Application Brief

Using the Security Features Inside the TPS546x24S Family of Step-Down Converters and Modules

Peter Miller

Protecting the Digital Bus

Traditionally, digitally controlled power solutions, whether using I2C, SMBus, PMBus®, SVI3, SVID or some other digital interface, have relied on the security of the bus controller devices to prevent malicious actors from gaining access and using the digital control to shut down the converter or even damage hardware. That was considered *good enough* for most applications. With the ever increasing presence of digital interfaces, and ever more sophisticated threats, that is no longer always sufficient to ensure the integrity of a system. When a device is connected to a remote interface, it is possible for remote actors to gain access the digital bus through one of the connected devices, and potentially send malicious commands over the bus. The TPS546x24S family of devices adds new, Manufacturer Specific commands to the PMBus interface to enable device designers to use the PMBus to configure a power device and then lock out access to commands that might be used to disrupt normal operation or damage sensitive components.

Direct drop-in compatible with the previous TPS546x24A family of stackable, PMBus enabled BUCK converters, the TPS546x24S family allows users of this popular device to upgrade their bus security without redesigning their existing hardware and simple modifications to their existing firmware.

EXT_WRITE_PROTECT (Command Code FBh) provides the designer with a 16-bit word for better control of the write options available in the TPS546D24S than the PMBus standard WRITE_PROTECT command (Command Code 10h). EXT_WRITE_PROTECT is a 16-bit word with each bit assigned to a command or group of commands, to disable write access to those commands. Unlike the PMBus Standard WRITE_PROTECT, EXT_WRITE_PROTECT offers options to disable writes to itself and disable writes to PASSKEY, which itself protects write access to EXT_WRITE_PROTECT. This, along with the flexibility to select which group of commands is, or is not write protected, allows system designers to protect their power solutions against malicious actors.

PASSKEY (Command Code FAh) provides the designer with a intermediate level of security between the open security of the TPS546x24A family and other legacy PMBus devices, and the permanent lock created by using EXT_WRITE_PROTECT to protect itself. PASSKEY is a 16-bit digital key. When set, it disabled write access to both EXT_WRITE_PROTECT and the User NVM store until the PASSKEY is written back to the device. To protect devices from brute force attacks, PASSKEY is limited to 3 failed PASSKEY write attempts per power-cycle.

PASSKEY allows the designer to provide a path for future updates to commands protected by EXT_WRITE_PROTECT with the cost and complexity of the PMBus Revision 1.5 Secure Device Application Profile's encryption based authenticated update, while still providing some protection against malicious actors. To minimize the potential of a breach resulting from a remote actor learning the PASSKEY, it is recommended that designers implement unique PASSKEYs on each device and or system, using the MFR_ID, MFR_MODEL, MFR_REVISION, and MFR_SERIAL values to build a hash to allow software updates to determine the PASSKEY rather than a common PASSKEY across all rails within a system or all systems.

Table 1. DC/DC Converters and Modules With PMBus Security Features

Part Number	Input Voltage	Output Current
TPS546A24S	2.95-V to 18-V	10-A
TPS546B24S	2.95-V to 18-V	20-A
TPS546D24S	2.95-V to 16-V	40-A
TPSM8S6C24	4-V to 16-V	35-A
TPSM8D6B24	4-V to 16-V	50-A (2x25-A)
TPSM8D6C24	4-V to 16-V	70A (2x35-A)

Levels of Security Settings EXT_WRITE_PROTECT and PASSKEY

Open

TPS546x24S devices are delivered from the TI factories in the “OPEN” security state, with PASSKEY and EXT_WRITE_PROTECT set to all 00h state. In this state, all commands with write access capability are write enabled and the User NVM store is access about through the STORE_USER_ALL command (Command Code 15h)

This level of security is useful for ease of programing devices and during early development when configuration changes might need to be quickly and easily entered into a device.

Write Protected

Users can program the TPS546x24S devices into a Write Protected state by setting the WRITE_PROTECT or EXT_WRITE_PROTECT to a non-zero value without setting bit 15 (Hardware Write Protect) and leaving PASSKEY set to the unlocked all 00h state. In this state, selected command groups have write access disabled, but EXT_WRITE_PROTECT can be written and updated at any time.

This level of security is useful in later states of development or during qualification, when charges are less likely, and verification of write protection’s interaction with firmware is necessary for product validation and qualification.

PASSKEY Protected

Users can program the TPS546x24S devices into a PASSKEY Protected state by setting the WRITE_PROTECT or EXT_WRITE_PROTECT to a non-zero value with setting bit 15 or bit 1 (PSK) and setting PASSKEY to a non-zero value. This uses the PASSKEY command to prevent casual write access EXT_WRITE_PROTECT while still leaving PASSKEY and EXT_WRITE_PROTECT available for changes.

This level of security is useful during early prototyping, in systems with limited or no remote access, or when the power rail serviced by the TPS546x24S device cannot induce system damage or is otherwise deemed non-critical.

Hardware Locked

Users can program the TPS546x24S devices into a Hardware Locked write protected state by setting EXT_WRITE_PROTECT to a non-zero value that includes bit 15 = b’1. Once set and stored to NVM, this prevents further writes to EXT_WRITE_PROTECT, preventing users, authorized or malicious, from accessing write protected PMBus commands through the bus. If a PASSKEY will not be used, it is recommended that users set EXT_WRITE_PROTECT bit 1 = b’1 with PASSKEY set to 0000h to prevent the setting of PASSKEY to an unknown value and altering the Write Protection.

This is the recommended Write Protection state for mass production systems that do not need changes to protected PMBus commands.

Locked with PASSKEY protected Non Volatile Memory (NVM)

Users can program the TPS546x24S devices into a state where EXT_WRITE_PROTECT is in a non-zero state with bit 15 = b’1, bit 1 = b’0, and bit 0 (Store) = b’0 while PASSKEY is set to a non-zero state. This prevents the changing of EXT_WRITE_PROTECT, and protects against changes to NVM boot values, but allows commands that are not protected by EXT_WRITE_PROTECT to update their NVM settings by unlocking the User STORE with the correct PASSKEY.

Double Locked

Users can program the TPS546x24S devices into a double-locked state by setting a non-zero PASSKEY, then setting EXT_WRITE_PROTECT with bit 15 = b’1, bit 1 = b’1, and bit 0 = b’1, then storing these values to NVM. Once in this state, EXT_WRITE_PROTECT is write protected by both EXT_WRITE_PROTECT and PASSKEY, while PASSKEY is protected by EXT_WRITE_PROTECT, preventing the unlocking of the PASSKEY.

For users looking for more advanced security features, PMBus Revision 1.5 Secure Device Application Profile offers digitally configured devices access to 256-bit encryption based attestation and command authentication to provide users with a secure method for verifying the authenticity of an installed device, and the means to allow authorized updates of PMBus commands while protecting them against unauthorized use.. EXT_WRITE_PROTECT provides the user with greater resolution to Write Protect features than the Standard PMBus Function. Each bit in the EXT_WRITE_PROTECT provides individual and independent WRITE_PROTECTION. The command profile and register map are shown below for reference.

Table 2. EXT_WRITE_PROTECT Command Profile

CMD Address	FBh
Write Transaction	Write Word
Read Transaction	Read Word
Format	Unassigned Binary (2 bytes)
Phased	No
NVM Back-up	EEPROM
Updates	At Boot-up

Table 3. EXT_WRITE_PROTECT Register Map

15	14	13	12	11	10	9	8
RW	RW	RW	RW	RW	RW	RW	RW
HWP	WP	TRIM	VOUT	VOF	WN	ITF	MAR
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
RW	RW	RW	RW	RW	RW	RW	RW
OP	CFG	VIN	SEQ	DAT	BOT	PSK	STR

Legend: RW = Read/Write; R = Read only

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265