ECEN 5823-001 / -001B

Internet of Things Embedded Firmware

Lecture #28

07 December 2017

Be Boulder.

University of Colorado Boulder

Agenda

- Class announcements
- Google Sign up sheet
- Final Exam
- Final Report
- Memory for the IoT and IIoT markets

Class Announcements

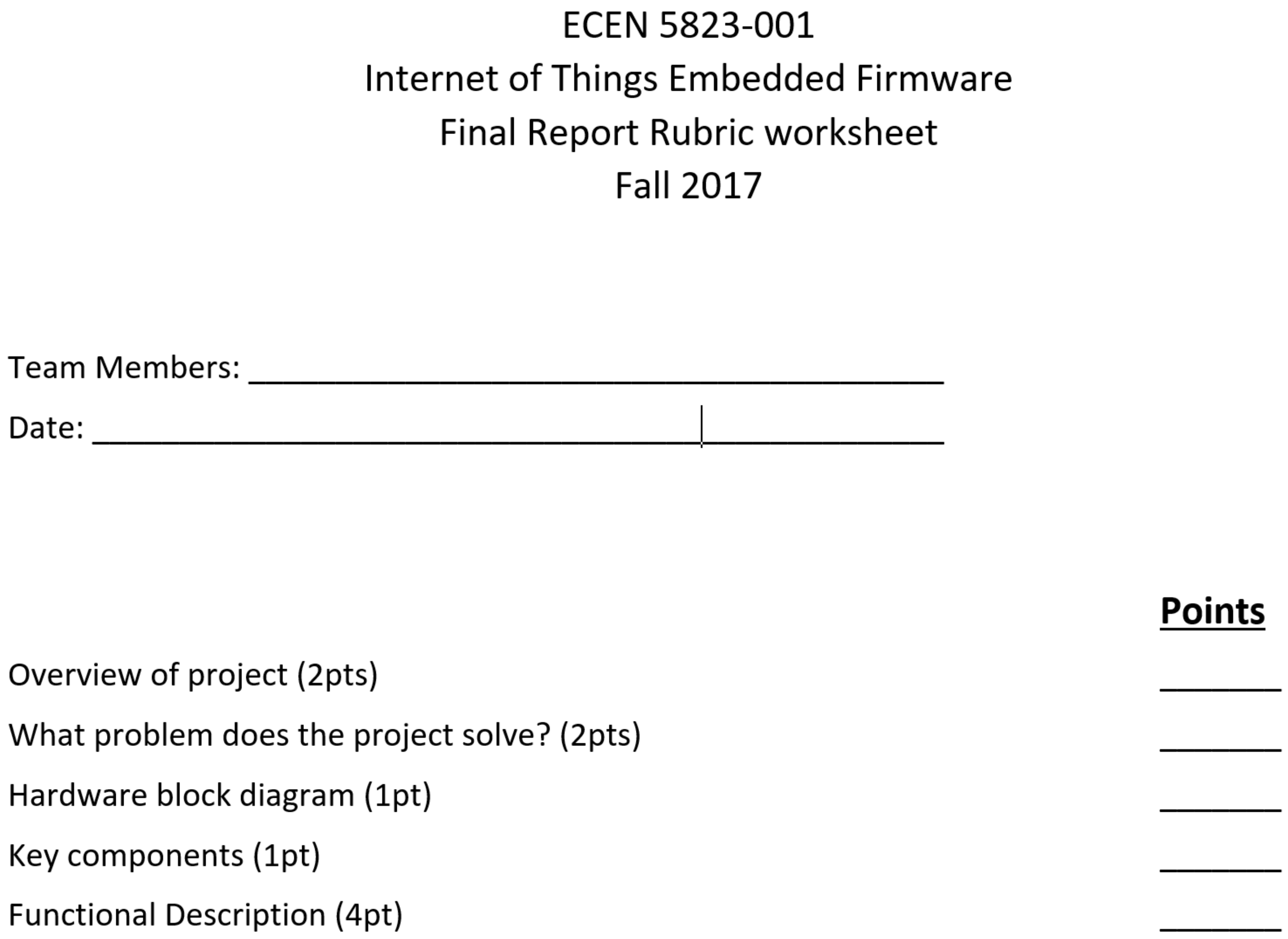
- Quiz 10 is due on Sunday the 10th at 11:59pm
- Any questions regarding the Course Project?
- Any questions regarding Bluetooth Mesh?

Final Exam

- When: Sunday the 17th at 1:30 to 4:00pm
- Where: ECCR 1B51
- Similar format to Mid-Term, D2L base
- Tentatively planning:
    - 40 questions (100% of Final Exam)
        - 2 hours for exam
        - Covering material since Mid-Term plus BLE
        - Any topic related to programming assignments plus course project
    - 5 bonus questions (up to +5% of Final Exam)
        - 5 minutes
        - Past quiz questions from quiz 7, 8, 9, and 10
- Distant Students can take the Final from 1:30pm on Sunday the 17th through 11:59pm on the 17th

Course Project Demo Sign up

- Here is the link to sign up for the course project demos. If you are a distant learning team and there are no appropriate times, we can target Friday the 15th or some other time. Another alternative for distant students is a video conference call. https://docs.google.com/a/colorado.edu/spreadsheets/d/19pyGBCRNCU37iTsneXGnOyGnfPwv31wxGi_yn6B3nuc/edit?usp=sharing



ECEN 5823-001
Internet of Things Embedded Firmware
Final Report Rubric worksheet
Fall 2017

Team Members: ____

Date: ____

	Points
Overview of project (2pts)	________
What problem does the project solve? (2pts)	________
Hardware block diagram (1pt)	________
Key components (1pt)	________
Functional Description (4pt)	________

ECEN 5823-001
Internet of Things Embedded Firmware
Course Project Rubric worksheet
Fa ll2017

Team Members: ______________________________________

Date: ____

Dev kit and sensors returned? ____________________________ (if no, -30%)

Points

Over the Air Updates (1pt) ________

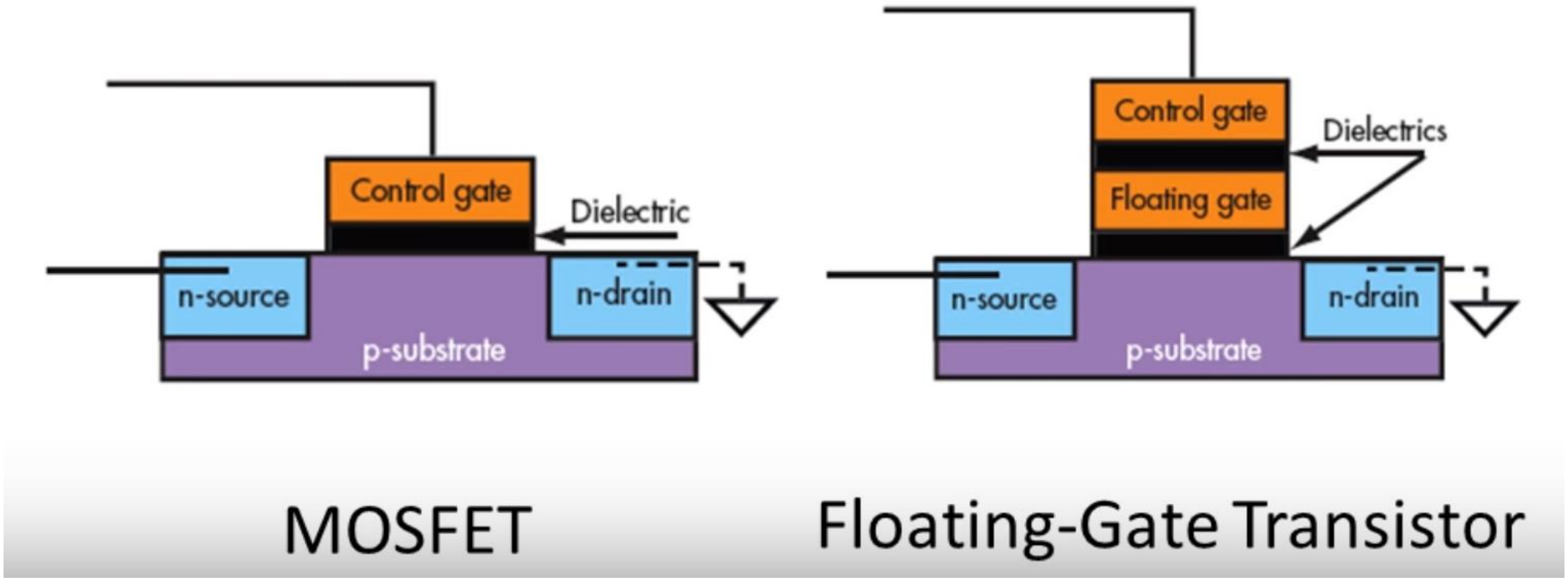
Persistent Memory (1pt) ________

Application use of LCD (1pt) ________

TX Power optimized to the application (1pt) ________

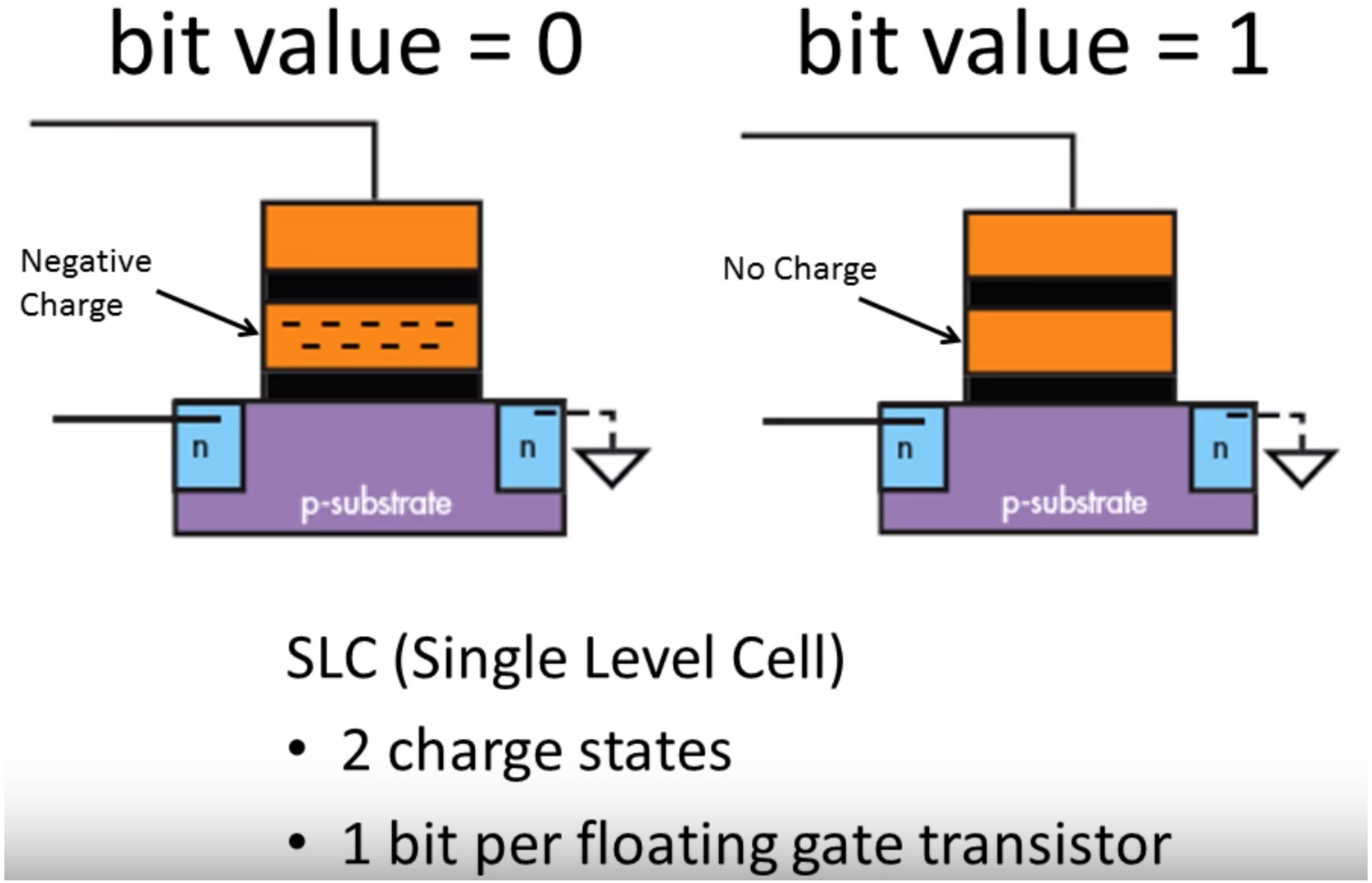
Optimized ConnInterval and SlaveLatency to application (1pt) ________

How does FLASH work?



https://www.youtube.com/watch?v=s7JLXs5es7I&t=140s

How does FLASH work?



bit value = 0

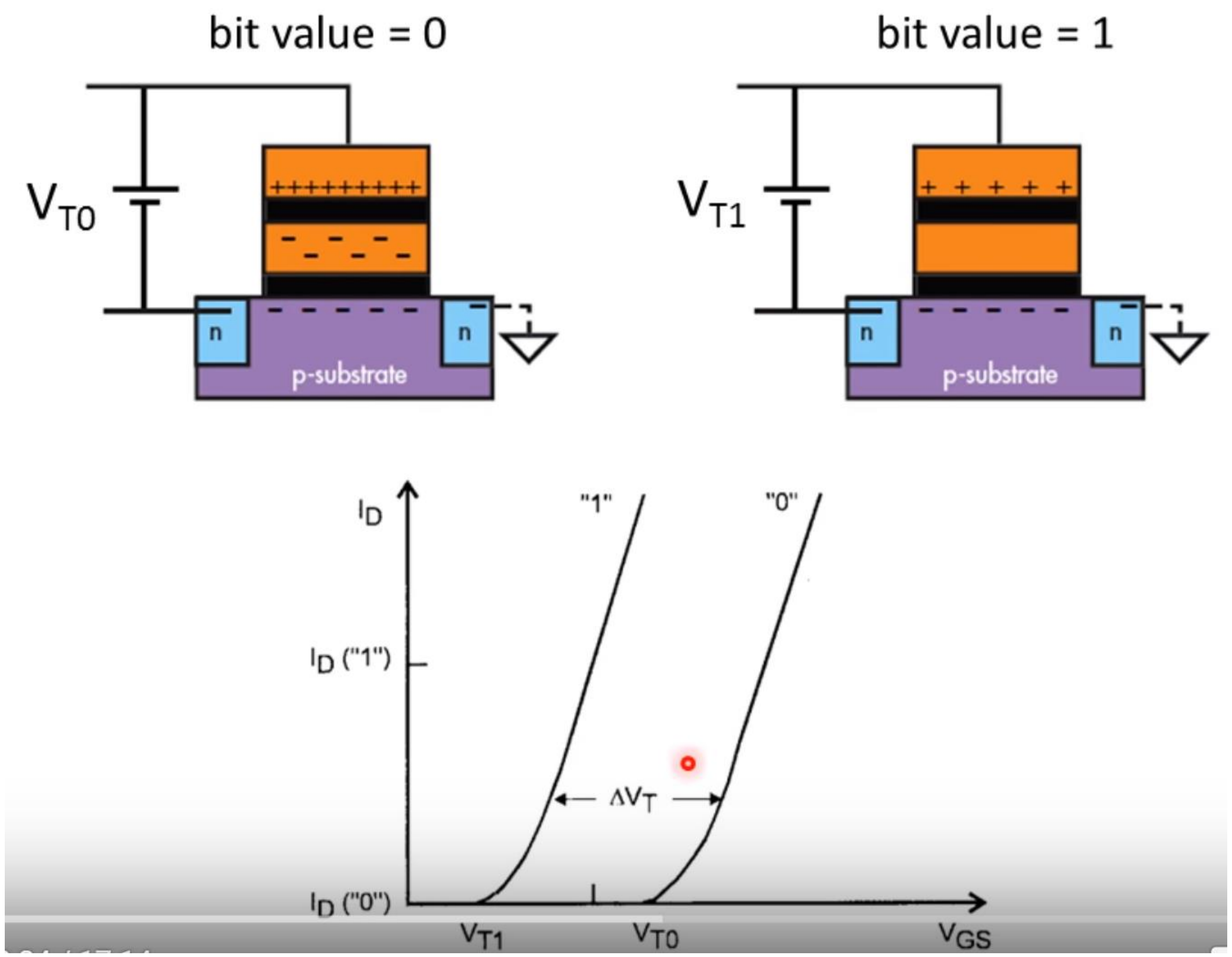
bit value = 1

SLC (Single Level Cell)

- 2 charge states
- 1 bit per floating gate transistor

https://www.youtube.com/watch?v=s7JLXs5es7I&t=140s

How does FLASH work?

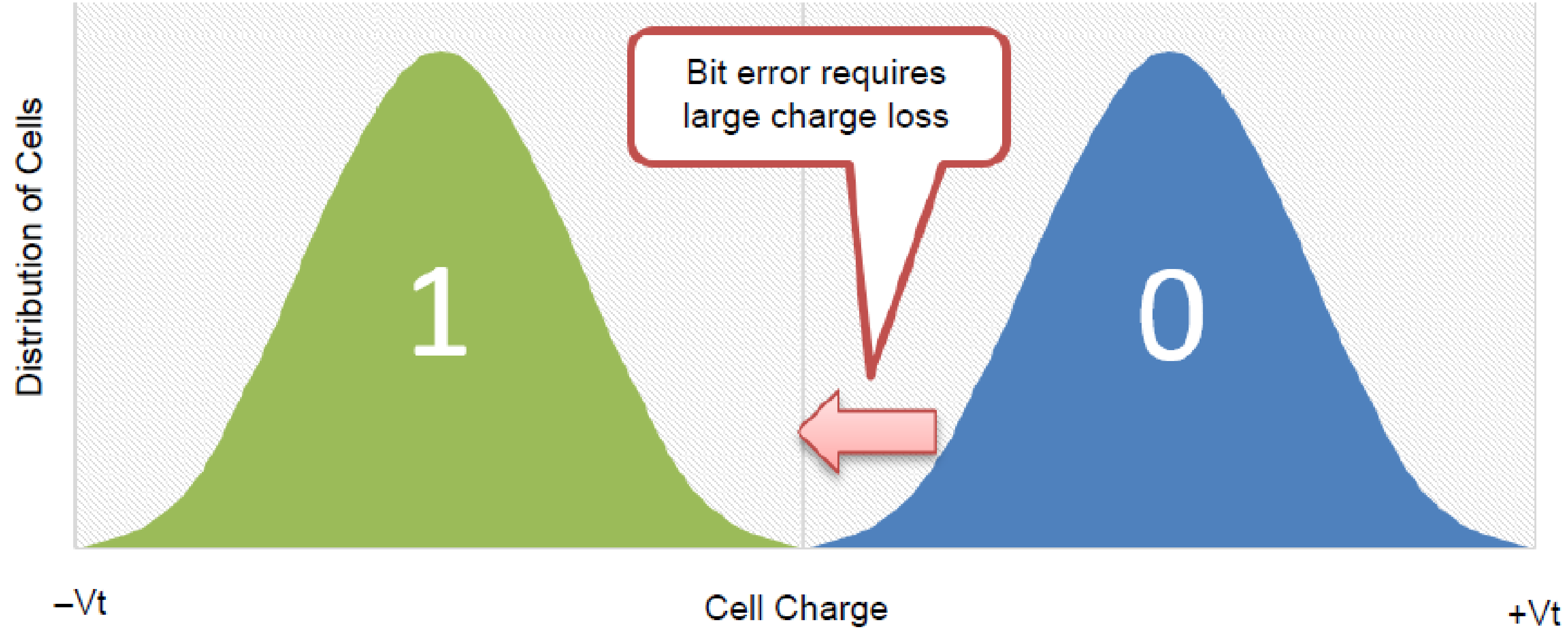


https://www.youtube.com/watch?v=s7JLXs5es7I&t=140s

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.

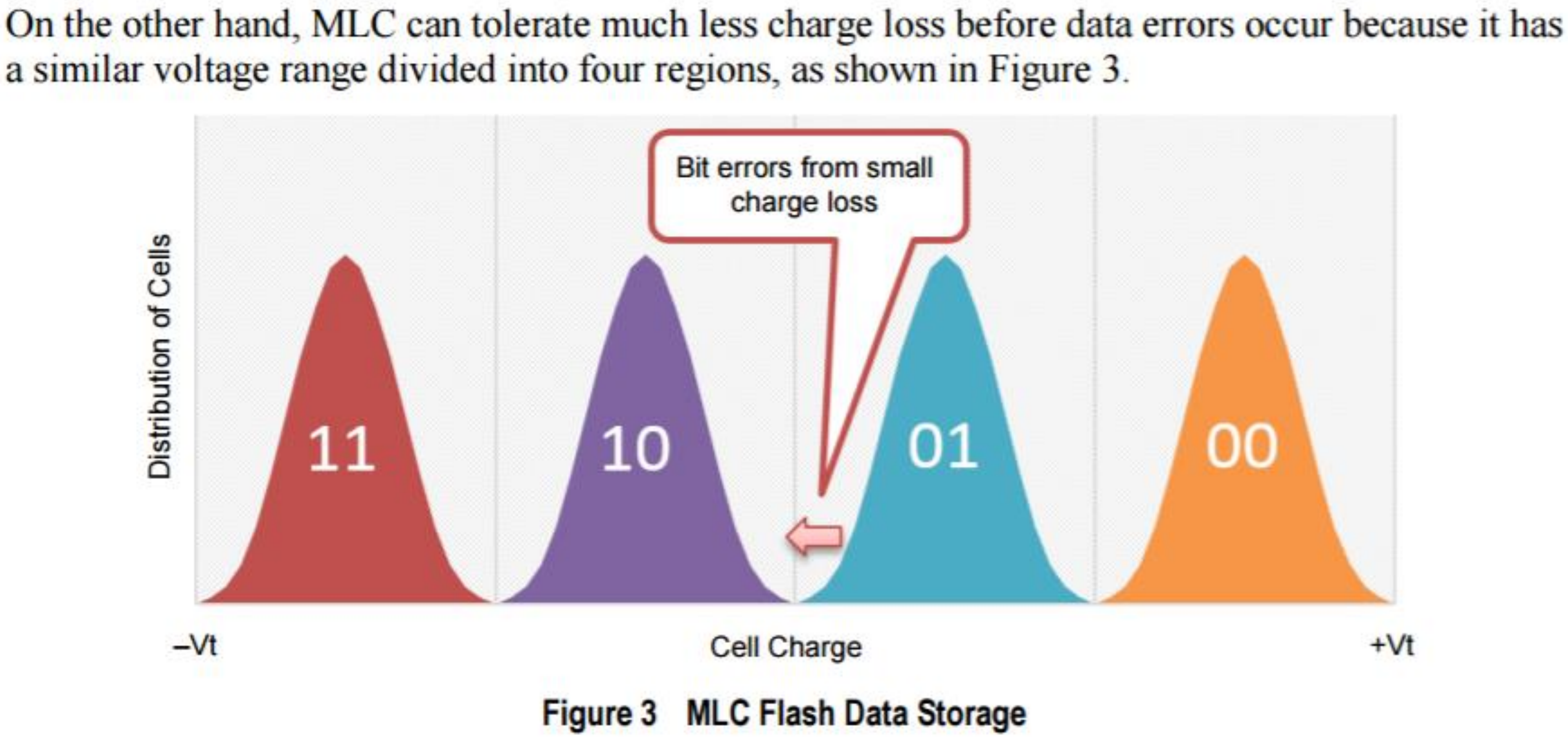
Because SLC flash memory is only divided into two voltage regions, it has more margin for charge loss before a bit flip occurs (a 0 becomes a 1), as shown in Figure 2.



Bit error requires large charge loss

Figure 2 SLC Flash Data Storage

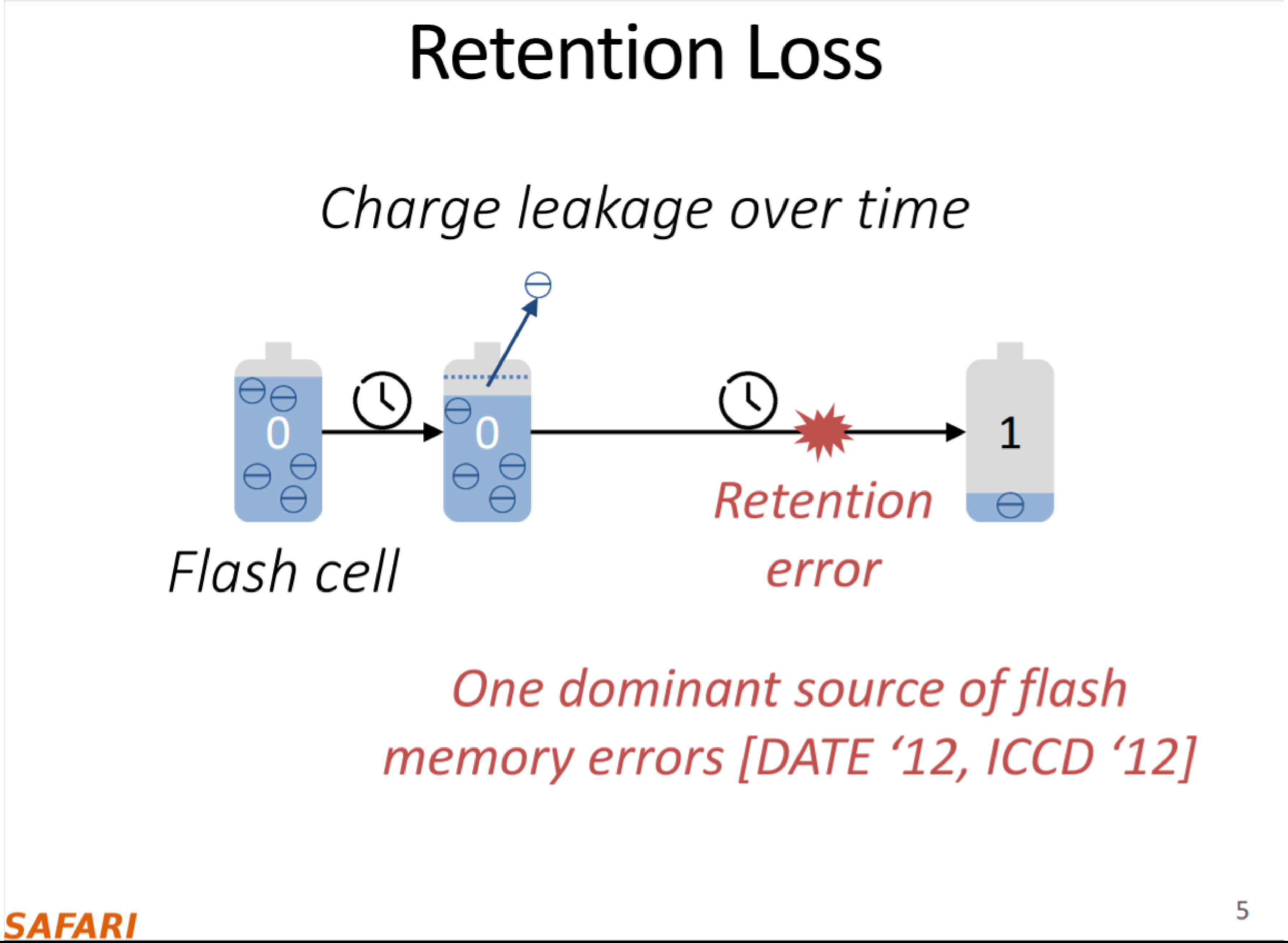
ublications/White%20Papers/0015_NANDflash_IO_20141211.pdf?v=20170217-161047



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

ublications/White%20Papers/0015_NANDflash_IO_20141211.pdf?v=20170217-161047



Retention Loss

Charge leakage over time

0

0

1

Flash cell

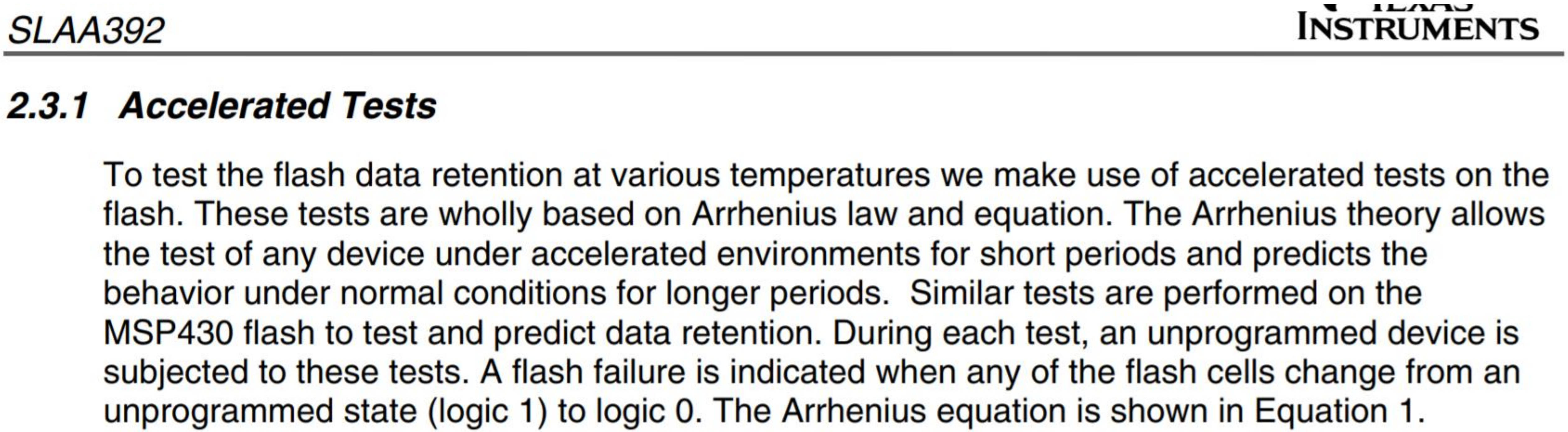
Retention error

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

https://users.ece.cmu.edu/~omutlu/pub/flash-memory-data-retention_yixin_hpca15-talk.pdf

Correction to TI application note SLAA334

- Understanding MSP430 Flash Data Retention, SLAA392



SLAA392 INSTRUMENTS

2.3.1 Accelerated Tests

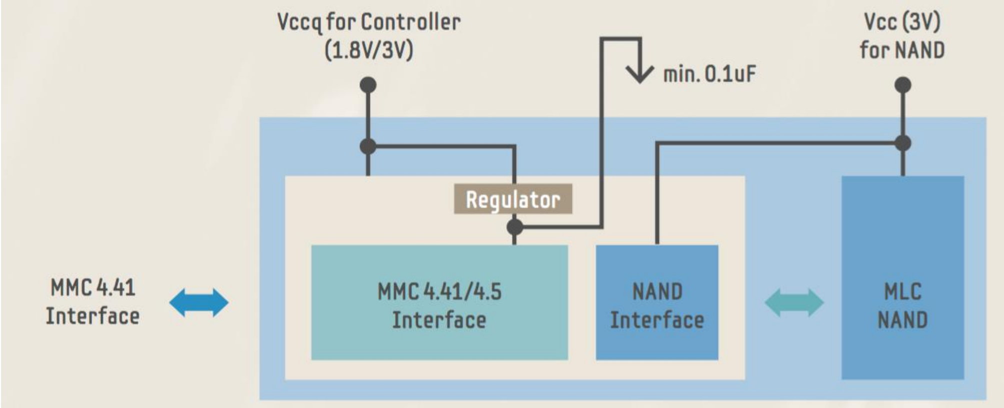
To test the flash data retention at various temperatures we make use of accelerated tests on the flash. These tests are wholly based on Arrhenius law and equation. The Arrhenius theory allows the test of any device under accelerated environments for short periods and predicts the behavior under normal conditions for longer periods. Similar tests are performed on the MSP430 flash to test and predict data retention. During each test, an unprogrammed device is subjected to these tests. A flash failure is indicated when any of the flash cells change from an unprogrammed state (logic 1) to logic 0. The Arrhenius equation is shown in Equation 1.

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

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

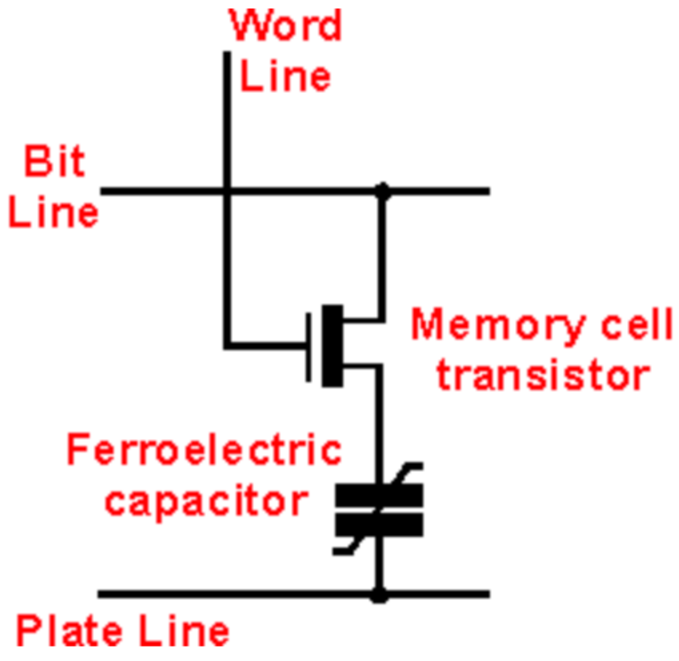
Example of NAND management offload

- 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)

https://www.hyperstone.com/en/S8-SD-eMMC-Flash-Memory-Controller-265.html

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”

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 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.

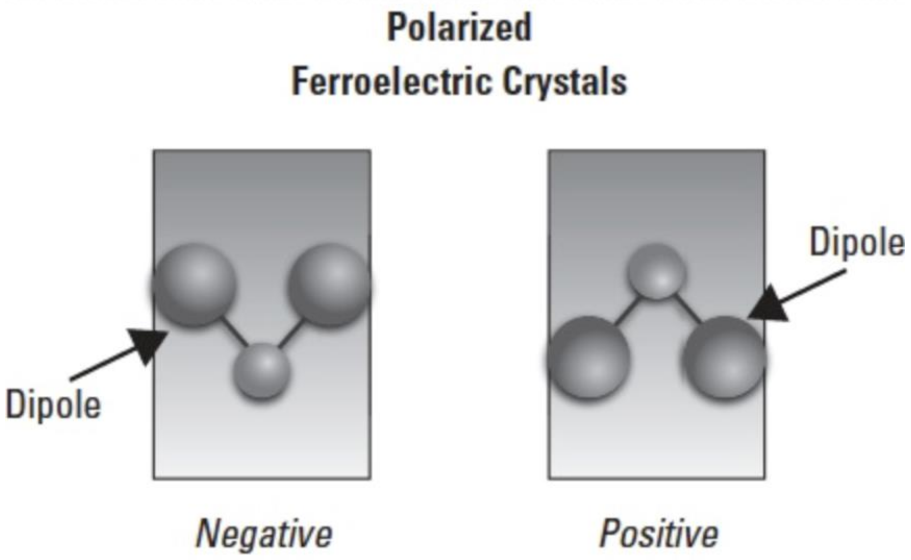


Figure 2-4. Dipole positions of ferroelectric crystals.

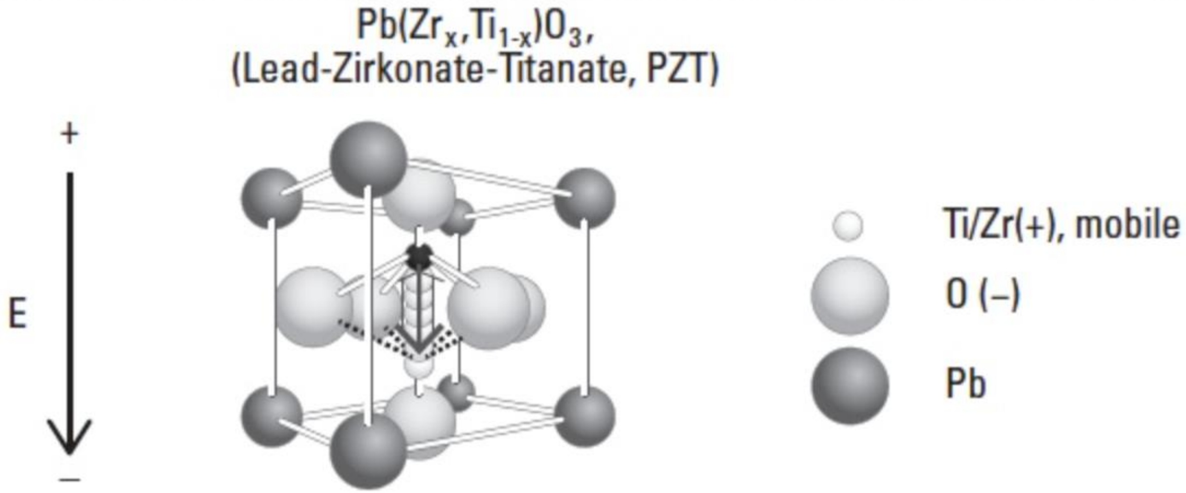


Figure 2-5. Lead-Zirconate-Titanate structure.

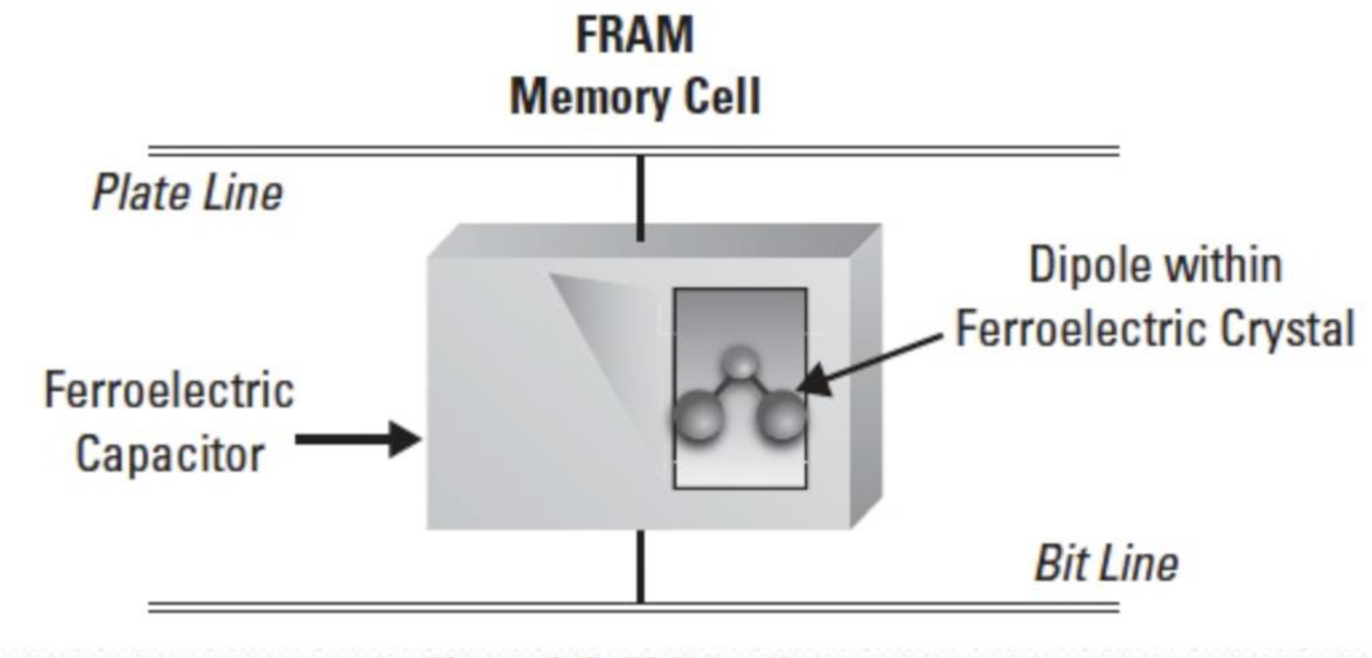
http://www.edn.com/design/systems-design/4394387/2/FRAM-MCUs-For-Dummies--Part-1

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.

http://www.edn.com/design/systems-design/4394387/2/FRAM-MCUs-For-Dummies--Part-1

FRAM Read Operation

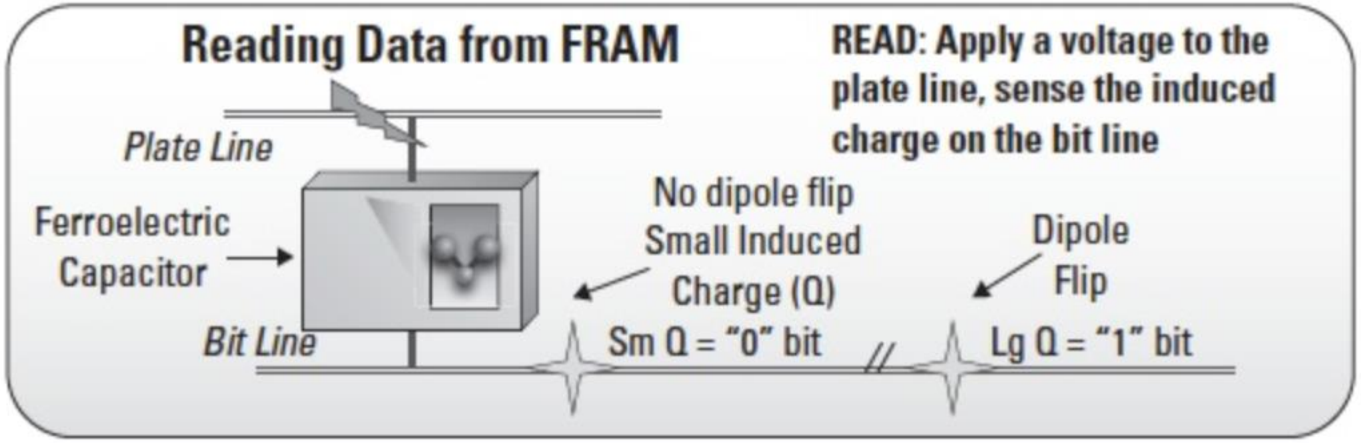

Reading Data from FRAM
READ: Apply a voltage to the plate line, sense the induced charge on the bit line
Plate Line
Ferroelectric Capacitor
Bit Line
No dipole flip Small Induced Charge (Q)
Sm Q = "0" bit
Dipole Flip
Lg Q = "1" bit

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 induc
- If the orien ving 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 ge 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.

http://www.edn.com/design/systems-design/4394387/2/FRAM-MCUs-For-Dummies--Part-1

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.

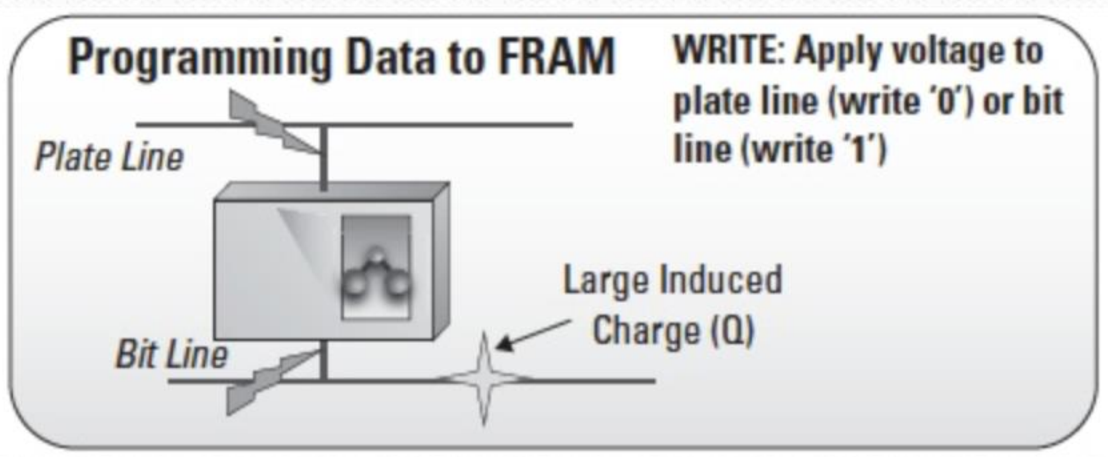
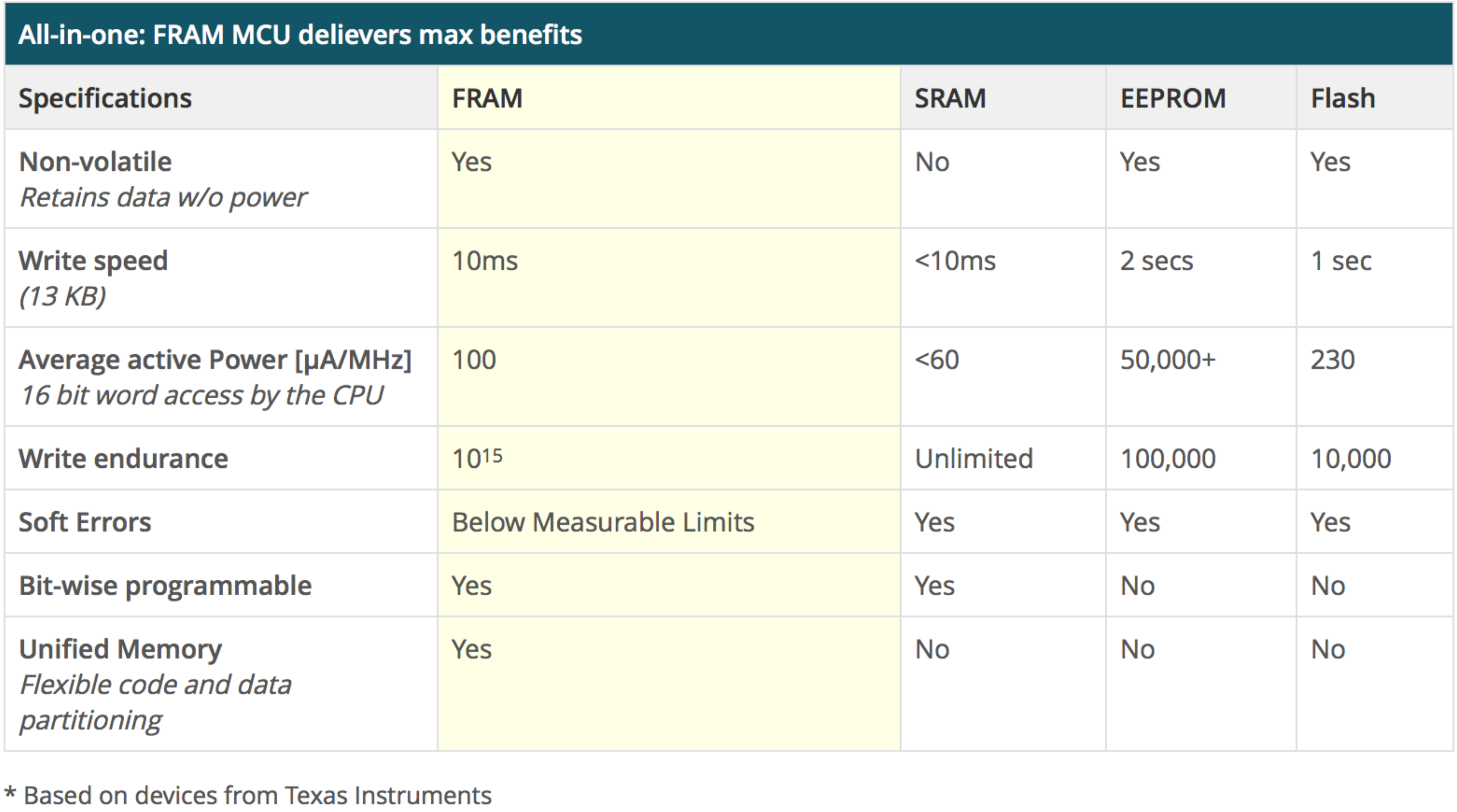

Programming Data to FRAM
WRITE: Apply voltage to plate line (write '0') or bit line (write '1')
Plate Line
Bit Line
Large Induced Charge (Q)

Figure 2-11. Writing to a FRAM cell.

http://www.edn.com/design/systems-design/4394387/2/FRAM-MCUs-For-Dummies--Part-1

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

EEPROM

- EEPROM – Electrically Erasable Programmable Read Only Memory
- A form of NOR flash that has been optimized for:
  - Byte writeable
  - Increased endurance
  - Possibly ECC
- Due to its optimization, it is more expensive to implement on a microcontroller than NOR flash
  - Larger cell size
  - Limits the EEPROM portion of a controller for data storage

Dynamic Memory (DDR3, DDR3L, LPDDR3

- DDRx – often referred to as (JEDEC) standard or commodity DRAM or just DRAM (DDR, DDR2, DDR3. etc.) JEDEC standard JESD79E, etc
- LPDDRx – Referred to as low power, mobile or wireless DRAM (LPDDR, LPDDR2, LPDDR3). Also defined by JEDEC standard JESD209A, etc
- In most system, the type of DRAM will be limited by the micro processor, DSP, or FPGA memory controller, thus the DRAM should be included in the decision of these devices.
- Most common DRAM in today's mobile devices will be DDR2 or DDR3

http://www.freescale.com/files/training/doc/dwf/DWF13_AMF_ENT_T1070.pdf

DDR3 comparisons

- LPDDR3
  - Core voltage: 1.2v (1.8v WL required)
  - I/O voltage: 1.2v
  - Max Data rate: DDR1600
  - Pin Cofig: 16x, 32x
  - Partial Array Self-Refresh: individual bank and segment masking for partial-bank modes
  - Deep Power Down Mode: Yes

- DDR3
  - Core voltage: 1.5v
  - I/O voltage: 1.5v
  - Max data rate: DDR2100
  - Pin Conf: 4x, 8x, 16x
  - Partial Array Self-Refresh: Optional
  - Deep Power Down Mode: No

- DDR3L
  - Core voltage: 1.3v
  - I/O voltage: 1.3v
  - Max data rate: DDR2100
  - Pin Conf: 4x, 8x, 16x
  - Partial Array Self-Refresh: Optional
  - Deep Power Down Mode: No

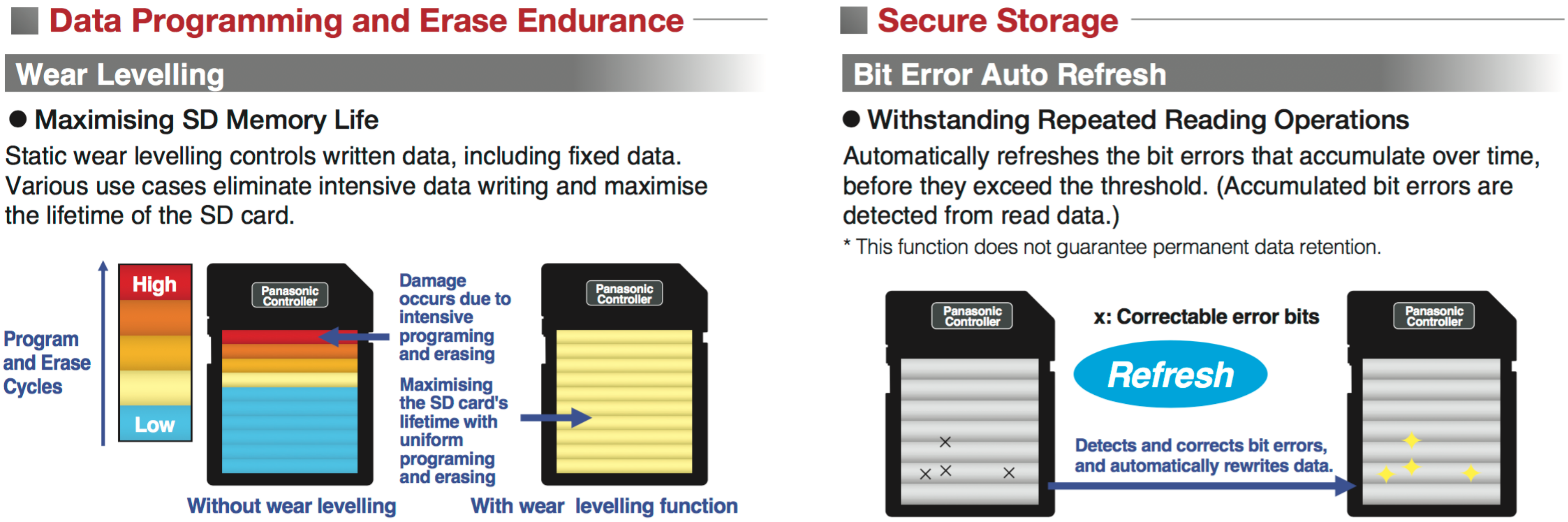
http://www.freescale.com/files/training/doc/dwf/DWF13_AMF_ENT_T1070.pdf

SDxx memory cards provide:

- SPI bus to interface to micro controllers
- Card Security
  - Commands to disable writes
  - Write-protect notch
  - Card password
  - DRM copy-protection
- Real World Performance Issues:
  - Write Amplification
  - File Fragmentation

https://en.wikipedia.org/wiki/Secure_Digital

Example of Industrial SD memory card



Data Programming and Erase Endurance

Wear Levelling

● **Maximising SD Memory Life**

Static wear levelling controls written data, including fixed data. Various use cases eliminate intensive data writing and maximise the lifetime of the SD card.

Program and Erase Cycles
High
Low
Panasonic Controller
Damage occurs due to intensive programing and erasing
Maximising the SD card's lifetime with uniform programing and erasing
Panasonic Controller
Without wear levelling
With wear levelling function

Secure Storage

Bit Error Auto Refresh

● **Withstanding Repeated Reading Operations**

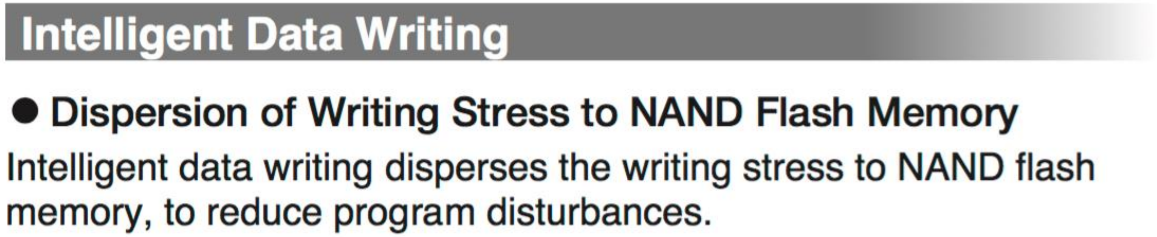
Automatically refreshes the bit errors that accumulate over time, before they exceed the threshold. (Accumulated bit errors are detected from read data.)

* This function does not guarantee permanent data retention.

Panasonic Controller
x: Correctable error bits
Refresh
Detects and corrects bit errors, and automatically rewrites data.
Panasonic Controller

Panasonic Industrial SD memory card brochure

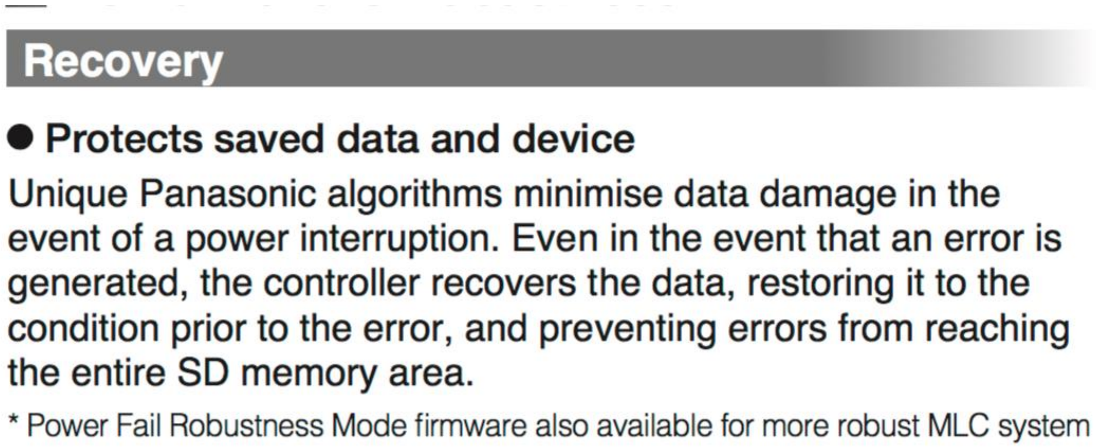
Example of Industrial SD memory card (Cont.)



Intelligent Data Writing

- **Dispersion of Writing Stress to NAND Flash Memory**

Intelligent data writing disperses the writing stress to NAND flash memory, to reduce program disturbances.



Recovery

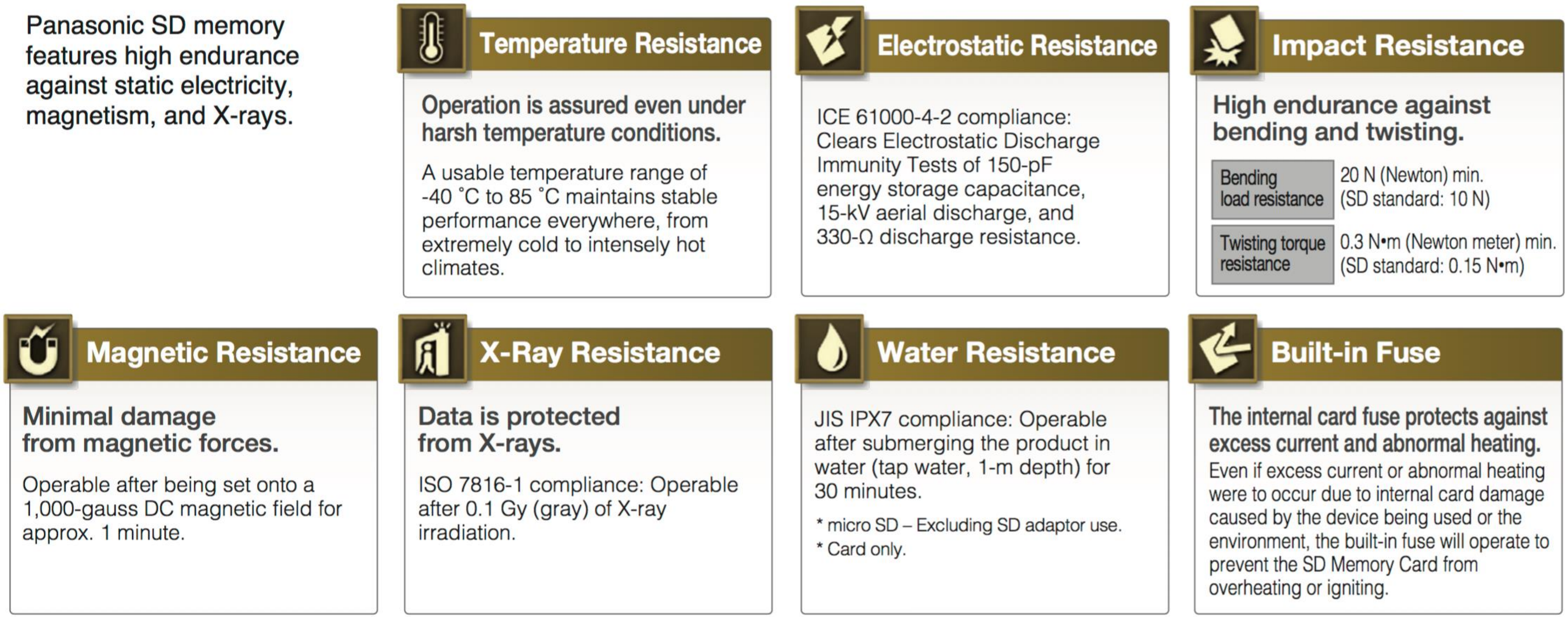
- **Protects saved data and device**

Unique Panasonic algorithms minimise data damage in the event of a power interruption. Even in the event that an error is generated, the controller recovers the data, restoring it to the condition prior to the error, and preventing errors from reaching the entire SD memory area.

* Power Fail Robustness Mode firmware also available for more robust MLC system

Panasonic Industrial SD memory card brochure

Example of Industrial SD memory card (cont.)



Panasonic SD memory features high endurance against static electricity, magnetism, and X-rays.

Temperature Resistance

Operation is assured even under harsh temperature conditions.

A usable temperature range of -40 ˚C to 85 ˚C maintains stable performance everywhere, from extremely cold to intensely hot climates.

Electrostatic Resistance

ICE 61000-4-2 compliance: Clears Electrostatic Discharge Immunity Tests of 150-pF energy storage capacitance, 15-kV aerial discharge, and 330-Ω discharge resistance.

Impact Resistance

High endurance against bending and twisting.

Bending load resistance	20 N (Newton) min. (SD standard: 10 N)
Twisting torque resistance	0.3 N•m (Newton meter) min. (SD standard: 0.15 N•m)

Magnetic Resistance

Minimal damage from magnetic forces.

Operable after being set onto a 1,000-gauss DC magnetic field for approx. 1 minute.

X-Ray Resistance

Data is protected from X-rays.

ISO 7816-1 compliance: Operable after 0.1 Gy (gray) of X-ray irradiation.

Water Resistance

JIS IPX7 compliance: Operable after submerging the product in water (tap water, 1-m depth) for 30 minutes.

* micro SD – Excluding SD adaptor use.

* Card only.

Built-in Fuse

The internal card fuse protects against excess current and abnormal heating.

Even if excess current or abnormal heating were to occur due to internal card damage caused by the device being used or the environment, the built-in fuse will operate to prevent the SD Memory Card from overheating or igniting.

Panasonic Industrial SD memory card brochure