Application Brief

使用 TPS546x24S 系列降压转换器和模块内部的安全特性

Peter Miller

保护数字总线

过去，数控电源解决方案（无论是使用 I2C、SMBus、PMBus®、SVI3、SVID 还是其他一些数字接口）依赖总线控制器器件的安全性，来防止恶意行为者获得访问权限和使用数字控制来关闭转换器甚至损坏硬件。对于大多数应用来说，这*已经足够*。随着数字接口不断增加并且威胁日益复杂化，这已不再总是足以确保系统的完整性。当器件连接到远程接口时，远程行为者有可能通过连接的器件之一访问数字总线，并且可能会通过总线发送恶意命令。TPS546x24S 系列器件向 PMBus 接口添加了特定于制造商的新命令，使器件设计人员能够使用 PMBus 配置功率器件，然后锁定对可能用于中断正常运行或损坏敏感元件的命令的访问权限。

TPS546x24S 系列与之前支持 PMBus 的 TPS546x24A 系列可堆叠降压转换器直接兼容，这种常见器件的用户无需重新设计现有硬件，只需对现有固件进行简单修改即可升级总线安全性。

EXT_WRITE_PROTECT（命令代码 FBh）为设计人员提供一个 16 位字，与 PMBus 标准 WRITE_PROTECT 命令（命令代码 10h）相比，能够更好地控制 TPS546D24S 中可用的写入选项。EXT_WRITE_PROTECT 是一个 16 位字，每个位都分配给一个命令或一组命令，以禁用对这些命令的写入访问。与 PMBus 标准 WRITE_PROTECT 不同，EXT_WRITE_PROTECT 提供禁用对自身进行写入以及禁用对 PASSKEY 进行写入的选项，PASSKEY 本身会保护对 EXT_WRITE_PROTECT 的写入访问。此外，系统设计人员还可以灵活选择哪组命令受写保护或不受写保护，从而保护其电源解决方案免受恶意行为者攻击。

PASSKEY（命令代码 FAh）为设计人员提供了中间级别的安全性，介于 TPS546x24A 系列和其他传统 PMBus 器件的开放安全性与使用 EXT_WRITE_PROTECT 创建用于自我保护的永久锁定之间。PASSKEY 是一个 16 位数字密钥。设置后，它会禁用对 EXT_WRITE_PROTECT 和用户 NVM 存储的写入访问，直到将 PASSKEY 写回器件。为防止器件遭受蛮力攻击，每次下电上电时 PASSKEY 写入尝试失败次数不得超过 3 次。

借助 PASSKEY，设计人员可以为受 EXT_WRITE_PROTECT 保护的命令的未来更新提供一条路径，其成本和复杂性与 PMBus 修订版 1.5 安全器件应用配置文件基于加密的身份验证更新相同，同时还能在一定程度上防范恶意行为者的攻击。为了尽可能降低由于远程攻击者了解 PASSKEY 而造成泄露的可能性，建议设计人员在每个器件或系统上实施独特的 PASSKEY，方法是使用 MFR_ID、MFR_MODEL、MFR_REVISION 和 MFR_SERIAL 值来构建哈希，以允许通过软件更新来确定 PASSKEY，而不是在系统内的所有电源轨或在所有系统中使用一个通用 PASSKEY。

表 1. 具有 PMBus 安全特性的直流/直流转换器和模块

器件型号	输入电压	输出电流
TPS546A24S	2.95V 至 18V	10A
TPS546B24S	2.95V 至 18V	20A
TPS546D24S	2.95V 至 16V	40A
TPSM8S6C24	4V 至 16V	35A
TPSM8D6B24	4V 至 16V	50A (2x25A)
TPSM8D6C24	4V 至 16V	70A (2x35A)

EXT_WRITE_PROTECT 和 PASSKEY 安全设置级别

开路

TPS546x24S 器件从 TI 工厂交付时处于“OPEN”安全状态，PASSKEY 和 EXT_WRITE_PROTECT 设置为全 00h 状态。在这种状态下，所有具有写入访问能力的命令都启用了写入功能，用户 NVM 存储可通过 STORE_USER_ALL 命令（命令代码 15h）进行访问

这种安全级别能够有效简化器件编程，并且对于早期开发阶段（可能需要快速轻松地将配置更改输入到器件中）也非常有用。

受写保护

用户可通过将 WRITE_PROTECT 或 EXT_WRITE_PROTECT 设置为非零值，而不设置位 15（硬件写保护），并将 PASSKEY 设置为解锁全 00h 状态，从而将 TPS546x24S 器件编程为受写保护状态。在这种状态下，所选命令组禁用了写入访问，但可以随时写入和更新 EXT_WRITE_PROTECT。

在开发后期或鉴定期间，这种安全级别非常有用，因为此时收费的可能性较小，而验证写保护与固件的交互对于产品验证和鉴定是必要的。

受 PASSKEY 保护

用户可通过将 WRITE_PROTECT 或 EXT_WRITE_PROTECT 设置为非零值，同时设置位 15 或位 1 (PSK)，并将 PASSKEY 设置为非零值，从而将 TPS546x24S 器件编程为受 PASSKEY 保护状态。这将使用 PASSKEY 命令防止随意写入 EXT_WRITE_PROTECT，同时仍保留 PASSKEY 和 EXT_WRITE_PROTECT 以备更改。

在早期原型设计过程中，在远程访问受限或无远程访问的系统中，或者当 TPS546x24S 器件所服务的电源轨不会造成系统损坏或被视为非关键电源轨时，这种安全级别非常有用。

硬件锁定

用户可通过将 EXT_WRITE_PROTECT 设置为非零值（包括位 15 = b’1），将 TPS546x24S 器件编程为硬件锁定写保护状态。一旦设置并存储到 NVM，就可以防止进一步写入 EXT_WRITE_PROTECT，从而防止授权用户或恶意用户通过总线访问受写保护的 PMBus 命令。如果不使用 PASSKEY，建议用户将 EXT_WRITE_PROTECT 的位 1 设置为 b’1，并将 PASSKEY 设置为 0000h，以防止将 PASSKEY 设置为未知值，以及防止更改写保护。

对于不需要更改受保护 PMBus 命令的大规模生产系统，这是建议的写保护状态。

使用受 PASSKEY 保护的非易失性存储器 (NVM) 锁定

用户可将 TPS546x24S 器件编程为这样一种状态：EXT_WRITE_PROTECT 处于非零状态，其中位 15 = b’1，位 1 = b’0，位 0（存储）= b’0，同时 PASSKEY 设置为非零状态。这可防止更改 EXT_WRITE_PROTECT，并防止更改 NVM 启动值，但允许不受 EXT_WRITE_PROTECT 保护的命令通过使用正确的 PASSKEY 解锁用户存储来更新其 NVM 设置。

双重锁定

用户可通过设置非零 PASSKEY，并设置 EXT_WRITE_PROTECT（其中位 15 = b’1，位 1 = b’1，位 0 = b’1），然后将这些值存储到 NVM，从而将 TPS546x24S 器件编程到双重锁定状态。一旦处于这种状态，EXT_WRITE_PROTECT 就会受到 EXT_WRITE_PROTECT 和 PASSKEY 的写保护，而 PASSKEY 会受到 EXT_WRITE_PROTECT 的保护，从而防止 PASSKEY 解锁。

对于寻求更高级安全特性的用户，PMBus 修订版 1.5 安全器件应用配置文件可为数字配置的器件提供对基于 256 位加密的证明和命令身份验证的访问权限，从而为用户提供验证已安装器件真实性的安全方法，以及提供允许对 PMBus 命令进行授权更新的方法，同时防止未经授权使用这些命令。EXT_WRITE_PROTECT 为用户提供了比标准 PMBus 功能具有更高分辨率的写保护功能。EXT_WRITE_PROTECT 中的每个位都提供单独且独立的 WRITE_PROTECTION。下面显示了命令配置文件和寄存器映射以供参考。

表 2. EXT_WRITE_PROTECT 命令配置文件

CMD 地址	**FBh**
写入事务	写入字
读取事务	读取字
格式	无符号二进制（2 字节）
相控	否
NVM 备份	EEPROM
更新	启动时

表 3. EXT_WRITE_PROTECT 寄存器映射

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

图例：RW = 读取/写入；R = 只读

重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265