White Paper:
The Effect of Power Failure on Disk Reliability

When using a disk drive, whether it is a flash disk or a rotating media disk, there may be repercussions due to a power failure during a disk write. The FAT file system is the prevalent standard because of its use in many desktop systems. However, the FAT file system was not designed with fault tolerance in mind. Power failures during disk writes can result in data loss, lost clusters, and invalid directory entries, all of which can make a disk drive unusable until it is fixed up or reformatted. This is the reason that applications such as CHKDSK or SCANDISK are needed on desktop PC systems. However, this is usually impractical in embedded systems.

Smaller flash disks, such as the 768k A: flash drive, are more prone to errors than larger flash disks if a power failure occurs during a disk write. Because of the small size, there are fewer flash blocks and also they are likely to be closer to being full. Both of these situations mean that a significant amount of erasing and rewriting will occur for the purposes of wear leveling. This means that writing a sector to flash will take longer and thus the chances of power failure occurring in the middle of a write are greatly increased. Note that wear leveling will copy and erase all sectors of the flash at one time or another, whether they are code, data, boot sector, or FAT. Thus, even though the application is just writing data to flash, the wear leveling code can be moving critical parts of the flash disk. It is possible that a power failure during a flash disk write can corrupt the disk to the point where a reformat is required. The chances of this occurring are reduced as the flash disk gets larger or faster.

There are a few things that can be done to make a system more reliable. The table below shows the advantages and disadvantages of various methods.

Method	Advantages	Disadvantages
Don't write to disk	No action needed	Not appropriate for all applications
Use advance power-down warning to flush data to disk	No data loss	Requires additional hardware for power-down warning (interrupt) and may require a battery for sufficient time to flush data
Use a fault-tolerant file system on the disk	Recovery is built into the operating system. Disk remains usable	Data loss still occurs (although recoverable). Not supported by all operating systems. Not supported on A: flash
Write to battery-backed RAM	Fault tolerance may be achieved by checksum or CRC. Writes are extremely fast	Requires a battery for data retention. Operating system may require special programming to allow direct access to memory. Capacity is smaller than other types of media
Output data to another system through serial port, network, or other method	Moves fault tolerance issues to another system, possibly a desktop system	Not appropriate for all applications. Requires a data connection
Accept errors	No action needed	Data loss occurs. May need to run recovery program or reformat disk

DOC1264
WPDISKREL.DOC 06/21/2004