ISO/IEC 14543-5-102

Edition 1.0 2020-02

INTERNATIONAL STANDARD

colour inside

Information technology – Home electronic system (HES) architecture – Part 5-102: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Remote universal management profile

ISO/IEC 14543-5-102:2020-02(en)

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

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

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

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and definitions clause of IEC publications issued between 2002 and 2015. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

ISO/IEC 14543-5-102

Edition 1.0 2020-02

INTERNATIONAL STANDARD

colour inside

Information technology – Home electronic system (HES) architecture – Part 5-102: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Remote universal management profile

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 35.240.67

ISBN 978-2-8322-7521-4

CONTENTS

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) ARCHITECTURE – Part 5-102: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Remote universal management profile

FOREWORD

1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees and ISO member bodies.

3) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC National Committees and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO, IEC or ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

5) ISO and IEC do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. ISO or IEC are not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC National Committees or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this ISO/IEC publication may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 14543-5-102 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

The list of all currently available parts of the ISO/IEC 14543 series, under the general title *Information technology – Home electronic system (HES) architecture*, can be found on the IEC website and ISO website.

The text of this standard is based on the following documents:

FDIS	Report on voting
JTC1-SC25/2898/FDIS	JTC1-SC25/2908/RVD

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

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

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

INTRODUCTION

ISO/IEC 14543-5 (all parts) specifies the services and protocol of the application layer for intelligent grouping and resource sharing (IGRS) devices and services in the home electronic system. Some parts reference Classes 1, 2 and 3, which are HES designations specified in the HES architecture standard, ISO/IEC 14543-2-1.

ISO/IEC 14543-5 (all parts) includes the following parts.

– ISO/IEC 14543-5-1: Core protocol
  - Specifies the TCP/IP protocol stack as the basis and the HTTP protocol as the message-exchange framework among devices.
  - Specifies a series of device and service interaction/invocation standards, including device and service discovery protocol, device and service description, service invocation, security mechanisms, etc.
  - Specifies core protocols for a type of home network that supports streaming media and other high-speed data transports within a home.
– ISO/IEC 14543-5-2#: Application profile
  - Based on the IGRS core protocol.
  - Specifies a device and service interaction mechanism, as well as application interfaces used in IGRS basic applications.
  - Multiple application profiles are specified, including:
    i) ISO/IEC 14543-5-21: AV profile
    ii) ISO/IEC 14543-5-22: File profile
– ISO/IEC 14543-5-3: Basic application
  - Includes an IGRS basic application list.
  - Specifies a basic application framework.
  - Specifies operation details (device grouping, service description template, etc.), function definitions and service invocation interfaces.
– ISO/IEC 14543-5-4: Device validation
  - Defines a standard method to validate an IGRS-compliant device.
– ISO/IEC 14543-5-5: Device type
  - Specifies IGRS device types used in IGRS applications.
– ISO/IEC 14543-5-6: Service type
  - Specifies basic service types used in IGRS applications.
– ISO/IEC 14543-5-7: Remote access system architecture
  - Specifies the architecture and framework for the remote access of IGRS devices and services in the home electronic system. The remote access communications protocol and application profiles are specified in the following parts of ISO/IEC 14543-5:
    i) ISO/IEC 14543-5-8: Remote access core protocol
    ii) ISO/IEC 14543-5-9: Remote access service platform
    iii) ISO/IEC 14543-5-101: Remote media access profile
    iv) ISO/IEC 14543-5-102: Remote universal management profile
    v) ISO/IEC 14543-5-11: Remote user interface
    vi) ISO/IEC 14543-5-12: Remote access test and verification
  - The relationships among these parts are specified in Part 5-7.

– ISO/IEC 14543-5-8: Remote access core protocol
  - Provides detailed system components, system function modules, basic concepts of IGRS remote access elements and their relationships, message exchange mechanisms and security related specifications.
  - Specifies interfaces between IGRS remote access (RA) client and service platforms. Defines co-operative procedures among IGRS RA clients.
– ISO/IEC 14543-5-9: Remote access service platform
  - Specifies the IGRS RA service platform (IRSP) architectures and interfaces among servers in the service platforms.
  - Based on ISO/IEC 14543-5-8: Remote access core protocol.
– ISO/IEC 14543-5-101 and ISO/IEC 14543-5-102: Remote access application profiles
  - Defines a device and service interaction mechanism for various applications.
  - Based on ISO/IEC 14543-5-8: Remote access core protocol.
  - Two profiles have been developed:
    i) ISO/IEC 14543-5-101: Remote media access profile. This part defines the common requirements for IGRS RA media users and devices in IGRS networks.
    ii) ISO/IEC 14543-5-102: Remote universal management profile. This part specifies a mechanism for integrating devices with both relatively high and low processing capabilities into IGRS networks. It also specifies universal remote device discovery and a management framework.
  - Additional application profiles will be specified in the future.
– ISO/IEC 14543-5-11: Remote user interface
  - Specifies adaptive user interface generation and remote device control mechanisms suitable for different remote access applications and devices.
– ISO/IEC 14543-5-12: Remote access test and verification
  - Defines a standard method to test and verify IGRS-RA compliant device and service interfaces.

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) ARCHITECTURE –

Part 5-102: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Remote universal management profile

1 Scope

This part of ISO/IEC 14543 specifies the system architecture and communication protocols of remote universal management profile to achieve intelligent grouping, resource sharing and service collaboration among different devices and controllers. The protocol features are:

a) remote universal device discovery and management framework that includes connection methods and network architecture, device configuration interfaces, management message formats and message exchange flows;

b) request/response message formats for four remote universal management profile device types: water heater, refrigerator, air conditioner, microwave.

This document is applicable to remote access of water heaters, refrigerators, air conditioners, microwave ovens at home, office or other remote environments, to achieve universal management and interactions among these controllers and devices.

2 Normative references

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

ISO/IEC 14543-5-1, *Information technology – Home electronic system (HES) architecture – Part 5-1: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Core protocol*

ISO/IEC 14543-5-7, *Information technology – Home electronic system (HES) architecture – Part 5-7: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Remote access system architecture*

ISO/IEC 14543-5-8, *Information technology – Home electronic system (HES) architecture – Part 5-8: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Remote access core protocol*

ISO/IEC 14543-5-9, *Information technology – Home electronic system (HES) architecture – Part 5-9: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Remote access service platform*

ISO/IEC 15045 (all parts), *Information technology – Home electronic system (HES) gateway*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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

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

3.1.1
account server
IGRS RA server that processes services related to user and device account information

3.1.2
application server
IGRS RA server or third-party server located outside of an IGRS RA system that processes application service-related logical functions

Note 1 to entry: The application server provides the approach to access application service logical functions (also called logics). By using the application server, IGRS RA user or device or other server can access the application service logics.

3.1.3
controlled device
device
physical device that is accessible to the controller

3.1.4
controller
physical device that can access a controlled device in the IGRS RA system

Note 1 to entry Controller is typically a mobile device or application such as a smart phone or smart pad, which is handled by an IGRS RA user.

3.1.5
device ID
unique identification of an IGRS RA device

EXAMPLE If the local part of a device ID is “#igrsdevice” and the domain name part of the user ID is “igrs.com”, the device ID is “#igrsdevice@igrs.com”.

Note 1 to entry A device ID consists of a local part and a domain name part. A “@” is used to separate the two parts. Each device ID starts with a “#”.

3.1.6
device verification code
string used to examine if the user has the authority to bind a device

Note 1 to entry: For a device without a user interface, the device verification code is used to bind a device to a user. The device owner guarantees the safety of the device verification code.

3.1.7
IGRS AS
basic service unit composed of one or multiple IGRS servers

Note 1 to entry: Each IGRS AS provides services for a dedicated user and/or device group and constructs an IGRS RA domain. This document defines all of the necessary requirements that allow different IGRS ASs to exchange messages with each other.

3.1.8
IGRS RA agent
functional entity which can provide the IGRS RA service to IGRS LAN devices

Note 1 to entry: The main functionalities of the IGRS RA agent are sending instructions to and receiving instructions from the IGRS RA service platform, and translating the instructions of local IGRS networks to and from those of the IGRS RA networks. The IGRS RA agent provides compatibility of the local IGRS devices to the IGRS RA devices.

3.1.9
IGRS RA device
physical device that is accessible to the IGRS RA user in the IGRS RA system

3.1.10
IGRS RA server
instantiation of a service provider that may be included in an IRSP

Note 1 to entry An IGRS RA server is deployed on the internet. It maintains relationships among IGRS RA user and IGRS devices. It also provides re-transmission of collaborative messages. The IGRS RA user and IGRS device can start a data connection to the IRSP and support interconnections using the data connection and re-transmission functions of the IRSP.

3.1.11
IGRS RA service platform
IRSP
collection of multiple IGRS RA servers that are deployed on the internet to maintain the relationships among IGRS RA user and IGRS RA device and to exchange collaborative messages

Note 1 to entry: IGRS RA user and device can establish connections to the IRSP, can send collaborative messages over these connections and can exchange messages in the servers of the IRSP.

3.1.12
IGRS RA user
entity that uses the IGRS RA devices and application services

Note 1 to entry Generally, an IGRS RA user is a human being. Each IGRS RA user has a unique user ID (identification). A bundle relationship can be established between one IGRS RA user and another. A binding relationship can be established between one IGRS RA user and one IGRS device.

3.1.13
message server
IGRS RA server that processes message exchanging logics (transmitting, receiving, forwarding and blocking, etc.)

3.1.14
server address
ID to identify the network location of a server in IGRS RA system

EXAMPLE One IGRS RA server address could be: “www.igrslab.com:8080”.

Note 1 to entry: Server address format in IGRS RA system is “domain name of server:port”.

3.2 Abbreviated terms

AS	autonomous system
HTTP	hypertext transfer protocol
ID	identification
IGRS	intelligent grouping and resource sharing
IRSP	IGRS RA service platform
LAN	local area network
RA	remote access
RUMP	remote universal management profile
TCP/IP	transmission control protocol/ internet protocol
UI	user interface
XMPP	extensible messaging and presence protocol
WAN	wide area network

4 Conformance

A system that conforms to this document shall be implemented according to Clauses 5 through 7, where the IGRS remote access capabilities including system architecture, message exchange mechanism and work flow shall conform to Clause 6, and the RUMP application protocol for specific device types shall conform to Clause 7.

5 IGRS RUMP overview

RUMP (remote universal management profile) protocol provides specific IGRS remote access application scenarios based on the remote management of all devices at home, office and other remote locations, which is applicable to not only devices with strong processing capability such as TV, PC, set-top box, etc., but also devices with weak processing capability such as refrigerator, microwave oven, washing machine, dishwasher, etc.

RUMP defines the configuration and interface of IP and non-IP devices, the overall system architecture of comprehensive remote control and management of a variety of home devices. It also defines the communication interface, message flow and message format for universal management of devices, as well as the type of connection and network structure between non-IP devices and IP devices.

RUMP offers an efficient solution for IP or non-IP devices to access IGRS network, as it resolves the requirements of defining common system structure, port, message format and message flow to enable remote access of different RUMP devices (with strong or weak processing capabilities).

The specific protocol contents are as follows.

a) Remote universal device discovery and management framework:
   - connection methods and network architecture;
   - device configuration interfaces;
   - management message formats;
   - message exchange flows.

b) Request/response message formats for four remote universal management profile device types:
   - water heater;
   - refrigerator;
   - air conditioner;
   - microwave.

6 IGRS RA and RUMP system architecture and message exchange model overview

6.1 IGRS RA system structure

A logical system diagram of IGRS RA is shown in Figure 1.

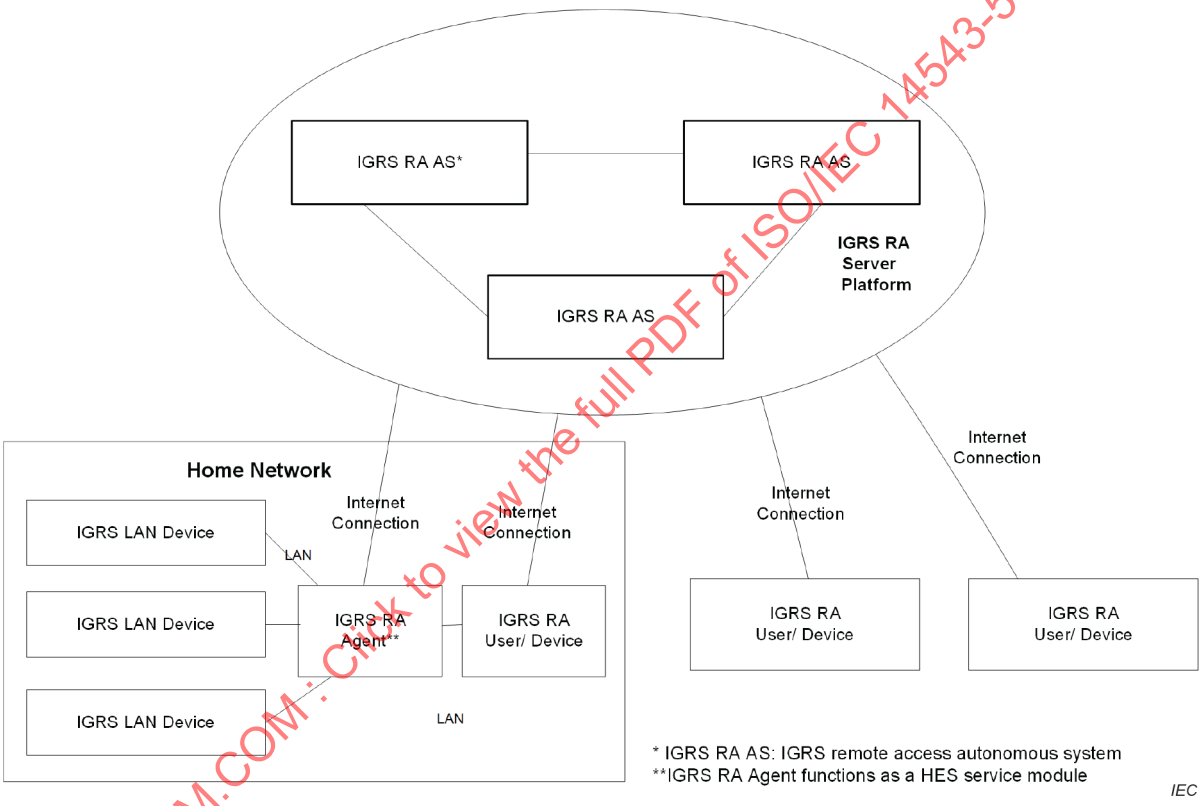

Figure 1 – IGRS RA system structure

As shown in Figure 1, IGRS RA system consists of IGRS RA user/device, IGRS RA server platform as defined in ISO/IEC 14543-5-7, ISO/IEC 14543-5-8 and ISO/IEC 14543-5-9, IGRS LAN device and IGRS RA agent (which is used for establishing a connection between IGRS RA user/device and IGRS LAN devices). All IGRS LAN devices and IGRS RA devices within a subnet shall use published IGRS protocols (ISO/IEC 14543-5-1) to interconnect with each other and establish a home IGRS subnet. That is, IGRS RA protocols are backward compatible to the published IGRS protocols.

When any IGRS RA device enters an IGRS home subnet, it operates as an IGRS LAN device. That IGRS RA device may not only connect to other IGRS LAN devices by the IGRS protocols, but also access IGRS RA service platform through a connection to the IGRS RA agent. In addition, if the IGRS RA user/device in the home LAN area is able to access the internet directly, it may build a connection to the IGRS RA service platform and access the IGRS RA services without any intermediary agent. For IGRS LAN device that cannot be discoverable

over the internet, an IGRS RA agent, which is also an HES gateway service module, shall be used instead.

IGRS RA agent may be an independent device or an IGRS RA device embedded with agent function. IGRS RA agent shall maintain active internet connections and may access IGRS RA service platform by those internet connections. Through the IGRS RA agent, IGRS LAN devices without IGRS RA functions may both access the IGRS RA service platform, and be accessed by other IGRS RA users/devices.

The IGRS RA user/device may still keep a persistent connection to the IGRS RA service platform if it maintains an internet access connection when it leaves home or office LAN environment.

6.2 RUMP protocol layer hierarchy

RUMP protocol layer hierarchy is shown in Figure 2.

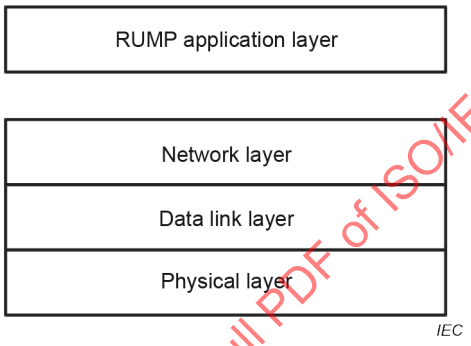

Figure 2 – RUMP protocol layer

RUMP application layer shall process specific RUMP command, and handle the application data transfer in the network, which includes point-to-point and point-to-multipoint data transfer. The physical layer, data link layer and network layer, as shown in Figure 2, may adopt any published standard communication protocols (WiFi®[1], Ethernet, etc.) to deliver the actual RUMP applications.

Figure 3 shows the message interaction flow process between two RUMP devices: a controller and controlled device.

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

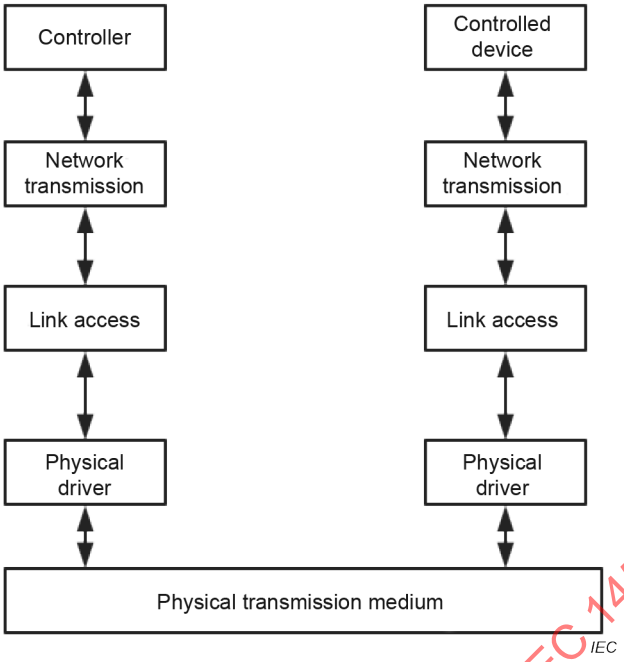

Figure 3 – RUMP message interaction flow

6.3 Server types

6.3.1 IGRS RA message exchange model in the IRSP

Different message exchange models in the IRSP are shown in Figure 4.

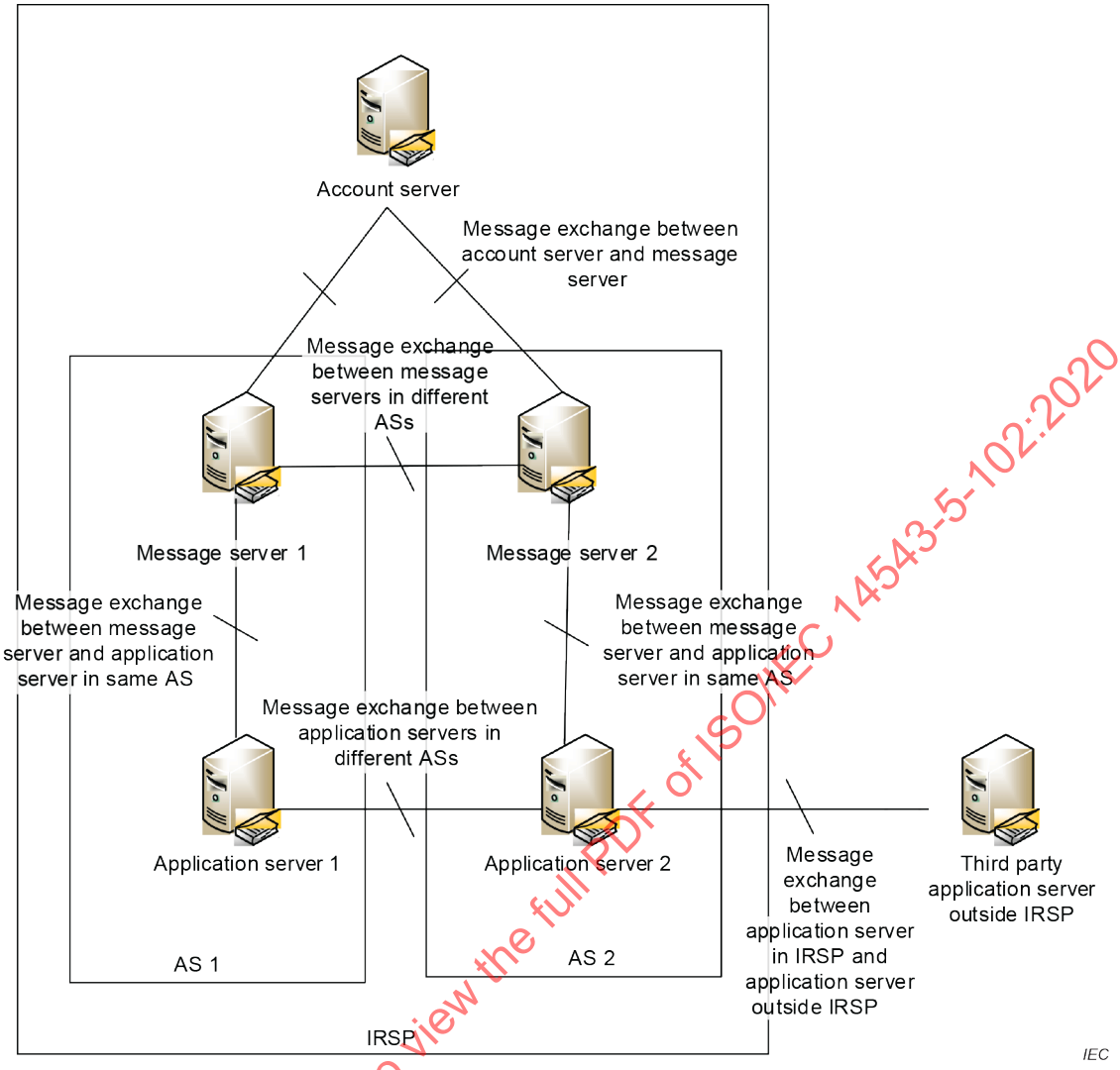

Figure 4 – Message exchange models in IGRS RA system

In IGRS RA system, different servers may exchange messages with each other directly.

6.3.2 Account server

The account server processes user and device account related contents on the IRSP. Generally, one IRSP has only one logical account server.

The functionalities of account server are:

a) managing all user and device accounts in all ASs;

b) verifying the global uniqueness of the local part of user or device ID when the user or device registers and when the user or device information is modified. This ensures that the IGRS RA user or device ID is unique in IGRS system;

c) processing the deletion of user or device account.

6.3.3 Message server

The message server processes message exchange logics (transmission, receiving, forwarding and blocking, etc.). Different from an account server, one IRSP may have multiple message servers. One AS may also have multiple message servers.

The functionalities of message server are:

a) verifying user and device login identification;

b) verifying the message exchange security between the user or device and user or device, and between the user or device and the IRSP;

c) managing relationships between the user or device and user or device;

d) handling message operations (transmission, receiving, storing, distribution, discarding, etc.).

In an IGRS RA system, there are several different types of message exchanges between the message server and account server, as well as between the message server and application server:

1) message exchange between the message server and account server;

2) message exchange between the message server and application server in the same AS;

3) message exchange between the message server and message server in different ASs;

4) message exchange between the message server and application server in different ASs.

6.3.4 Application server

The application server processes application services logics (content service, storage service, data analysis, etc.). Two types of application servers are considered in the IGRS RA system:

a) IRSP internal application servers shall follow application logics specified in the IGRS RA application profiles;

b) IRSP external application servers are owned and managed by third-party service providers.

These two types of application servers may exchange messages with each other and provide collaborative services to the user, device or AS.

6.3.5 IRSP external application server

This is a third-party owned and managed application server that exchanges messages with the IRSP and jointly provides collaborative services with IGRS servers.

6.4 Message exchange between user or controlled device and message server

6.4.1 Device registration management

The IGRS controlled device shall send a registration request message as in Message 1.

http(s)://*Domain Name of the Account Server*/register.xml?name=*device ID* & password=*Password*&domain=*Domain Name of the Message Service*&verifycode=*device verification code*&type=*device type*&vendor=*device vendor*&model=*device model*

Message 1: Device registration request message

where the “verifycode”, “type”, “vendor” and “model” are optional parameters. More information may be requested in addition to the above information.

NOTE 1 Italics indicate where content is to be inserted; all other text in message definitions is fixed in this document.

NOTE 2 All contents in the message definition are mandatory in this document.

NOTE 3 A device ID consists of a local part and a domain name part. A “@” is used to separate the two parts. Each device ID starts with a “#”. For example: #01aa0101# acff036e1230@igrs.com

EXAMPLE In an air conditioner use case:

Device ID: #01aa0101#acff036e1230 model number: 01 device type: air conditioner device manufacturer: aa

Device model number: 0101 verifycode: dc2b7c12fb

The request message may be shown below:

http(s)://domain name of account server /register.xml?name=#01aa0101#acff036e1230 &password=password&domain= domain name of message server &verifycode= dc2b7c12fb &type=air conditioner&vendor=aabb&model=0101

The functions and the relative information of the account server and the message service are specified in ISO/IEC 14543-5-9.

The service platform shall return a registration response message when it receives a registration request message from the device.

6.4.2 User/controller ↔ controlled device message exchange that needs response (control message)

In the IGRS RA system, the messages exchanged between users and devices shall all go through the IRSP. The IRSP shall identify the usability of the exchange request message from the source user or device and terminate the message exchange procedure when the following cases happen:

a) the source user or device does not have the message exchange rights with the target;

b) relationship between the source and target does not allow message exchange between them;

c) request message contains wrong contents.

Functional flow is shown in Figure 5.

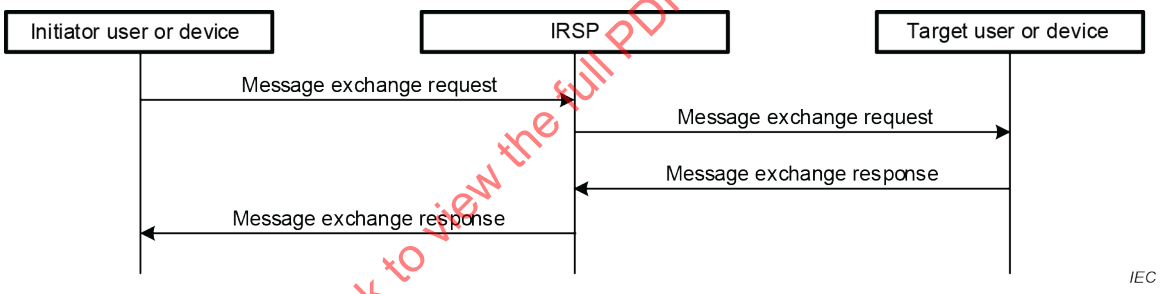

Figure 5 – Flow of message exchange between user/controller and controlled device that needs response

When a user/controller wants to exchange messages with another controlled device and needs the target controlled device to return a response message, the message exchange source shall send a message exchange request message to the IRSP as in Message 2.

```
<iq id='message SN' from='source user/controller ID' to='target controlled device ID' type='get'>
        <query xmlns='http://www.igrs.org/spec2.0/basic#control'>
                <data>request_data_base64</data>
        </query>
</iq>
```

Message 2: Exchange request message that needs response

EXAMPLE User name is 123@163.com, controlled device ID is #01aa0101#acff036e1230

Domain name of the message server is igrs.com

See message body format in 7.7, 7.8, 7.9, 7.10

Initiator user/controller identification: 123@163.com@ igrs.com

Target controlled device identification: #01aa0101#acff036e1230@igrs.com

request_data_base64: message body coded using base64

The IRSP shall receive the exchange request message and forward the received message to the target controlled device. The target controlled device processes according to the message contents and sends the response message to the IRSP. The response message shall be as shown in Message 3.

```
If successful:
<iq id='message SN' from='target controlled device ID' to='source user/controller ID' type='result'>
        <query xmlns='http://www.igrs.org/spec2.0/basic#control'>
                <data>response_data_base64</data>
        </query>
</iq>
If failed:
<iq id='message SN' from='target controlled device ID' to='source user/controller ID' type='error'>
        <error code='503' type='CANCEL'>
                <service-unavailable xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/>
        </error>
</iq>
```

Message 3: Exchange request response message for Message 2

EXAMPLE User name is 123@163.com, controlled device ID is #01aa0101#acff036e1230

Domain name of the message server is igrs.com

See message body format in 7.7, 7.8, 7.9, 7.10

Target controlled device identification: #01aa0101#acff036e1230@igrs.com

Initiator user/controller identification: 123@163.com@ igrs.com

response_data_base64: message body coded using base64

The IRSP shall forward the request response message to the source user/controller.

6.4.3 Controlled device ↔ user/controller message exchange that does not need response (status update)

Whenever the controlled device detects a status change, it shall send a status update message to IRSP. IRSP shall then forward the update message to the binding user/controller.

Functional flow is shown in Figure 6.

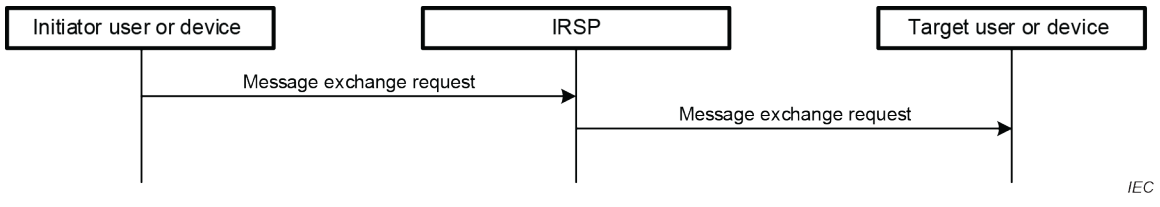

Figure 6 – Flow of message exchange between controlled device and user/controller that does not need response

This flow is used to exchange messages when one controlled device requests a message exchange with another user/controller but does not need the target user/controller to respond to the request. The source shall send Message 4 to the IRSP.

```
<message id='message SN' from='source controlled device ID' to='target user/controller ID'
type='normal'>
        <query xmlns='http://www.igrs.org/spec2.0/basic#status'>
                <data>data_base64</data>
        </query>
</message>
```

Message 4: Exchange request message that does not need response

EXAMPLE User name is 123@163.com, controlled device ID is #01aa0101#acff036e1230

Domain name of the message server is igrs.com

See message body format in 7.7, 7.8, 7.9, 7.10.

Initiator controlled device identification: #01aa0101#acff036e1230@igrs.com

Target user/controller identification: 123@163.com@ igrs.com

data_base64: message body coded using base64

IRSP shall receive the exchange request message and forward the message to the target user/controller. The target user/controller does not need to respond to the request.

6.4.4 Controlled device ↔ user/controller message exchange that does not need response (alarm message)

Whenever the controlled device detects an alarm warning, it shall send an alarm message to IRSP. IRSP shall then forward the update message to the binding user/controller.

The source shall send Message 5 to the IRSP.

```
<message id='message SN' from='source controlled device ID' to='target user/controller ID'
type='normal'>
        <query xmlns='http://www.igrs.org/spec2.0/basic#warning'>
                <data>data_base64</data>
        </query>
</message>
```

Message 5: Exchange request message that does not need response

EXAMPLE User name is 123@163.com, controlled device ID is #01aa0101#acff036e1230

Domain name of the message server is igrs.com

See message body format in 7.7, 7.8, 7.9, 7.10.

Initiator controlled device identification: #01aa0101#acff036e1230@igrs.com

Target user/controller identification: 123@163.com@ igrs.com

data_base64: message body coded using base64

6.4.5 Controlled device ↔ user/controller message exchange that that needs response (firmware version query)

When a user/controller wants to query the device firmware version with another controlled device, and needs the target controlled device to return a response message, the message exchange source shall send a message exchange request message to the IRSP as in Message 6.

```
<iq id='message SN' from='source user/controller ID' to='target controlled device ID' type='get'>
        <query xmlns='http://www.igrs.org/spec2.0/basic#version'>
                <data>request_data_base64</data>
        </query>
</iq>
```

Message 6: Exchange request message that needs response

EXAMPLE user name is 123@163.com, controlled device ID is #01aa0101#acff036e1230

Domain name of the message server is igrs.com

See message body format in 7.12

Initiator user/controller identification: 123@163.com@ igrs.com

Target controlled device identification: #01aa0101#acff036e1230@igrs.com

request_data_base64: message body coded using base64

The IRSP shall receive the exchange request message and forward the received message to the target controlled device. The target controlled device processes according to the message contents and sends the response message to the IRSP. The response message shall be as shown in Message 7.

```
If successful:
<iq id='message SN' from='target controlled device ID' to='source user/controller ID' type='result'>
        <query xmlns='http://www.igrs.org/spec2.0/basic#version'>
                <data>response_data_base64</data>
        </query>
</iq>
If failed:
<iq id='message SN' from='target controlled device ID' to='source user/controller ID' type='error'>
        <error code='503' type='CANCEL'>
                <service-unavailable xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/>
        </error>
</iq>
```

Message 7: Exchange request response message for Message 2

EXAMPLE User name is 123@163.com, controlled device ID is #01aa0101#acff036e1230

Domain name of the message server is igrs.com

See message body format in 7.12

Target controlled device identification: #01aa0101#acff036e1230@igrs.com

Initiator user/controller identification: 123@163.com@ igrs.com

response_data_base64: message body coded using base64

The IRSP shall forward the request response message to the source user/controller.

ISO/IEC 14543-5-8 gives additional detailed user/device interaction message flow requirements.

6.5 Workflow

6.5.1 LAN control

When controlled device and controller are connected to the same local network (i.e. same gateway/router), the controller is capable of discovering and interacting with the controlled device directly by establishing connection as defined in ISO/IEC 14543-5-1. The LAN control flow diagram is shown in Figure 7.

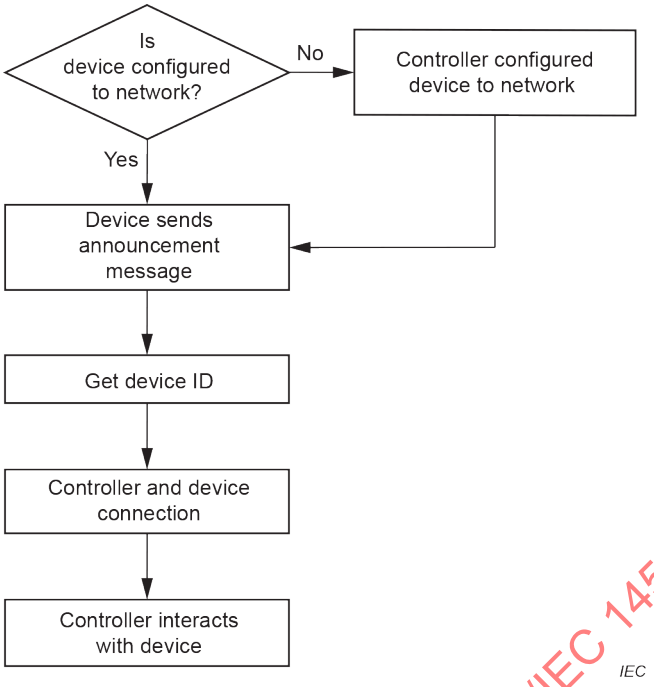

Figure 7 – LAN control flow diagram

a) When the controller first connects to the network, it uses the network setup tools to conduct the controlled device configuration in order to add the device to the same network.

b) To declare its presence, the controlled device sends announcement messages after it successfully connects to the current network. The controller shall then discover the device and acquire the device ID.

c) The controller requests connection with the controlled device.

d) The controller monitors the announcement message of the controlled device and acquires all the necessary controlled device information.

e) The controller may now interact with the controlled device.

6.5.2 WAN control

For the controller to interact with the controlled device remotely, it shall first establish a binding relationship with the controlled device in the IRSP as defined in ISO/IEC 14543-5-8. The controller–IRSP–device WAN interaction flow process is shown in Figure 8.

a) Controlled device shall first register with the IRSP.

b) User/controller logs in the IRSP.

c) User/controller successfully binds to the target controlled device by sending relationship establish request to the IRSP.

d) User/controller acquires the roster and controlled device ID.

e) The controller may now interact with the controlled device.

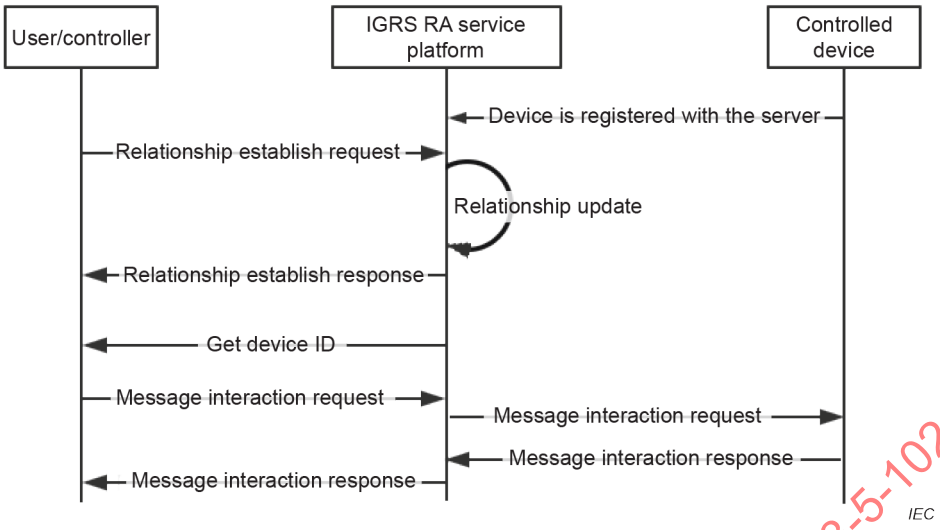

Figure 8 – Controller–IRSP–device WAN interaction process

7 RUMP

7.1 Protocol overview

RUMP shall specify the communication protocol format used for interaction among the controlled device, user/controller and IRSP. Only one data packet is sent for either the request or response message at any time. The specific request and response message format shall be in accordance with 7.5.

NOTE 1 For interoperability with other products, the specific RUMP message formats can be translated into HES-CLIP [HES Common Language Internal Protocol].

NOTE 2 Unless stated otherwise in this document, the hexadecimal data format always follows the order of most significant bits (msb) first.

7.2 Applications

The current set of RUMP protocols shall be applicable to the following device types: water heaters, air conditioners, refrigerators, microwave ovens, to be used at home, office or other remote locations. This protocol set may be extended to support additional RUMP device types.

7.3 Logical components

A RUMP network consists of at least one controller and one or many controlled devices.

a) Controller: a device that interacts with the controlled devices, such as an integrated controller, remote control terminal, mobile device (smart phone/smart pad) applications, etc.

b) Controlled device: a physical device, such as air conditioner, water heater, refrigerator, microwave oven, etc.

7.4 Device ID

In a RUMP network, device ID is the only corresponding identifier (globally unique) used by a controlled device. It shall consist of device type, manufacturer ID, device model number and unique device identifier.

a) Device type: two (2) characters long, which is used to identify the specific device types. The values are: 01 – water heater; 02 – air conditioner; 03 – refrigerator; 04 – microwave ovens.

b) Manufacturer ID: two (2) characters long, which is used to distinguish different manufacturers. The value ranges are: 01 to zz.

c) Device model number: four (4) characters long, which is used to distinguish different device models determined by the manufacturers. The value ranges are: 0001 to zzzz.

d) Unique device identifier: six (6) octets or twelve (12) characters long, which is used to identify the unique device. A typical value may be the device's MAC address.

Device ID shall begin with "#", and is separated with "#" after the device model number but before the unique device identifier. A summary of the device ID format is as follows:

#	Device type	Manufacturer ID	Device model number	#	Unique device identifier

Device ID definitions are given in Table 1.

Table 1 – Device ID definitions

Device ID composition	Note
Device type	2 characters, describes different device types
Manufacturer ID	2 characters, describes different manufacturers
Device model number	4 characters, describes different device models from different manufacturers
Unique device identifier	12 characters, defines unique device identifiers

EXAMPLE The device ID of a refrigerator is #01aa0101#acff036e1230

Device type: 01 (water heater)

Manufacturer ID: aa

Device model number: 0101

Unique device identifier: 0xacff036e1230

7.5 RUMP message format

A summary of RUMP message format is shown in Table 2.

Table 2 – RUMP message format

Message format	Note
Header	Header bits
Message identifier	Identify message types
Message body	Detailed message content
Checksum	Checksum bits: ~(sum of all bits)

Each field in a RUMP message is defined as follows.

a) Header: pre-defined header bits.

b) Message identifier: Identify specific message types. A detailed definition is shown in Table 3.

Table 3 – RUMP message identifier

Message body	Note
Control message	0x01
Response message	0x02
Query message	0x03
Status message	0x04
Version message	0x05
Alarm message	0x06

c) Message body: detailed data relevant to the specific device type (see 7.7, 7.8, 7.9, 7.10 for more details). If the message type is control message, then the message body shall be further divided as shown in Table 4.

Table 4 – Control message body

Message body	Note
Control type	Specific control functions
Data	Device control data

d) Checksum: Checksum bits: ~(sum of all bits) to verify message integrity.

7.6 RUMP response and status message format

The response and status message shall always return the current full status of the device. The response and status message format shall follow the same format as shown in Table 2. Its message body contains detailed data relevant to the specific device type (see 7.7, 7.8, 7.9, 7.10 for more details).

7.7 RUMP water heater

7.7.1 Water heater control message format

The water heater control message format is shown in Table 5.

Table 5 – Water heater control message format

Header	Message identifier	Control type	Data (integer type)	Checksum
0xDD	0x01	0x01 Switch	0: off 1: on	Checksum bits: ~(sum of all bits)
		0x02 Power level	0: 1 000 W 1: 2 000 W 2: 3 000 W	
		0x03 Temperature	30 to 80	
		0x04 Function type	0: medium heat 1: instant heating	
		0x05 Mode	0: night mode 1: heat preservation mode	
		0x06 Timer – hour	0 to 23	
		0x07 Timer – minute	0 to 59	
		0x08 to 0xFF: Reserved	This portion of control messages shall be ignored if used	

EXAMPLE Device type is 01, Manufacturer ID is aa, device model number is 0101, unique device identifier is accf03445566

Device ID is #01aa0101#accf03445566

Message identifier: control command

Type of control: switch 0x01

On: 1

The completer “on” command: <dd 01 01 01 1f>

7.7.2 Water heater response and status message format

The controlled device shall return a 0x02 response message to a controller-initiated control command (0x01). Similarly, the device shall return a 0x04 status message identifier to a controller-initiated query command (0x03).

The detailed water heater response and status message format is shown in Table 6.

Table 6 – Water heater response and status message format

Byte	Bit	Data	Note
1		0xDD	Header
2	b7-b0	0x02: response message 0x04: status message	Message identifier
3	b7-b0	0x00: off 0x01: on	
4	b2-b0	000b: medium heat 001b: instant heating 010b: night mode 011b: heat preservation mode	
	b7-b3	Reserved	
5	b7-b0	0x00: 1 000 W 0x01: 2 000 W 0x02: 3 000 W	Power level
6	b7-b0		Set temperature
7	b7-b0		Current temperature
8	b7-b0		Timer – hour
9	b7-b0		Timer – minute
10-19		Reserved	Default data set to all “0”, and all reserved bits in the received data stream shall NOT be interpreted
20	b7-b0		Checksum bits: ~(sum of all bits)

EXAMPLE A controller may receive the following message:

Bytes: <dd020102 02322812 1e000000 00000000 0000006e>

bytes[1]: header

bytes[2]: 0x02 denotes response message

bytes[3]: 0x01 denotes on

bytes[4]: 0x02 denotes night mode

bytes[5]: 0x02 denotes 3000 W

bytes[6]: 0x32 denotes to set the temperature at 50 °C

bytes[7]: 0x28 denotes the current temperature at 40 °C

bytes[8]: 0x12 denotes the reservation timer hour of 18:00 hours

bytes[9]: 0x1e denotes the reservation timer minute of 30 minutes.

7.7.3 Water heater alarm message format

The water heater alarm message is shown in Table 7.

Table 7 – Water heater alarm message format

Byte	Bit	Data	Note
1		0xDD	Header
2	b7-b0	0x06	Alarm message identifier
3	b0	0: normal 1: malfunction	Heat alarm
	b1	0: normal 1: malfunction	Sensor fault
	b7-b2	Reserved	Default data set to all "0", and all reserved bits in the received data stream shall NOT be interpreted
4-9		Reserved	Default data set to all "0", and all reserved bits in the received data stream shall NOT be interpreted
10			Checksum bits: ~(sum of all bits)

EXAMPLE A controller may receive the following alarm message:

Bytes: <dd060300 00000000 00e6>

bytes[1]: header

bytes[2]: 0x06 denotes alarm message

bytes[3]: 0x03 denotes heat and sensor fault alarm

7.8 RUMP air conditioner

7.8.1 Air conditioner control message format

The air conditioner control message format is shown in Table 8.

Table 8 – Air conditioner control message format

Header	Message identifier	Control type	Data (integer type)	Checksum
0xEE	0x01	0x01 Switch	0: off 1: on	Checksum bits: ~(sum of all bits)
		0x02 Function	0: auto 1: cool 2: heat 3: de-humidifier 4: air supply	
		0x03 Temperature setting	16 to 35	
		0x04 Fan speed	0 to 4	
		0x05 Direction	0: fix 1: up/down 2: left/right	
		0x06 Timer hour (off)	0 to 23	
		0x07 Timer minute (off)	0 to 59	
		0x08 Timer hour (on)	0 to 23	
		0x09 Timer minute (on)	0 to 59	

Header	Message identifier	Control type	Data (integer type)	Checksum
		0x10 Mode	0: quiet 1: sleep 2: dry heat	
		0x08 to 0xFF: Reserved	This portion of control messages shall be ignored if used	

7.8.2 Air conditioner response and status message format

The controlled device shall return a 0x02 response message to a controller-initiated control command (0x01). Similarly, the device shall return a 0x04 status message identifier to a controller-initiated query command (0x03).

The air conditioner response and status message format is shown in Table 9.

Table 9 – Air conditioner response and status message format

Byte	Bit	Data	Note
1		0xEE	Header
2	b7-b0	0x02: response message 0x04: status message	Message identifier
3	b7-b0	0x00: off 0x01: on	Switch
4	b7-b0	16 to 35	Temperature setting
5	b7-b0		Current temperature
6	b7-b0	0x00: auto 0x01: cool 0x02: heat 0x03: de-humidifier 0x04: air supply	Function
7	b3-b0	0 to 4	Fan speed
	b7-b4	0 to 2	Direction
8	b7-b0		Timer hour (off)
9	b7-b0		Timer minute (off)
10	b7-b0		Timer hour (on)
11	b7-b0		Timer minute (on)
12	b7-b0	0: Quiet 1: Sleep 2: Dry heating	Mode
13-19		Reserved	Default data set to all “0”, and all reserved bits in the received data stream shall NOT be interpreted
20			Checksum bits: ~(sum of all bits)

7.8.3 Air conditioner alarm message format

The air conditioner alarm message format is shown in Table 10.

Table 10 – Air conditioner alarm message format

Byte	Bit	Data	Note
1		0xEE	Header
2	b7-b0	0x06	Alarm message identifier
3	b0	0: normal 1: malfunction	External fan capacitance
	b1	0: normal 1: malfunction	Room temperature sensor
	b2	0: normal 1: malfunction	Indoor tube temperature sensor
	b3	0: normal 1: malfunction	Outdoor defrosting temperature sensor
	b7-b4	Reserved	Default data set to all “0”, and all reserved bits in the received data stream shall NOT be interpreted
4-9		Reserved	Default data set to all “0”, and all reserved bits in the received data stream shall NOT be interpreted
10			Checksum bits: ~(sum of all bits)

7.9 RUMP refrigerator

7.9.1 Refrigerator control message format

The refrigerator control message format is shown in Table 11.

Table 11 – Refrigerator control message format

Header	Message identifier	Control type	Data (integer type)	Checksum
0xBB	0x01	0x01 Function	0: quick cooling 1: quick freezing	Checksum bits: ~(sum of all bits)
		0x02 Refrigerator temperature	95 to 105 (−5 to 5)	
		0x03 Freezer temperature	80 to 93(−20 to −7)	
		0x04 Variable temperature	100 to 110 (0 to 10)	
		0x05 Mode	0: holiday mode 1: power-saving mode: a setting that allows the refrigerator to operate at a significantly lower power requirement 2: smart mode: a setting that allows the refrigerator to adjust internal temperature according to external environmental temperature, seasonal changes or regional settings	
		0x08 to 0xFF: Reserved	This portion of control messages shall be ignored if used	