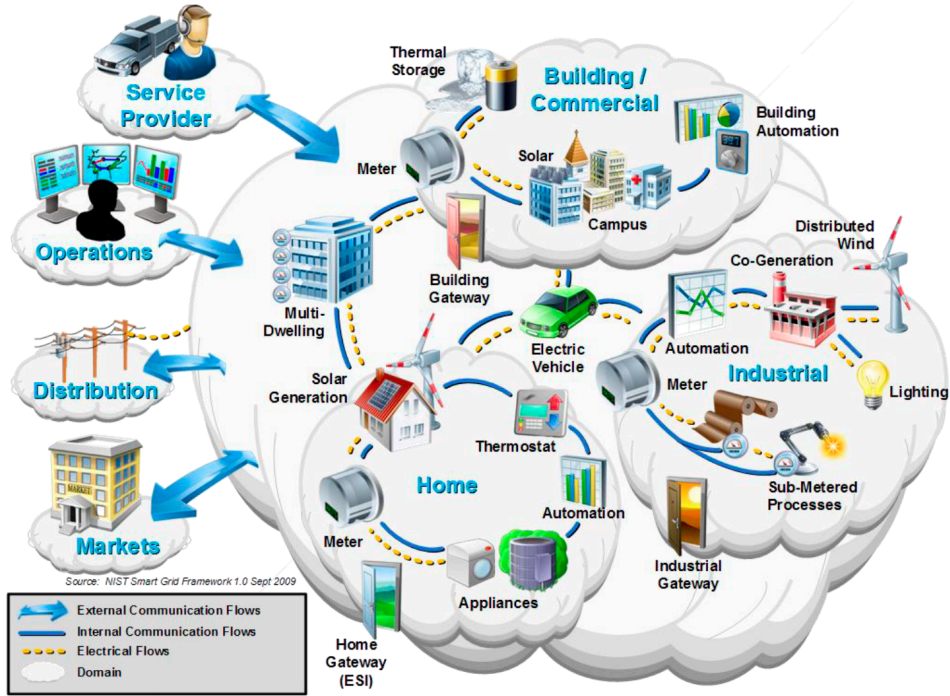


Fig. 5. Customer Conceptual Domain (NIST 1108 P192)

Figure 6 shows another representation based on the SGAM approach. We can see the metering information collected by the meter and sent to the MDMS (Meter Data Management System). From the MDMS, data is sent to the DMS system and to the trading system. Since the metering function can be implemented differently by each service provider, the model can vary. As shown in the figure, an independent chain of acquisition can also be used for load control functions. Very often, the metering infrastructure doesn't have the required bandwidth to fulfill these functions. Moreover, meters typically don't offer the required flexibility to easily implement new protection policies or software updates. In the house, we can have generation and storage capabilities. Based on the market conditions, the house controller may decide to store the excess of generation or send it to the power grid.

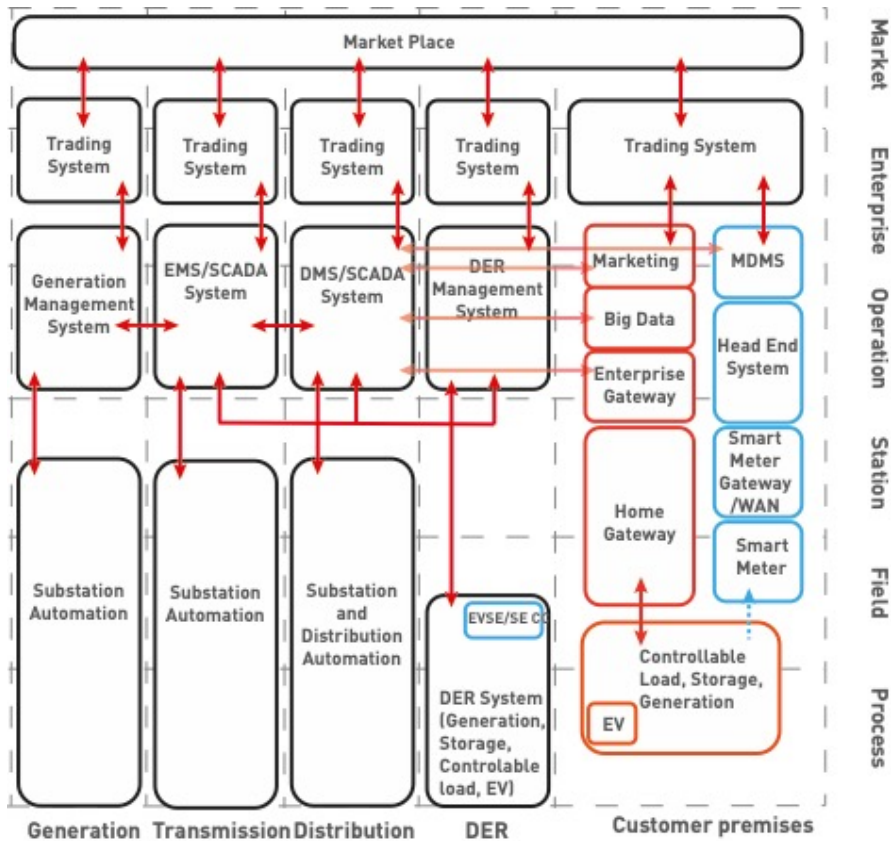


Fig. 6. Smartgrid Model for Home automation

5. Utility Use Cases for Connected Homes

This section presents use cases to describe how utilities can interact with connected homes. For this exercise, we use the approach described in IEC 62913-1 (Generic Smart Grid Requirements – Part 1: Specific application of the Use Case methodology for defining Smart Grid requirements according to the IEC System approach). In this document, we will describe the business use cases (BUC) that represent the enterprise high-level requirements and strategic goals. We will also describe the system use cases (SUC) that represent the different functions used for a connected home program.

5.1 Business Use Cases.

The business objectives for load management are upholding grid reliability, reducing the need for investments in new infrastructure, lowering the maintenance costs, and minimizing the use of polluting energy sources. To succeed, the business model will require increased visibility, improved forecasting and prediction and operational flexibility. For a system operator, flexibility is the capability of using many tools to manage the grid, including messaging the Customer to voluntarily, or immediately in case of an emergency, adapt their DERs’ behavior to help the grid. The flexibility comes from the optimal management of local devices such as electric vehicles, heat pumps, PV, or wind turbines. The grid-oriented allocation of flexibility can be used for capacity management.

Table 1 – List of Business Use Case

BUC 1	Peak Shaving	Reduce energy use during peak demand. Can be done using price signal or other informative signal. During the peak time, customers can use energy from their generation, storage devices or flexible loads.
BUC 2	Demand rate of change smoothing	To reduce the rate of change of energy demand. Customers can use energy from their generation or storage devices. They can also curtail or stagger their flexible loads.
BUC 3	Frequency regulation	The customers can participate in frequency regulation. This function requires more frequent communication with the service provider and faster response. The customers can modulate their energy demand by storing/retrieving energy from storage devices.
BUC 4	Volt-VAR support	The customers can participate in voltage support if they inject energy in the power system. The setting of the smart-inverter can be changed to raise/lower the voltage level on the service provider side.
BUC 5	Energy support	Same as peak shaving
BUC 6	Economic Demand Response (DR)	Reduce load in the energy market when the wholesale price is higher than the monthly published TSO (Transmission System Operator) net benefits price.
BUC 7	Emergency Demand	The customer can participate in emergency demands by shedding least essential residential load.
BUC 8	Spinning/synchronized Reserve Management: 10-minute response time	The customer can participate in spinning reserve by controlling the available energy in the storage device plus by offering flexible loads.
BUC 9	Day ahead Scheduling Reserves: 30-minute response time	The customer can participate in spinning reserve by controlling the available energy in the storage device plus by offering flexible loads. This Use Case differs from BUC 8 with a different time scale.
BUC 11	Coordinate the energy resources into the smart grid to respect voltage, power and energy limits	See BUC 4
BUC 12	Reactive/active Control	See BUC4
BUC 13	Grid Visibility	The home energy management system can measure power, energy, voltage level in real-time and send the information on-demand to the system operator.
BUC 14	Microgrid Functions	May include specific requirements for time sync, freq control, tie control, load shedding, load forecast

Many of these programs are similar, if not identical, and they all use Demand Response – voluntary management or direct control – functionalities to fulfil grid integrity needs. Many of these functionalities send control set-points to the customer’s home energy management systems directly or through an aggregator (Curtailment Service Provider (CSP)). The aggregator is responsible for demand response activity with a group of consumers. The aggregator identifies demand response opportunities for customers and implements the necessary equipment, operational processes and/or systems to enable demand response

both at the customer’s facility and directly into the appropriate wholesale market. However, the aggregator supports the needs of the whole or regional market and not necessarily local or hyper local needs.

5.2 Performance Requirements

Shown in the following tables are the different business use cases and their required performance. This table will help the utilities who want to realize connected homes to choose the right telecommunication technology and the appropriate cybersecurity measures.

For all the use cases, security and integrity are very important for the dependability, stability and reliability of the power system. Only use case number 13 requires privacy due to customer information. The volume of information to exchange is also very low in all the cases.

Latency is the characteristic of a communication system to deliver the information. Low latency means that the communication system should deliver the information within a very short period of time (sub-second).

Table 2 – Performance requirements for each use case

Functions	Privacy	Security	Integrity	Volume	Time Sync Accuracy and class	Latency
BUC - 1	Low	High	High	Low	Sec	High
BUC - 2	Low	High	High	Low	Sub-sec	Medium
BUC - 3	Low	High	High	Low	Sub-sec	Low
BUC - 4	Low	High	High	Low	Sub-sec	Medium
BUC - 5	Low	High	High	Low	Sub-sec	Medium
BUC - 6	Low	High	High	Low	Sec	Medium
BUC – 7	Low	High	High	Low	Sec	Low
BUC – 8	Low	High	High	Low	Sec	Medium
BUC – 9	Low	High	High	Low	Sec	High
BUC - 11	Low	High	High	Low	Sub-sec	Medium
BUC – 12	Low	High	High	Low	Sub-sec	High
BUC - 13	High	High	High	Low	Sec	Low
BUC – 14	Low	High	High	Low	Sub-sec	High

6. Communication technologies and protocols used by IoTs

Today, communications protocols and technologies used by IoT devices are many and not compatible with each other. Some protocols are designed to minimize energy consumption by IoTs. Figure 8 shows different communication technologies used by IoT devices in a residential setting. For each technology, the physical layer bit rate, operating frequency band, and coverage (largest circle = largest coverage) are plotted.

The physical layer protocols are typically backward compatible and interoperable when they are used in the same band. For example, 802.11g and 802.11n can interoperate in the 2.4 GHz band. 802.11a, 802.11n and 802.11ac can interoperate in the 5 GHz band.

6.1 Current Situation

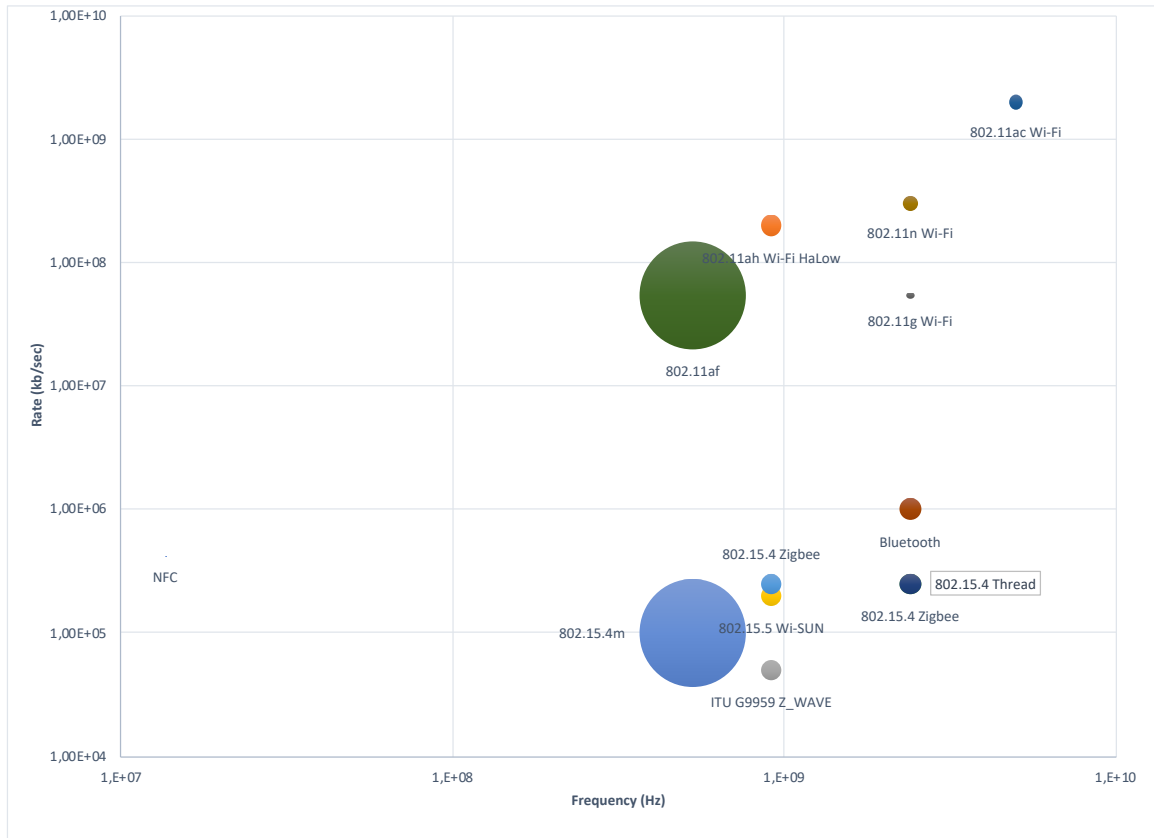


Fig. 7. Communication technologies

For the context of this report, the LAN is considered the customer’s Local Area Network. This network is sometimes referred to as the Home Area Network or HAN, but this term has negative connotations from early deployments (in conjunction with AMI) that were less successful. The customer network is most frequently based on 802.11 Wi-Fi, although 802.15.4 is also used for many connected devices with an interface gateway or hub. The 802.3 Ethernet is typically used in the residential LAN for short distance wired

connections. IEEE P1901 HomePlug has found limited application in the home-area LAN to extend Ethernet over power lines, often to connect to an 802.11 access point to provide whole-home coverage.

802.15.4

The 802.15.4 Smart Utility Network (SUN) PHY is designed to provide connectivity in an RF Mesh topology, which enables much larger effective range than a single RF link can support. 802.15.4 typically operates in unlicensed spectrum (the 915 MHz ISM band in North America, and other bands internationally), and provides data rates from 10 kbps to 300 kbps. Wi-SUN is typically deployed as part of a service provider AMI network; however, it can also provide connectivity to devices within the home.

802.15.4 provides the lower layers for the ZigBee protocol stack. It operates in the 915 MHz and 2.4 GHz bands and provides data rates of 100 kbps up to 800 kbps. A similar proprietary technology called Z-Wave also operates in the 915 MHz band. ZigBee and Z-Wave require a gateway to connect IoT devices to the Internet.

802.11

802.11, also known as Wi-Fi, is widely deployed in the home and is a good choice for IoT since it typically provides Internet connectivity directly without a gateway. 802.11n (Wi-Fi 4) operated in both the 2.4 GHz and 5 GHz bands. 802.11ac (Wi-Fi 5) operates only in the 5 GHz band.

Figure 8 shows the different communication stacks in use. Many protocols used proprietary stacks that are not compatible with each other.

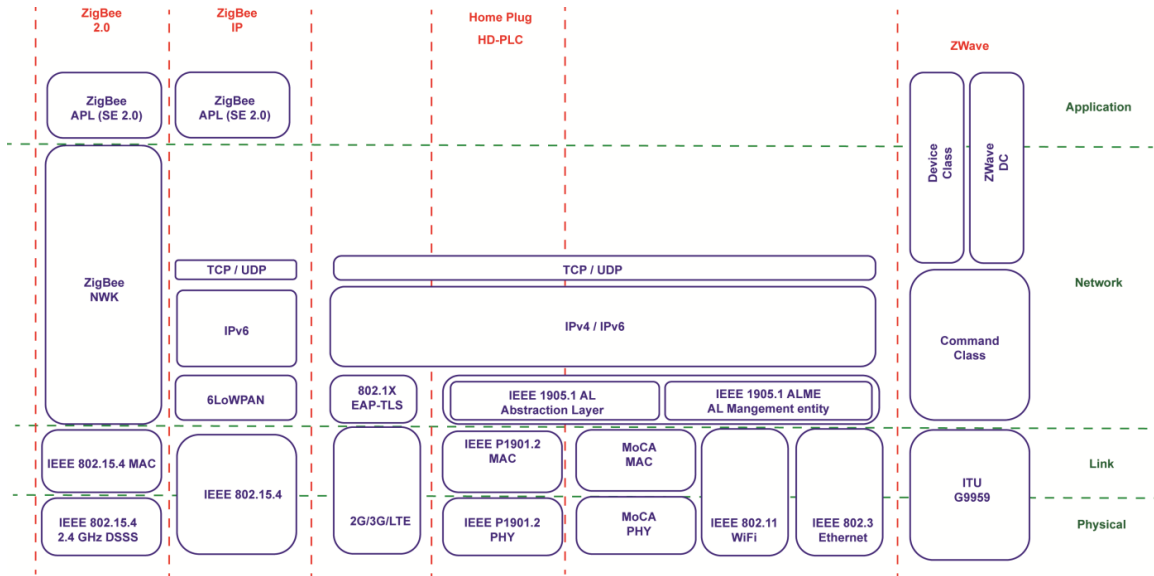


Fig. 8. IoT protocols

6.2 Emerging Solutions

802.11

The latest generation [Wi-Fi 6](#) based on IEEE 802.11ax was introduced in Fall 2019, and operates in both 2.4 GHz and 5 GHz bands. IEEE 802.11 products are also available for outdoor mesh networks that can provide wireless coverage over a metropolitan area. The IEEE 802.11ah HaLow standard has been completed to enable operation in the 915 MHz band, offering 2 to 4 times the range compared to 2.4 GHz Wi-Fi. As of 2019, products were not yet widely available.

802.15.4

The IEEE 802.15.4 SUN PHY (added with the 802.15.4g amendment) was further amended in 2019 with the 802.15.4x project. It provides higher data rates (up to 2.4 Mbps) at short range, and longer ranges at lower data rates. As part of the Wi-SUN FAN profile, the 802.15.4 SUN PHY can support utility-focused IoT both in the home and in the field.

Quality of Service

QoS is not a communications protocol but is a service that is implemented by many communications protocols and standards, to varying degrees, to measure the communication performance seen by the end-user. To enable end-to-end QoS, it must be coordinated through packet tagging at both Layer 2 and Layer 3. The Layer 2 prioritization and tagging are defined by IEEE, originally in 802.1p, which is now part of 802.1Q-2014.

IEEE 802.11 supports QoS. This feature is typically enabled on the access point using settings for Wireless Multimedia Extensions (WMM). These features are typically used for prioritizing voice, video, or gaming. Today's QoS implementations do not extend beyond the home network onto the WAN or Internet. QoS is rarely, if ever, used for energy-related IoT devices in a home setting.

Currently 802.15.4 does not have explicit support for 802.1Q. The standard includes a prioritized access method, but it is not used by higher layer protocols.

7. Connected home integration

7.1 High-level Architecture

Figure 9 proposes a high-level integration of the connected home. This architecture is composed of three main parts: the enterprise system, the cloud system and the edge system.

The IoTs are located at the edge of the system. The edge can be the home or home area. A gateway is recommended to connect the IoTs at the edge with the corporate communication system.

The second element is the communication system that can be owned by the service provider or a public communication provider. Many communication architectures are possible, and the figure shows direct communication between the cloud and the edge devices and communication thru substations.

At the enterprise level, the communication interface sends or receives information from the IoTs. The data dispatch sends the information to the subscribers such as the Big Data engine and the security asset management. The corporate applications use the results of big data analysis and other sources of information for system control, load forecasting and demand-response programs development. In this example, the OSS (Operating Support Systems) and BSS (Business Support Systems) communicate with CLM (Customer Loyalty System) to develop the DR programs, analyze their expected results, evaluate their costs and calculate the anticipated return on investment.

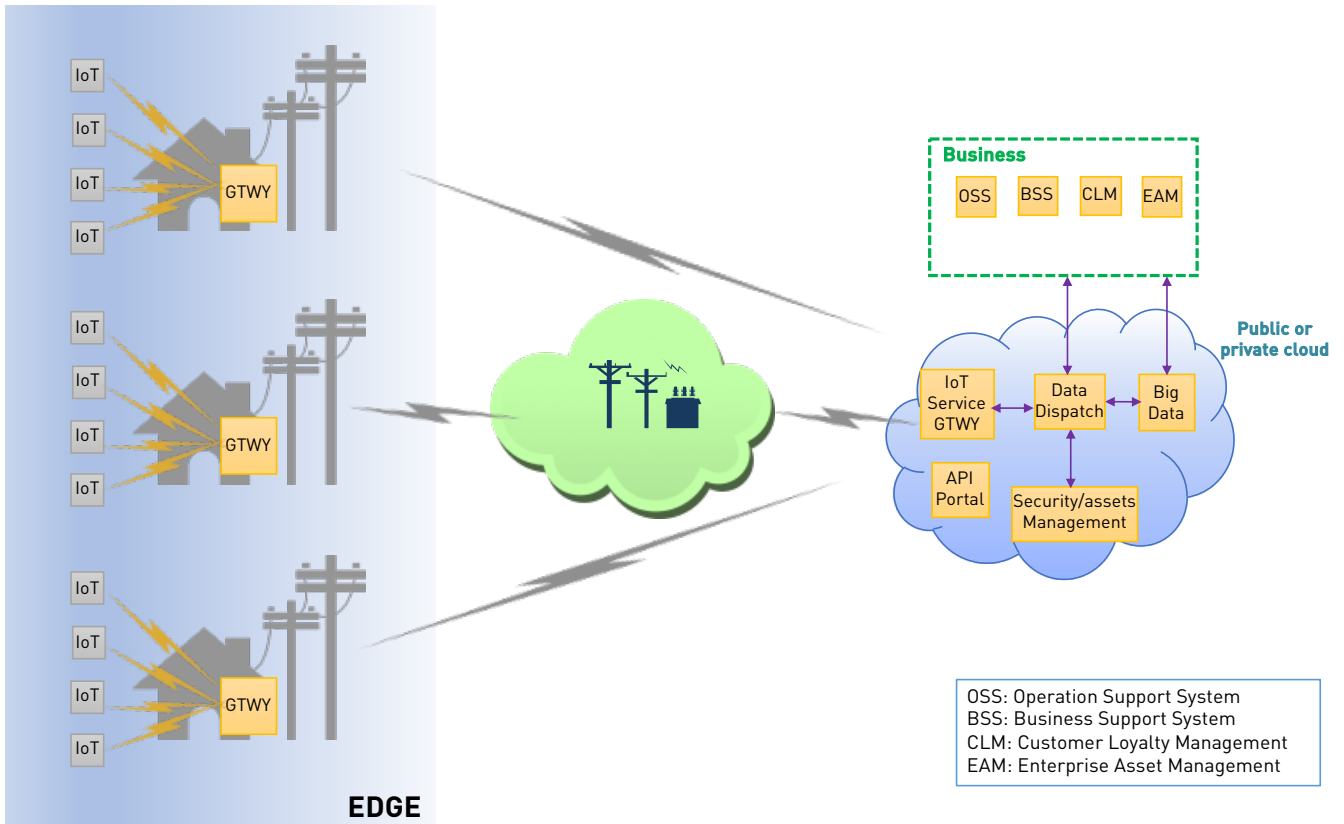


Fig. 9. - Architecture

7.2 Home Generic Architecture

Figure 10 shows a generic home architecture proposed in IEC 62913-2-3. Table 3 describes the different elements of the architecture. The home energy management system described in the previous sections is composed of EMG, CEM and DEM. In this model, the meter sends metering information to the control center and may process load management functions. In the case the meter doesn't have the capability to process load management functions, then these functions are supported by the HEMS or the HEMS Controller.

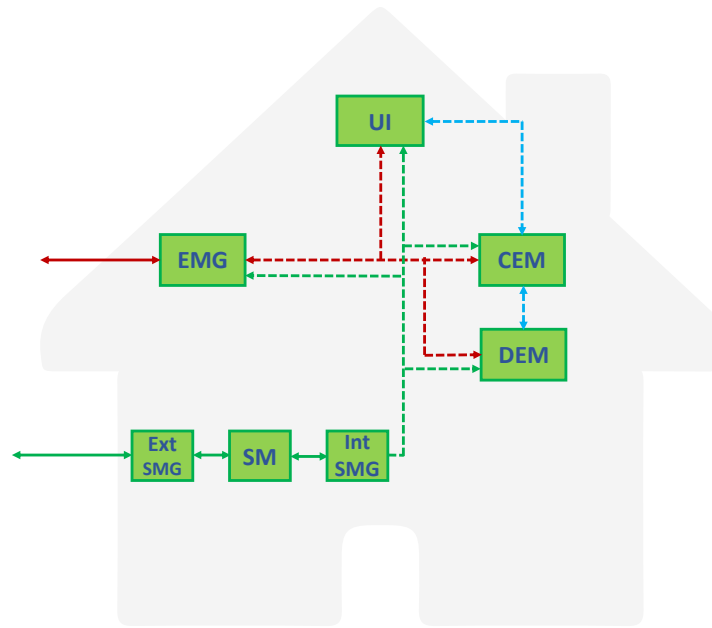







Fig. 10. Home generic architecture (IEC 62913-2-3 P47)

Table 3 - Functional Components

CEM	Customer Energy Management (HEMS)
DEM	Device Energy Management (HEMS)
EMG	Energy Management Gateway (HEMS)
SM	Smart Metering
SMG	Smart Metering Gateway
UI	User Interface

Table 4 - Flows of information

	Flexibility Request/Price/Incentive/Data
	
	Management/Data
	Flexibility Requests/Price Incentives/Data
	Flexibility Request / Price Incentives / Metering Data / Voltage Quality Data / Technical Data

7.3 Other Challenges for Domestic IoT Integration

Beside the basic cybersecurity practices, connected homes present some unique and challenging risks due to the nature of IoTs. One of the most challenging is the homeowner's illiteracy regarding technology, such as skill to properly configure their devices. A misconfigured device poses a high potential threat risk. The risk is limited when the communications stay inside the house perimeter, although troubles arise when the IoT devices start communicating outside. In recent years, malicious actors have exploited security holes in IoT devices, taking control of security cameras to organize DDOS attacks on other sites. Connecting these devices directly to the service provider communication system is a high security risk.

Another challenge is the poorly designed or poorly tested IoTs found for smart home applications. Time to market pressures cause devices to be released before all the tests are completed. Among the issues found are the problems of applications having too much privilege (right to access critical IoT resources) that hackers can exploit to take control of the IoT.

Since most of the IoTs are designed to keep the price low, we can't expect that they include more advanced security functions or be software upgradable. Most of these devices have limited processing capabilities to minimize their energy use. Very often, these devices don't communicate continuously and wake up only when events occurred.

8. Cybersecurity Architecture

The greater role of IoT devices in supporting the business functions listed in Table 1 necessitates reliable platforms and highly secured interfaces. Malfunction due to security threat may impact power system reliability. People who have little or no IT knowledge owning IoT devices poses a great security challenge to the service provider.

Figure 11 shows the SGAM architecture modified to indicate the three levels of cybersecurity that must be applied. For each level, different cybersecurity tasks and functions must be performed to assure the overall security.

Level 1 groups the cybersecurity requirements for IoTs. If the IoTs are owned by the service provider, their maintenance and configuration shall be done by the service provider, which offers a higher degree of security. It is more challenging to integrate IoTs owned by the homeowner and it is harder to guarantee the security, which creates weaknesses in the cybersecurity strategy. These IoTs may contain some mechanisms to assess the integrity of the database, the coherence of settings and trusted source for keys and certificates distribution. For example, a third-party software agent can be installed in the IoTs to secure device identity and user application data, securely enroll devices into operational environments and interact with hardware security components and root identity management systems via an onsite gateway. IoTs for energy management should also support the capability of having their software updated to include the latest cybersecurity features.

On Level 2, the edge gateway is the key component in the cybersecurity strategy. It supports authentication mechanisms and keys, keeps a list of trusted devices, maintains active and revoked keys lists, collects local events, and performs threat detection. The gateway has the capability of blocking any IoT that tries to perform unauthorized access to the service provider communication system. The gateway can also block IoTs that are not properly configured or don't have a trusted firmware version. The edge gateway works in partnership with the enterprise security system to get the latest information on threat alerts, IoT firmware version and trusted/untrusted IoTs.

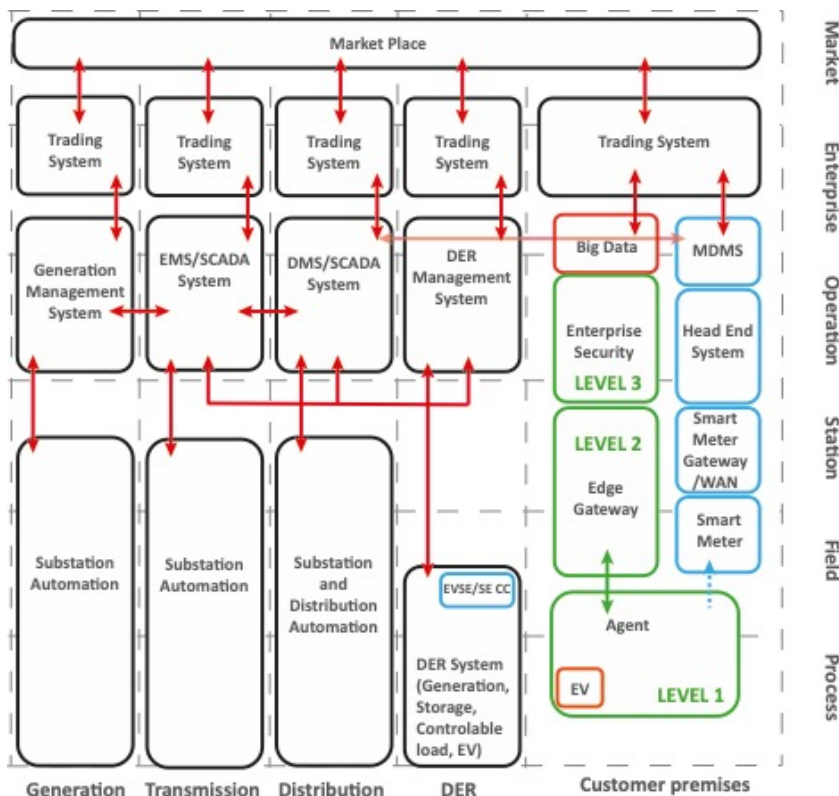


Figure 11: Three-level Hierarchy IoT Cybersecurity

On Level 3, the enterprise security system is monitoring all the gateways on the system. It performs statistics on communication and cybersecurity performance to detect any threat or weakness in the system. It can also use analytics to detect and prevent malicious or suspicious activities. In this way, big data techniques can be used to find patterns among all the IoTs access failures or to detect unusual behavior such as a customer trying to access their account in the middle of the night. The enterprise system also manages certificates and key distribution, maintains IoT firmware versions and performs statistics on IoT system performance.

9. Recommended Requirements for Connected Home Integration

9.1 Communications Utility

9.1.1 General requirements

All the communications should use IP stack to facilitate the integration and provide an upgrade path.

9.1.2 Physical and link layers.

The devices associated with IoTs used in a Connected Home don't have constraints regarding energy consumption. To facilitate integration, the IoTs should be compliant to one of the following levels 1 and 2 standards:

- 802.15.4
- 802.16
- 802.11
- 802.22
- 802.3
- 4G, 5G LTE

9.1.3 Network Layer

The IP protocol should be used at the network layer.

9.1.4 Transport Layer

TCP should be used at the transport layer.

9.1.5 Application Layer

The application protocol must support the following functions:

- **Open service:** A Device is opened according to mode (e.g., read-only, write-only, read-write). A handle shall be returned that describes the newly established connection to the Device.
- **Close service:** The connection to a Device that is described by handle is terminated. The service can be used to close a connection with a distant host or to deliberately disconnect a local IoT that is considered as unsafe.
- **Read service:** Reads data from the Connected Device .
- **Write service:** Writes data to the Connected Device.
- **Seek service:** Changes the current read/write set-point of the Device. The change may be an absolute value, a relative value to the existing set-point or a relative value to the maximum set-point of the device.
- **IOCTL service:** Performs the I/O control operation.

The following application layer protocols can be used:

- IEEE 2030.5
 - This protocol includes TLS protection
- IEC 61850-8-2
 - This protocol supports end-to-end protection as define in 62351-4
- DNP-3/IEEE 1815
 - This protocol shall use TLS protection as specified in 62351-3
- IEC 60870-5-101/104
 - This protocol shall use TLS protection as specified in 62351-3

9.2 Cybersecurity

9.2.1 Level 1

The requirements for Level 1 may vary if the IoT is managed by the service provider or by the homeowner.

Owned by service provider

- Must support authentication
 - Certificate based protection.
- Privacy
 - Critical internal databases must be encrypted.
- Tamper detection
 - The IoT must include tampering detection.
 - The IoT should be considered non reliable if tampered.
- Protection of communication
 - Confidentiality of messages via encryption.
- Record and report security events, firmware update, set-up changes

Owned by third parties

- Must support authentication
 - The device should be configured to allow the service provider access to data and the ability to control devices inside the home
 - Certificate based protection
- Privacy
 - Critical internal databases must be encrypted
- Device trustworthiness
 - The IoT must include tampering detection.
 - The IoT should be able reporting firmware version.
 - The IoT should be able to report a list of options.
 - The IoT should be able to report manufacturer and hardware version.
- Software Agent
 - The manufacturer should include a software agent.
 - The software agent must be approved by the service provider.
 - The software agent is responsible to manage the communication with the service provider and securely enroll devices into operational environments.
 - Secures device identity.
 - Secures user application data.

- Interacts with hardware security components.
- The software agent should also verify critical elements of the hardware such as firmware integrity, network connection and connection attempts.
- Protection of communication
 - Confidentiality of messages via encryption.

9.2.2 Level 2

At level 2, we have the point of connection between the IoT and the service provider network. The device at this level plays the role of a gateway.

- Acts as a bridge between the IoTs and the Enterprise.
- Supports authentication mechanisms and keys.
- Maintains a list of trusted devices.
- Manages Key certificate.
- Maintains active and revoked keys.
- Maintains a list of most recent firmware with signatures.
- Sends alarms to stakeholders in case of security risks.
- Collects local events.
- Analyzes events for threat detection.
- Authorizes/Blocks IoT access to Internet.
- Supports Home Energy Management Functions.

9.2.3 Level 3

At the corporate level, the following functions should be implemented to overview the cybersecurity status.

- Manages the IoT devices/onsite modules and their identity provisioning and license enforcement.
- Supports Device lifecycle management.
- Plays the root trust authority role for the IoT network.
- Supports and manages X.509 certificates.
- Securely issues and manages manufacturer and operational identities.
- Monitoring of the communications infrastructure itself, which can provide:
 - a degree of intrusion detection,
 - resource load utilization,
 - availability of components within the information system.
- Requires one set of identity management policies (e.g. same mechanism for all profiles).

9.3 Privacy

The IoT:

- shall protect private data with encryption,
- shall detect any data modifications,

- shall support authorization mechanism for data access:
 - Can be RBAC (Role-Based Access Control) mechanism,
- the transmitted data should be encrypted.

9.4 Time Synchronization

This section describes time synchronization techniques. Some of these techniques can give very high accuracy time synchronization down to a few tens of nanoseconds. Except for the microgrid use case, very high accuracy is not required at this moment.

Measured data in power systems are often required to have a time stamp. The accuracy requirement for time synchronization depends on how the data will be used. Sequence of event reporting of alarms may be measured with a time resolution of 1ms whereas phasor measurements need much greater accuracy to be compliant with the synchrophasor standard, C37.118.1-2018.

For local area measurements, for example within a substation, devices on a local network can be synchronized using a local time source and absolute time is not as important as relative time between devices. For wide area measurements involving devices at different geographic locations the absolute time becomes very important, particularly when time stamped data needs to be compared for protection and control purposes as well as postmortem analysis of faults and maloperations.

IoT devices are more likely to require absolute time synchronization for wide area measurements rather than relative time between local devices. Accuracy and security of the time stamp is dependent on use case. For remedial action, such as load shedding, cybersecurity is vital to maintain power system stability, but the time resolution requirement may be quite low in the order of a few seconds. Phasor measurement for islanding detection for distributed generation will need very accurate time synchronization of 1us or better.

9.4.1 Time Synchronization Methods

Network Time Protocol, or NTP, is a readily available time synchronization source with many public servers provided by NIST, Google, Microsoft, etc. However care should be taken not to query the time server more often than once every 4 seconds or service may be denied. IoT devices will be able to make good use of public servers and vendors or utilities may set up private servers if needed. Time will not be as accurate as synching to a GPS clock on a substation LAN but will be within a few hundred milliseconds which exceeds the requirements for many applications.

Radio Code Clock long wave radio frequency broadcasts can be used quite effectively to synchronize IoT devices. These provide very little resistance to tampering.

When connecting to a server, which may be a cloud-based application, the device time can be adjusted to match the server time. A local oscillator is used to maintain time between adjustments. As updates may be infrequent, a battery backed real time clock can be used when it is important to restore an approximate time after power cycling. Previous generations of electromechanical clocks used the fundamental power system frequency for

synchronization which is approximately 60Hz or 50Hz. Averaged over long periods of time there will be significant drift from absolute time and are of very limited use today as local oscillators are cheaper and more accurate.

IoT devices that require much higher accuracies can be fitted with internal or external GPS receivers. Cost is much higher than with NTP but will not be prohibitive for applications such as islanding detection. Antenna location and security may be problematic.

IEEE Std 1588-2008 was introduced for power system applications requiring high precision time synchronization and uses hardware time stamping to achieve nanosecond accuracy. This is also known as Precision Time Protocol, or PTP. A common base profile is specified in IEC/IEEE 61850-9-3:2016 and an extended profile is specified in IEEE C37.238-2017. This is less likely to be available in IoT device locations as this technology is not typically used in consumer products but is available in some commercial and industrial devices.

Inter Range Instrumentation Group, or IRIG, time codes such as IRIG-B are similarly less likely to be available in IoT device locations. Time accuracy of 1 to 10us can be achieved and may be available in commercial and industrial sites.

9.5 IoT Lifecycle

To ensure that the IoT won't cause any threat to the power system during its lifetime, some measures shall be taken throughout its lifecycle to mitigate risk. Figure 12 shows the different phases of the IoT lifecycle that are the same as other IEDs used by the utilities.

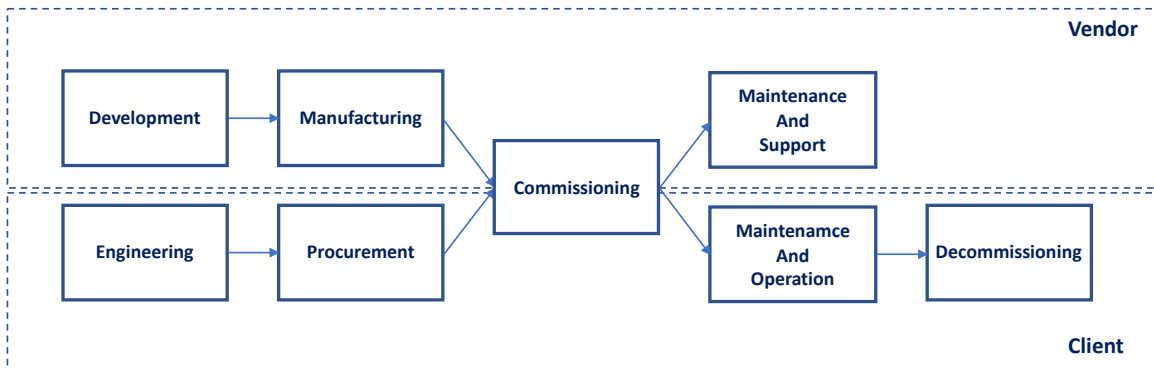


Figure 12: IoT lifecycle

We will describe in the next sections what are the specific requirements for each phase.

9.5.1 Development (vendor)

The vendor:

- shall perform a risk analysis of the environment of the future product,

- shall list all cybersecurity risks to be considered in the design phase,
- shall identify what can be the weaknesses and vulnerabilities,
- shall address cybersecurity during the design and development,
- shall maintain a traceability matrix of all the cybersecurity risks vs the countermeasures,
- shall maintain a list of all external software modules including version number, release date and signature.
- shall document its plan for providing validated software updates and patches as needed throughout the lifecycle of the device.

9.5.2 Engineering (Client)

The client:

- shall preform a risk and impact analysis of the future system product.
- shall identify the risks caused by the new IoT.
- shall design the system to mitigate the risk.
- shall define the policies for security management and audit.
- shall list of cybersecurity requirements for the procurement phase.

9.5.3 Manufacturing (Vendor)

The vendor:

- shall have a quality plan to assure the integrity of the IoT during all the manufacturing steps,
- shall have an audit process to verify that the quality plan is well observed.
- shall submit its IoT to an independent laboratory for cybersecurity assessment that includes:
 - Known vulnerability testing.
 - Malware testing.
 - Malformed input testing.
 - Structured penetration testing.
 - Software weakness analysis.

9.5.4 Procurement (Client)

The client:

- shall list in the procurement document all the required cybersecurity features,
- shall specify all the post-project requirements:
 - Support 24/7,
 - Duration of the support period (5 years for example).

9.5.5 Commissioning (Vendor and Client)

- The client and the vendor shall validate that all the cybersecurity requirements are included in the IoT.
- The client shall validate the documentation provided by the vendor.

- The client shall validate the vendor’s software support and update process.

9.5.6 Maintenance and Support (Vendor)

The vendor:

- shall implement a change management system,
- shall analyze and compile the client’s complaints and questions,
- shall verify if a cybersecurity problem affects any of the external software modules,
- shall correct any problem found in the internal or external software module,
- shall inform the client of any cybersecurity risks,
- shall document and distribute patches and software upgrade including vendor signature.

9.5.7 Maintenance and Operation (Client)

The client:

- shall support a change management system,
- shall test any soft patch or update received from the vendor,
- update IoT software using vendor and client signatures,
- audit IoT performances and tampering,
- analyze and record IoT cybersecurity events.

9.5.8 Decommissioning (Client)

The client

- shall erase from the decommissioned IoT all the critical information and parameters before its disposal.