Auf Nummer sicher

Industrie-USB-Sticks mit sicherem Langzeit-Datenerhalt und hoher Zyklenzahl

Flash-Speicher sind ein bewährtes und leicht handhabbares Speichermedium, ob als SSD, als USB-Stick oder SD-Speicherkarte. Ein prinzipbedingter Nachteil dieser Speichertechnologie ist die begrenzte Anzahl von Schreib-Lese-Zyklen, sodass häufige Speicherzyklen schneller zum Ausfall des Speichers führen. Mit neuen Speichermanagement-Technologien steuern die Hersteller von robusten Industrie-Flash-Speicherlösungen dagegen.

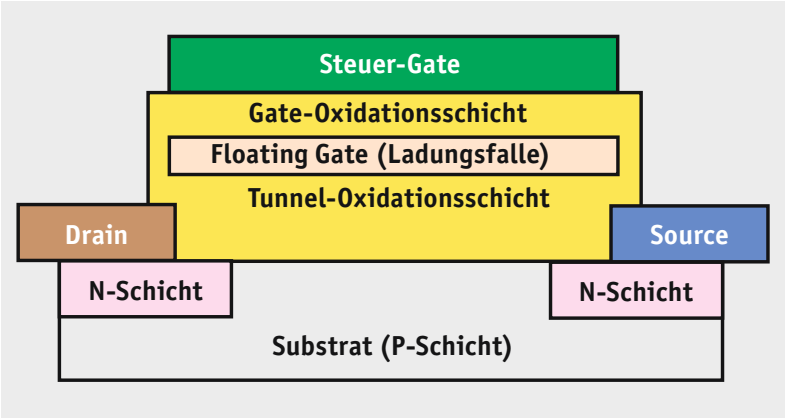

Bild 1: Der Aufbau einer MISFET-Zelle mit Floating Gate

Langlebig und zyklenfest

Nutzt man USB-Sticks im privaten Gebrauch, wird man nur selten erleben, dass diese ausfallen, sich nicht mehr lesen, beschreiben oder auch nur formatieren lassen. Das liegt an der relativ geringen Anzahl von Schreib-Lese-Zyklen, die diese Speichermedien durchlaufen müssen. Fällt ein solcher Speicherstick im Privatbereich aus, hält sich der Schaden regelmäßig in Grenzen – zumal oft die Inhalte auch auf weiteren Geräten wie einem Computer vorhanden sind. In industriellen Umgebungen allerdings können sich Ausfälle solcher Speicher fatal auswirken und hohe Schäden verursachen. Hier spielen Datensicherheit, Integrität und Stabilität eine vorrangige Rolle.

Man muss aber nicht unbedingt nur in der Industrie suchen: Auch im semiprofessionellen und privaten Bereich erlangen die genannten Eigenschaften eine immer höhere Priorität. Ein Beispiel ist etwa das Smart Home. Die meisten Zentralen dieser Systeme, so auch die CCU-Reihe von eQ-3, sind Linux-Systeme, die im internen Speicher Betriebssystem und Firmware enthalten. Zusätzliche Daten, beispielsweise von Daten-Logging-Anwendungen, Konfigurationen, Sensordaten, und eigene Programme werden bei solchen Systemen auf externe Speicher, SD-Karten oder USB-Speichermedien ausgelagert. Wenn, wie beim Raspberry Pi, diese Speichermedien auch die Betriebssystemdaten enthalten und dazu dieser Speicher auch noch für häufige Schreib-Lese-Zyklen benutzt wird, ist ein relativ schneller Ausfall des Speichermediums vorprogrammiert.

Deshalb kann hier der Einsatz eines Industrie-Flash-Speichers eine gute Investition in die Daten- und Betriebssicherheit des Gesamtsystems sein. Denn diese Speicher sind auf besonders viele Zyklen und hohe Datensicherheit spezialisiert.

Bild 2: In den höher integrierten Apacer-Industrie-USB-Sticks sind selektierte MLC-Chips von Toshiba/Kioxia verbaut. Bild: Toshiba Memory/Kioxia

Flash-Speicher – die geladenen Bits

Betrachten wir zunächst einmal die Grundfunktion des Flash-Speichers. Er beruht auf der nichtflüchtigen Speicherung von Informationen, wie man sie vom EEPROM (Electrically Erasable Programmable Read-Only Memory) kennt. Er benötigt also im Gegensatz zu anderen Speichertechnologien nicht ständig Strom zum Datenerhalt. Der Ursprung des Flash-Speichers manifestiert sich so auch im fachlich exakten Namen Flash-EEPROM. Wie funktioniert dieser?

Die Flash-Speicherzelle basiert auf einem quantenmechanischen Effekt von Halbleitern, hier speziellen MOSFETs, die zusätzlich zu den üblichen Bestandteilen eines MOSFETs, also Gate, Drain und Source, die den Elektronenfluss zwischen verschiedenen N- und P-Schichten (Kanal) realisieren, ein sogenanntes Floating Gate (Bild 1) aus Polysilizium enthalten. Dieses Floating Gate ist durch ein Dieelektrikum (Oxidationsschicht) sowohl vom Gate als auch vom Kanal zwischen Drain und Source isoliert.

Diese spezielle Ausführung des MOSFETs wird MISFET (Metal Isolator Solid State Field Effect Transistor) genannt. Jeder MISFET bildet eine Bit-Speicherzelle, die die als elektrischen Impuls über den sogenannten quantenmechanischen Tunneleffekt (Beschleunigung der Elektronen bei Anlegen einer Spannung zwischen Drain und Source und Laden des Floating Gates) eingeschriebene Information als elektrische Ladung auf dem Floating Gate hält. Diese elektrische Ladung erzeugt intern ein elektrisches Feld, das über den Ladungskanal zwischen Source und Drain ausgelesen wird, ohne dabei die Information auf dem Floating Gate zu löschen. Dies erfolgt erst durch das Anlegen einer hohen, negativen Löschspannung.

Moderne Flash-Speicher, wie wir sie heute mit enorm hohen Speicherdichten auf kleinstem Raum kennen, arbeiten dabei nach einem modifizierten Prinzip, Charge Trap Flash genannt. Hier wird die Ladung nicht auf dem beschriebenen Floating Gate gehalten, sondern auf Haftstellen (Trap) aus Silziumnitrid, die vom Kanal durch eine Tunneloxidschicht getrennt sind.

Schließlich unterscheidet man bei den Flash-Speichern noch zwischen der SLC- und MLC-Technik. Bei SLC-Zellen (Single Level Cell) wird genau ein Bit je Zelle gespeichert, also entweder 0 oder 1.

Bei MLC (Multi Level Cell) bzw. den Dreifach- und Vierfach-Zellen (TLC/QLC) speichert die Zelle durch das Anlegen genau definierter Ladungspegel zwei und mehr Bit pro Zelle. So kann dann die einfachste MLC bereits in einer Zelle die Binärwerte 00, 01, 10 und 11 speichern.

Bei den höher integrierten Apacer-Industrial-Sticks setzt Apacer z. B. Toshiba- (heute Kioxia) selektierte MLC-NANDs (Bild 2) ein und erreicht damit eine besonders hohe Speicherdichte. Hier speichert jede Zelle über acht Ladungspegel 3 Bits und damit acht Binärwerte je Zelle.

Diese Technik erfordert allerdings ein ausgefeiltes und leider auch zeitaufwendiges Lade-/Entlademanagement, sodass die Lese-/Schreibgeschwindigkeit gegenüber SLC sinkt.

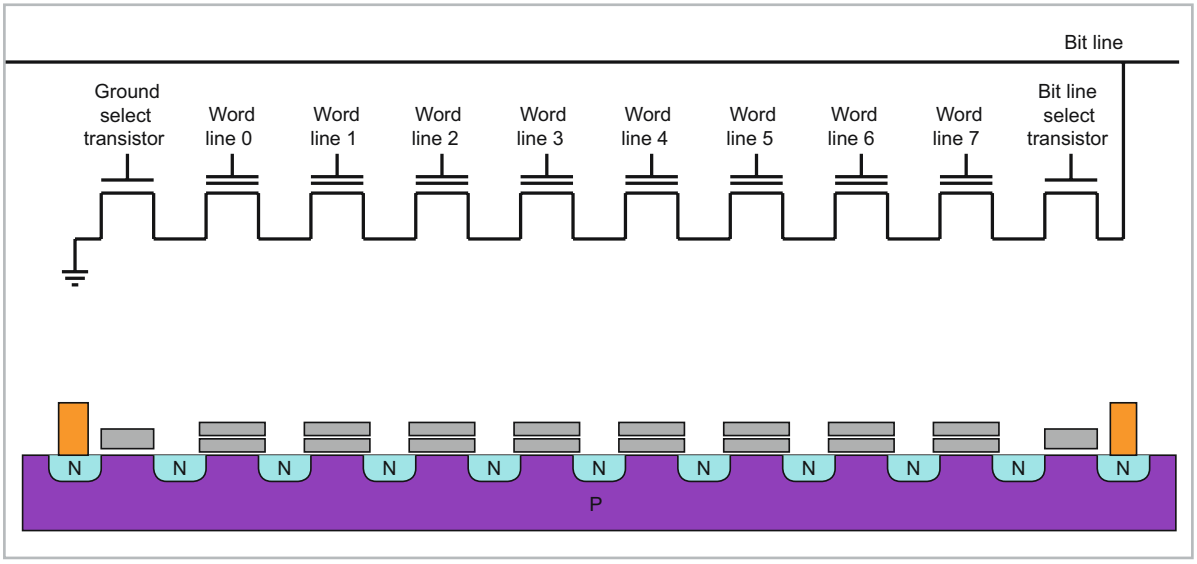

Bild 3: Aufbau und Struktur einer NAND-Zelle. Die einzelnen MOSFETs einer Zelle liegen in unterschiedlichen Seiten (Pages) innerhalb eines Blocks. Grafik: Cyferz in der Wikipedia auf Englisch, CC BY 2.5 [1]

Der NAND-Speicher

Die Speicherzellen eines Flash-Speichers, der bei den mobilen Speichern als NAND-Speicher ausgeführt ist, sind seriell angeordnet (Bild 3). Die Organisation dieser Speicherart erfolgt dabei Seiten- (Page) und Block-orientiert. Seiten bestehen aus bis zu 8 kBytes, sie sind wiederum zu mehreren Seiten in einem Block organisiert.

Bei der Fertigung der Speicher ist es nicht zu vermeiden, dass bereits in der Produktion defekte Blöcke auf dem Speicher vorhanden sind. Diese werden vom Speichermanagement des immer zugehörigen NAND-Controllers registriert und im späteren Speichermanagement mit Fehlerkorrekturalgorithmen umgangen. Diese Bad-Block-Tabellen enthalten auch später durch das Speichermanagement registrierte Bitfehler.

Hoher Verwaltungsaufwand für mehr Sicherheit und längere Haltbarkeit

Durch die Umladeeffekte im Bereich des Floating Gates bzw. der Traps wird die extrem dünne Isolationsschicht zu Kanal und Gate mit der Zeit geschädigt (Degeneration), bis hin zum Ausfall der Speicherzelle durch Fortfall der Oxidationsschicht. Je nach Technologie sind zwischen 3000 und mehr als eine Million Schreib-Lese-Zyklen je Zelle erreichbar. Das Speichermanagement sortiert dabei über integrierte Fehlerkorrekturalgorithmen systematisch einzelne defekte Zellen aus und schreibt die Daten auf Reservebereiche (Bad Block Replacement), Schutzbits bzw. Spare Area genannt.

Bei Fehlern in ganzen Bitreihen werden aufgrund der NAND-Organisationsstruktur der komplette Block gesperrt und die Daten durch den Speichercontroller umgelagert. Dabei wird logischerweise der verfügbare Speicherraum im Speicherbaustein immer geringer, bis der Speicher irgendwann unbrauchbar ist, da er zu viele Defektblöcke enthält.

Dieser Effekt ist auch bei modernsten Speichern nicht vermeidbar, man kann ihn aber ganz wesentlich hinauszögern, indem man ein ausgefeiltes Speichermanagement einsetzt.

So wird zum Beispiel die Echtzeit-Überwachungs-Softwarelösung S.M.A.R.T. eingesetzt, um die Nutzungsdaten des USB-Sticks kontrollieren zu können. Dabei werden die Gesamtzahl der beschädigten Blöcke ebenso überwacht wie die benötigten Lösch-, Lese- und Schreibzeiten sowie Lebensdauerprognosen erstellt. Diese Daten ermöglichen es dem Nutzer bzw. Systemadministrator, sich anbahnende Datenschäden rechtzeitig und im Echtzeitbetrieb zu erkennen. Über die S.M.A.R.T.-Software wird das zu erwartende Ende der Lebensdauer recht sicher analysiert. Bei den Apacer-MLC-NANDs sind dies 3000 P/E-Zyklen (Program/Erase-Zyklen), die der Hersteller garantiert, damit ist dann auch das Ende der Gewährleistung definiert. 3000 Zyklen klingt wenig, man darf diese Zahl aber nicht mit den gesamt möglichen Zellen-Schreib-Lese-Zyklen verwechseln. P/E-Zyklen sind vollständige durchschnittliche Löschzyklen des Gesamtspeichers (Average Erase Count). Im Vergleich dazu erreichen normale Consumer-Speicher bis zu 300 P/E-Zyklen.

Die integrierte Firmware arbeitet mit einem Fehlerkorrekturverfahren (ECC), das potenziell ungewöhnliche Änderungen und Korrekturen sofort erkennt, um das Schreiben falscher Daten zu vermeiden. Darüber hinaus kann das Verwaltungspersonal benutzerdefinierte Schreibschutzmechanismen nutzen, um Schreibschutzsektoren individuell zu konfigurieren und das Schreiben, Verändern und Löschen von Daten einzuschränken. So kann man auch in Zusammenarbeit mit dem Kunden spezielle Schutzmechanismen gegen Datenlecks einbauen, indem z. B. das nicht autorisierte Lesen und Schreiben verhindert wird und spezifische Verschlüsselungen sowie Produktidentifizierungscodes eingesetzt werden.

Unter Einsatz des exklusiven Hersteller- und Produktidentifikationscodes (VID/PIC) haben Unternehmen die Möglichkeit, den Schutz noch zu verbessern. Werksseriennummern binden darüber hinaus die USB-Produkte an bestimmte Geräte, um die Nutzung nachverfolgen und den Zugriff durch andere Geräte einschränken zu können.

In der Spieleindustrie helfen diese Eigenschaften dabei, Risiken zu vermeiden, die bei einem Materialwechsel auftreten, und Schwierigkeiten aus dem Weg zu gehen, die bei einer erneuten Überprüfung von Zertifizierungen auftreten können.

Eine der wichtigsten Techniken der intelligenten Speicherverwaltung und Lebensdauerverlängerung des Gesamtspeichers ist die Wear-Leveling-Funktion (Bild 4). Dabei sorgt die Speicherverwaltung für eine gleichmäßige Belegung aller Speicherzellen des Speichers, um dessen „Abnutzung" auszugleichen. Im Normalfall nutzt die Speicherverwaltung immer wieder die gleichen Blöcke, sobald diese einmal gelöscht und somit frei sind. So erhöht sich deren Degeneration, während andere Zellen bzw. Blöcke vielleicht bis zum Ausfall des Speichers nie beschrieben worden sind. Beim Wear Leveling ermittelt die Speicherverwaltung intern über eine Zuordnungstabelle die bisher nicht oder nur wenig genutzten Blöcke und beschreibt zuerst diese mit neuen Daten. So wird eine gleichmäßige Degeneration über den gesamten Speicher hinweg erreicht.

Das Wear Leveling, das mit verschiedenen Verteilungsalgorithmen (dynamisch/statisch/global, siehe [2]) betrieben wird, ist mit in die o. a. Gesamtstrategie zur Überwachung des Speichers eingebunden, bietet so eine frühzeitige Warnung des Nutzers vor finalem Verschleiß und ermöglicht ihm damit eine rechtzeitige Datensicherung. Dass diese Art der Datenverwaltung extrem komplex ist, kann man leicht nachvollziehen, entsprechend hoch ist der controllerseitige Aufwand und auch hier wird wieder die Schreib-/Lesegeschwindigkeit beeinträchtigt. Diese spielt aber im Industrieeinsatz eher selten eine herausragende Rolle, hier sind Datensicherheit und Datenintegrität wichtiger. Die hier erreichbaren Lese-/Schreibgeschwindigkeiten von bis zu 200 MB/s und 100 MB/s sind dennoch hoch genug für die meisten Anwendungen.

USB-Stick-Anwender kennen das gelegentlich auftretende Phänomen, dass es zu Datenverlusten kommen kann, wenn man einen USB-Stick einfach aus dem Gerät zieht, ohne ihn zuvor dem „Auswerfen" zu unterziehen. Noch schlimmer kann es kommen, wenn bei Schreib- und Lesevorgängen die Stromversorgung instabil ist oder gar (unbemerkt) ausfällt. Auch hierzu bieten Industrial-Sticks einen Fehlervermeidungsalgorithmus (Power Failure Management), der dies erkennt, Operationen definiert abschließt und eine Fehlermeldung im Analysesystem hinterlegt.

Letztlich spielt auch die Robustheit im industriellen Einsatz eine Rolle. Industrial-USB-Sticks sind mechanisch so ausgeführt, dass sie die strengen Militärnormen MIL-STD810G/MIL-STD202G erfüllen, die enorm hohe Anforderungen an Kriterien wie Stoßfestigkeit (bis zu 50 G (aktiver Betrieb)/1500 G (inaktiver Betrieb)), mechanische Stabilität und Umweltbedingungen stellen.

Die bei ELV angebotenen Apacer-Industrial-Sticks [3] mit Flash-Speicher auf MLC-Basis bieten ca. 3000 P/E-Zyklen anstatt der im Konsumentenbereich üblichen 300 P/E-Zyklen und damit eine ca. 10-fach höhere Haltbarkeit und Sicherheit der Schreib-Lese-Zyklen gegenüber Konsumenten-USB-Sticks. Mit einer hohen Schreib-/Lesegeschwindigkeit (95 MB/s und 190 MB/s), einer Haltbarkeit/Sicherheit der gespeicherten Daten gegenüber Datenverlust von bis zu zehn Jahren und einer MTBF (Meantime Between Failure) von bis zu 1.000.00 h stellen sie bei einem Betriebstemperaturbereich von 0 °C bis 70 °C in ihrem robusten Metallgehäuse ein zuverlässiges USB-Speichermedium dar. ELV

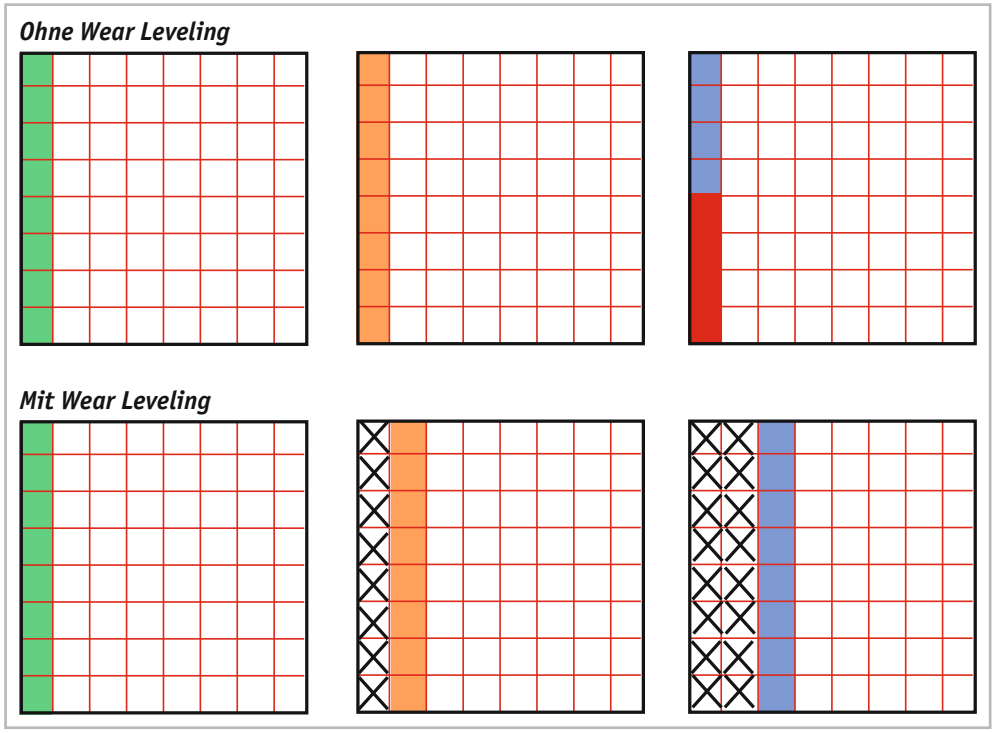

Bild 4: Das Wear-Leveling in symbolischer Darstellung:
Oben ist das „Speicherleben" ohne Wear Leveling zu sehen: Der Controller beschreibt zunächst einen Block im ersten Durchgang (grün). Wird dieser gelöscht, erfolgt das Beschreiben quasi wieder von Adresse null aus in gleicher Weise (orange). Haben nun einzelne Zellen durch das wiederholte Beschreiben ihr Lebensdauerende erreicht, fallen sie aus (rot) und der Block kann nicht mehr vollständig genutzt werden (blau) – er fällt vorzeitig aus, während andere Blöcke vielleicht noch nie genutzt wurden.
Beim Wear Leveling (unten) werden gelöschte Blöcke zunächst nicht beschrieben (Kreuze), sondern bisher nicht genutzte Blöcke benutzt, sodass alle Zellen gleichmäßig eingesetzt werden.

Weitere Infos:

[1] NAND-Zellstruktur
https://commons.wikimedia.org/w/index.php?curid=4571172
[2] Wear Leveling
https://en.wikipedia.org/wiki/Wear_leveling
[3] Apacer Industrial-USB-Sticks im ELVshop
https://de.elv.com: Artikel-Nr. 251458 (8 GB), Artikel-Nr. 251462 (128 GB)

Alle Links finden Sie auch online unter: de.elv.com/elvjournal-links