AN98556

Cypress High Voltage Sector Group Protection / Un-Protection

AN98556 highlights the High Voltage Sector Group Protection/Unprotection feature supported by Cypress S29AL-J, S29AS-J, and S29JL-J flash families, including the necessary circuitry to support in-system sector protection management.

1 Sector Protection

Each Cypress flash memory array is portioned into one or more banks and further subdivided into sections called sectors. For the following discussion, the term sector applies to both boot sectors and sector groups. A sector group consists of two or more adjacent sectors that are protected or unprotected at the same time. Reference respective flash data sheet to find details for that device's sector block grouping.

Each sector has control bits that can protect a sector by disabling program and erase functions within the address boundaries of the sector. Most devices can protect a combination of sectors which comprise the flash array. Flash devices use a control bit to manage the protection of individual sectors or a group of sectors. From the user perspective the sector protection can change one or more sectors into ROM type memory that cannot be altered during normal operation.

Cypress flash can use High Voltage Protection or Advanced Sector Protection to invoke the subject sector protection depending on the flash family. This document highlights the High Voltage Sector Group Protection/ Unprotection feature supported by Cypress S29AL-J, S29AS-J, and S29JL-J flash families, including the necessary circuitry to support in-system sector protection management.

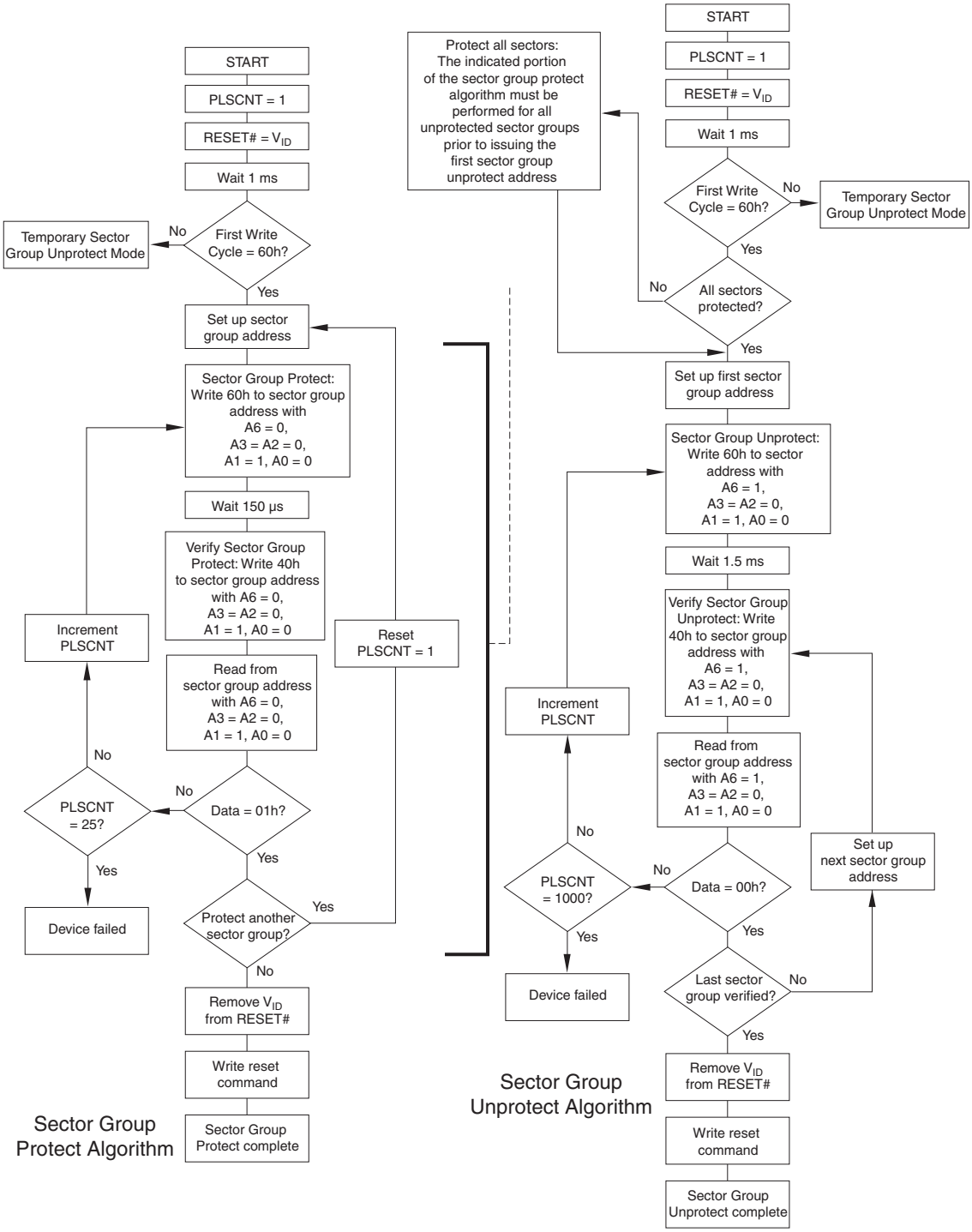
2 High Voltage Controlled Sector Group Protection

Sector protection is often used to safeguard critical portions the flash memory map such as boot / application code or critical data areas. The High Voltage Controlled Sector Group Protection Is a hardware based protection setup that secures the subject sector(s) against data corruptions such as from viruses or an erroneous flash access. This high voltage hardware sector group protection feature disables both program and erases operations in the specified sector group(s). The hardware sector group un-protection feature re-enables both program and erase operations in a once protected sector group. The Cypress High Voltage Controlled Sector Group Protection uses the high-voltage V_{ID} applied to RESET# as a key used to access the sector protection control bits.

Figure 1 provides an example of the S29AL-J Sector protection and un-protection algorithms; these algorithms highlight the steps necessary to complete the respective sector protect or unprotect process. Please note prior to completing a sector group unprotect, all unprotected sector groups must first be protected prior to the first sector group unprotect write cycle. Cypress flash ships all standard flash devices with sector groups in the unprotected state.

Please reference the respective data sheet to obtain the subject devices complete algorithms and timing diagrams. In cases where a module or system design does not support a high voltage source to the flash memory; flash can be pre-programmed and protected using many commercially available flash programmers prior to installing the flash in the system module.

Figure 1. High Voltage Protection Algorithm



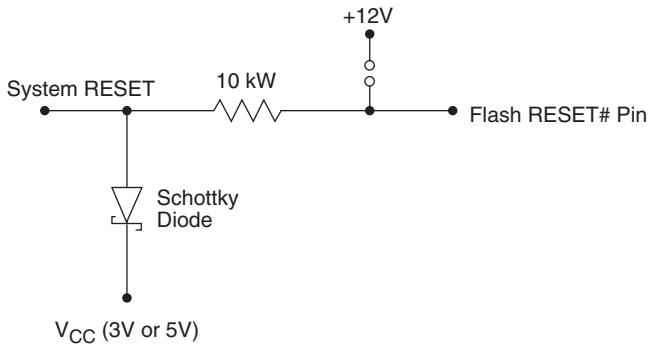
3. In-System Sector Protection Management

Cypress High Voltage Controlled Sector Group Protection allows management of the flash sector protection after the flash device is mounted on the system module. In such cases, there must be a module or system design provision to support the high voltage V_{ID} flash input requirements. This approach provides the option for memory to perform post assembly flash programming followed by sector protection later in the manufacturing processes. This type of configuration can also provide an option for updating software in the critical sectors after unit has been shipped to end customers. For in-system programming or reprogramming, Cypress flash can be temporarily unprotected by applying V_{ID} (11.5V to 12.5V) to the RESET# pin. When V_{ID} is removed from the RESET# pin, all sectors return to their previous state of protection. The flash families S29AL, S29AS, S29JL, and AM29F series allow the sector protection bits to be cleared and reprogrammed to protect a different combination of sectors, via software commands while the device is in the temporary unprotect mode. (See the respective data sheet sections entitled “Sector Protection / Un-protection” and “Temporary Sector Unprotect” for additional details.)

4 Method for Providing High Voltage Isolation to the System Reset

Cypress recommends that a design employ an interface between the system Reset signal and the RESET# pin of the flash. The RESET# input enables appropriate control to the flash State Machine during power up and power down, along with the rest of the system. This system reset uses standard logic levels as specified in the subject data sheet. To address the situation where the high voltage V_{ID} is applied to the flash RESET# pin, a small circuit can be added to the design. This circuit configuration enables the normal logic level inputs to function and to achieve system isolation from the high voltage V_{ID} when applied. Figure 2 shows the use of series resistor between the RESET# pin and the system level Reset signal along with a Schottky diode between the system reset and the system V_{CC}.

Figure 2. RESET# Pin Isolation Circuitry



When V_{ID} is not connected to the flash RESET# pin, the series resistor allows the normal logic level on the system reset to propagate to the flash memory. The flash RESET# pin is low capacitance, and in combination with the added resistor, the rise time of the reset signal is still typically <300 ns. The normal flash reset functionality is not hindered by the series resistor. When high voltage is applied to the RESET# pin, the resistor limits current flow to the system reset signal. The maximum current flow to the system reset (when the system asserts V_{IL} on the system reset signal) is 1.2 mA. The Schottky diode guarantees a clamp on the system reset signal to no more than V_{CC} + ~0.3V. ESD protection diodes already built into the inputs of other devices attached to the system reset signal could serve a similar purpose, but the typical 0.7V voltage rise induced by these diodes would clamp the voltage to a level which exceeds the V_{IH} max data sheet parameter. Use of a Schottky diode clamp provides a means not to exceed the V_{IH} parameter. The resistor and diode combination form the isolation circuitry and present very minimal additional system cost while enabling the flexibility of in-system sector protection management.

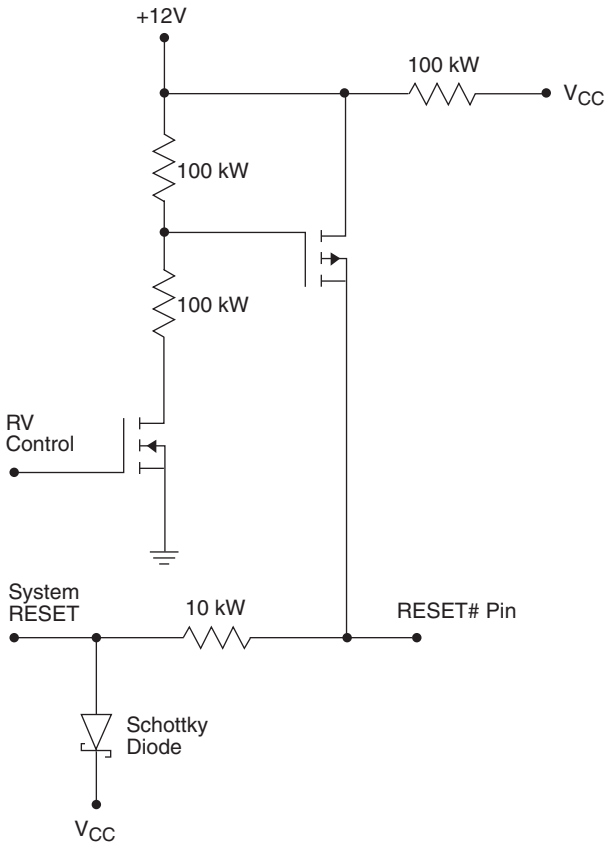
5. Methods for Providing High Voltage to the Flash Device RESET# Pin

The flash RESET# is a high impedance input and does not the V_{ID} signal to provide significant current; the voltage level is detected by the flash input. The rise and fall time, when transitioning between normal logic signal voltage levels and V_{ID}, must be limited to t_{VIDR} (500 ns) minimum. There must also be a delay of t_{RSP} (4 µs) after V_{ID} is reached before any writing to the flash memory is begun.

Some systems do not have 12V available, but can provide a 12V supply from an outside source such as a manufacturing test system, daughter card, debug system, or via an external cable or connection. Such an external supply may only be available at a factory or service center location. This method is the simplest in that only a connection to the flash RESET# pin needs to be provided. The voltage source and method for switching it on and off are external to the system being programmed. The system carries no burden of extra circuitry to create and control the high voltage. This approach also ensures that there is no way for the system to accidentally switch on the unlock voltage; without the external voltage supply to override sector protection.

For systems where a 12V source is available, it may be desirable to allow the 12V supply to be switched to the flash RESET# pin within the system. One suggestion for switching the V_{ID} level is shown in Figure 3. By placing a P-channel MOSFET between the V_{ID} source and the flash RESET# pin. The gate of the P-channel MOSFET is pulled up to V_{ID} through a 100 kΩ resistor. The gate of the P-channel device can be pulled down to ground by a TTL logic level controlled N-channel MOSFET. Depending on the operational characteristics of the P-channel MOSFET, and the characteristics of the RV Control signal, the gate voltage may require conditioning using a 5KΩ and 100 pF RC circuit. This allows the turn on and off delay of the P-channel to ensure that the rise and fall time of V_{ID} is ≥500 ns. The gate of the logic level N-channel MOSFET is driven by a system control signal to enable the sector protection unlock voltage. A 100 KΩ resistor from the V_{ID} source to V_{CC} is recommended for situations where the V_{ID} supply is not always connected (or not always active) to keep the MOSFETs properly biased.

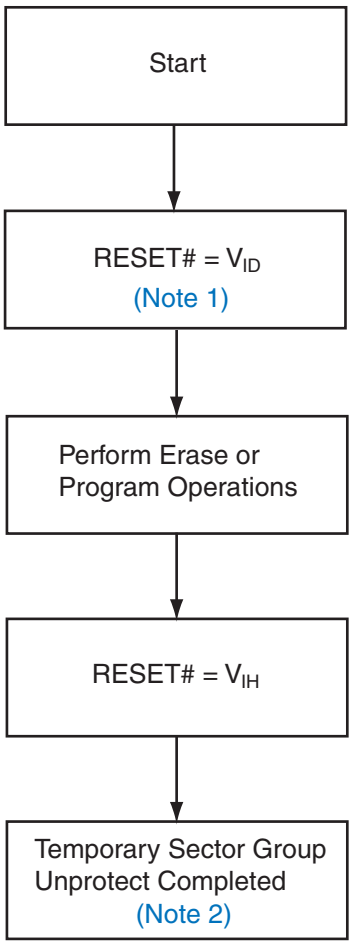
Figure 3. V_{ID} Routing Circuitry



Cypress High Voltage Sector Group Protection / Un-protection also supports a “Temporary Sector Group Unprotect” feature allowing the temporary un-protection of previously protected sector groups to change data in-system. The Sector Group Unprotect mode is activated by setting the RESET# pin to V_{ID}. During this mode,

formerly protected sector groups can be programmed or erased by selecting the sector group addresses. Once V_{ID} is removed from the RESET# pin, all the previously protected sector groups are protected again. Reference Figure 4 to see S29AL016 example of the Temporary Sector Group Unprotect Operation.

Figure 4. Temporary Sector Group Unprotect Operation



Notes:

1. *All protected sector unprotected. (If WP# = V_{IL}, the highest or lowest address sector remains protected for uniform sector devices; the top or bottom two address sectors remains protected for boot sector devices).*
2. *All previously protected sector groups are protected once again.*

6 Conclusion

Cypress NOR flash memory array is partitioned into one or more banks and further subdivided into sections called sectors. Cypress provides a high voltage sector group protection/un-protection feature to enable a designer the option to protect selected area in the flash memory array from inadvertent erasure or programming. This high voltage sector group protection/un-protection feature requires the application of super-voltage V_{ID} to the flash RESET# while executing the sector group protection or un-protection algorithm. This application note highlighted that high voltage sector group protection / un-protection feature can be used during programming on commercial programming equipment or via in-system with appropriate system design considerations.

Document History Page

Document Title: AN98556 - Cypress High Voltage Sector Group Protection / Un-Protection Document Number: 001-98556				
Rev.	**ECN No.**	**Orig. of Change**	**Submission Date**	**Description of Change**
**	–	–	10/28/2011	Initial version
*A	4958564	MSWI	10/12/2015	Updated in Cypress template
*B	5867912	AESATMP8	08/30/2017	Updated logo and Copyright.
*C	6545780	BWHIA	04/16/2019	Changed S9AL-J to S29AS-J in Overview and Sector Protection chapter on page 1

Worldwide Sales and Design Support

Cypress maintains a worldwide network of offices, solution centers, manufacturer's representatives, and distributors. To find the office closest to you, visit us at Cypress Locations.

Products

Arm® Cortex® Microcontrollers	cypress.com/arm
Automotive	cypress.com/automotive
Clocks & Buffers	cypress.com/clocks
Interface	cypress.com/interface
Internet of Things	cypress.com/iot
Memory	cypress.com/memory
Microcontrollers	cypress.com/mcu
PSoC	cypress.com/psoc
Power Management ICs	cypress.com/pmic
Touch Sensing	cypress.com/touch
USB Controllers	cypress.com/usb
Wireless Connectivity	cypress.com/wireless

PSoC® Solutions

PSoC 1 | PSoC 3 | PSoC 4 | PSoC 5LP | PSoC 6 MCU

Cypress Developer Community

Community | Projects | Video | Blogs | Training | Components

Technical Support

cypress.com/support

Cypress Semiconductor
198 Champion Court
San Jose, CA 95134-1709