ECEN 5823-001
Internet of Things Embedded Firmware

Lecture #17

23 October 2018

Be Boulder.

University of Colorado Boulder

Agenda

- Class Announcements
- Reading Assignment
- Course Project
- Quiz 7 Review
- Mid-term Review
- Memory for embedded applications

Class Announcements

- Quiz 8 due on Sunday, October 28th, at 11:59pm
  - This may be pushed to Wednesday, October 31st depending on how far I get in lecture on Thursday
- Course Project Proposal due Sunday, October 28th, at 11:59pm
- Based on class grades after mid-term, at this time no curve is planned

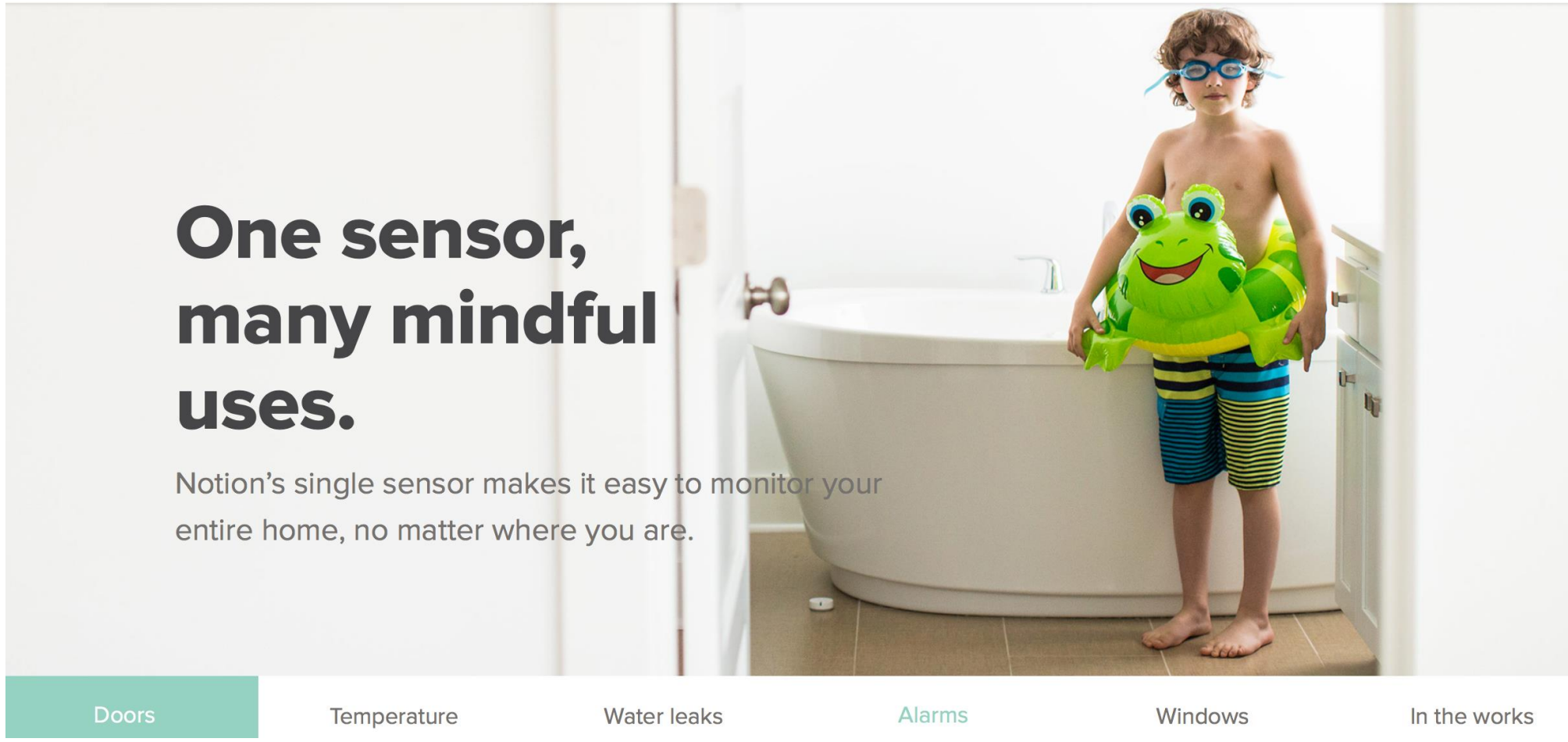
ECEN5823, -001B– Reading List
Internet of Things Embedded Firmware
Week 9

Reading Assignment

Note: The required reading below will be on Quiz 8 as well as lecture material

1. MSP430 Flash Memory Characteristics–SLAA334A
   http://www.ti.com/lit/an/slaa334a/slaa334a.pdf
2. NAND Flash Data Retention Embedded Systems
   https://cdn.selinc.com/assets/Literature/Publications/White%20Papers/0015_NANDflash_IO_20141211.pdf?v=20170217-161047
3. Bluetooth blog: In-Market Bluetooth Low Energy Devices and Bluetooth Mesh Networking by Martin Woolley
   a. http://blog.bluetooth.com/in-market-bluetooth-low-energy-devices-and-bluetooth-mesh-networking
4. Bluetooth blog: Bluetooth Mesh Security by Martin Wooley
   a. https://blog.bluetooth.com/bluetooth-mesh-security-overview

notion


One sensor, many mindful uses.
Notion's single sensor makes it easy to monitor your entire home, no matter where you are.
Doors
Temperature
Water leaks
Alarms
Windows
In the works

Course Project Proposal

ECEN 5823
Project Proposal Assignment
Fall 2018

Objective: To define and develop the scope of the Course Project in ECEN 5823, Fall 2018. The purpose of the course project is to further learn and develop your skills using Bluetooth Smart and/or Bluetooth Mesh

Note: You can use as much or as little of your previously developed code for ECEN 5823.

Project Proposal Due Date: Sunday, October 28th, at 11:59pm via D2L drop box

Three project options:

Course Project Proposal

ECEN 5823
Project Proposal Assignment
Fall 2018

Objective: To define and develop the scope of the Course Project in ECEN 5823, Fall 2018. The purpose of the course project is to further learn and develop your skills using Bluetooth Smart and/or Bluetooth Mesh

Note: You can use as much or as little of your previously developed code for ECEN 5823.

Project Proposal Due Date: Sunday, October 28th, at 11:59pm via D2L drop box

Three project options:

SILICON LABS | SUPPORT & COMMUNITY

Search silabs.com

MCUs | Wireless | More Products | Development Tools | Expert's Corner

Bluetooth ›

Zigbee & Thread ›

Proprietary ›

Wi-Fi ›

Multi-Slave Multi-Master Dual-Topology example

Follow

12/01/2016 | 01:58 pm

tmonte
Employee

Introduction

Course Project Time Line

- Course Project will comprise of the following deliverables
  - Project Proposal - due EOD Sunday, October 28th
  - Project Status Update 1 – due EOD Sunday, November 11th
    - Will include detailed flow chart
  - Project Status Update 2 – due EOD Tuesday, November 27th
  - Demo – due December 7th thru the 13th up to class time on the 13th
  - Final Report – due at demo

Extra Credit opportunities

	Towards final grade
• Bluetooth type of project (by November 18th)	+1.875 pts
• Mesh – Group messaging + Unicast + hopping	
• Early Demo	
• Project must be completely functional to receive this credit	
• Demo-ed 12/7 – 12/9	+2 pts
• Demo-ed 12/10 – 12/11	+1 pt

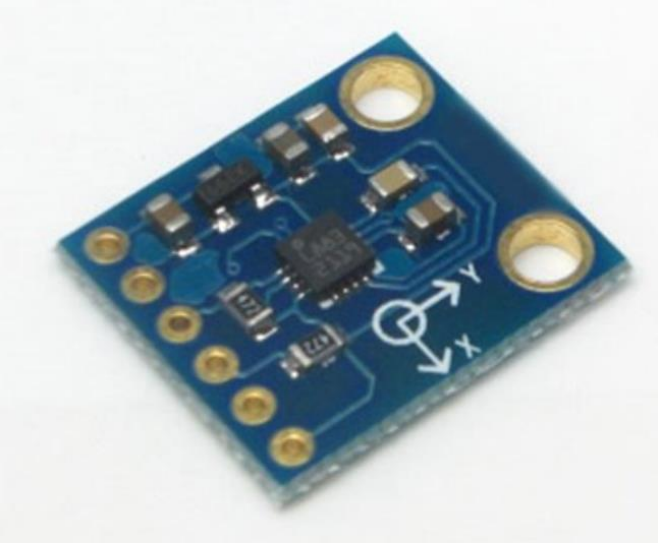
- Towards final grade clarification
  - If your final grade is an 86.5%, B, plus 3.875pts towards your final grade, your final grade would become a 90.375% or A-

Course Project credit breakdown (tentative)

- Project proposal 5.0% of course project grade
- Status report 1 10.0%
- Status report 2 5.0%
- Final project /Demo 75.0%
  - Detail breakdown will be provided at a later date
- Project Report 5.0%
  - Total 100.0%

Sensor examples

- 3-axis Magnetometer
  - GY-271 HMC5883L Triple Axis Compass Magnetometer Sensor Module



FEATURES	BENEFITS
3-Axis Magnetoresistive Sensors and ASIC in a 3.0x3.0x0.9mm LCC Surface Mount Package	Small Size for Highly Integrated Products. Just Add a Micro-Controller Interface, Plus Two External SMT Capacitors Designed for High Volume, Cost Sensitive OEM Designs Easy to Assemble & Compatible with High Speed SMT Assembly
12-Bit ADC Coupled with Low Noise AMR Sensors Achieves 2 milli-gauss Field Resolution in ±8 Gauss Fields	Enables 1° to 2° Degree Compass Heading Accuracy
Built-In Self Test	Enables Low-Cost Functionality Test after Assembly in Production
Low Voltage Operations (2.16 to 3.6V) and Low Power Consumption (100 µA)	Compatible for Battery Powered Applications
Built-In Strap Drive Circuits	Set/Reset and Offset Strap Drivers for Degaussing, Self Test, and Offset Compensation
I^2C Digital Interface	Popular Two-Wire Serial Data Interface for Consumer Electronics
Lead Free Package Construction	RoHS Compliance
Wide Magnetic Field Range (+/-8 Oe)	Sensors Can Be Used in Strong Magnetic Field Environments with a 1° to 2° Degree Compass Heading Accuracy
Software and Algorithm Support Available	Compassing Heading, Hard Iron, Soft Iron, and Auto Calibration Libraries Available
Fast 160 Hz Maximum Output Rate	Enables Pedestrian Navigation and LBS Applications

Picture from Amazon.com and data from Honeywell's HMC5883L data sheet

Sensor examples

- Barometric Pressure Temperature Sensor
  - BME280 Pressure Temperature Sensor Module with I2C

Key parameters

- Pressure range — 300 … 1100 hPa (equiv. to +9000…-500 m above/below sea level)
- Package — 8-pin LGA metal-lid; Footprint : 2.0 × 2.5 mm², height: 0.95 mm
- Relative accuracy (950 … 1050hPa @25°C) — ±0.12 hPa, equiv. to ±1 m
- Absolute accuracy (950 …1050 hPa, 0 …+40 °C) — typ. ±1 hPa
- Temperature coefficient offset (25 … 40°C @900hPa) — 1.5 Pa/K, equiv. to 12.6 cm/K
- Digital interfaces — I²C (up to 3.4 MHz); SPI (3 and 4 wire, up to 10 MHz)
- Current consumption — 2.7µA @ 1 Hz sampling rate
- Temperature range — -40 … +85 °C
- RoHS compliant, halogen-free
- MSL 1

Sensor supply voltage	V_{DD}	ripple max. 50mVpp	1.71	1.8	3.6	V
Interface supply voltage	V_{DDIO}		1.2	1.8	3.6	V

Picture from Amazon and Key parameters from Bosch BME280 data sheet

Sensor examples

- 3-axis accelerometer
  - SparkFun Triple Axis Accelerometer Breakout - MMA8452Q

MMA8452Q

Features

- 1.95V to 3.6V supply voltage
- 1.6V to 3.6V interface voltage
- ±2g/±4g/±8g dynamically selectable full-scale
- Output Data Rates (ODR) from 1.56 Hz to 800 Hz
- 99 µg/√Hz noise
- 12-bit and 8-bit digital output
- I^2C digital output interface
- Two programmable interrupt pins for six interrupt sources
- Three embedded channels of motion detection
  - Freefall or Motion Detection: 1 channel
  - Pulse Detection: 1 channel
  - Transient Detection: 1 channel
    - Orientation (Portrait/Landscape) detection with set hysteresis
    - Automatic ODR change for Auto-WAKE and return to SLEEP
    - High-Pass Filter Data available real-time
    - Self-Test
    - RoHS compliant
    - Current Consumption: 6 µA to 165 µA

Photo from the Sparkfun.com and the MMA8452Q features from its NXP data sheet

Sensor examples

- Gesture sensor
  - Sparkfun

- Features •
  - Ambient Light and RGB Color Sensing - UV and IR blocking filters
  - Proximity Sensing
    - Programmable driver for IR LED current - Saturation indicator bit
  - Complex Gesture Sensing
    - Four separate diodes sensitive to different directions
    - Interrupt driven I2C communication
  - I2C-bus Fast Mode Compatible Interface
    - Data Rates up to 400 kHz
    - Dedicated Interrupt Pin

Parameter	Symbol	Min	Typ	Max	Units	Test Conditions
IDD supply current [1]	I_{DD}		200	250	µA	Active ALS state PON = AEN = 1, PEN = 0
			790			Proximity, LDR pulse ON, PPulse = 8 (I_{LDR} not included)
			790			Gesture, LDR pulse ON, GPulse = 8 (I_{LDR} not included)
			38			Wait state

ECEN 5823-001
Internet of Things Embedded Firmware
Preliminary 10/20/2018
Fall 2018

Course Project Preliminary Rubric

Team Members: _____

Date: _____

		Points
Demonstrates theory, skills, and technology of project (20pts)		_____
Correctly programs requested code	_____ (10 pts)	
Correctly walks through code	_____ (5 pts)	
Demonstrates knowledge during code walk through	_____ (5 pts)	
Blue Gecko demonstrated operating in low energy (10 pts)		_____
Low Energy demonstrated using Energy Profiler	_____ (5 pts)	
Clearly described low energy principles implemented	_____ (5 pts)	

- Mesh: Friend storing messages for the Low Power node

Quiz 7 review

The low-power note continues sending Friend Poll messages until the friend node [Select] ▾

.

Quiz 7 review

Select which statement best belongs to an average or star performer.

getting noticed through slick power point presentations	[Choose]
using long-winded memos focused on their image and message	[Choose]
Selecting the right message for a particular audience	[Choose]
Selecting the right audience for a particular message	[Choose]

Quiz 7 review

To be a start performer, match the following:

Always a leader	[Choose]
Center of attention	[Choose]
alert your leader of trouble spots	[Choose]
sounding board to your leader	[Choose]
challenge your leader's decisions	[Choose]

Quiz 7 review

What differentiates a star performer leader from other types of leaders?

- do not assume that they know everything about other people
- they are not different than other leaders
- knows best for their followers at all times
- are omniscient

Quiz 7 review

A star performer's network is accomplished by ... (select all that apply)

- [ ] meeting experts at conferences
- [ ] group emails
- [ ] LinkedIn
- [ ] one-to-one interactions

Quiz 7 review

Star performers understand that leadership needs to take into account the following... (select all that apply)

- [ ] focused on their own work styles
- [ ] focused on their own ideas
- [ ] co-workers aspiration and needs
- [ ] interpersonal relationships of the team

Quiz 7 review

When a friend node receives a message for its low-power nodes, it is stored in an area called the [twowords].

Quiz 7 review

The average performer normally gets the wrong answer more frequently because ...

- ask the wrong people
- ask the work people or the right people are not in the network
- right people are not in the network
- they usually do get the right answer

Quiz 7 review

In the paper, "How to be a star engineer," select all the characteristics that were determined to be vital to be a high performer?

- [ ] organizational
- [ ] cognitive
- [ ] social
- [ ] willingness to help others
- [ ] psychological

Quiz 7 review

List the order of events in the Bluetooth Mesh network provisioning process.

Authentication	[Choose]
Exchanging public keys	[Choose]
Beacon	[Choose]
Invitation	[Choose]
Distribution of the provisioning data	[Choose]

Quiz 7 review

A star performer leader asks which type of questions?

- [ ] open-ended questions
- [ ] leading questions
- [ ] yes/no questions
- [ ] conversation starting questions

Quiz 7 review

In "How to be a star engineer," match the view of leadership by the type of performer.

Big vision	[Choose]
Big charisman	[Choose]
Making mostly key decisions	[Choose]
Helping a group create a clear vision	[Choose]
Finding resources to accomplish a tash	[Choose]
Guiding a project to successful completion	[Choose]

Quiz 7 review

To get ideas addressed, star performers will take their ideas directly to upper management bypassing their manager.

- True
- False

Mid-Term review

An IC's onboard ESD diodes are designed to protect the IC from which of the following type of events?

- [ ] Positive electrostatic discharge
- [ ] Bus contention due to multiple devices driving the I/O line
- [ ] Lightning strike
- [ ] Negative electrostatic discharge

Mid-Term review

Match which characteristic belongs best to a consumer versus an industrial Internet of Things device

20C to 40C operating temperature range	[Choose]
Priority is high reliability	[Choose]
Bluetooth Smart	[Choose]
Product life cycle > 25 years	[Choose]
Warranty < 1 year	[Choose]

Mid-Term review

Match the Blue Gecko's peripheral to its lowest energy mode of operation

CPU	[Choose]
I2C0 as the only master on the I2C bus	[Choose]
GPIO	[Choose]
LETIMER0	[Choose]
TIMER0	[Choose]

Mid-Term review

Complete the following C-code programming instruction to disable interrupts on warm up completed, WARMUP, in the ACMP interrupt enable register using good programming practices.

ACMP->IEN

Mid-Term review

Match the following low energy microcontroller characteristics to either an architectural decision by the design team or a feature that the low energy firmware engineer can take advantage

Well architected energy modes	[Choose]
Ultra Low Power Sleep Modes	[Choose]
Autonomous peripherals	[Choose]
Current Monitors	[Choose]
Higher and more efficient computational CPUs	[Choose]

Mid-Term review

One method to get around the high standby current of an active sensor is to turn it off when not in use by using a method called _____ (three word answer).

Mid-Term review

In Bluetooth Classic and Bluetooth Smart, a profile defines the behavior of both the master and slave.

- True
- False

Mid-Term review

Complete the following C-code programming instruction to clear just the WARMUP interrupt while in the ACMP ISR using good programming practices.

ACMP->IFC

Mid-Term review

Select all that apply or that are generally true regarding interrupts on an ARM Cortex-M4 micro controller by default

- [ ] The Cortex-M4 utilizes a vector interrupt architecture
- [ ] Interrupts are cleared upon reading the peripheral's interrupt flag, IF, register
- [ ] For an interrupt to be triggered, both the Interrupt Enable bit in the peripheral's IEN register needs to be set as well as the peripheral's interrupt needs to be enable in the NVIC register, Nested Vector Interrupt Controller.
- [ ] If an interrupt occurs while the interrupts are disabled to the processor by using CORE_ATOMIC_IRQ_DISABLE(), these interrupts are lost

Mid-Term review

Making an operation atomic by disabling interrupts can increase _____ (single word answer) latency which may negatively impact _____ systems.

Mid-Term review

If you are viewing the Energy Profiler of the Blue Gecko whose HFXO is running at 38MHz, and you measure the current to be 4.0uA, what energy state is it in?

- EM3
- EM2
- EM1
- EM0

Mid-Term review

Match all the following possible design considerations to the need of the system

Simpler designs	[Choose]
Making decisions on the Industrial Internet of Things device	[Choose]
Utilizing higher quality components	[Choose]
Driving processing power to the cloud	[Choose]

Mid-Term review

If you are viewing the Energy Profiler of the Blue Gecko running at 38MHz, and you measure the current to be 3.0mA, what energy state is it in?

- EM3
- EM2
- EM0
- EM1

Mid-Term review

What is the slave's system latency when the Connection Interval is set to 25mS and the Slave Latency is set to 4?

- 175mS
- 140mS
- 25mS
- 70mS
- 210mS
- 105mS

Mid-Term review

Match the following low energy microcontroller characteristics to reducing energy by either power or time

Inter peripheral communications	[Choose]
Higher frequency / higher efficiency CPU	[Choose]
Well architected energy modes	[Choose]
Autonomous peripherals	[Choose]

Mid-Term review

Why is scheduling the serving of interrupts required in Bluetooth Smart SoCs?

Mid-Term review

In programming a low energy micro controller, select all that would apply to achieve the lowest energy.

- [ ] Selecting 10MHz operation due to CMOS energy consumption is directly proportional to its frequency instead of 20 MHz
- [ ] Utilize DMA to retrieve data from a UART reception
- [ ] Poll the ADC to determine when the ADC conversion is completed
- [ ] Operate the I2C bus at 400KHz instead of 100KHz
- [ ] Disable all unused peripheral clocks

Mid-Term review

Match the Blue Gecko's peripheral to its lowest energy mode of operation

CPU	[Choose]
I2C0 as the only master on the I2C bus	[Choose]
GPIO	[Choose]
LETIMER0	[Choose]
TIMER0	[Choose]

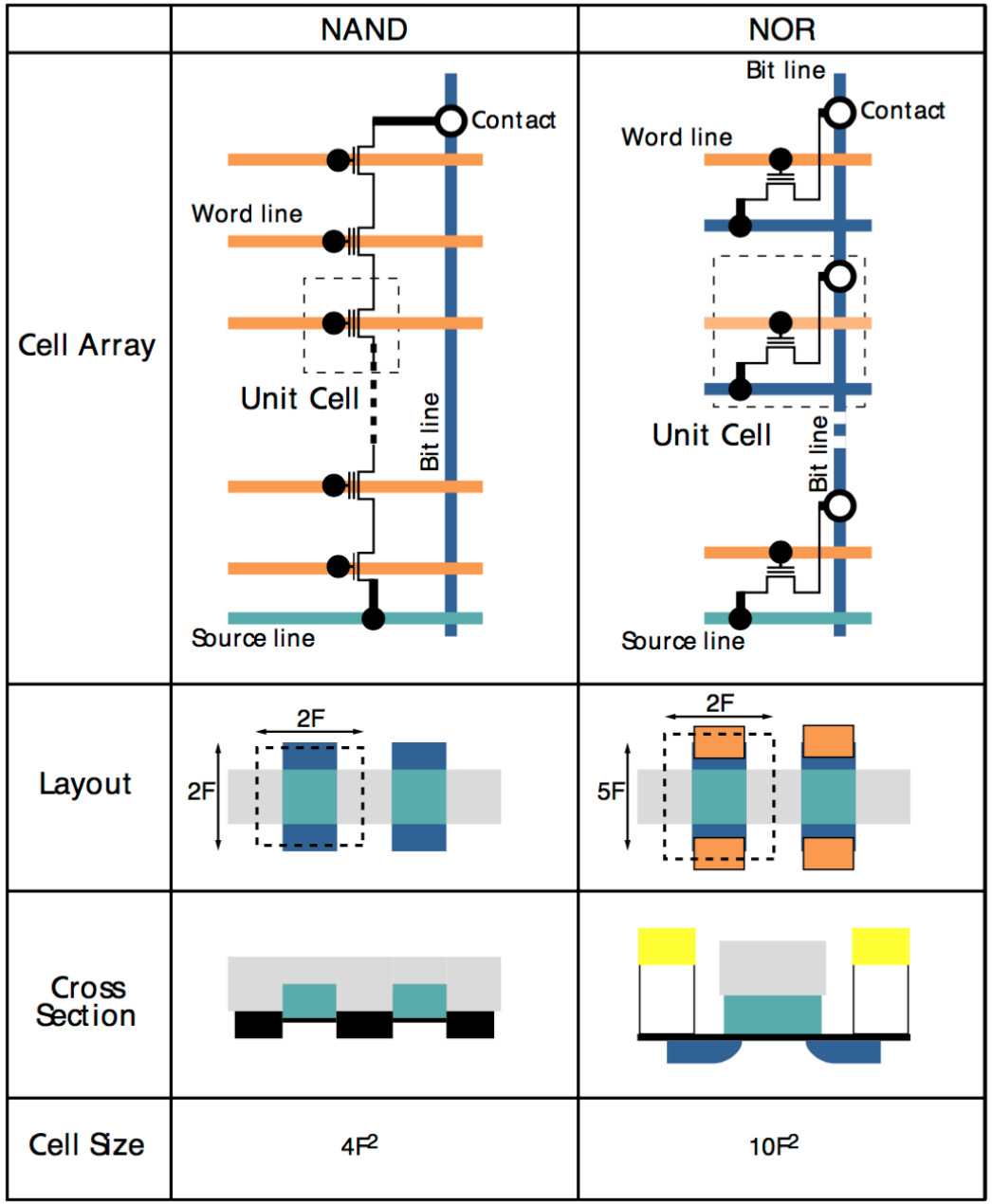
Differences between NOR and NAND Flash

- NOR
  - Quick random access to any memory location
  - 100% known good bits for the life of the part
  - Good for direct code execution
  - Fast program and erase cycles
  - Density: 1Mbit – 2Gbit
  - Larger cell and more expensive

- NAND
  - Slow initial access read access, then faster sequential reads
  - 98% bits are good when new and additional bits fail over time (ECC is required)
  - Good for data storage
  - Slower program and erase cycles
  - Density: 128Mbit – 1Tbit
  - Smaller cell and less expensive
  - SLC, MLC, TLC, 3d technologies

FLASH cell construction

- F = feature size
- NOR is 2.5x NAND cell size
- NAND Flash is very similar to a hard-disk drive. It is sector-based (page-based) and well suited for storage of sequential data. Random access can be achieved at the system level by shadowing the data to RAM, requiring RAM storage.

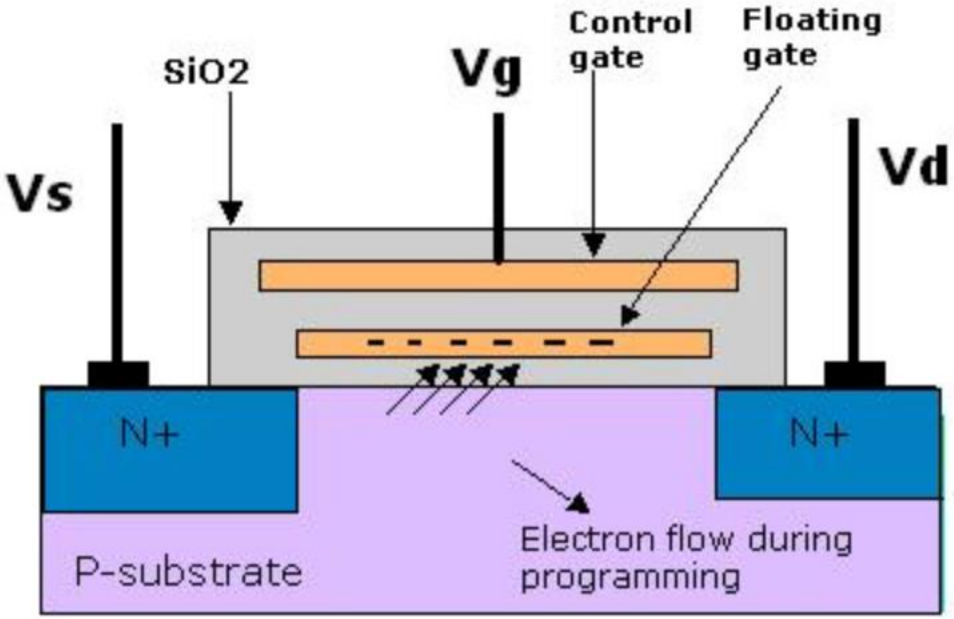


What type of FLASH for your controller

- Microcontroller
  - Smaller code size
  - NOR based
    - Fast random access to memory locations
    - Fast access times
    - All good bits
- Microprocessor or DSP
  - Larger code size
  - NAND based and moving to eMMC
    - Download executable code into SRAM for execution
    - Need ECC support to handle bad bits
    - Lower cost for larger code and storage requirements

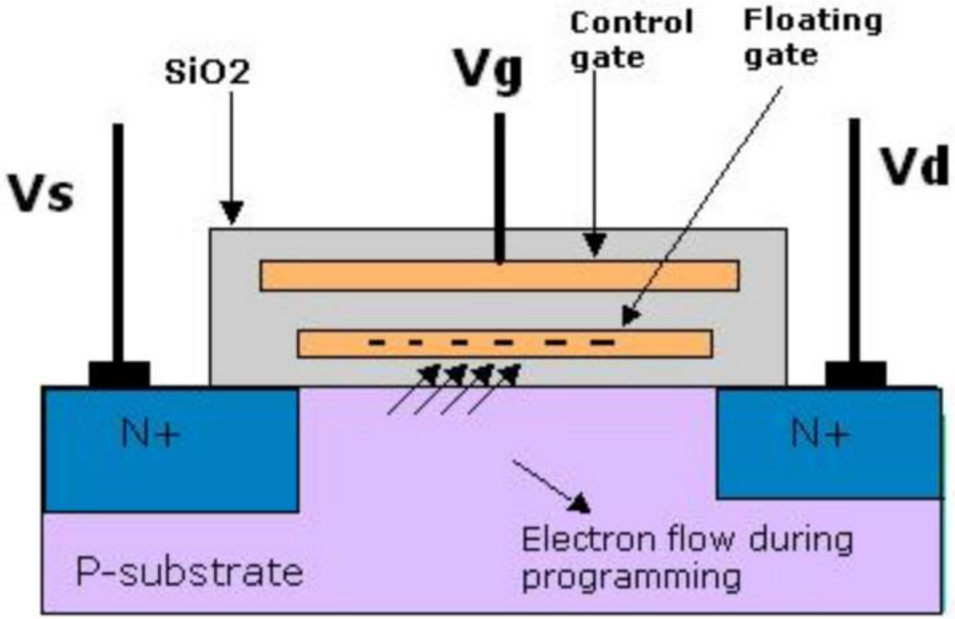
Basic NOR Gate (Working Principal)

- Flash stores the data by removing or putting electrons on its floating gate (see fig 5). Charge on floating gate affects the threshold of the memory element. When electrons are present on the floating gate, no current flows through the transistor, indicating a logic-0. When electrons are removed from the floating gate, the transistor starts conducting, indicating a logic-1. This is achieved by applying voltages between the control gate and source or drain.



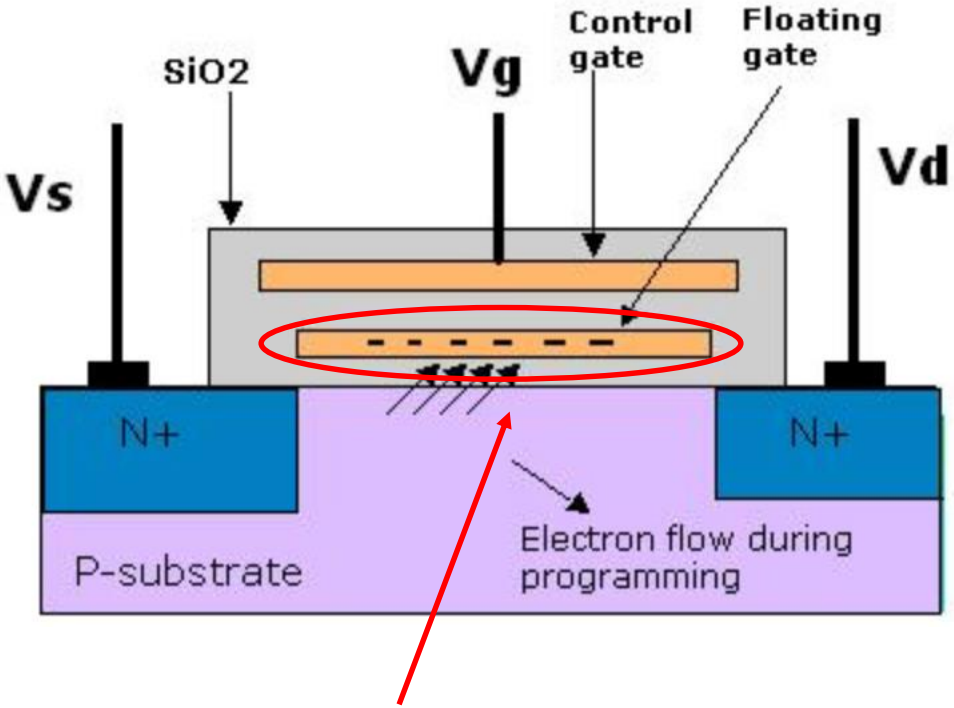
Basic NOR Gate (Erase Operation)

- The raw state of flash memory cells will be bit 1's, (at default state) because floating gates carry no negative charges. Erasing a flash-memory cell (resetting to a logical 1) is achieved by applying a voltage across the source and control gate (word line). The voltage can be in the range of -9V to -12V. And also apply around 6V to the source. The electrons in the floating gate are pulled off and transferred to the source by quantum tunneling (a tunnel current). In other words, electrons tunnel from the floating gate to the source and substrate.



Basic NOR Gate (Write Operation 1 of 3)

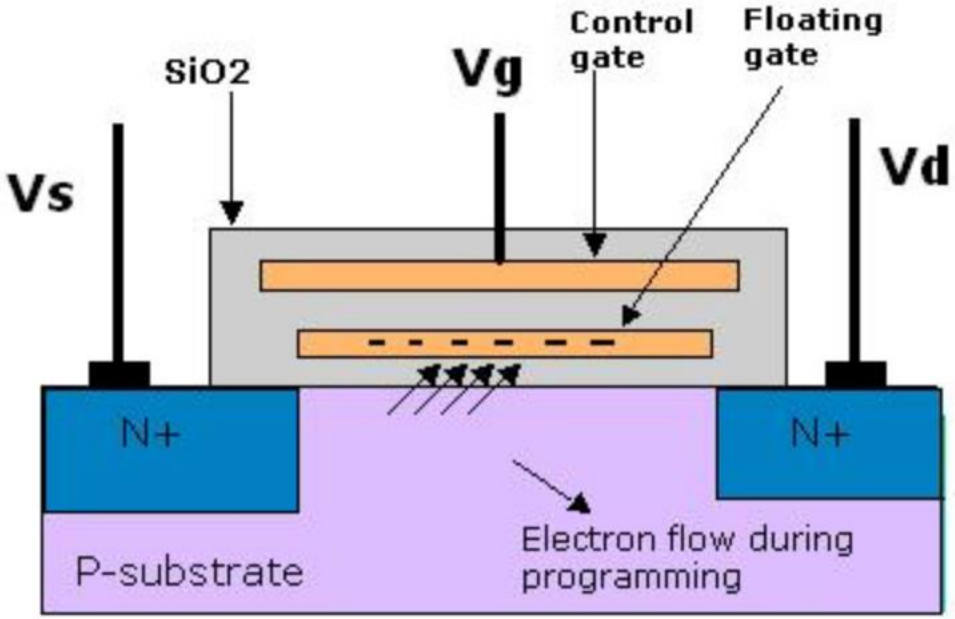
- A NOR flash cell can be programmed, or set to a binary "0" value, by the following procedure.
- While writing a high voltage of around 12V is applied to the control gate (word line). If high voltage around 7V is applied to Bit Line (Drain terminal), bit 0 is stored in the cell. The channel is now turned on, so electrons can flow from the source to the drain. Through the thin oxide layer electrons move to the floating gate. The source-drain current is sufficiently high to cause some high-energy electrons to jump through the insulating layer onto the floating gate, via a process called hot-electron injection.



Keeping the float gate charged correctly for reliability

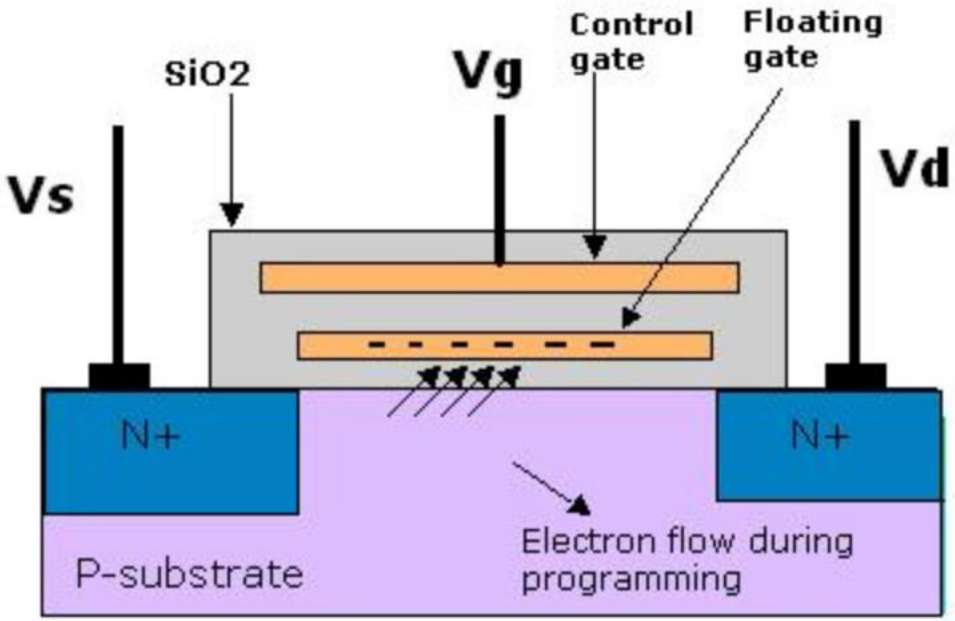
Basic NOR Gate (Write Operation 2 of 3)

- Due to applied voltage at floating-gate the excited electrons are forced through and trapped on other side of the thin oxide layer, giving it a negative charge on the floating gate. These negatively charged electrons act as a barrier between the control gate and the floating gate.



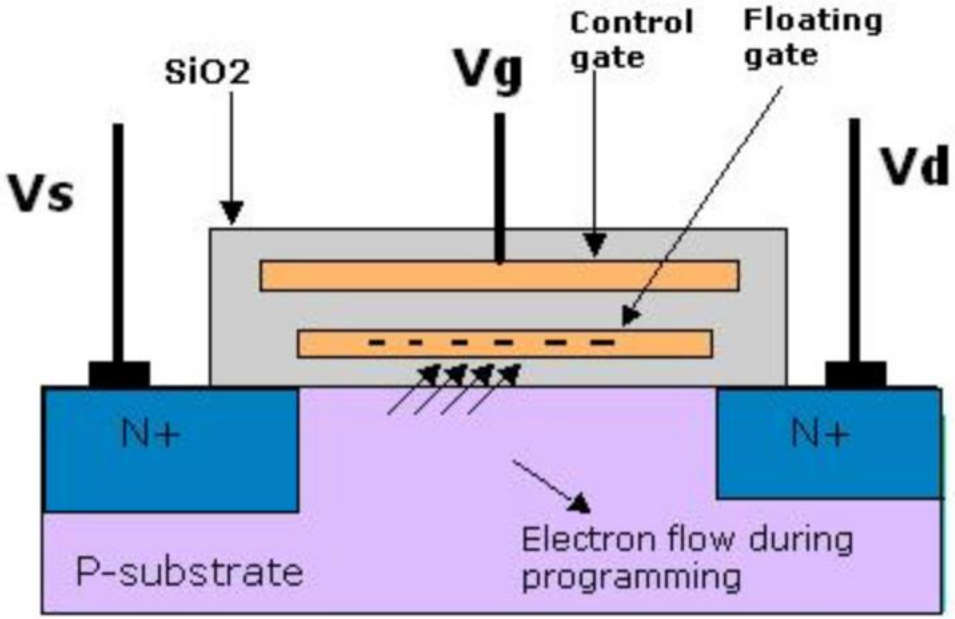
Basic NOR Gate (Write Operation 3 of 3)

- If low voltage is applied to the drain via the bit line, the amount of electrons on the floating gate remains the same, and logic state doesn't change, storing the bit 1. Since floating gate is insulated by oxide, the charge accumulated on the floating gate will not leak out, even if the power is turned off.
- A device called a cell sensor watches the level of the charge passing through the floating gate. If the flow through the gate crosses 50 percent threshold, it has a value of 1. When the charge passing through decline to below 50-percent threshold, than the value changes to 0.
- Because of the very good insulation properties of SiO2, the charge on the floating gate leaks away very slowly.



Basic NOR Gate (Read Operation)

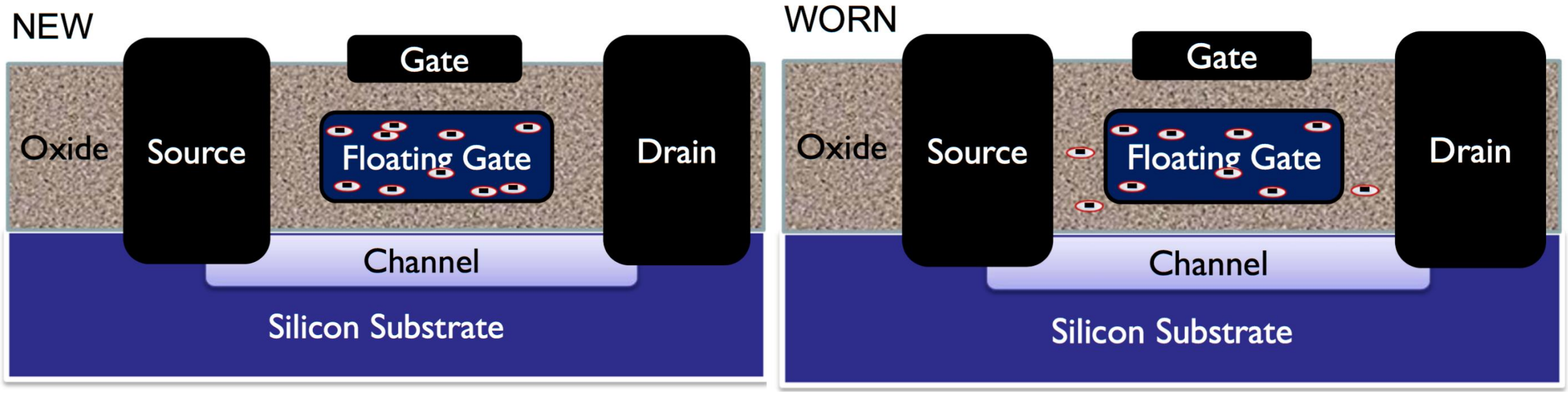
- Apply a voltage around 5V to the control gate and around 1V to the drain. The state of the memory cell is distinguished by the current flowing between the drain and the source.
- To read the data, a voltage is applied to the control gate, and the MOSFET channel will be either conducting or remain insulating, based on the threshold voltage of the cell, which is in turn controlled by charge on the floating gate. The current flow through the MOSFET channel is sensed and forms a binary code, reproducing the stored data.



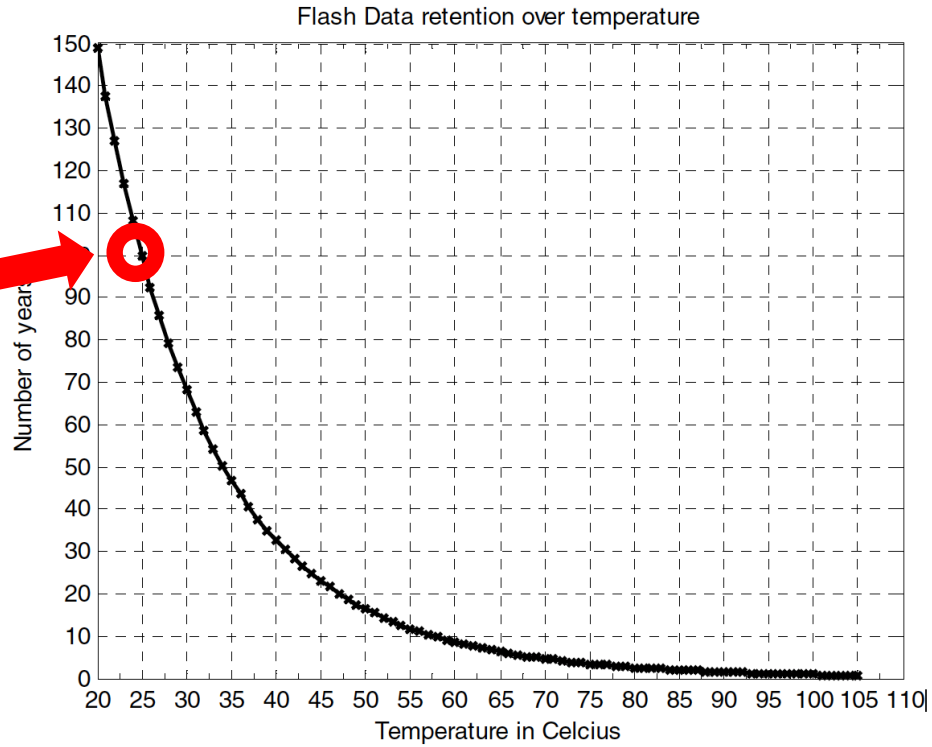
NOR failures due to over cycling Erase/Write operations

- Cycling Endurance
  - Each PROGRAM/ERASE operation can degrade the memory cell, and over time, the accumulation of cycles can prevent the device from meeting power, programming, or erasing specifications or from reading the correct data pattern.
- Data Retention
  - The dominant wear mechanism for charge loss and gain in NOR Flash memory occurs through electron trapping in the tunnel oxide of the Flash cell. This results in leakage through the insulator, and the damage primarily occurs during the ERASE/WRITE operations of a cell.

Flash memory wear-out: Electrons trapped in the tunneling oxide preventing a reliable read of a "0" or "1."



Data Retention versus Temperature



100 years at 25C

Data Retention errors increase as the leakage current increase electron migration with temperature. It can only happen to a floating gate which is positively charged. The value of a "0" can become a "1," and never a "1" to a "0"

Figure 1: Flash Data Retention vs Temperature for 170°C 420-Hour Test

The corner cases for 85°C and 105°C are slightly over 2 years and less than 9 months,

Data Retention vs Temperature dependency

- With higher temperatures, leakage current increases and, thus, the charge on the floating gate is reduced more quickly than at lower temperatures. This temperatures dependence follows the Arrhenius equation

$$AF = e^{-\frac{Ea}{k}\left(\frac{1}{T1} - \frac{1}{T2}\right)}$$

Where

AF = Acceleration factor
Ea = 0.6 eV = Activation energy
$k = 86.17 \times 10^{-6}$ = Speed constant
T1 = Temperature 1 (K)
T2 = Temperature 2 (K)

Example of data retention versus temperature

- At T_2 25C, the data sheet specifies data retention at 100 years
- At T_1 50C, what is the estimated data retention in years?
- 100 yrs / AF
- 100 yrs / $e^{-(\frac{0.6ev}{86.17x10-6})(\frac{1}{T1}-\frac{1}{T2})}$
- 100 yrs / $e^{-(\frac{0.6ev}{86.17x10-6})(\frac{1}{323}-\frac{1}{298})}$
- 100 yrs / $e^{1.8085}$
- 100 yrs / 6.101
- 16.39 yrs

NXP LPC15xx data sheet

Table 13. Flash characteristics

T_{amb} = −40 °C to +105 °C. Based on JEDEC NVM qualification. Failure rate < 10 ppm for parts as specified below.

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
N_{endu}	endurance	[1]	10000	100000	-	cycles
t_{ret}	retention time	powered	10	20	-	years
		not powered	20	40	-	years
t_{er}	erase time	page or multiple consecutive pages, sector or multiple consecutive sectors	95	100	105	ms
t_{prog}	programming time	[2]	0.95	1	1.05	ms

[1] Number of program/erase cycles.

[2] Programming times are given for writing 256 bytes to the flash. T_{amb} <= +85 °C. Flash programming with IAP calls (see *LPC15xx user manual*).

Data Retention of the NXP LPC15XX at 125C operating?

- At T_2 105C (378K), the data sheet specifies data retention at 10 years
- At T_1 125C (398K), what is the estimated data retention in years?
- 10 yrs / AF
- 10 yrs / $e^{-(\frac{0.6ev}{86.17x10-6})(\frac{1}{T1}-\frac{1}{T2})}$
- 10 yrs / $e^{-(\frac{0.6ev}{86.17x10-6})(\frac{1}{398}-\frac{1}{378})}$
- 10 yrs / $e^{0.9257}$
- 10 yrs / 2.524
- 3.96 yrs

How to get desired data retention times for systems in elevated temperature with long life?

- Data Retention time is based on when the cell is written, so rewriting the cell before the Data Retention time becomes an issue will "restart" the Data Retention clock.
- Is this a good solution? Maybe.
  - Can you guarantee or design that over the life span of the product that the number of Erase/Program cycles specified will not be surpassed
  - Erasing a flash cell is a relatively a high current operation
    - Can the system provide the current required?
    - Does the battery have enough charge to meet the battery life cycle requirements?
  - Writing to the flash takes a relatively long time, and the processor is limited capabilities / resources during the flash erase, programming, and refreshes

Since the failure mechanism is a "0" being read as an erroneous "1", then the cell can be just re-programmed!

Example of the high current to program flash

- Silicon Labs' EFM32LG Leopard Gecko
- Typical current consumption without flash programming @ 14MHz HFRCO
  - EM0 = 3.02mA
  - EM1 = 1.11mA
  - EM2 = 0.0017mA
  - EM3 = 0.0013mA
  - Em4 = 0.0009mA

Table 3.7. Flash

Symbol	Parameter	Condition	Min	Typ	Max	Unit
EC_{FLASH}	Flash erase cycles before failure		20000			cycles
RET_{FLASH}	Flash data retention	T_{AMB}<150°C	10000			h
		T_{AMB}<85°C	10			years
		T_{AMB}<70°C	20			years
t_{W_PROG}	Word (32-bit) programming time		20			µs
t_{PERASE}	Page erase time		20	20.4	20.8	ms
t_{DERASE}	Device erase time		40	40.8	41.6	ms
I_{ERASE}	Erase current				7[1]	mA
I_{WRITE}	Write current				7[1]	mA
V_{FLASH}	Supply voltage during flash erase and write		1.98		3.8	V

[1]Measured at 25°C

High current of programming flash memory

- Possible solutions are:
  - Program or refresh FLASH only when connected to an external power source
  - Increase the current capability of the battery
  - Increase the charge or capacity of the battery
  - Manage power of the system
    - Example:
      - BLE Radio can consume 15mA during transmit
      - Writing to the flash consumes 7mA
      - Processor in EMO while writing to the FLASH is 3mA
      - Total current during these operations combined is 25mA
      - Only perform writing to the flash when the radio is turned OFF

Limiting peak current during FLASH programming or refresh to 10mA

High current of programming flash memory

- Silicon Labs' Leopard Gecko EFMLG32 write to flash example
- Worst case is a page erase plus a full page write
- Page size is 2048 bytes or 512 4-byte words
  - Erase page 20.8ms
  - Write 512*20uS 1.0ms
  - Total time of 21.8ms
- To minimize the current spike on the battery for a BLE application that programmed while operating, the ConnInterval or SlaveInterval should guarantee at least 21.8ms with the radio off to program the flash

Table 3.7. Flash

Symbol	Parameter	Condition	Min	Typ	Max	Unit
EC_{FLASH}	Flash erase cycles before failure		20000			cycles
RET_{FLASH}	Flash data retention	T_{AMB}<150°C	10000			h
		T_{AMB}<85°C	10			years
		T_{AMB}<70°C	20			years
t_{W_PROG}	Word (32-bit) programming time		20			µs
t_{PERASE}	Page erase time		20	20.4	20.8	ms
t_{DERASE}	Device erase time		40	40.8	41.6	ms
I_{ERASE}	Erase current				7[1]	mA
I_{WRITE}	Write current				7[1]	mA
V_{FLASH}	Supply voltage during flash erase and write		1.98		3.8	V

[1] Measured at 25°C

Limitations due to the number of erase cycles before failure

- Silicon Labs' EFM32LG Leopard Gecko
- If a page of the flash had to be updated 1 time per hour based for sensor readings
  - 24*365 = 8,760 /yr
  - Requires a "fresh" flash sector 2.25 years
- Or, a page of flash had to be updated every 1 minute
  - 60*24*365 = 525,600
  - Requiring a "fresh" flash sector every 13.89 days

Table 3.7. Flash

Symbol	Parameter	Condition	Min	Typ	Max	Unit
EC_{FLASH}	Flash erase cycles before failure		20000			cycles
RET_{FLASH}	Flash data retention	T_{AMB}<150°C	10000			h
		T_{AMB}<85°C	10			years
		T_{AMB}<70°C	20			years
t_{W_PROG}	Word (32-bit) programming time		20			µs
t_{PERASE}	Page erase time		20	20.4	20.8	ms
t_{DERASE}	Device erase time		40	40.8	41.6	ms
I_{ERASE}	Erase current				7[1]	mA
I_{WRITE}	Write current				7[1]	mA
V_{FLASH}	Supply voltage during flash erase and write		1.98		3.8	V

[1]Measured at 25°C

Limitations due to the number of erase cycles before failure

- Possible solutions
  - Allocate enough flash to insure enough good “flash” pages for the life of the product
  - Example:
    - The case of a flash page is updated every hour
    - The product is an industrial application with a lifecycle projection of 20 years
    - Number of pages pages based on the previous example = 20 yrs / 2.25 yrs/page
      - ~ 8.89 pages
    - Total amount of flash dedicated for this storage = 2,048 bytes/page * 8.89 pages
      - 18,207 bytes
    - Solution: Purchase a microcontroller that had an additional 9 pages of flash available to allocate for data logging
    - Solution: Utilize an external Flash

Limitations due to the number of erase cycles before failure

- Possible solutions
  - Allocate enough flash to insure enough good “flash” pages for the life of the product
  - Example:
    - The case of a flash page is updated every minute
    - The product is an industrial application with a lifecycle projection of 20 years
    - Number of days over product life cycle = 20 * 365 = 7240 days
    - Number of pages pages based on the previous example = 7240 / 13.89 ~ 8,864 pages
    - Total amount of flash dedicated for this storage = 2,048 bytes/page * 8,864 pages
      - 18,153,472 bytes
    - Solution: ~~Purchase a microcontroller that had 18MB of additional memory~~
    - Solution: External Flash or change product specifications

Writing to the flash takes a long time

- Silicon Labs' Leopard Gecko EFMLG32 write to flash example
- During writes to flash in the Leopard Gecko, no access to flash memory is allowed
  - Not even instructions to execute
  - It will stall the processor
- Must plan the write to flash when access to flash will not be required
- Page size is 2048 bytes or 512 4-byte words
  - Erase page 20.8ms
  - Write 512*20uS 1.0ms
  - Total time of 21.8ms
- Must plan writes when no time critical interrupts can occur
  - For BLE operations, it should be planned between Connection Events so the ConnInterval or ServerLatency should be greater than the time to write to flash

Table 3.7. Flash

Symbol	Parameter	Condition	Min	Typ	Max	Unit
EC_{FLASH}	Flash erase cycles before failure		20000			cycles
RET_{FLASH}	Flash data retention	T_{AMB}<150°C	10000			h
		T_{AMB}<85°C	10			years
		T_{AMB}<70°C	20			years
t_{W_PROG}	Word (32-bit) programming time		20			µs
t_{PERASE}	Page erase time		20	20.4	20.8	ms
t_{DERASE}	Device erase time		40	40.8	41.6	ms
I_{ERASE}	Erase current				7[1]	mA
I_{WRITE}	Write current				7[1]	mA
V_{FLASH}	Supply voltage during flash erase and write		1.98		3.8	V

[1]Measured at 25°C

Correction to TI application note SLAA334

- Let's take a look at the TI SLAA334 statement

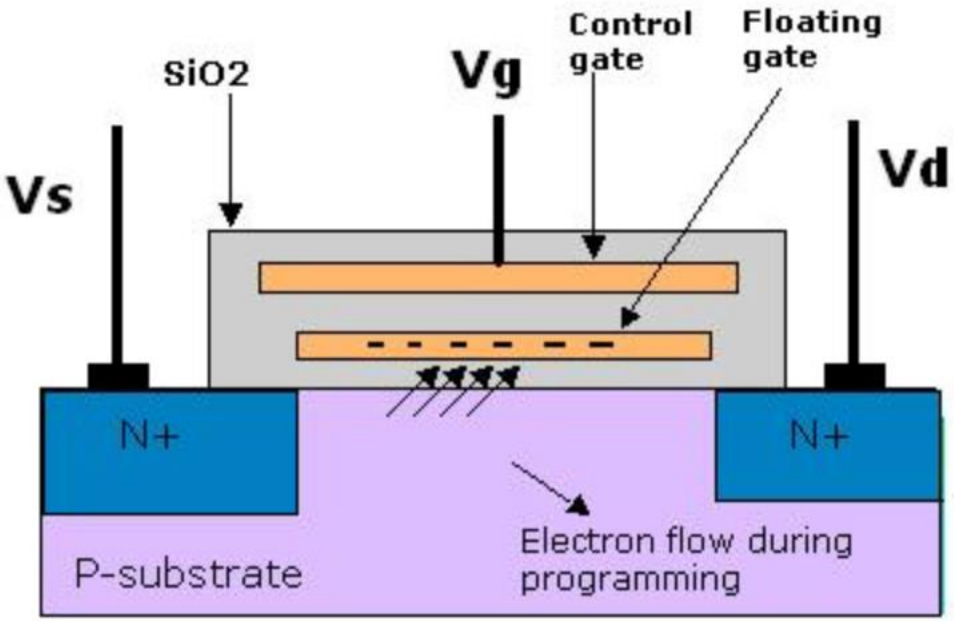
3.1 Data Retention

3.1.1 Leakage Mechanism

Data retention is limited by leakage current through the insulating oxide. Leakage can only occur if the floating gate is fully charged. Therefore, leakage only can flip an erased cell with the logic level 1 to a programmed cell with the logic level 0. According to Manabe [1], there are several phenomena that cause leakage.

Correction to TI application note SLAA334

- Let's think of a model of a NAND memory cell
- A "1" occurs when current flows from the source to the drain
- A "0" occurs when the free electrons in the substrate are moved and trapped in the floating gate, thus current cannot flow from the source to drain



Data Retention

In flash storage, data retention is the measure of how long the integrity of data can be guaranteed after being written to the flash drive without suffering from data corruption. Once a flash cell is charged, the electrons stored in the cell leak across the NAND gate over time, causing the charge on the cell to decrease. With enough leakage, the voltage level on the cell will drift into the neighboring region, causing the incorrect binary value to be read.

Because SLC flash memory is only divided into two voltage regions, it has more margin for charge loss before a bit flip occurs (a 0 becomes a 1), as shown in Figure 2.

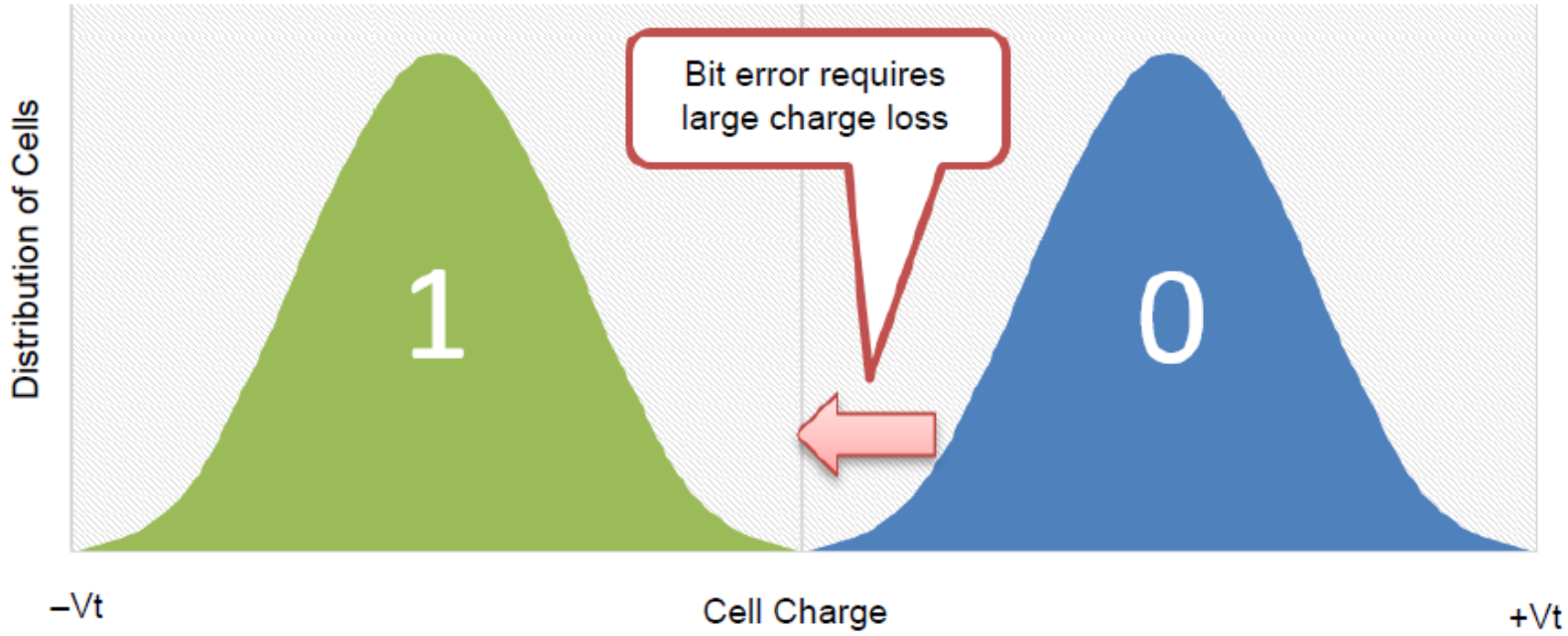


Figure 2 SLC Flash Data Storage

On the other hand, MLC can tolerate much less charge loss before data errors occur because it has a similar voltage range divided into four regions, as shown in Figure 3.

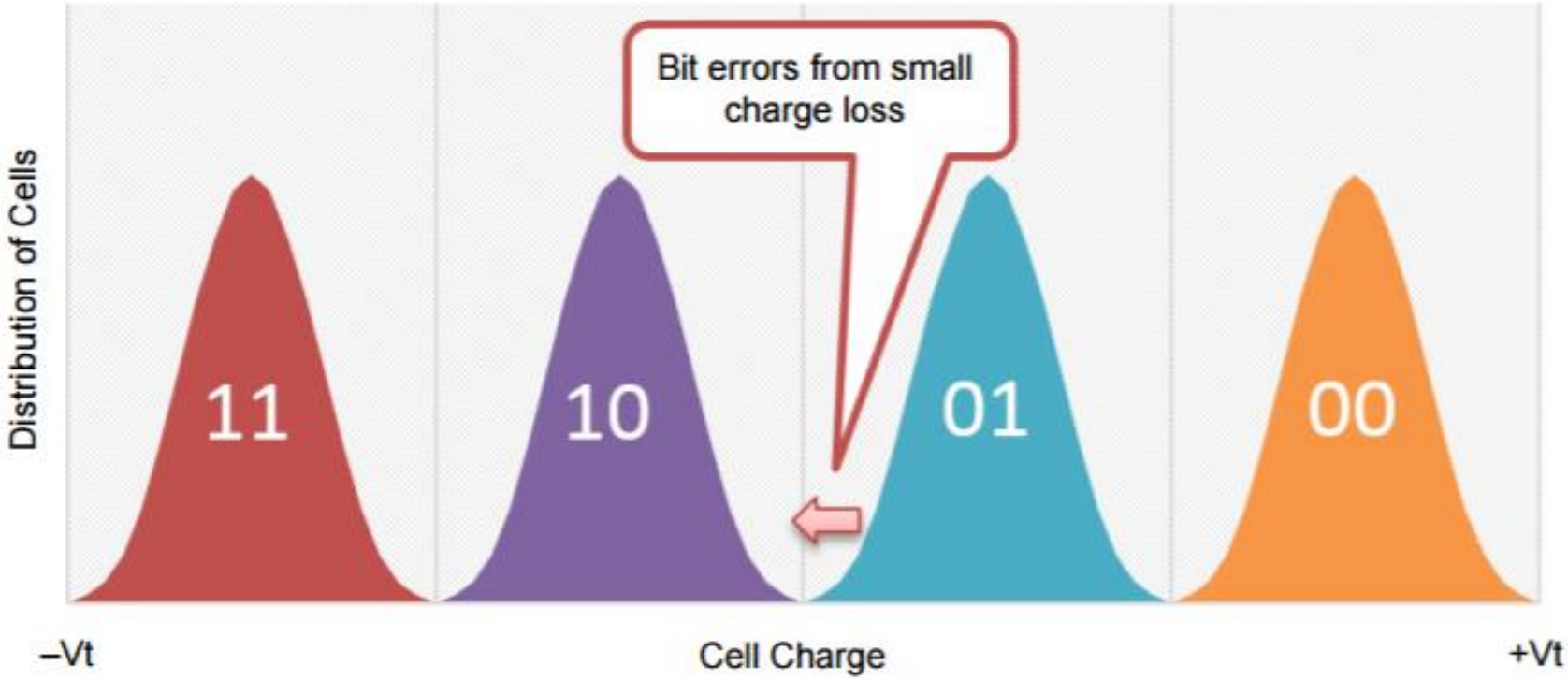
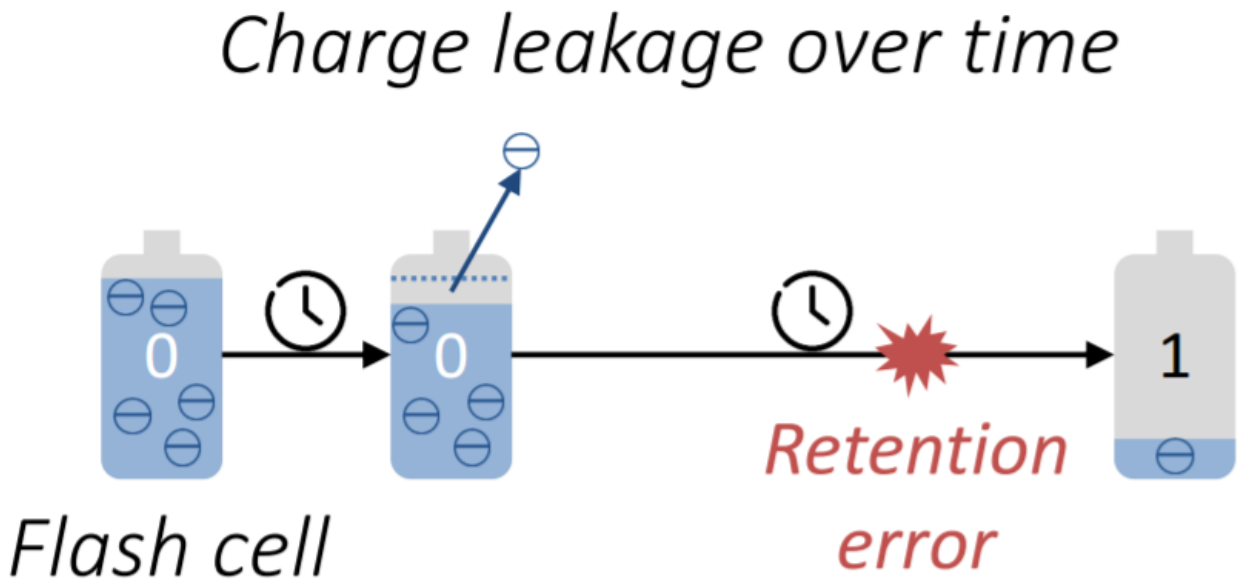


Figure 3 MLC Flash Data Storage

Retention Loss



One dominant source of flash memory errors [DATE '12, ICCD '12]

Correction to TI application note SLAA334

- Let's take a look at the TI SLAA334 statement

3.1 Data Retention

3.1.1 Leakage Mechanism

Data retention is limited by leakage current through the insulating oxide. Leakage can only occur if the floating gate is fully charged. Therefore, ~~leakage only can flip an erased cell with the logic level 1 to a programmed cell with the logic level 0.~~ According to Manabe [1], there are several phenomena that cause leakage.

Writing to the flash takes a long time

- Silicon Labs' Leopard Gecko EFMLG32 write to flash example
- During writes to flash in the Leopard Gecko, no access to flash memory is allowed
  - Not even instructions to execute
  - It will stall the processor
- Must plan the write to flash when access to flash will not be required
- Page size is 2048 bytes or 512 4-byte words
  - Erase page 20.8ms
  - Write 512*20uS 1.0ms
  - Total time of 21.8ms
- Must plan writes when no time critical interrupts can occur
  - For BLE operations, it should be planned between Connection Events so the ConnInterval or ServerLatency should be greater than the time to write to flash

Table 3.7. Flash

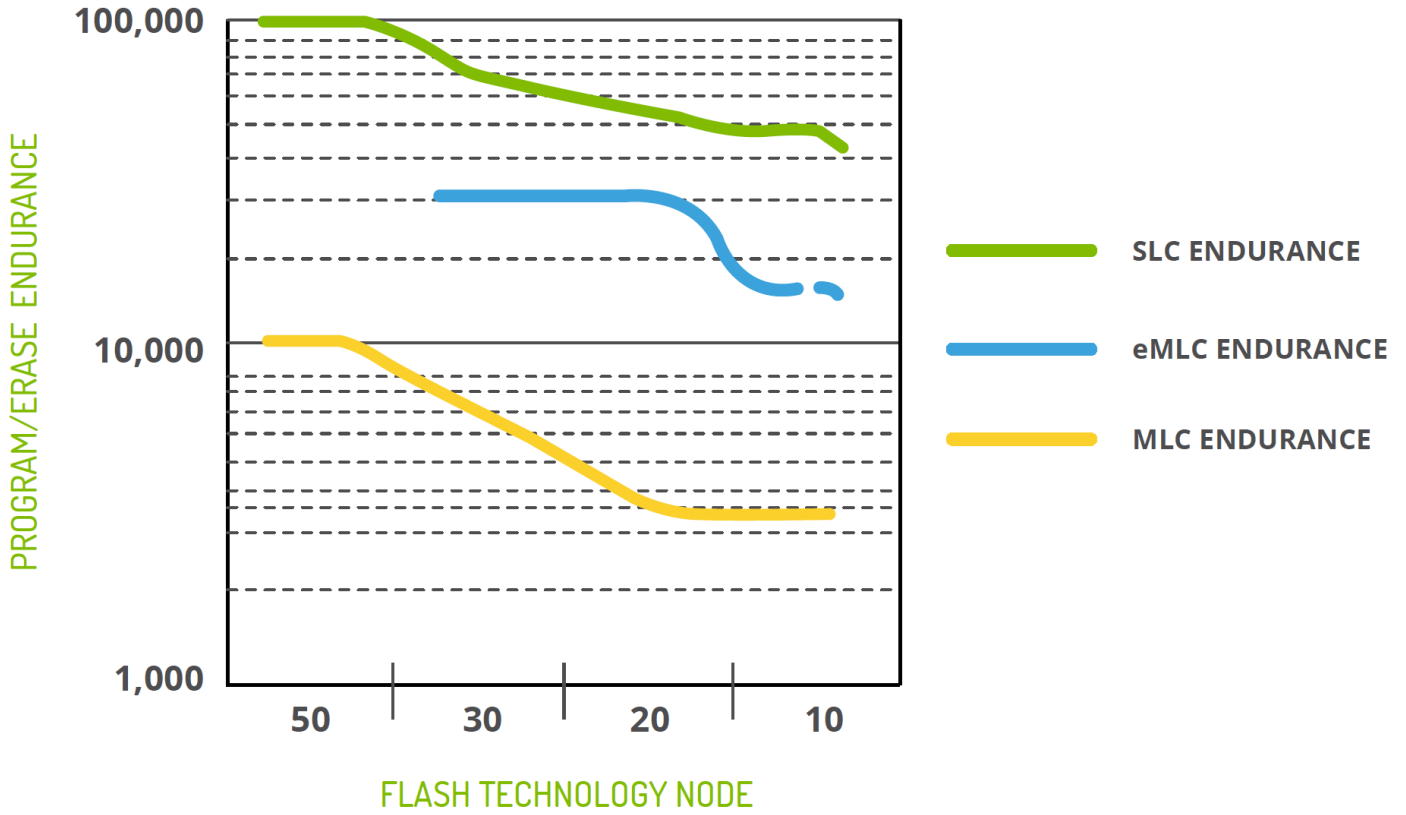
Symbol	Parameter	Condition	Min	Typ	Max	Unit
EC_{FLASH}	Flash erase cycles before failure		20000			cycles
RET_{FLASH}	Flash data retention	T_{AMB}<150°C	10000			h
		T_{AMB}<85°C	10			years
		T_{AMB}<70°C	20			years
t_{W_PROG}	Word (32-bit) programming time		20			µs
t_{PERASE}	Page erase time		20	20.4	20.8	ms
t_{DERASE}	Device erase time		40	40.8	41.6	ms
I_{ERASE}	Erase current				7[1]	mA
I_{WRITE}	Write current				7[1]	mA
V_{FLASH}	Supply voltage during flash erase and write		1.98		3.8	V

[1]Measured at 25°C

Writing to the flash takes a long time

- Solution: Find a time that critical interrupts can be turned off
  - In a BLE application, is there a time between ConnIntervals or ServerLatency?
  - Is there a time in the day that operation is not critical?
    - Example: micro converter on a solar panel during the solar panel daily wakeup
  - The product gets plugged in to charge
    - Example: A fit bit watch does not need to perform its primary role while plugged in to be charged
- Solution: Use an external Flash
  - External flash does not tie up a microcontroller's critical resources such as program memory
  - External flash such as eMMC have integrated algorithms to minimize data retention and other errors such as write disturb
  - External flash with the correct capacitance coupling can provide guaranteed write completion
  - Negative, an additional part resulting in higher part cost and board real estate

Endurance versus Moore's Law



Endurance goes down as the area to store the electrons in the floating gate gets smaller. Less electrons, less margin or separation between a "0" and a "1" state.

Cactus Technologies "SLC vs MLC NAND and The Impact of Technology Scaling White paper CTWP010"

NAND Technology types

- SLC
  - Single Level Cell
  - Each NAND cell is one bit, or two states (0,1)
- MLC
  - Multi Level Cell
  - Each NAND cell represents two bits, or four states (0,1,2,3)
- TLC
  - Tertiary Level Cell
  - Each NAND cell represents three bits, or 6 states (0,1,2,3,4,5)
- 3d
  - Memory cells stacked on top of each other (3d)
  - Can be SLC or MLC

NAND Technology comparisons

- SLC
  - Relatively fast read and write capabilities
  - Good endurance
  - And relatively simple error correction algorithms
  - More expensive than MLC and TLC since one bit for the same area
- MLC
  - Twice the density of SLC, thus less cost per bit than SLC
  - Roughly 1/3 the speed of SLC
  - And, Roughly 1/10 the reliability of SLC
  - Most common flash today – good balance between cost and performance

NAND Technology comparisons

- TLC
  - 3x the density of SLC
  - Much lower performance
  - Reliability is lowest of all NAND types
  - Good for applications that have low amounts of writes such as MP3 players
- 3d NAND
  - Technology based on stacking NAND cells
  - Increases the number of layers and steps in the manufacturing process
  - Enables costs to continued to go lower
  - Reliability increased over standard MLC due to larger feature size, better insulating material, and charge trap design

NAND failure mechanisms

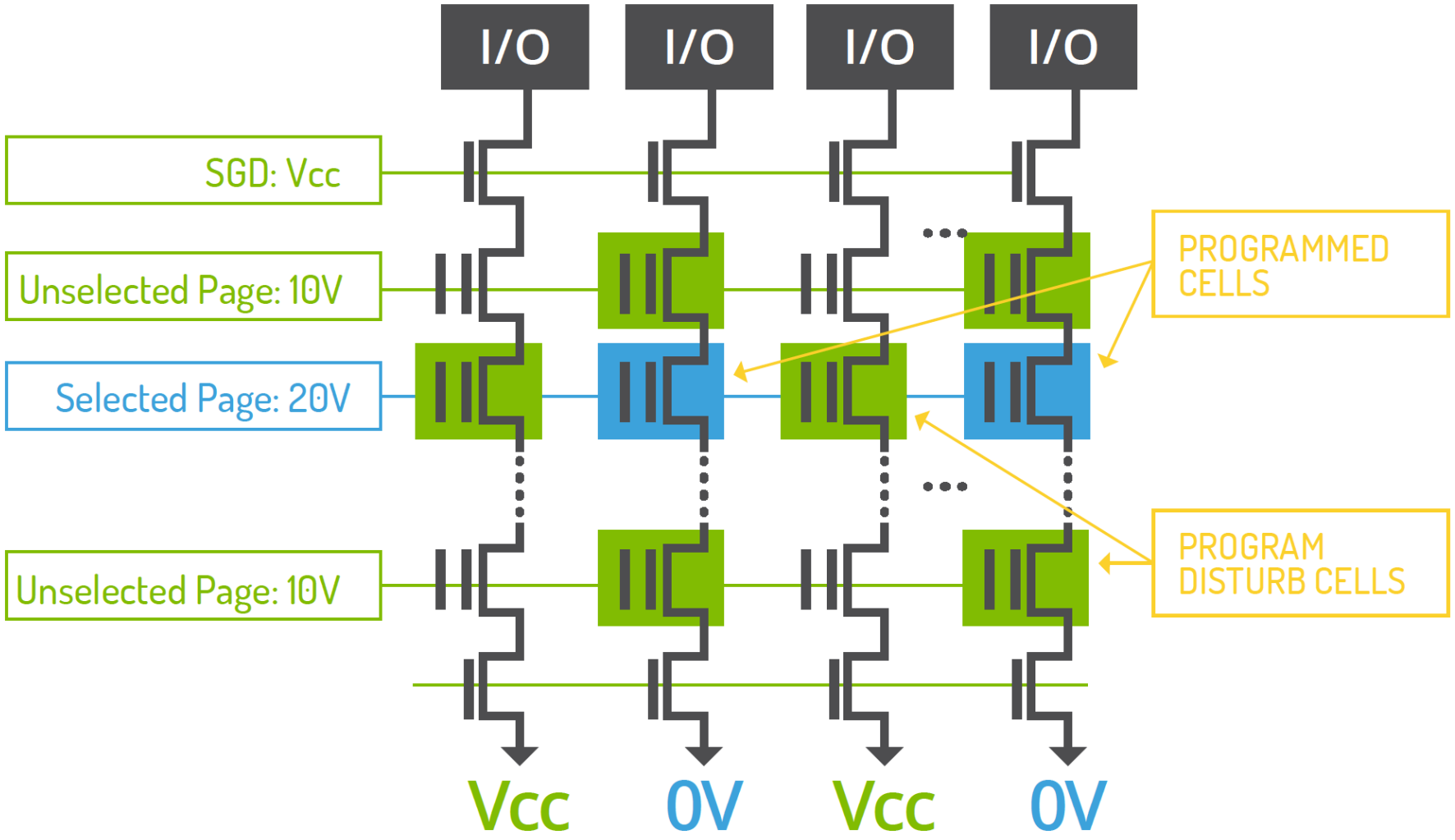
- Erase/Program cycle endurance
  - Same as NOR
- Data Retention
  - Same as NOR
- Reliability versus Moore's Law
  - Same as NOR
- Read Disturb
  - NAND failure mode
- Write Disturb
  - NAND failure mode

Write Disturb

Program disturb occurs in neighboring cells of the ones being programmed. This happens because the neighboring cells are exposed to voltage levels which are higher than normal. This setup causes these cells to appear to be weakly programmed. Fig.5 illustrations a representation of this problem:

A write disturbed error would result in a "1" bit going to a "0."

Why would MLC NAND be more sensitivity to write disturb errors?

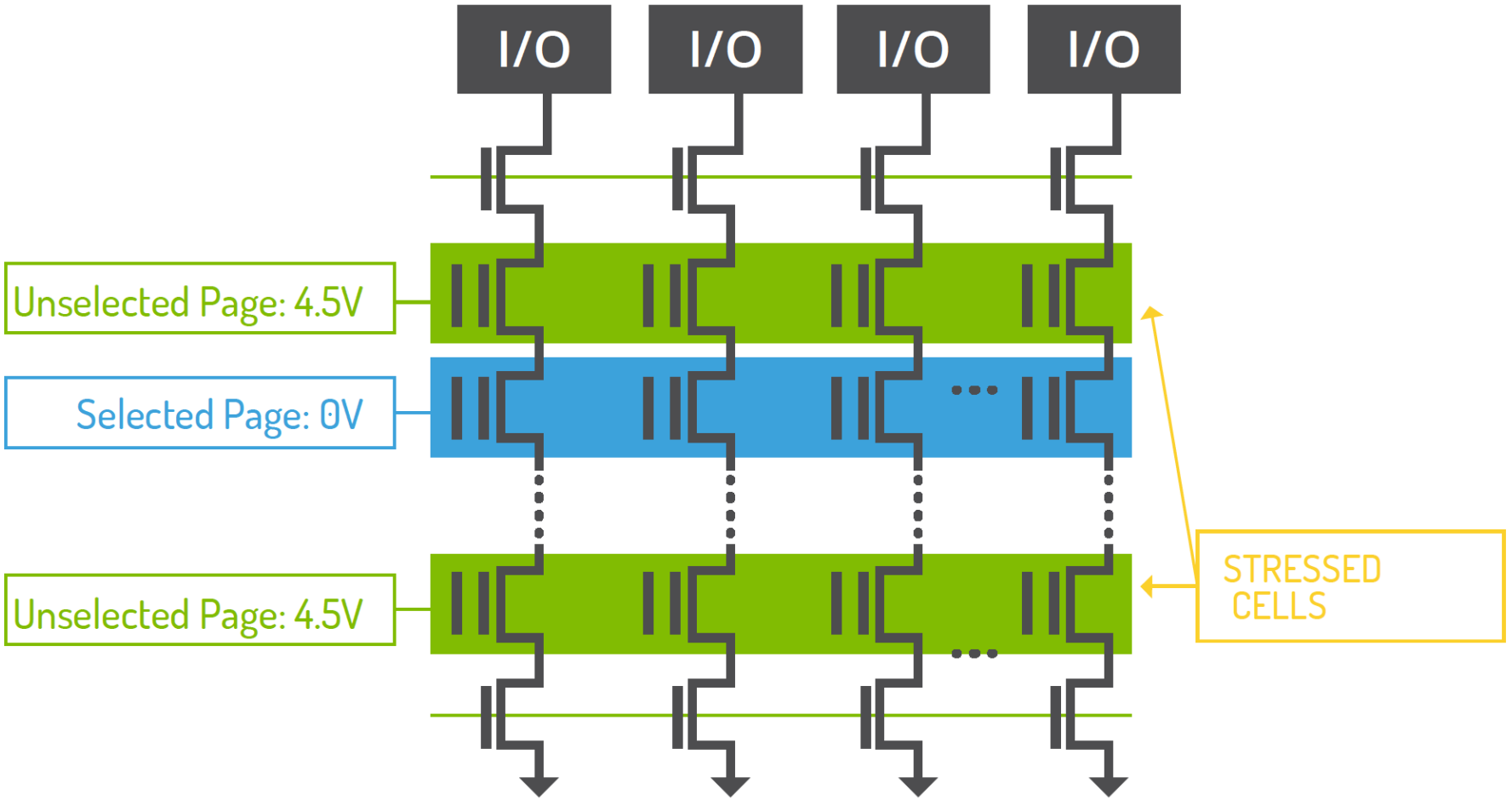


Read Disturb

Read disturb happens in neighboring cells of the ones being read due to stray charge being coupled to the floating gates of the unselected cells. This problem is not as severe as write disturb but is getting worse as flash geometry shrinks. Fig. 6 illustrates this scenario:

A read disturbed error would result in a "1" bit going to a "0."

Read disturb errors only occur on the adjacent cells, and not the cell read.



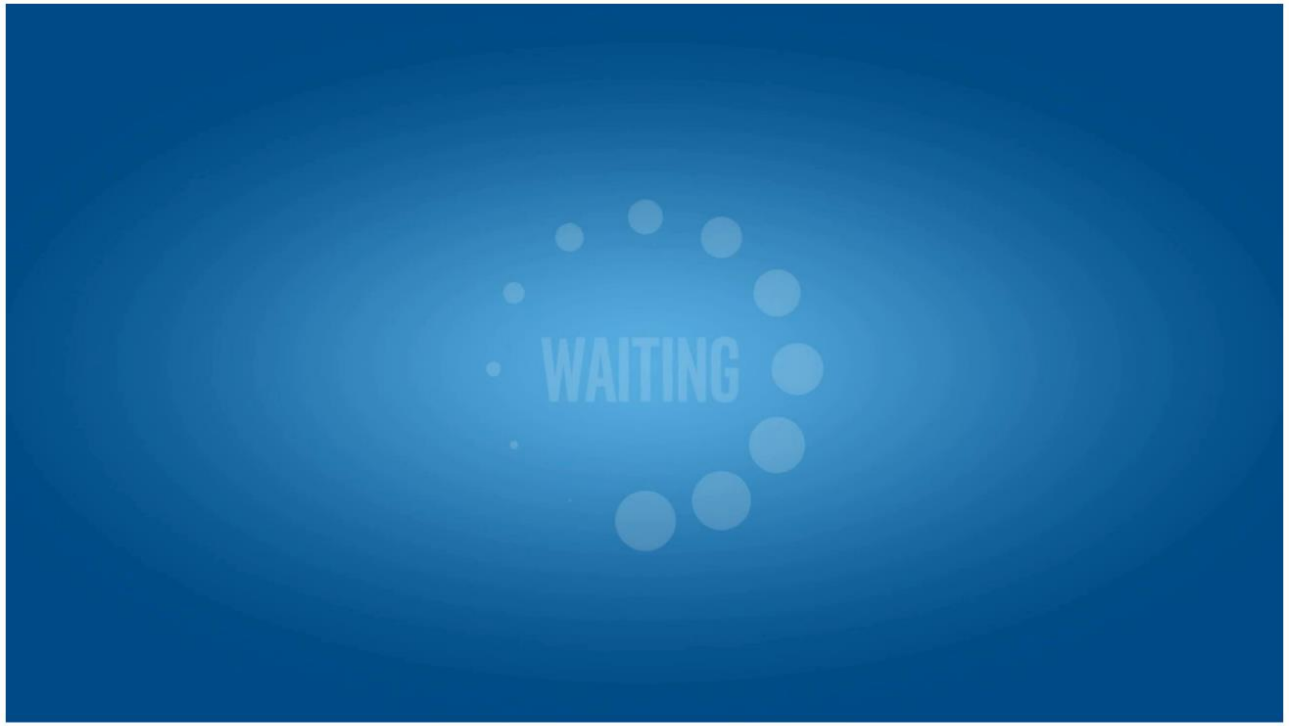
Dynamic (Global) Wear Leveling

- Dynamic wear leveling is a method of pooling the available blocks that are free of data and selecting the block with the lowest erase count for the next write. This method is most efficient for dynamic data because only the non-static portion of the NAND Flash array is wear-leveled. A system that implements dynamic wear leveling enables longer NAND Flash device life than a system that does not implement wear leveling.

Static Wear Leveling

- Static wear leveling utilizes all good blocks to evenly distribute wear, providing effective wear leveling and thereby extending the life of the device. This method tracks the cycle count of all good blocks and attempts to evenly distribute block wear throughout the entire device by selecting the available block with the least wear each time a program operation is executed. Static data is managed by maintaining all blocks within a certain erase count threshold. Blocks that contain static data with erase counts that begin to lag behind other blocks will be included in the wear-leveling block pool, with the static data being moved to blocks with higher erase counts.

Intel and Micron breaking the NAND technology limitations – 3D XPoint



3D XPoint™ Technology Revolutionizes Storage Memory

Intel engineers help shatter all the rules with 3D XPoint™ technology, a simple, stackable, and transistor-less design that creates fast, inexpensive, and nonvolatile storage memory with low latency to unleash your processor's true potential.

eMMC

- eMMC
  - Embedded MultiMediaCard Memory
  - MMC (MultiMediaCard)
    - Released in 1997 by SanDisk and Siemens AG
    - Based on NAND memory
    - Much smaller than other non-volatile cards in 1997 based on NOR Flash technology such as CompactFlash
  - Designed to solve NAND memory issues for the system designer
    - Perform ECC
    - Increase reliability
      - Static wear leveling
      - Dynamic (Global) wear leveling
    - System design becomes independent to NAND die changes resulting in ECC changes

Micron example of wear leveling benefits

- Consider a case without wear leveling. In a NAND Flash device with 4,096 total blocks and 2.5% allowable bad blocks in a system that updates 3 files comprised of 50 blocks each at a rate of 1 file every 10 minutes (or 6 files per hour), where a NAND host reuses the same 200 physical blocks for these updates, the NAND Flash device will wear out in under 1 year, leaving over 95% of the memory array unused.
- No wear leveling:

$$\text{Only 200 blocks are reused:} \frac{\text{10,000 cycles x 200 blocks}}{\text{50 blocks per file x 6 files per hour x 24 hours per day}} = \sim 278 \text{ days or } < 1 \text{ year}$$

Dynamic (Global) wear leveling example

- In a 4,096-block MLC device with a 10,000-cycle count, 75% static data, and a program and erase rate of 50 blocks every 10 minutes (or 6 files per hour), dynamic wear leveling results in device wear-out after approximately 4 years, with 75% of the blocks nearly unused.

$$\text{Wear leveling only dynamic data: } \frac{\text{10,000 cycles x 1,024 blocks}}{\text{50 blocks per file x 6 files per hour x 24 hours per day}} = \sim\text{1,422 days or <4 years}$$

Static wear leveling example

- Using the same example of a 4,096-block MLC device with a 10,000-cycle count, 75% static data, and a program and erase rate of 50 blocks every 10 minutes (or 6 files per hour), static wear leveling provides the best chance of extending the device life span beyond 15 years.

$$\text{Wear leveling static and dynamic data: } \frac{10{,}000 \text{ cycles x } 4{,}096 \text{ blocks}}{50 \text{ blocks per file x } 6 \text{ files per hour x } 24 \text{ hours per day}} = \sim 5{,}689 \text{ days or } > 15 \text{ years}$$

Preventing Read Disturbance

- InnoDisk Firmware is designed to resolve this issue by wear leveling and refresh (“re-charges”).
- With wear leveling feature, not only spread the program/erase count evenly on all blocks, but also can reduce the read access frequency to prevent Read Disturbance by reprogramming the data to different blocks.
- Alternatively, ECC (Error Correcting Code) can detect and fix the data where the electrical properties may have been altered by refresh. When error bits in a block reach a threshold of say 17 error bits out of 24 bits, the block is automatically refreshed. i.e. the data is deleted and re-written.
- This stops the controller from constantly reading blocks with too many error bits and prevents read disturbance.

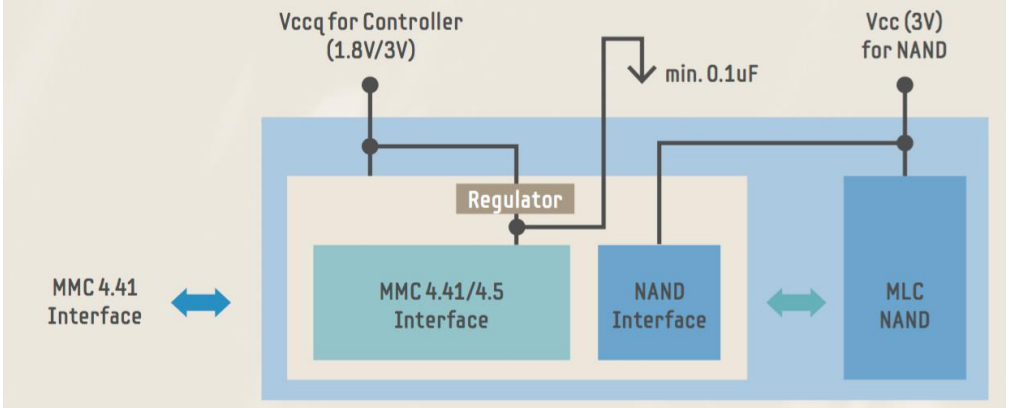
Wear Leveling Summary

Comparison [edit]

The following table compares static and dynamic wear leveling:[3]

Item	Static	Dynamic
Endurance	Longer life expectancy	Shorter life expectancy
Performance	Slower	Faster
Design Complexity	More complex	Less complex
Typical Use	SSDs[2]	USB Flash Drives

eMMC architecture



- eMMC memory is 2 die in one package
  - An EMMC controller
  - NAND memory
- eMMC advantages
  - Industry standard in both hardware and software
  - Enables the eMMC solution to be multi-source to enhance availability and reduce cost
  - Off loads the NAND management from the system firmware or hardware
  - System hardware and firmware does not need to change as NAND memory shrinks and changes ECC scheme – the change is supported by the eMMC controller

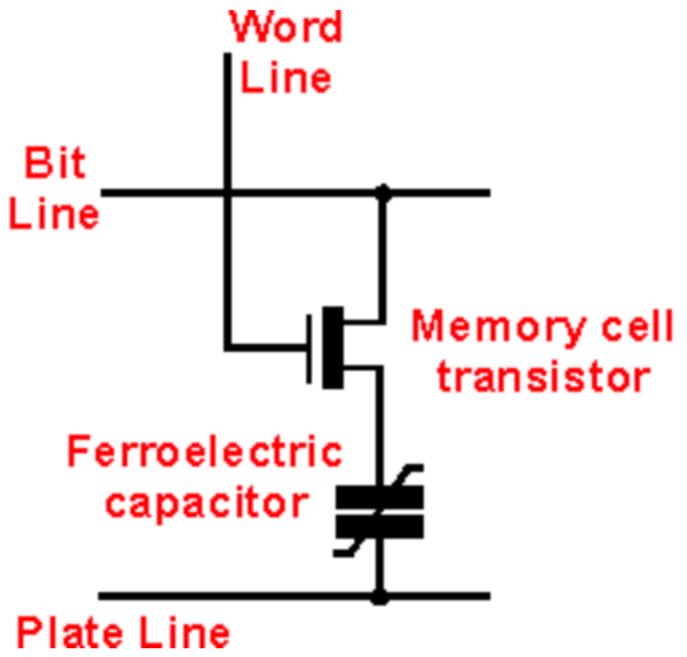
http://www.samsung.com/us/business/oem-solutions/pdfs/eMMC_Product%20Overview.pdf

Example of NAND management offload

- Hyperstone S8 NAND Management Features
  - hyReliability™ Flash Memory Management optimizing reliability, power fail safety, endurance, data retention, and performance
  - Read Disturb Management, dynamic data refresh to maximize data retention and refresh data subject to read disturbance
  - Static and Global Wear leveling to maximize write endurance
  - Bad Block Management
  - Complete Flash Translation Layer (FTL) for random Flash data access including mapping of logical block addresses (LBA) to physical block addresses (PBA)

FRAM

- Ferroelectric Random Access Memory (FRAM), also known as FeRAM or F-RAM, is a memory technology that combines the best of Flash and SRAM. It is non-volatile like Flash, but offers fast and low power writes, write endurance of 10^{15} cycles, code and data security that is less vulnerable to attackers than Flash/EEPROM



Basic Ferroelectric memory cell

Radio-Electronics.com "FRAM Ferroelectric Random Access Memory Tutorial"

FRAM Technology

- Molecular Structure
  - FRAM is a random access memory, meaning that each bit is read and written individually. This non-volatile memory is similar in structure to DRAM, which uses one transistor and one capacitor (1T-1C), but FRAM stores data as a polarization of a ferroelectric material (Lead-Zirkonate-Titanate). As an electric field is applied, dipoles shift in a crystalline structure to store information.
  - The use of crystal polarization as opposed to charge storage enables state retention, lower voltage requirements (as low as 1.5V) and fast write speeds when compared against Flash, EEPROM and SRAM technologies used in typical microcontroller.

http://www.ti.com/lsds/ti/microcontrollers_16-bit_32-bit/msp/ultra-low_power/msp430frxx_fram/what_is_fram.page?DCMP=ep-mcu-msp-fram-en&HQS=ep-mcu-msp-fram-b-lp-en#under

FRAM – Molecular Structure

In contrast to the complex charge storage mechanism used in EEPROM and flash, FRAM stores information through the use of a spontaneous, stable electric dipole found in the ferroelectric crystal. Intrinsically, the dipole atom within a ferroelectric crystal has either positive or negative orientation, as shown in Figure 2-4.

Applying an electrical field polarizes the material by creating large regions of the crystal with Ti/Zr ions all oriented the same direction (domains). By applying a voltage of opposite polarity above the coercive voltage, the Ti/Zr ions will have enough energy to overcome the energy barrier in the center of the cell to move to the other low-energy site as Figure 2-5 illustrates.

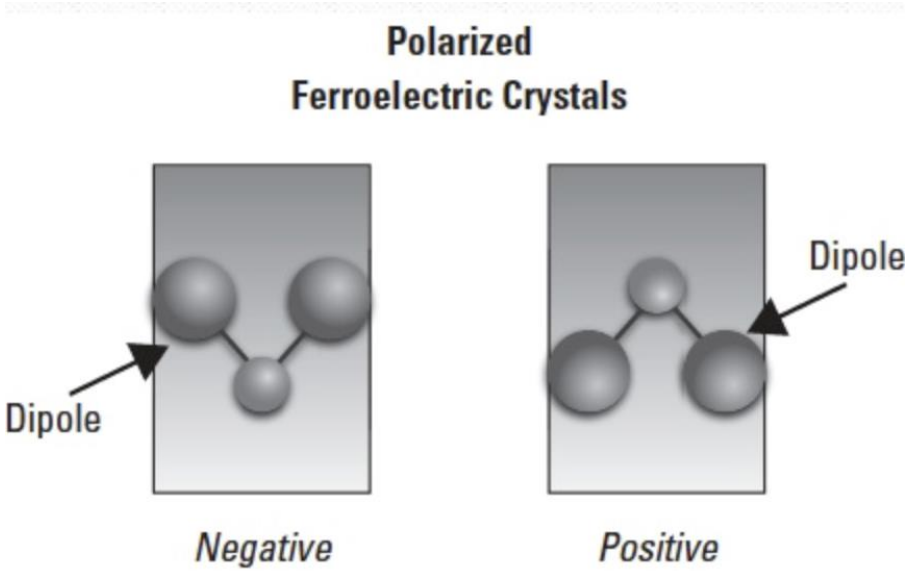


Figure 2-4. Dipole positions of ferroelectric crystals.

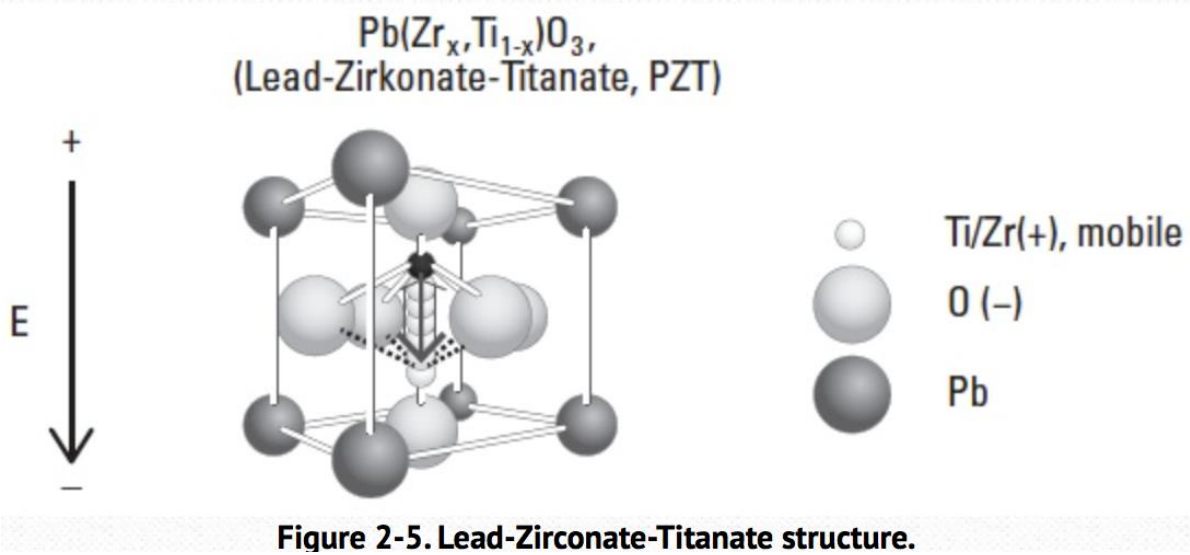


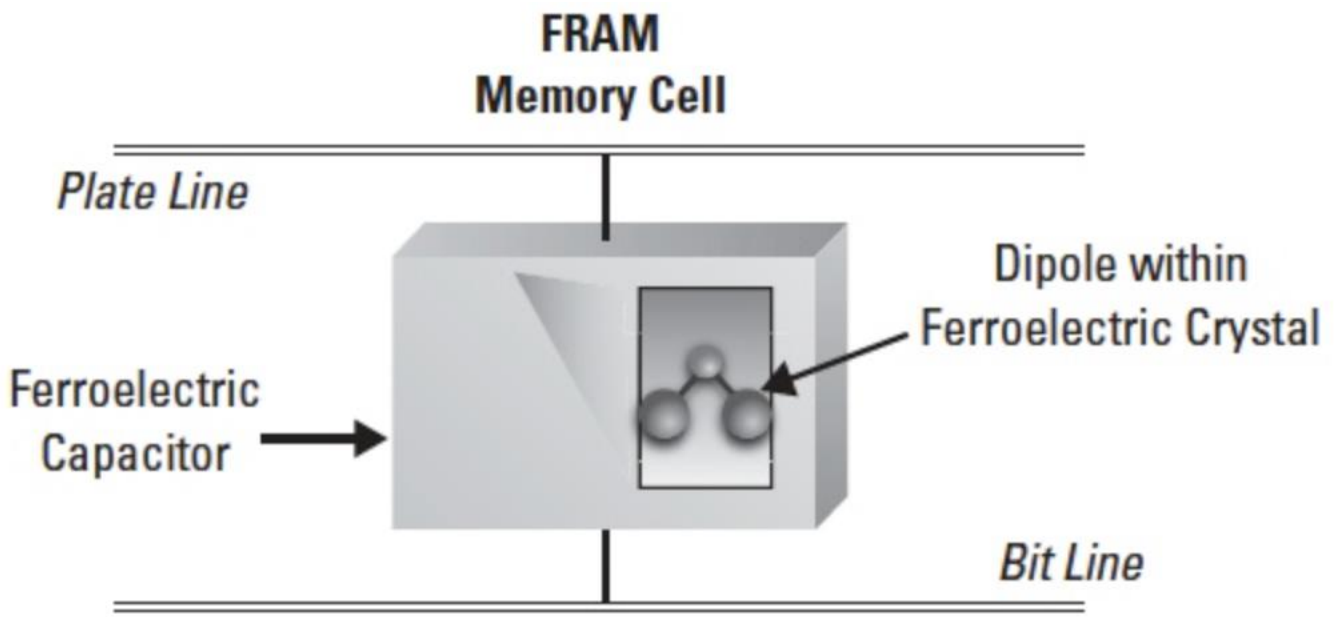
Figure 2-5. Lead-Zirconate-Titanate structure.

FRAM Technology

- Reliability/Security advantages of FRAM Technology
  - The lack of a charge pump removes a key vulnerability against physical attacks.
  - FRAM is also resistant to electric/magnetic fields as well as radiation. Since FRAM state is not stored as a charge, alpha particles are not likely to cause bits to flip and the FRAM Soft Error Rate (SER) is below detectable limits.
  - On top of this resistance to external interference, FRAM is anti-tearing, meaning power lost during a write/erase cycle will not cause data corruption.

http://www.ti.com/lsds/ti/microcontrollers_16-bit_32-bit/msp/ultra-low_power/msp430frxx_fram/what_is_fram.page?DCMP=ep-mcu-msp-fram-en&HQS=ep-mcu-msp-fram-b-lp-en#under

FRAM Read/Write Operations



- Read and write operations represent the fundamental way that data is accessed and stored in semiconductor memory.
- An FRAM memory cell consists of a ferroelectric capacitor containing crystalline PZT, which contain many ferroelectric domains, each of which has the same dipole orientation.
- The capacitor is connected to by a plate line and bit lines (see Figure 2-9) and a transistor switch to access the capacitor. For PZT materials, this is a titanium or zirconium ion in a lead/oxygen crystal lattice.

FRAM Read Operation

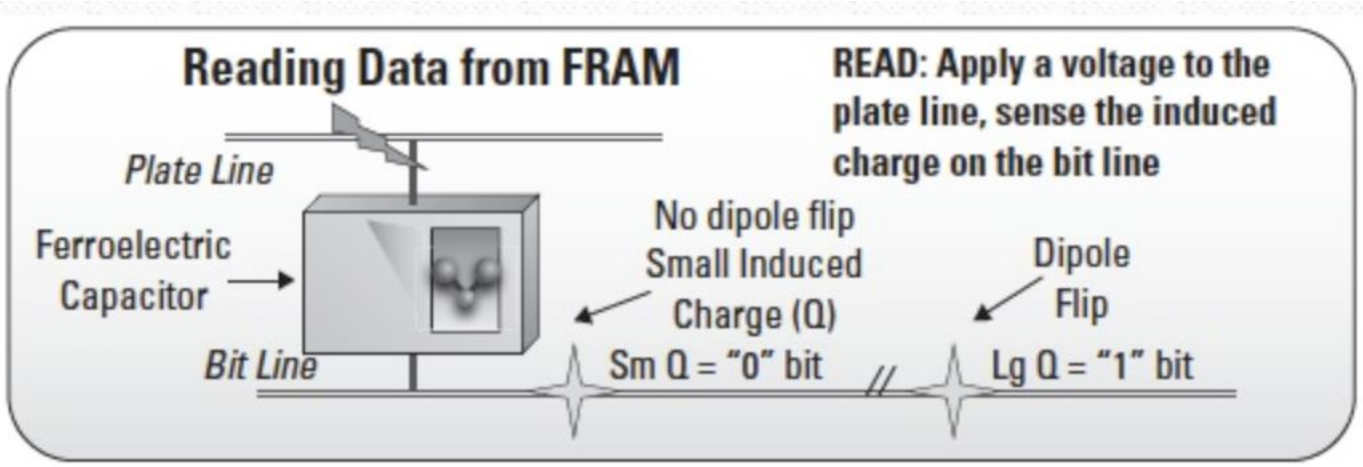


Figure 2-10. Reading a FRAM cell

- To read the data from a FRAM memory cell, a volt…d on the plate line; the key here is that you are al… …o a 0 state. If the voltage causes di… …on, then a large indu…
- If the orien… …ing voltage to the plate … …'t change and a small … …bit line. So, in reading the data from an … …a small induced charge is a 0 bit and a large induced … …is a 1 bit (see Figure 2-10).

Potentially changing the state in order to perform a read, FRAM always requires a memory state refresh after a read.

FRAM Write Operation

- Writing to FRAM is also simple. To write a 1, you apply a voltage to the bit line to force a change in the orientation of the dipole to a positive 1 bit. To write a 0, you apply voltage to the plate line to move state to 0.

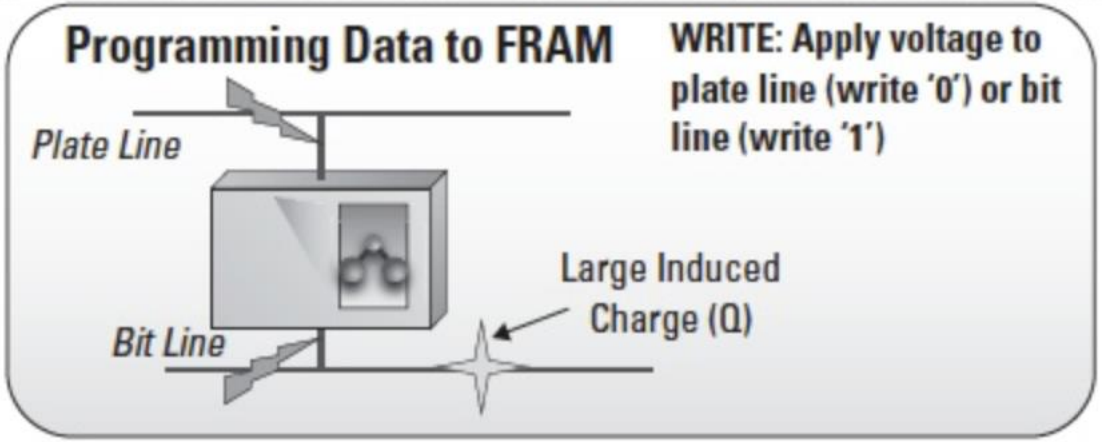


Figure 2-11. Writing to a FRAM cell.

FRAM memory comparisons

All-in-one: FRAM MCU delievers max benefits				
Specifications	**FRAM**	**SRAM**	**EEPROM**	**Flash**
Non-volatile *Retains data w/o power*	Yes	No	Yes	Yes
Write speed *(13 KB)*	10ms	<10ms	2 secs	1 sec
Average active Power [µA/MHz] *16 bit word access by the CPU*	100	<60	50,000+	230
Write endurance	10^{15}	Unlimited	100,000	10,000
Soft Errors	Below Measurable Limits	Yes	Yes	Yes
Bit-wise programmable	Yes	Yes	No	No
Unified Memory *Flexible code and data partitioning*	Yes	No	No	No

* Based on devices from Texas Instruments

http://www.ti.com/lsds/ti/microcontrollers_16-bit_32-bit/msp/ultra-low_power/msp430frxx_fram/what_is_fram.page?DCMP=ep-mcu-msp-fram-en&HQS=ep-mcu-msp-fram-b-lp-en#under

FRAM use cases

- Remote sensing or data logging
  - Lower energy
    - Fast writes
    - Low voltage and current is needed to change FRAM data
  - 10 billion times more cycles than Flash
- Over the air updates
  - Updating FRAM takes 100x less time and 250x less energy/bit
  - No pre-erase required
  - Data can be written on-the-fly
    - Data can be written to FRAM right out of the COMM channel, with no buffering required

http://www.ti.com/lsds/ti/microcontrollers_16-bit_32-bit/msp/ultra-low_power/msp430frxx_fram/what_is_fram.page?DCMP=ep-mcu-msp-fram-en&HQS=ep-mcu-msp-fram-b-lp-en#over-air

FRAM use cases (continued)

- Energy Harvesting
  - Low active duty cycle for non-volatile writes
    - Low average and peak write power leads to low average and peak power consumption of the MCU
  - Faster wakeup time
    - Variables stored in non-volatile FRAM Over the air updates
- Data Security
  - No charge pump needed
  - Resistance to external fields
    - Memory protected from some types of physical attacks
  - State retention on power fail, fast writes and 10 write cycles
    - FRAM is not susceptible to Soft Errors
    - Update security keys quickly and send notifications in case of certain state changes

http://www.ti.com/lsds/ti/microcontrollers_16-bit_32-bit/msp/ultra-low_power/msp430frxx_fram/what_is_fram.page?DCMP=ep-mcu-msp-fram-en&HQS=ep-mcu-msp-fram-b-lp-en#over-air

FRAM Advantages/Disadvantages

- **Advantages**
  - Lower power usage
  - Faster write performance
  - Much larger number of write-erase cycles
- **Disadvantages**
  - Lower storage density
  - Overall capacity limitation
  - Higher cost

The over riding disadvantage is cost. The FRAM cell structure is limited on how small the structure can be made. One limitation is that as structures become small, they tend to stop being ferroelectric. This effect is related to the ferroelectric's "depolarization field. ” Currently TI is building FRAM at 130nm linewidths where flash is being build in line widths as small as 16nm.

Radio-Electronics.com “FRAM Ferroelectric Random Access Memory Tutorial” and https://en.wikipedia.org/wiki/Ferroelectric_RAM#Density