Software Release Note

Z-Wave 500 Series SDK v6.82.01

Document No.:	SRN14615
Version:	6
Description:	-
Written By:	JFR;COLSEN;PSH
Date:	2020-04-23
Reviewed By:	NTJ;ABXAVIER;SCBROWNI;PSH
Restrictions:	None

Approved by:

Date	CET	Initials	Name	Justification
2020-04-23	10:54:43	JFR	Jorgen Franck	on behalf of NTJ

REVISION RECORD

Doc. Rev	Date	By	Pages affected	Brief description of changes
1	20190927	JFR	Section 1, 2 & 4	Initial draft based on SRN13926-11 – Z-Wave 500 Series SDK v6.81.06
2	20200312	JFR	Section 1, 2 & 4	Updated to SDK v6.82.1 release
3	20200404	JFR	Section 8 & 9	Added Product Life Cycle and Certification
4	20200414	JFR	Section 2	Bumped Z-Wave Protocol and Serial API Applications version to 6.09.00
5	20200421	SCBROWNI	All	Review
6	20200423	JFR	All	Minor typos

Table of Contents

List of Figures

List of Tables

1 INTRODUCTION

This chapter introduces the SDK as well as Z-Wave technology.

1.1 Introduction to the SDK

The Z-Wave 500 Series Software Development Kit (SDK) is intended to help developers create Z-Wave Plus compliant products in a fast and cost-effective manner. The software consists of Z-Wave libraries supporting controller/slave devices and a Z-Wave Plus Application Framework, as well as code for a broad range of home automation applications. For specific applications, it is probably easier to modify an existing sample app instead of using the MyProduct app as a starting point.

The Z-Wave 500 Series SDK version 6.82.01 is a mature release enabling support of Smart Start, etc. This patch release contains bug fixes compared to the Z-Wave 700 SDK v6.82.00. This release is intended for Z-Wave certified 500 Series based products entering volume production. All Z-Wave Plus Applications are Z-Wave certified. For details regarding functionality, refer to Chapters 3 and 4. Finally, refer to [11] for a detailed description of contents.

Note: Be aware that Z-Wave SDK 6.8x.xx requires Keil PK51 v9.54A.

1.1 Abbreviations

Abbreviation	Explanation
ACK	Acknowledge
API	Application Programming Interface
C	Command
CC	Command Class
CSA	Client-Side Authentication
DUT	Device Under Test
ID	Identifier
FLiRS	Frequently Listening Routing Slave. Communication to a FLiRS node can be established by a wakeup beam
NIF	Node Information Frame
NWI	Network Wide Inclusion (add node out of direct range)
NWE	Network Wide Exclusion (remove node out of direct range)
OTA	Over The Air (e.g., making a firmware update wireless)
OTW	Over The Wire (e.g., making a firmware update via the serial API interface)
S0	Security 0 Command Class
S2	Security 2 Command Class
SDK	Software Development Kit
SSA	Server-Side Authentication
TO	Test Observation (bug)

1.2 Introduction to Z-Wave Technology

Z-Wave is a wireless mesh protocol oriented towards the residential control and automation market, but it may also be used in light commercial environments. The technology provides a simple yet reliable method of wirelessly controlling lights and A/V equipment in homes. Z-Wave works in the unlicensed industrial, scientific, and medical (ISM) bands around 900 MHz (regional frequencies vary slightly). Each Z-Wave network can comprise up to 232 nodes. Nodes can retransmit messages in order to guarantee delivery. The typical communication range between two nodes is 100 feet.

The Z-Wave ecosystem offers a routing protocol stack and a complete Z-Wave Plus Application Framework of device types and command classes for interoperable deployments. Interoperability is ensured between all device types thanks to the Z-Wave certification program. The Z-Wave logo is only granted to products passing certification.

1.2.1 Protocol Stack Overview

Z-Wave offers a routing protocol that reliably transfers messages up to five hops away, i.e., up to 500 feet. The protocol stack consists of a PHY/MAC layer to control access to RF media, a transport layer to handle frame integrity and retransmissions, and a network layer with all its routing magic and application interfaces.

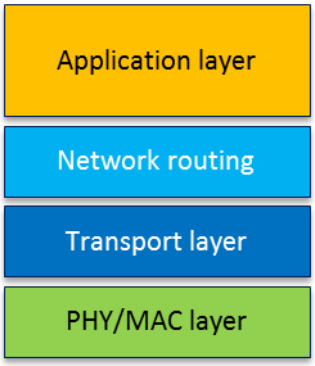

Figure 1. Z-Wave Protocol Stack

The maximum size of payload data is 46 bytes when routing is used. The Z-Wave protocol uses standard collision-avoidance methods—postponing a transmission a random number of milliseconds when media is busy. The Z-Wave transport layer controls the transfer of data between two nodes including acknowledgement and optional retransmission.

Multicast and broadcast may only be used in direct range. Broadcast and multicast may be used to reach more than one destination address. In the case of multicast, the same payload will be delivered to selected nodes only.

The Z-Wave application layer is responsible for handling application commands. Commands are divided into two classes: Z-Wave protocol and application-specific. Most protocol-related operations are just address assignment logic, but commands that are more complex are defined for advanced network management operations.

Each Z-Wave network has a unique 32-bit identifier called the Home ID. Every new node joining the network inherits the same Home ID from the primary controller. Individual nodes in the network are addressed using an 8-bit Node ID that is unique within the network.

1.2.2 Classic Z-Wave

The following text refers to classic nodes. Basically, the term “Classic Z-Wave node” describes previous generations of Z-Wave nodes that do not implement recently introduced features, such as Network-Wide Inclusion (NWI), Dynamic Route Resolution, and FLiRS communication.

1.2.3 Node Types

There are two main types of devices: controllers and slaves. Controllers can handle network management and communication with classic nodes. Slaves provide no network management capability.

1.2.3.1 Controllers

A controller node maintains a routing table for all operational links in the network. This table allows the controller to calculate routes between any two nodes in the network. The primary controller may refresh the routing table and distribute updated routing tables to other controllers.

Controllers come in three variants: portable, static, and bridge.

The portable controller is optimized for battery operation. It is typically used for remote control devices.

The static controller is intended for mains-powered control panels, gateways, or network managers. The static controller may also act as a repeater for other nodes.

1.2.3.2 Slaves

A slave device has simpler functionality than a controller and can be implemented without any external non-volatile storage. It may repeat a message for other nodes.

The WakeUp slave is a special variant that may be used for sensor-style devices, such as alarms and sensors.

Called “duty cycling” in the literature, the Frequently Listening Routing Slave (FLiRS) wakes up at fixed intervals to briefly listen for preamble patterns. This enables the design of products with battery lifetimes that are measured in years. Yet, it is possible to reach such devices on short notice.

WakeUp slaves and FLiRS nodes cannot operate as repeaters since they are sleeping most of the time to conserve battery life.

1.2.4 Network Operation

Management of Z-Wave nodes consists of two main operations: inclusion/exclusion and association. Inclusion adds a new node to the network. Exclusion removes a node. Only primary controllers can include and exclude nodes.

Association is the creation of a logical connection between applications. In other words, it defines what controls what. Association is handled by the application layer.

1.2.5 Routing Principles

Z-Wave uses source routing to reach a destination. Source routing allows the implementation of a lightweight protocol, thereby avoiding distributed routing tables in all repeaters. This limits the length of routes. Real-world deployments indicate that residential networks rarely have more than 2-hop routes. Z-Wave's support for 5-hop routes is sufficient and constitutes an efficient compromise.

The route is carried in the routing header, and every repeater forwards the frame according to the routing header. Only always-listening nodes can participate in routing, but routing may also be used to reach FLiRS nodes.

Network Wide Inclusion (NWI) allows a user to include a new node even though the new node is not within range of the primary controller. Dynamic route resolution allows a node to repair broken routes during normal operation. Classic nodes do not support NWI or dynamic route resolution.

Network Wide Exclusion (NWE) uses the same explorer strategy as Network Wide Inclusion (NWI) to accomplish out-of-range exclusion of nodes from the network. It is also possible to remove a specific node from the network by specifying the Node ID.

1.2.6 Application Development

Depending on node type functionality (e.g., controller vs. slave), developers may choose from a selection of libraries. On top of the chosen library, an application designer may choose from a wide range of Command Classes, including light control, sensors, garage port control, and many others. Command Classes are a collection of functionally related commands. A device may implement several functions and thereby support more Command Classes.

Z-Wave applications are designed to operate like state machines that are periodically polled from the Z-Wave library. This allows for the design of products with fewer CPU resources than are typically required for OSs with threads, tasks, priorities, etc., and this translates into inexpensive products that are well-suited for mass production. Depending on the actual product, an application may interface to the Z-Wave protocol stack in three ways:

1. A constrained device, like a light dimmer with one button, may have its application running in the on-chip 8051 MCU. In this configuration, the Z-Wave API is used directly via function calls provided by the binary image implementing the Z-Wave library.
2. Larger devices, like a remote control with display, may have its own host processor. The application designer may prefer to implement all application logic in the host processor, only running the Z-Wave protocol stack in the on-chip 8051 MCU. The Z Wave Serial API provides an abstracted version of the Z-Wave API that is accessed via an on-chip serial port. The application design principle for the Z-Wave part should still be a state machine that reacts to incoming events, callback functions, and timeouts.
3. Most advanced devices, such as IP gateways and PC-based light control servers, may use an even more abstracted API provided by the Network Management Command Class. In this model, all communication is carried in IP packets. The Z/IP Gateway library provides this mapping.

1.2.7 Managing Interoperability

Interoperability is a key part of the Z-Wave ecosystem. Every product must pass certification before it is allowed to bear the Z-Wave logo. The Z-Wave Alliance manages the Z-Wave certification program, but certification testing is performed by independent test houses. Certification ensures that a product correctly implements all device and command classes that it claims to support.

2 RELEASED VERSIONS

2.1 SDK 6.82.01

```
Z-Wave Framework and Certified Applications.................. v4_04_01
Z-Wave Protocol and Serial API Applications.................. v6_09_00
Z-Wave Serial API Application Interface.......................... v8

Tools
=====
IMA Tool..................................................... v0_99
NVM Converter................................................ v0_07
uVision Project Generator.................................... v1_16
```

3 OVERVIEW

The Z-Wave 500 Series SDK version 6.8x contains the following major enhancements compared to SDK version 6.7x:

- Smart Start
- FLiRS multicast
- Improved power management
- Improved Application Framework

4 DETAILED DESCRIPTION

4.1 Bug fixes (SDK 6.82.01+)

This release contains bug fixes; refer to [26] for details.

4.2 Bug fixes (SDK 6.82.00+)

This release contains bug fixes and documentation improvements.

4.3 Bug fixes (SDK 6.81.06+)

This release contains bug fixes and documentation improvements.

4.4 Recertified Apps (SDK 6.81.05+)

The five apps (Door Lock Key pad, Sensor PIR, Switch On/Off, Power Strip, and Wall Controller) have been recertified to ensure full compliance.

Notice: Certification does not include Z-Wave Plus v2 requirements.

4.5 NVM Converter (SDK 6.81.05+)

The NVM Converter Tool converts the NVM-based protocol data for a given Z-Wave network to a newer SDK version. Typically, it is used when upgrading a Gateway using a bridge-controller-based serial API to a newer SDK version to avoid reinstallation of the Z-Wave network. From SDK 6.51.00+ the conversion process is performed automatically during an OTA/OTW firmware update.

4.6 Bug Fixes (SDK 6.81.00-5+)

This release contains bug fixes and documentation improvements.

4.7 Smart Start (SDK 6.80.00+)

Z-Wave SmartStart aims to shift the tasks associated with the inclusion of an end device into a Z-Wave network away from the end device itself and towards the more user-friendly interface of the gateway.

Z-Wave SmartStart removes the need for initiating the end device to start inclusion. Inclusion is initiated automatically upon power-ON and is repeated at dynamic intervals for as long as the device is not included in a Z-Wave network. As the new device announces itself upon power-ON, the protocol

will provide notifications, and the gateway can initiate the inclusion process in the background without the need for user interaction or any interruption of normal operation. This improvement also removes the possibility of other devices being included, since the SmartStart inclusion process only includes authenticated devices.

By moving the device authentication process into the manufacturing and distribution phase or service provider domain, the end user is no longer required to do anything more than power on the device. This enables a simplified user experience in which the device is genuinely ready to use, right out of the box. The device manufacturer or service provider can now prepare inclusion prior to the devices ending up at the end user's house.

Building on the elements introduced by S2 security, the Z-Wave SmartStart is not only easy for the end user, but also secure. Z-Wave SmartStart uses the same device-specific keys (DSK) that form the foundation of the secure inclusion process of S2. Only authorized and intended devices are included in the Z-Wave network. Z-Wave SmartStart is based on the embedded SDK 6.8x and related gateway software components.

Smart start introduces several new APIs for using Learn mode and adding nodes to the network. For end nodes, the ZW_NetworkLearnModeStart() is now used to control learn mode, and for controller nodes, ZW_AddNodeToNetwork() is used. For details about the API see [3].

4.8 Smart Start and S2 QR Code Generation (SDK 6.80.00+)

Z-Wave devices supporting the Security 2 (S2) Command Class or Smart Start provisioning must provide a QR code physically on the device and the packaging. The actual marking and layout requirements are documented in [16], while the data string encoded in the QR code is specified in [24].

To facilitate on-the-fly generation of QR codes and S2 DSK to match the S2 Key pairs programmed into S2 and Smart Start devices, [25] defines a Production Control File that a device developer may hand over to the production facility doing the actual firmware programming, S2 key programming, and QR code printing. The Production Control File defines the labels to be printed and the data to go into the QR code.

The current SDK release contains two software utilities to assist developers in creating the control file and verifying the contents of a QR code:

- QrCodeEncoder.xlsm
    - Encoding of QR code fields
    - Single-sample generation of QR codes for prototyping
    - Generation of dynamic string for Production Control File with fields to be replaced during production
- QrCodeDecoder.xlsm
    - Decodes the string contained in a QR code using an arbitrary smart phone QR code scanner application

All gray fields should be left untouched.

The encoder automatically generates a production control file named "ZwSmartStart.csv file" in the same folder as the QrCodeEncoder file.

The utilities are implemented using Excel sheets, incorporating several macro functions for SHA-1 checksum calculation, QR code rendering, and control file generation. Therefore, utilities must be stored in a folder that is not write-protected.

4.9 FLiRS Multicast (SDK 6.80.00+)

Controllers can now send multicast to FLiRS nodes, so that they react simultaneously to a command if they are in range of the controller.

The FLiRS multicast is based on a special destination address, so nodes that are not a part of a FLiRS multicast group will not wake up when a FLiRS multicast frame is send. This functionality is based on a learning process in the FLiRS node that works in the following way:

1' transmission to a FLiRS multicast group:

1 Controller sends FLiRS multicast frame.
2 All FLiRS nodes ignore the frame.
3 Controller sends follow-up singlecast frame to all the FLiRS nodes in the group.
4 FLiRS nodes receive the follow-up singlecast; enable the FLiRS multicast address, and pass the frame to the application.

2' transmission to a FLiRS multicast group:

1 Controller sends FLiRS multicast frame.
2 All FLiRS nodes in the multicast group wake up, receive the frame, and pass it to the application.
3 Controller sends follow-up singlecast frame to all the FLiRS nodes in the group.
4 FLiRS nodes receive the follow-up singlecast and pass the frame to the application.

4.10 Improved Z-Wave Plus Framework (SDK 6.80.00+)

The Z-Wave Plus Application Framework is also improved in several places resulting in a simpler application development [19].

4.11 Improved Power Management (SDK 6.80.00+)

Power management is changed for better synchronization between application and protocol. The length of time battery powered nodes run at full power has been reduced considerably. For details about the new power management functionality, see the Z-Wave framework guide [19] and the function ZW_Power_Management_Init() in [3].

4.12 Command Class Version Version 3 (SDK 6.80.00+)

Version 3 of the Version Command class is now supported by the application.

4.13 MY Frequency Obsoleted (SDK 6.80.00+)

All the MY frequency targets have been obsoleted. Use ANZ frequency instead of MY frequency in Malaysia.

4.14 New Variants of MyProductPlus Application (SDK 6.80.00+)

Two sensor type variants have been added to the MyProductPlus application enabling support of battery-operated devices. The new battery-operated devices are as follows:

- Battery device supporting Command Class Battery
- Battery device supporting Command Class Battery and Command Class Wake Up.

4.15 Serial API Communication Interface Version (SDK 6.80.00+)

In SDK 6.80.0x, the Serial API communication interface was changed to Version 8, enabling host software to check that this version of the serial API supports Smart Start.

4.16 Intermediate Applications Removed (SDK 6.80.00+)

The intermediate applications are now available in SDK 6.61.01+.

4.17 Support for NVM Ultra-Deep Sleep (SDK 6.80.00+)

Z-Wave modules using Adesto AT45DBxxxE chips as external NVM can now use the ultra-deep sleep mode in sleep mode. Regarding a full list of recommended EEPROM/FLASH components as external NVM, refer to [20].

5 Z-WAVE PROTOCOL

The Z-Wave Protocol (Z-Wave API library) is a low-bandwidth, half-duplex protocol designed for reliable and robust wireless communication in low-cost control mesh networks. This version supports the 500 Series single chips in various configurations. For an overview, refer to [1], and, for a detailed description of the API calls, refer to [3]. The API consists of five different libraries: a Portable Controller library, a Static Controller library, a Bridge Controller library, a Routing Slave library, and an Enhanced 232 Slave library. The type of library used depends on the application features needed.

5.1 New Features

Refer to Chapters 3 and 4.

6 Z-WAVE FRAMEWORK AND EMBEDDED APPLICATIONS

The SDK contains code as well as compiled code for Z-Wave Plus embedded applications according to devices in [15]-[16] and command classes in [6]-[9]. The Z-Wave Plus embedded applications support both non-secure and secure S0/S2 in one target.

Associations must be configured to examine all the features in the Z-Wave Plus embedded applications. Setting up associations is fully supported by the Z-Wave PC-based Controller v5 and not older versions of the Z-Wave PC-based Controller.

The code can be used as-is to become familiar with Z-Wave, or it can be changed according to the needs of the application programmer.

A Z-Wave application based on earlier Z-Wave Single Chips requires porting of the source code to the 500 Series Single Chip. For details about porting, refer to [13], [14] and [3].

A Z-Wave Plus application based on earlier SDKs may also require porting to a newer version of the Z-Wave Plus Application Framework. For details, refer to [19].

6.1 Z-Wave Plus Application Certification Guidelines

Introduction of the S2 security solution mandates additional requirements to the certification program. A large portion of the S0/S2 security solution resides in the Z-Wave Protocol, but parts are also located in the Z-Wave Plus Application Framework and Z-Wave Plus Applications. The application developer must, therefore, be aware of the 24 command class requirement numbers [8] applicable for slave-based devices during development listed in the following table:

Command Class Requirement Numbers (Slaves)		
CC:009F.01.0E.11.008	CC:009F.01.05.11.018	CC:009F.01.00.11.09A
CC:009F.01.0E.11.003	CC:009F.01.05.11.017	CC:009F.01.00.11.04C
CC:009F.01.0D.11.007	CC:009F.01.00.11.070	CC:009F.01.00.11.034
CC:009F.01.0D.11.004	CC:009F.01.00.11.06E	CC:009F.01.00.21.00B
CC:009F.01.0D.11.003	CC:009F.01.00.11.061	CC:009F.01.00.21.009
CC:009F.01.0A.11.002	CC:009F.01.00.11.05E	CC:009F.01.00.21.008
CC:009F.01.08.11.007	CC:009F.01.00.11.092	CC:009F.01.00.21.007
CC:009F.01.06.11.003	CC:009F.01.00.11.051	CC:009F.01.00.11.050

Depending on the application in question, not all listed requirements may be relevant.

6.2 Door Lock with Key Pad

The Door Lock with Key Pad application shows a lock implementation with a built-in keypad. It supports user codes to open a door and thereby eliminates the need for traditional keys. Typically, it is possible to both lock and unlock the door remotely through the Z-Wave protocol. The Door Lock with Key Pad implementation is built upon the Z-Wave Plus Application Framework [19]. The Door Lock with Key Pad is based on Door Lock Keypad Device Type with Listening Sleeping Slave (LSS) as the Role Type and enhanced 232 slave. For detailed information, refer to [11].

6.3 My Product Plus

As an alternative to the Device Type code applications, use My Product Plus. This application contains the minimum framework for developing a Z-Wave Plus application. The My Product Plus implementation is built upon the Z-Wave Plus Application Framework [19]. For detailed information, refer to [11].

6.4 On/Off Switch

The On/Off Power Switch application shows a switch implementation to turn on any device that is connected to power. Examples include lights, appliances, etc. The On/Off Switch implementation is built upon the Z-Wave Plus Framework [19]. The On/off Switch is based on an On/Off Power Switch Device Type with Always On Slave (AOS) as the Role Type and enhanced 232 slave. For detailed information, refer to [11].

6.5 PIR Sensor

The PIR Sensor application shows a presence/movement detector implementation for controlling other devices and for sending notifications. The PIR Sensor implementation is built upon the Z-Wave Plus Framework [19]. The PIR Sensor is based on Sensor – Notification Device Type with Reporting Sleeping Slave (RSS) as the Role Type and routing slave. For detailed information, refer to [11].

6.6 Power Strip

The Power Strip application shows an extension block implementation to turn on a number of devices that are connected to power. Examples include lights, appliances, etc. The Power Strip implementation is built upon the Z-Wave Plus Framework [19]. The Power Strip is based on a Power Strip Device Type with Always On Slave (AOS) as the Role Type and enhanced 232 slave. The Power Strip application also shows how to implement a Multi-Channel device. For detailed information, refer to [11].

6.7 Production Test DUT

The Production Test DUT code for a device under test contains an example of how the basic tasks of testing devices in a Z-Wave network can be implemented using the Z-Wave API. Detailed information regarding the Production Test DUT code can be found in [11].

6.8 Production Test Generator

The Production Test Generator code contains an example of how the basic tasks of testing devices in a Z-Wave network can be accomplished using the Z-Wave API. The Z-Wave generator is used in conjunction with the Production Test DUT to verify the TX / RX circuits on Z-Wave-enabled products. Detailed information regarding the Production Test Generator code can be found in [11].

6.9 Serial API Plus

The Serial Applications Programming Interface (Serial API) allows a host to communicate with a Z-Wave chip. The host may be a PC or a less powerful embedded host CPU, such as that found in a remote control or a gateway device. This solution is typically used when the whole application cannot reside on the Z-Wave chip itself. The Serial API code contains an example of how to implement a serial UART interface to the Z-Wave protocol. The Serial API supports both controller and slave applications. For detailed information, refer to [11]. In addition, detailed information about the Serial API code and how to interface to the Serial API can be found in [18] and [3].

6.10 Wall Controller

The 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 controllers and wall-mounted AV controllers. Devices of this type can be either battery-operated or mains-powered. The Wall Controller implementation is built upon the Z-Wave Plus Framework [19]. The Power Strip is based on a Wall Controller Device Type with Always On Slave (AOS) as the Role Type and enhanced 232 slave. The Wall Controller shows how to implement an interrupt service routine (ISR) on the application level. For detailed information, refer to [11].

6.11 Z-Wave Plus Application Framework

The Z-Wave Plus Application Framework simplifies implementation of robust Z-Wave Plus-compliant and interoperable products. Many Z-Wave certification requirements are also handled by the Z-Wave Plus Application Framework, making it much easier to pass certification. The Z-Wave logo is only granted to products that have passed certification.

6.11.1 Application Command Handlers

The Application Command Handlers code contains an implementation of various command classes used by Z-Wave Plus applications. For detailed information, refer to [19].

6.11.2 Application Utilities

The Application Utilities code contains an implementation of various general-purpose functions used by Z-Wave Plus applications. A large part of the S0/S2 security solution now resides in the Z-Wave Protocol. For detailed information, refer to [19].

7 TOOLS

The SDK contains various tools for helping SW developers write and debug code.

NOTE: Some of the tools are no longer bundled together with the SDK but are available on ZTS as individual programs:

7.1 IMA Tool Box

The IMA Tool Box supports an installation and maintenance procedure that ensures easy installation and provides an operational qualification of the installation. Use this tool in combination with the Serial API based hex targets, which incorporate IMA functionality by default. The source code of IMA Tool Box is also included. For detailed information, refer to [2].

7.2 uVision4 Project Generator

The Keil uVision4 Project Generator creates uVision projects for sample applications. The makefile system can generate uVision projects for the Keil uVision4 IDE by calling the project generator.

8 PRODUCT LIFE CYCLE AND CERTIFICATION

Silicon Labs will add new features based on market requirements and continuously improve the Z-Wave Protocol to position the Z-Wave Ecosystem. The Z-Wave Protocol Life Cycle process provides rapid innovation, new features, and robust, mature protocol releases to Z-Wave Partners. The Z-Wave Protocol Life Cycle defines the maturation process of Z-Wave Protocol generations and consists of three phases divided into five Life Cycle stages.

Ascent Phase (BETA)

Silicon Labs releases new Z-Wave protocol generations (branches), i.e., initial BETA releases of Z-Wave Protocol generations that will introduce major new features/functions or support for new Z-Wave Single Chip generations. This release is not certified and is not eligible for certification.

Maturity Phase (ACTIVE/MAINTAINED)

Each new generation will generate follow-on matured releases to resolve protocol issues prioritized by Silicon Labs and based on input from Z-Wave Alliance Partners.

Decline Phase (MONITORED/OBSOLETE)

After a period of 17-24 months in the maturity phase, a branch/release is discontinued. For an additional period of up to 24 months, a discontinued branch/release will be monitored since products based on this branch may still be shipping or under warranty in the field.

Table 1. Z-Wave SDK Life Cycle Status

Series	Branch	SDK Version	Release Date [DD/MM/YYYY]	Life Cycle Status
500	6.8x.xx	6.82.01 GA	13/04/2020	Active
		6.82.00 GA	08/10/2019	Maintained
		6.81.06 GA	19/07/2019	Monitored
		6.81.05 GA	07/05/2019	Monitored
		6.81.04 GA	21/02/2019	Monitored
		6.81.03 GA	19/10/2018	Monitored
		6.81.02 GA	01/06/2018	Obsolete
		6.81.01 GA	22/03/2018	Obsolete
		6.81.00 GA	27/09/2017	Obsolete
		6.80.00 Beta	26/09/2017	Obsolete

A change in the Z-Wave SDK utilized for a specific device requires recertification; however, the type of certification required, the amount of testing needed, and the associated fees depend on the scope of the change.

Table 2. Z-Wave Certification in case of an SDK upgrade.

SDK Version	Upgrade to SDK Version	Type of Certification
6.82.01 GA	NA	-
6.82.00 GA	6.82.01 GA	Re-certification
6.81.06 GA	6.82.01 GA 6.82.00 GA	Full certification Full certification
6.81.05 GA	6.82.01 GA 6.82.00 GA 6.81.06 GA	Full certification Full certification NA
6.81.04 GA	6.82.01 GA 6.82.00 GA 6.81.05+ GA	Full certification Full certification NA
6.81.03 GA	6.82.01 GA 6.82.00 GA 6.81.04+ GA	Full certification Full certification NA
6.81.02 GA	6.82.01 GA 6.82.00 GA 6.81.03+ GA	Full certification Full certification NA
6.81.01 GA	6.82.01 GA 6.82.00 GA 6.81.02+ GA	Full certification Full certification NA
6.81.00 GA	6.82.01 GA 6.82.00 GA 6.81.01+ GA	Full certification Full certification NA

9 LEGAL

9.1 Disclaimer

Silicon Labs intends to provide customers with the latest, most accurate, and in-depth documentation of all peripherals and modules available for system and software implementers using or intending to use Silicon Labs products. Characterization data, available modules and peripherals, memory sizes and memory addresses refer to each specific device, and "Typical" parameters provided can and do vary in different applications.

Application examples described herein are for illustrative purposes only.

Silicon Labs reserves the right to make changes without further notice and limitation to the product information, specifications, and descriptions herein and does not give warranties as to the accuracy or completeness of the included information. Silicon Labs shall have no liability for the consequences of use of the information supplied herein. This document does not imply, or express copyright licenses granted hereunder to design or fabricate any integrated circuits. The products are not designed or authorized to be used within any Life Support System. A "Life Support System" is any product or system intended to support or sustain life and/or health, which, if it fails, can be reasonably expected to result in significant personal injury or death. Silicon Labs products are not designed or authorized for military applications. Silicon Labs products shall under no circumstances be used in weapons of mass destruction including (but not limited to) nuclear, biological or chemical weapons, or missiles capable of delivering such weapons.

9.2 Trademark Information

Silicon Laboratories Inc.®, Silicon Laboratories®, Silicon Labs®, SiLabs® and the Silicon Labs logo®, Bluegiga®, Bluegiga Logo®, Clockbuilder®, CMEMS®, DSPLL®, EFM®, EFM32®, EFR, Ember®, Energy Micro, Energy Micro logo and combinations thereof, "the world's most energy friendly microcontrollers", Ember®, EZLink®, EZRadio®, EZRadioPRO®, Gecko®, ISOmodem®, Micrium, Precision32®, ProSLIC®, Simplicity Studio®, SiPHY®, Telegesis, the Telegesis Logo®, USBXpress®, Zentri, Z-Wave and others are trademarks or registered trademarks of Silicon Labs.

ARM, CORTEX, Cortex-M0+, Cortex-M3, Cortex-M33, Cortex-M4, TrustZone, Keil and Thumb are trademarks or registered trademarks of ARM Holdings.

Zigbee® and the Zigbee logo® are registered trademarks of the Zigbee Alliance.

Bluetooth® and the Bluetooth logo® are registered trademarks of Bluetooth SIG Inc.

All other products or brand names mentioned herein are trademarks of their respective holders.

REFERENCES

[1] Silicon Labs, INS10243, Instruction, Z-Wave Protocol Overview.

[2] Silicon Labs, INS12712, Instruction, Z-Wave Network Installation and Maintenance Procedure User Guide.

[3] Silicon Labs, INS13954, Instruction, Z-Wave 500 Series Application Programming Guide v6.8x.0x.

[4] Silicon Labs, SDS10242, Software Design Specification, Z-Wave Device Class Specification.

[5] Silicon Labs, SDS10865, Software Design Specification, Z-Wave Security Application Layer.

[6] Silicon Labs, SDS13781, Software Design Specification, Z-Wave Application Command Class Specification.

[7] Silicon Labs, SDS13782, Software Design Specification, Z-Wave Management Command Class Specification.

[8] Silicon Labs, SDS13783, Software Design Specification, Z-Wave Transport-Encapsulation Command Class Specification.

[9] Silicon Labs, SDS13784, Software Design Specification, Z-Wave Network-Protocol Command Class Specification.

[10] Silicon Labs, SDS13548, Software Design Specification, List of defined Z-Wave Command Classes.

[11] Silicon Labs, INS13933, Instruction, Z-Wave 500 Series SDK Contents v6.8x.0x.

[12] Silicon Labs, INS12366, Instruction, Working in 500 Series Environment User Guide.

[13] Silicon Labs, APL12444, Application Note, Porting Z-Wave Appl. SW from ZW0301 to 500 Series.

[14] Silicon Labs, APL12445, Application Note, Porting Z-Wave Appl. SW from 400 to 500 Series.

[15] Silicon Labs, SDS11846, Software Design Specification, Z-Wave Plus Role Types Specification.

[16] Silicon Labs, SDS11847, Software Design Specification, Z-Wave Plus Device Types Specification.

[17] Silicon Labs, SDS12467, Software Design Specification, 500 Series Z-Wave Chip NVR Flash Page Contents.

[18] Silicon Labs, INS12350, Instruction, Serial API Host Appl. Prg. Guide.

[19] Silicon Labs, INS13953, Instruction, Z-Wave Plus Application Framework v6.8x.0x.

[20] Silicon Labs, INS12213, Instruction, 500 Series Integration Guide.

[21] Silicon Labs, INS13474, Instruction, Z-Wave Security Whitepaper.

[22] Silicon Labs, SDS13349, Software Design Specification, Security considerations in Home Control installations.

[23] Silicon Labs, APL13434, Application Note, FAQ: On the use of S0, S2 and Supervision CC in product design and deployments.

[24] Silicon Labs, SDS13937, Software Design Specification, Node Provisioning QR Code Format.

[25] Silicon Labs, INS13975, Instruction, Smart Start Production control.

[26] Silicon Labs, ERN14614, Errata Note, Known Test Observations SDK v6.82.1.

INDEX