ECEN 5823-001 / -001B

Internet of Things Embedded Firmware

Lecture #26

30 November 2017

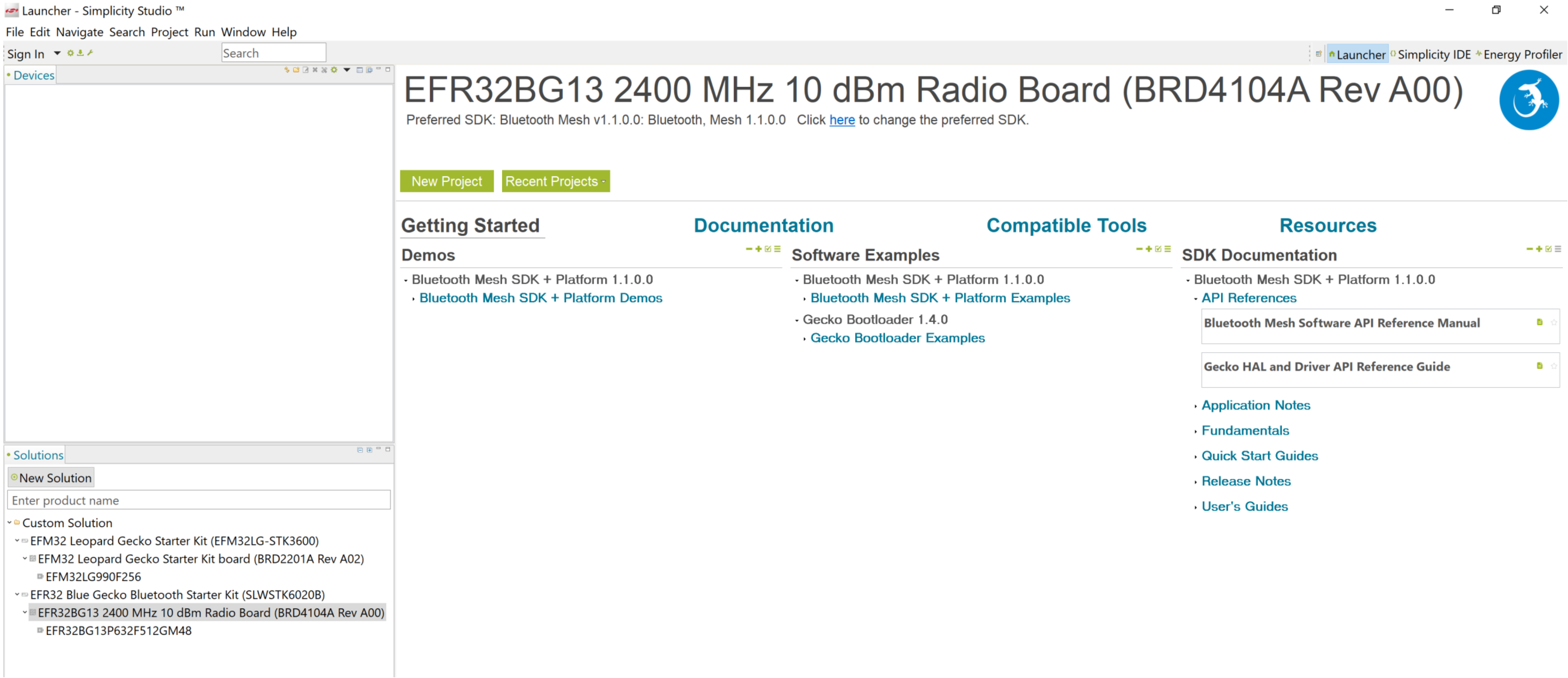
Be Boulder.

University of Colorado Boulder

Agenda

- Class announcements
- Bluetooth Mesh documentation
- ECEN 5013-003, ASIPs and IP Processor Core
- Course Project update #1 feedback
- Course Project update #2
- Quiz 9
- Memory for the IoT and IIoT markets

Bluetooth Mesh APIs



Custom Solution
- EFM32 Leopard Gecko Starter Kit (EFM32LG-STK3600)
  - EFM32 Leopard Gecko Starter Kit board (BRD2201A Rev A02)
    - EFM32LG990F256
- EFR32 Blue Gecko Bluetooth Starter Kit (SLWSTK6020B)
  - EFR32BG13 2400 MHz 10 dBm Radio Board (BRD4104A Rev A00)
    - EFR32BG13P632F512GM48

EFR32BG13 2400 MHz 10 dBm Radio Board (BRD4104A Rev A00)

Preferred SDK: Bluetooth Mesh v1.1.0.0: Bluetooth, Mesh 1.1.0.0   Click here to change the preferred SDK.

Getting Started | Documentation | Compatible Tools | Resources

Demos

- Bluetooth Mesh SDK + Platform 1.1.0.0
  - Bluetooth Mesh SDK + Platform Demos

Software Examples

- Bluetooth Mesh SDK + Platform 1.1.0.0
  - Bluetooth Mesh SDK + Platform Examples
- Gecko Bootloader 1.4.0
  - Gecko Bootloader Examples

SDK Documentation

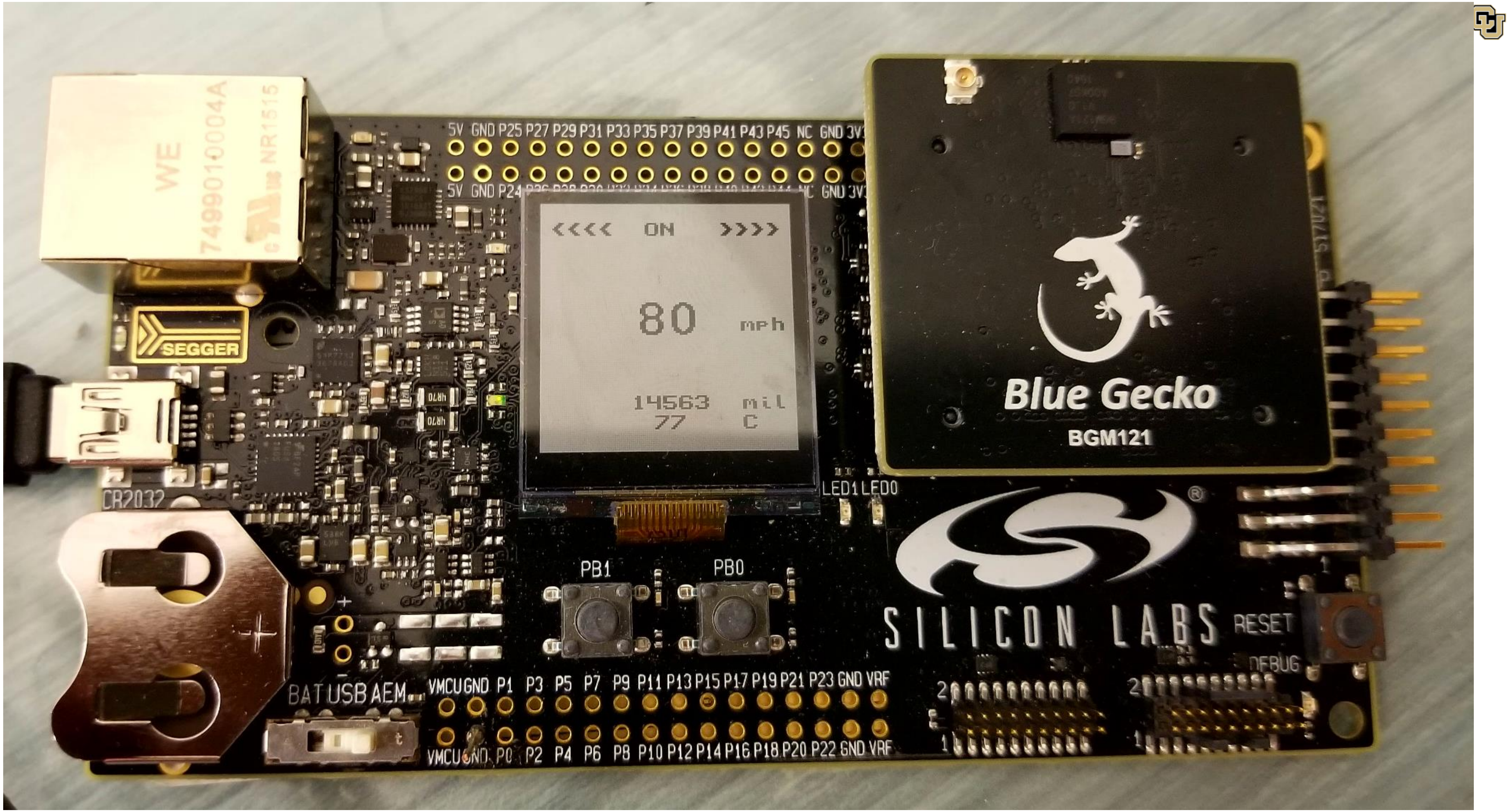
- Bluetooth Mesh SDK + Platform 1.1.0.0
  - API References
    - Bluetooth Mesh Software API Reference Manual
    - Gecko HAL and Driver API Reference Guide
  - Application Notes
  - Fundamentals
  - Quick Start Guides
  - Release Notes
  - User's Guides

Class Announcements

- No quiz this week
- Course Project Update #2 is due at 11:59pm this Wednesday the 6th
- Bonus #4, Implementing LCD and fully implementing scheduler, is due by 11:59pm this Saturday the 2nd
  - Since it is a bonus, it must be done during a convenient time for the instructing team and do not expect to get a time at 11:59 on the 18th to demo your OTA bonus assignment
  - This will not be used an excuse to request an extension
- Any questions regarding the Course Project?
- Any questions regarding Bluetooth Mesh?
- I will be forwarding up a google sheet to sign up for project demo times
  - Targeting by Monday the 4th

Course Project – 4th Bonus Opportunity

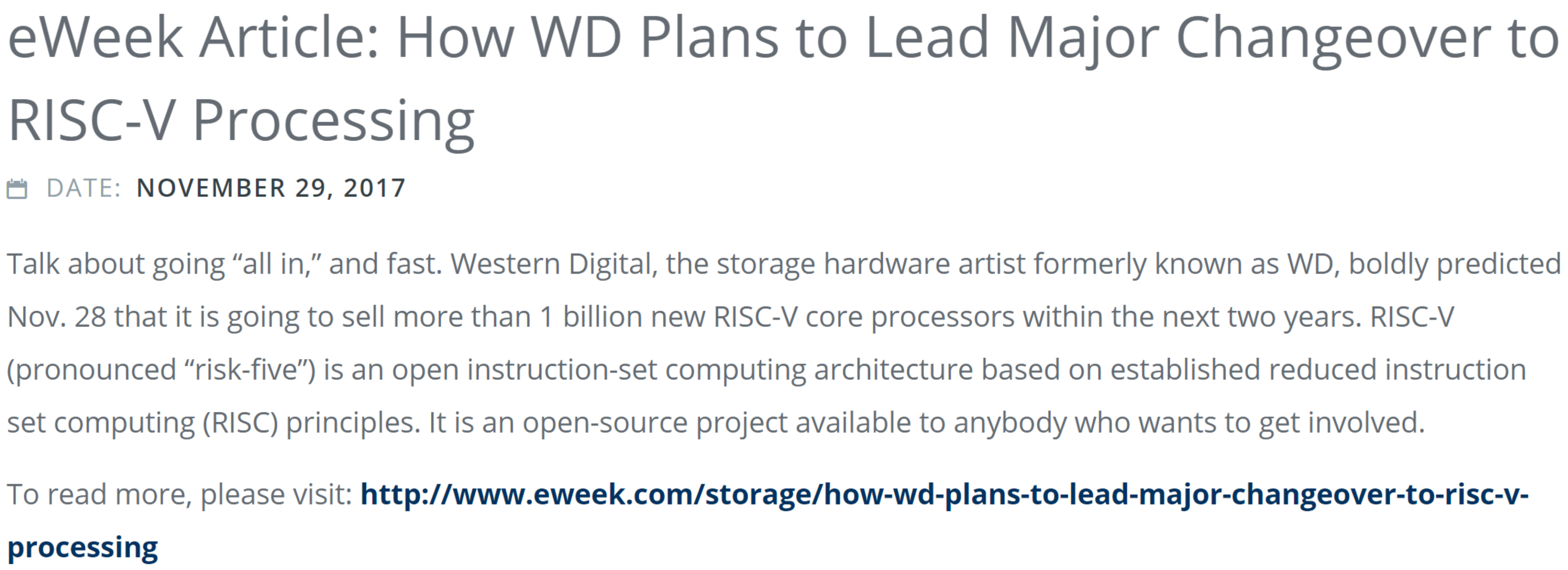
- Implementing LCD and fully implementing scheduler
- Opportunity is worth 1% towards your final grade!
- You will need demonstrate end application usage on the LCD and walking through code to demonstrate the proper minimal coding within Interrupt Handlers and using a scheduler to service the interrupts.
- Requirements to get the extra credit:
  - Must demo to one of the three instructing team members by Saturday, December 2nd, at 11:59pm
  - By being a bonus, you must demo during convenient instructing team availability and not expect availability at 11:58pm on December 2nd
  - For distant students, the demo should be arranged over video chat, skype, etc.


SEGGER
CR2032
<<<< ON >>>>
80 mph
14563 mil
77 C
Blue Gecko
BGM121
LED1 LED0
PB1
PB0
SILICON LABS
RESET
DEBUG
BAT USB AEM
VMCU GND P1 P3 P5 P7 P9 P11 P13 P15 P17 P19 P21 P23 GND VRF
VMCU GND P0 P2 P4 P6 P8 P10 P12 P14 P16 P18 P20 P22 GND VRF
5V GND P25 P27 P29 P31 P33 P35 P37 P39 P41 P43 P45 NC GND 3V3
5V GND P24

RISC-V conference

- 500 attendees
- Presentations from Companies and Universities from 4 continents
- Exploring RISC-V architectures to accelerate:
  - General Processing
  - Security
  - Interpretive based languages such as Java
  - Virtual Machines
  - Artificial Intelligence
  - And many more applications

RISC-V Conference



eWeek Article: How WD Plans to Lead Major Changeover to RISC-V Processing

DATE: **NOVEMBER 29, 2017**

Talk about going “all in,” and fast. Western Digital, the storage hardware artist formerly known as WD, boldly predicted Nov. 28 that it is going to sell more than 1 billion new RISC-V core processors within the next two years. RISC-V (pronounced “risk-five”) is an open instruction-set computing architecture based on established reduced instruction set computing (RISC) principles. It is an open-source project available to anybody who wants to get involved.

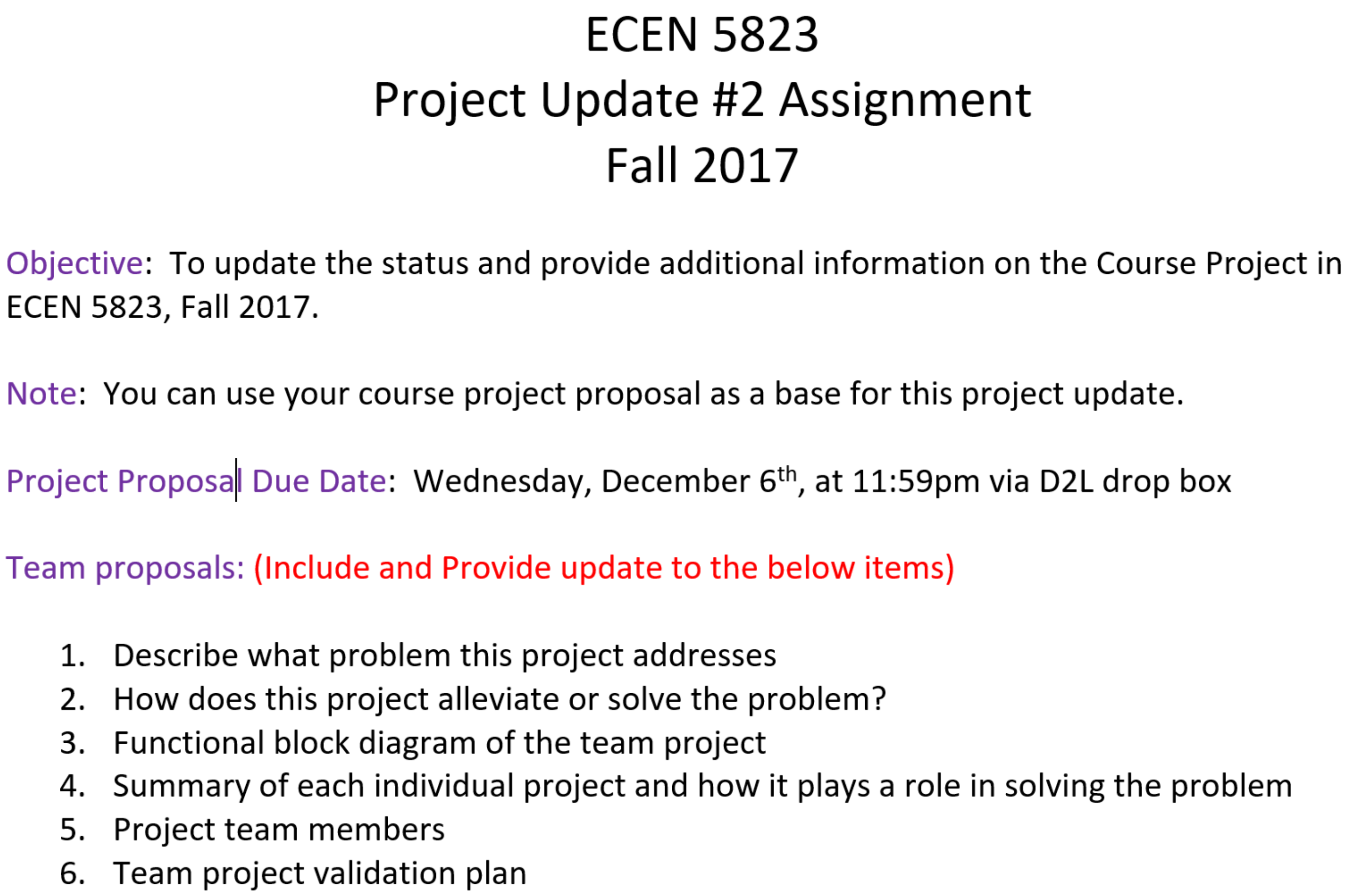
To read more, please visit: **http://www.eweek.com/storage/how-wd-plans-to-lead-major-changeover-to-risc-v-processing**

http://www.eweek.com/storage/how-wd-plans-to-lead-major-changeover-to-risc-v-processing

Project Update #1 feedback

- Generally very good
- But a majority of projects did not provide fine enough granularity in their verification test plans

Project Update #2



ECEN 5823
Project Update #2 Assignment
Fall 2017

Objective: To update the status and provide additional information on the Course Project in ECEN 5823, Fall 2017.

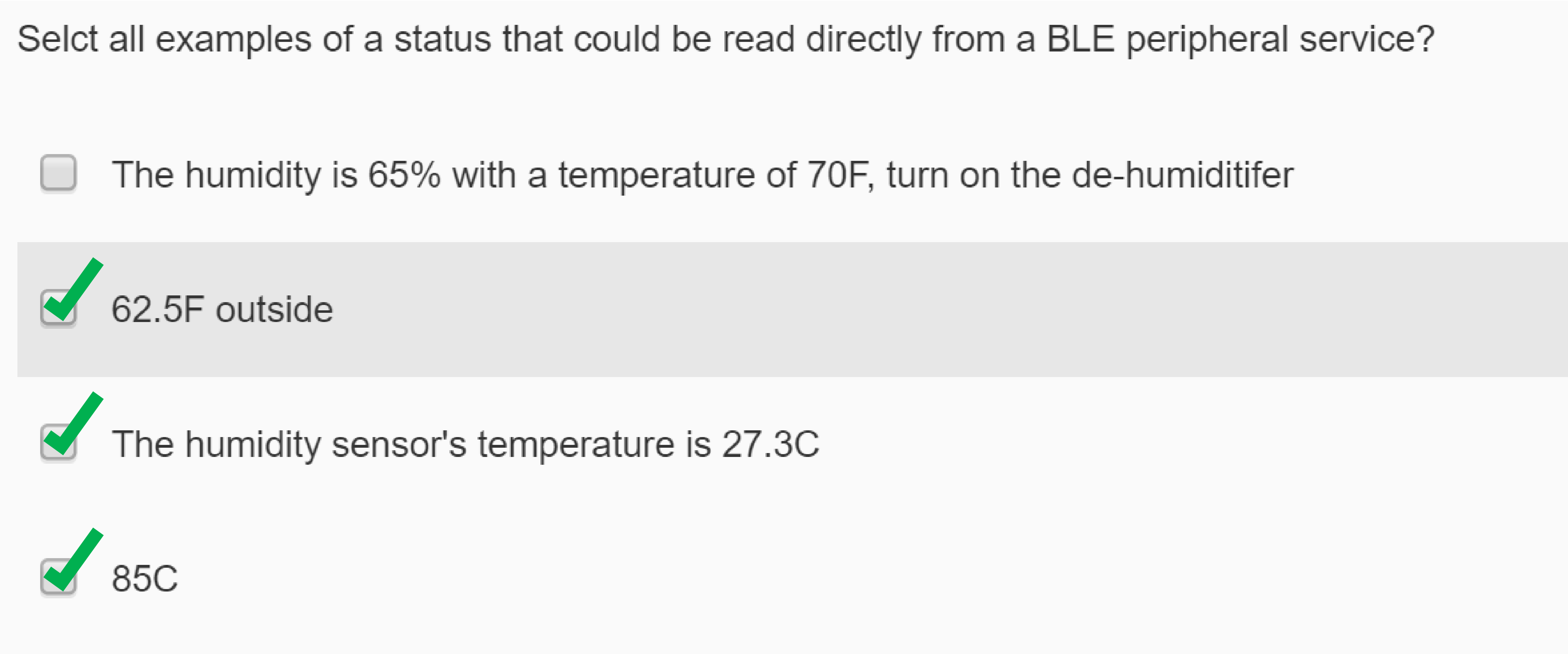
Note: You can use your course project proposal as a base for this project update.

Project Proposal Due Date: Wednesday, December 6th, at 11:59pm via D2L drop box

Team proposals: (Include and Provide update to the below items)

1. Describe what problem this project addresses
2. How does this project alleviate or solve the problem?
3. Functional block diagram of the team project
4. Summary of each individual project and how it plays a role in solving the problem
5. Project team members
6. Team project validation plan

Quiz 9 review



Selct all examples of a status that could be read directly from a BLE peripheral service?

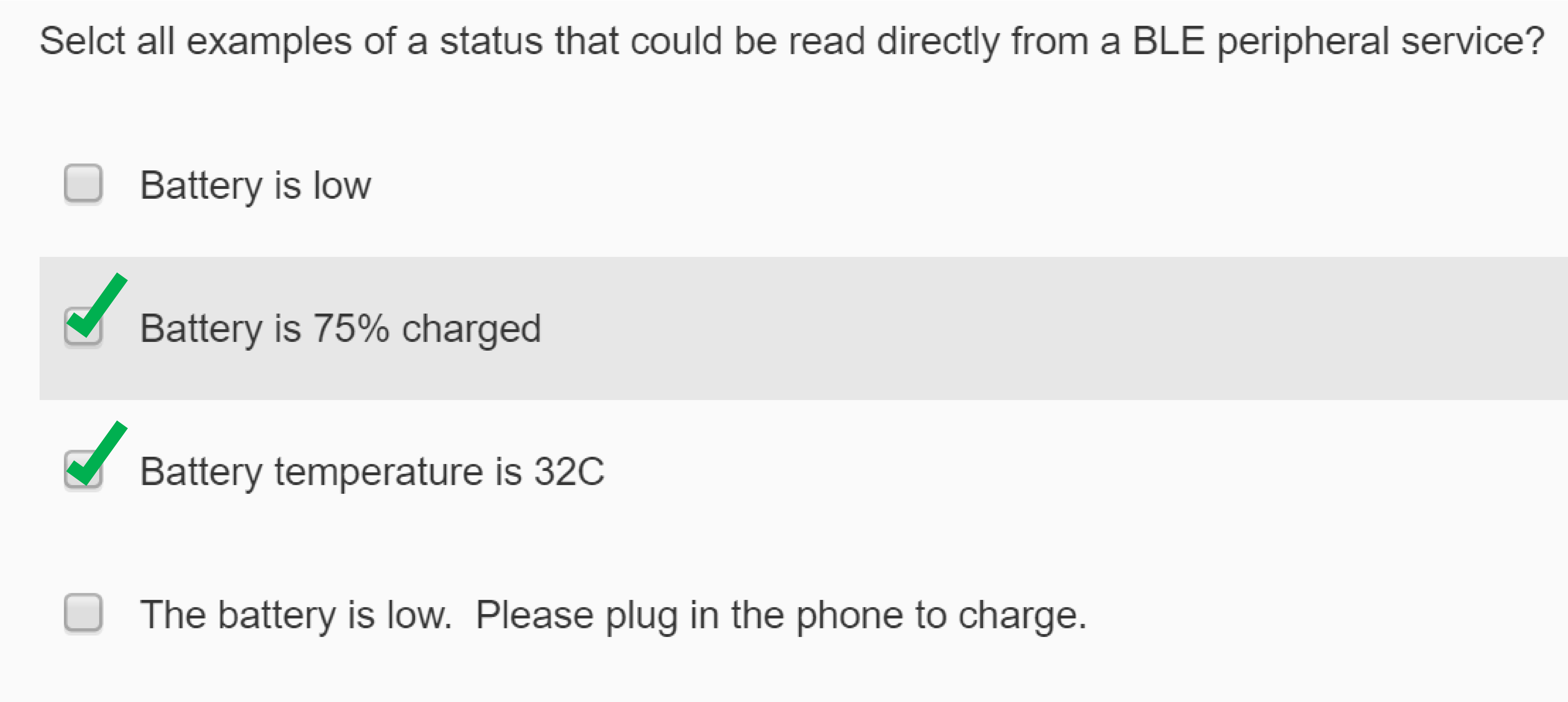
□ The humidity is 65% with a temperature of 70F, turn on the de-humiditifer

☑ 62.5F outside

☑ The humidity sensor's temperature is 27.3C

☑ 85C

Quiz 9 review



Selct all examples of a status that could be read directly from a BLE peripheral service?

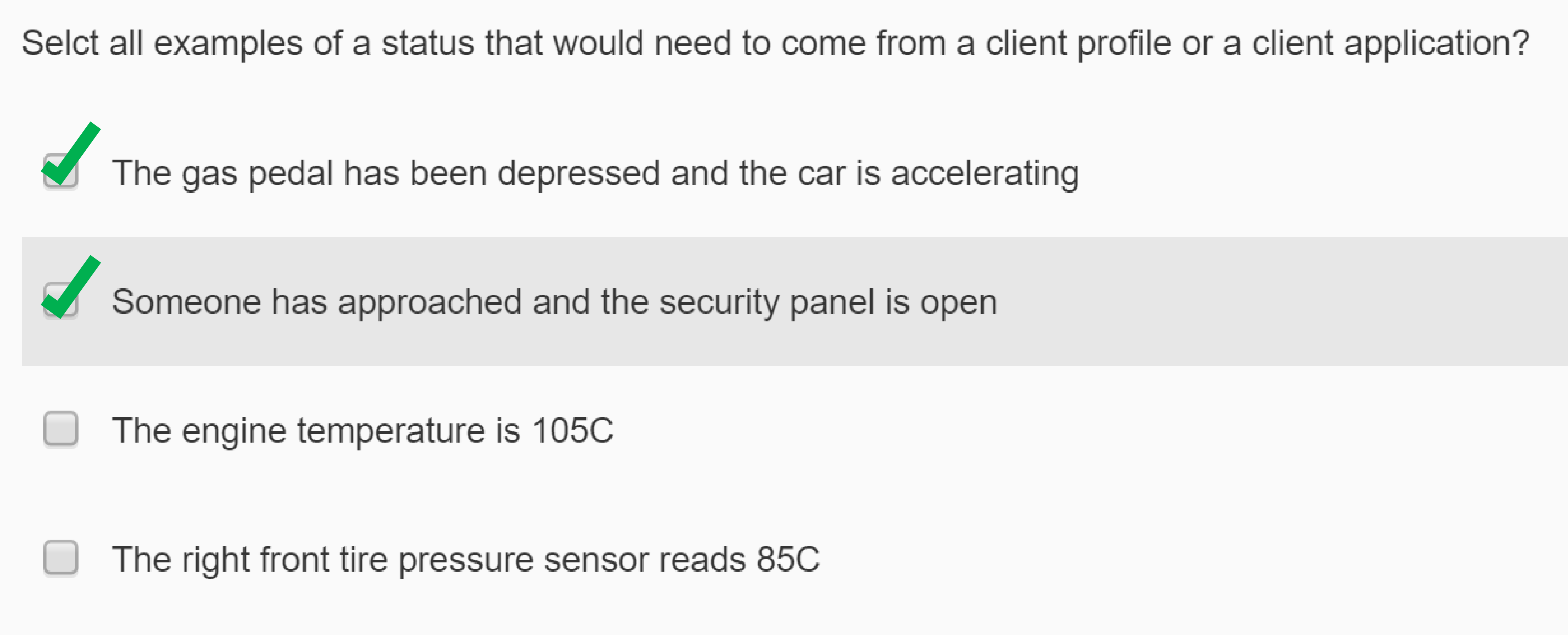
□ Battery is low

☑ Battery is 75% charged

☑ Battery temperature is 32C

□ The battery is low. Please plug in the phone to charge.

Quiz 9 review



Selct all examples of a status that would need to come from a client profile or a client application?

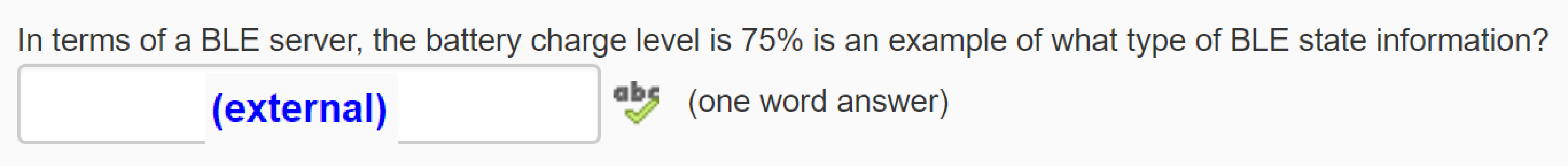
☑ The gas pedal has been depressed and the car is accelerating

☑ Someone has approached and the security panel is open

□ The engine temperature is 105C

□ The right front tire pressure sensor reads 85C

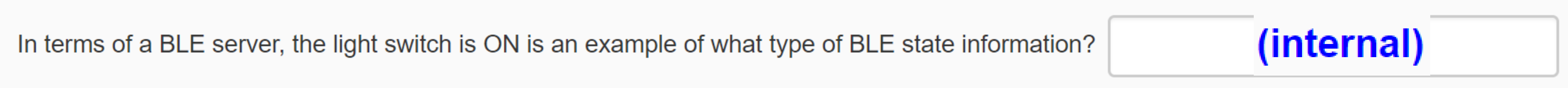
Quiz 9 review



In terms of a BLE server, the battery charge level is 75% is an example of what type of BLE state information?

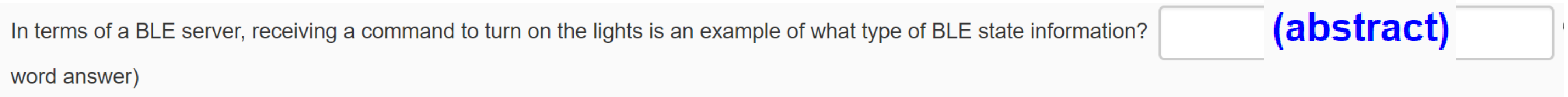
(external) (one word answer)

Quiz 9 review



In terms of a BLE server, the light switch is ON is an example of what type of BLE state information? (internal)

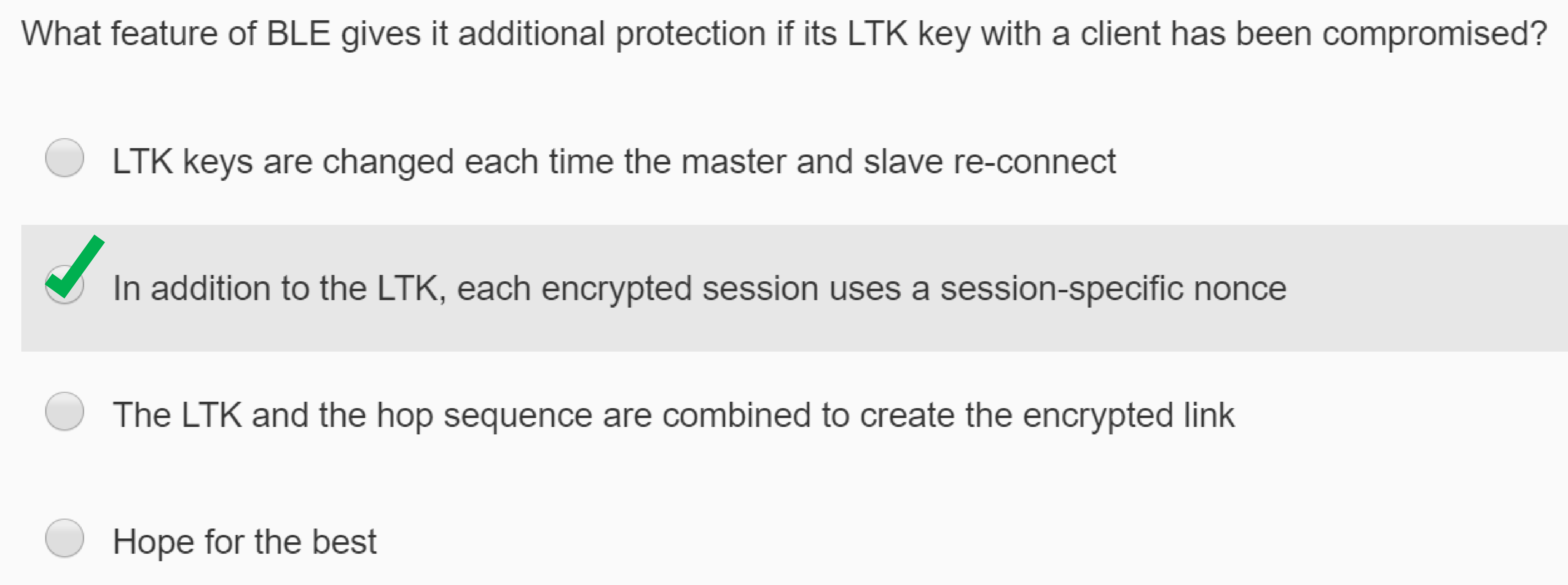
Quiz 9 review



In terms of a BLE server, receiving a command to turn on the lights is an example of what type of BLE state information? (abstract)

word answer)

Quiz 9 review



What feature of BLE gives it additional protection if its LTK key with a client has been compromised?

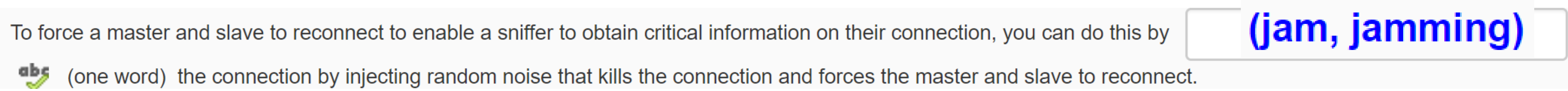
○ LTK keys are changed each time the master and slave re-connect

✓ In addition to the LTK, each encrypted session uses a session-specific nonce

○ The LTK and the hop sequence are combined to create the encrypted link

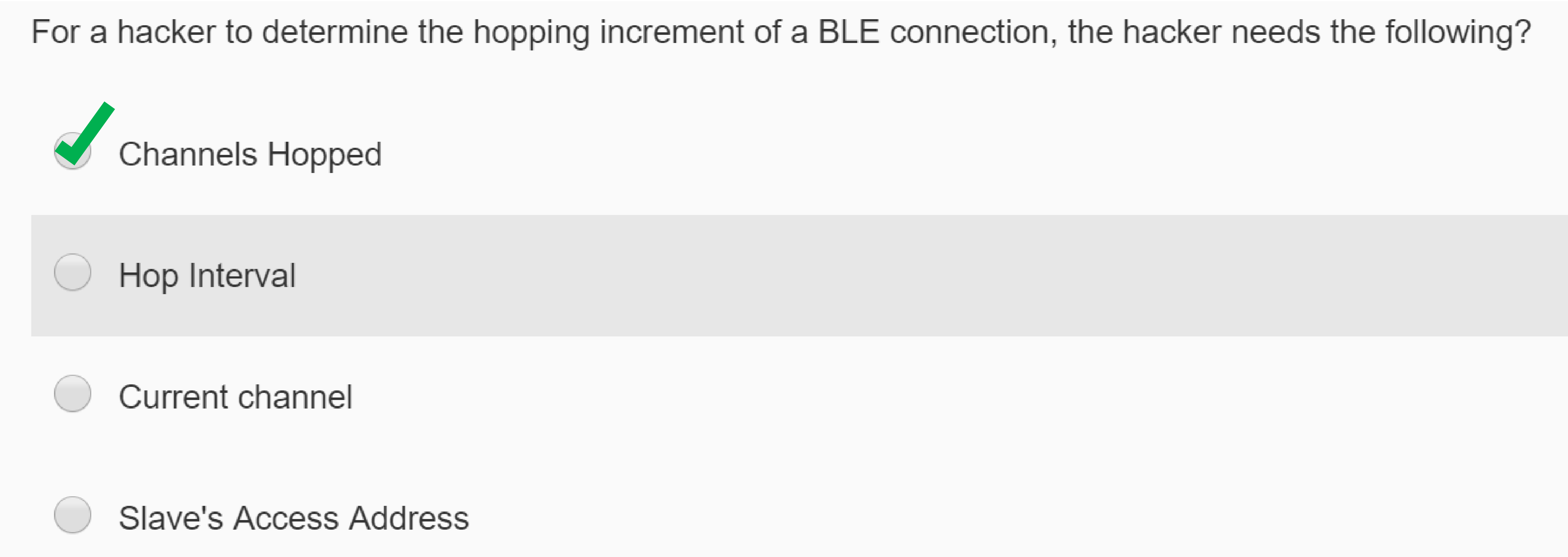
○ Hope for the best

Quiz 9 review



To force a master and slave to reconnect to enable a sniffer to obtain critical information on their connection, you can do this by (jam, jamming) (one word) the connection by injecting random noise that kills the connection and forces the master and slave to reconnect.

Quiz 9 review



For a hacker to determine the hopping increment of a BLE connection, the hacker needs the following?

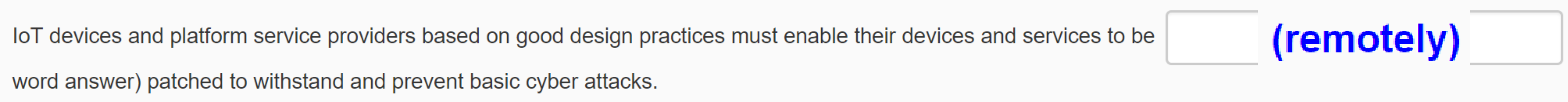
✓ Channels Hopped

○ Hop Interval

○ Current channel

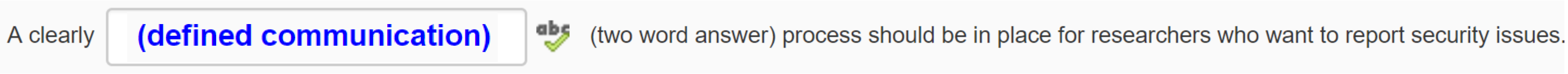
○ Slave's Access Address

Quiz 9 review



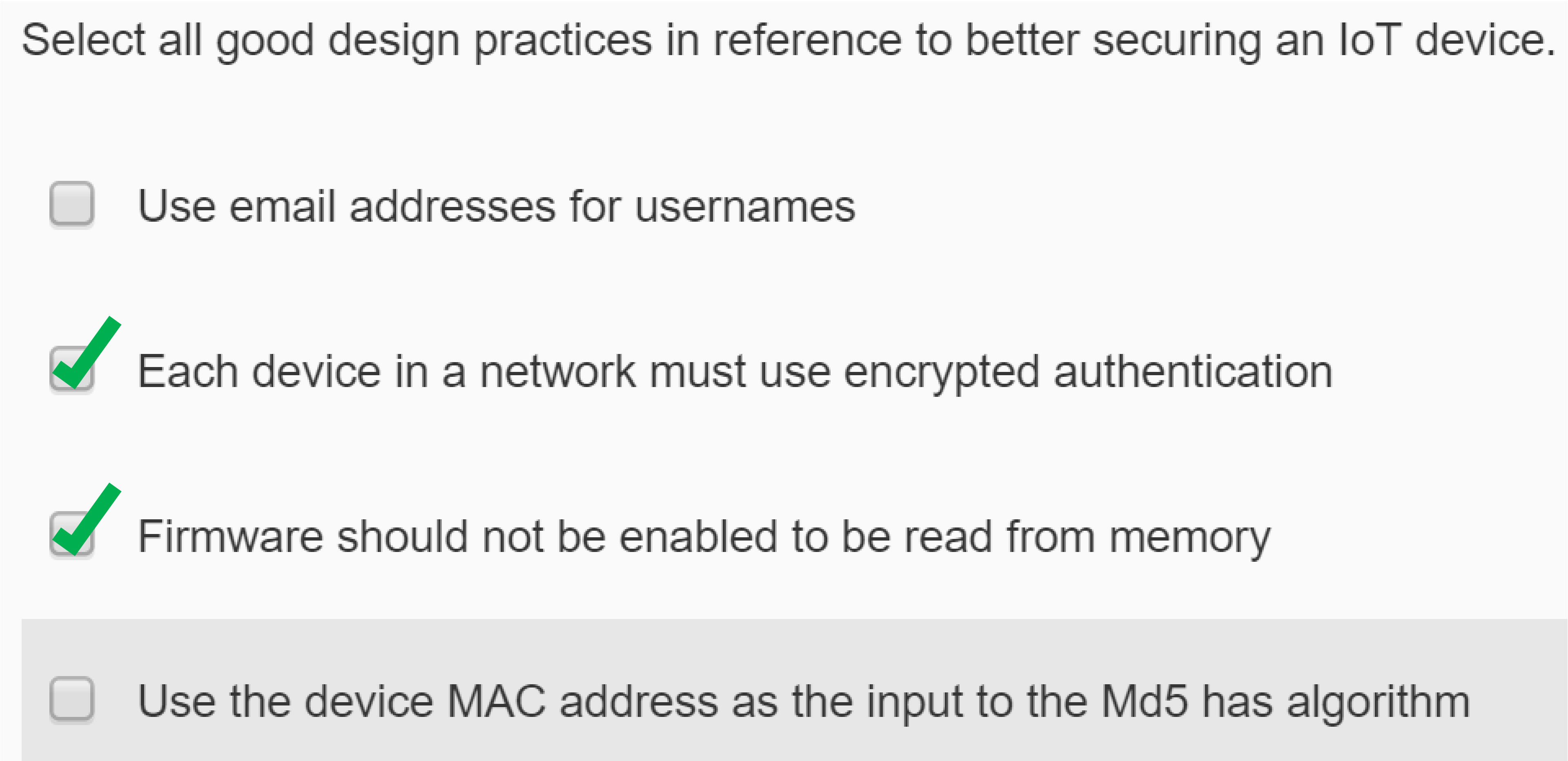
IoT devices and platform service providers based on good design practices must enable their devices and services to be (remotely) word answer) patched to withstand and prevent basic cyber attacks.

Quiz 9 review



A clearly (defined communication) (two word answer) process should be in place for researchers who want to report security issues.

Quiz 9 review



Select all good design practices in reference to better securing an IoT device.

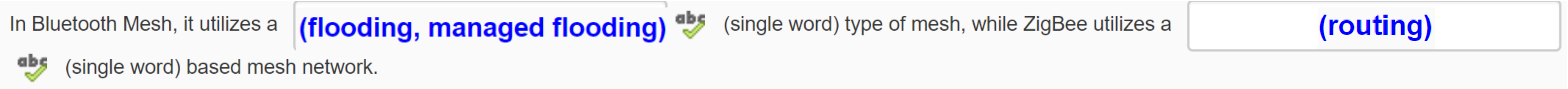
□ Use email addresses for usernames

☑ Each device in a network must use encrypted authentication

☑ Firmware should not be enabled to be read from memory

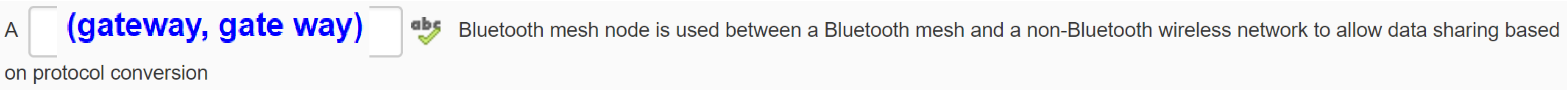
□ Use the device MAC address as the input to the Md5 has algorithm

Quiz 9 review



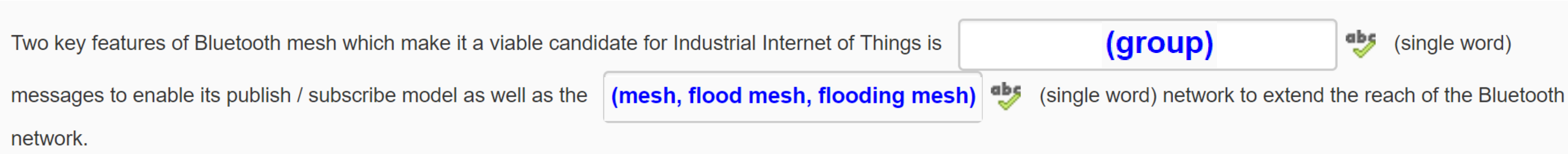
In Bluetooth Mesh, it utilizes a **(flooding, managed flooding)** (single word) type of mesh, while ZigBee utilizes a **(routing)** (single word) based mesh network.

Quiz 9 review



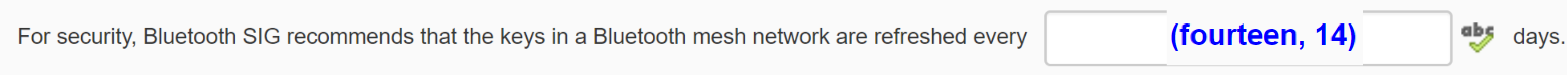
A (gateway, gate way) ✓ Bluetooth mesh node is used between a Bluetooth mesh and a non-Bluetooth wireless network to allow data sharing based on protocol conversion

Quiz 9 review



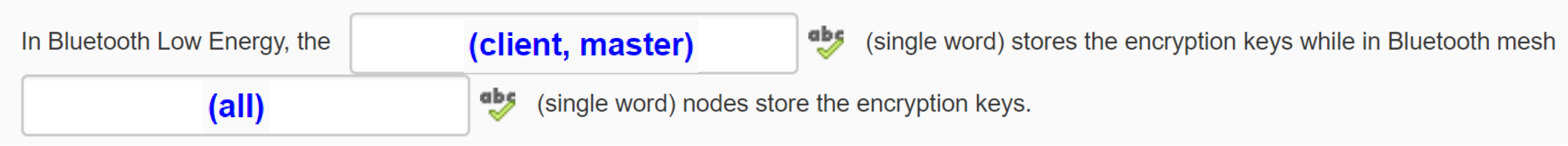
Two key features of Bluetooth mesh which make it a viable candidate for Industrial Internet of Things is **(group)** (single word) messages to enable its publish / subscribe model as well as the **(mesh, flood mesh, flooding mesh)** (single word) network to extend the reach of the Bluetooth network.

Quiz 9 review



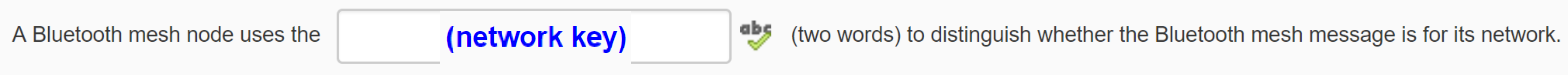
For security, Bluetooth SIG recommends that the keys in a Bluetooth mesh network are refreshed every (fourteen, 14) days.

Quiz 9 review



In Bluetooth Low Energy, the **(client, master)** (single word) stores the encryption keys while in Bluetooth mesh **(all)** (single word) nodes store the encryption keys.

Quiz 9 review



A Bluetooth mesh node uses the **(network key)** (two words) to distinguish whether the Bluetooth mesh message is for its network.

Differences between NOR and NAND Flash

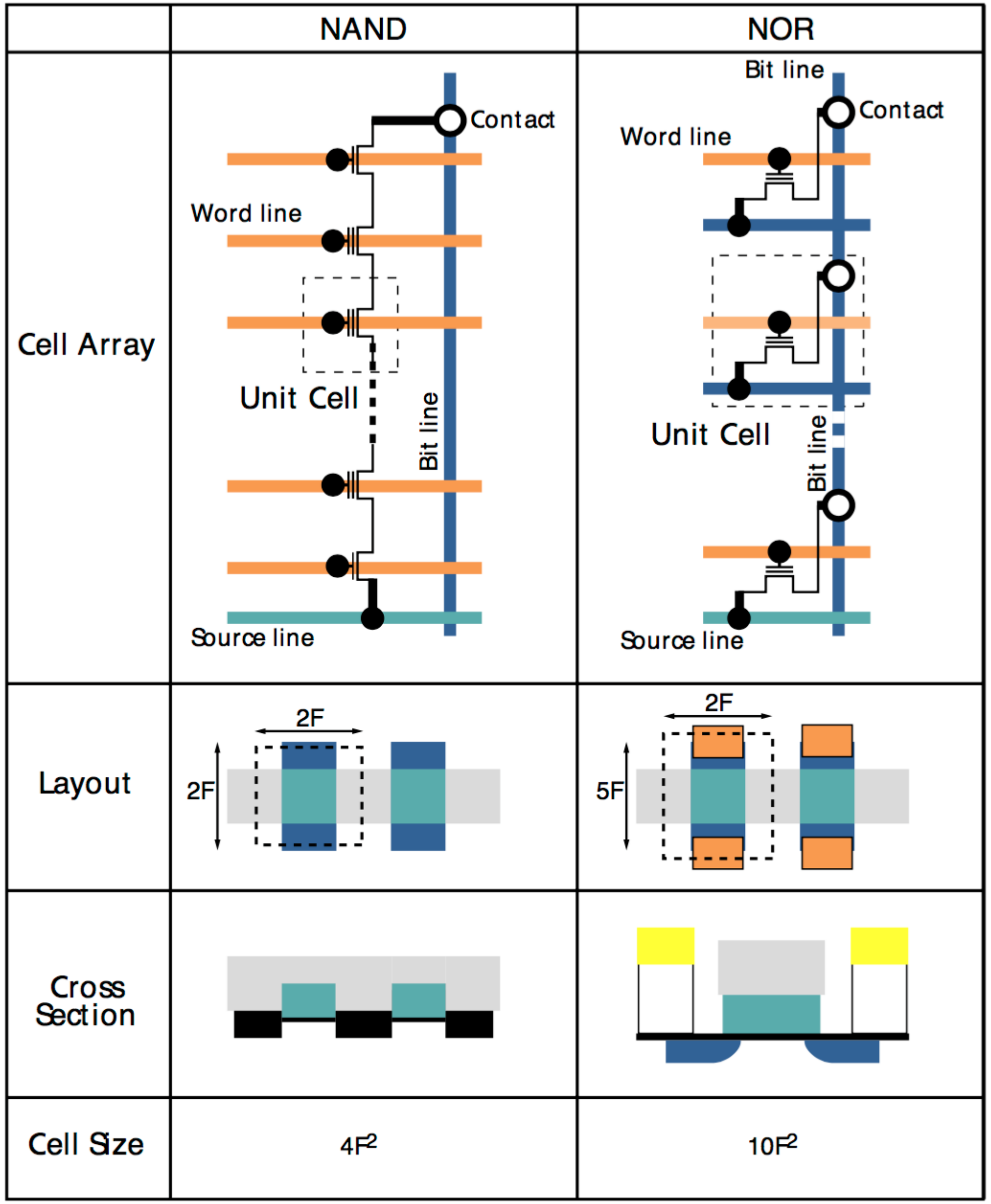
- NOR
  - Quick random access to any memory location
  - 100% known good bits for the life of the part
  - Good for direct code execution
  - Fast program and erase cycles
  - Density: 1Mbit – 2Gbit
  - Larger cell and more expensive

- 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

https://www.spansion.com/Support/Application%20Notes/FlashOverview_AN.pdf

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.



	NAND	NOR
Cell Array		
Layout		
Cross Section		
Cell Size	$4F^2$	$10F^2$

Contact
Word line
Unit Cell
Bit line
Source line
Bit line
Contact
Word line
Unit Cell
Bit line
Source line
2F
2F
2F
5F

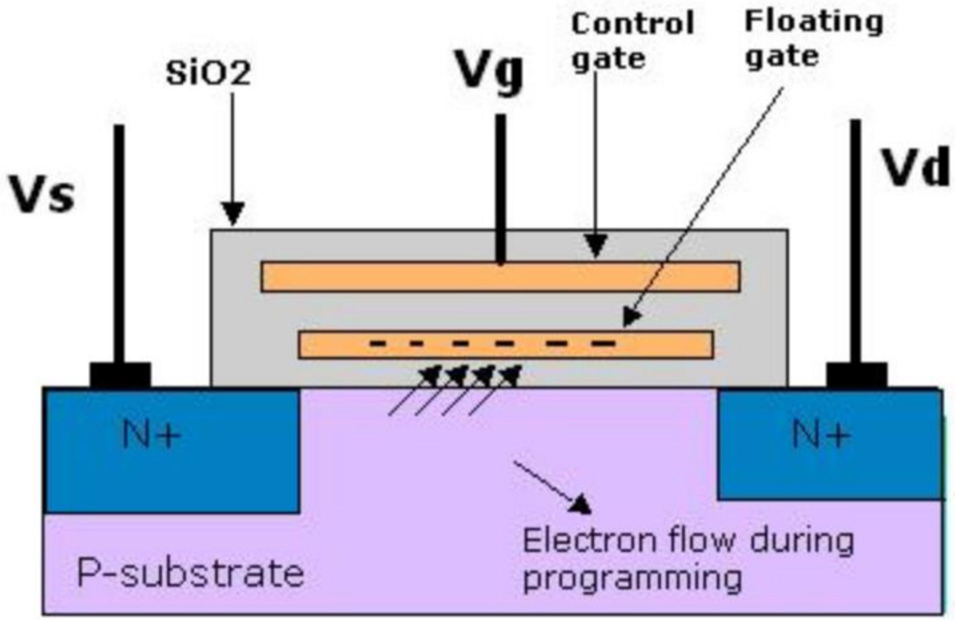
https://www.ece.umd.edu/~blj/CS-590.26/micron-tn2919.pdf

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)

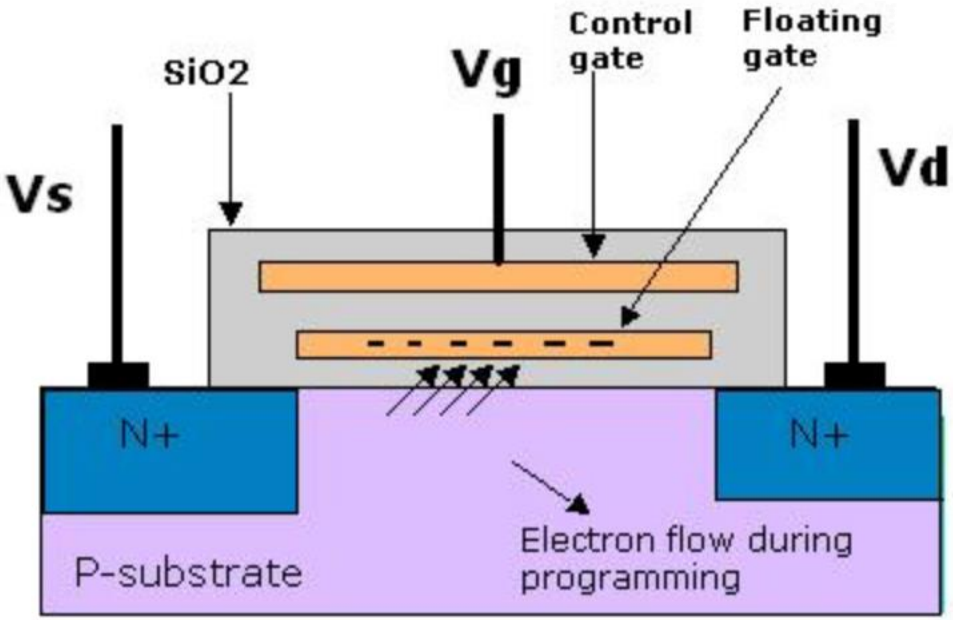
- Flash stores the data by removing or putting electrons on its floating gate (see fig 5). Charge on floating gate affects the threshold of the memory element. When electrons are present on the floating gate, no current flows through the transistor, indicating a logic-0. When electrons are removed from 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.



http://www.eeherald.com/section/design-guide/esmod16.html

Basic NOR Gate (Erase Operation)

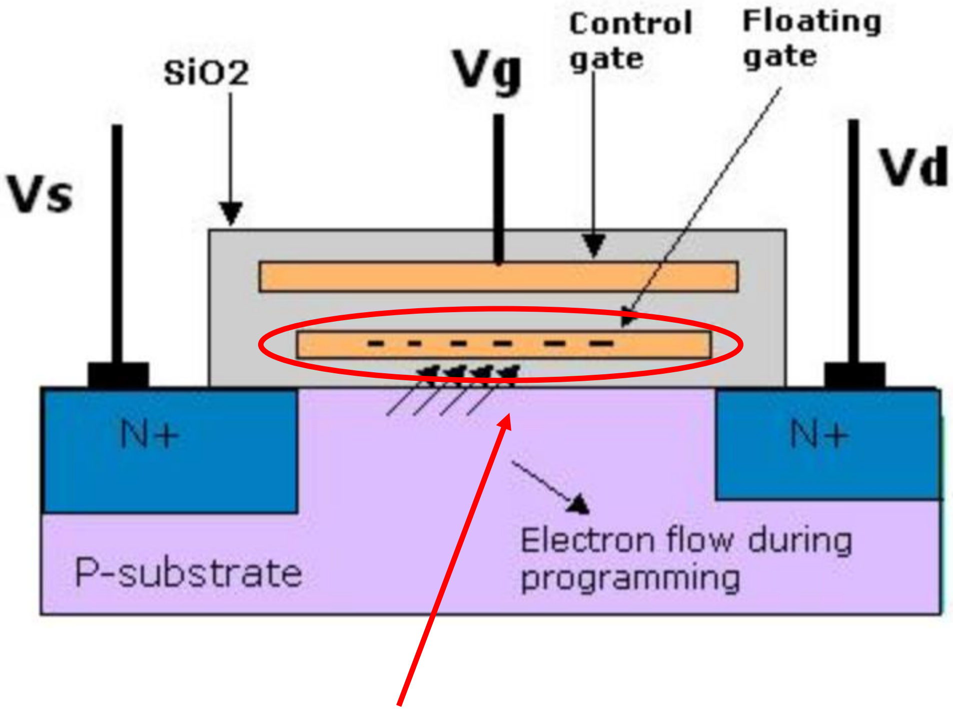
- The raw state of flash memory cells will be bit 1's, (at default state) because floating gates carry no negative charges. Erasing a flash-memory cell (resetting to a logical 1) is achieved by applying a voltage across the source and control gate (word line). The voltage can be in the range of -9V to -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.



http://www.eeherald.com/section/design-guide/esmod16.html

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.

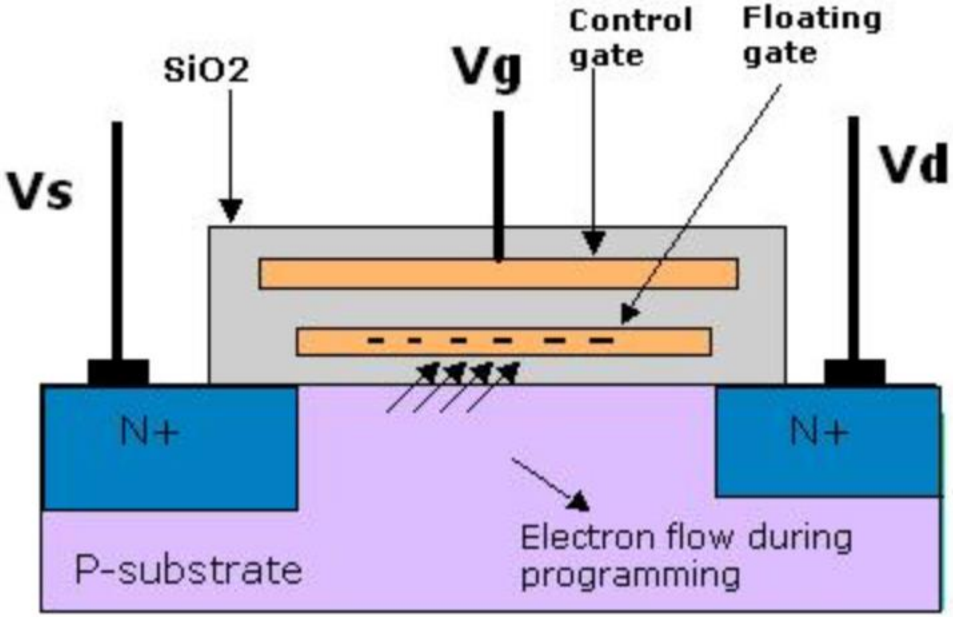


Keeping the float gate charged correctly for reliability

http://www.eeherald.com/section/design-guide/esmod16.html

Basic NOR Gate (Write Operation 2 of 3)

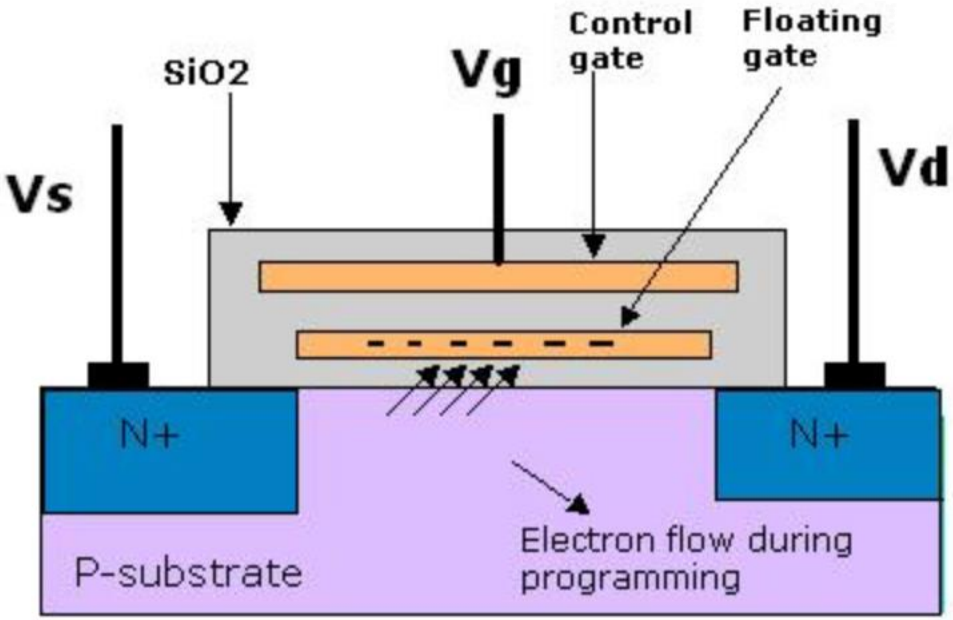
- Due to applied voltage at floating-gate the excited electrons are forced through and trapped on other side of the thin oxide layer, giving it a negative charge on the floating gate. These negatively charged electrons act as a barrier between the control gate and the floating gate.



http://www.eeherald.com/section/design-guide/esmod16.html

Basic NOR Gate (Write Operation 3 of 3)

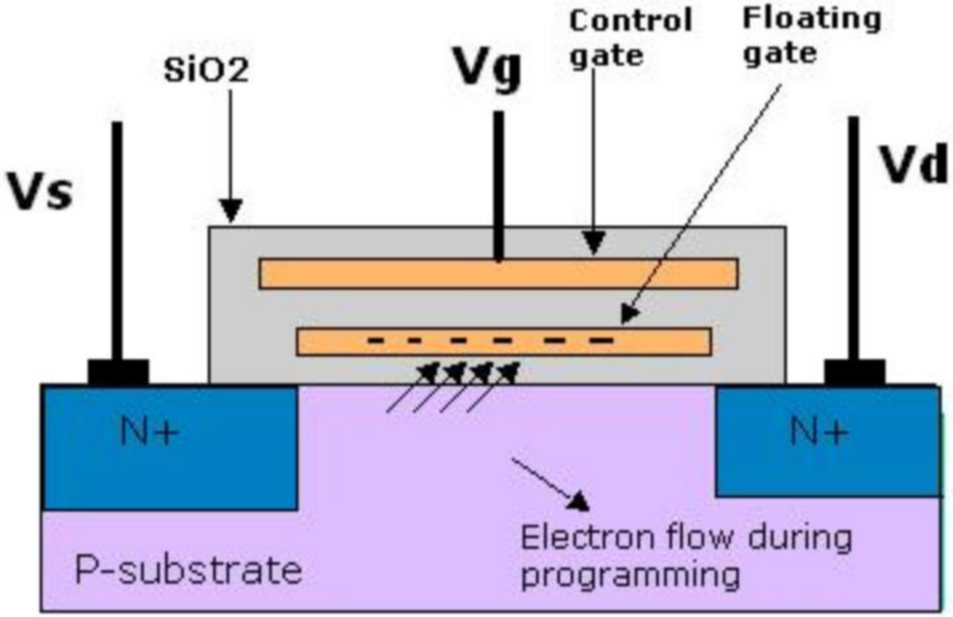
- If low voltage is applied to the drain via the bit line, the amount of electrons on the floating gate remains the same, and logic state doesn't change, storing the bit 1. Since floating gate is insulated by oxide, the charge accumulated on the floating gate will not leak out, even if the power is turned 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.



http://www.eeherald.com/section/design-guide/esmod16.html

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.



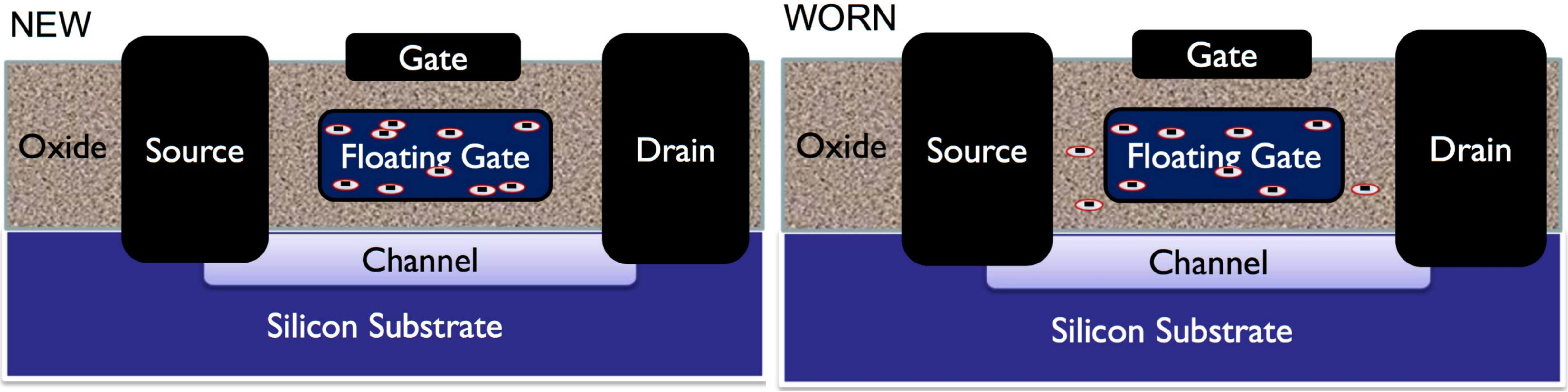
http://www.eeherald.com/section/design-guide/esmod16.html

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.

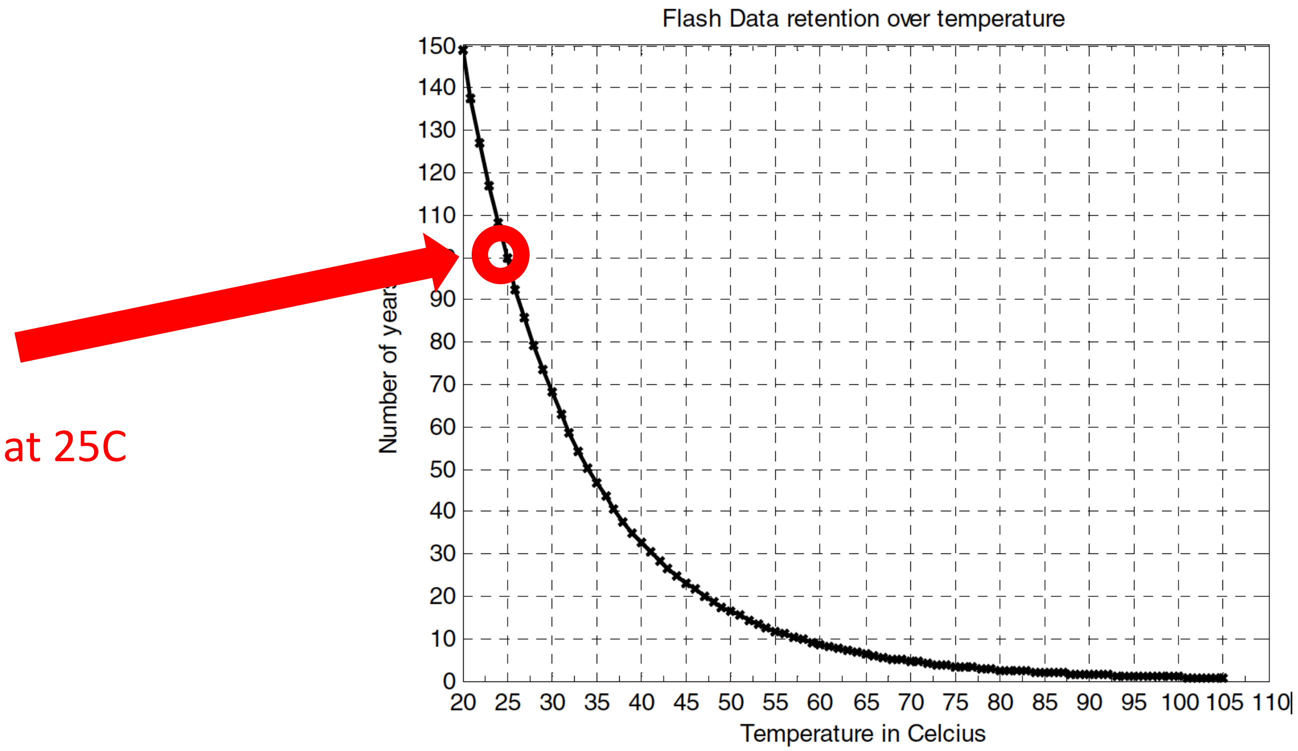
Micron TN-12-30: NOR Flash Cycling Endurance and Data Retention Introduction

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



http://www.snia.org/sites/default/education/tutorials/2009/spring/solid/JonathanThatcher_NandFlash_SolidState_Storage_ReliabilityV1-0-nc.pdf

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 with a positive charge, “1.” 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,

TI MSP430 flash reliability app note - slaa392