Co-funded by the Erasmus+ Programme of the European Union

International Master of Science on Cyber Physical Systems

Gap analysis: Identify any shortcomings of courses or expertise in all partners and make the necessary plan to compensate these shortcomings.

D1.3

Project Acronym	MS@CPS	**Project Number**	598750-EPP-1-2018-1-DE-EPPKA2-CBHE-JP
Date	2019-11-15	**Deliverable No.**	1.3
Contact Person	Rashid Jayousi	**Organisation**	AQU
Phone	+970 592 907 989	**E-Mail**	rjayousi@staff.alquds.edu
Version	3.0	**Confidentiality level**	Public

Version History

Version No.	Date	Change	Editor(s)
0	1/10/2019	Initial outline	Isam Ishaq, Rashid Jayousi, Salah Odeh
1	20/10/2019	Input from working groups integrated	Ezzaldeen Edwan, Ala' Khalifah, Nadia Aloui. Zaid Alhalhouli,
2		Intermediate version	
3		Final draft for QC	
4		Final version for delivery to EC, integrated	

Contributors

Name	Organization
Isam Ishaq	AQU
Rashid Jayousi	AQU
Salah Odeh	AQU
Ala' Khalifeh	GJU
Ezzaldeen Edwan	PTC
Nadia Aloui	CU
Zaid Alhalhouli	TTU
Bassam Bouaziz	USF

Disclaimer

This project has been funded with support from the European Commission. This publication reflects the views only of the author(s), and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

Introduction

As a result of the work done in D1.2 and in the workshop held at GJU in June, the core modules were identified and consequently the learning and objectives were decided upon. A survey amongst partner countries was conducted to identify the needed expertise and shortcomings of courses in all partners and make the necessary plan to compensate these shortcomings. This, combined with the previously conducted industrial workshops, is important to ensure the learning outcomes of the designed courses meet the national market and ICT sector needs. A report on needed key competencies and required skills within the national scope of partner countries is presented in this deliverable.

1.1 Scope

The scope of this deliverable is the universities in partner countries. This deliverable explores the various capacity building needed for the implementation of the CPS program in partner countries. This will help to identify the necessary training workshops to be conducted at later stages.

1.2 Relation to deliverables

This deliverable will act as the initial phase to identify topics and training needs in the following work packages.

1.3 Relation to work packages

This deliverable will act as a milestone for WP2 that is concerned in the development of the courses program structure and modules. This deliverable will help in the design and development of case studies and put them into action by working through the cases whether inside of the companies or in a simulated work environment.

1.4 Terminology

CPS: Cyber Physical System

Modules/Courses: These two words are used interchangeably to indicate a unit of the program to be implemented.

Partner Countries: Countries where the program to be implemented (Palestine, Tunisia, Jordan)

Program Countries: EU partners (Germany, Sweden, and UK)

Program: The master program (CPS) to be implemented

1. Methodology

In order to identify the needed expertise and shortcomings of courses to be implemented in partner countries, a survey is used for this purpose. This survey is presented in Appendix 1. The surveys are available in the repository.

The survey contains a list of the courses as well columns for the needed capacities and equipment needed for each partner country.

After the surveys were filed it was analyzed and summarized as can be seen in the next section.

2. Survey Results

Image 1 shows a snap shot of part of the survey results, the needed capacities and will be discussed in more details in the conclusion section.

The detailed table can be found in the following link:

https://erasmus_mscps.teams.uni-siegen.de/workpackages/wp1/_layouts/15/start.aspx#/SitePages/Home.aspx?RootFolder=%2Fworkpackages%2Fwp1%2FShared%20Documents%2FDeliverables&FolderCTID=0x012000A12A81137E814540BAEEBC3C93717EDA&View=%7BB612AD93%2D4197%2D4AB0%2D8384%2D538A493F9F0B%7D

This in the project repository under the documents section of the sub directory Workpackage 1.

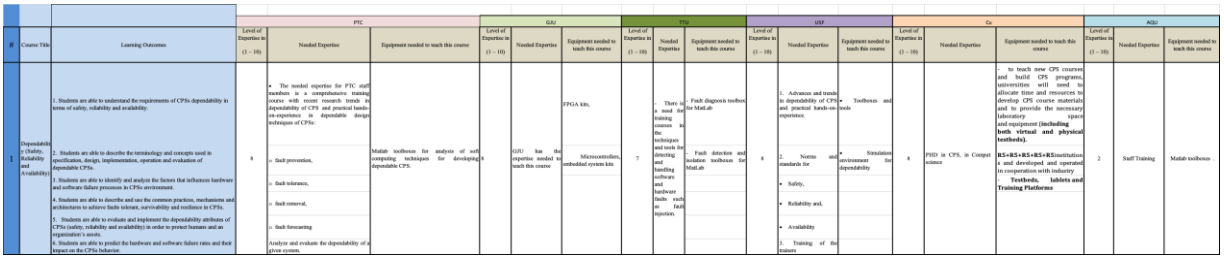

Image 1: A snap shot of part of the survey results

The survey was basically a table with the columns shown in Table 1 :

#	Course Title	Learning Outcomes	Level of Expertise in your institute (1 – 10)	Needed Expertise	Equipment needed to teach this course

Each row was dedicated to a course and the learning outcomes of the course listed in the adjacent cell in the table. Partners were asked to answer the following questions in the indicated cells:

- Level of Expertise in your institute
- Needed Expertise (1 – 10)
- Equipment needed to teach this course

The survey was prepared for the following courses with the given learning outcomes:

2.1 Dependability (Safety, Reliability and Availability)

1. Students are able to understand the requirements of CPSs dependability in terms of safety, reliability and availability.
2. Students are able to describe the terminology and concepts used in specification, design, implementation, operation and evaluation of dependable CPSs.
3. Students are able to identify and analyze the factors that influences hardware and software failure processes in CPSs environment.
4. Students are able to describe and use the common practices, mechanisms and architectures to achieve faults tolerant, survivability and resilience in CPSs.
5. Students are able to evaluate and implement the dependability attributes of CPSs (safety, reliability and availability) in order to protect humans and an organization's assets.
6. Students are able to predict the hardware and software failure rates and their impact on the CPSs behavior.

2.2 Security and Privacy

1. Students can identify major types of threats, risks, attacks and vulnerabilities of information, application, and network security and privacy in Cyber Physical System environments and develop a security model to prevent, detect, and recover from them.
2. Students are able to understand and examine how the major security tools, techniques, and approaches such as access control management, firewalls, anti-virus software, intrusion prevention systems, proper backups and restores management systems, and proper secure protocols work in detail for testing, monitoring, tracking and auditing of security threats and vulnerabilities of Cyber Physical Systems and how the security tools can be deployed in practice taking into account associated strengths and weaknesses
3. Students can demonstrate ability to independently select and exercise the appropriate practices and technologies necessary to solve concrete problems in cyber and information security related to confidentiality (cryptographic solutions), integrity (authentication such as biometric), availability (for example, intrusion detection solutions), and privacy protection in their homes and professional environments.
4. Students are able to design and develop a security architecture for Cyber Physical Systems to ensure service continuity and reliability
5. Students are able to design operational security and privacy policies, strategies, and standards and practices for Cyber Physical Systems and recognize the role of management in enforcing security and privacy policies, standards and practices.
6. Students can demonstrate capabilities to apply the security and privacy knowledge in new areas within Cyber Physical Systems, in particular cloud computer security, security on the Internet of Things (IoT), and security of blockchain technology applications.
7. Student can describe and compare the common cryptographic encryption and decryption algorithms and the tools to ensure data integrity such as hashing, symmetric and asymmetric encryption, certificates, and methods of implementing cryptography.
8. Students are able to systematically and independently solve complex problems of research and development in the field of security and privacy of Cyber Physical Systems by analyzing, formulating sub-tasks, and proposing and implementing innovative solutions.
9. Students are able to identify and assess security and privacy risks in Cyber Physical System environments to mitigate, avoid, and transfer these risks.

10. Students are able to understand the data attributes such as confidentiality, possession or control, integrity, authenticity, availability, and utility, any of which can make it vulnerable to attack.

2.3 Cloud Computing

1. Describe fundamental concepts of cloud computing and differentiate between service and deployment models of cloud computing.
2. Illustrate fundamental concepts of cloud storage and compare different types of cloud file systems and databases.
3. Examine cloud programming models and apply them to solve problems on the cloud.
4. Discuss resource virtualization and their role in enabling the cloud computing model.
5. Assess the performance, scalability, and availability of the underlying cloud technologies.
6. Identify security and privacy issues in cloud computing.
7. Deploy applications over commercial cloud computing infrastructures such as Amazon Web Services (AWS), Windows Azure, and Google AppEngine.

2.4 Control systems

1. understand the core principles behind CPS. A solid understanding of these core principles is important for anyone who wants to integrate cyber and physical components
2. develop models and controls. In order to understand, design, and analyze CPS, it is important to be able to develop models for the various relevant aspects of a CPS design and to design controllers for the intended functionalities based on appropriate specifications
3. Identify the relevant dynamical aspects. Identify which types of phenomena of a CPS have a relevant influence for the purpose of understanding a particular property of a particular system.
4. Computational Thinking.

   - identify safety specifications and critical properties

   - understand abstraction in system designs

   - express pre- and post-conditions and invariants for CPS models

   - Developing correct CPS designs

   - use formal methods tools for CPS

5. CPS Skills.

   - understand the semantics of a CPS model

   - develop an intuition for operational effects

   - Understand opportunities and challenges in CPS and verification.

2.5 Embedded Systems

1. Demonstrate knowledge and understanding of the fundamental principles embedded systems design, explain the process and apply it.
2. Demonstrate knowledge and understanding of the microprocessor technology both for hardware and software.
3. Design embedded systems based on microprocessor.
4. Demonstrate knowledge and understanding of Hardware/Software co-design techniques for microprocessor-based embedded systems, apply techniques in design problems.

5. Program microprocessors in C using Integrated Development Environments.
6. From an abstract description design and implement a small but typical embedded time-ordered application for one emulated target machine

2.6 Real time systems

1. Understanding principles of embedded systems design; be aware of architectures and behaviors of embedded systems.
2. Specify needs to create a real-time system and where real-time requirements are needed
3. Design an application with real-time constraints.
4. Solve scheduling problems and apply them in real time applications in industry
5. Discover the usual methods for Real Time Specification. SADT, SART, and will focus on the UML specification

2.7 Sensors and actuators

1. Explain fundamental physical and technical base of sensors and actuators,
2. Develop an understanding of measurement principles, signal conditioning and data acquisition systems.
3. Develop systematic techniques for specifying transducers best suited to a range of applications.
4. Understand the design concepts and operation of a broad range of actuator devices.
5. Give in depth consideration of the performance envelopes and basis of selection of different actuator and microactuator types.

2.8 Wireless Communication Networks

1. Summarize and describe the properties, characteristics and design different types of Communication Networks, Protocols and TCP/IP Suite.
2. Build a deep understanding for Wireless Channel and Signal Encoding Techniques in terms of Antennas, Spectrum Considerations, Line-Of-Sight Transmissions and Signal Encoding Criteria.
3. Explain and Summarize the Orthogonal Frequency Division Multiplexing (OFDM) and the types of Spread Spectrum.
4. Apply knowledge of Coding and Error Control in order to compare error recovery processes among different types of codes.
5. Explain and describe the Architecture, Services, Access Control and Physical Layers of IEEE 802 standards for the Wireless LAN (WLAN) and Bluetooth Technologies.
6. Explain, describe and summarize the Wireless Mobile Networks and Long Range Communication Networks such as Satellite Networks and WiMAX technologies and their related standards.

2.9 Distributed Systems

1. Summarize and describe general properties, characteristics, design and different types of distributed systems.
2. Explain distributed architectures and processes in an industrial enterprise.
3. Explaining the rules communicating processes and data transmissions in distributed systems.
4. Describe how processes can synchronize and coordinate their actions.
5. Apply appropriate data replication methods to improve reliability and performance of distributed systems.
6. Use appropriate techniques in order achieve fault tolerance and recovery process.

2.10 Entrepreneurship

1. learn how to think on ideas that have business, marketing values and solves a problem in an efficient and distinguished way.
2. Define the target market, competitors, the competitive advantage, and learn how to conduct a market research study and analysis
3. Learn how to build a successful team and identify the needed resources
4. Learn the different business models that can be used to monetize the proposed idea
5. Know how market the business idea and reach the customers
6. Learn different methodologies and mechanisms used to raise funding
7. How to write a successful business plan.

The following expertise is needed to deliver the course efficient:

- Business development
- Marketing skills
- Basic financial knowledge
- Entrepreneurship practical experience is preferred

No special hardware is needed for this course.

2.11 Distributed Control Systems

1. Describe sensors, instrumentation, and process control as their relation to DCSs.
2. Know DCS organization and operation
3. Understand networking, HMI, and alarm features of DCSs
4. Understand Issues and procedures to perform DCS maintenance and troubleshooting
5. Compare and implement advanced Process Controllers in DCSs
6. Describe and evaluate the latest trends related to DCSs such as industrial Internet, Internet of Things, Mobile and remote devices.
7. Apply HMI and SCADA design of DCSs

2.12 Human-Computer Interaction

1. Interpret user-centered designs and explore their associate interdisciplinary nature.
2. Describe and use HCI design principles, standards and guidelines.
3. Apply an interactive design process and universal design principles to designing user-interfaces.
4. Compare state-of-the-art technologies for user interaction design.
5. Evaluate the user-centered rationale for an interactive system design project.
6. Implement, using a collaborative approach, user centered designs in industrial application.

2.13 Mobile and Ubiquitous Computing

1. Describe and discuss the emerging topics (vision, motivation, challenges) of pervasive and ubiquitous computing as well as context-aware computing and their applications.
2. Explain and show the ability to implement concepts related to the design and utilization of smart (mobile) systems.
3. Understand the major concepts and components of wireless and mobile networks
4. Describe and discuss the next generation mobile systems (e.g., smartphones, tablets) and their application areas.

5. Demonstrate basic knowledge in developing smartphone applications using various platforms, toolkits, APIs and third-party libraries.
6. Develop and research in the different topics related to ubiquitous computing such as Sensing and Basic Electronics; Tangible Computing; Wearable Computing; Sustainability and Technology.

2.14 Industrial Communication Protocols

1. Explain the rationale behind the technological development of industrial networks from telemetry systems to modern SCADA systems
2. Identify and explain the reasons behind the differences between industrial network communication protocols and the protocols used in general computer networking.
3. Investigate the relevance and applicability of the seven layers OSI model to commonly used industrial protocols such as Ethernet IP, Modbus, Profibus and DNP3
4. Compare and evaluate the relative strengths and weaknesses of different industrial protocols for particular applications.
5. Select an industrial protocol and use it in an application such as building services, power
6. systems automation, water treatment and factory automation

2.15 Internet of Things

1. Able to understand the application areas of IOT .
2. Able to realize the revolution of Internet in Mobile Devices, Cloud & Sensor Networks
3. Able to understand building blocks of Internet of Things and characteristics
4. Able to design and program some IOT based devices and prototypes
5. Able Secure the elements of an IoT device
6. Able to design an IoT device to work with a Cloud Computing infrastructure.
7. To be familiar with the key wireless technologies used in IoT systems, such as WiFi, 6LoWPAN, Bluetooth and ZigBee

2.16 Low power networks

1. Become informed as to why WSNs are underpinning the evolution to the Internet of Things.
2. Discover the challenges of providing connectivity to devices that are operating in highly variable and lossy RF environments.
3. Build a solid understanding of the wireless protocols that have been defined to support connectivity of low power devices.
4. Understand the different mechanisms important for enabling sensors and other low power devices to connect to the Internet.
5. Learn key routing protocols for sensor networks and main design issues.
6. Reveal what higher layer protocols are enabling applications and services to run over wireless Low Power Networks.
7. Understand the Sensor management, sensor network middleware, operating systems.

2.17 Mobile Communication Networks

1. Understand the main principles of the different mobile communication systems, and track their evolution paths.
2. Develop a thorough knowledge of the system architecture for the traditional and the emerging cellular communication networks, and compare their architectures in terms of their components, interfaces, and interactions.

3. Evaluate the technical issues in the existing mobile communication networks including. coverage area, interference analysis, handoff strategies, channel assignment, trunking efficiency, security, and multiple access techniques.
4. Apply radio resources' management principles to evaluate the capacity and the spectral efficiency of the existing cellular communication networks, and to design new systems.
5. Analyze and calculate the path loss, fading profiles, and effects of multi-path propagation in various cellular environments.
6. Understand the technical strategies in the design of LTE and discuss the technical features of the emerging cellular communication systems.

2.18 Network Optimization

1. Apply the different optimization methods, a powerful tool for solving problems involving constrained optimization of time averages.
2. Understand the theory of dynamic decision making for networks and other stochastic systems.
3. Formulate the complex problems in the standard form of minimizing an objective subject to an additional set of constraints. This includes linear and convex programs and their counterparts.
4. Implement the knowledge of the modern optimization algorithms for routing problems, shortest path, minimum-cost flow and maximum flow.
5. Explore hot-topic problems of opportunistic scheduling, approximate scheduling, dynamic data compression, efficient energy allocation.
6. Become skilled to apply the theory by formulating and solving their own problems that involve dynamic decisions and implement a research projects.

2.19 Machine Learning

1. Describe the principles of Human Computer Interface systems, and give examples to illustrate the concepts of the subject.
2. Learn a theoretical knowledge and practical experiences in the fundamental aspects of designing, implementing and evaluating interfaces.
3. Compare state-of-the-art technologies for user interaction design.
4. Analyze the system requirements.
5. Design effective and usable graphical computer interfaces
6. Apply contemporary techniques for implementing interfaces, and have experienced building applications through prototyping tools, window-based systems, and toolkits
7. Interpret user centred designs and explore their associate interdisciplinary nature.
8. Evaluate the user-centered rationale for an interactive system design project.
9. Implement, using a collaborative approach, user centered designs in industrial applications.

3. Findings

The main findings are shown in Table 2.

Table 2: Survey Results Summary

#	Course Title	Needed Expertise	Equipment needed
1	Dependability (Safety, Reliability and Availability	There is a need for training courses in the techniques and tools for detecting and handling software and hardware faults such as fault injection.	Fault diagnosis toolbox for MatLab Fault detection and isolation toolboxes for MatLab
2	Security and Privacy	Both faculty and technicians at labs need practical training courses in the following security tools and technologies: Network Security Monitoring tools, Encryption Tools, Web Vulnerability Scanning tools, Network Defence Wireless Tools, Packet Sniffers, Firewall, PKI Services, Managed Detection Services.	Lab for software and network security with security tools and technologies: Network Security Monitoring tools, Encryption Tools, Web Vulnerability Scanning tools, Network Defence Wireless Tools, Packet Sniffers, Firewall, PKI Services, Managed Detection Services.
3	Cloud Computing	Faculty at TTU need practical training courses of the top cloud computing services such as: - Amazon Web Services - Microsoft Azure - Google Cloud - etc.	Subscriptions of cloud computing services in order to explore the features and capabilities of these services.
4	Control systems	Available	Available
5	Embedded Systems	The faculty at TTU need intensive training course in designing embedded systems, best software toolboxes and hardware for developing embedded systems, programmable boards.	Latest Hardware and software for constructing case studies in embedded systems.

7	SENSORS AND ACTUATORS	Available	- Equipments are needed, Sensors and actuators
8	Wireless Communication Networks	Partially needed	Simulators
10	Entrepreneurship	Available	No equipments
11	Distributed Control Systems	Needed a training course in using HMI and SCADA for developing distributed control systems.	Computer Lab with HMI and SCADA software.
12	Human-Computer Interaction	Need a training course in the latest technologies used in HCI such as: BCI, Motion Capture, 3D capture, 3D Projection, VR and AR.	HCI Lab with latest equipment and technologies in HCI field
13	Mobile and Ubiquitous Computing	Needed	-Sensors, simulators
14	Industrial Communication Protocols	Needed	Simulators and various software
15	Internet of Things	Needed	Research and teaching lab with wireless technologies (WiFi, 6LoWPAN, bluetooth and ZigBee)
17	Mobile Communication Networks	Needed	
18	Network Optimization	Available	-
19	Machine Learning	Available	-

From the table above, we can see training is needed for the different topics mainly embedded systems, internet of things, distributed control, security, dependability, safety, reliability and availability. Various equipment are required such sensors, actuators, laptops, tablets, as well as various software's such as MATLAB and network simulators.

4. Conclusion

After reviewing the results of the different surveys from partner countries and analysing it, the findings were summarised in table 2 that shows the main needed expertise from partner countries.

In the previous deliverable we had identified the main modules and possible courses as well as the ILOs. Looking at the proposed needed capacities and labs we can conclude what is mainly needed is mostly practical training within the curriculum and a shared pedagogy.

For the labs there is a need to carry on the discussion on the case studies needed and build upon it what sort of labs are needed and this was started in the last workshop at USF.

5. Appendix I

International Master of Science on Cyber Physical Systems

D1.3 Survey

Introduction

As a result of the work done in D1.2 and in the workshop held at GJU in June, the core modules were identified and consequently the learning and objectives were decided upon. We use this survey to identify the needed capacity to implement these modules in partner countries in terms of human and lab resources and make the necessary plan to compensate these shortcomings.

The following table shows the different modules and the courses under each module, the ones shaded are the core courses.

Embedded systems [CU]-USI Embedded platforms (hardware and software) Real-time systems Sensors and actuators Control systems **Advanced communication networks [PTC]-USI** Internet of things Distributed systems (open industrial) Cloud computing Low power networks Network optimization	**Safety and Security [TTU]-HERT** Security (privacy, data integrity) Dependability (Safety, reliability, availability) **AI and advanced computing [USF]-HERT** Machine learning Big data analytics Multi-agent systems Anomaly detection Computer vision Semantic web Optimization Theory and Algorithms

Industrial communication protocols Mobile communication networks Wireless communication networks (knowledge and design of APIs) **Entrepreneurship [GJU]-KTH** Innovation and entrepreneurship (incl. project work) Project management	Software engineering **Human/Machine Systems [AQU]-KTH** Human machine interaction Mobile and Ubiquitous Computing Distributed control systems

The ILOs for each course are shown in the table below.

#	Course Title	Learning Outcomes	Level of Expertise in your institute (1 – 10)	Needed Expertise	Equipment needed to teach this course
1	Dependability (Safety, Reliability and Availability	1. Students are able to understand the requirements of CPSs dependability in terms of safety, reliability and availability. 2. Students are able to describe the terminology and concepts used in specification, design, implementation, operation and evaluation of dependable CPSs. 3. Students are able to identify and analyze the factors that influences hardware and software failure processes in CPSs environment. 4. Students are able to describe and use the common practices, mechanisms and architectures to achieve faults tolerant, survivability and resilience in CPSs. 5. Students are able to evaluate and implement the dependability attributes of CPSs (safety, reliability and availability) in			

		order to protect humans and an organization's assets. 6. Students are able to predict the hardware and software failure rates and their impact on the CPSs behavior.			
2	Security and Privacy	1. Students can identify major types of threats, risks, attacks and vulnerabilities of information, application, and network security and privacy in Cyber Physical System environments and develop a security model to prevent, detect, and recover from them. 2. Students are able to understand and examine how the major security tools, techniques, and approaches such as access control management, firewalls, anti-virus software, intrusion prevention systems, proper backups and restores management systems, and proper secure protocols work in detail for testing, monitoring, tracking and auditing of security threats and			

		vulnerabilities of Cyber Physical Systems and how the security tools can be deployed in practice taking into account associated strengths and weaknesses 3. Students can demonstrate ability to independently select and exercise the appropriate practices and technologies necessary to solve concrete problems in cyber and information security related to confidentiality (cryptographic solutions), integrity (authentication such as biometric), availability (for example, intrusion detection solutions), and privacy protection in their homes and professional environments. 4. Students are able to design and develop a security architecture for Cyber Physical Systems to ensure service continuity and reliability 5. Students are able to design operational security and privacy policies, strategies,			

		and standards and practices for Cyber Physical Systems and recognize the role of management in enforcing security and privacy policies, standards and practices. 6. Students can demonstrate capabilities to apply the security and privacy knowledge in new areas within Cyber Physical Systems, in particular cloud computer security, security on the Internet of Things (IoT), and security of blockchain technology applications. 7. Student can describe and compare the common cryptographic encryption and decryption algorithms and the tools to ensure data integrity such as hashing, symmetric and asymmetric encryption, certificates, and methods of implementing cryptography. 8. Students are able to systematically and independently solve complex problems of			

		research and development in the field of security and privacy of Cyber Physical Systems by analyzing, formulating sub-tasks, and proposing and implementing innovative solutions. 9. Students are able to identify and assess security and privacy risks in Cyber Physical System environments to mitigate, avoid, and transfer these risks. 10. Students are able to understand the data attributes such as confidentiality, possession or control, integrity, authenticity, availability, and utility, any of which can make it vulnerable to attack.			
3	Cloud Computing	1. Describe fundamental concepts of cloud computing and differentiate between service and deployment models of cloud computing. 2. Illustrate fundamental concepts of cloud storage and compare different			

		types of cloud file systems and databases. 3 Examine cloud programming models and apply them to solve problems on the cloud. 4. Discuss resource virtualization and their role in enabling the cloud computing model. 5. Assess the performance, scalability, and availability of the underlying cloud technologies. 6. Identify security and privacy issues in cloud computing. 7. Deploy applications over commercial cloud computing infrastructures such as Amazon Web Services (AWS), Windows Azure, and Google AppEngine.			
4	Control systems	1. understand the core principles behind CPS. A solid understanding of these core principles is important for anyone who wants to integrate cyber			

		and physical components 2. develop models and controls. In order to understand, design, and analyze CPS, it is important to be able to develop models for the various relevant aspects of a CPS design and to design controllers for the intended functionalities based on appropriate specifications 3 Identify the relevant dynamical aspects. identify which types of phenomena of a CPS have a relevant influence for the purpose of understanding a particular property of a particular system. 4. Computational Thinking. - identify safety specifications and critical properties - understand abstraction in system designs - express pre- and post-conditions and invariants			

		for CPS models - Developing correct CPS designs - use formal methods tools for CPS 5. CPS Skills. - understand the semantics of a CPS model - develop an intuition for operational effects - Understand opportunities and challenges in CPS and verification.			
5	Embedded Systems	1. Demonstrate knowledge and understanding of the fundamental principles embedded systems design, explain the process and apply it 2.Demonstrate knowledge and understanding of the microprocessor technology both for hardware and software. 3. Design embedded systems based on microprocessor.			

		4. Demonstrate knowledge and understanding of Hardware/Software co-design techniques for microprocessor-based embedded systems, apply techniques in design problems. 5. Program microprocessors in C using Integrated Development Environments. 6. From an abstract description design and implement a small but typical embedded time-ordered application for one emulated target machine			
6	Real time systems	1. Understanding principles of embedded systems design; be aware of architectures and behaviors of embedded systems. 2. Specify needs to create a real-time system and where real-time requirements are needed 3. Design an application with real-time constraints. 4. Solve scheduling problems and apply them in real time			

		applications in industry 5. Discover the usual methods for Real Time Specification. SADT, SART, and will focus on the UML specification			
7	SENSORS AND ACTUATORS	1. Explain fundamental physical and technical base of sensors and actuators, 2. Develop an understanding of measurement principles, signal conditioning and data acquisition systems. 3. Develop systematic techniques for specifying transducers best suited to a range of applications. 4. Understand the design concepts and operation of a broad range of actuator devices. 5.Give in depth consideration of the performance envelopes and basis of selection of different actuator and microactuator types.			

8	Wireless Communication Networks	1. Summarize and describe the properties, characteristics and design different types of Communication Networks, Protocols and TCP/IP Suite. 2. Build a deep understanding for Wireless Channel and Signal Encoding Techniques in terms of Antennas, Spectrum Considerations, Line-Of-Sight Transmissions and Signal Encoding Criteria. 3. Explain and Summarize the Orthogonal Frequency Division Multiplexing (OFDM) and the types of Spread Spectrum. 4. Apply knowledge of Coding and Error Control in order to compare error recovery processes among different types of codes. 5. Explain and describe the Architecture, Services, Access Control and Physical Layers of IEEE 802 standards			

		for the Wireless LAN (WLAN) and Bluetooth Technologies. 6. Explain, describe and summarize the Wireless Mobile Networks and Long Range Communication Networks such as Satellite Networks and WiMAX technologies and their related standards.			
9	Distributed System	1. Summarize and describe general properties, characteristics, design and different types of distributed systems. 2. Explain distributed architectures and processes in an industrial enterprise. 3. Explaining the rules communicating processes and data transmissions in distributed systems. 4. Describe how processes can synchronize and coordinate their actions.			

		5. Apply appropriate data replication methods to improve reliability and performance of distributed systems . 6. Use appropriate techniques in order achieve fault tolerance and recovery process.			
10	Entrepreneurship	1. learn how to think on ideas that have business, marketing values and solves a problem in an efficient and distinguished way. 2. Define the target market, competitors, the competitive advantage, and learn how to conduct a market research study and analysis 3. Learn how to build a successful team and identify the needed resources 4. Learn the different business models that can be used to monetize the proposed idea 5. Know how market the business idea and reach the customers	1	The following expertise is needed to deliver the course efficient: - Business development - Marketing skills - Basic financial knowledge - Entrepreneurship practical experience is preferred	No special hardware.

		6. Learn different methodologies and mechanisms used to raise funding 7. How to write a successful business plan.			
11	Distributed Control Sytems	1. Describe sensors, instrumentation, and process control as their relation to DCSs. 2. Know DCS organization and operation 3. Understand networking, HMI, and alarm features of DCSs 4. Understand Issues and procedures to perform DCS maintenance and troubleshooting 5. Compare and implement advanced Process Controllers in DCSs 6. Describe and evaluate the latest trends related to DCSs such as industrial Internet, Internet of Things, Mobile and remote devices. 7. Apply HMI and SCADA design of DCSs			

12	Human-Computer Interaction	1. Interpret user-centered designs and explore their associate interdisciplinary nature. 2. Describe and use HCI design principles, standards and guidelines. 3. Apply an interactive design process and universal design principles to designing user-interfaces. 4. Compare state-of-the-art technologies for user interaction design. 5. Evaluate the user-centered rationale for an interactive systems design project. 6. Implement, using a collaborative approach, user centred designs in industrial application.			
13	Mobile and Ubiquitous Computing	1. Describe and discuss the emerging topics (vision, motivation, challenges) of pervasive and ubiquitous computing as well as context-aware			

		computing and their applications. 2. Explain and show the ability to implement concepts related to the design and utilization of smart (mobile) systems. 3. Understand the major concepts and components of wireless and mobile networks 4. Describe and discuss the next generation mobile systems (e.g., smartphones, tablets) and their application areas. 5. Demonstrate basic knowledge in developing smartphone applications using various platforms, toolkits, APIs and third-party libraries. 6. Develop and research in the different topics related to ubiquitous computing such as Sensing and Basic Electronics; Tangible Computing; Wearable Computing; Sustainability and Technology.			

14	Industrial Communication Protocols	1. Explain the rationale behind the technological development of industrial networks from telemetry systems to modern SCADA systems 2. Identify and explain the reasons behind the differences between industrial network communication protocols and the protocols used in general computer networking. 3. Investigate the relevance and applicability of the seven layer OSI model to commonly used industrial protocols such as EthernetIP, Modbus, Profibus and DNP3 4. Compare and Evaluate the relative strengths and weaknesses of different industrial protocols for particular applications. 5. Select an industrial protocol and use it in an application such as			

		building services, power systems automation, water treatment and factory automation			
15	Internet of Things	1. Able to understand the application areas of IOT . 2. Able to realize the revolution of Internet in Mobile Devices, Cloud & Sensor Networks 3. Able to understand building blocks of Internet of Things and characteristics 4 .Able to design and program some IOT based devices and prototypes 5. Able Secure the elements of an IoT device 6. Able to design an IoT device to work with a Cloud Computing infrastructure. 7. To be familiar with the key wireless technologies used in IoT systems, such as WiFi, 6LoWPAN, bluetooth and ZigBee			
16	Low power networks	1. Become informed as to why			

		WSNs are underpinning the evolution to the Internet of Things. 2. Discover the challenges of providing connectivity to devices that are operating in highly variable and lossy RF environments. 3. Build a solid understanding of the wireless protocols that have been defined to support connectivity of low power devices. 4. Understand the different mechanisms important for enabling sensors and other low power devices to connect to the Internet. 5. Learn key routing protocols for sensor networks and main design issues. 6. Reveal what higher layer protocols are enabling applications and services to run over wireless Low Power Networks.			

		7. Understand the Sensor management, sensor network middleware, operating systems.			
17	Mobile Communication Networks	1. Understand the main principles of the different mobile communication systems, and track their evolution paths. 2. Develop a thorough knowledge of the system architecture for the traditional and the emerging cellular communication networks, and compare their architectures in terms of their components, interfaces, and interactions. 3. Evaluate the technical issues in the existing mobile communication networks including. coverage area, interference analysis, handoff strategies, channel assignment, trunking efficiency, security, and multiple access techniques. 4. Apply radio resources' management principles to evaluate the			

		capacity and the spectral efficiency of the existing cellular communication networks, and to design new systems. 5. Analyze and calculate the path loss, fading profiles, and effects of multi-path propagation in various cellular environments. 6. Understand the technical strategies in the design of LTE and discuss the technical features of the emerging cellular communication systems.			
18	Network Optimization	1. Apply the different optimization methods, a powerful tool for solving problems involving constrained optimization of time averages. 2. Understand the theory of dynamic decision making for networks and other stochastic systems. 3. Formulate the complex problems in the standard form of minimizing an objective subject to an additional set of			

		constraints. This includes linear and convex programs and their counterparts. 4. Implement the knowledge of the modern optimization algorithms for routing problems, shortest path, minimum-cost flow and maximum flow. 5. Explore hot-topic problems of opportunistic scheduling, approximate scheduling, dynamic data compression, efficient energy allocation. 6. Become skilled to apply the theory by formulating and solving their own problems that involve dynamic decisions and implement a research projects.			
19	Machine Learning	1. Demonstrate the main concepts of Machine Learning (ML) terms and algorithms (supervised, unsupervised and reinforcement learning). 2. Explore and recognize			

		various practical benefits of ML for real-world problems. 3. Identify the significant components in a production ML system. 4. Implement and apply algorithms of ML using appropriate programming languages, libraries, and frameworks. 5. Evaluate correctness and performance of ML model. 6. Develop ML models for solving real-world problems in various domains such as healthcare, marketing, transportation, social media, etc.			