International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2070

(01/2015)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

Requirements and architecture of the home energy management system and home network services

Recommendation ITU-T Y.2070

International
Telecommunication
Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	**Y.2000–Y.2099**
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2070

Requirements and architecture of the home energy management system and home network services

Summary

Recommendation ITU-T Y.2070 provides the requirements and architecture of the home energy management system (HEMS) and home network (HN) services. The HEMS supports energy efficiency and reduction of energy consumption by monitoring and controlling devices such as home appliances, storage batteries and sensors connected to the HN from the HEMS application.

While the algorithm for the energy efficiency and reduction of energy consumption runs in the HEMS application, the development of a platform (PF) is desired which provides common functions to enable the application to access the devices and to support the efficient development of applications. This is not only applies for the HEMS, but also for other HN services such as home security and healthcare. This Recommendation provides common requirements for the HN services to support the HEMS as the widely known HEMS is mainly considered one of the HN services. It also describes the reference architecture and the functional architecture including the functional relationship for the HEMS and the other HN services.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2070	2015-01-13	13	11.1002/1000/12420

Keywords

Home energy management system, home network, home network service.

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

1 Scope ... 1

2 References ... 1

3 Definitions ... 1

3.1 Terms defined elsewhere ... 1

3.2 Terms defined in this Recommendation ... 2

4 Abbreviations and acronyms ... 3

5 Conventions ... 4

6 Overview ... 4

6.1 HN service architecture ... 4

6.2 HEMS based on HN service architecture ... 5

6.3 Merits of HN service architecture ... 7

7 Requirements ... 8

7.1 Requirements for the device ... 8

7.2 Requirements for HGW ... 8

7.3 Requirements for management PF ... 9

7.4 Requirements for security ... 10

8 Reference architecture ... 10

9 Functional architecture ... 12

9.1 Device ... 13

9.2 HGW ... 14

9.3 Management PF ... 14

9.4 Application ... 15

10 Functional relationship ... 16

10.1 Device operation ... 16

10.2 Application execution ... 18

10.3 Management ... 19

11 Security support ... 20

11.1 HEMS model for security ... 20

11.2 Security functions ... 21

Appendix I – Deployment model with WoT ... 23

Appendix II – Examples of HN applications ... 25

II.1 Home security ... 25

II.2 Customer support with controlling access right to device ... 25

II.3 Room facility coordination for better sleep ... 26

Appendix III – Security considerations based on [ITU-T X.1111] ... 27

Bibliography ... 30

Recommendation ITU-T Y.2070

Requirements and architecture of the home energy management system and home network services

1 Scope

This Recommendation provides the requirements and architecture of the home energy management system (HEMS) and home network (HN) services. The HEMS supports energy efficiency and reduction of energy consumption by monitoring and controlling devices such as home appliances, storage batteries and sensors connected to the HN from the HEMS application with the HN service architecture. The HEMS is one of the HN services. The other HN services, such as home security and healthcare, are provided with the same architecture as the HEMS and by monitoring and controlling the devices from the application specific to the service. In this Recommendation, the requirements, the reference architecture and the functional architecture including functional relationship are described to support the HEMS and the other HN services.

This Recommendation covers the followings:

- overview of the HN service architecture for the HEMS and other HN services;
- requirements for the device, home gateway (HGW) and management platform (PF) in the HN service architecture as well as the security required for the architecture;
- reference architecture with four ways to connect to the devices from the HGW according to the device type: basic device (IP based and non-IP based) and non-basic device (connecting to the HGW directly or through the adapter);
- functional architecture with the entities: device, HGW, management PF and application;
- functional relationship with three functional categories in the functional architecture: device operation, application execution and management;
- security model and functions for the HN services mainly describing the HEMS.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1111] Recommendation ITU-T X.1111 (2007), *Framework of security technologies for home network.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 demand response [b-FG-Smart Terminology]: A smart grid feature that allows consumers to reduce or change their electrical use patterns during peak demand, usually in exchange for a financial incentive. Mechanisms and incentives for utilities, business, industrial, and residential customers to cut energy use during times of peak demand or when power reliability is at risk. Demand response is necessary for optimizing the balance of power supply and demand.

NOTE – Smart grid [b-FG-Smart Terminology]: A two way electric power delivery network connected to an information and control network through sensors and control devices. This supports the intelligent and efficient optimization of the power network.

3.1.2 device object [b-ECHONET Lite]: A logical model of the information held by equipment devices or home electrical appliances such as sensors, air conditioners and refrigerators, or of control items that can be remotely controlled. The interface form for remote control is standardized. The information and control target of each device is specified as property, and the operating method (setting and browsing) is specified as a service.

3.1.3 home network [b-ITU-T J.190]: A short-range communications system designed for the residential environment, in which two or more devices exchange information under some sort of standard control.

3.1.4 presence [b-ITU-T Y.2720]: A set of attributes that characterize an entity relating to the current status.

3.1.5 smart meter [b-FG-Smart Terminology]: Smart meter is a premise device to monitor and control of electrical power usage of home devices based on "demand response information" from home devices. But, it is not recommended that the smart meter controls directly per each premise appliances because of the private security policy. To control and manage the each premise appliances, it is required for home management system such as home gateway and home server to support the control and management.

3.1.6 web of things [b-ITU-T Y.2063]: A way to realize the IoT where (physical and virtual) things are connected and controlled through the world wide web.

3.1.7 web resource [b-W3C WCterms]: A resource, identified by a URI, that is a member of the web core.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 adapter: An entity used to connect a non-basic device to the home gateway by converting the dedicated communications protocol to the IP based protocol and the dedicated data model to the abstract data model.

3.2.2 device management: A variety of functionalities to manage a collection of the devices including primary capabilities: auto-configuration and dynamic service provisioning, software/firmware image management, software module management, status and performance monitoring, and diagnostics.

3.2.3 fault diagnosis: An example of a maintenance action, which is a sequence of elementary maintenance activities carried out for a given purpose.

3.2.4 home controller: A small computer for the application for the home energy management system to monitor and control the home equipment such as home appliances and storage batteries to reduce energy consumption.

3.2.5 home energy management system: A computer system comprising a software platform providing basic support services and a set of applications providing the functionality needed for the effective operation of home equipment, such as home appliances and storage batteries, so as to assure adequate security of energy supply at minimum cost.

3.2.6 home gateway: An always on, always connected device which acts as the central point connecting the devices on the home network to the applications on the wide area network, and monitors and performs actions on data flows within the home network as well as on bi-directional communication flows between the home network and the wide area network.

3.2.7 home network resource: A device (e.g., home appliance, storage battery, sensor), a network device (e.g., hub and access point in the home network) and network capacity for data transmission among them for the home network services.

3.2.8 in-home display: A user screen device to present home energy consumption information. Users can optionally control their home devices with its user interfaces.

3.2.9 managed agent: A software program running on the device to set the configuration information and to collect the information of the device. The managed agent gets the information from the resource management function on the management platform for the configuration of the device and sends the collection of the internal status of the device to it for various home network services including remote management and fault diagnosis.

3.2.10 management platform: A platform which has common functions providing the interface and the management for the home network applications, and the virtual device management and the resource management for the home gateway and the devices.

3.2.11 wide area network: An IP based communication network that covers a wide geographical area including the Internet and accommodates devices and local area networks.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CPU	Central Processing Unit
DB	Database
DR	Demand Response
EV	Electric Vehicle
HEMS	Home Energy Management System
HGW	Home Gateway
HN	Home Network
HTTP	Hypertext Transfer Protocol
IHD	In-Home Display
IP	Internet Protocol
L2	Layer 2
LAN	Local Area Network
MAC	Message Authentication Code
NAT	Network Address Translation
PF	Platform
SOAP	Simple Object Access Protocol
WAN	Wide Area Network

WoT	Web of Things
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

5 Conventions

In this Recommendation,

- The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.
- The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview

This overview clause describes the HN service architecture. The HEMS is one of the HN services. There are other HN services, such as the home security service, for example, which detects a suspicious person with the human aware sensors. The HEMS and other HN services are provided with the HN service architecture. Clause 6.1 describes the HN service architecture. Clause 6.2 describes how the HEMS is provided by the HN service architecture by replacing the HN applications with the HEMS application.

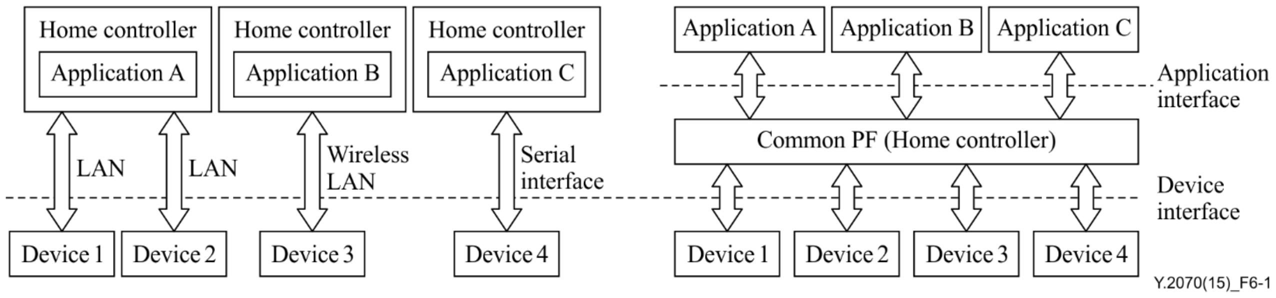
With the more widespread deployment of HN services and the increase of the devices connected to the HN, it is more complicated and more difficult for application developers to develop applications for the HN; a deep knowledge about the HN devices and communications protocols is required. Therefore, the development of an architecture for the HN services to support the application developers is important and forms the background of this Recommendation.

NOTE –The term “Internet” is used in the description in clause 6 to support a clear understanding by the reader. However, it should be understood as the wide area network (WAN), which includes the Internet. The term WAN is used from clause 7 onward in this Recommendation.

6.1 HN service architecture

HN applications have been developed to run on dedicated home controllers, which are located in the home. As shown in Figure 6-1(a) individual access, every home controller connects to one or more devices (home equipment) such as home appliances and storage batteries, each of which has its own dedicated communication interface at the device interface. For this reason, each application needs to be developed to meet with the device interface of the connecting device in order to monitor and control the device.

On the other hand, as the communications protocols are standardized, devices are connecting with the standardized protocol to the common PF, which works on the home controller as shown in Figure 6-1(b). In this, common access, diagram, it is possible to abstract the device interface by the common PF and the devices can be accessed from HN applications which are also connected to the common PF at the application interface.



(a) Individual access (b) Common access

Figure 6-1 – Two access types for HN services

Figure 6-2 below shows an HN service architecture that is composed of two types of architecture.

Figure 6-2(a) shows an architecture in which all of the devices and the home controller are placed inside the home, and the applications and the common PF work on the home controller. This is referred to as the aggregate type architecture in this Recommendation. Figure 6-2(b) shows an architecture in which the devices are located inside the home, but the applications can be placed on the Internet. The functions of the common PF are separately distributed to the HGW inside the home and the management PF on the Internet, instead of on the home controller. This architecture enables the applications to access the devices from the Internet. This architecture is referred to as the distribute type architecture in this Recommendation.

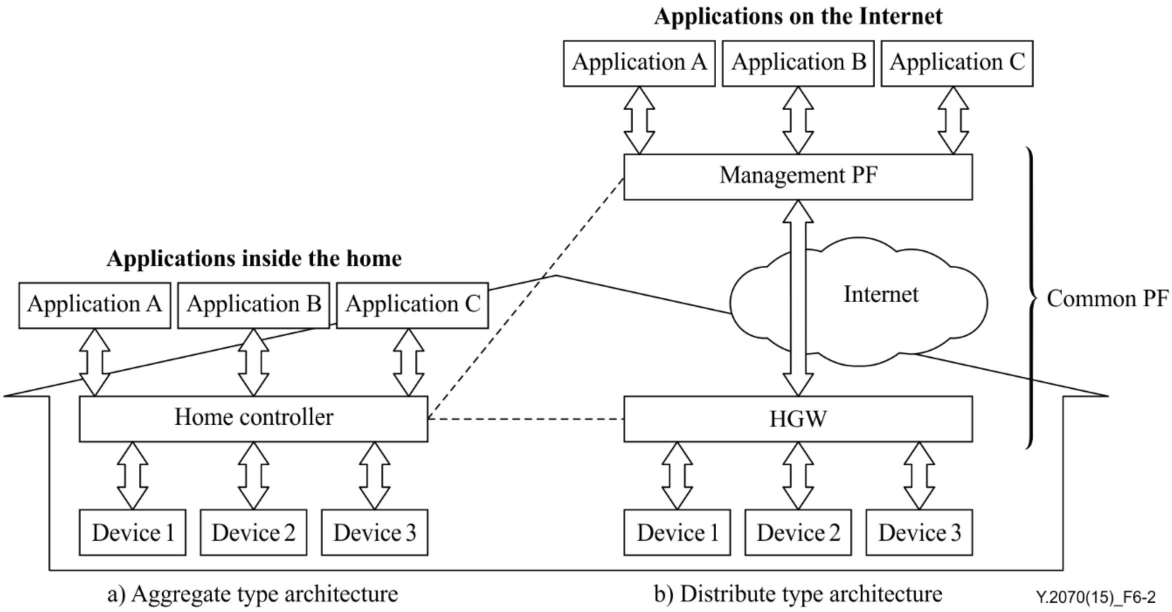


Figure 6-2 – The HN service architecture

Both types of the architecture are within the scope of this Recommendation since both architectures have the same functions of the common PF. In the following clauses, however, the distribute type architecture is mainly described.

6.2 HEMS based on HN service architecture

The HEMS, based on the HN service architecture, is described in this clause, clarifying the features of the architecture.

6.2.1 HEMS and HN service architecture

The HEMS is generally considered to provide the following services:

- Visualization of the energy consumption by the entire house, or by selected devices such as home appliances, storage batteries with power sensors and the smart meter.
- Realization of energy-efficiency and/or cutting energy usage during peak demand by monitoring and controlling the devices.

The HEMS application is one of the HN applications; therefore, the architecture for the HEMS can be the same as that for other HN services which are within the HN service architecture.

The HN service architecture applied for the HEMS is shown in Figure 6-3. This is the distribute type architecture shown in Figure 6-2(b), where by the HEMS application replaces the HN applications.

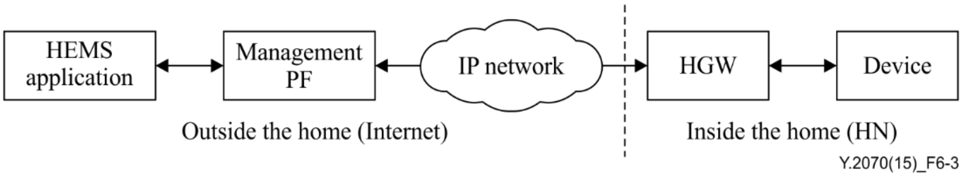


Figure 6-3 – HEMS based on HN service architecture

In Figure 6-3, everything to the left of the HGW (on the left side of the dotted line) is considered the Internet (outside the home) and everything to right hand side is considered the HN (inside the home).

Devices such as home appliances, storage batteries and power sensors connected to the HN are monitored and controlled from the HEMS application on the Internet in this architecture, and in order to do so, the HGW bridges the Internet and the HN. The HGW converts the various types of communications protocols used for communication with the devices to the protocol, which is used on the Internet for communication with the management PF. The management PF is placed on the Internet and provides a web-based application interface. The HEMS application runs through this interface.

With the HGW and the management PF, it is possible for the HEMS application to discover and identify devices connected to the HN and to access them using their identifiers. In this way, the HEMS application monitors and controls the individual devices and enables the HEMS.

By making use of a standardized communication protocol between the HGW and the management PF, the HEMS application does not need to take into consideration the interfaces of the devices or the communications protocols used between the HGW and the devices. The devices are represented as web resources by the management PF. Therefore this architecture supports application developers by allowing them to develop applications without deep knowledge about multiple device interfaces and communications protocols.

6.2.2 HEMS examples

This clause describes two HEMS examples based on the HN service architecture; these show the features of the architecture.

In Figure 6-4, devices such as a home appliance, e.g., an air conditioner, and power sensors are connected to an HGW in the home, using various networks and protocols such as standardized communications protocols and dedicated communications protocols depending on the interface of each device. A HEMS application runs on the Internet and connects to the devices through the HGW and the management PF. In this architecture, the HEMS application collects the electronic power consumption data of the home appliance from the power sensors through the HGW and the management PF, and sends the data to visualize the energy consumption in the web text-based format to the web browser on the in-home display (IHD). It may be also possible to make the system send the data to web browser on a smart phone so that the end users can refer to the energy consumption from outside the home.

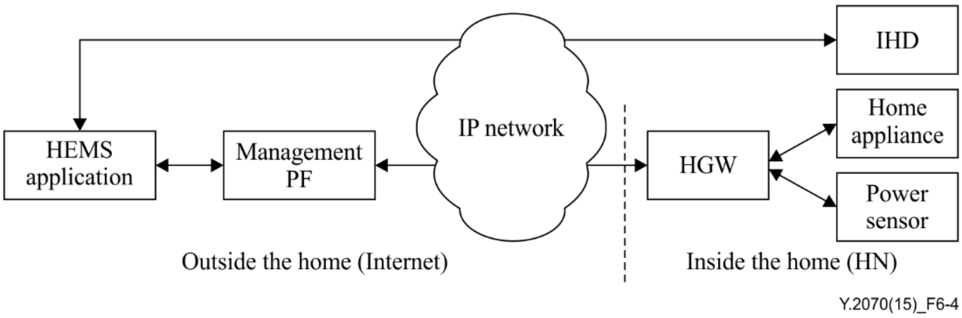


Figure 6-4 – Visualization of energy consumption with IHD

This service may provide the end user with a visualization of the energy consumption in a graphical representation, e.g., for the past week. For this service, the management PF stores the data received from the power sensors and provides them to the HEMS application when required.

In Figure 6-5, a HEMS application makes use of a utility company's service, such as the demand response (DR) service. This architecture enables new services by combining Internet-based services. This is the main feature of this architecture in which the application is placed on the Internet.

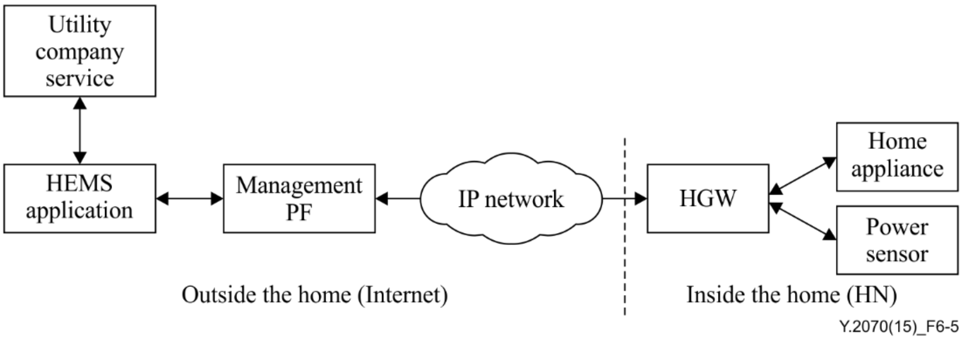


Figure 6-5 – Energy consumption control with DR

6.3 Merits of HN service architecture

The previous clauses showed the HN service architecture and how to apply the architecture to the HEMS. Although some of the merits of the architecture are described in the previous clauses, they are also summarized below.

As described in clause 6.1, the HN service architecture is composed of the aggregate type architecture (Figure 6-2(a)) and the distribute type architecture (Figure 6-2(b)), and both architectures have the same functions of the common PF. The merits of the HN service architecture (both the aggregate type architecture and the distribute type architecture) are described below in items 1) through 3).

1) It enables application developers to develop applications with the application interface on the common PF (i.e., the home controller in the aggregate type architecture and the management PF in the distribute type architecture) to provide various services.

2) It enables easier and lower-cost introduction of services for end users who can install by themselves devices that support plug-and-play functionality. It is not necessary for the end users to be concerned about the connections to the devices.

3) It enables the common PF to maintain the entire system and the HN resources remotely. The common PF provides functions for auto-configuration of devices and for detection of faults

occurring on the HN. These functions make the system more stable and provide services at a lower cost.

The distribute type architecture has a function on the management PF to cooperate with devices and applications working on networks that have different policies. Thus, there are some additional merits to the distribute type architecture; these are described below in items 4) through 6).

4) It avoids increasing hardware resources, such as central processing unit (CPU) or memory on the home controller which would lead to an increase in service costs when providing other HN services in addition to the HEMS. It enables modifying/adding applications on the Internet without hardware restrictions.

5) It enables the applications to easily monitor and control the devices on the HN with the management PF, which provides the application programming interface (API) needed to access the devices. This access is enabled even in the case where a firewall and network address translation (NAT) protects the devices from illegal access from the Internet.

6) It enables easy development of security-conscious applications by providing functions for the authentication and the authorization for the devices and the HGW, and the encryption for the HN.

7 Requirements

This clause describes requirements for the device, the HGW and the management PF in the HN service architecture, as well as for the security required for the architecture. Since the functions of the HEMS are specified in clause 6.2, the following requirements are extracted for the HEMS. As the HN service architecture is applied not only for the HEMS but also for other HN services, the following are also requirements for these other HN services as well. The requirements for the applications are out of the scope of this Recommendation.

7.1 Requirements for the device

The following are requirements for the device:

1) requirement for device operation

   - device object

     It is required to have a device object which is an abstract data model representing the functions of the device.

   NOTE – For a device that does not have a device object, the adapter or the HGW connecting to the device directly is required to have a device object.

2) requirements for management:

   - managed agent

     It is required to respond to the resource information collector function of the HGW.

     It is required to check the status of the device itself for fault diagnosis.

     It is required to set the configuration of the device and the network device such as the hub and the access point in the HN.

7.2 Requirements for HGW

The followings are requirements for the HGW:

1) requirement for device operation

   - data format and protocol (hypertext transfer protocol (HTTP)/Internet protocol (IP)) conversion

It is required to convert the format of the device object to that of the virtual device and Internet protocol (IP) to HTTP as the protocol which delivers the format on the WAN with the secure communication to the management PF.

2) requirements for management

- resource information collector

  It is required to discover the devices that are newly connected to the HN, identify each of them and manage their status.

  It is required to collect the internal status of each device and other HN resources, and the traffic status of the HN in order to determine the cause of any fault when the HN service is not working well.

3) requirements for application execution

- application for disconnect

  It can optionally work autonomously, continuing to control devices and store data with a backup purpose application in case of network disconnection from the management PF.

  It can optionally take some tasks with the backup purpose application and work with the management PF.

7.3 Requirements for management PF

The followings are requirements for the management PF:

1) requirements for device operation

- virtual device

  It is required to provide a web-friendly representation corresponding to the device object.

  It is required to monitor and control the virtual device.

  It can optionally be enabled to take the plural functions in one physical device as plural virtual devices and the plural physical devices as one virtual device.

NOTE – The physical device represents the device connected to the HN. The term physical device is used to distinguish it from a virtual device.

2) requirements for management

- resource management

  It is required to discover, activate, monitor and control the devices connected to the HGWs.

  It is required to identify the devices globally unique from the applications.

  It is required to register the HGW's profile, give the HGW an identifier, register the end user who owns the HGW and identify the HGW with the authenticated user information.

3) requirements for application execution

- application management

  It is required to have the capability of authenticating and authorizing applications with acceptance by the end user to connect to the devices.

  It can optionally store the data received from the devices through the HGW.

- application interface

  It is required to have a web-based application interface for the HEMS and other HN services.

7.4 Requirements for security

The following are requirements for security:

- secure communication

  It is required to securely communicate between the devices and the application through the WAN.

NOTE – HEMS security requirements to support secure communication are listed in Table III.2.

- device authentication

  It is required for the management PF to have the capability to authenticate the devices.

8 Reference architecture

This clause describes the reference architecture for the HEMS. This architecture can also be applied to other HN services.

Figure 8-1 shows the distribute type reference architecture and the reference points of the architecture.

In Figure 8-1, the left side of the HGW is the WAN (i.e., outside the home) and right side is the HN. The HGW is IP based and it bridges the WAN and the HN.

This reference architecture is shown with the categorized devices; basic device and non-basic device. The basic device has a device object which is an abstract data model representing functions of the device. The interface of the basic device is provided to the HGW with the abstract data model and is represented in the management PF as virtual devices, which the applications monitor and control.

There are some standardized specifications for the interface of the basic device. Some of them support IP based communications protocols and the others support non-IP based protocols. Therefore, the two types of basic devices are those having the interface for the IP based protocol and those having the interface for the non-IP based protocols.

The non-basic device does not have the device object. Since it supports its dedicated interface, an adapter is required to connect a non-basic device to the HGW. If the HGW provides the function of the adapter, the non-basic device can be connected directly to the HGW.

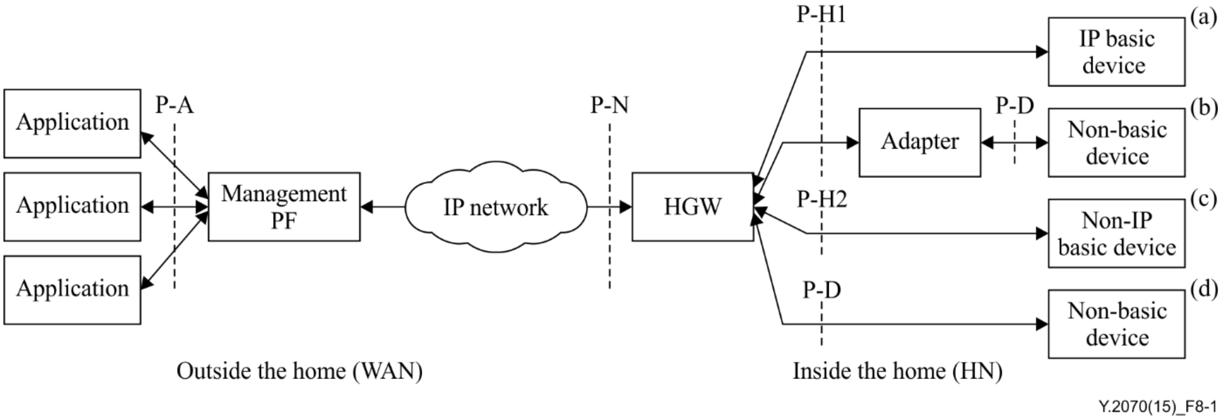


Figure 8-1 – Reference architecture and reference points

In Figure 8-1, the following reference points are defined. The application interface in Figure 6-1 corresponds to the P-A reference point in Figure 8-1. The device interface shown in Figure 6-1 corresponds to the P-H1, the P-H2 and the P-D reference points in Figure 8-1.

1) P-A reference point

The P-A reference point allows the applications to access the management PF through web-based application interfaces and to monitor and control the physical devices connected to the HN as logical devices of web resources. This reference point enables the applications to create and delete the logical devices, and to read and update the properties for them.

2) P-N reference point

The P-N reference point allows the management PF to access the HGW, placed in the home, through the WAN. This reference point enables the management PF to activate the devices, to get their status, and control them by specifying the property's value as a function of the resource management.

3) P-H1 reference point

The P-H1 reference point allows the HGW to access the basic device with the IP based communications protocol (IP based basic device), and the adapter which converts the non-basic device connecting it to the basic device. This reference point enables the HGW to activate the devices, get the status of, and control them by specifying the property's value.

4) P-H2 reference point

The P-H2 reference point allows the HGW to access the basic device with the non-IP based communications protocol (non-IP based basic device). This reference point enables the HGW to activate the devices, get the status of, and control them by specifying the property's value.

5) P-D reference point

The P-D reference point allows the adapter and the function of the adapter equipped in the HGW to access the non-basic device with the dedicated communications protocol, which connects to the device interface. This reference point enables the HGW to activate the devices, get the status of, and control them by specifying the property's value.

The devices in the home are connected to the HGW through the HN in one of four ways. The following is a description of the devices from (a) to (d) shown in Figure 8-1.

Device (a) is an IP based basic device that connects directly to the HGW at the P-H1 reference point. It makes use of the IP based communications protocol between the device and the HGW as the device has an interface to connect to the protocol. [b-ECHONET Lite] is one of such communications protocols.

Device (b) is a non-basic device and supports its dedicated interface. To connect to the HGW, this device requires an adapter which converts the dedicated communications protocol implemented by the interface of the device to the IP based protocol, and which converts the dedicated data model to the abstract data model. Therefore, device (b) will be recognized as a basic device by the adapter. A battery charger for electric vehicles (EVs) connecting to the HN with a serial interface is an example of this type of device.

Device (c) is a basic device, but supports the non-IP based communications protocol only because the non-IP based communications protocol is used for communication directly with the HGW.

Device (d) is a non-basic device and it is the same as device (b). In Figure 8-1, the device connects to the HGW directly since the HGW has functions of the adapter for device (d).

The HGW has a function to discover the newly-installed devices automatically. The HGW receives notifications of the installation of the devices and alarms when malfunctions occur. This raises the system's reliability. It also allows the end users the ability to easily install devices and to get the HEMS and other HN services started. The HGW converts the various types of the communications protocols, used for communicating with the devices, to the protocols which are used on the WAN for communication with the management PF at the P-N reference point. For example, the communications protocol used for communication with the devices will be converted into HTTP.

The communication between the HGW and the device (through the adapter) may not be encrypted regardless of whether the IP or non-IP based communications protocol is used. However, the communication between the HGW and the management PF through the WAN is encrypted or is on a secured communications protocol such as HTTP to ensure secure communication. HTTP can be utilized on the standardized device management protocol such as [b-BBF TR-069].

The management PF is a server that provides the web-based application interface on the WAN. The applications run through the interface at the P-A reference point. By making use of the standardized communications protocol between the HGW and the management PF, the applications do not need to take into consideration the interface of the devices or the communications protocols used on the HN. The devices are represented as web resources by the management PF. In this way the application developers can develop applications without deep knowledge about the devices.

NOTE – A deployment model with the web of things (WoT) specified in [b-ITU-T Y.2063] is shown in Appendix I.

9 Functional architecture

This clause describes the functional architecture for the HEMS. This architecture can also be applied to other HN services.

Figure 9-1 shows the distribute type functional architecture for the IP based basic device. The functions in this architecture are composed of three categories: device operation, application execution and management. The details for each category are described in clause 10. Although the device is shown as an IP based basic device in Figure 9-1, this architecture can also be applied to other types of devices with the appropriate deployment of the functions between the HGW and the device. The architectures for each type of device are shown in clause 10.1.1 to 10.1.4. The architecture between the management PF and the application is the same for all types of devices as shown in Figure 9-1.

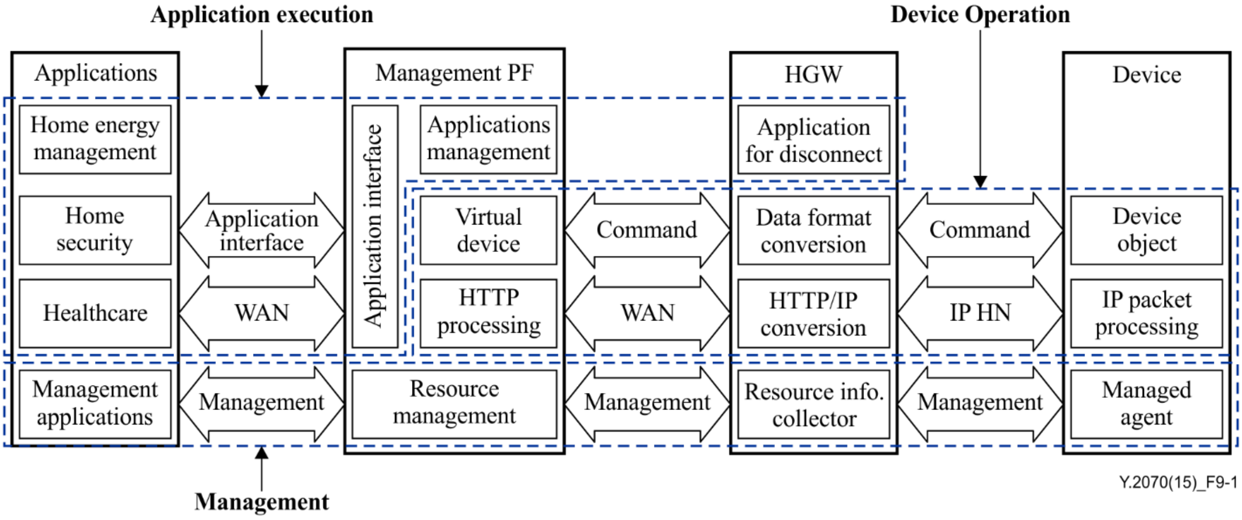


Figure 9-1 – Functional architecture for IP based basic device

The devices have their own proprietary functions. The functions are defined as profiles and are transmitted with communications protocols to the application via the HGW and the management PF. This architecture enables the application to monitor and control the devices.

Although Figure 9-1 shows the IP based communications protocol for the IP based basic device, the IP based, the non-IP based and the dedicated communications protocols can be used for the communication between the HGW and the devices as described in clause 8. The commands transmitted between the HGW and the devices provide control methods for the HGW to the devices such as "GET" to get their status, "SET" to specify their properties and/or set the value and "INFORM" to request notification about their status and the events that have occurred in them. The HGW converts the communications protocol into HTTP and communicates to the management PF through the WAN.

The communications protocol for device management such as [b-BBF TR-069] can be used between the HGW and the management PF. [b-BBF TR-069] refers to the generalized device data model with extensible markup language (XML) in [b-BBF TR-181] and this data model is communicated between them with commands such as "GET", "SET" and "INFORM". The XML format is specified for each communications protocol used between the HGW and the devices.

The management PF stores device status and configuration data transmitted via the HGW. The management PF manages virtual devices and provides them to the application through a web-based application interface so that the application developers can develop applications to control the physical devices as web resources.

The following clauses describe each entity. The functions of the device and the HGW are described for the IP based basic device. The functions for other types of devices are shown in clause 10.1.2 to 10.1.4. The functions for the management PF and the applications are common to all types of devices.

NOTE – Examples of HN applications are described in Appendix II.

9.1 Device

The IP based basic device provides the following functions:

1) functions for device operation
   - device object;
   - IP packets processing.
2) function for management
   - managed agent.

Device object and managed agent are described in the following clauses. IP packet processing is not described, as it does not require specific operations.

9.1.1 Device object

The basic device has the device object. It is composed of properties that specify the device functions which are independent of the implementation of the manufacturers. The properties are logical internal items to get the device status and to control the device functions, which can be remotely accessed and controlled from the application. The data form for the remote control is specified as the tuple of <property, value>. Since the device object is specified for each type of device (e.g., home appliance, storage battery), existing home appliances made by different manufacturers would be remotely controlled in exactly the same way.

For example, air conditioners have properties of operating status, temperature setting and operation mode, which are defined as the property configurations in [b-ECHONET Lite]. [b-SEP 2.0] and [b-ISO/IEC 14543-3-x] also define similar property configurations. The HGW specifies the property to get the data (value) from them. To configure or control them, it specifies the property and sets the appropriate value. For example, to set the targeted temperature of an air conditioner, it specifies the property, which is appointed for the targeted temperature and sets the appropriate value (e.g., 25 (degrees)).

9.1.2 Managed agent

The managed agent is a function for the management to keep the HN stable. It is important to get the information about all of the HN resources because lack of this information could cause failure of fault detection thus, making determination of the causes of the fault difficult. The managed agent holds the internal status of the device and transfers it on demand to the resource management function of the management PF via the resource information collector of the HGW. This detail is described in clause 10.3.

9.2 HGW

The HGW bridges the WAN and the HN. It provides the following functions when it connects to the IP based basic device:

1) function for device operation
   - data format and protocol (HTTP/IP) conversion.
2) function for management
   - resource information collector.
3) function for application execution
   - application for disconnect.

9.2.1 Data format and protocol (HTTP/IP) conversion

This is a function of the device operation to convert the communications protocol. On the WAN, HTTP is usually utilized as the communications protocol. Thus, the HGW converts the communications protocol used on the HN to HTTP.

The tuple of <property, value> of the physical devices is communicated to the HGW through the HN and put into HTTP at the HGW for further communication with the management PF. It is widely known that [b-BBF TR-069] specifies the simple object access protocol (SOAP) based communications protocol; thus it is one of the candidate communications protocols for the device management between the HGW and the management PF. The extensible messaging and presence communications protocol (XMPP) is also a candidate.

9.2.2 Resource information collector

This is a management function used to collect information about the HN resources, for each of the HGW devices, and to deliver it to the resource management function on the management PF. This function also discovers the devices newly connected to the HGW, and sets the configuration for these devices. The HGW gives a unique identifier to each of the devices for management.

9.2.3 Application for disconnect

The application for disconnect function provides a backup purpose application to keep the devices connected to the HN working when the WAN is disconnected for any reason. If the WAN disconnects, this backup purpose application sets the proper configuration for the situation instead of the application running on the WAN. The application interface for this backup application is based on HTTP and provides the API, which manages the device object using the converted data format.

9.3 Management PF

The management PF manages the physical devices as virtual devices and provides them as web resources to the application through the web-based application interface. The management PF provides the following functions:

1) functions for device operation
   - virtual device;
   - HTTP processing.
2) function for management
   - resource management.
3) functions for application execution

- applications management;
- application interface.

These functions are described in the following clauses, except for HTTP processing: it is not described because it does not require specific operations.

9.3.1 Virtual device

The virtual device is the device representation corresponding to the device object of the basic device connected to the HN. The properties of the device are represented in XML format in order to be easily handled by the web applications. The function is described in clause 10.1.

The virtual device provides two functions for the device abstraction. The first function provides abstraction of the devices' properties and the communication protocols. For example, if vendor A and vendor B give different properties to similar functions of their air conditioners, the management PF creates a virtual device by converting the property of the devices (e.g., air conditioners) to the same properties.

The second function provides virtual separation to the plural virtual devices which are made from the plural functions in one physical device. For example, an air conditioner controlling its power based on its motion sensor has the property based on the data detected by the motion sensor. Thus, the air conditioner has two functions: air conditioning and motion sensing. Two virtual devices (i.e., air conditioning device and a motion sensing device) will be created from one physical device (i.e., air conditioner).

9.3.2 Resource management

The resource management on the management PF provides the function to gather information of the HN resources which the managed agent collects. It also manages the internal status of the device, the network device and the network capacity for each HGW to detect fault and to provide the fault processing. The details are described in clause 10.3.

9.3.3 Applications management

The applications management registers the information of the application and holds the relationships between the applications and the devices. This function delivers data from the devices to the appropriate applications. In addition, it has the historical data management function which stores the data received from the devices instead of the applications. The function provides the data of the devices, for example for the past 24 hours, in responding to the requirement of the application.

9.3.4 Application interface

The application interface is a web-based interface used to monitor and control the devices through the HGW from the application by accessing the virtual devices on the management PF as web resources. This makes it possible, therefore, for application developers to develop applications with this interface.

This interface does not support the management as shown in Figure 9-1.

9.4 Application

Although the architecture in this Recommendation does not require common functions for the applications, three functions in the applications which provide the following three operations that make use of the functions of the management PF are described in this clause. These three functions are: the device management function, the device operation function and the fault diagnosis function as shown in Figure 9-2. Every application in the application entity shown in Figure 9-1 can have these functions.

The three functions are described below with their corresponding operation.

1) function: device management, operation: registration

The applications that access the devices are registered to the applications management function in the management PF. This operation is performed by the device management function in the application and enables exclusive control to the devices and specifies the application to which the data of the devices is delivered automatically.

2) function: device operation, operation: monitor & control

The device operation function in the application monitors and controls the devices by getting and setting the configurations. ON / OFF control to the devices is one example. This operation is performed by monitoring and controlling the virtual devices in the management PF which is described in clause 10.2. The operation from the virtual devices to the physical devices on the HN is described in clause 10.1.

3) function: fault diagnosis, operation: fault detection

The fault diagnosis function in the application gets the status and configuration data of the HN resources. This function connects to the resource management in the management PF and gets the HN related information detected by the resource management and provide it to those applications which need the information.

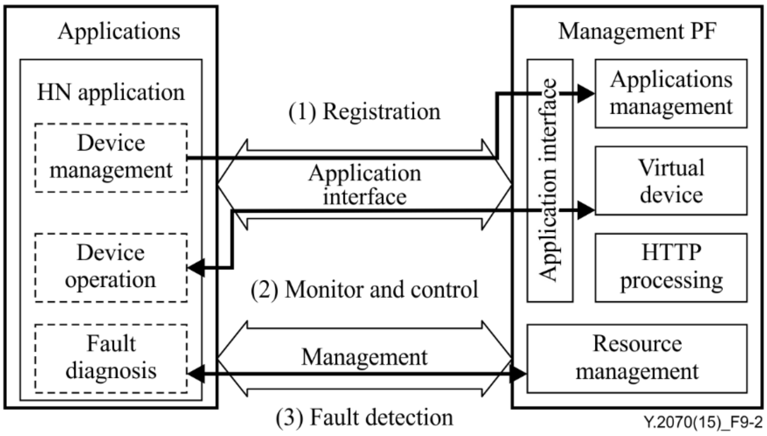


Figure 9-2 – Three operations for the HN applications

10 Functional relationship

In this clause, details of the three functional categories: device operation, application execution and management shown in Figure 9-1 are described to clarify the relationship between the entities.

10.1 Device operation

The device operation provides a function to monitor and control the devices from the management PF. Since there are four ways to connect to the devices from the HGW according to the device types shown in Figure 8-1, four operations for each device type are described in the following clauses.

10.1.1 Operation for IP based basic device

Figure 10-1 shows the functional architecture for the IP based basic device operation (i.e., device (a) in Figure 8-1). The IP based basic device has two functions; device object and IP packets processing. The virtual device on the management PF is the device representation corresponding to the device object of the basic device. The applications remotely monitor and control the devices by specifying the properties of the virtual devices through the application interface.

The two-tuple of <property, value> is the data form used to control the device. The device command is transferred to the HGW on the IP based communications protocol through the HN and to the management PF on the HTTP based protocol through the WAN. The HGW converts the device command between the HN and the WAN since the form of the tuples on the HN is different from that on the WAN. Therefore, the HGW has two functions: data format conversion that converts the form of the tuple, and protocol (HTTP/IP) conversion that converts the communications protocol on the HN to HTTP.

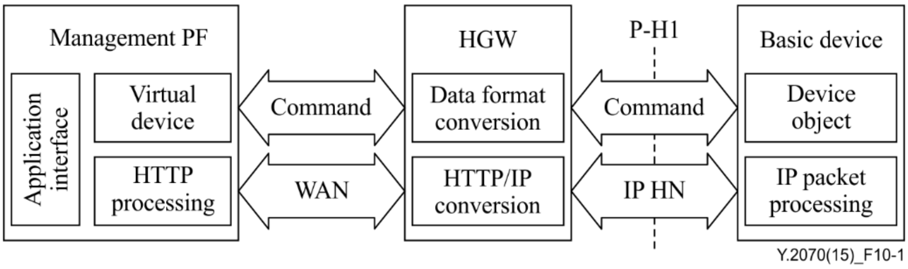


Figure 10-1 – Functional architecture for IP based basic device operation

10.1.2 Operation for non-IP based basic device

Figure 10-2 shows the functional architecture for the basic device used to connect to the HGW with the non-IP based communications protocol (i.e., device (c) in Figure 8-1). In this case, the device command is transferred at the P-H2 reference point. The layer 2 (L2) frame processing function can be used to convert the non-IP based communications protocol, which the device supports, to the IP based protocol in the HGW. The communications protocol between the HGW and the management PF can be the same as the IP based basic device shown in Figure 10-1.

The device interface of [b-SEP 2.0] supports the P-H2 reference point.

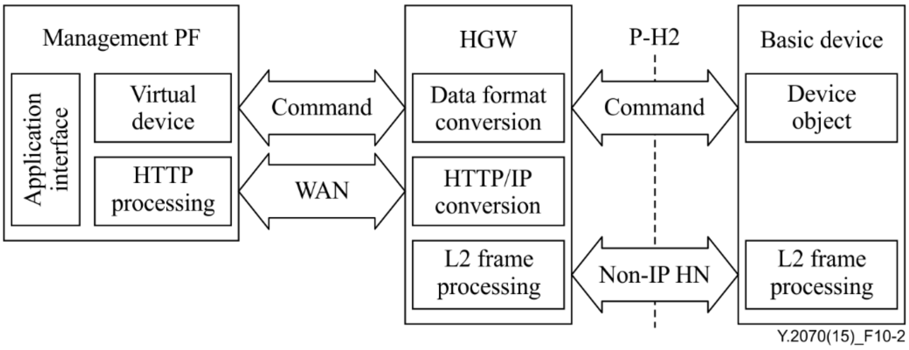


Figure 10-2 – Functional architecture for non-IP based basic device operation

10.1.3 Operation for non-basic device with adapter

Figure 10-3 shows the functional architecture for the non-basic device operation with the adapter (i.e., device (b) in Figure 8-1). This Recommendation defines the non-basic device for the existing devices that do not have the device object. The non-basic device does not have the device object, but has the dedicated interface, for example the serial interface, at the reference point P-D. The adapter has the device object and provides the same interface as the basic device. The adapter, placed between the device and the HGW, works to convert the non-basic device to be recognized as a basic device at the reference point P-H1. In this way, the adapter converts the dedicated protocol to the IP based protocol such as [b-SEP 2.0], [b-ECHONET Lite], [b-ISO/IEC 14543-3-x] and [b-BACnet]. The device object is provided in the device abstraction function. The device abstraction function also provides the device interface conversion function that converts the property of the device to the operational procedure to the device at the reference point P-D.

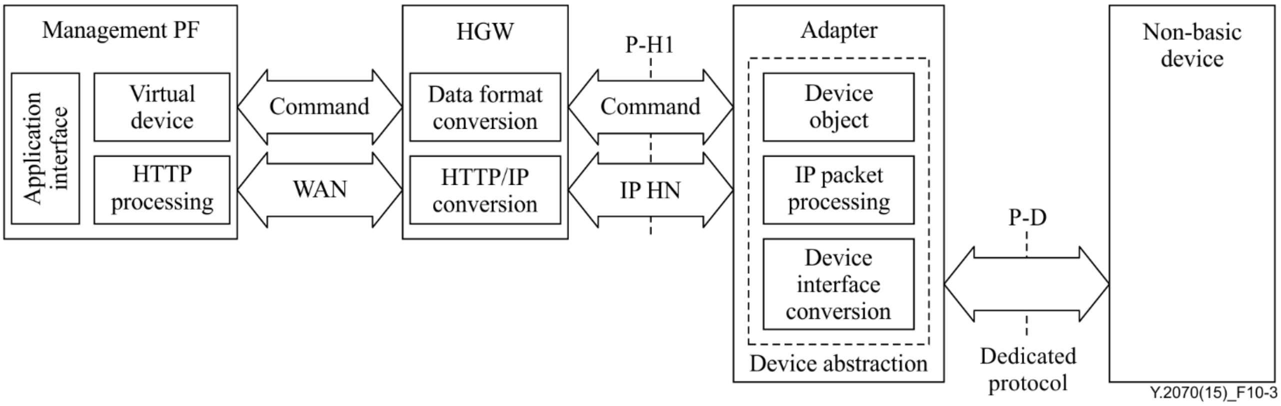


Figure 10-3 – Functional architecture for non-basic device operation with adapter

10.1.4 Operation for non-basic device with adapter function in HGW

Figure 10-4 shows the functional architecture for the non-basic device operation connecting directly to the HGW (i.e., device (d) in Figure 8-1). For the non-basic device, the HGW equips the function of the adapter (the device abstraction function) instead of placing the adapter to connect to the device directly. The device abstraction function inside the HGW provides the same interface as the basic device. The device abstraction function also supports the operational procedure at the reference point P-D and the non-basic device connects to the HGW directly as shown in Figure 10-4.

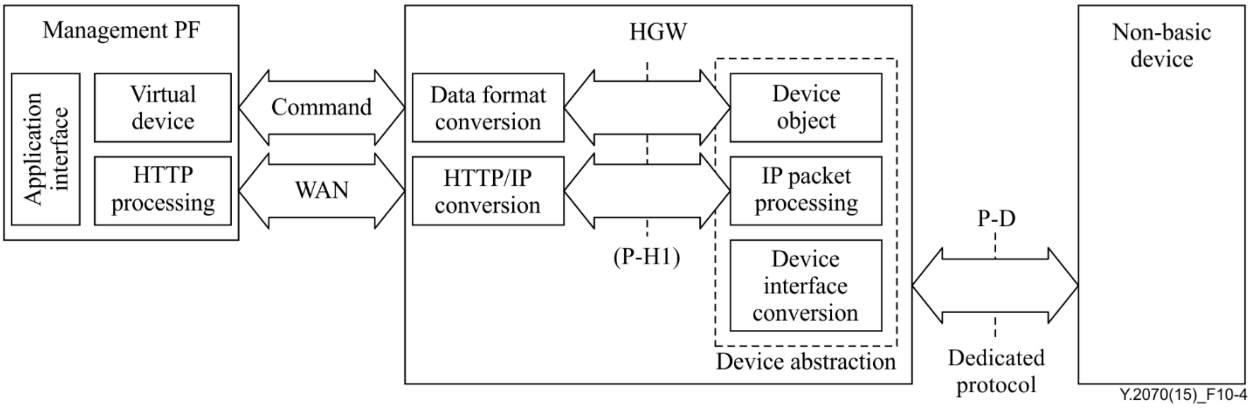


Figure 10-4 – Functional architecture for non-basic device operation with adapter function in HGW

10.2 Application execution

Setting and getting the value of the property of the virtual device on the management PF by the application results in monitoring and controlling the physical devices connected to the HN. As shown in Figure 10-5, the application interface on the management PF converts the virtual device to the web resource, enabling the application to monitor and control the physical devices with the HTTP protocol.

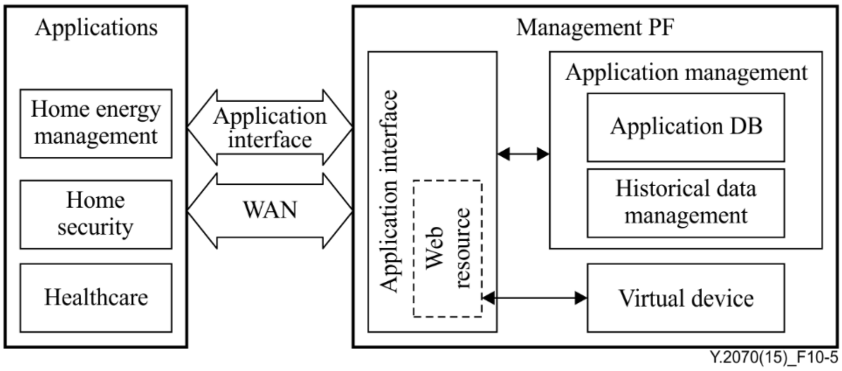


Figure 10-5 – Functional architecture for application execution

The applications management is composed of two functions: application database (DB) and historical data management.

The application DB maintains a list of the applications connected to the management PF through the WAN. The application DB is used to deliver data to the targeted application from the HGWs and the other applications.

The historical data management function is described in clause 9.3.3.

10.3 Management

The HN is sometimes very complex; many different types of technologies may co-exist in the HN. The devices connected to the HN are used in a variety of fields. The HN could have a complicated topology composed of various HN resources (e.g., devices and/or access points). It could be difficult to manage and maintain the HN for end users, since there is no administrator or technician in the home. Therefore, resource management is provided to support a variety of fault determination processes and fault recovery processes, including easy configuration with no administrators and with remote administrators.

Figure 10-6 shows the functional architecture of the management for the HN with the basic devices. For the non-basic devices, which do not have the managed agent, the adapter or the HGW provides the managed agent.

There is the resource management function in the management PF, which holds the information and configuration data of the HN resources. The HGW has the resource information collector function. It gets status, performance and configuration data of the HN resources, detects faults and provides fault processing. It also provides easy configuration procedures of the HN resources for end users. It configures the HN resources with minimum settings required for their operation. The managed agent on the device executes configuring and gathering the home environment information by the instruction from the resource information collector function on the HGW. The management application is the application for use by remote administrators such as call centers and customer support centers. It provides a function to display the entire resource information for faults diagnosis and to set the specified properties for recovery operation from such faults.

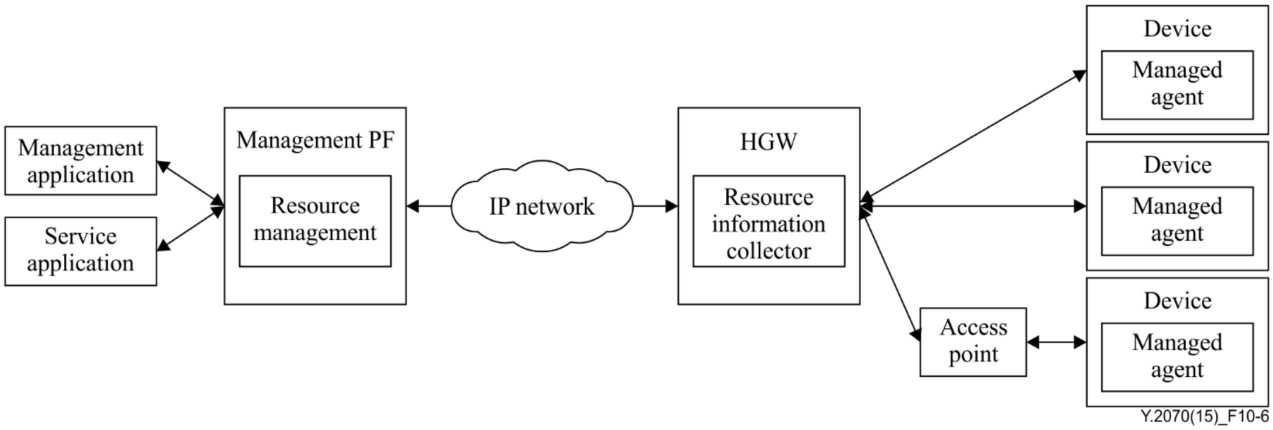


Figure 10-6 – Functional architecture for management for basic device

11 Security support

This clause describes the security model and functions for the HN services, especially the HEMS. The general security requirements and technologies for the HN are described in [ITU-T X.1111]. This Recommendation applies the technologies in [ITU-T X.1111] to the HN service architecture to establish secure communications between the device and the application through the WAN. A HEMS model for security is shown in clause 11.1. As the result of the security considerations on the HEMS model in Appendix III, the security functional architecture is shown in clause 11.2.

11.1 HEMS model for security

This clause describes a HEMS model for security shown in Figure 11-1 which is based on the distribute type architecture shown in Figure 6-4. Since the HEMS is just one of the HN services, this model can also be applied to the general HN model.

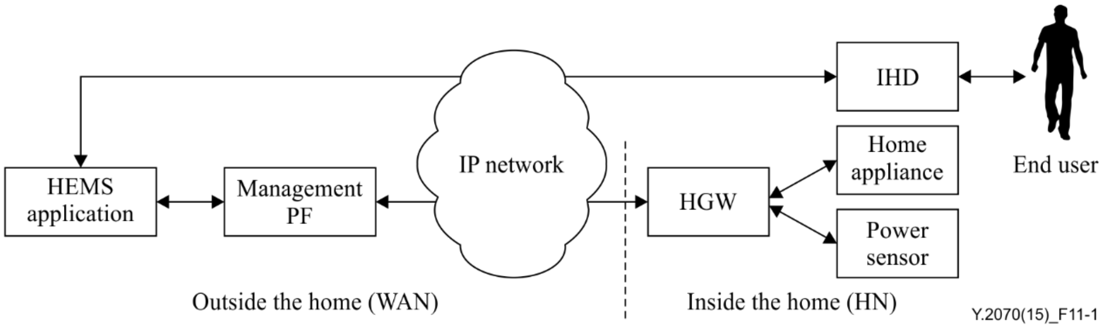


Figure 11-1 – HEMS model for security

In Figure 11-1 the end user uses the web browser on an IHD to connect to the HEMS application with a secure connection. The web browser on the IHD connects to the HEMS application through a broadband router in the home. The HEMS application collects data of the devices (e.g., home appliance properties and power sensor properties) and controls them in response to instructions from the end user.

The HN security is specified in [ITU-T X.1111] and this Recommendation refers to [ITU-T X.1111] as a framework for security technologies in the HN.

The entities and the relationships in this model are required to be specified since they are different from those in [ITU-T X.1111]. There are six entities in this model: end user, IHD, HEMS application, management PF, HGW and device such as home appliance or power sensor. There are five relationships in this model: between end user and IHD, IHD and HEMS application, HEMS application and management PF, management PF and HGW, and HGW and device.

In Appendix III, the security considerations of this model are described based on the process in [ITU-T X.1111] and the relationship between the security functions and this model is shown in Table III.3.

11.2 Security functions

The devices are expected to have some of the security functions specified in [ITU-T X.1111]. Figure 11-2 shows the security functional architecture derived from the result of the considerations in Appendix III based on the technologies in [ITU-T X.1111]. In Figure 11-2, the security functions shown with a solid line or dotted line represent required functions or optional functions respectively. Although nine security functions are specified in Table III.3 of Appendix III, the security functions in Figure 11-2 are simplified into three functions (i.e., anti-availability, message authentication and entity authentication) taking [b-ISO/IEC 27000] into account. The anti-availability function provides protection from attacks by an unauthorized entity. The message authentication function protects information being transmitted from modification, to maintain accuracy and completeness. The entity authentication function identifies the device to protect it from making information of the entity available to unauthorized entities.

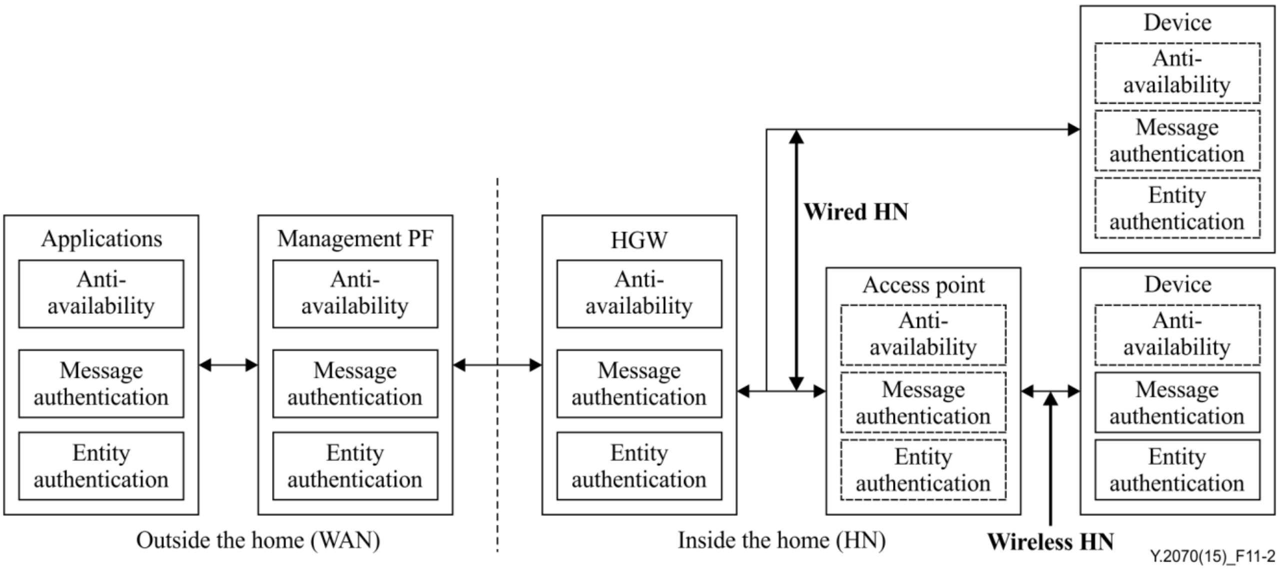


Figure 11-2 – Security functional architecture

Since actual devices such as home appliances and sensors do not have capabilities of the full security functions, in many cases because of its low performance, two solutions to compensate for the limitation of the device's security functions are provided as described below.

First, the management PF and the HGW support security functions as shown in Figure 11-2. In addition, the broadband router (not shown in Figure 11-2), which is usually placed between the WAN and the HN, generally has firewall functions. In this way, the devices connecting to the HGW with the wired HN are usually allowed to have no security functions and the devices connecting with the wireless HN are allowed to have only the least security functions required for the wireless connection. Therefore, the message authentication function and the entity authentication function between the device and the access point are required for the secure wireless connection as shown in Figure 11-2.

NOTE – The security functions on the access point shown in Figure 11-2 are those which are required from the HGW through the wired HN and are optional functions.

Another solution is to provide the following entity authentication functions for the HGW and the device by the resource management in the management PF described in clause 10.3. When the HN is maintained to be secure, this is a simple and effective method to provide the entity authentication.

1) HGW authentication

The authentication information of the HGW is pre-registered in the management PF until the HGW connects to the management PF for the first time. When the first connection to the HGW is established, the resource management compares it with the pre-registered information. The information is managed in the resource management function.

2) device authentication

The information identifying the devices is pre-registered in the management PF until they connect to the HGW to accommodate the case where devices do not have the capability of the security functions. The device authentication is provided as a function and is used to determine consistency between their pre-registered information in the management PF and their data when they connect to the HGW.

3) device access control

The entity authentication function to the physical devices is provided as a function of access control to the virtual devices in the management PF.

Appendix I

Deployment model with WoT

(This appendix does not form an integral part of this Recommendation.)

In [b-ITU-T Y.2063] the physical device on the WoT is divided into two categories: constrained device and fully-fledged device.

- constrained device: A constrained device cannot connect to the Internet and has no functionality of the web. The device interacts with an agent of the WoT broker.
- fully-fledged device: A fully-fledged device has the functionalities of the web. The device can interact, not only with the WoT broker, but also with the services on the web.

The constrained device and the fully-fledged device do not have the device object and hence they correspond to the non-basic device described in this Recommendation. The constrained device communicates with the HGW through the adapter then further communicates with the management PF. The fully-fledged device can also communicate with the management PF by way of the HGW.

In this Recommendation, the HGW, which has the function of the resource information collector, manages all of the devices connected to it through the HN including constrained devices and fully-fledged devices.

[b-ITU-T Y.2063] defines the WoT broker and the physical devices can be accessed as web resources through it from the application. Its functional architecture is divided into the service layer and the adaptation layer where the service layer corresponds to the management PF and the adaptation layer corresponds to the HGW in this Recommendation.

The web adaption function of the WoT broker supports only the adaptation of the communications protocol to the web protocol for communication between the physical devices and the WoT services. Therefore the web broker supports the P-D reference point only in this Recommendation. Figure I.1 shows the deployment model in which the HGW is connected to a constrained device and a fully-fledged device.

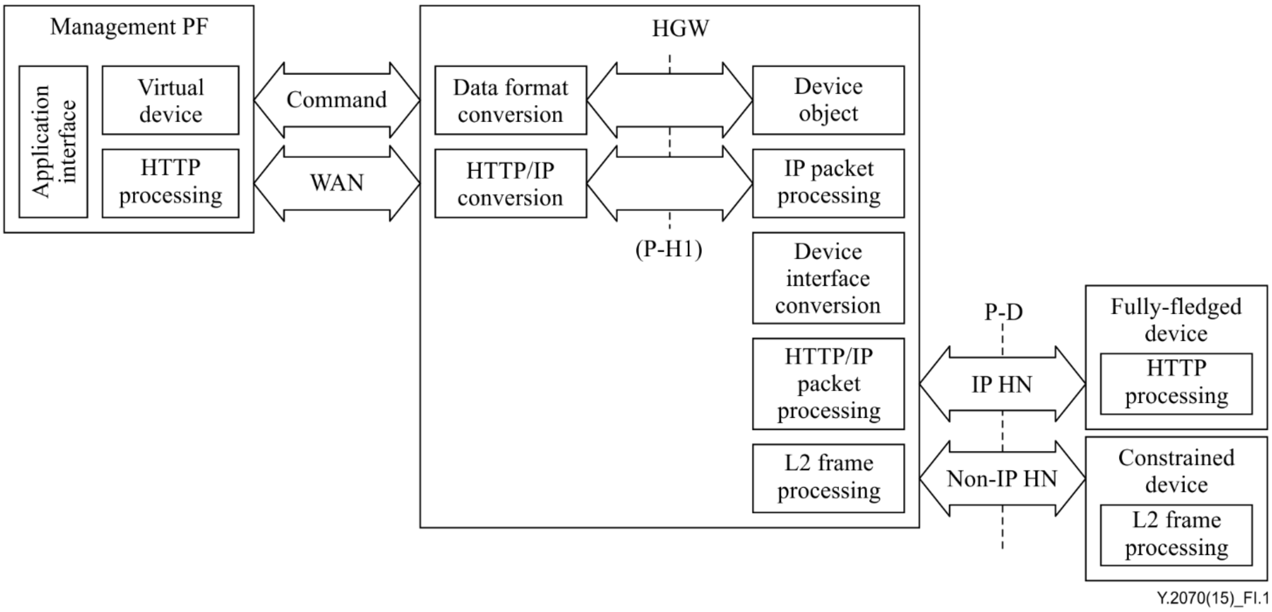


Figure I.1 – Deployment model with WoT

The management PF provides the virtual devices to the application developers to be treated as web resources through the web-based application interface so that they can develop applications for the mash-up service defined in [b-ITU-T Y.2063], which is a combined service integrating WoT services in a WoT broker with web services outside of the WoT broker.

In this way the architecture in this Recommendation provides the HEMS and the other HN services with the WoT.

Appendix II

Examples of HN applications

(This appendix does not form an integral part of this Recommendation.)

The distribute type architecture can be applied to various HN services. The following are examples of HN applications that support these services.

II.1 Home security

A home security application detects threats using sensors installed in the home and alerts the security company to dispatch security guards. The sensors, such as human-aware sensors which detect suspicious persons, or fire sensors which detect a fire, are connected to the home security application through the HGW and the management PF.

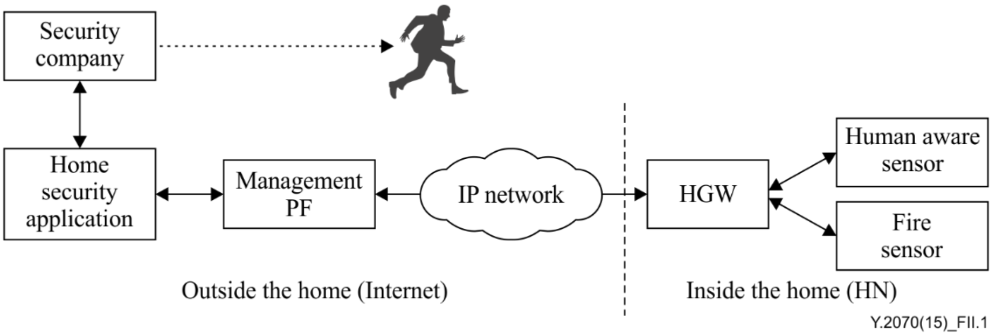


Figure II.1 – Architecture with home security application

II.2 Customer support with controlling access right to device

Customer support is an important service as the HN is getting more complex with the variety of devices being connected. When the service does not work well, it is difficult to determine why and where the fault happens. The example shown in Figure II.2 assumes that two different customer support services are separately provided through the same management PF for each of the supporting devices (appliances) produced by companies A and B respectively.

When the devices produced by more than two different companies are installed on the HN, the challenge for each device company is that each company could get fault information about the devices produced by the other company. Most of device companies prevent other companies from getting this information.

Figure II.2 shows three services running on the management PF. In this case, the HN service provider's application is able to get diagnostic information, such as network disconnections through the management PF. The customer support service gets the detailed diagnostic information about the supporting device (e.g., the customer support service for company A gets the detailed fault information about the supporting device produced by company A). This service is provided because the management PF has a function for distributing information to the proper services.

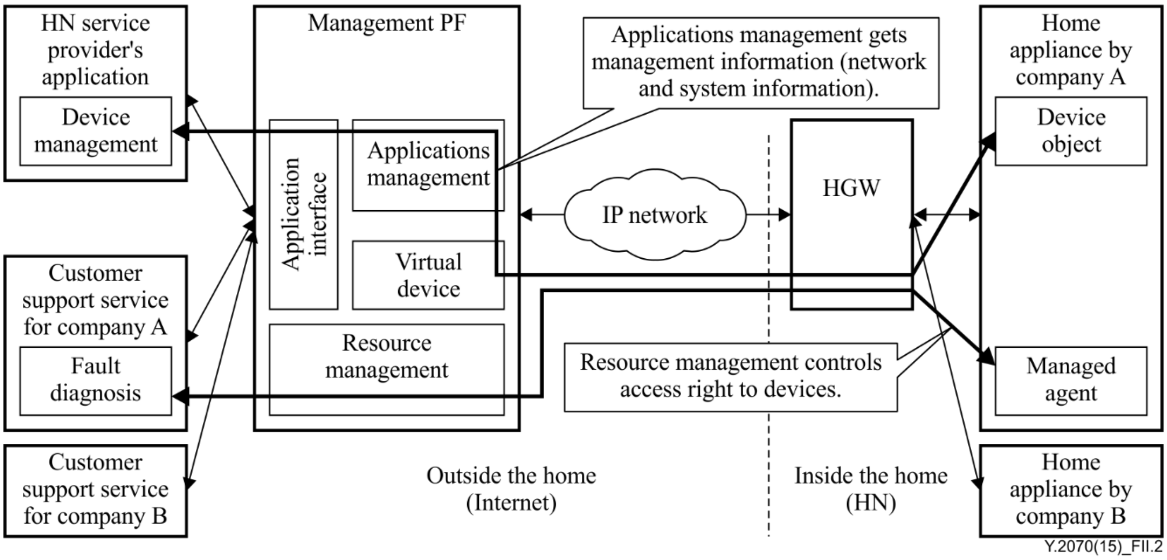

HN service provider's application
Device management
Customer support service for company A
Fault diagnosis
Customer support service for company B
Management PF
Application interface
Applications management
Virtual device
Resource management
Applications management gets management information (network and system information).
IP network
HGW
Resource management controls access right to devices.
Outside the home (Internet)
Inside the home (HN)
Home appliance by company A
Device object
Managed agent
Home appliance by company B
Y.2070(15)_FII.2

Figure II.2 – Architecture with customer support application

II.3 Room facility coordination for better sleep

The room facility coordination service for better sleep maintains a suitable environment for sleep by adjusting room temperature, humidity and illumination by controlling the air conditioner and the lighting fixture. To achieve the condition for better sleep, sleep sensors monitor the sleep pattern, heart rate, breathing rate and snoring of the user to calculate the condition for better sleep.

As the sleep sensor information is highly sensitive, the management PF strictly controls and delivers it to the proper service. In this case, the sleep monitoring service gets the data delivered from the sleep sensor exclusively. It provides the information about the suitable environment for better sleep to the room facility coordination service, as metadata, through an external interface. Then the room facility coordination service controls the air conditioner and the lighting fixture.

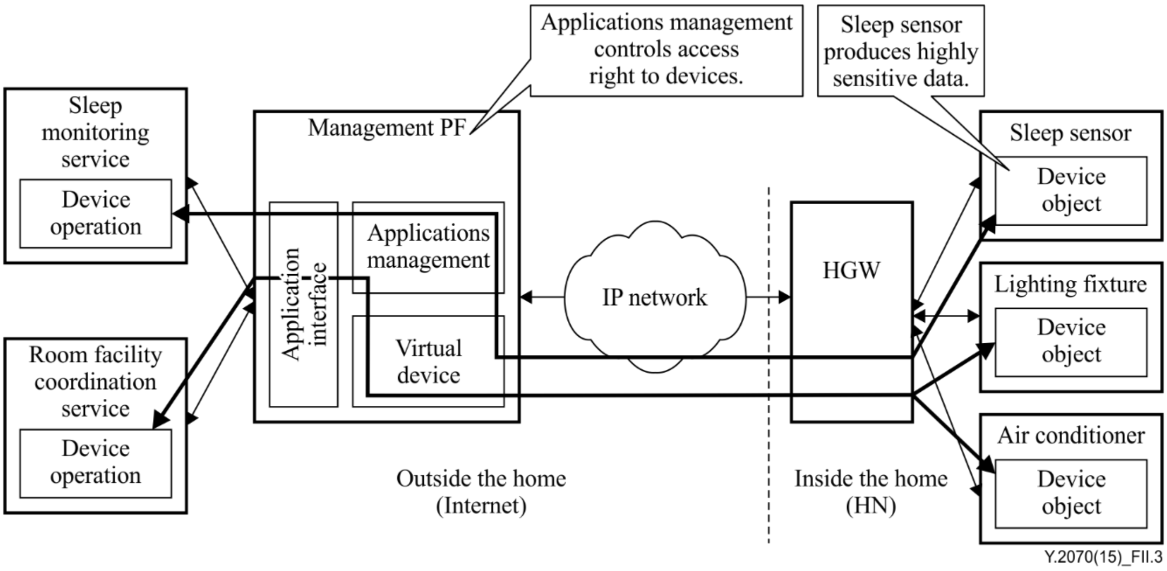


Figure II.3 – Architecture with room facility coordination application for better sleep

Appendix III

Security considerations based on [ITU-T X.1111]

(This appendix does not form an integral part of this Recommendation.)

[ITU-T X.1111] defines entities, relationship between the entities, security threats and security requirements, and describes security functions based on them. In Figure 11-1, there are six entities from the end user to the device and five relationships between them. Table III.1 shows the relationships of the security threats to the HEMS model.

Table III.1 – Relationship of security threats to HEMS model

Entity or relations	**General security threats**					
	Disclosure/ Eavesdropping	**Interrup-tion**	**Modification/ Injection**	**Unauthorized access**	**Repudiation**	**Packet abnormal-forwarding**
Device	Y	Y	Y	Y		
HGW	Y	Y	Y	Y		Y
MPF	Y	Y	Y	Y		
Application	Y	Y	Y	Y		
IHD	Y	Y	Y	Y		
User/IHD				Y		
IHD/Application	Y	Y	Y	Y		
Application/MPF	Y	Y	Y	Y		
MPF/HGW	Y	Y	Y	Y	Y	
HGW/Device	Y	Y	Y	Y	Y	
NOTE – MPF and user stand for the management PF and the end user respectively. The notation "xxx/yyy" in the column of "Entity or relations" means the relation between xxx and yyy. The letter "Y" in a cell designates that a particular threat exists for a specific entity or relation.						

Although in [ITU-T X.1111] there are descriptions about mobile-oriented security threats, these are out of the scope of this Recommendation; it focuses on the security from the HN application to the devices. Table III.2 shows the relationships between the HEMS security requirements, the threats and the functions based on the security requirements listed in [ITU-T X.1111].

Table III.2 – Relationship of HEMS security requirements, threats and functions

Security requirement	General security threats	Security functions
Data confidentiality	Disclosure/Eavesdropping Unauthorized access	Encryption Access control Key management
Data integrity	Modification/Injection Packet abnormal-forwarding	Integrity Message authentication code (MAC) Digital signature Notarization Key management
Authentication	Disclosure/Eavesdropping Interruption Modification/Injection Unauthorized access Repudiation	MAC Digital signature Notarization Key management
Non-repudiation	Repudiation	Digital signature Notarization Key management
Access control or authorization	Disclosure/Eavesdropping Interruption Modification/Injection Unauthorized access	Encryption MAC Entity authentication Digital signature Access control Key management
Availability	Interruption	MAC Entity authentication Digital signature Access control Key management Anti-availability
Privacy security	Disclosure/Eavesdropping	Encryption MAC Entity authentication Digital signature Access control Key management
Communication flow security	Packet abnormal-forwarding	Integrity MAC Entity authentication Access control Key management

The relationship between the security functions and the HEMS model for security (see Figure 11-1) are sorted in Table III.3 based on the security functions listed in Table III.2.

Table III.3 – Relationship between security functions and model

Entity or relations		Security Function								
		Encryption	**Integrity**	**MAC**	**Entity authentication**	**Digital signature**	**Notarization**	**Access control**	**Key management**	**Anti-availability**
Stored data	Device	Y	Y	Y	Y	Y	–	–	–	Y
	HGW	Y	Y	Y	Y	Y	Y	Y	Y	Y
	MPF	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Application	Y	Y	Y	Y	Y	Y	Y	Y	Y
	IHD	Y	Y	Y	Y	Y	Y	Y	Y	Y
Communication data	User/IHD	Y	–	–	Y	Y	–	–	Y	Y
	IHD/Application	Y	Y	Y	Y	Y	–	Y	Y	Y
	Application/MPF	Y	Y	Y	Y	Y	Y	Y	Y	Y
	MPF/HGW	Y	Y	Y	Y	Y	–	Y	Y	Y
	HGW/Device	Y	Y	Y	–	–	–	–	–	Y

NOTE – MPF and user stand for the management PF and the end user respectively. The notation "xxx/yyy" in the column of "Entity or relations" means the relation between xxx and yyy. The letter "Y" in a cell designates that a particular security service can be provided by a corresponding security function.

When taking the relationship between the security functions and the model in Table III.3 into consideration, the security functions required for the entities in the architecture provided in this Recommendation are shown in Figure 11-2.

The security functions are simplified into three functions shown in Figure 11-2, taking [b-ISO/IEC 27000] into account. They are the anti-availability, message authentication and entity authentication function. The common functions such as encryption and key management are omitted. The other functions are merged into the three functions. These functions correspond to the requirements of the information security: availability, integrity and confidentiality specified in [b-ISO/IEC 27000].

NOTE – [b-ISO/IEC 27000] provides the information security management system. The requirements are defined as follows:

- **availability**: property of being accessible and usable upon demand by an authorized entity;
- **integrity**: property of accuracy and completeness;
- **confidentiality**: property that information is not made available or disclosed to unauthorized individuals, entities or processes.

Bibliography

[b-ITU-T J.190]	Recommendation ITU-T J.190 (2002), *Architecture of MediaHomeNet that supports cable-based services*.
[b-ITU-T Y.2063]	Recommendation ITU-T Y.2063 (2012), *Framework of the web of things*.
[b-ITU-T Y.2720]	Recommendation ITU-T Y.2720 (2009), *NGN identity management framework.*
[b-ISO/IEC 14543-3-x]	ISO/IEC 14543-3-x:2006/2007, *Information technology – Home Electronic System (HES) architecture – Part 3-x.*
[b-ISO/IEC 27000]	ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
[b-BACnet]	ANSI/ASHRAE, *Standard 135-2004*.
[b-BBF TR-069]	Broadband Forum (2011), *TR-069 Amendment, 4CPE WAN Management Protocol.*
[b-BBF TR-181]	Broadband Forum (2012), *TR-181 Issue 2 Amendment 6, Device Data Model for TR-069.*
[b-ECHONET Lite]	ECHONET Consortium, *ECHONET Lite Specification Version 1.10.*
[b-FG-Smart Terminology]	ITU-T FG Smart Deliverable (2011), *Smart Grid Terminology.*
[b-SEP 2.0]	ZigBee Alliance, *Smart Energy Profile 2.0 Application Protocol.*
[b-W3C WCterms]	W3C (1999), *Web Characterization Terminology & Definitions Sheet.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015