Remote Access DFGT – 2
Product / Protocol Specification

Document Information

Info	Content
Author(s)	Ronald Daris
Revision	7
Document Status	WIP
Date	December 12, 2014
Distribution	For Customer use
VPM Number	DP14010
Keywords	firecrest; winchat; sfeerhaard; gateway

This document is based on the Product / Protocol Specification template, version 2.0 of the ACS Software Development Process.

Revision History

Rev.	Date	Author	Description
1	October 22, 2012	Ronald Daris	Initial draft
2	December 18, 2012	Ronald Daris	• Removed function 06 Read Exception status • Assigned Modbus Register numbers • Added mac address as 3 registers
3	March 1, 2013	Ronald Daris	• Appendixes added • Added information to Registers 40011, 40102, 40300-40304 • Removed register 40405, this is now part of register 40304 • Added Future functions
4	November 26, 2013	Ronald Daris	• HW type removed from Registers 40201-40210 • Register 41009 added (apply IP settings) • Added wave settings, registers • Added OEM settings, registers • Added status bits • Added command for wave, light and boost fan • Added IP discovery • Added service interface registers like settings
5	June 6, 2014	Ronald Daris	• Added explanation of RSSI registers 40205/40206 • Chapter future functions updated
6	July 28, 2014	Ronald Daris	• Added temperature control • Added service/factory write function • Added Status bits • Added generic registers
7	December 12, 2014	Ronald Daris	• Registers 40200 and 40201: write only • Register 40300: read only • Removed Registers 40315, 40316, 40431, 40432, 40510 and 40511 • Register 40500-40509: read only • Registers 40600 - 40820: read only added • Added registers 41001, 41002, 41003, 41100-41139, 41200-41219 and 41300-41329

Table of Contents

1 Introduction

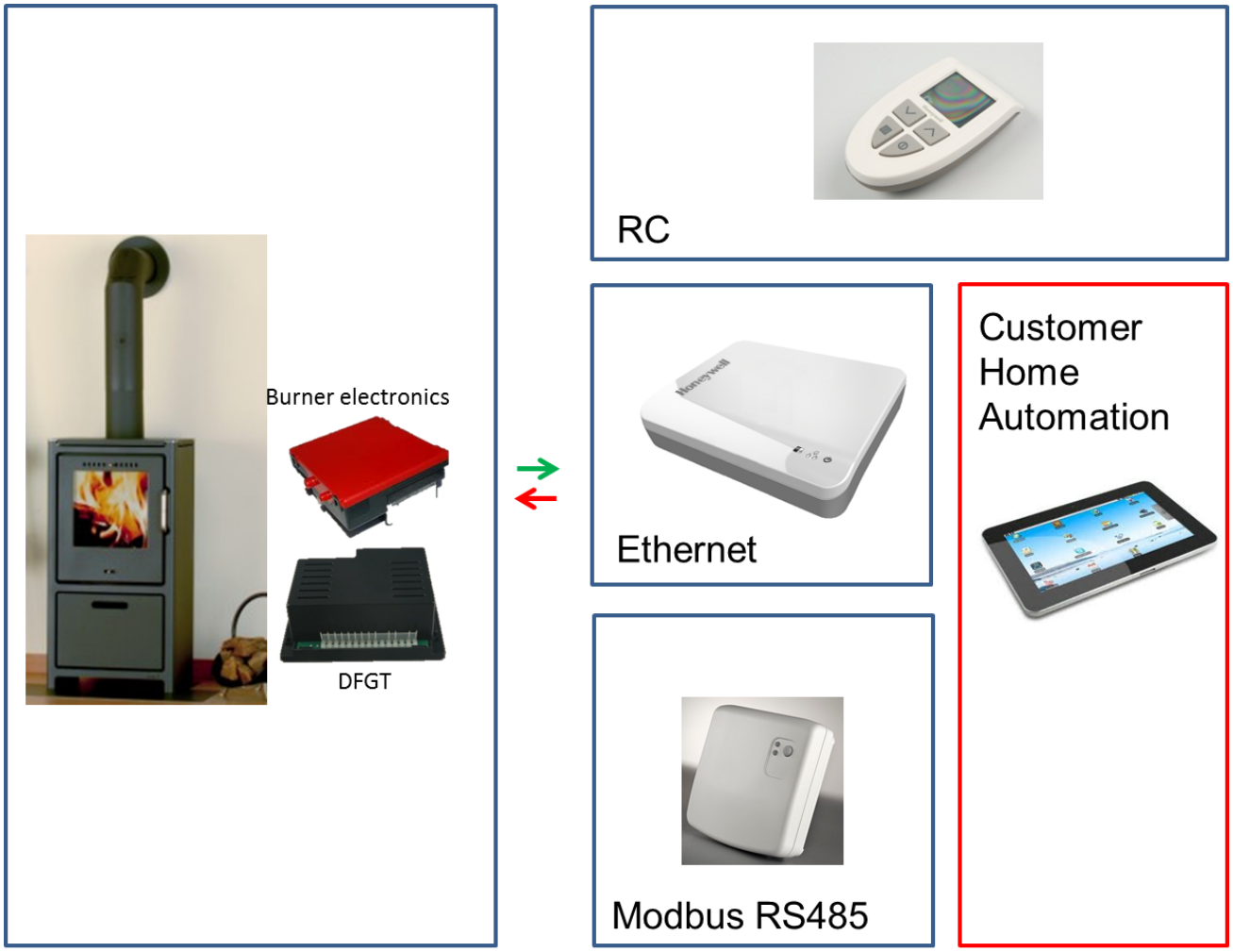
1.1 Purpose

This System Specification describes the capabilities and characteristics of the product identified including design constraints, and other factors as necessary.

1.2 Scope

This system Specification applies to decorative fire systems with Honeywell controls. The system consists of

- A fireplace with a burner controller and RF receiver (DFGT)
- A remote user interface
- And optional an RF interface to enable customer home automation



The Ethernet and Modbus devices open the communication for 3rd party applications (red square) to control the fireplace.

Either an Ethernet or Modbus device can be connected together with a remote control to the fireplace.

1.3 Terms, Acronyms and Abbreviations

Below are the terms, acronyms, and abbreviations used within this document.

Term, Acronym, Abbreviation	Definition

Term, Acronym, Abbreviation	Definition
APP	Android/iOs/Windows application to control the fireplace
DFGT	Decorative Fireplace controller for Gas applications
DFRC	Decorative Fireplace Remote control
RC	Remote Control
RF	Wireless protocol
Pilot Flame	The small flame in the fireplace to ignite the main burner
DBI	Direct Burner Ignition (ignition without pilot flame)

1.4 References

Abbreviation	Reference Element	Description
Modbus	Modbus_Messaging_Implementation_Guide_V1_0b.pdf	Modbus TCP/IP implementation
	Modbus_Application_Protocol_V1_1b.pdf	Modbus Application Protocol
	Modbus_over_serial_line_V1_02-1.pdf	Modbus RS485 implementation

2 Product info

2.1 Modbus over TCP/IP (Ethernet)

2.1.1 User Interface

The device has a (hidden) button and 5 LED's. 2 LED's are located at the RJ45 connector and 3 LED's are on the top of the product.

Front LED indications:

- Power/Error indication
- RF communication
- Modbus connection active

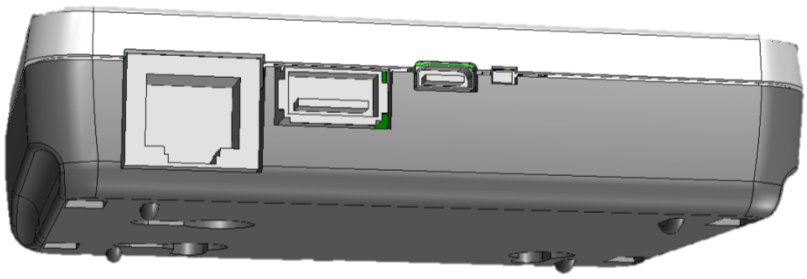
RJ45 Led indications:

- Ethernet connection
- IP address assigned

A short press on the button will initiate a binding with a fireplace.

A long press (10 seconds) on the button will clear all settings

2.1.2 Connections



Connections:

- RJ45 (female) connector Ethernet (10/100Mbit)
- Micro USB B connector to power the device
- USB A connector (no function at this moment)

2.1.3 Communications

The Ethernet device is working according a Modbus TCP/IP Server device (acting as a slave).

The Modbus server listens on TCP port 502 (fixed). Multiple concurrent connections are **not** supported.

To allow multiple devices to connect to the device the client (APP) should close the connection ASAP. The device will close the connection automatically when there is no communication for at least 3 minutes.

2.2 Modbus RS485

Future product, ask your supplier for availability.

2.2.1 User Interface

The device has a button and 2 LED's.

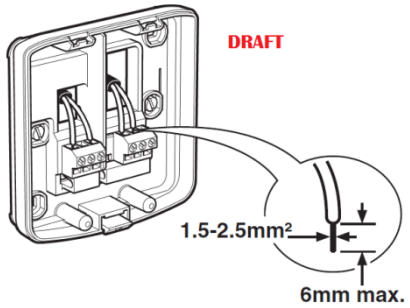
The exact function of the LED's is not determined at this moment.

Some possible LED indications:

- Power/Error indication
- RF communication
- RS485 Communication

The button will be used to reset all setting back to factory defaults and to initiate/accept binding with an RF device.

2.2.2 Connections



Terminal	Function
1	RS485 A
2	GND (shielding)
3	RS485 B
4	Power supply (9V DC / 24V AC)

Terminal	Function
5	GND

2.2.3 Communications

The Modbus RS485 device is working as a slave. The initial slave address is 207.

The default communication rate is 19200 8-E-1 (8 data bits, EVEN parity and 1 stop bit).

It’s possible to change the baud rate via a special Modbus function (see next chapter).

3 Modbus Protocol

The device will support Modbus functions:

- 03 Read Holding Registers
- 06 Write Single Registers
- 16 Write Multiple Registers
- 11 Get com event counter
- 43 Read device Identification (sub code 14) (content TBD according Honeywell standard)

Functions 01, 02, 04, 05, 06, 15, 17, 20, 21, 22, and 24 are not supported. Usage of these functions will result in an Exception code 01 (ILLEGAL FUNCTION)

Holding registers can be read only. Writing to a read only holding registers will be ignored (no exception raised)

Note: Input reading registers are not used.

Reading or writing to a Holding register that doesn't exist result in exception code 02 (ILLEGAL DATA ADDRESS).

Note: This is also the case when multiple registers are accessed in a function and one or more registers don't exist and some registers might exist.

When a register is read that doesn't have actual data yet, for instance after power-up. The exception code 05 (ACKNOWLEDGE) will be returned. The master should retry after some while.

Standard real numbers are communicated as IEEE-754 32 bits floating point.

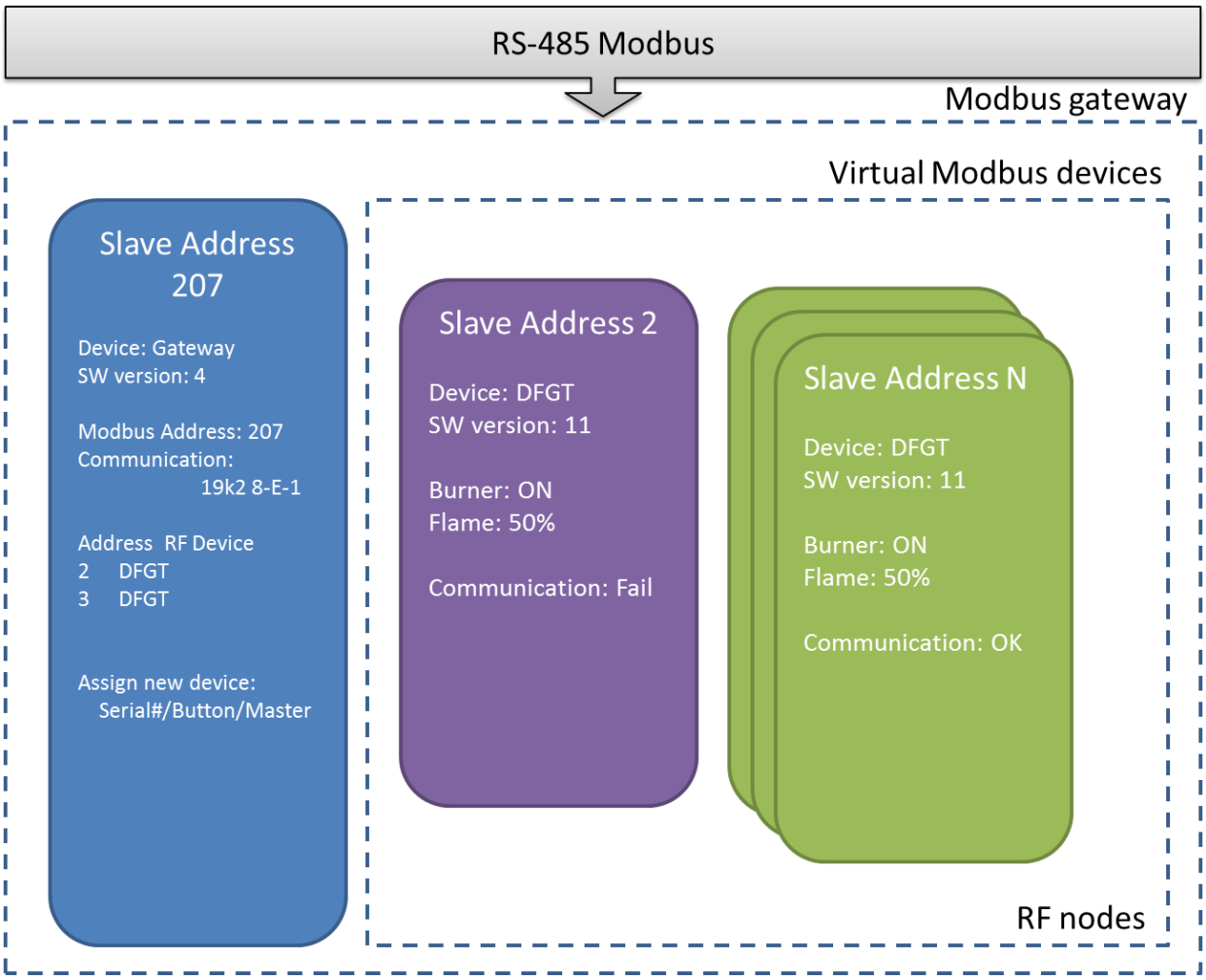
32 bits values are composed by 2 consecutive 16 bits holding registers.

A Modbus master can read/write a single word of a 32 bits register in two separate packets. The 32 bits value is cached in the gateway to maintain data integrity. The lowest register has to be read/write before highest register.

The byte/word sequence of a 32 bits registers is according TBD…

When there is a communication error with an RF device all functions on the (virtual slave) will return the exception 0B (GATEWAY TARGET DEVICE FAILED TO RESPOND)

3.1 Addressing



Typical address overview

The gateway will respond on multiple slave addresses (RS485) or Unit Identifiers (TCP/IP).

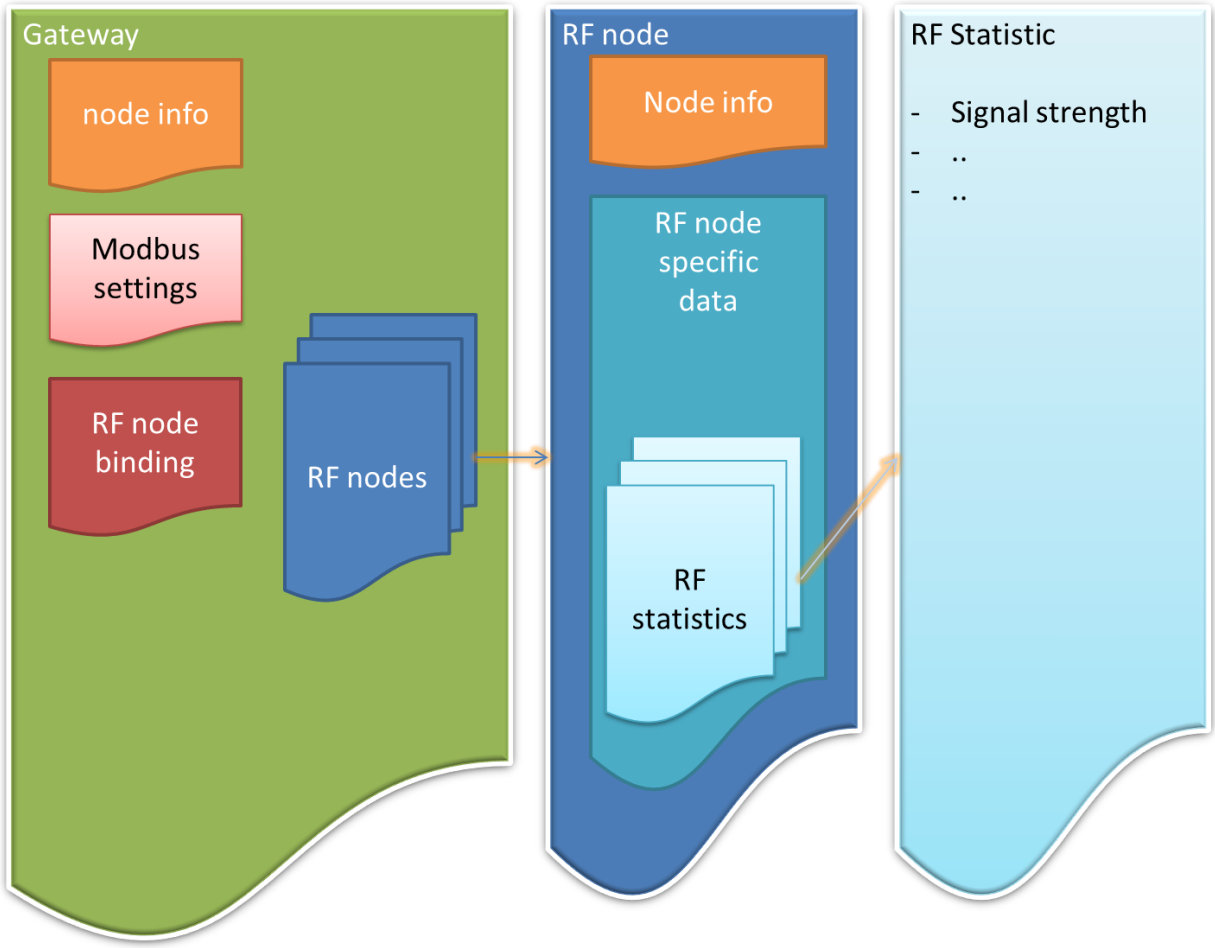
- The address to communicate to the gateway itself
- Each RF device that is bound to the gateway has its own address

The initial slave address (RS485) of the gateway itself is 207 and can be altered by the master.

The Unit Identifier (Ethernet) of the gateway itself is 1 and cannot be altered.

When a DFGT is bound to the device via the push button the gateway will automatically assign an (new) address to the node, starting from 2. When binding is initiated via Modbus the Modbus Master is in control of the address assignment.

Note: When a installer replaces the DFGT without removing the old device or without performing a factory reset the new DFGT gets a new address assigned and the old DFGT will have a communication failure. The APP must use the **new** assigned address for correct operation.



3.2 Holding Registers Gateway

Reg No.	Read Write	Function / Name
40000	R-	Gateway info HW type (2)
40001	R-	Gateway info SW version
40002-40003	R-	32 bits RF Serial number
40004-40006	R-	MAC address of the device (48 bits)
40010	RW	RF protocol: 0 Standard Honeywell RF protocol 1 Legacy decorative fireplace protocol note: is used to communicate with current DFGT modules

<table>
<tr><th>Reg No.</th><th>Read Write</th><th>Function / Name</th></tr>
<tr><td>40011</td><td>RW</td><td>Baud rate of the RS485 communication (default 6 - 19200 only RS485)
<table>
<tr><th>Value</th><th>Baud rate</th><th>Value</th><th>Baud rate</th></tr>
<tr><td>0</td><td>300</td><td>5</td><td>9600</td></tr>
<tr><td>1</td><td>600</td><td>6</td><td>19200 (default)</td></tr>
<tr><td>2</td><td>1200</td><td>7</td><td>38400</td></tr>
<tr><td>3</td><td>2400</td><td>8</td><td>57600</td></tr>
<tr><td>4</td><td>4800</td><td>9</td><td>115200</td></tr>
</table></td></tr>
<tr><td>40012</td><td>RW</td><td>Slave address of this device (default 207 only RS485)</td></tr>
<tr><td>40100</td><td>RW</td><td>Push button binding
0 Disabled (not possible to initiate binding via button
1 Enabled (default)</td></tr>
<tr><td>40101</td><td>-W</td><td>Initiate binding with DFGT.
The value written will become the slave address / Unit Identifier of the RF node when the binding is completed successfully.
Note: If another RF node is already assigned to this address the old node is removed before the binding procedure is started.</td></tr>
<tr><td>40102</td><td>R-</td><td>Actual Binding status
0 N/A (default)
1 Binding procedure initiated (waiting on response of RF node)
2 Binding completed successfully
100 Binding failed, no answer
101 Binding failed, incompatible device
102 Binding failed, node list is full
103 Binding failed ModBus address or UID is invalid (Range 2 to 255)</td></tr>
<tr><td>40110</td><td>-W</td><td>Remove bounded RF node
The value written is de slave address / Unit Identifier of the RF node that will be removed from the bound RF node list.</td></tr>
<tr><td>40200</td><td></td><td>Number of bound RF nodes</td></tr>
<tr><td></td><td>R-</td><td>List of RF nodes and their used slave addresses / Unit Identifier</td></tr>
<tr><td>40201</td><td></td><td>LSB Assigned slave address / UID</td></tr>
<tr><td>40202..</td><td></td><td>LSB Assigned slave address / UID</td></tr>
<tr><td>40210</td><td></td><td>LSB Assigned slave address / UID</td></tr>
<tr><td>41000</td><td>RW</td><td>IP address assignment
0 AUTO, try to use DHCP otherwise use fixed IP address
1 DHCP assigned IP and DNS address
2 Fixed IP and DNS address</td></tr>
</table>

Reg No.	Read Write	Function / Name
41001-41002	RW	32 bits IP address of this device Default 192.168.0.207 when DHCP is not used
41003-41004	RW	32 bits IP mask of TCP/IP settings Default 255.255.255.0 when DHCP is not used
41005-41006	RW	32 bits IP address of the default gateway (router) Default 0.0.0.0 when DHCP is not used
41007-41008	RW	32 bits IP address of the DNS server Default 0.0.0.0 when DHCP is not used
41009	-W	Writing the value 54321 will store and activate new IP settings
41100	RW	Magic number Factory Tool Ask Honeywell for number so device can be used during production setup.
42000-42999	RW	1000 values can be used by APP to store product specific information. The device itself doesn't use this data. For instance a time schedule can be stored. note: values should not be written more than 100k times

3.3 Holding Registers DFGT

Reg. No.	Read Write	Function / Name
40000	R-	RF Node info HW type (1)
40001	R-	RF Node info SW version
40002-40003	R	32 bits RF Node Serial number
40100	R-	RF node info Last seen Number of seconds ago the last message was received from this device. Note: When the burner is OFF there is no communication
40101	R-	RF Communication status 0 No Error 1 Error Note: A communication error only occurs when the burner is ON or an action needs to be carried out and no response is received.

Reg. No.	Read Write	Function / Name
40200	-W	Fireplace action 0 no action 1 Turn fireplace OFF (appliance specific) 2 Turn pilot OFF 3 Turn main burner OFF (appliance specific) 4 Turn Second burner OFF 5 Turn Light OFF 6 Turn Boost Fan OFF 7 Turn wave OFF 8 Turn Temperature Control OFF 100 Turn Pilot ON 101 Turn Main Burner ON 102 Turn Second Burner ON 103 Turn Light ON 104 Turn Boost Fan ON 105 Turn wave ON 106 Turn Temperature Control ON 1000 Reset fireplace
40201	-W	The requested flame height. (0-100%) Note 1: The main burner must be switched ON with the previous command before this value is used. For correct ignition this value is ignored for xx seconds after ignition. Note 2: This value is ignored when temperature control is active. Note 3: **Due to legislation on the used RF frequency it's not allowed to write this value more than once every 10 seconds. This limitation can be overruled for a few seconds when there is user interaction at that moment.**
40202	RW	Communication time-out in minutes (default 60 min) The fireplace is turned OFF when there is no communication with the Modbus Master (RS485) or TCP/IP Client for at least this time.

Reg. No.	Read Write	Function / Name
40203	R-	Fireplace Status (bit flags) xxxxxxxxxxxxxxx1 Fault xxxxxxxxxxxxxx1x Pilot flam ON xxxxxxxxxxxxx1xx Main Burner ON xxxxxxxxxxxx1xxx Second Burner ON xxxxxxxxxxx1xxxx Low battery DFRC xxxxxxxxxx1xxxxx 230V phase fault xxxxxxxxx1xxxxxx Reset fireplace can be initiated by customer xxxxxxxx1xxxxxxx Boost Fan ON xxxxxxx1xxxxxxxx Light ON xxxxxx1xxxxxxxxx Wave active xxxxx1xxxxxxxxxx Flame height **cannot** be changed by user at this moment xxxx1xxxxxxxxxxx A Remote Control is bound to the appliance xxx1xxxxxxxxxxxx A Gateway is bound to the appliance (always 1) xYYxxxxxxxxxxxxx YY Temp Control state: 00 = Temp Control not possible 01 = Temp Control Possible (not Active) 10 = Temp Control Active 11 = Temp control error (like RF fault DFRC) 1xxxxxxxxxxxxxxx 1 = Ignition is **not** allowed at this moment
40204	R-	When an fault is active this number gives more detail on the exact failure
40205	R-	RSSI level of the messages received by the gateway This value should be multiplied by -0.5 before shown to the user. A value of -90 after multiplication is a very bad signal a value between -30 to -55 is excellent.
40206	R-	RSSI level of the messages received by the DFGT This value should be multiplied by -0.5 before shown to the user
40207	R-	**Rounded** (0.5°C) actual Room Temperature [°C] Value must be divided by 10 to get a correct value. Example: Value 205 equals 20.5°C
40250	RW	Temperature Control Setpoint [°C] (steps of 0.5°C) Read value must be divided by 10 to get a correct value. Write value must be multiplied by 10. Example: Value 190 equals 19°C

<table>
<tr><th>Reg. No.</th><th>Read Write</th><th>Function / Name</th></tr>
<tr><td>40300-40304</td><td>R-</td><td>10 OEM bytes
Bytes are programmed during production inside the DFGT and can be used to identify or release specific functions for the customer
It’s advisable to transfer info like:
Open / Closed fireplace
DBI or Pilot ignition
Second burner present
Model/Brand number to check if APP is allowed to be used or to know what logo to show
But also other things like production year/week can be programmed.<table><tr><th>Register</th><th>MSB</th><th>LSB</th></tr><tr><td>40300</td><td>OEM byte 1</td><td>OEM byte 0</td></tr><tr><td>40301</td><td>OEM byte 3</td><td>OEM byte 2</td></tr><tr><td>40302</td><td>OEM byte 5</td><td>OEM byte 4</td></tr><tr><td>40303</td><td>OEM byte 7</td><td>OEM byte 6</td></tr><tr><td>40304</td><td>OEM byte 9</td><td>OEM byte 8</td></tr></table>OEM byte 9: A Honeywell assigned number that can be programmed during production inside the DFGT by the fireplace manufacturer.
This number can be used by the APP to check if the appliance is not from the competitor. Ask your Honeywell sales representative for an unique number or number range.</td></tr>
<tr><td>40305-40314</td><td>RW</td><td>20 OEM bytes (10 registers).
Can be used by the App to store device specific information. For instance to store location information like text “Living room”</td></tr>
<tr><td>40400-40419</td><td>RW</td><td>Factory settings DFGT. Only Individual write is possible but is only intended for service people. Do not make this data writeable for end users. Some data might be protected by the DFGT and individual write is not possible.</td></tr>
<tr><td>40420</td><td>RW</td><td>Wave interval time [s]
Total period of wave pattern is 20 times this interval time.
Note: from valve position 1 to 15 can takes up to 5 seconds. So a small interval time and a large difference might not be visible for the end user.</td></tr>
<tr><td>40421-40430</td><td>RW</td><td>Wave pattern, values that can be used 1 – 15
20 values together make the pattern of the wave.(layout as OEM bytes)
Note: This settings are only stored once a day in none volatile memory, therefor the setting might be lost after a (rare) power interruption</td></tr>
<tr><td>40500-40509</td><td>R</td><td>Factory settings DFRC</td></tr>
<tr><td>40600</td><td>R</td><td>Size of Fault history buffer</td></tr>
</table>

Reg. No.	Read Write	Function / Name
40601-40620	R	Fault history array. Register 40601 contains the most recent occurred error Each entry contains one fault. See service manual of product for the possible fault numbers
40700	R	Size of Fault counters array
40701-40720	R	Fault counters array. Register 40701 counts the number of time fault 0 has occurred Register 40702 counts the number of time fault 1 has occurred etc. See service manual of product for the possible fault numbers
40800	R	Size of Operation counters and actual data number array
40801-40820	R	Operation counters and actual data array See service manual of product for the meaning of the counters and actual data
41001	R	Write Result Factory Settings DFGT 0 = Fault 1 = Busy 2 = Completed (OK)
41002	R	Write Result Factory Settings DFRC 0 = Fault 1 = Busy 2 = Completed (OK)
41003	R	Write Result Factory Settings OEM 0 = Fault 1 = Busy 2 = Completed (OK)
41100-41139	-W	Factory settings DFGT. The value range of each registers is 0-255 Note: Individual write is not possible, all registers should we written in one message.
41200-41219	-W	Factory settings DFRC. The value range of each registers is 0-255 Note: Individual write is not possible, all registers should we written in one message.

Reg. No.	Read Write	Function / Name
41300-41329	-W	Factory settings OEM. The value range of each registers is 0-255 Note: Individual write is not possible, all registers should we written in one message.

4 Installation instruction

4.1 Modbus over TCP/IP

When the power and Ethernet connection are made the device gets it IP address from the DHCP server. Default if no DHCP server is available it will use a fixed IP address. Both Ethernet LEDs will be ON when the DHCP server has assigned the IP address, otherwise only one LED will be ON.

The APP needs the IP address of the device to be able to control it. Either the APP scans for the device(s) or the user must enter the IP address. The Unit Identifier of the device is 1.

4.1.1 IP address discovery

To detect the IP-address of the device automatically the device is supporting mDNS, part of the Apple Bonjour mechanism.

The mDNS query response contains:

- Service Record:

  HWBRDG-DF._modbus._tcp.local. 3600 IN SRV 0 0 502 HWBRDG-DF.local.

  <Instance Name> = HWBRDG-DF (this name is specific for the fireplace gateway)
  <Service Type> = ._modbus._tcp
  <Domain> = local.
  <TTL> = 3600
  <port> = 502
  <target> = HWBRDG-DF.local.

- Pointer Record:

  _modbus._tcp.local. 3600 PTR HWBRDG-DF._modbus._tcp.local.

A mDNS query response message is broadcasted after the Ethernet link is made and repeated every hour.

It is also send as a mDNS response on a query for the service type _modbus._tcp.local

According to the mDNS protocol all message are send to multicast address 224.0.0.251 UDP port 5353

Note:

The device does **not** support the Automatic Private IP Allocation that's using IP address range 169.254.0.0 – 169.254.255.255.

Because not all routers supports the mDNS protocol broadcast correctly this mDNS packet is also send every 10 seconds to UDP port 35353 to IP-address 255.255.255.255

4.2 Modbus RS485

After initial power-up the slave address of the device is 207. If needed the slave address can be changed to any other address.

4.3 Binding procedure

Before the Ethernet or Modbus device can be used the gateway must be bound to the DFGT.

To bind the product the DFGT must be set in to binding mode by pressing the button on the DFGT or via a power cycle of the DFGT. Within 5 minutes this Ethernet or Modbus device must initiate binding.

Note: The DFGT only supports one binding to a control device, so either a RC or a gateway can be used to control the fireplace.

Note: In case multiple fireplaces are in binding mode within range and it's unclear with device will be successfully bound.

4.3.1 Push button binding

When the user presses the button on the device it tries to connected with another device that is also in binding mode at that moment. When the binding is successful the RF node gets automatically a Modbus slave address Unit Identifier assigned.

The first used slave address / Unit Identifier is 2. This number is incremented for every new binding.

Note: Because each RF node will get a slave address on the RS485 bus it's not advisable to use the push button binding method when multiple devices are connected to the RS485 bus.

4.3.2 Modbus binding

Via a Modbus command the binding can be initiated. Together with the command the slave address / Unit Identifier of the new RF node is send to Modbus slave. This new slave address / Unit Identifier can be used to communicate with the RF node after the binding is successful completed.

Single Bound RF nodes can be removed from the device via the remove bounded RF device holding register command.

5 Safety restrictions

5.1 Remote control

For safety reasons (regulations) it's might be an issue if the fireplace is controlled (ignited) from outside the house. So it's advisable to disable the connection to the gateway from a public IP address and only setup a connection from the same subnet as the where the Modbus device is.

Note: viewing the actual status is no problem from outside.

5.2 Remote reset

For safety reasons (regulations) it's not allowed to automatically perform a reset operation, it must be **manually** triggered.

Within 24h it's not allowed to reset too often. The "*Reset fireplace can be initiated by customer*" flag indicates if it's allowed to perform a reset. If this flag is not set the reset command is ignored by the DFGT.

5.3 Communication Timeout

Either due to malfunction of a smartphone/tablet, router or the absence of the smartphone the fireplace is automatically shut down when there is no Modbus communication for at least 60 minutes (setting).

The fireplace DFGT itself also performs a shutdown when there is no RF communication with the Modbus device for a specific time.

Note: when Wi-Fi is turned off on a phone or tablet a shutdown might occur unintentionally.

5.4 Encryption

The Modbus over TCP/IP communication is not encrypted or protected in any way. So it's not advisable to communication via the internet (WAN).
Hence it's still possible to perform port forwarding on the router to get access from outside.

5.5 Legislation RF frequency

Due to legislation on the used RF frequency (868.3MHz) it's not allowed to communicate more than 1% in time. Therefor the App must limit the communication with the fireplace when the user is not actively operating the device. In general it should not write values more often than once every 10 - 30 seconds.

6 Future functions

A future Ethernet gateway can setup a permanent encrypted connection with a server on the internet. This server is providing a way of communicating with the gateway behind a router (or firewall) from anywhere on the internet.

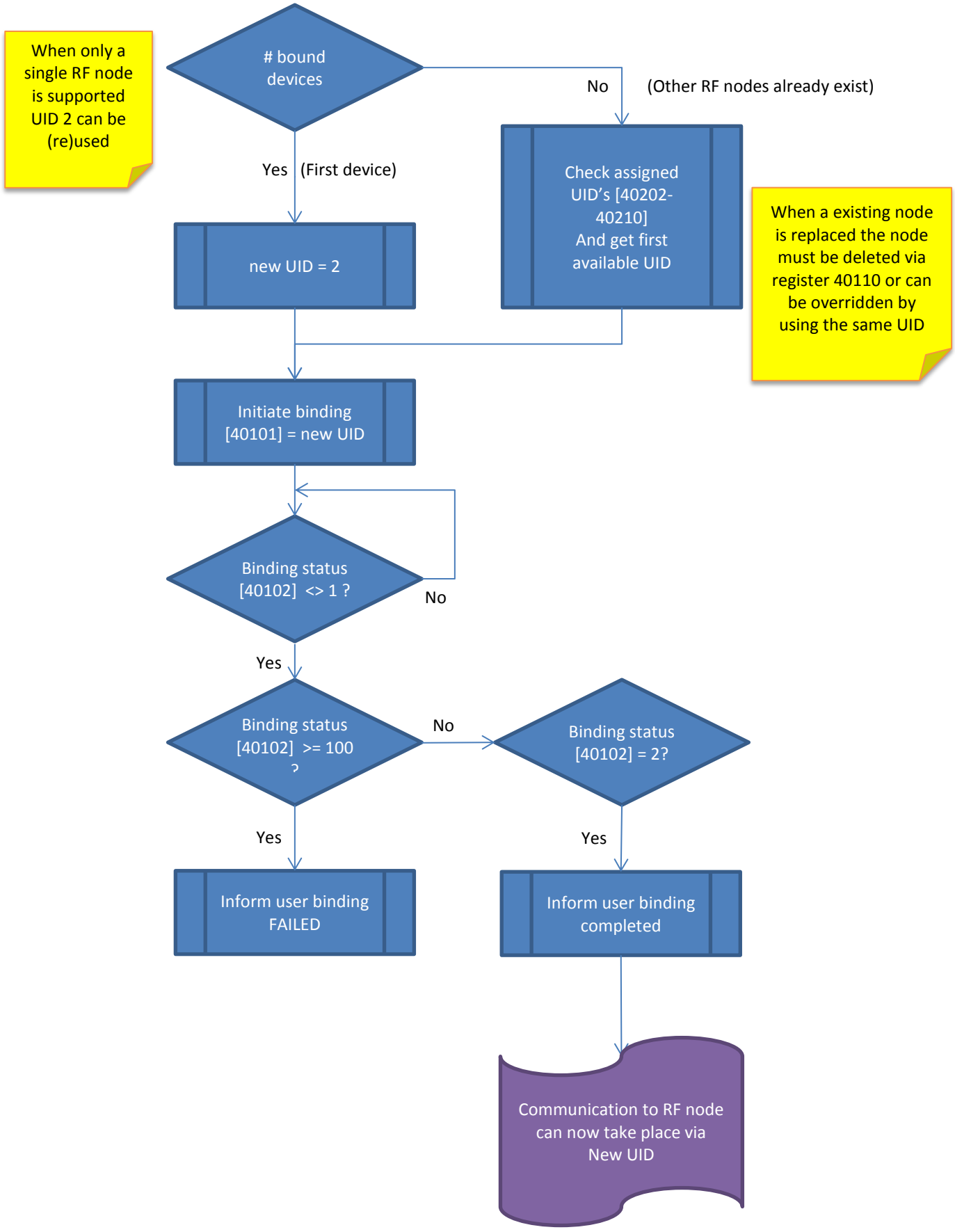
This server also gives the possibility to have concurrent connections to multiple user interfaces (phones, tablets) to a single gateway.

It's not allowed to send continuously commands or flame height via the APP in this case.

Some new control functions might be added like:

- Time schedule temperature control
- AES encryption

Appendix A Adding New RF device via Ethernet Modbus



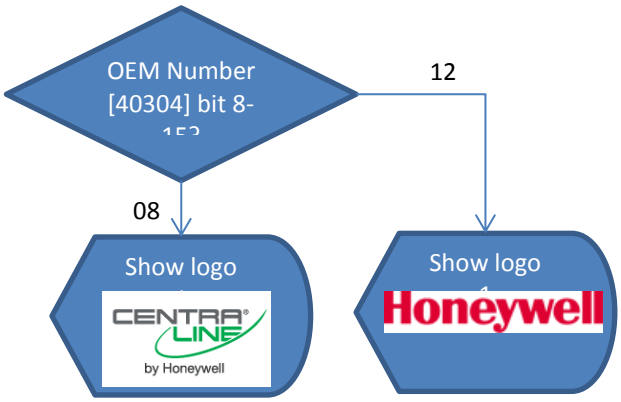
Appendix B Detecting device Capabilities

It's up to the fireplace manufacturer if he want to use this auto detection mechanism. It's also possible to let the consumer select it's model number

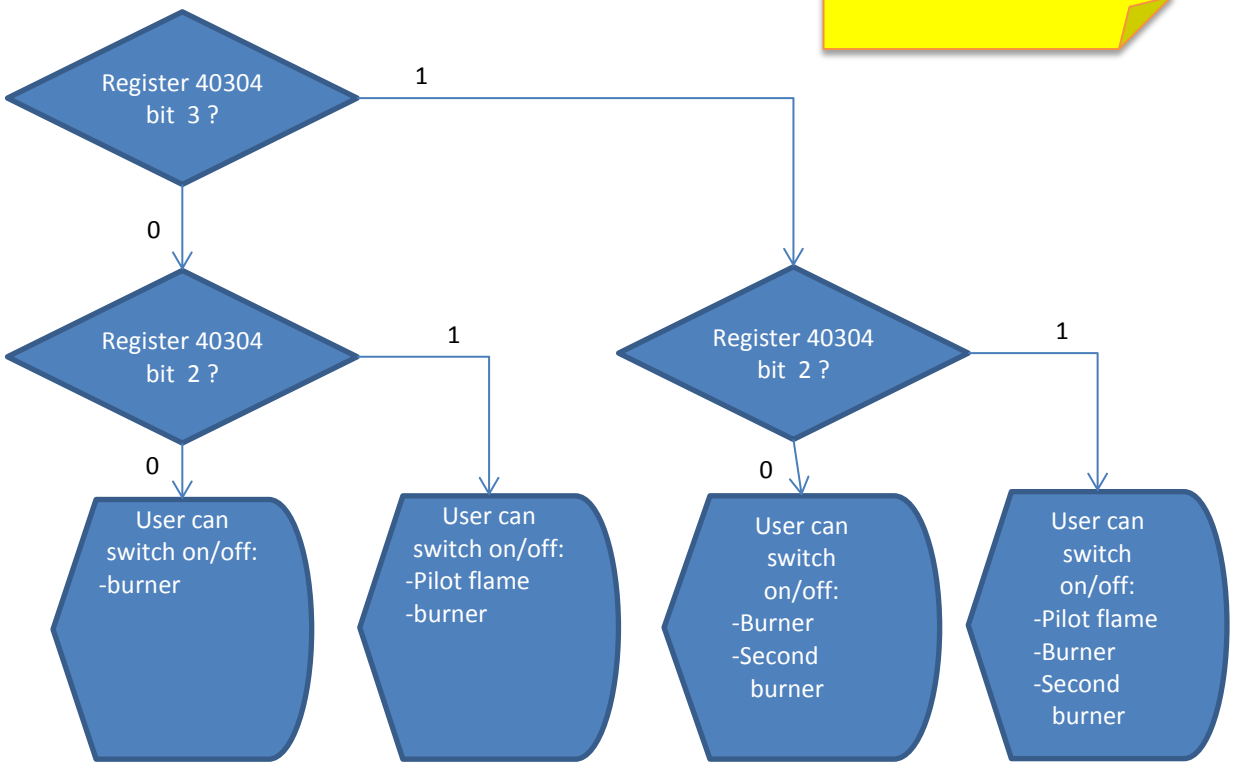
Registers 40300 – 40304 are programmed inside the appliance during production. The meaning of the values is manufacturer specific

The following data is used as an **example**.

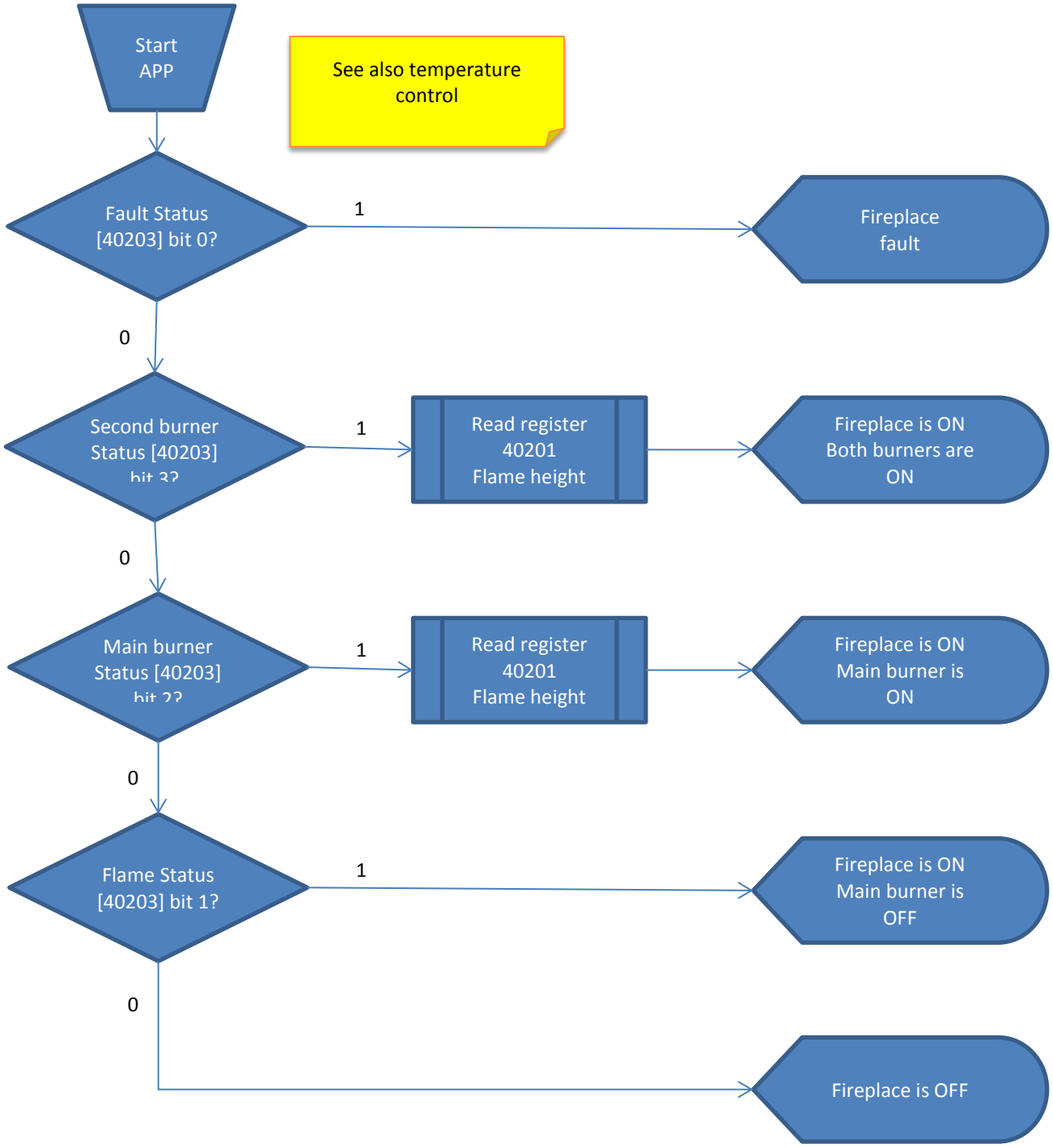
40304 bit 0: 0 = Closed fire place
1 = Open Fireplace
bit 1: 0 = DBI Application
1 = Pilot Application
bit 2: 0 = Intermitted pilot
1 = Standing pilot
bit 3: 0 = single burner
1= double burner
bit 8-15: manufacturer number



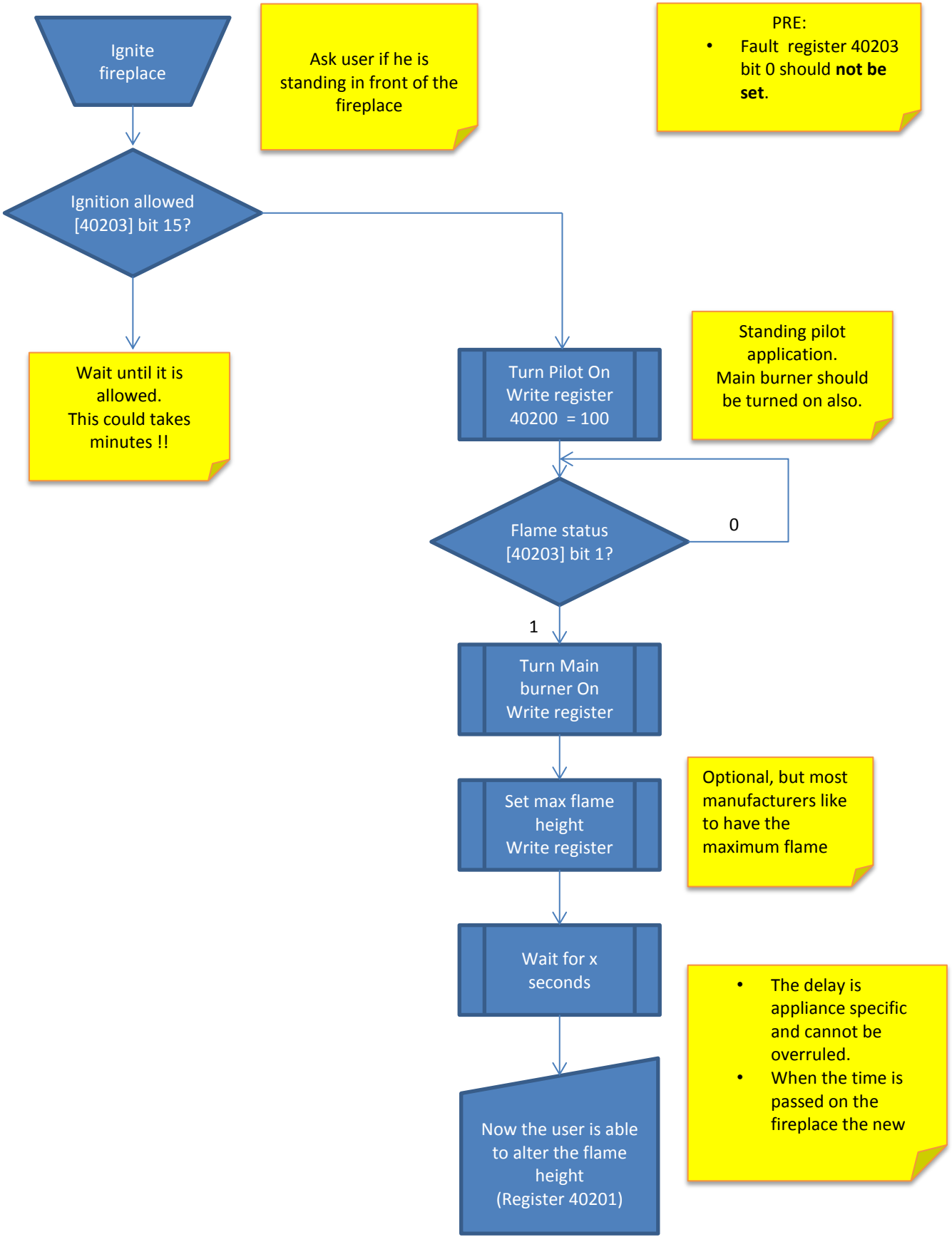
The manufacturer number can be made unique so every fireplace manufacturer has its own number and a generic app can be used for different brands



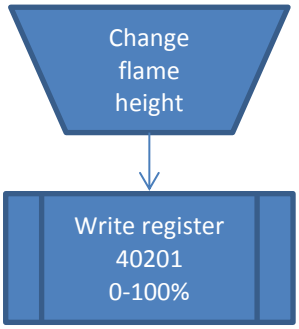
Appendix C User interaction APP is started

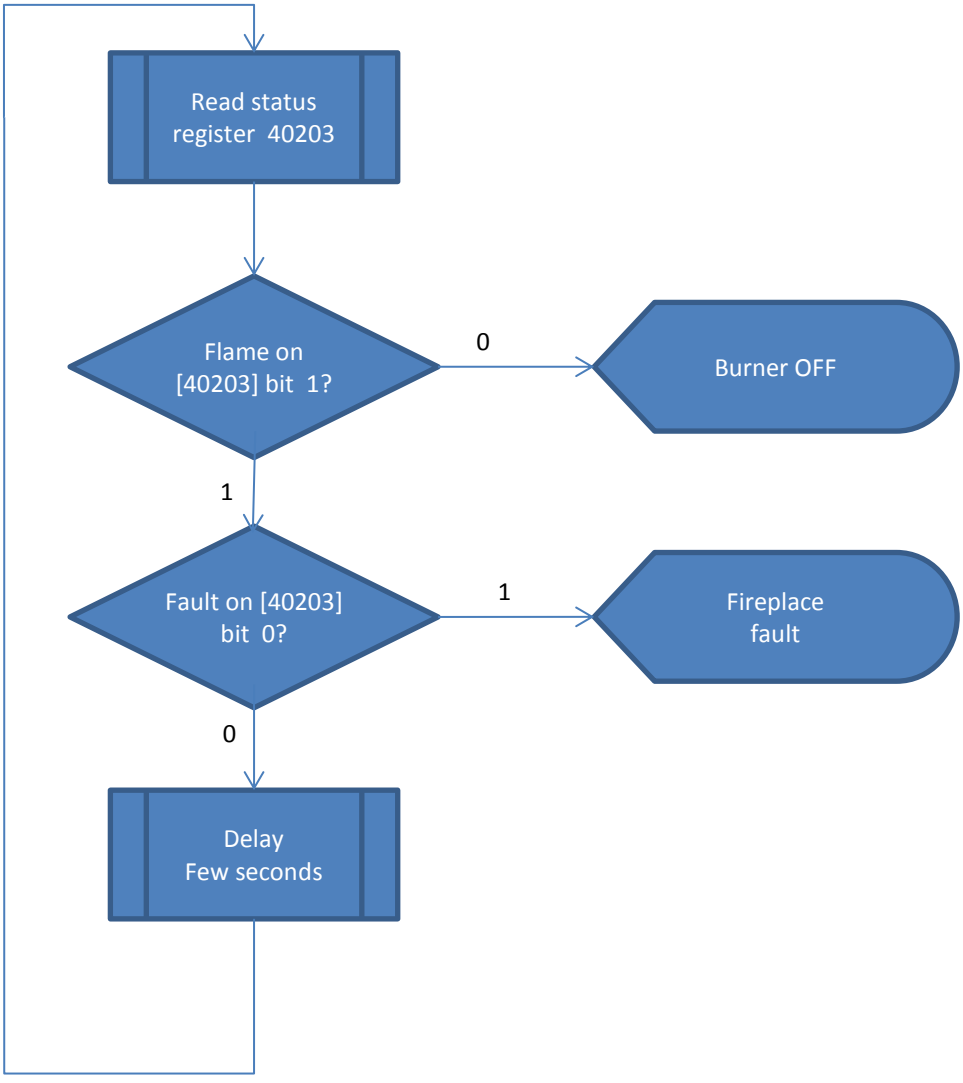


Appendix D User interaction ignite fireplace

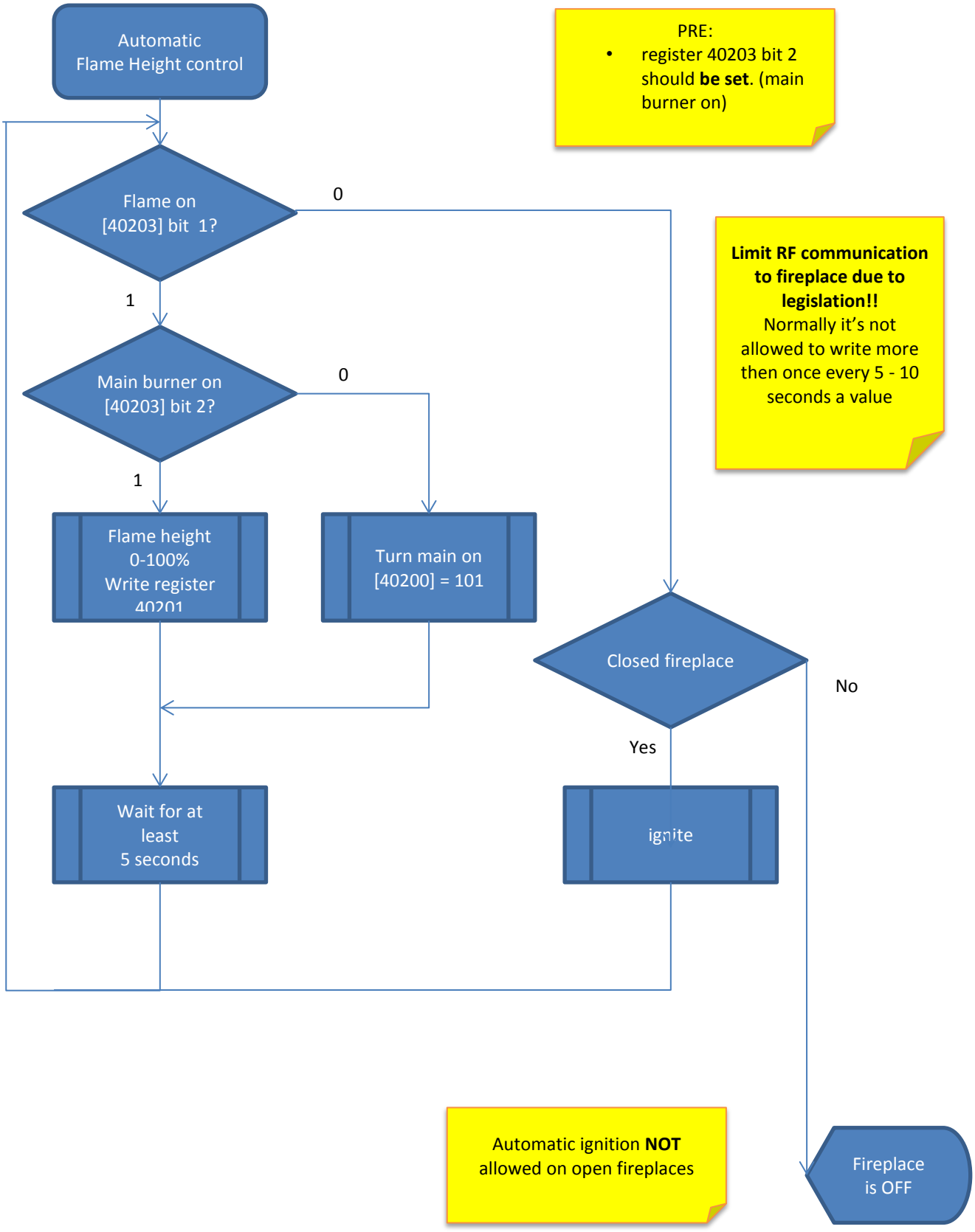


Appendix E Normal use fireplace

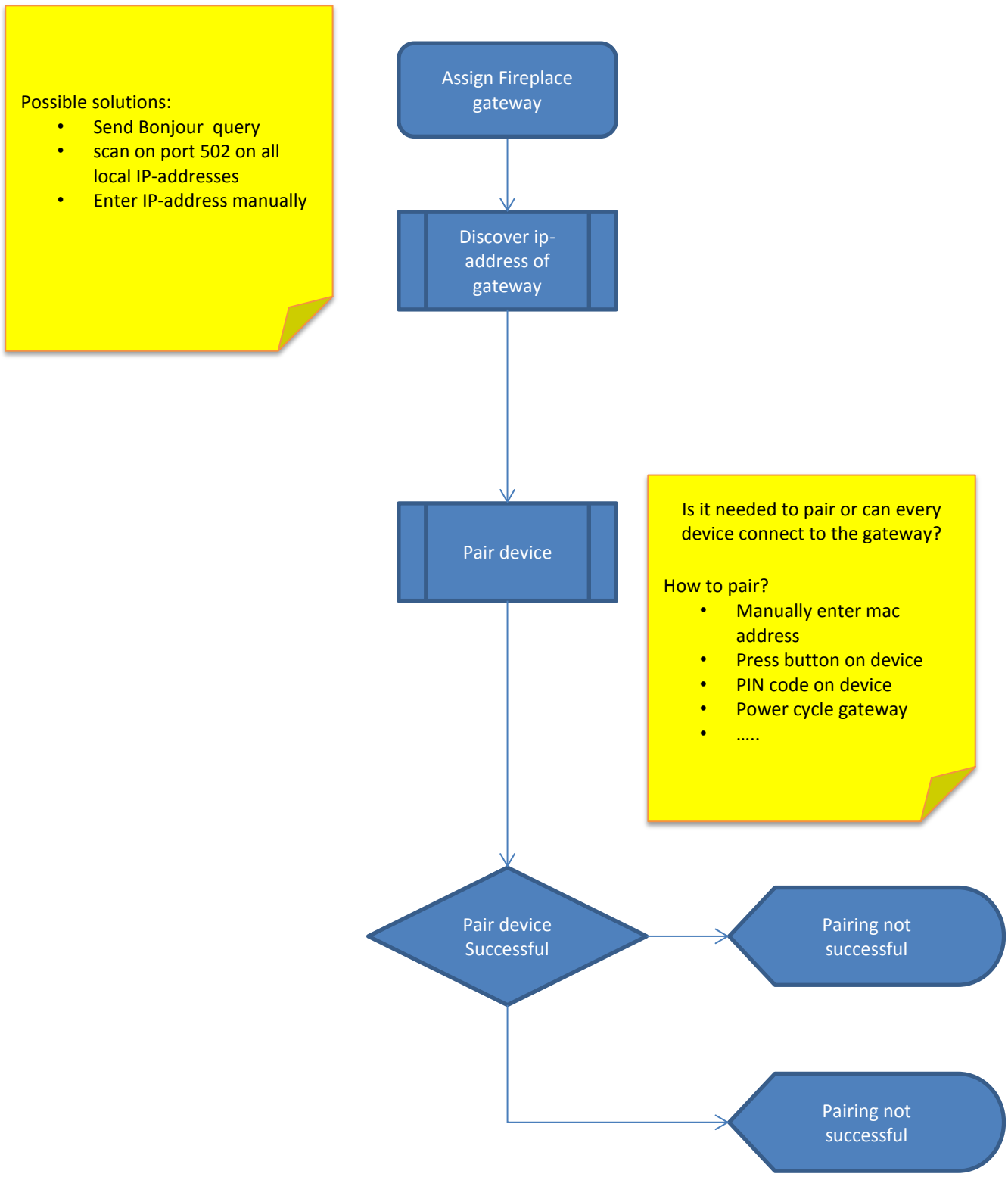




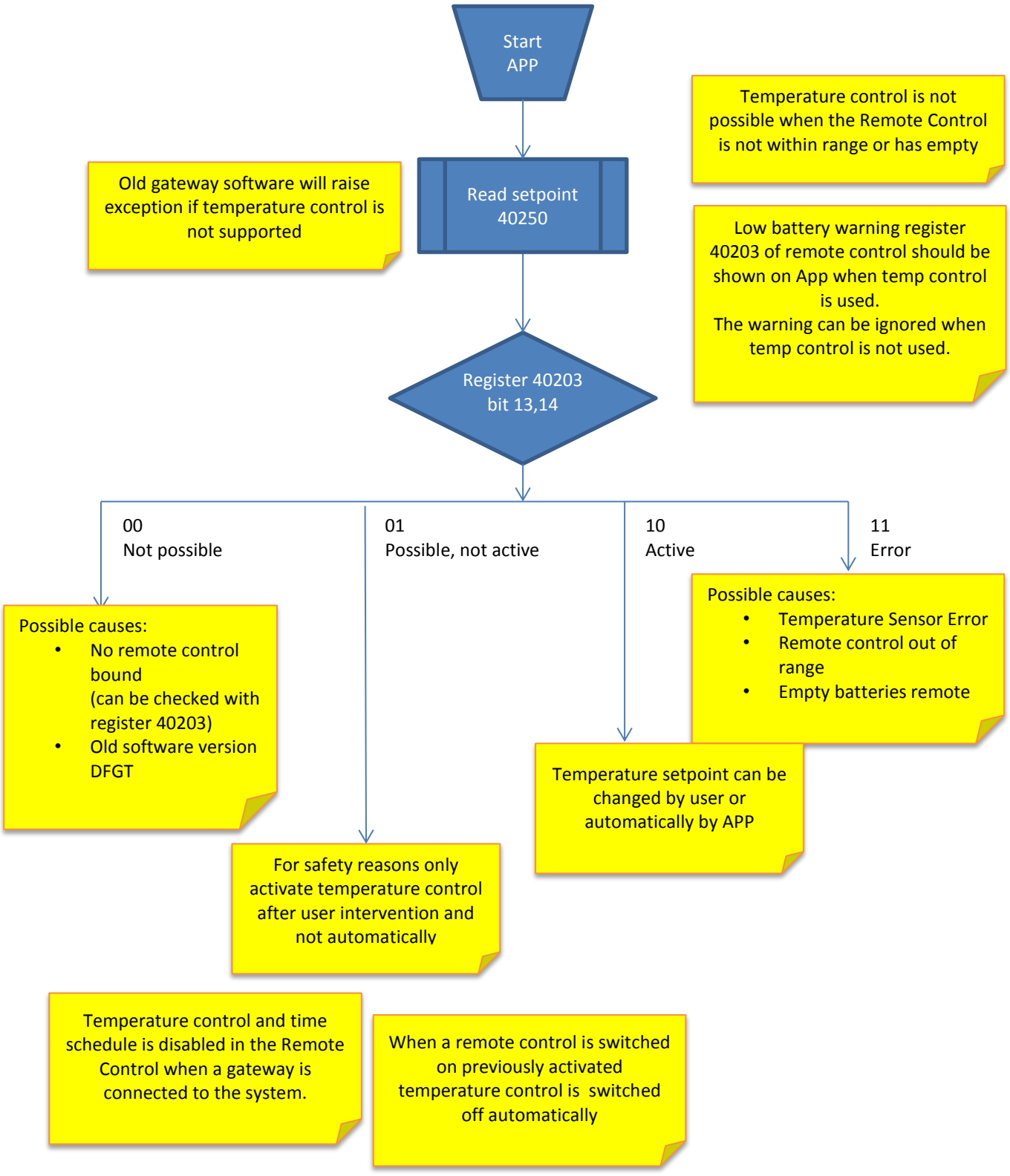
Appendix F Automatic flame height control fireplace



Appendix G Assign fireplace to APP



Appendix H Temperature control



Appendix I Use gateway as factory tool