Embedded Systems

4th Stage

Lecture Five

Assist. Prof. Dr. Yasir Amer Abbas

Computer Engineering Department

2022

Embedded System Hardware

Lecture Five

Memories
Communication
Output
Electrical Energy: Energy Efficiency, Generation, and Storage
Secure Hardware

5. Embedded System Hardware

5.4 Memory

5.4.1 Conflicting Goals

Data, programs, and FPGA configurations must be stored in some kind of memory. Memories must have a capacity as large as required by the applications, provide the expected performance and still be efficient in terms of cost, size, and energy consumption.

5. Embedded System Hardware

5.1 Memory

5.4.2 Memory Hierarchies.

The **exact structure of the hierarchy** depends on **technological parameters** and also on **the application area**. Typically, we can identify at least the following levels in the memory hierarchy

- **Processor registers** can be seen as the fastest level in the memory hierarchy, with only a limited capacity of at most a few hundred words
- The **working memory** (or **main memory**) of computer systems implements the storage implied by processor memory addresses. Usually it has a capacity between a few Megabytes and some Gigabytes and is volatile.
- Typically, ***there is a large access speed difference between the main memory and registers.*** Hence, many systems include some type of buffer memory. Frequently used buffer memories include caches, translation look-aside buffers, and scratchpad memory (SPM). In contrast to PC-like systems and compute servers, ***the architecture of these small memories should guarantee a predictable real-time performance***. A combination of small memories containing frequently used data and instructions and a larger memory containing the remaining data and instructions is generally also more energy efficient than a single, large memory.

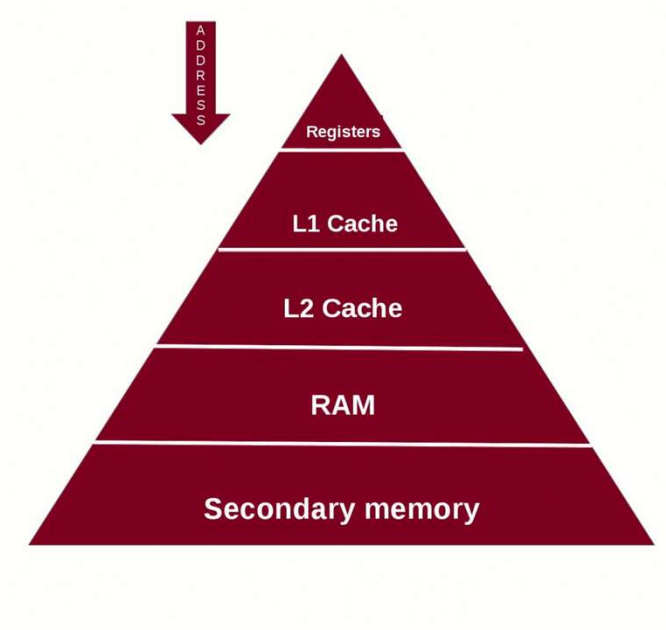
5. Embedded System Hardware

5.4 Memory

5.4.2 Memory Hierarchies.

Memories introduced so far are normally implemented in volatile memory technologies. In order to provide persistent storage, some different memory technology must be used.

For embedded systems, flashmemory is frequently the best solution. In other cases, hard disks or Internet-based storage solutions (like the "cloud") may be used.



5. Embedded System Hardware

5.4 Memory

5.4.3 Register Files

- The mentioned impact of the storage capacity on access times and energy consumption applies even to small memories such as register files. Figure 5.1 shows the cycle time and the power as a function of the size of memories used as register files.
- The power needs to be considered due to frequent accesses to registers, as a result of which they can get very hot.

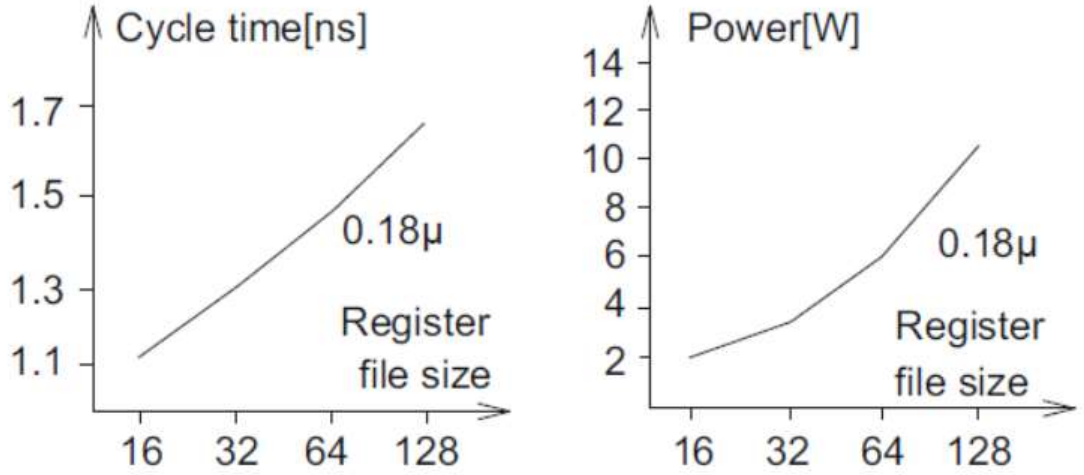


Fig. 5.1 Cycle time and power as a function of the register file size

5. Embedded System Hardware

5.4 Memory

5.4.4 Caches

For caches it is required that the hardware checks whether or not the cache has a valid copy of the information associated with a certain address. This check involves comparing the tag fields of caches, containing a subset of the relevant address bits . If the cache has no valid copy, the information in the cache is automatically updated.

5.4.5 Scratchpad Memories

Alternatively, small memories can be mapped into the address space **Fig. 5.2.** Such memories are called scratchpad memories (SPMs) or tightly coupled memories (TCM). SPMs are accessed by a proper selection of memory addresses. There is no need for checking tags, as for caches. Instead, the SPM is accessed whenever some simple address decoder is signaling an address to be in the address range of the SPM. SPMs are typically integrated together with processors on the same die. Hence, they are a special case of on-chip memories.

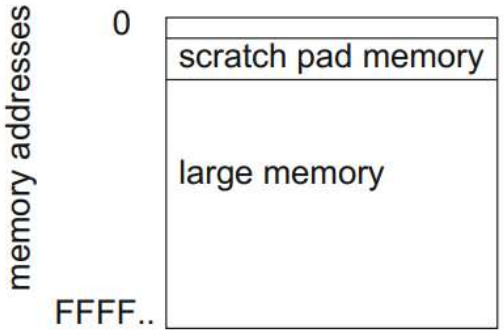


Fig. 5.2 Memory map with scratchpad included

5. Embedded System Hardware

5.5 Communication

Information must be communicated before it can be processed in an embedded system. Communication is particularly important for the Internet of Things. Information can be communicated through various channels.

Channels are abstract entities characterized by the essential properties of communication, such as ***maximum information transfer capacity*** and ***noise parameters***. The probability of communication errors can be computed using communication theory techniques.

The physical entities enabling communication are called communication media. Important media classes include: wireless media (radio frequency media, infrared), optical media (fibers), and wires.

There is a huge variety of communication requirements between the various classes of embedded systems. In general, connecting the different embedded hardware components is far from trivial. Some common requirements can be identified.

5. Embedded System Hardware

5.5 Communication

5.5.1 Requirements

The following list contains some of the requirements that must be met:

• **Real-time behavior**:

This requirement has far-reaching consequences on the design of the communication system. Several low-cost solutions such as standard Ethernet fail to meet this requirement.

• **Efficiency**:

Connecting different hardware components can be quite expensive.

For example, point-to-point connections in large buildings are almost impossible. Also, it has been found that separate wires between control units and external devices in cars significantly add to the cost and the weight of the car. With separate wires, it is also very difficult to add new components. The need of providing cost-efficient designs also affects the way in which power is made available to external devices. There is frequently the need to use a central power supply in order to reduce the cost.

• **Appropriate bandwidth and communication delay**:

Bandwidth requirements of embedded systems may vary. It is important to provide sufficient bandwidth without making the communication system too expensive.

5. Embedded System Hardware

5.5 Communication

5.5.1 Requirements

• **Support for event-driven communication**: polling-based systems provide a very predictable real-time behavior. However, their communication delay may be too large and there should be mechanisms for fast, event-oriented communication. For example, emergency situations should be communicated immediately and should not remain unnoticed until some central controller polls for messages.

• **Robustness**: Cyber-physical systems may be used at extreme temperatures, close to major sources of electromagnetic radiation, etc. Car engines, for example, can be exposed to temperatures less than −20 and up to +180 degrees Celsius (−4 to 356 degrees Fahrenheit).

• **Fault tolerance**: Despite all the efforts for robustness, faults may occur. Cyber physical systems should be operational even after faults, if at all feasible. Restarts, like the ones found in personal computers, cannot be accepted.

• **Maintainability, diagnosability**: obviously, it should be possible to repair embedded systems within reasonable time frames.

• **Security/privacy**: Ensuring security/privacy of confidential information may require the use of encryption.

5. Embedded System Hardware

5.5 Communication

5.5.2 Electrical Robustness

There are some basic techniques for electrical robustness. Digital communication within chips is normally using so-called single-ended signalling. For single-ended signalling, signals are propagated on a single wire (see Fig. 5.3).

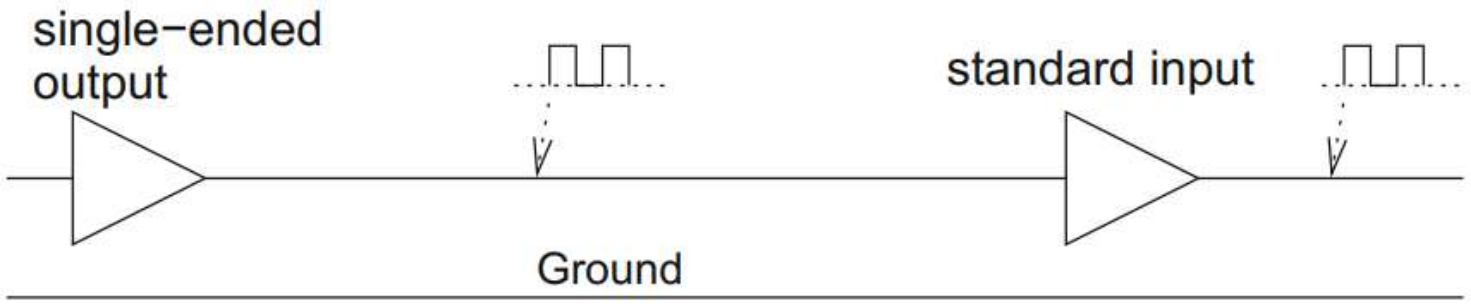


Fig. 5.3 Single-ended signalling

5. Embedded System Hardware

5.5 Communication

5.5.3 Guaranteeing Real-Time Behavior

- For internal communication, computers may be using dedicated point-to-point communication or shared buses.
- Point-to-point communication can have a good real-time behavior, but requiresmany connections and theremay be congestion at the receivers. Wiring is easier with common, shared buses. Typically, such buses use priority-based arbitration if several access requests to the communication media exist.
- ***Priority-based arbitration comes with poor timing predictability***, since conflicts are difficult to anticipate at design time. Priority-based schemes can even lead to "starvation" (low-priority communication can be completely blocked by higher priority communication). In order to get around this problem, *time division multiple access* (TDMA) can be used

5. Embedded System Hardware

5.5 Communication

5.5.4 Examples

1. **Sensor/actuator buses**: Sensor/actuator buses provide communication between simple devices such as switches or lamps and the processing equipment. There may be many such devices, and the cost of the wiring needs special attention for such buses.

2. **Field buses**: Field buses are similar to sensor/actuator buses. In general, they are supposed to support larger data rates than sensor/actuator buses. Examples of field buses include the following:

A. Controller Area Network (CAN): This bus was developed in 1981 by Bosch and Intel for connecting controllers and peripherals. It is popular in the automotive industry, since it allows the replacement of a large amount of wires by a single bus. Due to the size of the automotive market, CAN components are relatively cheap and are therefore also used in other areas such as smart homes and fabrication equipment.

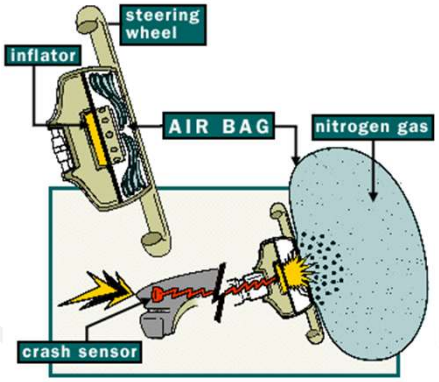
5. Embedded System Hardware

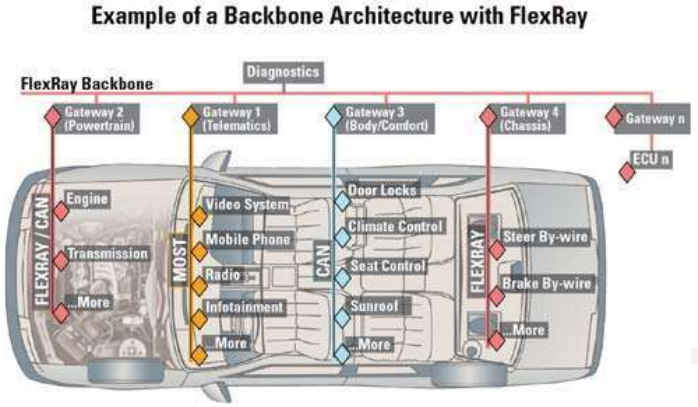
5.5 Communication

5.5.4 Examples

B. The **Time-Triggered-Protocol (TTP)** for fault-tolerant safety systems such as air bags in cars.

C. **FlexRay™** is a TDMA (Time-division multiple access) protocol which has been developed by the FlexRay consortium (BMW, Daimler AG, General Motors, Ford, Bosch, Motorola, and Philips Semiconductors). FlexRay is a combination of a variant of the TTP and the byte flight protocol. FlexRay includes a static as well as a dynamic arbitration phase. The static phase uses a TDMA-like arbitration scheme. It can be used for real-time communication, and starvation can be avoided. The dynamic phase provides a good bandwidth for non-real-time communication. Communicating partners can be connected to up to two buses for fault tolerance reasons. Bus guardians may protect partners against partners flooding the bus with redundant messages, socalled babbling idiots. Partners may use their own local clock periods.





5. Embedded System Hardware

5.5 Communication

5.5.4 Examples

D. **LIN** (local interconnect network) is a low-cost communication standard for connecting sensors and actuators in the automotive domain.

E. **MAP**: MAP is a bus designed for car factories.

F. **EIB**: The European installation bus (EIB) is a bus designed for smart homes.

5. Embedded System Hardware

5.5 Communication

5.5.4 Examples

3. The **Inter-Integrated Circuit** (I2C) Bus is a simple low-cost bus designed to communicate at short distances (meter range) with relatively low data rates. The bus needs only four wires: ground, SCL (clock), SDA (data), and a voltage supply line. Data and clock lines are open collector lines

4. Wired multimedia communication: for wiredmultimedia communication, larger data rates are required.

Example: **MOST** (media-oriented systems transport) is a communication standard for multimedia and infotainment equipment in the automotive domain . Standards such as IEEE 1394 (FireWire) may be used for the same purpose.

5. Embedded System Hardware

5.5 Communication

5.5.4 Examples

5. **Wireless communication**:This kind of communication is becoming more popular. There are several standards for wireless communication, including the following:

A. **Mobile communication** is becoming available at increased data rates. 7 Mbit/s is obtained with HSPA (high-speed packet access). About ten times higher rates are available with **long-term evolution (LTE)**.

B. **Bluetooth** is a standard for connecting devices such as mobile phones and their headsets over short distances.

C. **Wireless local area networks** (WLANs) are standardized as IEEE standard 802.11, with several supplementary standards.

D. **ZigBee** (see http://www.zigbee.org) is a communication protocol designed to create personal area networks using low-power radios. Applications include home automation and the Internet of Things.

E. **Digital European Cordless Telecommunications (DECT)** is a standard used for wireless phones. It is being used throughout the world, except for different frequencies used in North America

5. Embedded System Hardware

3.6 Output

Output devices of embedded/cyber-physical systems include:

• **Displays**: Display technology is an area which is extremely important. Accordingly, a large amount of information exists on this technology. Major research and development efforts lead to new display technology such as organic displays.

Organic displays are emitting light and can be fabricated with very high densities. In contrast to LCD displays, they do not need backlight and polarizing filters. Major changes are, therefore, expected in these markets.

• **Electro-mechanical devices**: These influence the environment through motors and other electro-mechanical equipment.

5. Embedded System Hardware

5.6 Output

5.6.1 Digital-to-Analog Converters

A Digital to Analog Converter (DAC) converts a digital input signal into an analog output signal. The digital signal is represented with a binary code, which is a combination of bits 0 and 1. This chapter deals with Digital to Analog Converters in detail.

5.6.2 Sampling Theorem

Suppose that the processors used in the hardware loop forward values from ADCs unchanged to the DACs.

5.6.3 Pulse-width Modulation

PWM signals can be generated by comparing a counter against a value stored in a programmable register

5.6.4 Actuators

n actuator is a component of a machine that is responsible for moving and controlling a mechanism or system. There is a huge amount of actuators . Actuators range from large ones that are able to move tons of weight to tiny ones with dimensions in the µm area

5. Embedded System Hardware

5.7 Electrical Energy: Energy Efficiency, Generation, and Storage

General constraints and objectives for the design of embedded and cyber-physical systems have to be obeyed for hardware design. Among the different objectives, we will focus on energy efficiency.

5.7.1 Energy Efficiency of Hardware Components

A comparison between these technologies and changes over time (corresponding to a certain fabrication technology) shown in Fig. 5.4. The figure reflects the conflict between efficiency and flexibility of currently available hardware technologies.

The diagram shows the energy efficiency GOP/J in terms of number of operations per unit of energy of various target technologies as a function of time and the target technology

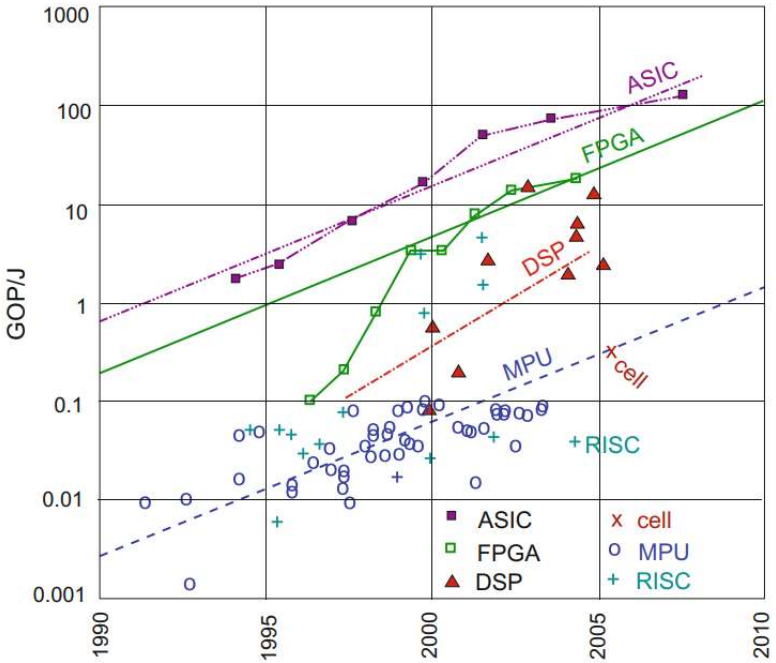


Fig. 5.4 Hardware efficiency

5. Embedded System Hardware

5.7 Electrical Energy: Energy Efficiency, Generation, and Storage

5.7.1 Energy Efficiency of Hardware Components

In this context, operations could be 32-bit additions. Obviously, the number of operations per Joule is increasing as technology advances to smaller and smaller feature sizes of integrated circuits. However, for any given technology, the number of operations per Joule is largest for hardwired application-specific integrated circuits (ASICs).

For reconfigurable logic usually coming in the form of field programmable gate arrays (FPGA), this value is about one order of magnitude less.

For programmable processors, it is even lower. However, processors offer the largest amount of flexibility, resulting from the flexibility of software

.

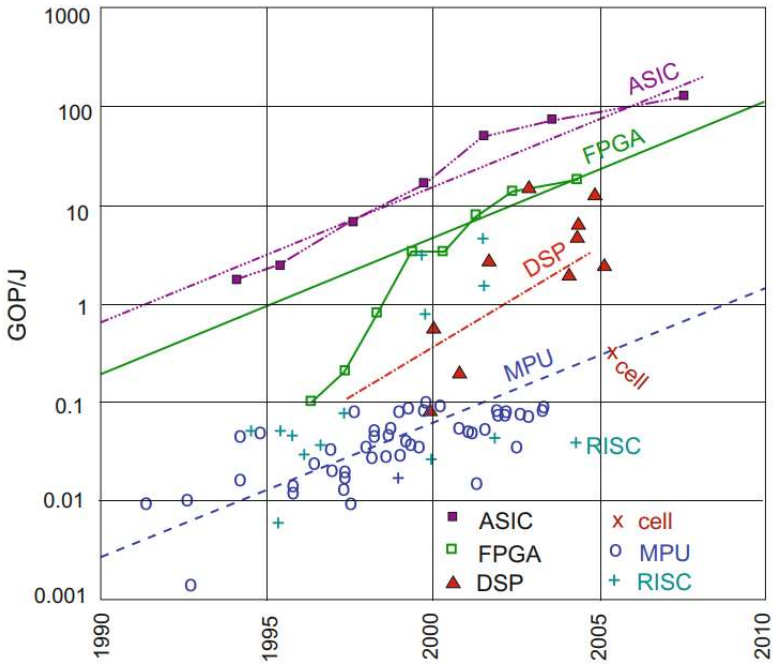


Fig. 5.4 Hardware efficiency

5. Embedded System Hardware

5.7 Electrical Energy: Energy Efficiency, Generation, and Storage

5.7.1 Energy Efficiency of Hardware Components

5.7.1.1 The Case of Mobile Phones

For smart phones, computational requirements are increasing at a rapid rate, especially for multimedia applications.

5.7.1.2 Sensor Networks

Sensor networks used for the Internet of Things are another special case. For sensor networks, there may be even much less energy available than for mobile phones. Hence, energy efficiency is of utmost importance, comprising of course energy efficient communication.

5. Embedded System Hardware

5.7 Electrical Energy: Energy Efficiency, Generation, and Storage

5.7.2 Sources of Electrical Energy

For all others, energy must be made available via other techniques. In particular, this applies to sensor networks used in IoT systems where energy can be a very scarce resource. Batteries store energy in the form of chemical energy..

1. Photovoltaics allows the conversion of light into electrical energy. The conversion is usually based on the photovoltaic effect of semiconductors. Panels of photovoltaic material are in widespread use

2.The **piezoelectric** effect can be used to convert mechanical strain into electrical energy. Piezoelectric lighters exploit this effect.

3.**Thermoelectric generators** (TEGs) allow turning temperature gradients into electrical energy. They can be used even on the human body.

4.**Kinetic energy** can be turned into electrical energy. This is exploited, for example, for some watches. Also, wind energy falls into this category.

5.**Ambient electromagnetic radiation** can be turned into electrical energy as well.
• There are many other physical effects allowing us to convert other forms of energy into electrical energy

5. Embedded System Hardware

3.8 Secure Hardware

In particular, security is important for the Internet of Things. If security is a major concern, special secure hardware may need to be developed. Security may need to be guaranteed for communication and for storage. Security has to be provided despite possible attacks. **Attacks** can be partitioned into the following:

• **Software attacks** which do not require physical access: the deployment of software Trojans is an example of such an attack. Also, software defects can be exploited. Buffer overflows are a frequent cause of security hazards.

• Attacks which require physical access and which can be classified into the following:

– **Physical attacks**: These try to physically tamper with the system. For example, silicon chips can be opened and analysed. The first step in this procedure is de-packaging (removing the plastic covering the silicon). Next, micro-probing or optical analysis can be used. Such attacks are difficult, but they reveal many details of the chip.

5. Embedded System Hardware

3.8 Secure Hardware

– **Side-channel attacks**: These try to exploit additional sources of information complementing the specified interfaces.

Timing analysis may reveal which data is being processed. This is especially true if execution times of software are data-dependent. Security-relevant algorithms should be designed such that their execution time.

Power analysis is a second class of attacks. Power analysis techniques include simple power analysis (SPA) and differential power analysis (DPA). In some cases, SPA may be sufficient to compute encryption keys directly from simple power measurements. In other cases, advanced statistical methods may be needed to compute keys from small statistical fluctuations of measured currents.

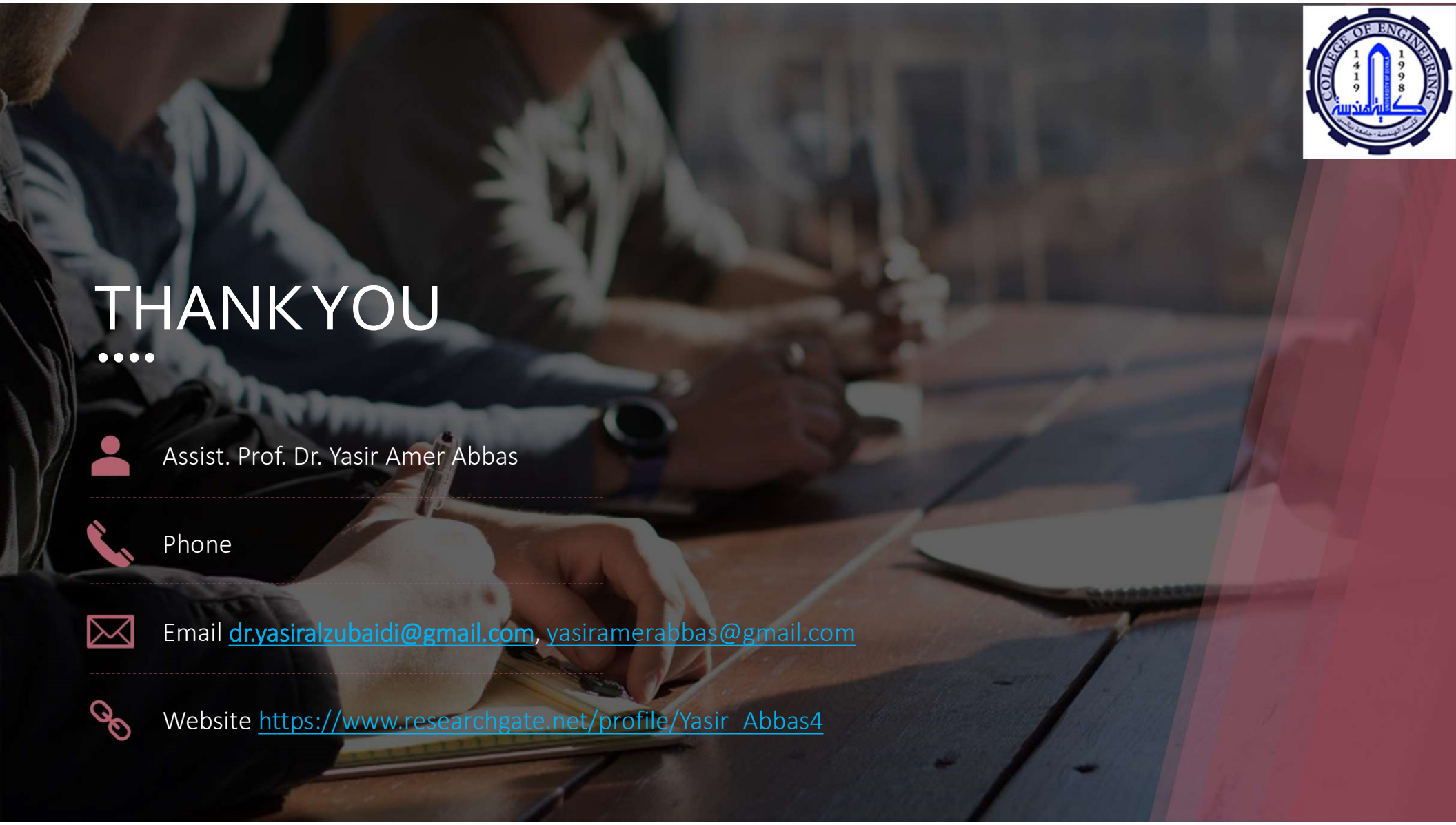
Analysis of electromagnetic radiation is a third class of side-channel attack.

5. Embedded System Hardware

3.8 Secure Hardware

The following **challenges** exist for the design of counter measures:

1. **Processing gap**: Due to the limited performance of embedded systems, advanced encryption techniques may be too slow, in particular if high data rates have to be processed.
2. **Battery gap**: Advanced encryption techniques require a significant amount of energy. This energy may be unavailable in a portable system. Smart cards are a special case of hardware that must run using a very small amount of energy.
3. **Flexibility**: Frequently, many different security protocols are required within one system and these protocols may have to be updated from time to time. This hinders using special hardware accelerators for encryption.
4. **Tamper resistance**: Mechanisms against malicious attacks need to be built in. Their design is far from trivial. For example, it may be difficult if not impossible to guarantee that the current consumption is independent of the cryptographic keys that are processed.
5. **Assurance gap**: The verification of security requires extra efforts during the design.
6. **Cost**: Higher security levels increase the cost of the system.



THANK YOU

Assist. Prof. Dr. Yasir Amer Abbas

Phone

Email dr.yasiralzubaidi@gmail.com, yasiramerabbas@gmail.com

Website https://www.researchgate.net/profile/Yasir_Abbas4