Instruction

How to Use Certified Apps in Z-Wave 700

Document No.:	INS14278
Version:	8
Description:	-
Written By:	JFR;AYURTTAS;COLSEN;JSMILJANIC
Date:	2020-01-14
Reviewed By:	JFR;NOBRIOT;COLSEN;KEWAHID;JKA;RREYES;SEROMAN1;SCBROWNI
Restrictions:	

Approved by:

REVISION RECORD

Doc. Rev	Date	By	Pages affected	Brief description of changes
1	20181205	AMUNKHAUS	ALL	Initial release of document.
2	20180212	AMUNKHAUS	ALL	Reviewed for release.
3	20180226	AMUNKHAUS	ALL	Fixed certification issues.
4	20190318	JFR	5.1.1 5.2.3 5.6.4 5.6.1 5.4.4 5.2.3 5.4.1 5.1.2 5.2.4 5.3.1	Clarified reset to factory default. Removed Association Group having ID 2 from Door Lock Key Pad. Removed Trigger association group 3: Multilevel Switch Set from Wall Controller. Removed Basic CC as supported from Wall Controller. Updated button actions for Sensor PIR. Updated association group description wrt. door lock configuration/operation and user code. Removed Security CC (S0) as supported from Sensor PIR. Added SmartStart description including QR code readout. Updated buttons interface description and added BTN3. User default code added. Removed Switch Multilevel CC from root NIF.
5	20190704	CHOLSEN	5.3.2	Corrected endpoints.
6	20190712	SCBROWNI	All	Minor typos
7	20190902	JESMILJA	5.2.2	Updated Table 4 with correct mapping of CC Basic for Door Lock Key Pad
8	20191230	JFR	All	Changed 7.11 to 7.1x

Table of Contents

Table of Figures

Table of Tables

1 ABBREVIATIONS

Abbreviation	Explanation
AGI	Association Group Information
AOS	Always on slave
BEA	Button Extension Adapter
FLiRS	Frequently Listening Routing Slave
IDE	Integrated Development Environment
LSS	Listening Sleeping Slave
RSS	Reporting Sleeping Slave
S0	Security 0 Command Class
S2	Security 2 Command Class
SDK	Software Development Kit
ZAF	Z-Wave Plus v2 Application Framework

2 INTRODUCTION

2.1 Purpose

The purpose of this document is to describe how to use the Z-Wave certified applications which comes as part of the Z-Wave SDK 7.1x.

2.2 Audience and Prerequisites

The audience is Z-Wave Developers.

It is assumed developers already have the development environment up and running, as per the instruction " INS14280 Z-Wave 700 Getting Started for End Devices" [10].

3 SOFTWARE AND HARDWARE

This section will present the hardware that comes as part of the development kit and the needed software to start developing Z-Wave devices. For a guide in how to setup and connect the hardware, refer to [10].

3.1 Hardware Needed

The Z-Wave development kit contains the following:

- WSTK Main Development Board, 2 pcs.
- BRD4200A Radio Board with ZGM130S intended end device development, 2 pcs.
- BRD8029A EXP Board, 2 pcs.
- UZB7 Controller USB Dongle
- Zniffer USB Dongle

Figure 1: Content of the Z-Wave Development Kit

3.1.1 Main Development Board

The Main Development Board connects to the PC using USB. It features a coin cell holder, supports Advanced Energy Monitor for battery measurements and energy profiling, as well as expansion headers for easy expansion. It has an on-board SEGGER J-Link for debugging, a low-power 128x128 pixel LCD, user LEDs / pushbuttons, and breakout pads for attaching the Z-Wave development board.

Figure 2: Main Development Board

3.1.2 Z-Wave Development Radio Boards

Two Z-Wave Development Radio Boards targeted for end device development are included in the kit. Another radio board targeted for controller development can be purchased as an add-on to the kit.

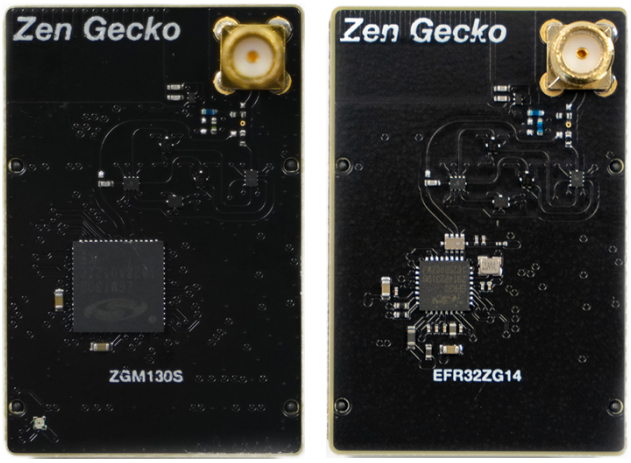


Figure 3: Z-Wave Development Radio Boards (Left: BRD4200A, Right: 4201A)

The possible options are:

- BRD4200A Radio Board with ZGM130S used for end device development [included]
- BRD4201A Radio Board with EFR32ZG14 used for controller development [add-on]
- BRD4202A Radio Board with ZGM130S with no SAW filters used for end device development [add-on]

While BRD4200A and BRD4202A are intended for end devices, it can also be used for Controller development. The difference is the BRD4200A / BRD4202A comes as a SiP module, provides IO, and as such has a higher cost.

The boards include World Wide SAW filter configuration, so the same development boards can be used to test all regions.

3.1.3 Recommendation on SAW filters

For Z-Wave gateways (outside EU freq.) with LTE embedded, it is recommended to analyze the specific need for a SAW filter in depth. Optionally, a SAW filter bank can be added and controlled via the SAW0 and SAW1 output pins for operation in different regions. This means:

No SAW

- End-devices and gateways without LTE modem embedded no SAW filter is recommend.
- Gateways on EU frequency with LTE modem embedded no SAW filter is recommend.

SAW recommended

- Gateways with LTE embedded on U and H related frequencies using a SAW filter is recommend.

3.1.4 EXP Board

The EXP Board is an adapter to be connected to the EXP-header of the WSTK main board. The EXP Board enables the platform to run the provided Z-Wave certified application by expanding the available buttons and LEDs. The EXP Board offers the following features:

- 4 push buttons
- 1 slide switch
- 4 LEDs

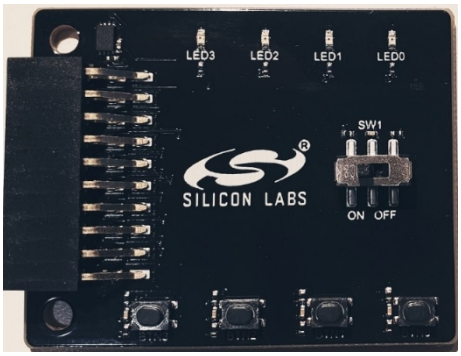


Figure 4: Button Extension Adapter

LED0 on the expansion board is wired in parallel with LED0 on the mainboard (both will turn on/off at the same time).

BTN0 and BTN1 on the expansion board are wired in parallel with PB0 and PB1 on the mainboard.

3.2 Software Needed

All you need to start developing Z-Wave devices is Simplicity Studio.

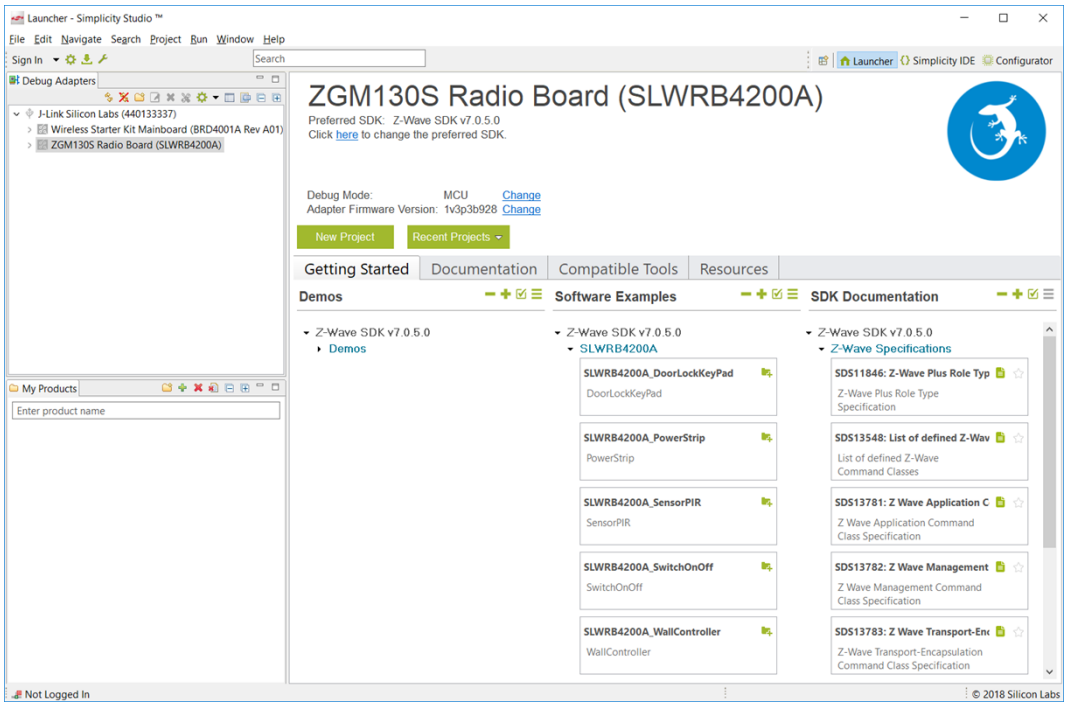


Figure 5: Simplicity Studio—IDE for Developing Z-Wave Devices

Download the installer from silabs.com, where you will also find additional training material for how to develop, compile, debug, and measure energy consumption.

When connecting the development board with the Z-Wave Radio Development Board attached, the IDE will auto-discover the hardware and show the available Z-Wave certified applications.

4 SDK AND FRAMEWORK INTRODUCTION

4.1 SDK 7.1x Overview

With the release of Z-Wave 700, both hardware, software, and specifications have improved.

The hardware is now based on the Silicon Labs EFM32™ Gecko family, a 32-bit Microcontroller based on the powerful ARM® Cortex®-M3 core. This change has resulted in power consumption being reduced by 80%, the point-to-point range has been increased to over 100 meters, and the mesh range increased to over 400 meters. With fast wake-up and back to sleep-mode, battery powered sensors can now last for ten years using a single coin cell.

To leverage off the powerful hardware, the software has been redesigned. Now the software uses a Real Time Operating System to divide the Z-Wave protocol and the application into independent tasks, an event driving architecture to ensure no direct function calls between protocol and application, and a power manager to automatic power down to lowest possible power mode. While everything has been redesigned, existing customers will find the Z-Wave Framework has been kept, thereby ensuring easy development.

Specifications have been updated to the Z-Wave Plus v2 to ensure interoperability between all Z-Wave products and vendors, and backward compatibility with all existing products. Z-Wave 700 devices work seamlessly with the world's largest ecosystem of interoperable smart products.

4.2 Z-Wave Plus v2 Specification

Each product must follow the Z-Wave Plus v2 specification to be able to pass the certification program and ensure interoperability in the ecosystem of existing products. The primary focus is ease of use for consumers, which can be summarized into the following:

- Shopping does not require intensive knowledge about which products work with which other products.
- Installation is as simple as possible and intuitive.
- Operating the products does not require any technical knowledge.
- No tricky maintenance procedures, such as exclude/include, are needed.

To accomplish this vision, several new requirements are added to the original Z-Wave Plus specification. These additions include:

- Both Security-2 (S2) and SmartStart are now mandatory to increase security while keeping the inclusion process simple.
- Each product must support Identify functionality, i.e. must feature a visible LED for identification purpose, making it easy to identify a product.
- All actuators must support Basic command class, guaranteeing that any controller can control any actuator.

- Any state change must now be reported, making sure the controller always knows the true status of a device.
- OTA Firmware update is mandatory to support for all nodes, and dynamic capabilities are now allowed as a controller must have an option to re-interview a node to detect any new / changed capabilities.

For more information about the specifications, refer to [7] and [8].

4.3 Z-wave Plus v2 Framework

The purpose of the Z-Wave Plus v2 Framework is to facilitate the implementation of robust Z-Wave Plus v2 Compliant products.

The framework is described in full detail in [9]. It is strongly recommended that you read this document before developing your own Z-Wave Application. A short outline can be read here to give the overview.

The ZAF consists of three blocks:

- **Transport Layer:**
  This layer handles all communication with the protocol, which includes single cast, multicast, Multi-Channel encapsulation, delivery of bundled commands, etc.
- **Command Class Handlers:**
  These handlers parse and compose Command Class frames.
- **Utilities (Utils):**
  Utilities are composed of different modules. Among them, there are modules for handling I/O communication specific for the hardware bundled with the SDK. Other modules are battery monitoring and firmware updating, etc.

Figure 6 below outlines the Z-Wave Plus Framework modules.

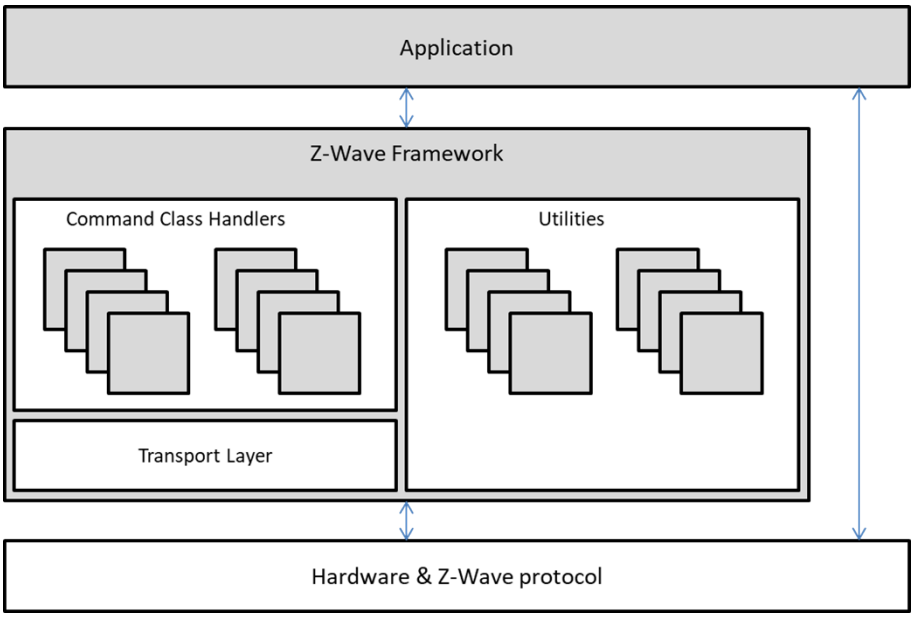


Figure 6: Z-Wave Plus v2 Application Framework

4.4 Libraries

This section introduces the different libraries available in the SDK 7.1x. See [6], [9] for more information.

Overall the SDK has 2 libraries: controller library and slave library. The controller library is used for controllers running Z/IP Gateway and will not be used by end devices. The slave library is used by all the Z-Wave certified applications for end devices.

The slave library can be configured for always on (mains powered) devices or for battery devices.

- Always on Slave (AOS): End devices which are main powered. They are always listening and act as repeaters in the network. Example usages are on/off switches.

- Reporting Sleeping Slave (RSS): Battery operated devices, which remain in sleep mode until they are triggered. Example usages are door/windows sensors and motion sensors.

- Listening Sleeping Slave (LSS): Also known as a Frequently Listening Routing Slave (FLiRS). A special variant of battery operated devices, which provide a mechanism to wake up the device within one second, with battery drain very close to that of a fully asleep device. The FLiRS device alternates between sleep mode and a partially awake mode in which it is listening for a special wakeup beam signal at the rate of once per second. When the FLiRS device receives this beam, it immediately fully wakes up. If the device does not hear a Beam it goes back to full sleep for another period until it partially awakes again and listens for a beam. It is this partially awake mode combined with the special beam that provides for battery lives on par with fully sleeping devices while providing communications latencies of around one second. Example uses are door locks.

4.5 Association Groups and Endpoints

An association is the creation of a logical connection between nodes. It provides the ability to instruct a slave device to directly control other slave device(s) upon activation. A device must support at least one association group (group 1), which is designated for “Lifeline Reporting" (as defined by the Z-Wave Plus v2 Device Type, see [8]). Each group is responsible for controlling and/or reporting specific commands, e.g. a temperature measurement. One group can hold multiple commands if needed.

Association Group Information (AGI) enables Machine-to-Machine interfacing as well as human user interpretation of available association groups, thus eliminating the need for paper-based documentation.

All device-centric events are mapped to the Lifeline group. This includes events such as Battery Low, Tamper Alarm, and Device Reset Locally. The Lifeline concept allows a gateway to set up just one association from a device to get all it needs.

In the example of a motion sensor, the sensor reading is mapped to the Lifeline group, while another association group targets local application functionality such as turning on a lamp based on movement.

Endpoints is the ability for a device to support multiple controllable endpoints within one device. Each endpoint specifies device and command classes supported and can be controlled individually.

4.6 Security

Security 0 was the first version of security. This command class provides a framework for establishing encrypted communications within a Z-Wave network. However, the key exchange at inclusion is vulnerable to interception.

The Security 2 is the latest Security Command Class and is required for all Z-Wave 700 devices. The S2 defines three types of security layers:

- S2 Access Control
- S2 Authenticated
- S2 Unauthenticated

S2 security operates with the concept of a network key. All nodes may use this key to communicate to each other. S2 divides the logical Z-Wave network into three dedicated security classes, with each one having a unique network key. A given S2 security class not only identifies the network key to use but also dictates the rules applying to authentication of a new node during inclusion. The “S2 Access Control” class is the most trusted class, intended for access control devices like door locks and garage doors. The “S2 Authenticated” class is used for all normal household devices such as sensors and light dimmers. The “S2 Unauthenticated” class is the least trusted class and is only intended for the most constrained controllers that, due to a limited user interface, are not capable of authenticating a node joining the network.

In a wireless environment, there is a real risk that a foreign node is included accidentally or due to malicious intent. The S2 authentication process allows an including controller to verify that a joining node is indeed the physical device that it claims to be. Depending on the UI, an including controller may allow the user to enter a Device-Specific Key (DSK) string of decimal digits that can be read visually or scanned as a QR code.

Giving that SmartStart is mandatory for Z-Wave 700 devices, all Z-Wave 700 based devices must request either S2 Access Control or S2 Authenticated. If requesting S2 Authenticated, a node must also request S2 Unauthenticated for backwards combability.

Refer to [3] and [8] for more information.

5 Z-WAVE PLUS V2 APPLICATIONS

Because starting application development from scratch is difficult, the Z-Wave SDK comes with several Z-Wave certified applications covering the most frequent use cases.

The Z-Wave SDK 7 includes Z-Wave Plus v2 slave applications which are implemented according to the Z-Wave Plus v2 specifications [1], [2], [3], [4], [5], [6], [7] and [8].

5.1 Overview of Z-Wave certified Applications

The SDK comes with the following Z-Wave certified applications:

- **Door Lock**
  Shows an implementation of a door lock. It supports user codes and, thereby, eliminates the need for traditional keys. It is possible to both lock and unlock the door remotely through Z-Wave.
- **Power Strip**
  Shows an extension block implementation to turn on a number of devices that are connected to power. Examples include lights, appliances, etc.
- **Sensor PIR**
  Shows a presence/movement detector implementation for controlling other devices and for sending notifications.
- **Switch On/Off**
  Shows a switch implementation to turn on any device that is connected to power. Examples include lights, appliances, etc.
- **Wall Controller**
  Shows a push button switch panel implementation to control devices in the Z-Wave network from push buttons (physical or virtual) on a device that is meant to be mounted on a wall. Examples include scene and zone controller, wall mounted AV controllers.

All applications are built on the Z-Wave Plus v2 Framework [9].

All Z-Wave certified applications can be operated in any Z-Wave network with other Z-Wave certified devices from other manufacturers. All mains operated nodes within the network will act as repeaters regardless of vendor to increase reliability of the network.

Refer to Table 1 for an overview of the functionality covered by the applications.

Table 1. Functionality Covered by the Z-Wave Plus v2 Applications

Functionality	Door Lock	Power Strip	Sensor PIR	Switch On/Off	Wall Controller
Role Type					
Always On Slave		✓		✓	✓
Reporting Sleeping Slave			✓		
Listening Sleeping Slave	✓				
Multi channel					
Endpoints		✓			
Security					
S2 Access	✓				
S2 Authenticated		✓	✓	✓	✓
S2 Unauthenticated		✓	✓	✓	✓
S0	✓	✓		✓	✓
Main functionality					
Binary Switch		✓		✓	
Central Scene					✓
Door Lock	✓				
Firmware Update	✓	✓	✓	✓	✓
Multilevel Switch		✓			
Notification		✓	✓		
User Code	✓				

5.1.1 General User Interface

The following user interface applies to all the Z-Wave Plus v2 certified applications.

Table 2: General User Interface

Button/LED	Action	Description
RST	Press	Resets the firmware of an application (like losing power). All volatile memory will be cleared.
BTN1	Press	Enter learn mode (sending node info frame) to add/remove the device. Removing the device from a network will reset it.
	Hold for at least 5 seconds and release	Perform a reset to factory default operation of device and a Device Reset Locally Notification Command is sent via Lifeline.
LED1	n/a	Blinks with 1 Hz, when learn mode is active. Used for Indicator Command Class

5.1.2 SmartStart

SmartStart enabled products can be added into a Z-Wave network by scanning the Z-Wave QR Code present on the product with a controller providing SmartStart inclusion. No further action is required and the SmartStart product will be added automatically within 10 minutes of being switched on in the network vicinity. The Z-Wave certified applications are not labeled with a QR Code. However, QR Code are generated internally in the 700 SoC and can be retrieved via Simplicity Studio. Right click on your connected hardware in the 'Debug Adapters' section in Simplicity Studio. Then right-click and select 'Device Configuration'. From this menu, select 'Z-Wave Device Settings'.

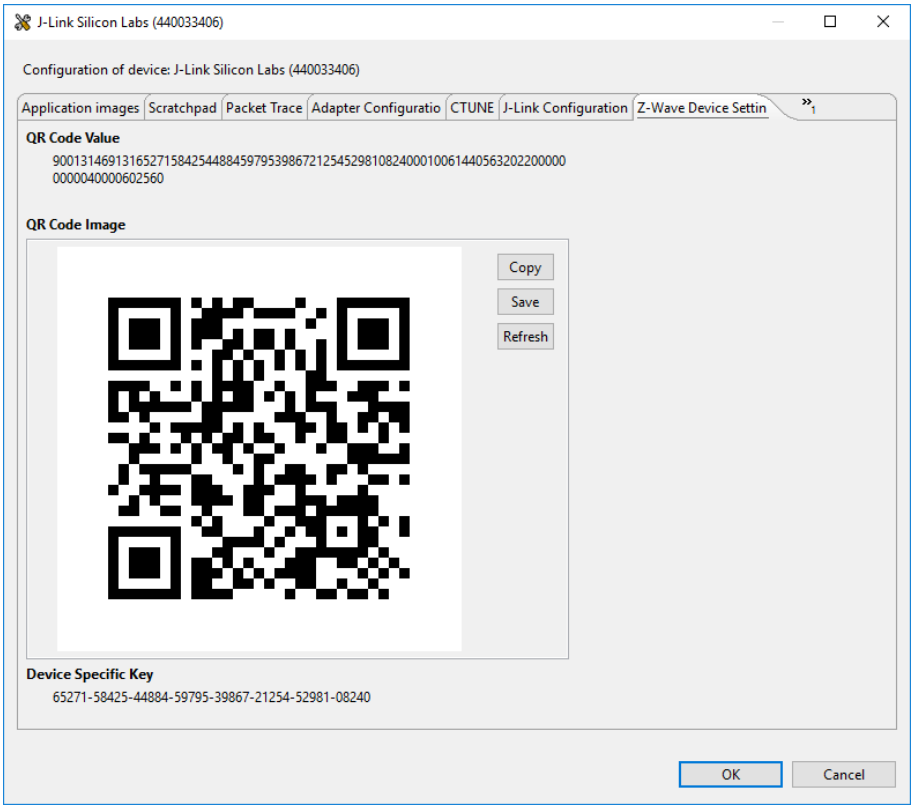


Figure 7. QR Code image and value.

In this view the entire QR Code Value and the corresponding QR Code Image is shown. In addition, the Device Specific Key (DSK) is shown.

This DSK can be compared against the Z-Ware UI, PC Controller dialog box or other Controller UI. If needed, the first decimal group of the DSK can be typed in for S2 secure inclusion.

5.2 Door Lock

The Z-Wave certified Door Lock application shows a lock implementation. It will support user codes to open a door and thereby eliminate the need for traditional keys. It is possible to both lock and unlock the door remotely through the Z-Wave protocol.

The Door Lock application is based on:

- Role Type: Listening Sleeping Slave (LSS / FLiRS)
- Supporting Device Type: Actuator
- Device Type: Lock
- Generic Type: Entry Control
- Specific Type: Door Lock
- Requested security keys: S0 and S2_ACCESS
  The Door Lock features depends on the security level.

The full set of features only work when securely added to a network by a controller supporting security.

Graphical representation (Icon Types):

Not implemented Door lock functionality:

- Timed Operation mode
- Door Lock condition
- Inside Door Handle State
- Functionality handling Lock timeout
- Target mode
- Auto-Relock, Hold And Release, Block to Block, and Twist Assist

5.2.1 Supported Command Classes

The Door Lock application implements mandatory and some optional command classes. The table below lists the supported Command Classes, their version, and their required Security class if any.

Table 3. Door Lock Supported Command Classes

Command Class	Version	Required Security Class
Association	2	S0 or Access Control
Association Group Info	3	S0 or Access Control
Basic	2	S0 or Access Control
Battery	1	S0 or Access Control
Device Reset Locally	1	S0 or Access Control
Door Lock	4	S0 or Access Control
Firmware Update Meta Data	5	S0 or Access Control
Indicator	3	S0 or Access Control
Manufacture Specific	2	S0 or Access Control
Multi Channel Association	3	S0 or Access Control
Powerlevel	1	S0 or Access Control
Security 0	1	None
Security 2	1	None
Supervision	1	None
Transport Service	2	None
User Code	1	S0 or Access Control
Version	3	S0 or Access Control
Z-Wave Plus Info	2	None

5.2.2 Basic Command Class Mapping

The Basic Command Class is mapped according to Table 4.

Table 4: Basic Command Class mapping for Door Lock

Basic Command	Mapped Command
Basic Set (Value)	Door Lock Operation Set (Door Lock Mode)
Basic Report (Current Value, Target Value, Duration)	Door Lock Operation Report (Current Value, Target Value, Duration)

5.2.3 Association Groups

Table 5 shows the available association groups including supported command classes.

Table 5: Association Groups Available in Door Lock

ID	Name	Node count	Description
1	Lifeline	5	Supports the following command classes: • Device Reset Locally: triggered upon reset. • Battery: Triggered upon low battery. • Door Lock: Triggered upon a change in door lock configuration. • Door Lock: Triggered upon a change in door lock operation. • Indicator Report: Triggered when LED1 changes state. • User Code: Triggered upon a user code record is modified.

5.2.4 Usage of Buttons and LED Status

Besides the general functionality described in Table 2, the following buttons and LEDs are used. Refer to Table 6 and Table 7 for details.

Table 6. Door Lock Buttons Interface

Button	Action	Description
BTN0	Button up/down	If the outside door handle state is active: Button down sets the outside door handle mode active. Button up sets the outside door handle mode inactive.
BTN2	Button press	Sends Battery Report.
BTN3	Button press	Simulates entering a user code on a key pad. The entered user code is hard-coded with the value of the default user code of the application. The default user code is 1234. A valid user code entry (i.e. button press) toggles the Door Lock Mode between Secured and Unsecured. If the user code for user ID 1 is changed to something else than the default user code, the Door Lock Mode can no longer be toggled by pressing this button.

Table 7. Door Lock LED Status Interface

LED	Description		
LED0	Latch:	Led on -> latch open [bit 0]	Led off -> latch closed [bit 1]
LED3	Bolt:	Led on -> bolt locked [bit 0]	Led off -> bolt unlocked [bit 1]

5.2.5 Firmware Update

This section will describe backward compatibility when upgrading the Door Lock application from one SDK to a newer version.

SDK 7.1x is the first SDK running on Z-Wave 700.

5.2.6 Z-Wave Certification

The Door Lock passes certification with certification number **ZC12-19030005**.

5.3 Power Strip

The Z-Wave certified Power Strip application shows an extension block implementation used to turn on several devices that are connected to power. Examples include lights, appliances, etc.

The Power Strip Z-Wave certified application implements several endpoints, which can be controlled individually.

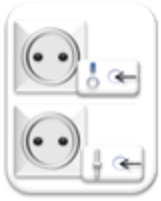
The Power Strip application is based on:

- Role Type: Always On Slave (AOS)
- Supporting Device Type: Actuator
- Device Type: Binary Switch
- Generic Type: Switch Binary
- Specific Type: Not Used
- Requested security keys: S0, S2_UNAUTHENTICATED and S2_AUTHENTICATED

- Endpoint 1 Device Type: Binary Switch
- Endpoint 1 Generic Type: Switch Binary
- Endpoint 1 Specific Type: Not Used

- Endpoint 2 Device Type: Multilevel Switch
- Endpoint 2 Generic Type: Switch Multilevel
- Endpoint 2 Specific Type: Not Used

Graphical representation (Icon Types):



Power Strip supports the “push mode” only of Notification CC and transmits the following notification types/events:

- Power Management
  - Overload detected (both endpoint 1 and 2)

5.3.1 Supported Command Classes

The Power Strip application implements mandatory and some optional command classes. The table below list the supported command classes, their version, and their required Security class if any.

Table 8. Power Strip Supported Command Classes

Command Class	Version	Required Security Class
Association	2	Highest Granted Security Class
Association Group Info	3	Highest Granted Security Class
Basic	2	Highest Granted Security Class
Device Reset Locally	1	Highest Granted Security Class
Firmware Update Meta Data	5	Highest Granted Security Class
Indicator	3	Highest Granted Security Class
Manufacture Specific	2	Highest Granted Security Class
Multi Channel	4	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 0	1	None
Security 2	1	None
Supervision	1	None
Switch Binary	2	Highest Granted Security Class
Transport Service	2	None
Version	3	Highest Granted Security Class
Z-Wave Plus Info	2	None

5.3.1.1 Supported Command Classes: Endpoint 1

Endpoint 1 implements the following command classes.

Table 9: Power Strip, Endpoint 1, Supported Command Classes

Command Class	Version	Required Security Class
Association	2	Highest Granted Security Class
Association Group Info	3	Highest Granted Security Class
Basic	2	Highest Granted Security Class
Multi Channel Association	3	Highest Granted Security Class
Notification	8	Highest Granted Security Class
Security 0	1	None
Security 2	1	None
Supervision	1	None
Switch Binary	2	Highest Granted Security Class
Z-Wave Plus Info	2	None

5.3.1.2 Supported Command Classes: Endpoint 2

Endpoint 2 implements the following command classes.

Table 10: Power Strip, Endpoint 2, Supported Command Classes

Command Class	Version	Required Security Class
Association	2	Highest Granted Security Class
Association Group Info	3	Highest Granted Security Class
Basic	2	Highest Granted Security Class
Multi Channel Association	3	Highest Granted Security Class
Notification	8	Highest Granted Security Class
Security 0	1	None
Security 2	1	None
Supervision	1	None
Switch Multilevel	2	Highest Granted Security Class
Z-Wave Plus Info	2	None

5.3.2 Basic Command Class mapping

The Basic Command Class is mapped according to Table 11.

Table 11: Basic Command Class mapping for Power Strip

Endpoint	Basic Command	Mapped Command
1	Basic Set (Value)	Binary Switch Set (Value)
	Basic Report (Current Value, Duration)	Binary Switch Report (Value, Duration)
2	Basic Set (Value)	Multilevel Switch Set (Value)
	Basic Report (Current Value, Duration)	Multilevel Switch Report (Value, Duration)

5.3.3 Association Groups

Table 12, Table 13, and Table 14 show the available association groups.

Backwards compatibility for non-Multi Channel devices forces the root device AGI table to contain all the association groups mentioned in each of the endpoints AGI tables except from group 1, the Lifeline group.

Association groups for Root Device:

Table 12: Association Groups Available in Power Strip: Root Device

ID	Name	Node count	Description
1	Lifeline	5	Supports the following command classes: • Device Reset Locally: triggered upon reset. • Notification: triggered by the endpoints • Indicator Report: Triggered when LED1 changes state.
2	alarm EP 1	5	Mirror of endpoint 1, group 2
3	alarm EP 2	5	Mirror of endpoint 2, group 2

Association groups for Endpoint 1:

Table 13: Association Groups Available in Power Strip: Endpoint 1

ID	Name	Node count	Description
1	Lifeline	0	Mirror of root device, but without node count.
2	alarm EP 1	5	Notification report on overload.

Association groups for Endpoint 2:

Table 14: Association Groups Available in Power Strip: Endpoint 2

ID	Name	Node count	Description
1	Lifeline	0	Mirror of root device, but without node count.
2	alarm EP 2	5	Notification report on overload.

5.3.4 Usage of Buttons and LED Status

Besides the general functionality described in Table 2, the following buttons and LEDs are used. For details, refer to Table 15 and Table 16.

Table 15. Power Strip Buttons Interface

Button	Action	Description
BTN0	Key press	Switch on/off endpoint 1
BTN2	Key press	Dimming or switch on/off endpoint 2. Pressing push button turn light on/off and holding push button perform dimming of light (toggle up/down)
BTN3	Key press	Toggles the transmission of an “Overload detected” notification. The first transmission, when enabled, will always be the first in the following list. The notifications will be transmitted in the following pattern: 1. Notification from endpoint 1: Overload detected 2. Notification from endpoint 1: No event 3. Notification from endpoint 2: Overload detected 4. Notification from endpoint 2: No event One notification will be transmitted every 30 second.

Table 16. Power Strip LED Status Interface

LED	Description
LED0	Endpoint 1 (switch on/off)
RGB (on module)	Endpoint 2 (dimmer)

5.3.5 Firmware Update

This section will describe backward compatibility when upgrading the Power Strip application from one SDK to a newer version.

SDK 7.1x is the first SDK running on Z-Wave 700.

5.3.6 Z-Wave Certification

The Power Strip passes certification with certification number **ZC12-19030003**.

5.4 Sensor PIR

The Z-Wave certified Sensor PIR application shows a presence/movement detector implementation for controlling other devices and for sending notifications.

The Sensor PIR application is based on:

- Role Type: Reporting Sleeping Slave (RSS)
- Supporting Device Type: Data reporting
- Device Type: Notification sensor
- Generic Type: Sensor Notification
- Specific Type: Notification Sensor
- Requested security keys: S2_UNAUTHENTICATED and S2_AUTHENTICATED

Graphical representation (Icon Types):

Sensor PIR transmits the following notification types/events:

- Home Security
  - Motion detection (unknown location)

Sensor PIR supports the “push mode” only of Notification CC.

5.4.1 Supported Command Classes

Sensor PIR implements mandatory and some optional command classes. The table below lists the supported Command Classes, their version, and their required Security class if any.

Table 17. Sensor PIR Supported Command Classes

Command Class	Version	Required Security Class
Association	2	Highest granted Security Class
Association Group Info	3	Highest granted Security Class
Battery	1	Highest granted Security Class
Device Reset Locally	1	Highest granted Security Class
Firmware Update Meta Data	5	Highest granted Security Class
Indicator	3	Highest granted Security Class
Manufacture 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
Wake Up	2	Highest granted Security Class
Z-Wave Plus Info	2	None

5.4.2 Basic Command Class Mapping

Basic Command Class is not mapped to any of the supported command classes.

5.4.3 Association Groups

Table 18 shows the available association groups.

Table 18: Association Groups Available in Sensor PIR

ID	Name	Node count	Description
1	Lifeline	5	Supports the following command classes: • Device Reset Locally: triggered upon reset. • Battery: triggered upon low battery. • Notification: triggered upon a movement detection (simulated by button BTN2). After a while, a cancel notification will be issued. • Indicator Report: Triggered when LED1 changes state.
2	Basic Set	1	Upon a movement detection (simulated by button BTN2), nodes associated in this group will first receive a Basic Set with 0xFF (turn on) and after a while receive a Basic Set with 0x00 (turn off).

5.4.4 Usage of Buttons and LED Status

Besides the general functionality described in Table 2, the following buttons shown in Table 19 are also used. No LEDs are used.

Table 19. Sensor PIR Buttons Interface

Button	Action	Description
BTN0	Hold for at least 1 second and release	Sends Battery Report (only if device is not sleeping)
BTN2	Hold for at least 1 second and release	Simulates a “Motion detected”.
Hw-reset	”reset”	Sends Wake Up Notification.

5.4.5 Firmware Update

This section will describe backward compatibility when upgrading the Sensor PIR application from one SDK to a newer version.

SDK 7.1x is the first SDK running on Z-Wave 700.

5.4.6 Z-Wave Certification

Sensor PIR passes certification with certification number **ZC12-19030002**.

5.5 Switch On/Off

The Z-Wave certified Switch On/Off application shows a switch implementation which turns on any device that is connected to power. Examples include lights, appliances, etc.

The Switch On/Off application is based on:

- Role Type: Always On Slave (AOS)
- Supporting Device Type: Actuator
- Device Type: Binary Switch
- Generic Type: Switch Binary
- Specific Type: Not Used
- Requested security keys: S0, S2_UNAUTHENTICATED and S2_AUTHENTICATED
  The Switch On/Off features do not depend on the security level.

Graphical representation (Icon Types):

5.5.1 Supported Command Classes

The Switch On/Off application implements mandatory and some optional command classes. The table below lists the supported Command Classes, their version, and their required Security class.

Table 20. Switch On/Off Supported Command Classes

Command Class	Version	Required Security Class
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
Device Reset Locally	1	Highest granted Security Class
Firmware Update Meta Data	5	Highest granted Security Class
Indicator	3	Highest granted Security Class
Manufacture Specific	2	Highest Granted Security Class
Multi Channel Association	3	Highest granted Security Class
Powerlevel	1	Highest granted Security Class
Security 0	1	None
Security 2	1	None
Supervision	1	None
Transport Service	2	None
Version	3	Highest granted Security Class
Z-Wave Plus Info	2	None

5.5.2 Basic Command Class mapping

The Basic Command Class is mapped according to Table 21.

Table 21: Basic Command Class Mapping for Switch On / Off

Basic Command	Mapped Command
Basic Set (Value)	Binary Switch Set (Value)
Basic Report (Current Value, Duration)	Binary Switch Report (Value, Duration)

5.5.3 Association Groups

The following association groups shown in Table 22 are available.

Table 22: Association Groups Available in Switch On / Off

ID	Name	Node count	Description
1	Lifeline	5	Supports the following command classes: • Device Reset Locally: triggered upon reset. • Binary Switch Report: Triggered when switch changes state. • Indicator Report: Triggered when LED1 changes state.

5.5.4 Usage of Buttons and LED Status

Besides the general functionality described in Table 2, the following buttons shown in Table 23 and Table 24 are also used.

Table 23. Switch On / Off Buttons Interface

Button	Action	Description
BTN0	Press	Toggle LED0

Table 24. Switch On / Off LED Status Interface

LED	Description
LED0	Switch: LED ON indicates SWITCH ON / LED OFF indicates SWITCH OFF.

5.5.5 Firmware Update

This section will describe backward compatibility when upgrading the Switch On/Off application from one SDK to a newer version.

SDK 7.1x is the first SDK running on Z-Wave 700.

5.5.6 Z-Wave Certification

The On/Off Switch passes certification with certification number **ZC12-19030001**.

5.6 Wall Controller

The Z-Wave certified Wall Controller application shows a push button switch panel implementation to control devices in the Z-Wave network from push buttons (physical or virtual) on a device that is meant to be mounted on a wall. Examples include scene and zone controller, wall mounted AV controllers.

The Wall controller application implements a wall mounted switch that has three individually configurable buttons. Each button has support for on/off and dimming.

The Wall Controller application is based on:

- Role Type: Always On Slave (AOS)
- Supporting Device Type: Actuator
- Device Type: Central Scene
- Generic Type: Wall Controller
- Specific Type: Not Used
- Requested security keys: S0, S2_UNAUTHENTICATED and S2_AUTHENTICATED
  The Wall Controller features do not depend on the security level.

Graphical representation (Icon Types):

5.6.1 Supported Command Classes

Wall Controller implements mandatory and some optional command classes. The table below lists the supported Command Classes, their version, and their required Security class if any.

Table 25. Wall Controller Supported Command Classes

Command Class	Version	Required Security Class
Association	2	Highest granted Security Class
Association Group Info	3	Highest granted Security Class
Central Scene	3	Highest granted Security Class
Device Reset Locally	1	Highest granted Security Class
Firmware Update Meta Data	5	Highest granted Security Class
Indicator	3	Highest granted Security Class
Manufacture Specific	2	Highest Granted Security Class
Multi Channel Association	3	Highest granted Security Class
Powerlevel	1	Highest granted Security Class
Security 0	1	None
Security 2	1	None
Supervision	1	None
Transport Service	2	None
Version	3	Highest granted Security Class
Z-Wave Plus Info	2	None

Use case:

Wall controller's tree buttons are configurable to control nodes. Each button action is sent over life-line as scene actions. Current figure shows an example of this:

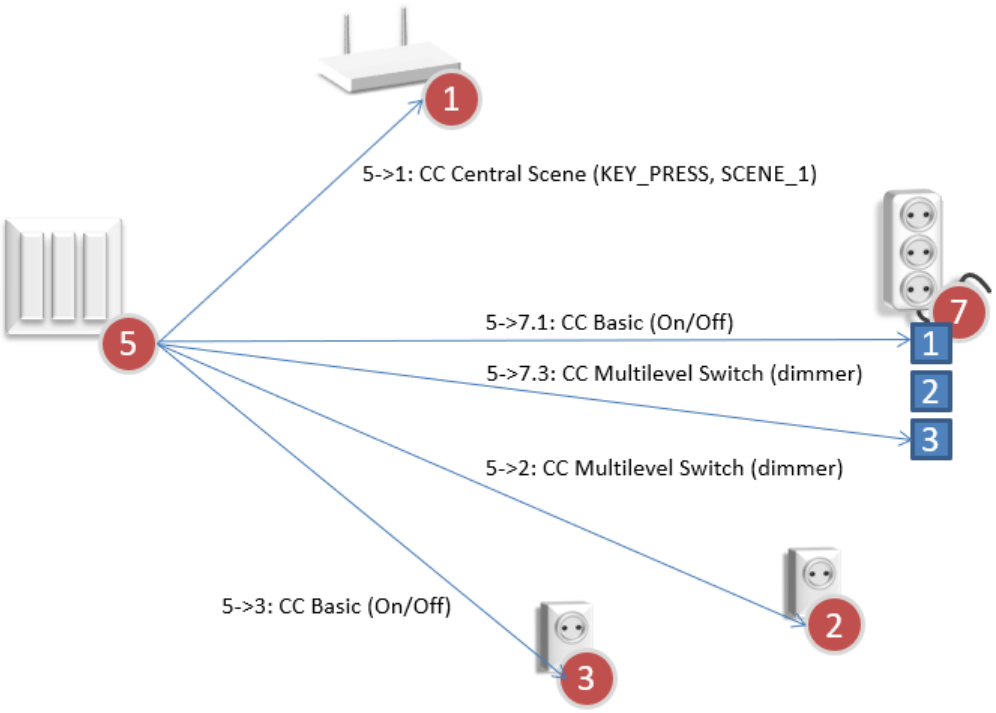


Figure 8. Wall Controller (node 5) example of Central Scene.

5.6.2 Basic Command Class mapping

Basic Command Class is not mapped to any of the supported command classes.

5.6.3 Association Groups

The following association groups shown in Table 26 are available.

Table 26: Association Groups Available in Wall Controller

ID	Name	Node count	Description
1	Lifeline	5	Supports the following command classes: • Device Reset Locally: triggered upon reset. • Central Scene: triggered by button press. • Indicator Report: Triggered when LED1 changes state.
2	BTN0	5	Basic Set Command
3	BTN0	5	Switch Multilevel CC
4	BTN2	5	Basic Set Command
5	BTN2	5	Switch Multilevel CC
6	BTN3	5	Basic Set Command
7	BTN3	5	Switch Multilevel CC

5.6.4 Usage of buttons and LED Status

Besides the general functionality described in Table 2, the following buttons shown in Table 27 are also used.

No LEDs are used.

Table 27. Wall Controller Buttons Interface

Button	Action	Description
BTN0 Button on Wall Controller: 1	Press	• Lifeline with Central Scene Key Attribute “Key Pressed 1 Time” • Trigger association group 2: Basic Set
	Hold start	• Lifeline with Central Scene Key Attribute “Key Held Down” • Trigger association group 3: Multilevel Switch Start Level Change
	Hold release	• Lifeline with Central Scene Key Attribute “Key Held Down” • Trigger association group 3: Multilevel Switch Stop Level Change
BTN2 Button on Wall Controller: 2	Press	• Lifeline with Central Scene Key Attribute “Key Pressed 1 Time” • Trigger association group 4: Basic Set
	Hold start	• Lifeline with Central Scene Key Attribute “Key Held Down” • Trigger association group 5: Multilevel Switch Start Level Change
	Hold release	• Lifeline with Central Scene Key Attribute “Key Held Down” • Trigger association group 5: Multilevel Switch Stop Level Change
BTN3 Button on Wall Controller: 3	Press	• Lifeline with Central Scene Key Attribute “Key Pressed 1 Time” • Trigger association group 6: Basic Set
	Hold start	• Lifeline with Central Scene Key Attribute “Key Held Down” • Trigger association group 7: Multilevel Switch Start Level Change
	Hold release	• Lifeline with Central Scene Key Attribute “Key Held Down” • Trigger association group 7: Multilevel Switch Stop Level Change

5.6.5 Firmware update

This section will describe backward compatibility when upgrading the Wall Controller application from one SDK to a newer version.

SDK 7.1x is the first SDK running on Z-Wave 700.

5.6.6 Z-Wave Certification

The Wall Controller passes certification with certification number **ZC12-19030004**.

REFERENCES

[1] Silabs, SDS13781, Software Design Specification, Z-Wave Application Command Class Specification.
[2] Silabs, SDS13782, Software Design Specification, Z-Wave Management Command Class Specification.
[3] Silabs, SDS13783, Software Design Specification, Z-Wave Transport-Encapsulation Command Class Specification.
[4] Silabs, SDS13784, Software Design Specification, Z-Wave Network-Protocol Command Class Specification.
[5] Silabs, SDS13548, Software Design Specification, List of defined Z-Wave Command Classes.
[6] Silabs, SDS11846, Software Design Specification, Z-Wave Plus Role Type Specification.
[7] Silabs, SDS14223, Software Design Specification, Z-Wave Command Class Control Specification.
[8] Silabs, SDS14224, Software Design Specification, Z-Wave Plus v2 Device Types Specification.
[9] Silabs, INS14259, Instruction, Application Framework Z-Wave Plus V2 SDK7.
[10] Silabs, INS14280, Instruction, Z-Wave 700 Getting Started for End Devices.