ECEN 5023-001, -001B, -740

Mobile Computing & IoT Security

Lecture #1

17 January 2017

Be Boulder.

University of Colorado Boulder

Introductions (continued)

- Keith Graham
  - Email address: Keith.A.Graham@Colorado.EDU
  - Office: ECEE122
  - Office hours: T/Th 5:30-6:20pm, by appointment, and via email
- TA
  - Shivasankar Gunasekaran
    - Shivasankar.Gunasekaran@Colorado.EDU
    - Office hours: TBD
  - Omkar Seelam
    - Omkar.Seelam@Colorado.EDU
    - Office hours: TBD

Agenda

- Class Announcements
- Course Goals and Expectations
- Project and Tool demo
- Mobile Computing Applications and Covered Topics
- Where is the money in IoT?
- IIoT versus IoT
- Reading list
- Quiz #1

Class Announcements

- The class currently has 2 students on the waiting list
- Quiz #1 is due at 11:59 on Sunday, January 22nd, 2017
- ESE lab, ECEE 287
  - Card access for ESE students and students taking ESE courses only
  - Must apply for card access via web form

ESE lab rules

- All students enrolled in an ESE course (except ECEN 5613) will be granted access to the ESE Lab (ECEE 287) with completion of the web form
- The policy will be strictly enforced. Students only need to submit the form once for ESE Lab access
- **NOTE:** Students enrolled in ECEN 5613 must use ECEE 1B28 for that course, and NOT the ESE Lab in 287

ESE lab rules

- The link below serves as both an agreement on lab policy and an access request form for the labs
- We will not be accepting student lab access requests through any other means. If students are enrolled in a course that uses a lab, their request will be automatically granted
- If they request non-course access through a faculty member, we will be emailing that faculty member for a response before granting access
  - https://goo.gl/forms/YaBXQHATHELA2FIk2
- Embedded students should not be using the 281/282 labs
  - These labs are for the undergraduate students

Rationale

- To meet the demands of the fast growing markets of mobile computing and Internet of Things, students graduating the ESE program will be able to make appropriate engineering decisions based on their product's ecosystem to design products that meet their solution's energy, product lifecycle, and communication requirements while taking into consideration the appropriate security requirements.
- Accenture estimates that the Industrial Internet of Things (IIoT) could contribute by 2030 $14.2 trillion US dollars in world output. For the US, it could contribute $6.1 to $7.1 trillion US dollars by 2030 which could result in the US GDP growing an additional 2.3% more than currently forecasted.
- The growth of IIoT solutions disrupt many markets as these markets transform from service economies to outcome economies. Per the World Economic Forum, an Outcome Economy is a marketplace where businesses compete on their ability to deliver quantifiable results that matter to customers rather than just selling a product or service. The outcome could be measured energy savings, increased product yields, or increased machine uptime.
- As the IIoT transforms business, it will also transform the labor market as many lower skilled jobs are replaced by intelligent systems that require higher skilled workers to maintain and make creative decisions.

Description and Content

- The course material will convey both technical and industry requirements to enable proper engineering architectural decisions as well as implementation. The course will explore through weekly and course projects low energy firmware design concepts, extending FLASH memory data retention reliability, Bluetooth, and developing a secure manufacturing process of micro controller firmware and encryption keys. The programming assignments will be “coding to the metal” to control individual micro controller peripherals and utilizing them in the most energy efficient ways.

Description and Content (continued)

- Topics covered:
  - Low Energy versus Low Power design
  - Wireless Computing tradeoffs: Available resources, application, infrastructure
  - Interrupt or event driven firmware
  - Wireless standards: applications and tradeoffs
  - Bluetooth: protocols and profiles
  - Designing for product lifecycle of 20+ years
  - Embedded system security, “hacking,” attack surfaces
  - Designing embedded systems with security in mind
  - Course project will incorporate Bluetooth communications, low power sensors, and low energy design concepts

Class Objective

- Event based firmware and Advanced Peripheral design concepts to enable low energy designs
- Balancing system design between backend and embedded processing
- Memory technologies and their applications in a battery powered device
- Flash memory limitations and how to extend Flash memory for higher reliability
- Bluetooth / BLE / Bluetooth Smart, ZigBee / Thread, and WiFi and their end applications
- Bluetooth Smart client and peripheral device architecture, requirements, and application
- System engineering, software-hardware integration, testing and troubleshooting
- Energy Harvesting
- NFC applications
- Hacking Attack Surfaces: debug ports, wireless communications, open key exchange, tampering, manufacturing
- Security topics: Tamper proofing, cryptography, key exchange, TPM, and secure manufacturing

Expected Outcome

You will be able to …

- Make engineering tradeoffs to determine where the processing power of a solution should reside; front or backend.
- Develop event based “code to the metal” firmware enabling low energy solutions.
- Determine the wireless protocol that best address their application and ecosystem.
- Develop Bluetooth solutions that are optimized for energy and the application.
- Design for flash longevity in embedded solutions for consumer and industrial applications.
- Know the security weak points or attack surfaces of an embedded product.
- Design security into an embedded solution.

Class structure

- On average, each week the lectures will be covering both theory and concepts as well as implementing low energy design principles in hardware/firmware
- Tuesday will be focusing on theory and concepts while on Thursday the lecture will be split between theory and concepts with low energy design practices
- Most weeks, these low energy design principles will then have a weekly homework programming assignment
- These assignments will not require the purchase of lab equipment or the use of a lab, but will require access to a computer running Windows, Mac OS, or Linux OS

Class structure (continued)

- Quizzes
  - Will be published, put on D2L, by the end of Sunday and will be due by the end of the following Sunday
  - Two attempts will be available for each quiz with best grade used for scoring and there will be one hour to complete each attempt
  - One quiz will be dropped from the total
- Homework assignments
  - Will generally be assigned at Thursday's lecture and will be due the end of day the next Wednesday
  - No assignments will be dropped

Class structure (continued)

- Prerequisites
  - Knowledge of assembly and C programming, digital logic design, and embedded computer architecture
  - Students should have had at least one course in each of these subjects
  - ECEN 5013, Embedded Software Essentials, is a recommended prerequisite
  - Students should also have experience using a microcontroller Integrated Development Environment (IDE) and its associated tools including its debugger and register views
- Expectations
  - Lectures, Programming Assignments/Course Project, Readings, and Quizzes will require on average 10-14 hours per week of work
  - For on campus students, class attendance is expected. For distant learners, live video streaming and videos will be made available

Development boards provided for ECEN5023

- Silicon Labs' Leopard Gecko STK3600 starter kit. The description can be found at https://www.silabs.com/products/mcu/32-bit/Pages/efm32lg-stk3600.aspx

- Atmel's Low Power Cortex-M0 Bluetooth Smart development kit, SAMB11 Xplained Pro Evaluation Kit. The description can be found at http://www.atmel.com/devices/ATSAMB11.aspx?tab=tools

Note: These development boards will be provided to the students at no charge, but the boards will be required to be returned upon completion of the course project demo

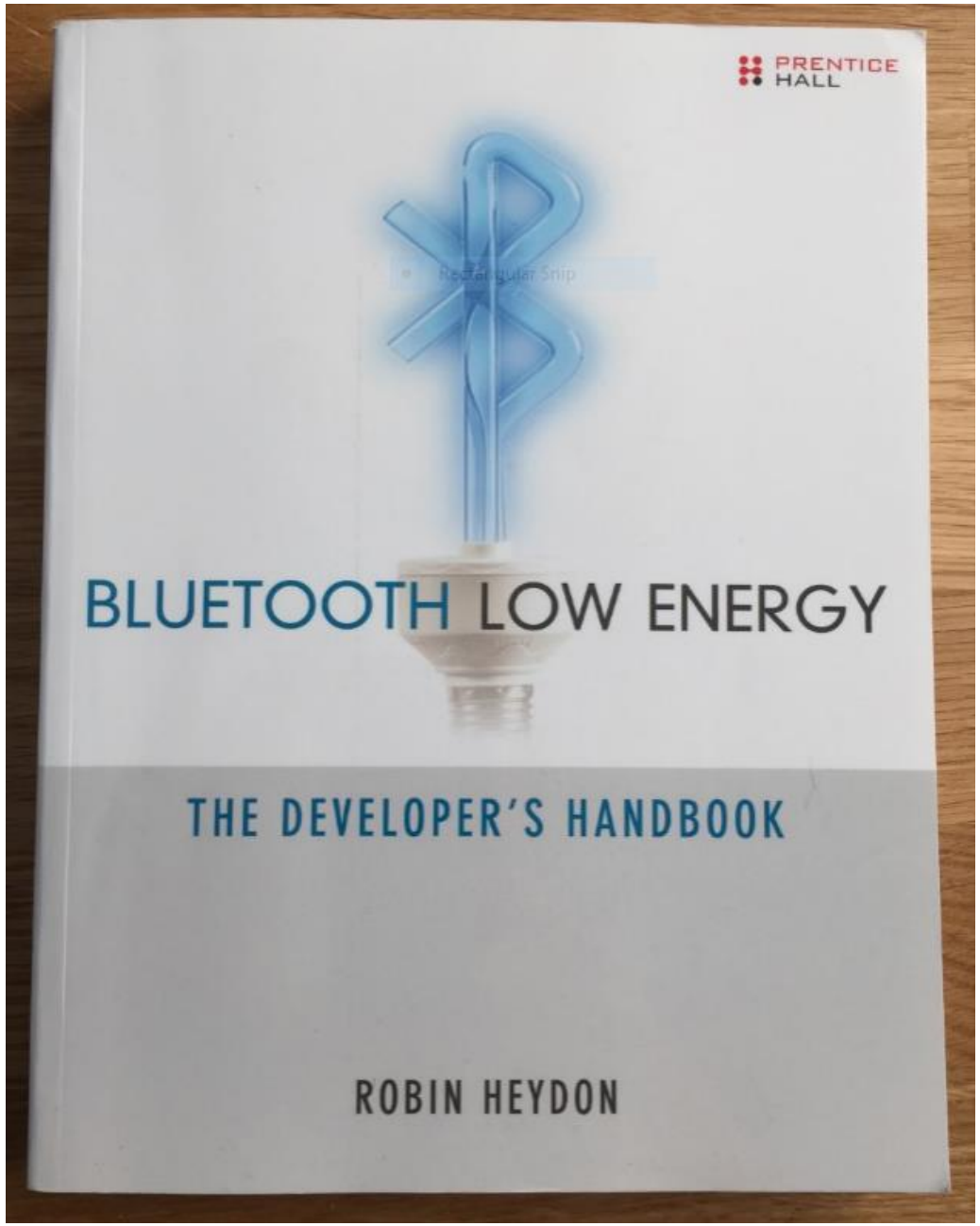
Homework programming assignments

- The homework programming assignments will be designed to build upon previous assignments
- By the start of the course project, the students will already have experienced with event driven firmware as well as low energy firmware concepts
- Homework assignments (subject to change):
  - Exercise: Introduction to the Simplicity development environment.
  - #1: Interrupt based programming using LETIMER including developing a sleep() routine and comparing energy profiles across different energy modes.
  - #2: Develop a routine to self calibrate the ULFRCO oscillator.

Homework programming assignments

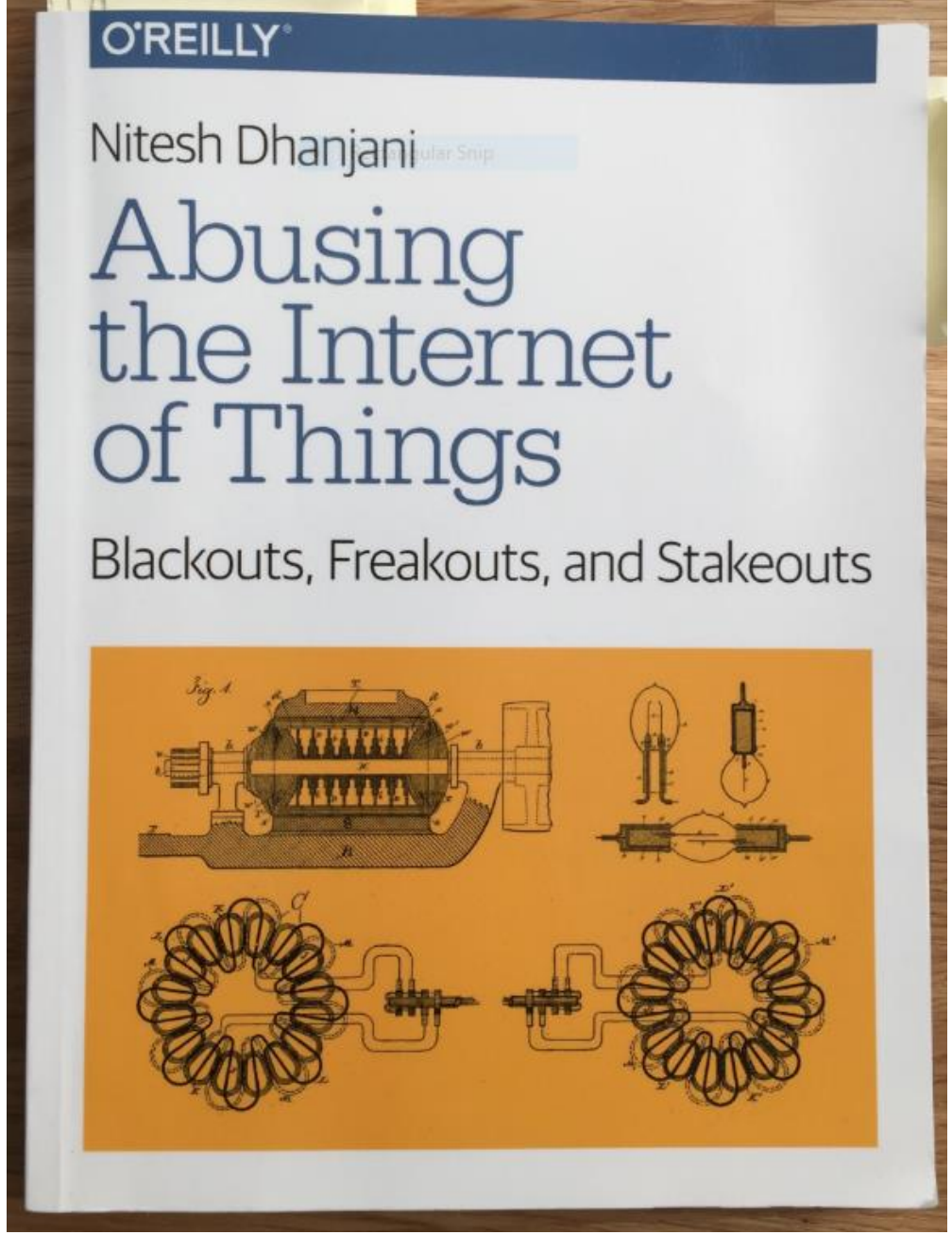
- Homework assignments (continued):
  - #3: Program the Analog to Digital Converter, ADC, to take temperature measurements and send an alert if out of set temperature limits and explore utilizing DMA to enable energy savings
  - #4: Add an external I2C peripheral to the Leopard Gecko STK
  - #5: Using Leopard Gecko's LEUART to send the temperature via the ATSAMB11 to a mobile device
  - #6: Using a mobile device to communicate via the ATSAMB11 to set the temperature trip point on the Leopard Gecko

Required book for Bluetooth portion of course



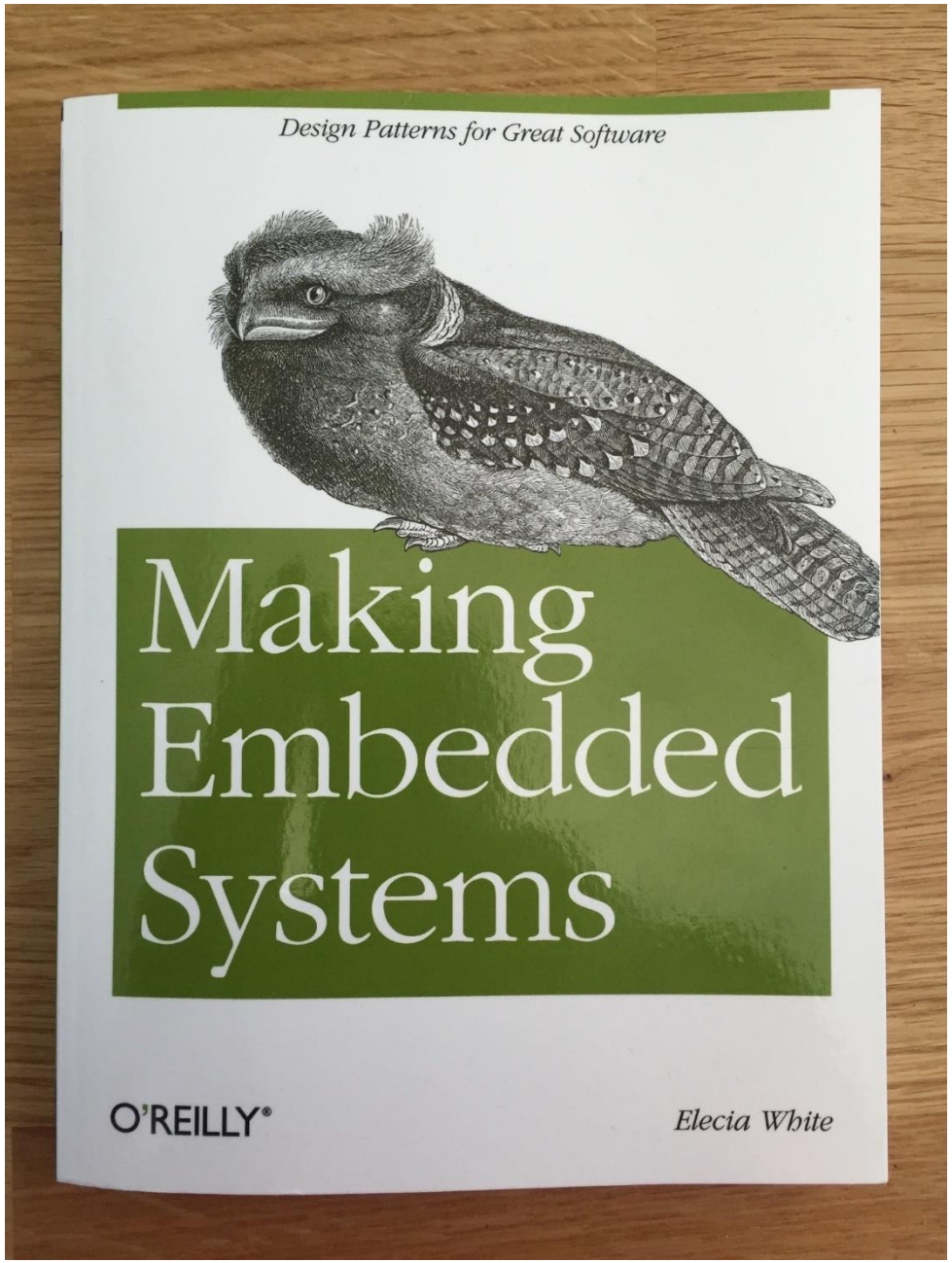
"Bluetooth Low Energy, The Developer's Handbook," by Robin Heydon
ISBN: 9780132888363

Required book for Internet Things of Security portion of course



"Abusing the Internet of Things: Blackouts, Freakouts, and Stateouts," by Nitesh Dhanjani ISBN: 9781491902332

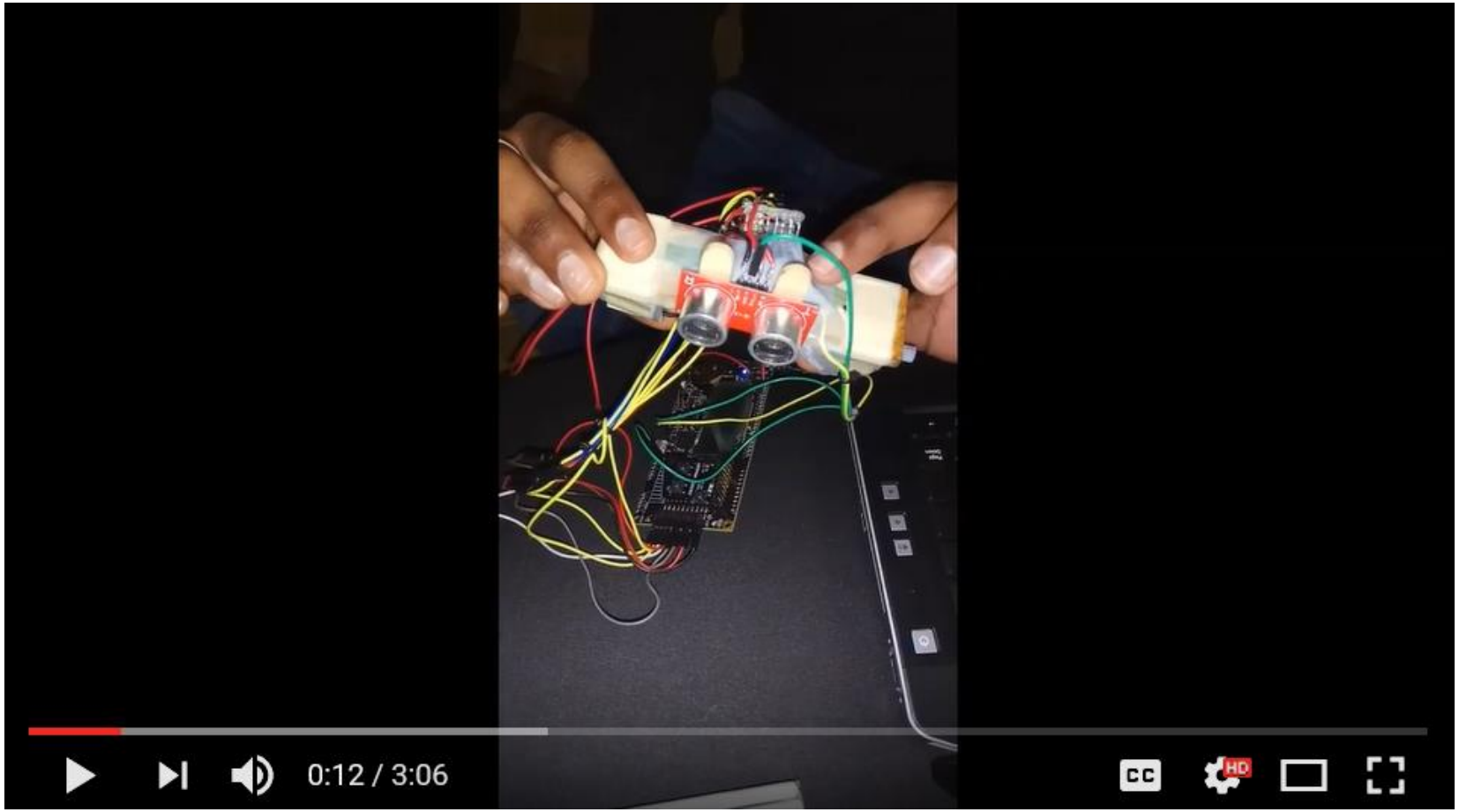
Recommend book for this course for students who would like an embedded C reference book



Course Project

- There will be one course project that will combine the low energy design principles and Bluetooth radio taught throughout the course utilizing the Atmel ATSAMB11 Xplained Pro Evaluation Kit an the Silicon Labs Leopard Gecko STK3600. The course project will include developing a product proposal that will include a Bluetooth Smart device in a cohesive application such as home security, retail, etc.. This project will include developing code as a Bluetooth Smart device providing the associated services for external sensors. The project/product will need to support Bluetooth notifications, indications, as well as attribute writes/reads, and attribute commands.

Example project from Fall 2016



Evaluation and Grading Procedures

- The course grade will be based on in-class participation, homework assignments, quizzes, course project, and 2 exams. The grade proportions are as follows:
  - Homework and Class Participation 20%
  - Course projects 30%
  - Quizzes 10%
  - Final and Mid-term Exam 40%
- Grading will be based on total points accumulated from each of these areas. Assignment of grades will be based on an absolute scale of:

A : 92.50+%
A-: 90.00 – 92.49%
B+: 87.50 – 89.99%
B : 82.50 – 87.49%
B-: 80.00 – 82.49%
C+: 77.50 – 79.99%
C : 72.50 – 77.49%
C-: 70.00 – 72.49%
D+: 67.50 – 69.99%
D : 65.00 – 67.49%
Fail: < 65.00%

Evaluation and Grading Procedures

- Upon the professor's discretion, assignment of grades can be based on both absolute and relative standards if it would be helpful to the overall class. To receive an A grade in this assignment of grades option, a student must show mastery of the material and need to acquire more than 90% of the points possible. A student earning less than 50% of the points possible will be given a failing grade. In between these marks, grades will be assigned on a curve using a mean and standard deviation method.
- **Make-up Exam Policy:** No make-up exams are given except for medical or other similar hardships where advanced arrangements are made with the instructor; or in case of non-selective medical emergencies with physician's note or documentation. Otherwise, failure to take the exam at the scheduled time will result in a zero grade in the exam.

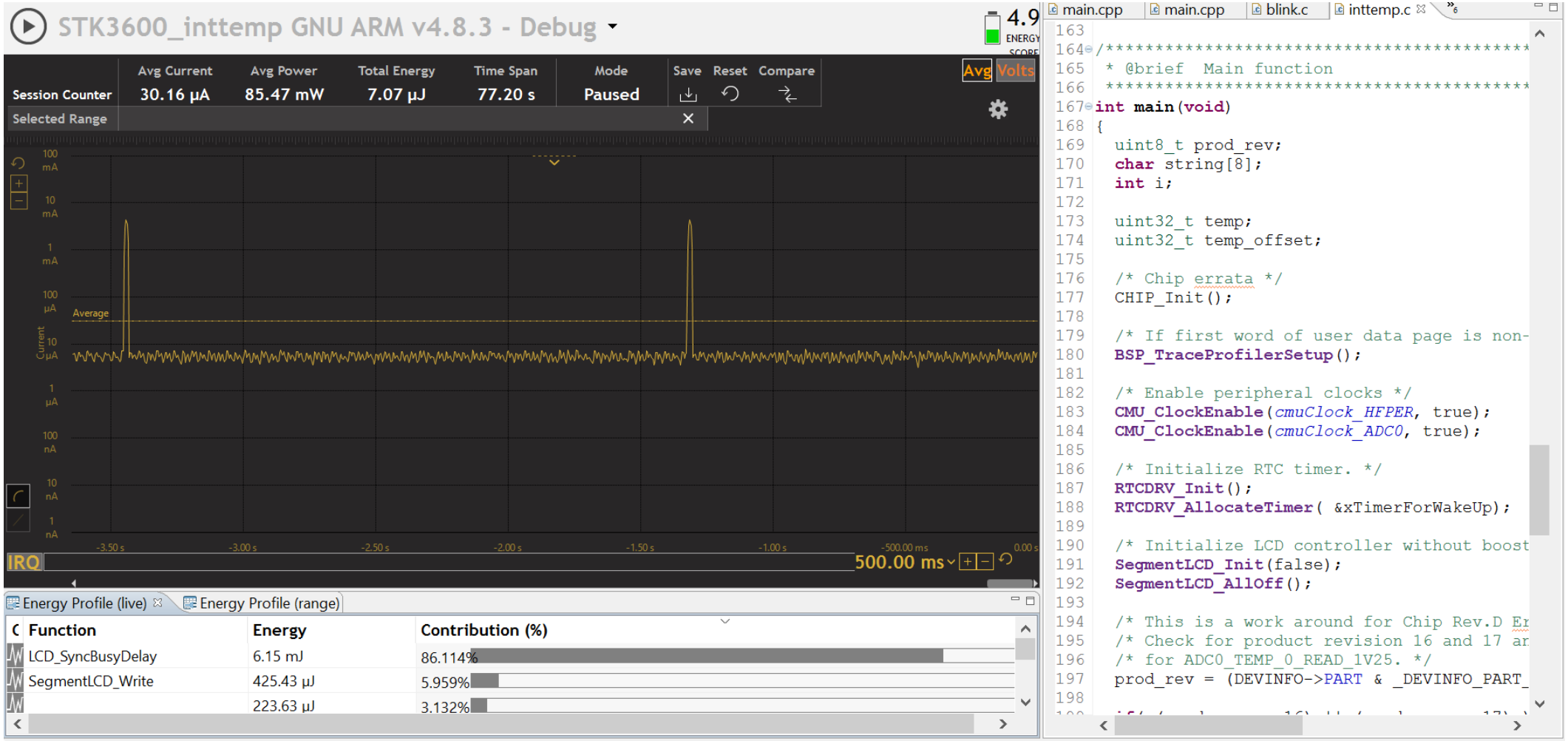
D2L

- Syllabus and other course material will be inside the “Course file” folder
- Lectures, Homework and Reading assignments will be located in their weekly folder
- Quizzes will be administered through the D2L course site
- Homework assignments will be delivered via “drop box” on D2L

Slack

- A Mobile Computing and Internet of Things Security Slack team will be set up for this course
- The Slack channels/forums will be a valuable place to look for answers, ask questions, and to help others. As you work through problems, you may find documentation errors or lack of documentation that may have already been solved in the forum. The forum will be proctored by the instructor and course TAs. As in all engineering projects, collaboration and sharing knowledge of issues and solutions is very productive.
  - Please feel free to create new threads and help out others!
- In the coming week, everyone in the class will be invited to the course Slack team

Energy Profiler demo



What is mobile computing for ECEN 5023-001?

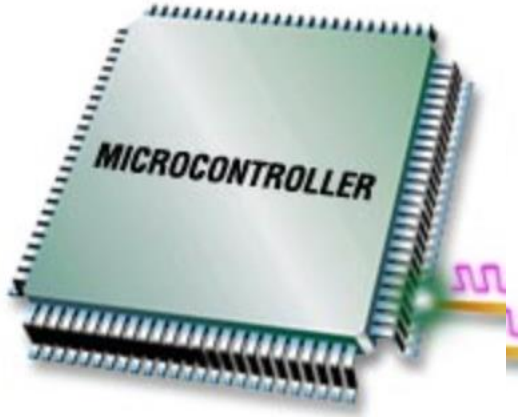
- Wikipedia **Definition**. • **Mobile computing** as a generic term describing ability to use the technology to wirelessly connect to and use centrally located information and/or application software through the application of small, portable, and wireless **computing** and communication devices.

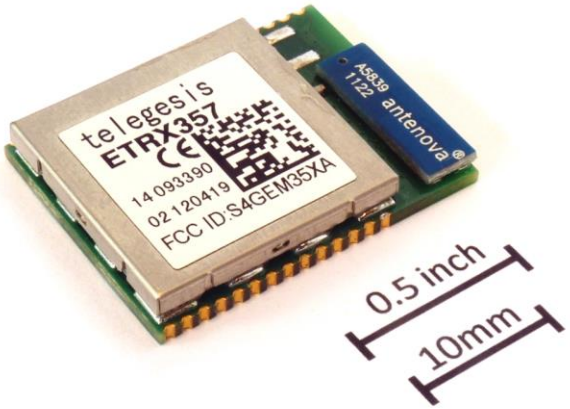
Mobile computing for ECEN 5023-001

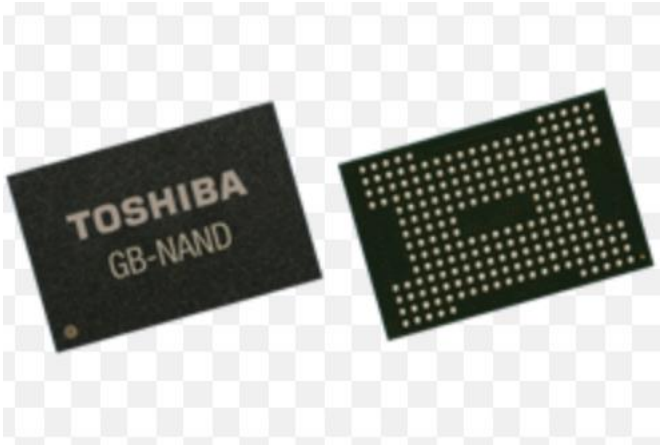
What are key factors in designing for mobile computing?

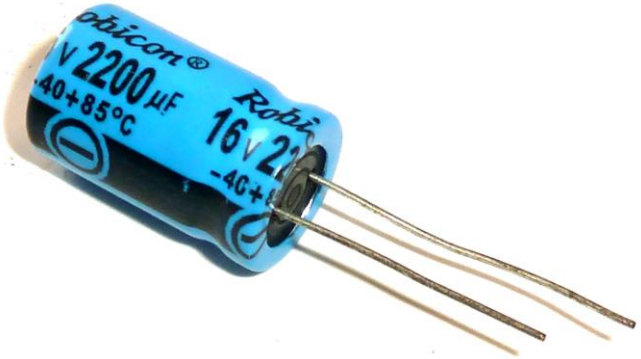
- Battery Life
  - Everyone would like their smart phone or watch to last longer.
- Communications (Radios)
  - Different standards for different industries
- Operating Temperature
  - Benign or harsh
- Physical Durability
  - Survive the accidental drop
- Warranty
  - Needs to match the market segment sold into
- Security
  - As these devices are becoming more prevalent, security needs are growing

What components will this class focus on?







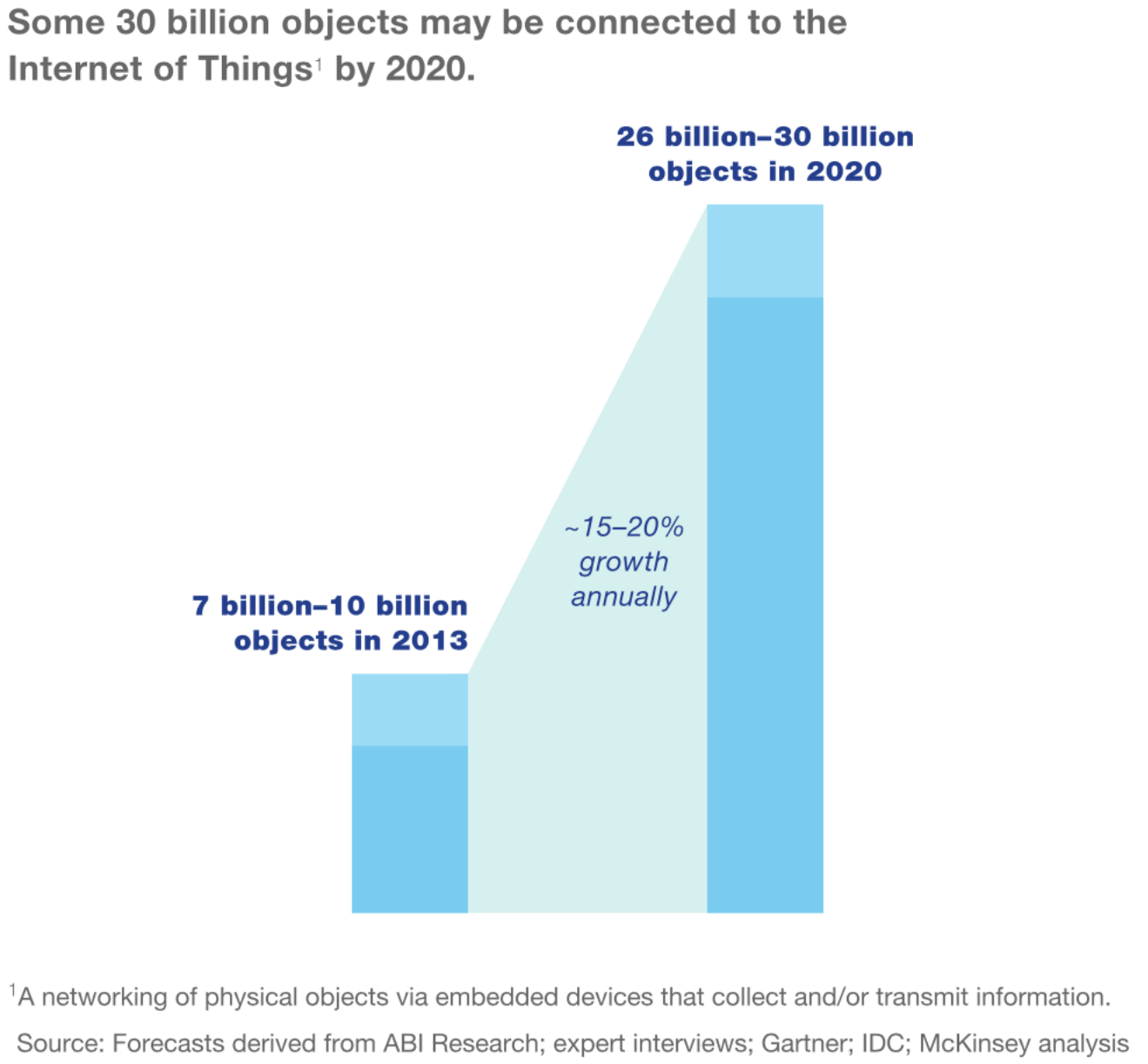


What is an IoT device?

- The **Internet of Things** (**IoT**) is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.[1] The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure,[2] creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit.[3][4][5][6][7][8] Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020.[9]

Growth will generate new problems and create new opportunities

- What will be some of the issues as the number of connected devices grows to 30+ billion and beyond?
  - Capacity?
    - Bandwidth
    - IOPs
  - Security



Where is the money in (consumer) IoT?

- Selling the device?
  - Fitbit, Garmin Running watches, Bluetooth door locks, ….
  - A recent InfoWorld article proclaims "The Internet of Things is not paying the rent." In it, Adobe's VP of Mobile Matt Asay cites data from Vision Mobile and McKinsey & Co. to point out that "less than 10 percent of IoT developers are making enough to support a reasonably sized team," and that "developers need to get real about what they're selling and to whom," which "probably involves a 'dull' enterprise-facing business." This begs the question, how do you make money in the IoT?

Where is the money in (consumer) IoT?

- IoT-as-a-Service?
  - Home/Security Automation, Smart Sprinkler Systems, ….
  - Internet of Things companies could potentially transition away from one-off IoT platform sales and into business models that allow for accretive growth by means of data and feature monetization. In this cloud-based approach, companies could establish service plans or provide additional features to end users similar to how your cell phone or cable company operate, generating recurring streams of income that continue to flow after the initial platform sale (or perhaps, giveaway) to help offset ongoing maintenance, service, and support costs.

Industrial Internet of Things (IIoT)

- The Industrial Internet of Things will combine the reach of the Internet with a new ability to directly control the physical world, including machines, factories, and infrastructure.
- Growth of “digital labour” in the form of smart sensors, intelligent assistants, and robots will transform not just the ability to manage and operate their assets, but also transform the skills and mix of the workforce.
- New jobs will be created in the form of IIoT device and robot designers, internet optimization, and software engineering to create the ecosystem or fabric for these IIoT devices to operate.

Outcome Economy

- Manufacturing economy: A marketplace based on producing and selling products
- Service economy: A marketplace based on providing services rather than manufacturing or producing goods. (Cambridge dictionary)
- Outcome economy: A marketplace where businesses compete on their ability to deliver quantifiable results that matter to customers rather than just selling products or services, e.g. energy saved, crop yield or machine uptime. Delivering customer outcomes requires sellers to take on greater risks. Managing such risks requires automated quantification capabilities made possible by the Industrial Internet. (World Economic Forum)

To achieve the Outcome Economy

- Companies will need to focus on the “why” behind the buy
  - Connected sensors are moving the physical world online making it quantifiable and accessible
  - Applying advanced analytics to this data with the correct external data and domain models will give companies a better understanding of interaction and how to optimize to achieve the desired business outcome
- Reliability will be a key component in the Outcome Economy
  - Industrial products are designed for years or decades. IIoT devices will need to have obsolesces that match these industrial products and can be added to existing machinery without compromising its integrity or reliability
- Real-Time responses are often critical in manufacturing, energy, transportation and healthcare.
  - Today’s internet “real-time” is a few seconds, but real-time in industrial equipment usually means sub-millisecond

Real-Time

- How will Real-Time responses in sub-milliseconds for industrial application over today's internet "real-time" of several seconds drive architecture decisions of an IIoT device?
  - Drive processing power and decision making to the device
  - And/or
  - Localized IIoT routers or access points

Reliability

- How will reliability drive architecture decisions of an IIoT device?
  - If practical, drive the processing power up into the backend/cloud
  - Smaller and simpler design = higher reliability
  - Minimize low reliability components such as mechanical, FLASH memory, electrolytic capacitors
  - Increase costs by utilizing higher quality components

Industry Internet of Things – Reliability example!

- Stupid phone tricks
  - https://www.youtube.com/watch?v=w4H0BR_8wy8

The battle between Real-Time versus Reliability?

- In making the architecture tradeoffs, which requirement wins the battle, Real-Time versus Reliability?
  - Real-Time? The asset needs to be protected
    - Example: Imagine a driverless car not able to make the decision in real-time to prevent an accident
  - Reliability? The asset needs to be protected throughout the asset lifecycle
    - Example: Imagine a driverless car whose sensor stopped working which resulted in an accident
  - Real-Time and Reliability both need to win!
    - Real-Time by architecture
    - Reliability by design

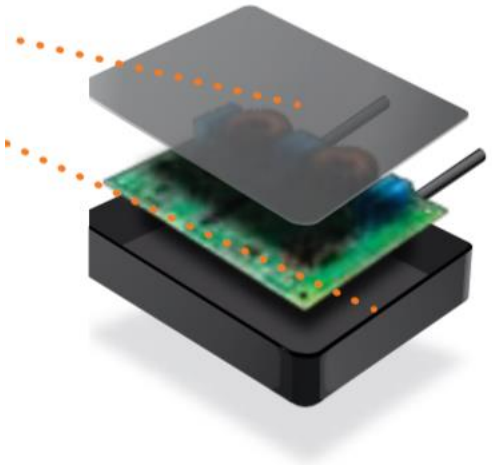
IoT / IIoT critical differences

Consumer IoT

- Benign ambient temperatures
  - 20C to 40C
- Lifecycles < 5 years
- Priority => Cost
- Wireless connectivity
  - Bluetooth, WiFi, Zwave, ZigBee

Industrial IoT

- Extreme temperatures both low and high
  - -25C to +85C
- Life cycles > 25 years
- Priority => High reliability
  - Mission critical
- Wireless connectivity
  - WiFi, ISM, Licensed



Features:

- High efficiency power conversion
- Fast and accurate MPPT per PV module
- Ampt Mode™ technology to increase inverter output power
- String Stretch™ technology to build longer strings
- Output voltage and current limits
- Instrument-grade precision measurement
- Optional two-way wireless communication
- Independent power optimization without reliance on communication
- Inverter and PV module compatible
- Compatible with 3rd party monitoring
- Utility-strength operation and stability
- High reliability
- 25 year warranty

Ampt-x Converter Model	V40-x	V50-x	V100-x
Electrical*			
Input			
Maximum module power (Pmax) at STC	260 W	320 W	360 W
Maximum module voltage (Voc) at coldest design temperature	46 V	58 V	102 V
Module MPP DC voltage range	10 - 38 V	17 - 48 V	25 - 80 V
Maximum module current (Imp) at STC	8.5 A	9.2 A	6.1 A**
Maximum module short circuit current (Isc) at STC	9.2 A	9.2 A	6.7 A
Output			
Maximum converter output voltage	33.3 V	40.6 V	63.6 V
Maximum converter output current	9.4 A	9.2 A	6.7 A**
Maximum converter output power	260 W	320 W	360 W
Maximum operating efficiency	99.0%	99.2%	99.2%
Mechanical			
Ambient temperature operating range	-40°F to +158°F (-40°C to +70°C)		
Dimensions	5.9 x 4.7 x 1.4 in. (15 x 11.9 x 3.6 cm)		
Weight	12 oz. (0.3 kg)		
Cooling	Convection		
General			
Communication	Two-way wireless (optional)		
Compliance	CSA to UL 1741, FCC Part 15 Class B IEC 62109, 61000-6-1, 61000-6-3		
Demonstrated MTBF at 40°C continuous	90 million hours		
Warranty	25 years		

* Standard test condition (STC) irradiation level of 1000 W/m² at 25°C.
** 6.1 A input and 6.7 A output at 60°C. 5.45 A input and 5.55 A output at 70°C.

> 85C with temperature rise inside of box

Xeta2-E

9.6 kbps - 3.5 Mbps Ethernet Radio
Broad/Narrowband 216 MHz-232 MHz

Security

- AES 128/ 256-bit encryption
- Password authentication
- VLAN network segregation

Transmitter	
Frequency Range	216 – 232 MHz
Output Power	10mW to 8W, step size 10mW
Range – Line of Sight	70+ miles
Modulation	BPSK, QPSK, 8-PSK, 16 QAM, 2-4 Level GFSK, 32-QAM
RF Data Rate	9.6 kbps to 3.5 Mbps

Environmental

- -40°C to +85°C operating temperature range. *-55°C available.*
- 95% operating humidity @ 40°C non-condensing.

Insert http://www.xetawave.com/documents/Xeta2-EDataSheet.pdf Here

TRANSPARENT TECHNOLOGIES
BEYOND AMR

Register features:

- Compact, fully encapsulated package for all meter environments.
- Large 8-digit LCD display showing totalization, measuring units and direction of flow.
- Zero-drag magnetic sensor for meter magnet tracking.
- Embedded high-resolution datalogging down to magnet-by-magnet turns.
- Flowrate and meter test functions.
- 20-year warranted battery life (10-yr full/10-yr prorated).

Specifications:

Temperature:	-40F° to 185F° (-40C° to +85C°)
Humidity:	100%
Submersion:	IP68 Fully Submersible
Battery:	19.0Ah D-Cell

http://www.metronfarnier.com/wp-content/themes/metron_theme/PDF%20Downloads/Innov8%20Registers/Innov8%20Datasheet.pdf

T701i WIFI Thermostat

T701i Specifications

Specifications

T701i Thermostat	
The display range of temperature	41°F to 95°F (5°C to 35°C)
The control range of temperature	44°F to 90°F (7°C to 32°C)
Load rating	1 amp per terminal, 1.5 amp maximum all terminals combined
Display accuracy	± 1 °F
Swing (cycle rate or differential)	Heating is adjustable from 0.2°F to 2.0°F Cooling is adjustable from 0.2°F to 2.0°F
Power source	18 to 30 VAC, NEC Class II, 50/60 Hz for hardwire (common wire) Battery power from 2 AA Alkaline Energizer batteries
Operating ambient	32° to +105° (O° to + 41°C)

Kwikset Kevo Bluetooth Door Lock

What is Kevo's warranty?

Your Kwikset Kevo products are backed by one of the most comprehensive warranty programs available. You can feel confident that with the purchase of Kwikset you have selected the best quality product, backed by the best customer service available. Your Kwikset Kevo deadbolt product comes with a lifetime mechanical and finish warranty along with a 1 year electronic warranty to the original residential user of the product against defects in material and workmanship as long as the original user occupies the residential premises upon which the product was originally installed.

Security and Data Privacy

- Digital models of the physical world including the collection of new customer usage and product data creates security concerns:
  - The use of “big data” in the backend must be managed in a secure fashion as well as individual’s data
  - In the distributed world of IoT/IIoT, the connections between the device and the backend need to be secured
  - The IoT/IIoT hardware and software must be secured or at a minimum detect intrusion and be able to be isolated from the network
  - If the IoT/IIoT is controlling an asset, the asset hardware and software must be secured

IoT security breach

- **Building Infrastructure:** The Department of Homeland Security recently disclosed a 2012 breach in which cybercriminals managed to penetrate the thermostats of a state government facility and a manufacturing plant in New Jersey. The hackers exploited vulnerabilities in industrial heating systems, which were connected to the Internet and then changed the temperature inside the buildings. *(On the surface, that might seem harmless, but think about the damage that cybercriminals could do with unfettered access to the controls that govern most major buildings today. The smart building might not seem so smart if for example, the bad guys activate the water sprinkler systems in a data centre or mess with the elevators.)*

IoT security breach

- **The Kitchen:** This breach that recently occurred in the UK boggles the mind. Hackers attacked IoT-connected devices in kitchens across the country, with almost comical outcomes. Smart toasters are forcing consumers into reconsidering eating habits by refusing to toast any bread that isn't considered 'healthy'. Smart Fridges and freezers across the UK are shutting down as soon as ice cream is detected. *(The message is abundantly clear. Leave that white bread on the grocery store counter and stock up on whole wheat, and while you're there, put down those high-fat/high-calorie frozen goodies in favour of good old wholesome fruit).*

IoT/IIoT topics to be covered

- Choosing the right controller for the application based on network, system, and end application requirements
- Designing reliability to meet the target asset or end application
- Security at the embedded product level

Reading List

Below is a list of required reading for this course. Questions from these readings will be on the weekly quiz.

- Silicon Labs' "Manage the IoT on an Energy Budget" https://www.silabs.com/Support%20Documents/TechnicalDocs/manage-the-iot-on-an-energy-budget.pdf
- "State Machines for Event-Driven Systems" http://www.barrgroup.com/Embedded-Systems/How-To/State-Machines-Event-Driven-Systems

Recommended readings. These readings will not be on the weekly quiz, but will be helpful in the class programming assignments and course project.

- Silicon Labs' Simplicity User Guide, AN0822 http://www.silabs.com/Support%20Documents/TechnicalDocs/AN0822-simplicity-studio-user-guide.pdf
- Silicon Labs' Energy Optimization Application Note, AN0027 http://www.silabs.com/Support%20Documents/TechnicalDocs/AN0027.pdf

Quiz

- Due by 11:59pm on Sunday, January 22nd, 2016
- Will cover topics discussed in the reading material as well as in lecture from January 17th onward

Survey

- This survey will help enable the instructing team to provide any additional resources that are necessary
- Due by 11:59pm on Sunday, January 22nd, 2016

Discussion topics for next lecture

- Low Power versus Low Energy Design
- What Makes a Low Energy Microcontroller
- Clock tree
- How to address register's and their bits
- Energy modes
- Keeping Track of the Energy State
- Exercise assigned