FireAvert Z-Wave® 800 Integrator's Guide

Rev. A1

November 6, 2025

Contents

Introduction

This document exists to define the Z-Wave® Controller integration details needed to support the Z-Wave enabled FireAvert product. In order to understand how the device operates, it will be helpful to review the background of how the device functions at a high level.

Background

The **FireAvert device** (hereafter just **device**) connects in-line with the energy source for a heating or cooking **appliance** (usually a stove) - either gas or electric. The device contains a relay or shutoff valve to intelligently disconnect the cooking appliance from its energy source when smoke alarms are detected to ensure any fires that are starting or have started due to unattended cooking or cooking mishaps can be dealt with or even prevented entirely.

The FireAvert product is not intended to replace the user's own responsibility and good judgement in preventing fires, especially rapidly combusting fires such as grease and oil fires which fail to emit smoke before igniting.

Device Functionality

The device has two major subsets of functions - the 'core functionality' and the 'Z-Wave functionality'. The 'core functionality' autonomously performs most of the work of the device, with the audio processing and core safety and shutoff logic, while the 'Z-Wave functionality' provides integration with a Z-Wave network - Sending notifications to the controller, appropriate control of the device, and so forth.

The FireAvert is a relatively complex device that contains unique safety features with behavior that intersects multiple Command Classes, so the Z-Wave representation of the device is not particularly intuitive. It is paramount to understand the 'core functionality' of the device so that its capabilities can be effectively utilized.

It is important to note that the 'Z-Wave functionality' is **NOT** required for the device to operate safely. Network integration simply expands the capabilities of the device - allowing it to interact with the other devices in the network and strengthen the protection provided beyond what is possible with the device alone - but the device will continue to protect the home and prevent fires regardless of if the network is down or non-existent.

Core Functionality

The FireAvert device contains a microphone and audio processing logic to listen for smoke alarms, and a relay to shut off electric power or gas flow to the appliance to which it is connected.

Activation

If the FireAvert device detects a smoke alarm, the following occurs:

- If the device is attached to an electric appliance, it determines if the appliance is drawing enough current to be considered 'on'. If the appliance isn't on, it is not the source of the smoke.
- If the device is attached to a gas appliance, there is no checking for an 'on' state. The device, for safety reasons, assumes that the appliance is the source of the smoke.

If the device determines that the appliance is the potential source of the smoke, the appliance is shut off (the device is **triggered** or **activated**), either by closing the gas valve or disengaging the relay.

Re-arm

Once the device has activated (e.g. triggered) and power has been removed from the appliance, the re-arming process for gas and electric appliances differs slightly. However, the common thread is that the Z-Wave interface has **no** control of the electric relay or gas valve until there are no smoke alarms detected. When that condition is met, the following steps can take place to re-arm the device:

- For a **gas** appliance, the valve will remain closed until one of several interlock operations occur. The user must go and physically interact with the device before the device is put into a **re-armable** state. These physical interactions ensure that a user is verifying that reopening the gas valve will not result in a more dangerous situation (e.g. house explosion).
  - Because Z-Wave has no protected lockout mechanism, a gas appliance **CANNOT** be re-armed remotely via the Z-Wave network without this interaction. Attempting to do so will be rejected and an alarm will be sent to the controller.
- An **electric** appliance does not require physical interaction, rather, after a set time period, the device will attempt to self-re-arm by measuring the momentary current draw. If the current is too high because the appliance's heating elements were left in the **ON** state, the device will immediately shut off.
  - This process will repeat several times, after which the device will require user intervention to become **re-arm-able**.
  - Sending a Z-Wave re-arm request, using the Binary Switch endpoint, to a device controlling an electric appliance will always result in the device re-arming, regardless of the power state of the appliance's heating elements.

Z-Wave® Functionality

As the core functionality of the device revolves around notifying the network of behavior of the largely autonomous FireAvert device, and existing smoke alarms in the Z-Wave ecosystem present as Notification Sensors, the root device type is defined as a Notification Sensor.

The device will notify the controller via Lifeline of the following state changes - Device Trigger/Re-arm (Binary Switch Report) - Appliance Power On/Off (Notification Report) - Smoke Detected/Silenced (Notification Report)

Now, while the device contains a physical relay or gas valve (or **actuator** in Z-Wave terminology), for safety reasons, full control akin to a more typical Z-Wave Binary Switch cannot be extended to the controller, and the device will exhibit some **non-default behavior** in regards to Binary Switch functionality. However, the following operations are allowed:

- The controller may send a Binary Switch Get to retrieve the state of the actuator at any time.
- The controller may send a Binary Switch Set (0x00) to shut off the actuator at any time.
- A Binary Switch Set (0x01) command from the controller only **requests** a re-arm of the actuator. If rejected due to lockouts or unmet requirements for re-arming the device, the node will respond with an Application Status Rejected or Supervision Fail.
- The appropriate Binary Switch Report message will be sent via Lifeline to the controller when the device shuts off or is re-armed in addition to any applicable notifications listed below in the Notifications section.
- Binary Switch operations, when triggered with Supervision encapsulation, will by default return a Supervision::Working status, followed by a Supervision Success or Fail when the device is able to set the switch to the requested state, or is rejected.

Other helpful Z-Wave functionalities include:

- The 'Re-arm-able' state of the device can be retrieved by the controller using a Z-Wave configuration parameter.
- The device will send an unsolicited Notification to Lifeline when the device is re-arm-able, or a re-arm operation is rejected due to the device being in a non-re-arm-able state.

Z-Wave Plus® Information

End Point	Type	Value
N/A	Role Type	Always On End device (AOS) (0x05)
N/A	Requested security keys	S2_ACCESS_CONTROL, S0
N/A	Manufacturer ID	FireAvert (0x045D)
N/A	Product ID	0x0601
0 or 1	Generic Type	Sensor Notification (0x07)
0 or 1	Specific Type	Notification Sensor (0x01)
0 or 1	Icon Type	Sensor Notification Smoke Alarm (0x0C01)
2	Generic Type	Switch Binary (0x10)
2	Specific Type	Not Used (0x00)
2	Icon Type	Generic On/Off Power Switch (0x0700)

Because the device requests the highest level S2 Access Control security keys for safety, an S2-enabled controller MUST be used with this device.

Z-Wave Network Operation

The FireAvert Z-Wave device supports both SmartStart and Classic network inclusion by following the steps outlined in the table below:

Function	Action	Description
Add (SmartStart)	Automatic	To add device to network using SmartStart: - Scan the device's SmartStart QR code into the controller's SmartStart manifest. How to do this will vary by controller - consult the controller documentation if needed. - Power on the device. SmartStart inclusion will begin automatically.
Add (Classic)	Button Press	To add device to network using Classic inclusion: - Set the controller to Classic Inclusion mode. How to do this will vary by controller - consult the controller documentation if needed. - Hold the button on device for 3 seconds. The device will be put into Classic Inclusion mode and the onboard LED will begin flashing green. - If the controller is not in Inclusion mode, the device will stay in Inclusion mode for 60 seconds before returning to an idle state.
Remove (Classic/SmartStart)	Button Press	To remove a device from the network: - Set the controller to Exclusion mode. How to do this will vary by controller - consult the controller documentation if needed. - Hold the button on device for 3 seconds. The device will be put into Exclusion mode and the onboard LED will begin flashing green. - If the controller is not in Exclusion mode, the device will stay in Exclusion mode for 60 seconds before returning to an idle state.
Factory Reset	Button Press	To force the FireAvert device back to its factory default settings: - Hold the button on the controller for 10 seconds. All settings will be cleared and the device reset.

Note that when the network inclusion is started manually (Classic inclusion, not SmartStart), the device blinks by the indicator LED at 1 Hz with LED is On for 100 ms then LED is Off for 900 ms.

Long Range Support

The FireAvert Z-Wave device supports inclusion using Z-Wave Long Range. SmartStart MUST be used in order for the device to be included in a Long Range network.

Supported Command Classes

The FireAvert Z-Wave device supports a number of Command Classes, most of which are required. The following is a list of supported Command Classes.

Command Class	Version	Required Security Class
Application Status	1	None
Association	2	Highest granted Security Class
Association Group Info	3	Highest granted Security Class
Basic	2	Highest granted Security Class
Binary Switch	2	Highest granted Security Class
Configuration	1	Highest granted Security Class
Device Reset Locally	1	Highest granted Security Class
Firmware Update	5	Highest granted Security Class
Indicator	3	Highest granted Security Class
Manufacturer Specific	2	Highest granted Security Class
Multi-Channel Association	3	Highest granted Security Class
Notification	8	Highest granted Security Class
Powerlevel	1	Highest granted Security Class
Security 2	1	None
Supervision	1	None
Transport Service	2	None
Version	3	Highest granted Security Class
Z-Wave Plus Info	2	None

Indicator Command Class Information

The onboard LED on the front of the FireAvert device is what is used for the Indicator CC to identify the device.

When the Identify functionality is engaged, the LED on the front of the device will flash green in accordance with the parameters provided in the Identify command.

Association Group Configuration

ID	Name	Description
1	Lifeline	Supports the following commands (CCs): - Device Reset Locally (Device Reset Locally CC): when factory reset. - Binary Switch Report (Binary Switch CC): when actuator changes state. - Indicator Report (Indicator CC): when indicator light changed. - Notification Report (Notification CC): see Notifications section.

Lifeline (Group 1) Node Count

Node Count	Endpoints
X	Root
0	1 (Sensor)
0	2 (Switch)

X: For Z-Wave node count is equal to 5 and for Z-Wave Long Range it is 1.

Multichannel Association Group Information

This end node functionally does NOT utilize Multichannel Association Groups. The node will report an association group node count of 0 for all non-root endpoints.

Supervision & Application Status

This device supports both Supervision Encapsulation and the Application Status CC for reporting the outcome of a command back to a controlling node.

See the Z-Wave Functionality section for information on when a Supervision Fail or Application Rejected frame is sent to the controller.

Application Busy is unused and will never be returned in response to a command.

Dynamic Capabilities

While there are no capability changes via a configuration parameter or physical change that would require a reset or re-interview, the controlling node must able to gracefully handle an Application Rejected or Supervision Fail in response to a Binary Switch Set.

It is recommended that upon receipt of an Application Rejected status that the controlling node query the state of the relay with **Binary Switch Get**.

Basic Command Map

For backward compatibility reasons, the Basic Command Class actions must be mapped to a Command Class that best represents the device. For the FireAvert device, the Basic Command Class is mapped to the Binary Switch (on end-point 2) that is responsible for controlling the internal power relay that powers the appliance.

Basic Command	Mapped Command
Basic Set	Binary Switch Set
Basic Get	Binary Switch Get
Basic Report	Binary Switch Report

Notifications

Z-Wave sends unsolicited Notification Report messages when the FireAvert device changes states or activates. These notifications are always sent from Multi-Channel endpoint 1 to all nodes listed in the root's Lifeline Association Group. The following is a list of notifications the FireAvert device can emit and under what conditions it will emit them.

Notification Type	Notification Event/State	Description
Smoke Alarm (0x01)	Supports the following event/state: - State idle (0x00) - Smoke detected (0x02)	***Smoke detected*** will be sent under the following conditions: FireAvert device hears an existing, independent Smoke Alarm sound for 30 seconds ***State idle*** will be sent under the following conditions: FireAvert device no longer hears an existing, independent Smoke Alarm sound
Power Management (0x08)	Supports the following event/state: - State idle (0x00) - Power has been applied (0x01)	***Power has been applied*** will be sent under the following conditions: - Appliance current detected ***State idle*** will be sent under the following conditions: - No appliance current is detected for 5 minutes
Appliance (0x0C)	Supports the following event/state: - State Idle / No Event (0x00) - Safety Interlock Engaged (0x16)	***Safety Interlock Engaged*** will be sent under the following conditions: - Device is not safe to arm and remote re-arm requests will be rejected ***State Idle / No Event*** will be sent under the following conditions: - Device is safe to re-arm

Alarms

The Alarm CC is a legacy command class that was superseded by the Notification CC - however, the function of this CC is still allowed in the case that there is unsolicited information that needs to be sent that is not well served by any of the existing Notification Types. A Z-Wave Notification report contains two 1-byte fields - **Alarm Level** and **Alarm Type** - that are ordinarily set to 0x00, but when Alarm bytes are used these can be any values insofar they are properly documented.

The Z-Wave enabled FireAvert device uses the following values for these bytes when sending Appliance (0x0C) notifications described below:

Event	Notification Type/Event	Alarm Type	Alarm Level
Device Re-arm Lockout	Appliance (0x0C) Safety Interlock (0x16)	0x0C	0x01
Device Re-arm Ready	Appliance (0x0C) No Event (0x00)	0x0C	0x00

Configuration

User can change the default settings for the configuration parameters listed below. After a factory reset, all of these parameters will be set to their default values.

All configuration values are read only and will only take the form of whole numbers (0,1,2, etc.).

Bulk Configuration commands are NOT supported on this device.

Safe to Arm

Parameter #	1
Size	1
Range	0..1
Default	N/A
Access	Read only
Description	0 if FireAvert is not re-arm-able, 1 if it is re-arm-able.

Trigger Count

Parameter #	2
Size	2
Range	0..65535
Default	0
Access	Read only
Description	The number of times the device has been activated (triggered).

Recommended Platform Automations & Useful Tips

Configuration Retrieval

Because the Safe to Arm and Trigger Count read-only configurations can be linked to useful UI elements, it is recommended that these configuration values be retrieved with a Configuration Get command when the FireAvert device sends one (or more) of the following:

- Binary Switch Report
- Notification Report of type 0x0C (Appliance)

Power Warn

Dangerous conditions can occur if an appliance is left on even if there is no smoke. In addition to smoke detection, the FireAvert device can be a helpful tool in monitoring the state of the appliance.

It is recommended that the Power Management notifications be used in tandem with a timer or geofence within the ecosystem to alert the occupants that the appliance has been left on, for example, when an occupant leaves the house, or it has been on continuously for a period long enough to be clear it has been left on by mistake.