128Mb/256Mb/512Mb SEMPER™ Secure flash

Quad SPI, 1.8V/3.0V

Register for the SEMPER™ Secure access program to access the complete datasheet.

Device overview

- **Highlights**
  - Security features
    - Array partitioning with up to eight secured regions
    - Device identifier composition engine (DICE)
    - Asymmetric and symmetric key algorithms support
    - Authenticated read, program, and erase operations
    - Encrypted read, program, and erase operations
    - Ephemeral session key generation
    - Secured storage for keys and user monotonic counters
    - Fast secured boot support
  - Safety features
    - Functional safety with the industry's first ISO26262 ASIL B compliant and ASIL D ready NOR flash
    - Infineon endurance flex architecture provides high-endurance and long retention partitions
    - Data integrity CRC detects errors in memory array
    - SafeBoot reports device initialization failures, detects configuration corruption, and provides recovery options
    - Built-in error correcting code (ECC) corrects single-bit error and detects double-bit error (SECDED) on memory array data
    - Sector erase status indicator for power loss during erase
- **Architecture**
  - Infineon 45-nm MIRRORBIT™ technology that stores two data bits in each memory array cell
  - Sector architecture options
    - Uniform: Address space consists of all 256 KB sectors
    - Hybrid
      Configuration 1: Address space consists of thirty-two 4 KB sectors grouped either on the top or the bottom while the remaining sectors are all 256 KB
      Configuration 2: Address space consists of thirty-two 4 KB sectors equally split between top and bottom while the remaining sectors are all 256 KB
  - Page programming buffer of 256 or 512 bytes
  - OTP secure silicon array of 1024 bytes (32 × 32 bytes)
- **Interface**
  - Quad SPI
    - Supports 1S-1S-4S, 1S-4S-4S, 1S-4D-4D, 4S-4S-4S, 4S-4D-4D protocols
    - SDR option runs up to 83 MBps (166 MHz clock speed)
    - DDR option runs up to 102 MBps (102 MHz clock speed)
  - Dual SPI
    - Supports 1S-2S-2S protocol
    - SDR option runs up to 41.5 MBps (166 MHz clock speed)

- SPI
  - Supports 1S-1S-1S protocol
  - SDR option runs up to 21 MBps (166 MHz clock speed)
- Interrupt pin to indicate device status
- Hardware reset through CS# signaling method (JEDEC) / individual RESET# pin / DQ3_RESET# pin

- **Identification**
  - Serial flash discoverable parameters (SFDP) describing device functions and features
  - Device identification, manufacturer identification, and unique identification

- **Data integrity**
  - 128 Mb devices
    - Minimum 320,000 program-erase cycles for the main array
  - 256 Mb devices
    - Minimum 640,000 program-erase cycles for the main array
  - 512 Mb devices
    - Minimum 1,280,000 program-erase cycles for the main array
  - All devices
    - Minimum 300,000 program-erase cycles for the 4 KB sectors
  - Minimum 25 years data retention

- **Supply voltage**
  - 1.7 V to 2.0 V (HS-T)
  - 2.7 V to 3.6 V (HL-T)

- **Grade / temperature range**
  - Industrial (–40°C to +85°C)
  - Industrial Plus (–40°C to +105°C)
  - Automotive AEC-Q100 Grade 3 (–40°C to +85°C)
  - Automotive AEC-Q100 Grade 2 (–40°C to +105°C)
  - Automotive AEC-Q100 Grade 1 (–40°C to +125°C)

Packages
- 24-ball BGA 6 × 8 mm
- 16-pin SOIC (300 mil)
- 8-contact WSON wettable flank 6 × 8 mm (single I/O SPI only)

Performance summary

Maximum read rates

Transaction	Initial access latency (cycles)	Clock rate (MHz)	MBps
SPI read	0	50	6.25
SPI fast read	9	166	20.75
Dual read SDR	7	166	41.5
Quad read SDR	10	166	83
Quad read DDR	7	102	102

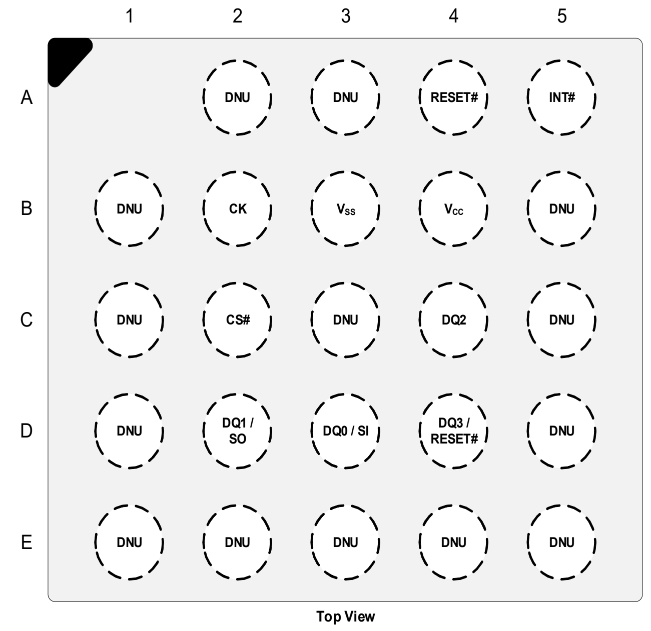
Typical program and erase rates

Operation	KBps
256B page programming (4 KB sector / 256 KB sector)	595 / 533
512B page programming (4 KB sector / 256 KB sector)	753 / 898
256 KB sector erase	331
4 KB sector erase	95

Typical current consumption

Operation	Current (mA)
SDR read 50 MHz	14
SDR read 166 MHz	53
DDR read 102 MHz	50
Program	50
Erase	50
Standby (HS-T)	0.011
Standby (HL-T)	0.014
Deep power down (HS-T)	0.0013
Deep power down (HL-T)	0.0022

1 Pinout and signal description



	1	2	3	4	5
A		DNU	DNU	RESET#	INT#
B	DNU	CK	V_{SS}	V_{CC}	DNU
C	DNU	CS#	DNU	DQ2	DNU
D	DNU	DQ1 / SO	DQ0 / SI	DQ3 / RESET#	DNU
E	DNU	DNU	DNU	DNU	DNU

Figure 1 **24-ball BGA pinout configuration**[1]

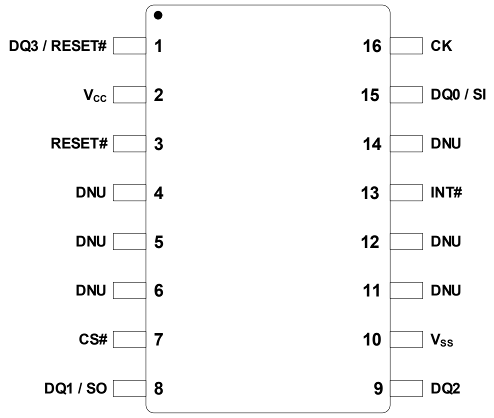


Figure 2 **16-pin SOIC package (SO316), top view**

Note

1. Flash memory devices in BGA packages can be damaged if exposed to ultrasonic cleaning methods. The package, data integrity, or both may be compromised if the package body is exposed to temperatures above 150°C for prolonged periods of time.

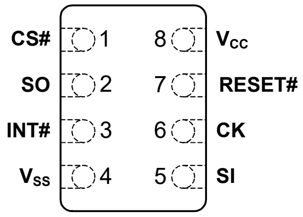


Figure 3 8-connector package (WSON 6 × 8), top view[2]

Table 1 Signal description

Symbol	Type	Mandatory/ Optional	Description
CS#	Input	Mandatory	**Chip Select (CS#).** All bus transactions are initiated with a HIGH to LOW transition on CS# and terminated with a LOW to HIGH transition on CS#. Driving CS# LOW enables the device, placing it in the Active mode. When CS# is driven HIGH, the device enters Standby mode, unless an internal embedded operation is in progress. All other input pins are ignored and the output pins are put in HIGH IMPEDANCE state. On parts where the pin configuration offers a dedicated RESET# pin, it remains active when CS# is HIGH.
CK			**Clock (CK)**. Clock provides the timing of the serial interface. Transactions are latched on the rising edge of the clock. In SDR protocol, command, address and data inputs are latched on the rising edge of the clock, while data is output on the falling edge of the clock. In DDR protocol, command, address and data inputs are latched on both edges of the clock, and data is output on both edges of the clock.
DQ0 / SI	Input/output		**Serial Input (SI)** for single SPI protocol. **DQ0 Input/ Output** for Dual or Quad SPI protocol.
DQ1 / SO			**Serial Output (SO)** for single SPI protocol. **DQ1 Input/ Output** for Dual or Quad SPI protocol.
INT#[3]	Output (open drain)	Optional	**System Interrupt (INT#)**. When LOW, the device in indicating that an internal event has occurred. The signal is intended to be used as a system level interrupt for the device to indicate that an on-chip event has occurred. INT# is an open-drain output.
DQ2	Input/output	Mandatory	**DQ2 Input/ Output** for Quad SPI protocol
DQ3 / RESET#	Input/Output (weak pull-up)		**RESET#** for single and dual SPI protocol. This signal can be configured as RESET# when CS# is HIGH or Quad SPI protocol is disabled. **DQ3 Input/ Output** for Quad SPI protocol. The signal has an internal pull-up resistor and can be left unconnected in the host system if not used for Quad SPI transactions or RESET#
RESET#[3]	Input (weak pull-up)	Optional	**Hardware Reset (RESET#)**. When LOW, the device will self initialize and return to the Array Read state. DQ[3:0] are placed into the HIGH IMPEDANCE state when RESET# is LOW. RESET# includes a weak pull-up, meaning, if RESET# is left unconnected it will be pulled up to the HIGH state on its own.
V_{CC}	Power supply	Mandatory	Core Power Supply
V_{SS}	Ground supply		Core Ground
DNU	–	–	**Do Not Use.**

Notes

[2] WSON package supports Single I/O SPI only.

[3] Both INT# and RESET# pins are supported in all packages.

2 General description

SEMPER™ Secure flash products with Quad SPI interface are high-speed CMOS, MIRRORBIT™ NOR flash devices. SEMPER™ Secure devices are designed for Functional Safety with development according to the ISO 26262 standard to achieve ASIL-B compliance and ASIL-D readiness.

These devices support traditional SPI single-bit serial input and output, optional two-bit (Dual I/O or DIO) as well as four-bit wide Quad I/O (QIO) and Quad Peripheral Interface (QPI) protocols. In addition, there are DDR read transactions for QIO and QPI that transfer address and read data on both edges of the clock.

Note that due to a limited number of pins, devices with WSON package support Single I/O SPI interface only. No Quad SPI commands are supported. The QUADIT bit (CFR1x[1]) should not be set to 1 in devices with WSON package.

In SEMPER™ Secure flash devices, the main array address space can be configured to have up to eight secured regions. These regions can have different level of security that are defined by users. SEMPER™ Secure devices provide secured storage for keys and monotonic counters that can be used by cryptographic functions. SEMPER™ Secure devices have an integrated hardware cryptographic accelerator to perform cryptographic functions such as random number generation, hashing, encryption, and decryption.

SEMPER™ Secure devices can be operated in two modes: Crypto mode and Normal mode. Users enter and exit Crypto mode by issuing the Enter Crypto and Exit Crypto mode SPI transactions. Security-related commands are communicated between the host and the device in packet format once the device is in Crypto mode. There are a limited set of normal SPI commands that are supported in Crypto mode for basic functions, such as Status Read and Reset. In Normal mode, read operations are burst oriented. Read transactions can be configured to use either a wrapped or linear burst. Wrapped bursts read from a single page. Linear bursts can read the memory array contiguously; however, it will not cross a secured region boundary.

The erased state of each memory bit is a logic ‘1’. Programming changes a logic 1 (HIGH) to a logic 0 (LOW). Only an erase operation can change a memory bit from a ‘0’ to a ‘1’. An erase operation must be performed on a complete sector (4 or 256 KB).

SEMPER™ Secure flash provides a flexible sector architecture. The address space can be configured as either a uniform 256 KB sector array, a hybrid configuration in which thirty-two 4 KB sectors are either grouped at the top or at the bottom and all other sectors are 256 KB, or a hybrid configuration in which sixteen 4 KB sectors are grouped at the top of the address space, sixteen 4 KB sectors are grouped at the bottom of the address space, and all other sectors are 256 KB.

The page programming buffer used during a single programming operation is configurable as either 256 bytes or 512 bytes. The 512-byte option provides the highest programming throughput.

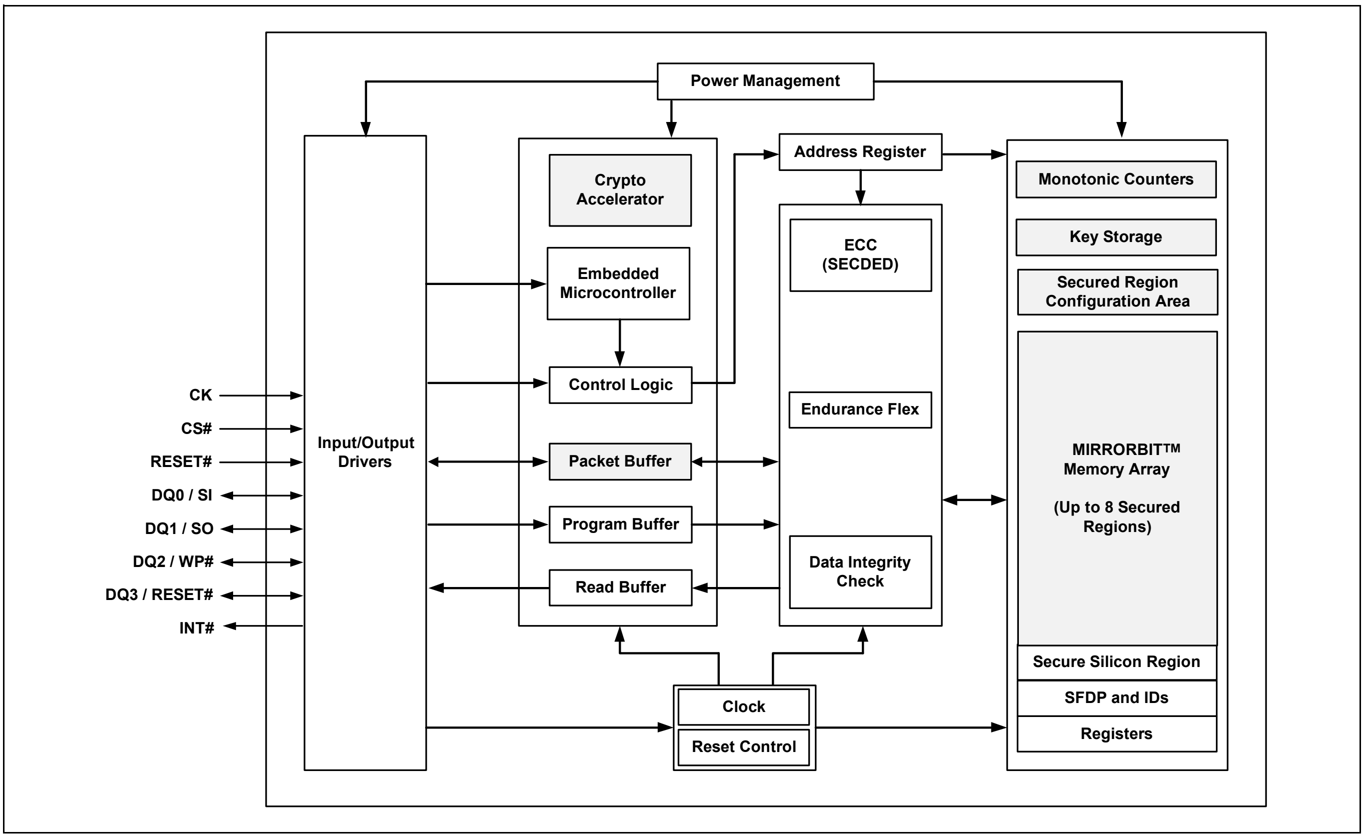


Figure 4 **Logic block diagram**[4]

Note

4. Gray scale denotes security functions.

The SEMPER™ Secure flash with Quad SPI family consists of 1.8-V and 3.0-V voltage options.

The device control logic is subdivided into two parallel operating sections: the host interface controller (HIC) and the embedded algorithm controller (EAC). The HIC monitors signal levels on the device inputs and drives outputs as needed to complete read, program, and write data transfers with the host system. The HIC delivers data from the currently entered address map on read transfers; places write transfer address and data information into the EAC command memory, and notifies the EAC of power transition, and write transfers. The EAC interrogates the command memory, after a program or write transfer, for legal command sequences and performs the related Embedded Algorithms.

Changing the non-volatile data in the memory array requires a sequence of operations that are part of embedded algorithms (EA). The algorithms are managed entirely by the internal EAC. The main algorithms perform programming and erase of the main flash array data. The host system writes command codes to the flash device. The EAC receives the command, performs all the necessary steps to complete the transaction, and provides status information during the progress of an EA.

Executing code directly from flash memory is often called eXecute-In-Place (XIP). By using XIP with SEMPER™ Secure flash devices at the higher clock rates with Quad or DDR Quad SPI transactions, the data transfer rate can match or exceed traditional parallel or asynchronous NOR flash memories while reducing signal count dramatically. Note that when in Crypto mode, Authenticated Read or Encrypted Read operations are not suitable for XIP function because the reads are in packet format, which reduces throughput.

Infineon endurance flex architecture provides system designers the ability to customize the NOR flash endurance and retention for their specific application. The host defines partitions for high endurance or long retention, providing up to 1+ million cycles or 25 years of data retention.

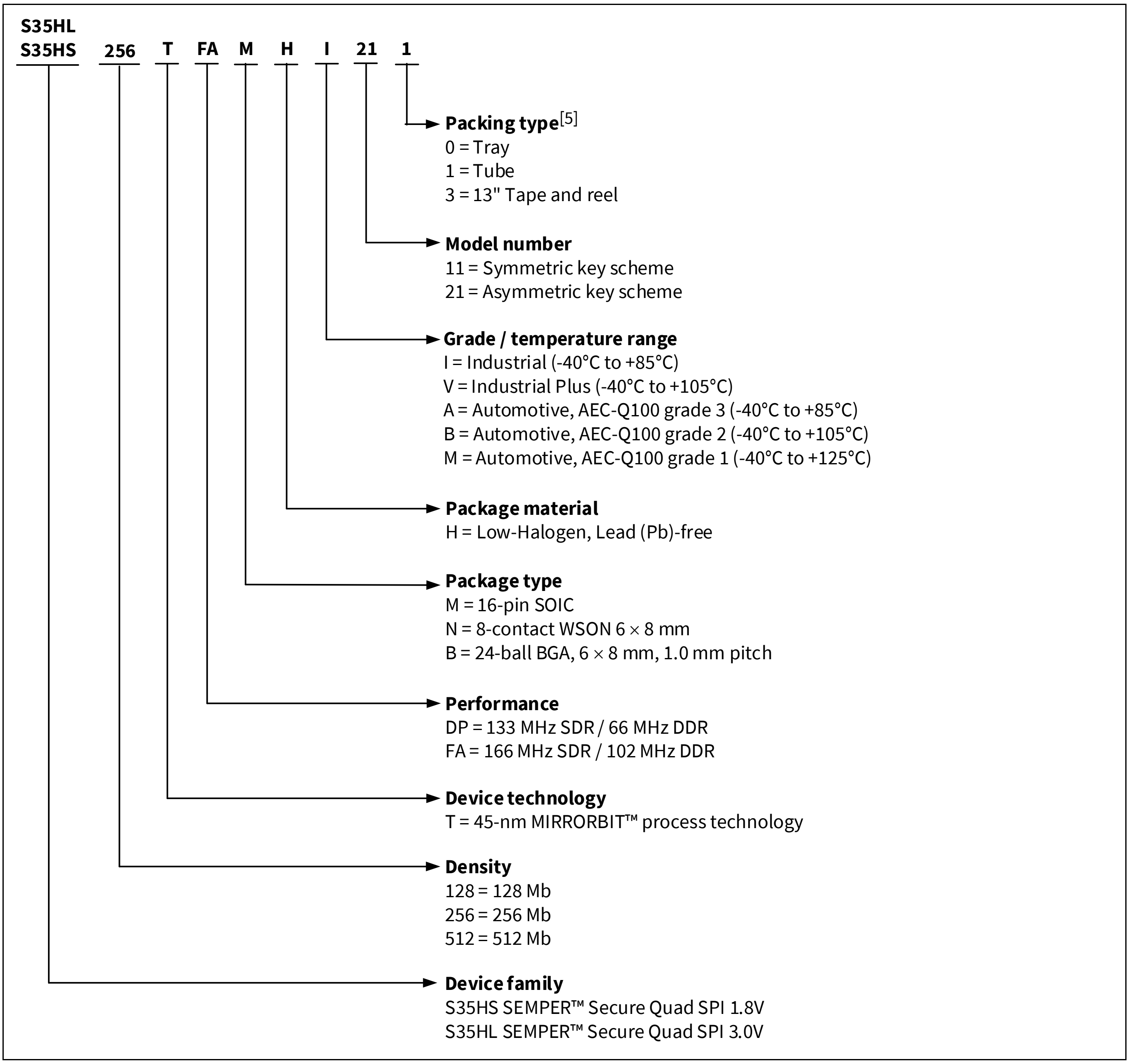
The SEMPER™ Secure flash with Quad SPI device supports error detection and correction by generating an embedded Hamming ECC during memory array programming. This ECC is then used for single-bit and double-bit error detection and single-bit correction during read.

The SEMPER™ Secure flash with Quad SPI device has built-in diagnostic features providing the host system with the device status.

- Program and erase operation: Reporting of program or erase success, failure and suspend status
- Error detection and correction: 1-bit and/or 2-bit error status with address trapping and error count
- Data integrity check: Error detection over memory array contents
- SafeBoot: Reporting of proper flash device initialization and configuration corruption recovery
- Sector erase status: Reporting of erase success or failure status per sector
- Sector erase counter: Counts the number of erase cycles per sector

3 Ordering information

The ordering part number is formed by a valid combination of the following:



Packing type[5]
0 = Tray
1 = Tube
3 = 13" Tape and reel

Model number
11 = Symmetric key scheme
21 = Asymmetric key scheme

Grade / temperature range
I = Industrial (-40°C to +85°C)
V = Industrial Plus (-40°C to +105°C)
A = Automotive, AEC-Q100 grade 3 (-40°C to +85°C)
B = Automotive, AEC-Q100 grade 2 (-40°C to +105°C)
M = Automotive, AEC-Q100 grade 1 (-40°C to +125°C)

Package material
H = Low-Halogen, Lead (Pb)-free

Package type
M = 16-pin SOIC
N = 8-contact WSON 6 × 8 mm
B = 24-ball BGA, 6 × 8 mm, 1.0 mm pitch

Performance
DP = 133 MHz SDR / 66 MHz DDR
FA = 166 MHz SDR / 102 MHz DDR

Device technology
T = 45-nm MIRRORBIT™ process technology

Density
128 = 128 Mb
256 = 256 Mb
512 = 512 Mb

Device family
S35HS SEMPER™ Secure Quad SPI 1.8V
S35HL SEMPER™ Secure Quad SPI 3.0V

Register for the SEMPER™ Secure access program to access the complete datasheets, application notes, models, software, solution development kit (SDK), and evaluation kits.

Note

[5] See Packing and Packaging Handbook on **www.infineon.com** for further information.

Revision history

Document version	Date of release	Description of changes
**	2020-05-22	Initial release.
*A	2022-06-08	Migrated to Infineon template. Updated new SEMPER™ Secure access program link. Minor text updates.

Trademarks

All referenced product or service names and trademarks are the property of their respective owners.

Edition 2022-06-08

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Go to www.infineon.com/support

Document reference

002-30419 Rev. *A

IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics (“Beschaffenheitsgarantie”).

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer’s compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Infineon Technologies in customer’s applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer’s technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies’ products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.