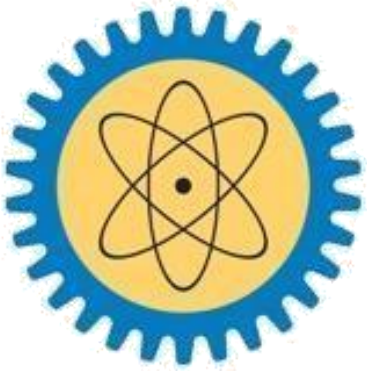

BUSITEMA UNIVERSITY

*Pursuing Excellence*

## FACULTY OF ENGINEERING AND TECHNOLOGY

## DEPARTMENT OF COMPUTER ENGINEERING AND INFORMATICS

# Proposed Master of Science in Cyber Physical Systems Engineering

**October 2023**

# TABLE OF CONTENTS


1.0 BACKGROUND ..... 4
1.2. Justification Of the Master Science in Cyber Physical Systems Engineering Programme ..... 6
1.3. Title ..... 7
1.4. Programme Objectives And Outcomes ..... 7
1.5. Learning Outcomes Of The Programme ..... 7
1.6. Opportunities For The Graduates. ..... 7
2.0 RESOURCES ..... 8
2.1 Human Resource ..... 8
2.2. Technical And Infrastructure Facilities ..... 8
2.3. Programme Funding ..... 9
3.0 PROGRAMME REGULATIONS ..... 10
3.1. Programme Duration ..... 10
3.2. Admission Requirements ..... 10
3.3. Target Group ..... 10
3.4. Aspects On Gender And Equity ..... 11
4.0 EXAMINATION REGULATIONS ..... 11
4.1. General Regulations ..... 11
4.2. Method Of Assessment ..... 11
4.3. Grading Of Courses ..... 11
4.4. Calculation Of Cumulative Grade Point Average (Cgpa) ..... 12
4.5. Course Retaking ..... 12
4.6. Academic Progress ..... 13
4.7. Dissertation ..... 13
4.8. Requirements For The Award Of The Degree ..... 13
4.9. Classification Of The Award ..... 14
4.10. Quality Assurance ..... 14
5.0. PROGRAM STRUCTURE ..... 14
5.1. Programme Courses ..... 14
5.2 Syllabus ..... 15
5.3. Skills Courses ..... 15
6.0. PROGRAMME STRUCTURE AND DETAILED COURSE CONTENT ..... 16
6.1. Program Structure ..... 16
**6.2 DETAILED COURSE DESCRIPTION YEAR 1: SEMESTER** I ..... 17
6.2.1 CPS81101 Modelling of CPS ..... 17
6.2.2 CPS81102: Network Security ..... 19
6.2.3 CPS81103 Internet of Things ..... 21
6.2.4 CPS81104 Real Time Operating System ..... 23

6.2.5 CPS 81105: Privacy in the Digital Age....25
6.2.6 CPS81106 Cloud Technologies and Architectures....28
6.3 DETAILED COURSE DESCRIPTION YEAR 1: SEMESTER 2....30
6.3.1 CPS 81201 Embedded System design....30
6.3.2 CPS81202 Cryptographic And Communication Security....33
6.3.3 CPS 81203 Business process modelling and analysis....35
6.3.4 CPS81204 Research Methods....37
6.3.5 CPS81205 Networked and Distributed Control Systems....39
6.3.8 CPS81208 Smart Grids:....41
6.4. DETAILED COURSE DESCRIPTION YEAR 2: SEMESTER 1....44
6.4.2 CPS82102: Seminar Series....44
6.4.3 CPS82103 Scholarly Writing....45
APPENDIX A: PROGRAMME FUNDING....46
APPENDIX C: HUMAN RESOURCES....47

## 1.0 BACKGROUND OF THE UNIVERSITY

Busitema University (BU) is a multi-campus model public University located in the Eastern region of Uganda established under the Universities and other Tertiary Institutions Act, 2001. The establishment of Busitema University was enacted by Parliament on the 10th of May, 2007 as provided by Instrument 2007 No. 22 made on 25th of May, 2007. The main campus (headquarters) is located at Busitema along the Jinja-Tororo highway about 225km away from Kampala capital. The other campuses are situated at Nagongera, Namasagali, Arapai, Mbale, Pallisa and Kaliro. The University focuses on relevant and critical study programs in Engineering, Science Education, Health Sciences, Natural Resources and Environmental Sciences, Agriculture and Animal Sciences, Management Sciences and Vocational Education. From its establishment, it was dedicated to improving equitable access to University Education in the region with a population of approximately ten million people but without any public university by then. The Faculty of Health Sciences is strategically located in Mbale city within the Mbale Regional Referral Hospital complex that serves a wide catchment population in Eastern Uganda.

**Mandate of the University:** To provide higher education through teaching, research and community outreach.

**Vision**: "A Centre of academic and professiona Innovation".

**Mission**: "To provide inclusive high standard t industrialization and sustainable development".

**Philosophy:** To foster socioeconomic transformation of communities through research and innovation

**Motto:** Pursuing excellence

**Core values:** The core values of Busitema University are:
a) Respect

b) Professionalism

c) Customer first

d) Innovativeness

e) Integrity

f) Excellence

### 1.1 PROGRAMME BACKGROUND

The computing disciplines is trending toward integrated sensing, control of networked physical objects and infrastructure, and connecting them to the Internet and to each other. As the amount of information, critical services, and interconnected computers and 'things' in the cooperate and cyberspace is steadily increasing the complexity, the number, sophistication, and impact of malpractices are becoming more and more significant. In the last decades, governmental and non-governmental organisations have become aware of this problem. However, the existing computer

workforce has not been sufficient for satisfying the increasing demand for qualified computer professionals in the emerging computer disciplines, and the shortfall will increase in the next years. Meanwhile, to address the increasing demand for cybernetic data management and cybersecurity professionals, academic institutions have been establishing various computer disciplines particularly, master in computer science programs, masters in Artificial Intelligence and related fields in computing.

The need for computer professionals appeared in the early years of the digital era, when the first mainframe computers were developed. As networked computers and systems have progressively come to dominate computing and communication platforms, the volume and severity of cybercrimes have increased to an extent that Cyber Physical Systems and Internet of Things is now an underpinning area of computer systems. Owing to the huge impact cybercrime has in the economy and safety of organisations and countries, the importance of Cyber Physical Systems has grown to such a level that it is now considered key innovative and protective discipline.

The use of computational resources to achieve different capabilities is in existence for several decades. However, many modern systems have high degree of complexities and also the scale of these systems is large and/or has distributed nature. For example traffic control system in a city requires modelling of traffic flows in different areas and optimizing different performance objectives by appropriately taking routing decisions, and decisions about actuating different signals for smooth traffic flow; this is a large scale distributed system. There are several other domains where CPS examples can be seen e.g. Healthcare, Robotics, Automotive, Power Grid, Avionics and Transportation. Such system necessitates a deeper understanding of system behaviour and also provides feedback to augment system design to achieve overall objectives from the system. Emergence of ubiquitous computing and communication has open enormous opportunities to provide new capabilities to systems e.g. robotics assisted remote surgery.

Many (small) systems can work in collaborative/cooperative manner to achieve a larger overall objective. The examples can be seen in robotics and modern warfare where collaboration/cooperation achieves larger objectives. The communication capability also provides a possibility of distributed learning for systems. Hybrid system modelling is one of the possible approaches to model CPS. Hybrid system approach allows inclusion of both continuous time and discrete time states (variables) in the model.

The seamless integration of cyber system with physical system also poses several challenges towards system security against possible system attacks. With modelling of physical system, it is necessary to model different possible attacks and to provide adequate security at hardware and software to ensure overall system security in all scenarios.

The cyber component includes hardware and associated software. The design of cyber component also requires software level abstraction to have system level model of cyber component. This also allows designing a very high reliability system as the model allows a predictable behaviour.

Conventionally software is developed without formal models and largely depends on programmer experience and knowledge; however, requirement of safety, reliability in CPS demand higher level

of abstractions at software level as well. This allows the system remains correct and secure by design.

The university vision is to be “a center of technology and innovation” whereas the mission is “to p quality research and outreach for industrial program is in line with the vision and mission as well as the University Strategic Plan (2020/21 –

2024/25) under objective 2: Increasing High Impact Research, Innovation and Entrepreneurship, the university will “increase the number of gradu quality.”

### 1.2. Justification Of the Master Science in Cyber Physical Systems Engineering Programme

Historically, the computing field has grown steadily with the advent of new technologies for business, governments and personal use.

Currently, there is a growing concern among governments that the cyberspace will become the next theatre of warfare. Despite the disparate increasing prominence of the discipline, the existing computer scientist and or cybersecurity workforce cannot satisfy the increasing demand for qualified computer professionals. While the number and sophistication of computer systems increase, the shortfall is expected to worsen in the next years 'the demand for the (computers scientist) workforce is expected to rise to 6 million (globally) by 2019, with a projected shortfall of 1.5 million' stated Michael Brown, (former) CEO of Symantec (Setalvad 2015; Cisco 2015; Frank 2016; Randstad Technologies 2016), already there is a shortfall. Aware of this problem, several academic institutions worldwide have defined and offer computer Science programs to address the shortage of cyberspace professionals. In particular, ACM has under taken special initiatives to develop educational guidelines to the development of computer Science programs on the post-secondary level.

Advances in CPS will enable capability, adaptability, scalability, resiliency, safety, security, and usability that will expand the horizons of these critical systems. CPS technologies are transforming the way people interact with engineered systems, just as the Internet has transformed the way people interact with information. New, smart CPS drive innovation and competition in a range of application domains including aeronautics, building design, energy, electrical power grids, healthcare, manufacturing, and transportation,

This innovative, multidisciplinary program is designed to meet the demand for a new kind of specialist: one who can engineer new interactive services, acquire, fuse, and process the data collected from sensors, actuators, controllers, and other devices, and develop architectures to interconnect these elements as part of larger, more diverse systems.

The introduction of a Masters programme in Cyber Physical Systems Engineering at Busitema University will provide opportunities for talented Ugandans to get the necessary leadership empowerment, academic and professional confidence to spearhead the much-needed innovations

and research to the country’s and the Regions as increasing the number of skilled human resources that is critically lacking in tertiary institutions.

Currently there is no University in the Uganda that is offering this unique and emerging field of research, Busitema University is better placed to tap into this opportunity

### 1.3. Title

The title of the programme**MasterofScience**is:**inCyber**" **Physical Systems Engineering"**

### 1.4. Programme Objectives and Outcomes

#### 1.4.1. Overall Objective

The program aims to produce competent engineers who can design, monitor and manage systems that are built from seamless integration of physical system and cyber systems.

#### 1.4.2. Specific Objectives

The objectives of the program are

1. To Impart an in-depth knowledge of the theoretical and practical aspects of designing systems that are built from seamless integration of physical system and cyber systems.
2. To develop skills and competency required to manage modern Physical cyber systems.
3. To imparts knowledge of several tools for modelling physical systems and tools for designing cyber components.
4. To develop research skills which will help students grow with the technological advancements and engage in the design and development of new technologies

### 1.5. Learning Outcomes of the Programme

On graduation, learner will be able:

1. To analyse overall specifications of CPS and translate it to the different sub-systems design requirements.
2. Demonstrate Adequate competency to model overall CPS using Hybrid system and other approaches and validate the model.
3. Demonstrate the capability to co-design hardware-software architecture in distributed environment.
4. Apply knowledge of Machine Learning algorithms and Distributed Control algorithms.
5. Develop methods to embedded security in overall design of CPS.
6. Manage applications like smart grid, mobile networks and different systems of smart city.

### 1.6. Opportunities for The Graduates.

The emerging of the fourth industrial revolution. Artificial intelligence, machine learning and cyber physical systems are all changing how we live and work. With the skills gained from this programme, learners will be able to develop the technology of the future. Careers could be in;

- Cyber security

ii Financial technology
iii Networked systems
iv Robotics and autonomous systems
v Smart product and service design and development
vi Artificial intelligence engineering

Graduates of the programme will find employment in organizations such as:

a) Telecommunication service industry, such as MTN, Artel, UCC and other.

b) Communication control systems, such as Civil Aviation,

c) Tel medics, Automated production lines and others

d) Management and Leadership positions.

e) Banks and other financial institutions

f) Energy technological industries.

g) Defense and Police forces as signalers and image interpreters.

## 2.0 RESOURCES

### 2.1 Human Resource

Busitema University Faculty of Engineering already has qualified staff with PhDs in Computer Science, Mathematical Engineering, Information Security and other relevant areas. Relevant qualified staff are also available in sister faculties such as the Faculty of Science and Education, Faculty of Health Sciences, Faculty of Management Sciences. The above staff will offer fulltime teaching and research services of the programme. **See Appendix C**.

### 2.1.1 Academic staff

The BCT department has got a pool of qualified and competent academic staff who facilitate the running of the BCT programme. The list of staff is shown in **appendix C**

### 2.2. Technical And Infrastructure Facilities

### 2.2.1 Academic Equipment

Busitema University has 4 computer laboratories with 80 state of the art computers. In addition each student is encouraged to own a laptop with the reduced cost of computers.

### 2.2.2 Reference Materials

The BCT department has got a number of electronic books which the lecturers use for preparing lectures. The library in collaboration with the BCT department has acquired a good number of

recently published books in computing fields. Busitema University library is stocked with up-to-date information resources. The information resources in the University Library are usable and accessible by both students and lecturers. the University Library has ample space for graduate students and provides access to print books, print journals, electronic journal databases, a well-stocked reference section and connections to many online databases like the Uganda Scholarly Digital Library. The print collection is beefed up by the broad variety of electronic resources provided by the University Library and accessible online at http://busitema.lib.ac.ug. Through the document delivery service, users who fail to get access to full-text articles from the available databases can make requests for articles, which are delivered, to them at no cost. Library users can also access the Online Public Access Catalogue (OPAC) to get bibliographic information about the collections found in the College Library. Below is a list of all electronic databases that Busitema University subscribes to;

i Institute of Electrical and Electronic Engineers (IEEE)
ii Springer Verlag
iii E-library (eBook database)
iv Science Direct
v Association of Computing Machinery (ACM) Digital Library
***See appendix B***

### 2.2.3 E-Learning Platforms

Busitema University has an eLearning platform known as BUOLE ( https://lms.busitema.ac.ug and it is expected that courses will be developed as interactive online modules on Buele. Students in the Department of Computer Engineering and Informatics have adequate access to computers. Each student at postgraduate level is expected to have a personal computer. This creates a good environment for e-learning blended teaching. All courses in the new curriculum will be taught in a blended way. All course materials will be put on Buele. Staff will, as much as possible, make use of e-learning facilities like discussion forum and drop boxes for assignments. This will increase student activity/participation and reduce staff effort (e.g. staff will not need to dictate notes). This in turn will increase the material covered and taken in by the students. **(see appendix B)**

### 2.2.4 Physical facilities

These include lecture rooms and computer labs. The University has 4 computer labs and sufficient lecture rooms. The Department of Computer and Informatics is housed in the Faculty of Engineering and Technology with a block constructed by IDB. The block mainly accommodates offices for administration and teaching staff, conferencing facility, two teaching labs, 8 lecture rooms a conference hall and specialized laboratories i.e. communication lab and Electronic lab. The block sufficiently caters for all the lecture and laboratory space requirements at the faculty.

### 2.2.4 Financial resources

The Department of BCT Budget is mainly supported by the main university finance pool, whose major income source is the Government.

## 2.3. Programme Funding

The main source of funding for the programme shall be through tuition fees (self or private institutional student sponsorships). See Appendix A. Various resources shall also be generated by faculty staff under the programme through bankable research and outreach projects, consultancies 9

and donor support, some of which resources will be used to strengthen programme facilities and activities.

## 3.0 PROGRAMME REGULATIONS

### 3.1. Programme Duration

The Master of Science in Cyber(four - Physicalsemester)programme Systemby Taught Courses and Dissertation. During the training:

i A student must complete an approved program of courses totaling to 36 Credit Units in year one and 18 Credit Units in year two of the programme.

ii A student must submit a Dissertation on an approved topic that carries a minimum of 7 Credit Units in year two. Joint internal and external examination of the Dissertation is mandatory.

iii The Minimum Graduation load for the programme is therefore 54 CUs.

### 3.2. Admission Requirements

To be eligible to apply for the Master of Science in Cyber Physical Systemsthe candidate must hold any of the following:

1. A Bachelor'sComputerdegreeScienceofsecondin-class lower division and above from a recognized university.
2. A Bachelor's degree in Computer-classlowerdivision Engineeriandabove from a recognized university.
3. A Bachelor's degree -inclass lowerDatadivisionScienceandabovefrom a of s recognized university.
4. A Bachelor's degree in -classSoftwarelowerdivisionandengineerinabovefrom a recognized university.
5. lower division and above in the Software Engineering or Computer Engineering
6. A Bachelor'ssecond-classdegreelowerdivisionofand above in Information Technology with a principal pass in Mathematics or Physic at A-Level or its equivalent.

### 3.3. Target Group

The programme is designed for graduates from computing (Computer Science, Computer Engineering, data Science, Artificial Intelligence and Software Engineering) and closely related fields, who wish to gain advanced specialized knowledge in Cyber Computing. The broad target groups include but not limited to:

1. those interested in pursuing both academic and professional careers requiring advanced Specialized knowledge in Cyber System and IoT.
2. professionals interested pursuing careers in the fields of Cyber Technology, IoT, network security, Application of AI, and cloud computing, among others.

#### 3.3.1. Projected Student numbers

It is proposed that the programme starts with 15 students in 2024/25 academic year and the number shall be increased gradually to 15 students per intake over a period of 3 years as shown in Table 1.

The increase in student number will take into account both infrastructures, human and financial resource capacity to handle the programme. Table 1: Projected student numbers

| **ACADEMIC YEAR** | **2024/25** | **2025/26** | **2026/27** | **2027/28** |
|---|---|---|---|---|
| **Student Number Admitted** | 15 | 15 | 15 | 15 |
| **Cumulative student numbers** | 15 | 30 | 30 | 30 |

### 3.4. Aspects On Gender And Equity

Uganda is actively promoting gender-conditionandfor equ sustainable development, Busitema University has a strong affirmative policy. The current female enrollment at graduate level at the Faculty of Engineering is about 10% compared to about 30% and increasing at undergraduate levels.

The programme will specifically target female candidates with a view to increasing the percentage to 25%.

## 4.0 EXAMINATION REGULATIONS

### 4.1. General Regulations

The general Master's degree regulations of Studies Handbook shall apply.

### 4.2. Method Of Assessment

Assessment will be done through coursework which will include home assignments, class room and take-home tests, project work and presentations and written examination. Course work will carry a total of 40% and written examination carries 60%. The overall pass mark is 60%.

### 4.3. Grading Of Courses

Each course shall be graded out of a maximum of 100% marks and assigned an appropriate letter grade as shown below: To record a pass mark in a course unit, a student must achieve a minimum mark of 60%. The student must also have attended at least 70% of all scheduled classes and practicals and presentations.

| Marks % Point | | | |
|---|---|---|---|
| 80-100 | A | 5.0 | Excellent |
| **75-79** | B+ | 4.5 | Very good |
| **70-74** | B | 4.0 | Good |

| | | | |
|---|---|---|---|
| **65-69** | C+ | 3.5 | Fairly good |
| 60-64 | C | 3.0 | Satisfactory |
| **0-59** | D | 0.0-2.5 | Fail |

### 4.4. Calculation Of Cumulative Grade Point Average (Cgpa)

The programme shall be conducted on the credit unit basis. One credit unit shall be equivalent to one contact hour per week per semester or a series of 15 contact hours. And one contact hour shall be equivalent to one hour of lecture/ tutorial or two hours of laboratory/ practical work.

The Grade Point Average (GPA) shall be calculated using the following formula:

$$GPA = \frac{\sum_{i=1}^{n} (PG_i \times CU_i)}{\sum_{i=1}^{n} CU_i}$$

Where $PG_i$ is the Grade Point score in course $i$; $CU_i$ is the number of Credit Units of course $i$; and $n$ is the number of courses taken in that semester or recess term. CGPA is calculated using a formula similar to the one above, but $n$ is the number of course taken from the beginning of the program up to the time when the CGPA is being calculated.

### 4.5. Course Retaking

i A student shall retake a Course or Courses when next offered again in order to obtain at least the Pass Mark (60%) if he/she had failed during the first assessment in the course or courses.

ii A student who has not done course work will not be allowed to sit for final examinations

iii A student who has failed to obtain at least the Pass Mark (60%) during the Second Assessment in the same Course or Courses retaken shall receive a warning.

iv A student may retake a Course or Courses when next offered again in order to improve his/her Pass Grade(s) if the Pass Grade(s) got at the first Assessment in the Course or Courses were low. A student who fails to attain higher marks after retaking to improve, the examination results of the first sitting are recorded on the transcript and shall not be recorded as Retake.

v Where a student misses to sit examinations for justified reasons, his/her results shall be not recorded as Retake when the examination(s) is/are next offered.

vi Attend all the prescribed lectures/ tutorials/ practicals/fieldwork in the Course or

vii Courses;

viii Satisfy all the requirements for the course-work component in the Course or Courses;

ix Shall sit for the University Examinations in the course or courses.

x A student shall who accumulates more than four (4) Retake Courses will be requested to stay put.

xi Students are required to register for retake course(s) first before registering for new courses offered in that semester and the retake courses should fit into the approved normal load so as to avoid timetable clashes.

xii A final year student whose final Examination Results have already been approved by the Graduate Board and has qualified for the Award of the MSc. in Materials Engineering Degree, shall not be permitted to retake any Course(s).

xiii When a student has retaken a course the better of the two Grades he/she has obtained in that course shall be used in the computation of his/her cumulative Grade Average (CGPA).

xiv Whenever a course or courses has/have been retaken, the Academic Transcript shall accordingly indicate so.

xv Students shall pay for retake(s) registered for.

### 4.6. Academic Progress

At the end of every semester, students' pro
Progress, Probationary Progress, and Discontinuation.

#### 4.6.1. Normal progress

This occurs when a student has passed (Grade point of 3.0) all the courses that he/she has taken so far, since the beginning of the program.

#### 4.6.2 Probationary Progress

A student who has obtained the Grade Point (GP) of less than 3.0 shall be placed on probation. Such a student shall be allowed to progress to the next semester/academic year but shall still retake the course(s) he/she has failed the assessments in later on and obtained at least the pass mark (60%) in the course(s).

#### 4.6.3 Discontinuation

When a student accumulates three consecutive probations based on CGPA he/she shall be discontinued.

i A student who fails to obtain at least the Pass Mark (60%) during the Third Assessment in the same course or courses retaken shall be discontinued from his/her studies at the University.

ii A student who has overstayed on the programme by more than five (5) years shall be discontinued from his/her studies at the University.

### 4.7. Dissertation

Students are required to demonstrate their ability to independently undertake research and analysis. Each student will be required to pursue and complete the dissertation. To pass the dissertation, the candidate shall satisfy the supervisor(s), reviewers and examiners in the written report and in project presentation(s).

### 4.8. Requirements For The Award Of The Degree

The degree of Master of Engineering in Cyber Physical Systems Engineering shall be awarded to a candidate who obtains 51 credit units, gained from 12 courses. Furthermore, the student will have to pass all the courses in a period stipulated by the University Senate and Council.

### 4.9. Classification Of The Award

The degree of Master of Science in Cyber Physical Systems Engineering shall be awarded to a student who fulfills all the requirements for the programme. The Master degree shall not be classified.

### 4.10. Quality Assurance

The quality assurance practices like the other programmes in the Faculty of Engineering in particular, and Busitema University in general shall apply. A student will be required to attend at least 70% of the lectures given in a course, do and pass all the coursework assignments, tests and laboratory exercises before he/she can sit for a written examination. Performance of each of the lecturers assigned to teach the students shall also be closely monitored to ensure they comply with the curriculum requirements. This will be partly achieved through giving the students assessment forms to assess their teaching staff on the content taught, mode of delivery, self-explanation; appearing for lectures, tutorials and at practical field study trips sessions.

The Department management makes at least one meeting with every class every semester. In this meeting, general quality issues are addressed. Students are also given a chance to raise any questions that are answered and/or addressed by the Department management.

As a practice at Busitema University, student results are reviewed every semester by a senior external academician. This is to bring a 'foreign view' of the examiners write reports on their view of the curriculum/examinations. Some recommendations can be implemented immediately while others have to be implemented in a longer term. The department will make the maximum possible use of external examiners' reports as a m in the revised program.

## 5.0. PROGRAM STRUCTURE

The Master of Science in Cyber Physical Systems Engineering curriculum offers rigorous technical courses in both fundamental and advanced, emerging areas of Cyber Physical Systems. the academic coursework will give learners formal training in engineering software, systems, platforms, products for complex business challenges and Data Analytics, they will work on the design, control and optimization of cyber-physical systems, through a combination of core and elective courses, and project work. The program involves both theory and practice and welcomes students with diverse interests in control theory, wireless communication, data analysis, IoT design, implementation and management

.

### 5.1. Programme Courses

The programme explores both the principles of Cyber Physical Systems and the many ways these principles are applied to various roles in the Cyber Physical Systems Engineering discipline. the MCPSE curriculum offers three breadth areas that enable students to gain a wider range of specialized skills, thus preparing them to work in many roles. The courses are covered from three

knowledge area regarded as breadth areas. These breadth areas include: Cloud Computing, Theory and Security, Artificial Intelligence and IoT.

### 5.2 Syllabus

Table 2: Syllabus breakup

| **Domain** | **Allied Courses** | **Credit Unit [Hrs]** | **Percentage [%]** |
|---|---|---|---|
| Cloud Computing for the CPS | 1. Modelling of CPS<br>2. Embedded System design<br>3. Real time operating system<br>4. Networked and distributed Control system<br>5. Digital Signal Processing | 15 | 23 |
| Theory and Security | 1. Privacy in the digital Age<br>2. Network security<br>3. Cryptography and communication Security<br>4. Cloud Technologies and Architecture | 12 | 19 |
| Artificial Intelligence and IoT | 1. Business process modeling and analysis<br>2. Learning decision making<br>3. Embedded and IoT systems<br>4. Security and Privacy<br>5. Design and Analysis of CPS<br>6. Smart grid | 18 | 27 |
| General Research Courses | 1. Research Methods<br>2. Seminar series<br>3. Scholarly Writing | 3<br>3<br>3 | |
| MSc Dissertation | 1. Proposal<br>2. Dissertation | 5<br>7 | 31 |
| Total | | 66 | 100 |

### 5.3. Skills Courses

Table 3: Hands on Skills courses in the programme.

| **Domain** | | **Allied Course Unit** |
|---|---|---|
| 1 | Cloud Computing for the CPS | 1. Modelling of CPS<br>2. Embedded System design<br>3. Digital Signal Processing |
| 2 | Theory and Security | 1. Network security<br>2. Cryptography and communication Security |
| 3 | Artificial Intelligence and IoT | 1. Business Process modeling and Analysis<br>2. Embedded and IoT systems<br>3. Design and Analysis of CPS |

## 6.0. PROGRAMME STRUCTURE AND DETAILED COURSE CONTENT

### 6.1. Program Structure

The MCPS. programme just like the other programmes in Busitema will be run on semester system. The Tables below outline the courses and their loading to be offered in the programme.

**Table 3: First Year Courses**

| Semester | Course Code | Course Name | LH | TH | PH | CH | CU |
|---|---|---|---|---|---|---|---|
| **ONE** | CPS81101 | Modelling of CPS | 30 | 0 | 45 | 45 | 3 |
| | CPS81102 | Network security | 30 | 30 | 0 | 45 | 3 |
| | CPS81103 | Internet of things | 30 | 30 | 0 | 45 | 3 |
| | CPS 81104 | Real time operating system | 30 | 0 | 45 | 45 | 3 |
| | CPS 81105 | Privacy in the digital Age | 30 | 0 | 45 | 60 | 3 |
| | CPS81106 | Cloud Technologies and Architecture | 30 | 30 | 0 | 45 | 3 |
| | Sub-Total | | | | | | 18 |
| | | | | | | | |
| **TWO** | CPS81201 | Embedded System design | 30 | 0 | 45 | 45 | 3 |
| | CPS81202 | Cryptography and communication Security | 30 | 0 | 45 | 45 | 3 |
| | CPS81203 | Business process modeling and analysis | 30 | 30 | 0 | 45 | 3 |
| | CPS81204 | Research Methods | 30 | 30 | 0 | 45 | 3 |
| | | | | | | | |
| | | **Electives* (SELECT two)** | 30 | 30 | 0 | 45 | 3 |
| | CPS81205 | Networked and distributed Control system | 30 | 30 | 0 | 45 | 3 |
| | CPS81206 | Embedded and IoT systems | 30 | 30 | 0 | 45 | 3 |
| | CPS81207 | Design and Analysis of CPS | 30 | 30 | 0 | 45 | 3 |
| | CPS81208 | Smart grid | 30 | 30 | 0 | 45 | 3 |
| | CPS81209 | Digital Signal Processing | 30 | 30 | 0 | 45 | 3 |
| | CPS81210 | Learning decision making | 30 | 30 | 0 | 45 | 3 |
| | Sub-Total | | | | | | 18 |
| | **Grand** | | | | | | **36** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Total** | | | | | | |

**Table 4: Second Year Courses**

| **Semester** | **Course Code** | **Course Name** | **LH** | **TH** | **PH** | **CH** | **CU** |
|---|---|---|---|---|---|---|---|
| | CPS82101 | Dissertation Proposal | 0 | 0 | 315 | 105 | 5 |
| | CPS82102 | Seminar Series | 45 | 0 | 0 | 45 | 3 |
| | CPS81205 | Scholarly Writing | 0 | 0 | 135 | 45 | 3 |
| | Sub-Total | | | | | | **11** |
| | | | | | | | |
| **TWO** | CPS82201 | MSc. Dissertation | 0 | 0 | 315 | 105 | 7 |
| | Sub-Total | | | | | | **`7** |
| | **Grand Total** | | | | | | **54** |

### *6.2 DETAILED COURSE DESCRIPTION YEAR 1: SEMESTER I*

#### 6.2.1 CPS81101 Modelling of CPS Course description

This course develops a solid basis for students to model and simulate cyber-physical systems using computer-based object-oriented equation-based modeling languages and tools with the goal of building models with high reusability. It presents theories, design methods, and tools that help handle the growing complexity and heterogeneity of embedded and cyber physical systems, by offering a new vista on system design, where correct-by-construction abstraction, refinement, and composition techniques are pursued to substantially reduce design time and errors. Methodologies and tools will be illustrated on several applications, including robotic motion planning, car electronics, building automation, and electrical power systems control. During the lab sessions, the students will work on specific design cases using both industrial-strength and research-oriented software platforms.

**Learning objectives:**

1. To develop a toolset of theory, methods, computer languages and software tools for modeling and simulating cyber-physical systems.
2. To develop skills, of modelling, designing, simulating and analyzing dynamic characteristics of cyber-physical systems.

**Learning Outcomes**

1. Comprehend the fundamental principles of modeling and simulation of continuous, discrete, hybrid and timed-clocked systems that lead to the formulation of cyber-physical system models.
2. Comprehend and apply computer-and-equation based object-oriented languages for modeling of cyber-physical systems using the any Modeling language eg MatLab, Modelica or any other.
3. Comprehend and explain methods used for symbolic transformation of computer models, efficiency issues in numerical solutions and effect of nonlinearities, higher-and-varying index problems, initialization methods, event handling, and other numerical issues related to mathematical solvers used for simulation and co-simulation.
4. Construct simulation models for cyber-physical systems using the Modelica language in Modelica Environments such as Dymola and OpenModelica.
5. Comprehend and explain the concept of real-time simulation, and hardware-in-the-loop simulation.
6. Comprehend concepts of embedded systems, and apply solutions for real-time simulation with an embedded system in-the-loop.

**Course Contents / Topics**

**Introduction:** Cyber-Physical Systems (CPS); CPS Design Challenges; Model-Based Design and Design Methodologies; Simulation, Validation, Verification, and Synthesis; Platform-Based Design and Contract-Based Design.

**Modeling:** Introduction to Models of Computation; Languages and Tools for System Design; Mathematical Background; Notions of Complexity and Computability. - Week 3. Concurrent Models of Computation: Finite State Machines; Synchronous/Reactive Model.

**Concurrent Models of Computation**: Process Networks; Dataflow; Petri Nets, Timed Models; Discrete-Events (DE) Model, Continuous-Time Model; Acausal Model; Mixed Models; Hybrid Systems.

**Interfaces for System Design:** Types; Ontologies; Behavioral Types; Interfaces and System Specification; Interfaces and Compositional Methods; Assume-Guarantee Reasoning, Contracts; Contract Operations and Relations; Compatibility, Consistency, Composition, Refinement.

**Analysis**: Cyber-Physical System Requirements (Functional, Extra-functional, Safety, Liveness, Reliability, Real-Time); Specification Languages; Temporal Logic; Overview of Requirement Analysis and Validation Techniques. Core Engines for Algorithmic System Verification; Satisfiability (SAT) Solving; Satisfiability Modulo Theories (SMT) Solving; Optimization; Reachability Analysis and Model Checking. Project Midterm Review.

**Design Space Exploration and Synthesis:** Cyber-Physical Systems Architectures; Mapping and Synthesis; Architecture Exploration; Optimization-Based and Simulation-Based Techniques for Mapping and Synthesis, Verification and Synthesis of Controllers; Algorithmic Synthesis Techniques; Optimization-Based Controller Design, Fundamentals of Real-Time Operating Systems and Scheduling.

**Applications:** Modeling and Design of Power Distribution Networks; Modeling and Design of Building Automation and Control Systems. Advanced Topics (based on available time and student interest): Security and Privacy; Stochastic Systems; Machine Learning and System Design.

**Mode of Delivery**

i Lectures: Lectures will be conducted and students will be taken through the theoretical and practical aspects of the course.
ii Student projects: Students will be given projects at the start of the course and these will be continuous projects building on the techniques taught in class. At the end of the course, students will complete projects.

**Mode of Assessment**

i Progressive assessment (40%). This will consist of theory and practical assignments (projects).
ii Final exam (60%). Part of the final exam may be a project

**References**


1. E. A. Lee and S. A. Seshia, "Introduction-PhysicalSystems Approach," Second Ed., http://LeeSeshia.or
2. R. Alur, "Principles-Physicalof SCystems,"ber MIT Press,
3. Francois E. Cellier and Ernesto Kofman,-Verlag "C New York, Inc. Secaucus, NJ, USA, 2006. ISBN:0387261028
4. P. Fritzson, Principles of Object-Oriented Modeling and Simulation with Modelica 3.3: A Cyber Physical Approach. Wiley-IEEE Press, 2014. ISBN: 978-1-118-85912-4.
5. Michael M. Tiller, Modelica by Example. E-book. On-line: http://book.xogeny.com
6. Dymola, FMI Toolbox and Papyrus-RT User Manuals (Digital version with the software)


### 6.2.2 CPS81102: Network Security

**Course Description**

In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed no time at which security does not matter. Two trends have come together to make the topics of this course of vital interest. First, the explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This, in turn, has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Second, the disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security. This course introduces a concise survey of the cryptographic algorithms and protocols underlying network security applications, including encryption, hash functions, digital signatures, and key exchange. It also Covers important network security tools and applications, including Kerberos, X.509v3 certificates, PGP, S/MIME, IP Security, SSL/TLS, SET, and SNMPv3 and Finally the course looks at system-level security issues, including the threat of and countermeasures for intruders and viruses and the use of firewalls and trusted systems.

**Course Objectives**

The objectives of the course are

1. To equip the student with the principles of security specifically in networks
2. To equip students with approached of compromising networks
3. To equip students with techniques of mitigating network attacks

**Learning Outcomes**

Upon completion of this course, the student shall:

1. Have an understanding of network security protocols and applications;
2. Have an understanding of threat models, attacks that compromise security, and techniques for achieving security;
3. Be able to provide security assessment of networks;
4. Have ability to use the basic concepts of secure communication via insecure networks to design secure architectures;
5. Describe and justify relevant alternatives and decision recommendations;
6. Implement security management in networks.

**Detailed Course Content**

Teaching of this course will done in modules. Each module will be a complete unit of teaching and will be assessed independently during continuous assessments. The content of the modules will include:

(i) *Introduction (5 hours)*

Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security.

(ii) *Symmetric Encryption and Message Confidentiality (5 hours)*

Symmetric Encryption Principles, Symmetric Block Encryption Algorithms, Random and Pseudorandom Numbers Stream Ciphers and RC4, Cipher Block Modes of Operation

(iii) *Public-Key Cryptography and Message Authentication (5 hours)*

Approaches to Message Authentication, Secure Hash Functions, Message Authentication Codes, Public-Key Cryptography Principles, Public-Key Cryptography Algorithms. Digital Signatures,

(iv) *Key Distribution and User Authentication (5 hours)*

Symmetric Key Distribution Using Symmetric Encryption, Kerberos Key Distribution Using Asymmetric Encryption, X.509 Certificates, Public-Key Infrastructure, Federated Identity Management,

(v) *Transport-Level Security (5 hours)*

Web Security Considerations, Secure Socket Layer and Transport Layer Security Transport Layer Security HTTPS Secure Shell (SSH)

(vi) *Wireless Network Security (5 hours)*

IEEE 802.11 Wireless LAN Overview, IEEE 802.11i Wireless LAN Security, Wireless Application Protocol Overview, Wireless Transport Layer Security, WAP End-to-End Security

(vii) *Electronic Mail Security (5 hours)*

Pretty Good Privacy, S/MIME, Domain Keys Identified Mail

(viii) *IP Security (5 hours)*

IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange, Cryptographic Suites

(ix) *Intruders (5 hours)*

Intrusion Detection, Password Management, Malicious Software, Types of Malicious Software, Viruses, Virus Countermeasures, Worms, Distributed Denial of Service Attacks

**Study Materials**

Materials shall include textbooks, Journal/conference papers and simulators

**Mode of Study**

Teaching delivery shall be based on conventional in-class interaction between lecturers and students. The teaching shall follow the content of the suggested text book in addition to other teaching materials such as papers where possible. Students are expected to learn through lectures and different assessment exercises which shall include quizzes, research coursework, and project. Research course work will be based on identifying a security problem that a student or a group of students will independently research on and present at the class. A project on the other hand may require some programming skills where students to implement various security mechanisms such as firewalls in real systems.

**Mode of Assessment**

Assessment shall be by course work - that will largely constitute take home research assignments (40%) and final examination (60%). Part of the final exam may be a practical project.

**Reading List**


1. Fundamentals of Network Security by J. Canavan; Artech House (2013)
2. Network Security Essentials: Applications and Standards 4$^{th}$ Edition, By William Stallings (2011)
3. Eric Rescorla, SSL and TLS: Designing and Building Secure Systems, Addison Wesley Professional 2000 [4] Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, John Wiley & Sons 1995


### 6.2.3 CPS81103 Internet of Things

**a. Course Description**

This course covers the applications of the Internet of Things (IoT) and their relevance to developing countries, with a focus on low-cost, open and sustainable solutions as well as Policy and regulation

that apply. Exponentially developing technologies that spawn new services and applications, coupled with regulatory reform, changing legal frameworks and the emergence of new markets, have given rise to increased demands for training and skills development. Further, the impact of convergence and globalization has intensified the ongoing challenge to people in these sectors to remain informed of local developments and international trends and practices. The IoT technology has the potential to change the world, just as the Internet did. This is very much starting to happen, as the continual decrease in size, cost, and energy consumption of wireless devices is dramatically boosting the number of mobile objects. The number of mobile objects composing the IoT will significantly grow: in 2020, between 12 and 50 billion devices are expected to be connected with each other, a 12 to 50-fold increase from 2012. This implies that the traffic generated will explode. The huge amount of traffic will require standardized interfaces and IP address utilization, such as IPv6. The course will cover Introduction to Internet of Things and ICT Standards and Regulation. Stake holders & echo system in communications Technology & Services. QoS regulation in Communications Networks. Enabling policies for Sustainable Communications and Information Technology services.

**b. Course Objectives**

The objectives of the course are to:

1. introduce students to the concepts of IoT.
2. Understand IoT Market perspective.
3. explore the interconnection and integration of the physical world and the cyber space.
4. design & develop IOT Devices.
5. provide Data and Knowledge Management skills with the use of Devices in IoT Technology.
6. understand State of the Art IoT Architecture.
7. understand the real World IoT Design Constraints, Industrial and Commercial Automation in IoT.

**c. Learning Outcomes**

By the end of the course, students should be able to:

1. demonstrate an understanding of the fundamentals of IoT and Wireless sensor network communications
2. Demonstrate an understanding of the basic principles, practices and regulatory objectives to be achieved in licensing services; administering universal service obligations and resources.
3. Design, implement and Deploy an IoT solution
4. Work with IoT open software and open hardware platforms
5. Demonstrate an understanding of the basic principles, practices and regulatory objectives to be achieved in administering competition policy; transparent and efficient interconnection and facilities leasing policy; and tariff and rate regulation.

**d. Detailed Course Content**

i Introduction To IoT *(3 hours)*

ii WSN; MAC, IEEE 802.15.4; WSN Communications (802.15.4, Wifi, Gprs, Bt)*(6 hours)*

iii Routing, RPL *(6 hours)*

iv Design and Deployment of IoT solution. Open Software, Open Hardware And rduino. Introduction To Middleware *(6 hours)*

v Law, regulation, governance and the institutional framework; Licensing and monitoring; Competition policy and resource management; Internet policy and the Internet in effective regulation *(6 hours)*

vi Universal access, universal service and the digital divide; Net neutrality and the open nternet. *(6 hours)*

vii .Interconnection and facilities-leasing; *(5 hours)*

viii Price and tariff regulation *(5 hours)*

ix Quality of service and consumer protection *(5 hours)*

**e. Study Materials**

The materials shall include textbooks, journal/conference papers, and several freely available open online educational resources.

**f. Mode of Study**

Teaching will be by lectures, presentations, demonstrations, discussions, and guided self-paced studies learning.

**g. Mode of Assessment**

Coursework (Assignments and projects) (40%) and final examination (60%).

**h. Reading List**


1. Arshdeep, B. and Vijay, M. *Internet of Things: A Hands-On Approach* 2014. Vijay Madisetti, USA.
2. Maciej, K. *Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry.* 2016. WILEY Publishing.
3. Li, S. and Xu, L. D. *Securing the Internet of Things* 2017. Syngress, Boston, USA.
4. Adria,n M. and Hakim C. *Designing the Internet of Things (1st ed.)* 2013. WILEY Publishing, Boston, USA.


### 6.2.4 CPS81104 Real Time Operating System

**Course Description**

This course is designed to prepare students in designing and programming embedded devices and systems based on real time operating systems. Most embedded computer systems have dedicated microprocessors as their computational and controlling elements and run real-time operating systems. This course covers concepts, programming languages, tools, hardware, and methodologies used in the construction of real-time operating systems and their peripheral components.

**Course Objectives**

This course is designed to prepare students to advance knowledge and understanding on the following:

1. Operating systems and their advantages to embedded systems design
2. RTOS Basic Principles
3. RTOS development tools and environments
4. Practical RTOS systems and applications
5. HW/SW Co-synthesis algorithms
6. System partitioning for HW/SW co-design
7. Special HW/SW architectures

**Learning outcomes**

1. Know the characteristics and application areas of embedded systems and real-time operating systems; understand the basic components of embedded computer systems and their interactions among different components (including hardware and software).
2. Demonstrate expertise in reading peer reviewed papers in real-time operating systems and explain them in writing.
3. Understand and modify Window programs that communicate to peripheral devices such as parallel ports, etc. and write code that can be loaded to real hardware or to control the simulator.
4. Use circuit diagrams to represent and modify logic.
5. Use electronic equipment to debug hardware, load the compiled code onto the target system by using a chip programmer, etc.
6. Use hardware design language VHDL to design and verify embedded systems.
7. Use software simulator and in-circuit hardware to test and debug C code written for embedded systems.
8. Write application code and system code for different types of real-time operating systems.

**Indicative Content**

***A. Embedded real time operating systems (rtos)***

Operating Systems (OS) and Real-Time Operating Systems (RTOS). Embedded RTOS. Software development methods and tools: Run-time libraries. Writing a library. Porting kernels. Concurrent Programming and Concurrent Programming Constructs. Task Scheduling and Task Interaction. Basic Scheduling methods, scheduling algorithms. Tasks, threads and processes. Context switching. Multitasking. Communication, Synchronisation. Semaphores and critical sections. Example RTOS systems. (E.g. Embedded Linux, Windows CE, Micrium, VxWorks etc.). Programming and debugging Embedded Systems. Practical examples and case studies.

***B. Hardware/software co-design***

Embedded Processors; Hard and Soft Processor Macros (e.g. Altera Nios and Xilinx Microblaze, ARM). A brief overview of peripherals. Architectural Models. HW/SW Partitioning and partitioning algorithms. Distributed systems. Memory architectures, architectures for control-dominated systems. Architectures for data-dominated systems. Compilation techniques for

embedded processor architectures. Modern embedded architectures. Architecture examples in multimedia, wireless and telecommunications. Examples of emerging architectures. Multiprocessor and multicore systems.

**Mode of Delivery**

i Lectures: Lectures will be conducted and students will be taken through the theoretical and practical aspects of the course.
ii Student projects: Students will be given projects at the start of the course and these will be continuous projects building on the techniques taught in class. At the end of the course, students will complete projects.

**Mode of Assessment**

i Progressive assessment (40%). This will consist of theory and practical assignments (projects).
ii Final exam (60%). Part of the final exam may be a project.

**References**


1. Amos, D, Lesea, A and Richter, R, 2011. FPGA-Based Prototyping Methodology Manual: Best Practices in Design-for-Prototyping. S.l.: Synopsys Press. ISBN 9781617300042
2. Bailey, D. G., 2011. Design for Embedded Image Processing on FPGAs. Singapore: John Wiley & Sons (Asia). ISBN 9780470828496
3. Berger, A, Embedded Systems Design: An Introduction to Processes, Tools, and Techniques. Berkeley, CA: CMP Books. ISBN 9781578200733
4. Bertolotti, I. C and Manduchi, G, Real-Time Embedded Systems: Open-Source Operating Systems Perspective. London: CRC. ISBN 9781439841549
5. Valvano, Jonathan W., [no date]. Embedded Systems: Introduction to the Arm® Cortex(TM)-M3: ISBN 9781477508992


### 6.2.5 CPS 81105: Privacy in the Digital Age

**a) Course description**

Privacy is a growing concern in our modern society. We interact and share our personal information with a wide variety of organizations, including financial and healthcare institutions, web service providers and social networks. Many times such personal information is inappropriately collected, used or shared, often without our awareness. This course introduces privacy in a broad sense. Cases to be studied are online tracking, surveillance and Internet censorship, big data, privacy engineering, Internet of Things, and location privacy.

**b) Course objectives**

This course will enable students to;

i Understand the basic concepts in privacy and data protection as well as the regulatory approaches to privacy in the digital age.

ii Understand the general and specific legal instruments involved with privacy rights and data protection in Africa and beyond.
iii Understand the meaning and manifestations of new technologies.
iv Understand Data privacy: the motivations for data privacy and common implementations
v Understand online privacy: online tracking and anonymous communication systems.
vi Know opportunities and implications of using AI/ML in privacy.

**c) Learning out comes**

The intention is for the student to be able to:

1. Understand major areas that intersect with privacy especially in the digital age is cybersecurity
2. Gain better knowledge of how various concepts and principles in data protection are being used to strike a balance between innovation and human rights with respect to data protection
3. Gain more knowledge on the status of data protection
4. Analyze and differentiate between various online tracking mechanisms and ways to mitigate such tracking techniques.
5. Explain how anonymous communication networks like Tor work and how they help users preserve their online anonymity
6. Study privacy implications of using AI/ML on big data. Also explore ways to design better privacy-preserving and transparent ML algorithms.
7. Understand various side-channel leaks and inference attacks.
8. Analyze privacy regulations/frameworks

**d) Mode of delivery**

This course will be delivered through lectures, practical and case studies and will be assessed through course works and exams

**e) Detailed course content**

**1: Introduction to privacy and data protection.**

i This introductory module sets the stage for the course with analyses and
ii Basic understanding of the right to privacy in general and data privacy in particular
iii Key concepts with respect to data protection;
iv The historical development of data protection and the right to privacy
v The relationship between the right to privacy and other human rights;
vi Policy and regulatory approaches to data privacy and concludes with key principles on privacy by design.

**2: Overview of the legal framework on privacy**

i Various existing legal and institutional systems with respect to data protection including regional standards on the right to privacy and data protection
ii The principles governing the lawful processing of data; scope of application; data processing formalities; rights of data subjects and obligations of data controllers.

**3: Legitimate restrictions on the right to privacy**

i Limitations to the right to privacy. Given the legally accepted practices of limitations of rights under international human rights law
ii Internal and external limitations on the right to privacy in international human rights law;
iii Examines the interference with the right to privacy and communications surveillance and highlights surveillance-enabling laws and privacy

**4: Privacy and cyber security**

i Relationship between privacy and cyber security.
ii The concept of cyber security; examines the international legal frameworks on cyber security
iii The risks and vulnerabilities associated cyber security threats and how these impacts on privacy and highlights global cyber security initiatives.
iv The inter-relationship between the two concepts has made it important to understand how they intersect and what this means for the protection of personal information.
v Privacy implications of using AI/ML on big data. Also explore ways to design better privacy-preserving and transparent ML algorithms

**5: Emerging issues –privacy in the digital age**

i Prevalent challenges that arise in the context of the right to privacy and the rapid technological advances in the digital age.
ii The key challenges posed by new technologies to privacy; assessment of data protection frameworks on new technologies in Africa;
iii Examining the concept of data minimization; conceptualization of cross-border data transfer; ensuring compliance with existing data protection frameworks and discussing the issues of data sovereignty and data localization.
iv De-anonymization attacks on databases.
v K-anonymity, l-diversity, t-closeness and differential privacy to anonymize and protect PII (personally identifiable information) in databases.
vi Online tracking mechanisms and ways to mitigate such tracking techniques.
vii Anonymous communication networks like Tor work and how they help users preserve their online anonymity
viii Study privacy implications of using AI/ML on big data. Also explore ways to design better privacy-preserving and transparent ML algorithms.
ix Side-channel leaks and inference attacks.
x Analyze privacy regulations/frameworks (briefly look at existing and emerging privacy regulations)
xi Compare and contrast users' attitudes and
xii Design and evaluate usable privacy notices.

**f) Course Assessment**

Students will be assessed by coursework which will be comprised of assignments and tests, and will constitute 40%, and final written examination that will constitute 60%.

**g) References**


1. .Romansky, R., I. Noninska. Globalization and Digital Privacy. Electrotechnika & Electronica (E+E), ISSN: 0861-4717, Bulgaria, 11/12 (vol.50), 2015, pp. 36-41
2. Thussu, D. K., International Communication: Continuity and Changes (3rd ed.), Bloomsbury Academic, ISBN: 978-1-7809-3265-1, 2019 (370 p.). Kim, J., M. Hastag. Social Network Analysis: Characteristics of Online Social Networks after a Disaster. International Journal on Information Managements, 1 (vol. 38), Feb 2018, pp. 86-96; https://doi.org/10.1016/j.ijinfomgt.2017.08.003
3. Sunstein, C. R. #Republic: Divided Democracy in the age of Social Media. ISBN 978-0-691-18090-8, Princeton University Press, 2018 (316 p.). [5] Samreen, S. N., N. Kharti-Valmik, S. M. Salve, P. N. Khan. Introduction to Cloud Computing. International Research Journal of Engineering and Technology, 2 (vol. 5), 2018,pp. 785-788 ( https://irjet.net/archives/V5/i2/IRJET-V5I2174.pdf).
4. Kulkarni, T. R., V. Waghmare, D. Chaudrhary, P. Kulkarni. Security Implementation in Cloud Computing Using User Behavior Profiling and Decoy Technology. World Journal of Technology, Engineering and Research, 1 (vol. 3), 2018, pp. 108-113.
5. Lin, Jie et al., A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal, 5 (vol. 4), Oct 2017,pp. 1125-1145, DOI: 10.1109/JIOT.2017.2683200
6. Ray, P. P. A Survey on Internet of Things Architectures. Journal of King Saud University –Computer and Information Science, 3 (vol. 30), July 2018, pp.291-319.
7. Oussous, A. et al. Big Data Technologies: A Survey. Journal of King Saud University – Computer and Information Science, 4 (vol. 30), Oct 2018, pp. 431-448 (https://doi.org/10.1016/j.jksuci.2017.06.001)


### 6.2.6 CPS81106 Cloud Technologies and Architectures

**a. Course Description**

Cloud Computing technologies are emerging as a common way of provisioning infrastructure services, applications and general computing and storage resources on-demand. Cloud computing enables new possibilities for highly elastic and potentially infinite computing power with scalability, big data analytics, and support for delivery of mission critical secure enterprise applications and services. During this course student will gain hands-on experience with various types of cloud models and explore areas such as programming models and application development for cloud systems, cloud management technologies, the underlying system architectures, data centers, virtualization, and cloud storage. The course prepares graduates to enter a range of professional positions related to cloud systems, including developing cloud-based applications, managing cloud systems and designing cloud infrastructures.

**b. Course Objectives**

The objectives of the course are to:

1. provide an understanding of the field of Cloud Computing, its enabling technologies, main building blocks, and architectures
2. provide hands-on experience for solving relevant and cloud computing real-world problems
3. develop the skills needed to become a practitioner or carry out research projects in the Cloud Computing domain

**c. Learning Outcomes**

At the end of this course, students will have:

1. an understanding of the field of Cloud Computing, its enabling technologies, main building blocks, and architectures
2. gained hands-on experience for solving relevant and real-world problems through projects that utilize various cloud tools including programming models and cloud systems such as Amazon, Microsoft Azure, Google App Engine, etc
3. developed the skills needed to become a practitioner or carry out research projects in the Cloud Computing domain

**d. Detailed Course Content**

The course is broken up into the following topics.

*Cloud Computing Systems and Architectures (10 hours)*

This topic will provide a broad overview of cloud computing, its history, technology overview, benefits, risks and the economic motivation for it. The topic will also cover cloud computing types: Infrastructure as a service (IaaS), Software as a service (SaaS), Platform as a service (PaaS) - Architectures and Models: local/distributed, private/public, hybrid. The topics will involve experimentation through case studies using popular cloud systems like Amazon S3, EC2, Force.com, MS Azure, Google App Engine, etc.

*Cloud Computing Technologies (10 hours)*

Sub topic will include Virtualisation - Multi-tenancy - Data management - Elastic and resilient environments - Cloud and Load Balancing. Students will learn how virtualization can allow software and hardware images (e.g., virtual machines) to run side-by-side on a single cloud data center yet provided security, resource and failure isolations. They will understand how virtualization enables clouds to offer software, computation, and storage as services as well as attain agility and elasticity properties. We will discuss resource virtualization in detail and present multiple examples from 27 Xen and VMware. Finally, we will present real use cases such as Google App Engines and Amazon EC2.

*Programming Models for Cloud Computing (10 hours)*

Students will be given an overview on a variety of cloud-applicable programming models. Students will understand the benefits and limitations of each so that they can assess applicability based on the problem domain. Students will gain working experience in one

(or two) of these programming models. Upon completion of this module students will be able to: Explain the fundamental aspects of parallel and distributed programming model, demonstrate an understanding of the different cloud programming models (Dryad, MapReduce, Spark, GraphLab, Pregel).

*Challenges and Trends (5 hours)*

This topic will cover Data and Information Integration - Security/Trust Management and Governance - Legislative and economic environment - Cloud computing future trends.

**f. Study Materials**

The materials shall include textbooks, journal/conference papers, cloud platforms, and several freely available online resources.

**g. Mode of Study**

The teaching will be highly student centered. It will involve teaching, online/class room discussions, demonstrations, group/individual projects and self guided research. A student will be expected to do self-paced research in each of the module.

**h. Mode of Assessment**

- Progressive assessment (40%). This will include in-class quizzes and cross-module projects
- End of semester examination (60%). Part of the final exam may be a practical project.

**i. Reading List**


1. [1] Thomas Erl, Robert Cope, and Amin Naserpour. *Cloud Computing Design Patterns* 2015: Prentice Hall Press. Available: http://dl. acm.org/citation.cfm?id=2810076
2. [2] Michael J. Kavis. *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)* 2014: WILEY. Available: http://eu.wiley.com/WileyCDA/WileyTitle/ productCd-1118617614.html
3. [3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. *A view of cloud computing* 2010: WILEY. Available: http://dx.doi.org/ 10.1145/1721654.1721672


## 6.3 DETAILED COURSE DESCRIPTION YEAR 1: SEMESTER 2

### 6.3.1 CPS 81201 Embedded System design

**Course Description**

An embedded system is some combination of hardware and software that is designed for a particular function. In a world where control and robotic systems are gaining more ground in the physical, industrial, and medical environment, it is important to deploy systems that are reliable and secure. Intelligent machines are a permanent part of the global landscape. There is need for more

expertise in analysing, developing, and implementing optimal control systems. Majority of embedded designs are closed loop control systems, as opposed to open loop control. This course unit is aimed at providing students with theoretical and practical skills in the design and development of advanced embedded systems. Students will be able to learn theoretically and practical needed to optimise embedded system designs using microcontrollers or DSP devices. While combining electrical and computing skills, the students will be challenged in research and design for systems/applications such as: Embedded software for controlling the power grid; Automatic vehicles; Car-to-car communication; Flying robots; Verification techniques; Multi-core architectures; and Energy-efficient wireless communication.

**Course Objectives**

By the end of the course, students should be able to

1. To develop an understanding of embedded systems architectures for the purpose of creating prototypes or products for a variety of applications.
2. To determine specification, model and build embedded systems
3. To select optimal hardware characteristics suitable for building embedded system for a particular problem domain.
4. To critically apply evaluation/validation approaches to assess the performance of the different embedded system platforms and determine those suited for particular implementation.
5. Critically appraise and recommend improvements that should be made on existing embedded system implementations
6. To develop student's' understanding of how the wireless infrastructure, longevity, security, and the mission critical nature of the end application, affect the design architecture, the design considerations, and the design techniques used when developing IoT end-node devices

**Learning Outcomes**

After completing the course, students are expected to develop and demonstrate knowledge and understanding, skills and other attributes in the following areas:

i ***Knowledge and understanding*** to address the hardware/software trade-offs inherent in embedded systems.

ii ***Intellectual skills*** to identify and analyse the constraints and characteristics of embedded systems, to interpret the particular requirements of real-time systems and to evaluate and select best case algorithms for embedded/control system applications

iii ***Practicle skills*** to derive and apply practical embedded/control theory algorithms. Also, practical skills in developing difference equations for optimal design of embedded systems.

iv ***Transferable skills*** to communicate, work independently, evaluate ones work objectively, develop and demonstrate the capacity to learn in unfamiliar situations.

**Detailed Course Content**

***Embedded Computer Architecture***: study hardware architectures for embedded systems. Students will be required to examine the salient issues in the decision-making process, including tradeoffs between hardware and software implementations, processor and operating system selection, and IP creation or acquisition. The challenge in this topic is to combine the many characteristics of

embedded systems into a good hardware structure with focus on ensuring efficiency (low-power or efficient design methods, or compilers), cost-effectiveness (high volumes or low development costs), reliability, fail-safety, small size, sufficient performance and real-time requirements.

***Embedded Design***: Subtopics in this section include specifications and modeling of embedded systems, embedded systems hardware, and system software.

***Embedded System Validation***: This topic focuses on techniques and methods for assessing the correctness and reliability of information and communication technology systems. Should present validation tools illustrating the broad application range of formal methods and techniques. Students should be able to describe the essential characteristics of the main formal techniques, gather informal plain text requirements and transform these into a set of formal requirements, write formal specifications in different specification formalisms, apply abstraction techniques to hide implementation details, interpret the meaning of error messages produced by different validation tools, and complete and correct specifications.

***Quantitative Evaluation and Optimisation of Embedded Systems***: understand the kind of formalisms used when quantitative aspects, such as time, probability and resource usage. Apply two forms of formalisms - dataflow graphs and Markov chains. It should extend students' knowledge of the formal semantics and the process equivalences and logics that are involved, plus gain understanding of how to verify properties through algebraic manipulation, calculation and model-checking.

***Real-time Systems***: the theory and practice of real-time system design as applied in embedded systems requiring guaranteed task completion times. Subtopics include theoretical basis for real-time techniques, several scheduling algorithms and their schedulability analysis techniques.

**Course Assessment:**

The course assessment will be the inform of tests and assignments (40%) and final written examination (60%), totaling 100%.

**Mode of delivery**

This course is delivered using a total of 30 lecture hours and 45 practicle hours. The total contact hours of the course are therefore, 45 contact hours. The detailed mode of delivery is as detailed below;

i Lectures, tutorial/practical sessions as well as demonstrations.
ii Individual and group-based tutorial.
iii Wide range of simulation software and other tools will be used to support the student's learning process.
iv Individual literature review of current trends in embedded systems developments softwares and processors.
v Group homework where students will be exposed to real-life case studies
vi Individual and group presentations.
vii Coursework will be a practical-based case study. Students will be presented with a complex real-life problem of industrial, environmental, security or healthcare for which they must develop solutions by applying embedded systems concepts. Students will be expected to analyse, select, design simulate appropriate solutions to such engineering problems. Coursework

will be based on continuous and progressive assessment for all learning outcomes.

**Reading List/References**

(i). Peter Marwedel (2018). Embedded System Design: Embedded Systems, Foundations of Cyber-Physical Systems, and the Internet of Things. 3rd Edition, Springer.

(ii). Jonathan Valvano (2017). Embedded Systems: Real-Time Operating Systems for Arm Cortex M Microcontrollers.

(iii). James K. Peckol (2009). Embedded Systems: A Contemporary Design Tool, 2nd Edition, Wiley India Pvt. Limited, ISBN: 978-1119457503

(iv). Robin Heydon (2012). Bluetooth Low Energy: The Developer's Handbook, Prentice Hall, ISBN: 9780132888363

### 6.3.2 CPS81202 Cryptographic And Communication Security

**a) Course Description**

Computing professionals are facing new challenges as a result of increasing commonality and complexity in the use of computer-based systems in the practical world. More and more developers and users are demanding for the provision of secure systems to protect the resources from abuse. This requirement has been compounded by the emergence and rapid expansion of the Internet and the popularity of the applications such as E-commerce. This subject focuses on standards, architectures and technologies used to ensure security of computer-based systems and the related resources. Topics include Introduction to computer security, models of security, elementary cryptography, software security, vulnerabilities, threats, defenses, secure-software development processes. Security in networks threats and defenses; secure system design principles, techniques and security evaluation; and privacy, ethics and legal issues.

**b) Objectives**

The course aims at introducing students to modern security standards, architectures and technologies used to ensure security of computer-based system resources.

**c) Learning Outcomes**

Upon completion of this course, the learner will be able to:

1. Identify and describe the main types of cryptographic primitives.
2. Evaluate and describe current cryptographic algorithms.
3. Explain the basics of public key infrastructures.
4. Describe the role of certificate authorities and certificate repositories.
5. Compare and contrast centralized infrastructures and decentralized infrastructures.
6. Understand the various standards involved in establishing an interoperable Internet PKI.
7. Describe interoperability issues with PKI standards, and describe how the common Internet protocols use and implement the PKI standards.

**d) Teaching methods**

Teaching will be through taught lectures, tutorial discussions.

**e) Course Content**

**1. Introduction** **4hours**

i Motivation and Importance
ii Basic Concepts: Confidentiality, Integrity, Availability, and Trust
iii Security Policies
iv Privacy and data protection
v Protocol and system security
vi Basic cryptography

**2. Cryptography** **10 hours**

i Classical Cryptography
ii Reductions
iii Simulation-based security
iv Composition
v Security proofs
vi One-way and hash functions
vii Pseudo-randomness
viii Symmetric encryption and authentication
ix Public-key encryption
x Digital signature schemes
xi Some cryptographic protocols
xii Some cryptanalytic techniques

**3. Access Control** **6hours**

i Authentication
ii Authorisation

**4. Protocols** **4hours**

i A Simple Authentication Protocol
ii Real-World Security Protocols

**5. Software** **6hours**

i Software Flaws and Malware
ii Insecurity in Software
iii Operating Systems (OS) and Security
iv Protecting Programs, Data and Information

**f) Mode of assessment**

This course will be assessed through assignments and class tests (40%) and the final written examination (60%).

**g) References**

1. Mark Stamp, ”Information Security: Princi
(ISBN 0471738484)

2. Mathew Bishop, “ComputerandScience”,Security:AddisonAr W
3. Charles P. Pfleeger and Shari Lawrence Pf
   Prentice Hall, 2003
4. William Stalling, “Crptography and Networ
   Hewlett-Pakard Professional Books, 2000
5. M. Howard, D. LeBlanc: “Writing Secure Cod
6. Wm. Arthur Conklin, Gregory B. White, Chuck Cothren, Dwayne Williams and Roger L. Davis,” Principles of Computer Security+ a

### 6.3.3 CPS 81203 Business process modelling and analysis

**Course Description**

Modelling, analysis and design skills are indispensable to BPM success. With increased globalisation, companies face stiffer competition, and successful companies cannot afford to harbour inefficiencies if they are to be competitive. Furthermore, customers are becoming more demanding. Therefore, business processes must be designed to ensure they are effective and meet customer requirements. A well-designed process will improve efficiency and deliver greater productivity. In this course, you will acquire a solid understanding and develop skills in practical techniques for process modelling, analysis and design.

**Course Objectives**

1. To broaden students' understanding of the theory of process modelling and business systems development
3. To build a deeper understanding of the operations of business organization, their relationships and functional structure and the advantage of considering the process-oriented view of organisations
4. To deepen students' knowledge of the business process, management systems, their structure and how processes fit into the overall organisation objectives;
5. To facilitate students to acquire knowledge of the analytical tools that can be used to model, analyse, understand, and design business processes;
6. To familarise students with skills in different simulation softwares used as tools for analysing business processes.
7. To acquint students with skills required to depict business processes via maps and models to prepare for analysing and improving business process performance.
8. To demonstrate to students the significance of creating the right context for process modelling and defining clear boundaries.

**Learning Outcomes**

After completing the course, students are expected to develop and demonstrate knowledge and understanding, skills and other attributes in the following areas:

i ***Knowledge and understanding*** in information Systems modelling in business, Business Process Management Systems, Systems Implementation and development, Enabling IT tools and technologies

ii ***Intellectual skills*** to formulate and express problems in the IS/IT and the business domain, Analyse and evaluate academic literature within IS/IT and

computing, and Develop an independent and strategic viewpoint within the IS/IT and computing domain.

iii ***Practical skills*** to plan and implement IS/IT projects, write reports, analyse, design, implement and evaluate IT systems, use a variety of IT and computing tools and techniques to solve systems problems.

iv ***Transferable skills*** to communicate, work independently, evaluate ones work objectively, develop and demonstrate the capacity to learn in unfamiliar situations.

**Detailed Course Content**

i Overview of Business Processes.
ii Evolution of Enterprise Systems Architectures
iii Introduction to Business Process Modelling
iv Approaches to Business Process Modelling and Analysis
v Business process management Systems
vi Business Modelling with Unified Modelling Language
vii Business Process Methodology

**Course Assessment:**

The course assessment will be the information of tests and assignments (40%) and the final written examination (60%), totaling 100%.

**Mode of delivery**

This course is delivered using a total of 30 lecture hours and 30 tutorial hours. The total contact hours of the course are, therefore, 45 contact hours. The detailed mode of delivery is as shown below:

i Lectures, tutorial/practical sessions, as well as demonstrations.
ii Individual and group-based tutorial.
iii A wide range of computer-based learning and other tools will be used to support the student's learning process.
iv Use of real- life case studies and individual literature review of current developments in the business process modelling field.
v Seminars and debates in which staff and students are proactive and interactive are used.
vi The coursework will be a practical-based case study. Students will be presented with a complex real-life organisational system within which they must apply business process modelling concepts and strategic analysis to prepare a process-based system. Students will be expected to review, select and design appropriate applications, and support their process-view systems intervention. Students will also be expected to comment on their work, and its applicability to strategic business process modelling in different organisational and/or industrial settings. Coursework will be based on continuous and progressive assessment for all learning outcomes.

**Reading List/References**

1. John Jeston (2014). Business Process Management: Practical Guidelines to Successful Implementations. 4th Edition. Routledge.

2. Mathias Weske (2012). Business Process Management: Concepts, Languages, Architectures; 2nd Edition, Springer
3. Marlon Dumas, Marcello La Rosa, Jan Mendling, and Hajo A. Reijers (2018). Fundamentals of Business Process Management; 2nd Edition,
4. Emrah Yayici (2015). Business Analysis Methodology Book: Business Analyst's Guide to Requirements Analysis, Lean UX
5. Gert H. N. Laursen and Jesper Thorlund (2017). Business analytics for managers: taking business intelligence beyond reporting. 2nd Edition, Wiely.
6. Business Process Analysis by Geoffrey Darnton with Moksha Darnton
7. Workflow Patterns - Wil M.P. van der Aalst, AHM ter Hosftede
8. Business Process Management Demystified: A Tutorial on Models, Systems and Standards for Workflow Management Wil M.P. van der Aalsts
9. Eriksson, H and Penker, M (2000) Business Modelling with UML: Business Patterns at Work OMG Press.
10. Leffingwell, D and Wirig, D (2000) Managing Software Requirements: A Unified Approach, Object Technology Series Addison- Wesley
11. Darnton, G and Darnton, M. (1997) Business Process Analysis. Thomson Business Press.
12. Harrington. J. H, Esseling. EK.C and van Nimwengen, H (1997) Business Process Improvement: WorkbookMcGraw-Hill
13. Guy Doumeingts & Jim Browne (1997). Modelling Techniques for Business Process Re-engineering and Benchmarking: IFIP TC5 WG5.7
14. Manuel Laguna, Johan Marklund (2018). Business Process Modeling, Simulation and Design.

### 6.3.4 CPS81204 Research Methods

**a) Course description**

This module seeks to establish the link between the real world problems and Management literature. It further explores the role of literature review in converting real problems into research questions. Applied research methodologies, deductive and inductive research methodologies their use and limitations. The nature and sources of business data. Using qualitative research methods to solve business problems, including action research, grounded theory, ethnography and their limitations. Techniques of qualitative research including interviews, observations, interpretation and analysis of qualitative data. Using quantitative research methods in business and management and limitations. Techniques of quantitative research methods including questionnaire, sampling methods, descriptive and inferential statistics including contingency tables and tests of independence. Presentation and analysis of quantitative data. Criteria for evaluation of alternative research methods. Writing research projects and reporting research findings.

**b) Course objectives**

This course will enable students to;

1 Appreciate the nature of ICT / management research.

2 Formulate and clarify a research topic.

3 Understand Qualitative research methods, questionnaire design, sample size, sampling methods.

4 Analyse quantitative data, descriptive and inferential statistics including contingency tables, chi-square test of independence.

5 Develop an appropriate style, the need for continual revision and meeting the assessment criteria.

**c) Learning outcomes**

Upon successful completion of this module, students will be able to:

1 Use and compare different research methodologies, explain how different methods complement each other and examine when one might be more appropriate than the other.

2 Demonstrate a clear understanding of the type and source of business data handling techniques.

3 Analyse quantitative and qualitative business / management data and arrive at appropriate conclusions.

4 Assess and use appropriate research methods in applied business / management situations.

5 Design, conduct and record research in business and management.

6 Critically evaluate research methods used in applied business/management situation.

**d) Course content**

| | | |
|---|---|---|
| i | An Overview –Formulating and Classifying a Research Topic | **4hours** |
| ii | Literature Review –Developing the Problem | **4hours** |
| iii | Deciding on a Research Methodology | **5hours** |
| iv | Ethical Issues and Business Research | **4hours** |
| v | Sources and Types of Data –Selecting Samples | **4hours** |
| vi | Qualitative Research: Data Collection Techniques | **5hours** |
| vii | Analyzing Qualitative Data | **5hours** |
| viii | Quantitative Research –Collecting Data Using Questionnaires | **4hours** |
| ix | Analyzing Quantitative Data | **4hours** |
| x | Writing and Presenting Research Reports | **4hours** |

**e) Teaching methods**

Teaching will be through lecture sessions and case Studies

**f) Mode of Assessment**

Assessment will be through take home assignments and course work.

**g) References**


1. Saunders, M.N.K. Lewis, P.and Thorn hill,, A. (2003) Research Methods for Business (3rdedn). Prentice Hall.
2. Michel R, Roy W, and Clark, M (2000)
3. Parrington, D. Essential Skills for management Research,. Sage
4. Sarankntakos, (2005) Social Research., Palgrave McMillan, New York
5. Ghosh B.N (1992) Scientific Method of Research.( R.E), Sterling.
6. Walters D, (1998) Essential Qualitative Methods: A Guide for Business, Financial Times Prentice Hall. London.
7. Cooper D. & Schindler P.S.(2003) Business Research Methods ($8^{th}$ ed), McGraw Hill.
8. Maylor H., Blackmon K, (2005) Researching Business and Management, Palmgrave McMillan, New York


### 6.3.5 CPS81205 Networked and Distributed Control Systems

**a) Course description**

This is an advanced research-led course in the study of networks and distributed systems, developing students' knowledge and skills in network protocols and technologies, mobile systems, multimedia and distributed systems. Emphasis is placed on DCS operation, networking, HMI, and Alarms.

b) **Course Objectives**

i To review sensors, instrumentation, and process control

ii To cover DCS Organization and operation

iii To summarize the most important Networking, HMI, and Alarm features of DCSs

iv To highlight Maintenance and Troubleshooting procedures and issues

v To review Advanced Process Controllers in DCSs

vi To cover Latest trends related to DCSs

c) **Learning Outcomes**

Upon completion of this course, the student will be able to:

i Have a working knowledge of sensors, instrumentation, and process control as they relate to DCSs.

ii Have a working knowledge of DCS Organization and operation

iii Have practical knowledge of Networking, HMI, and Alarm features of DCSs

iv Gain practical awareness of the issues and procedures to perform DCS Maintenance and Troubleshooting

v Understand an advanced Process Controllers in DCSs

vi Gain practical overview of Latest trends related to DCSs

vii Understand Sensors, instrumentation, and process control as they relate to DCSs.

**d) Detailed Course Outline**

1. Introduction to DCS

    i DCS Hardware Component and architecture

    ii Hardware Installations and Design

    iii Best Practice : System Architecture

    iv Basic Logic Programming

    v Basic HMI Programming

2. Engineering, Design and development

    a. Logic programming

        i. Function Block

        ii. Customize Function Block

        iii. Global object function block

        iv. Download/upload

3. HMI programming

    i Create and design application

    ii Setup communication

    iii Setup screen and Tag

    iv Setup alarm

    v Setup data logging and trending

    vi Optimize tag using global object

    vii Setup redundant system

    viii Setup security

4. Maintenance

i Troubleshooting
ii Diagnostic
iii Online Modification
iv Backup and Restore

5. Networked control systems
   i Consensus over networks with applications in synchronization and opinion dynamics
   ii Estimation and control over imperfect communication channels (erasure, delay, etc.)
   iii Stabilization over rate-limited and quantization channels
   iv Distributed estimation and Kalman filtering
   v Network protocol design via distributed optimization
   vi Decentralized optimal control and information patterns
   vii Security and privacy in networked control systems
   viii Any other topic of interest if time permits

**e) Course Assessment**

Students will be assessed by coursework which will be comprised of theory and practical assignments and will constitute 40%, and final written examination that will constitute 60%.

**f) REFERENCES**


1. Computer Networks: A Systems Approach, Peterson and Davie (5th edition). Morgan Kaufmann.
2. Alberto Bemporad, Maurice Heemels, and Mikael Vejdemo-Johansson. *Networked Control Systems.* Lecture Notes in Control and Information Sciences, Vol. 406, Springer-Verlag London, 2010.
3. Serdar Yüksel *Stochastic*and *Networked*Tamer*Control*Başar*Systems:.Stabilization and Optimization under Information Constraints.* Springer Science & Business Media, 2013.
4. Mehran Mesbahi and Magnus Egerstedt. *Graph Theoretic Methods in Multiagent Networks.* Princeton University Press, 2010.
5. Francesco Bullo. *Lectures on Network Systems* (http:motion.me.ucsb.edu/book-lns)
6. Francesco Bullo, Jorge Cortes, and Sonia Martinez. *Distributed Control of Robotic Networks: A Mathematical Approach to Motion Coordination Algorithms.* Princeton University Press, 2009.


### 6.3.8 CPS81208 Smart Grids:

**Course Description**

Communication and information technologies have taken an increasingly important role in monitoring and controlling physical systems. The electric power grid is a canonical example of a cyber-physical system in which the physical electrical grid is monitored by a network of sensors and other intelligent devices to continuously monitor, control, and dynamically manage the network to ensure near-perfect reliability. In contrast to the traditional grid in which generation, transmission, and distribution were clearly distinct and managed by well-defined entities, the smart grid allows integration of renewables (e.g., solar, wind) at every layer of the grid (transmission and distribution). Furthermore, there is an increasing need to finely monitor the grid to better manage and conserve energy resources through an array of devices from phasor management units (PMUs) at the transmission levels and Advanced Metering Infrastructure (AMI) such as smart meters at the distribution level. These requirements call for an end-to-end communications, control, and computation (cyber) architecture integrated with the physical network. In this course we will learn about electric power system operations specifically the core operations implemented in current state-of-the-art Energy Management Systems and evaluate their vulnerability to cyberattacks. We will also use an existing software platform with core EMS functionalities to test attacks. Part of the course will focus on machine learning based methods to design better anomaly detectors that go beyond state of the art to enable both event-based and malicious data changes. The course will involve several guest lecturers with expertise in cyberattacks, distributions systems, PMUs, and data analytics.

**Objectives**

1. To equip students the understanding of fundamental principles, generalizations, operations, and economies of smart power grids
2. To explore factual knowledge (terminology, classifications, methods) of cyber-physical systems.
3. To impart skills od designing and protecting smart power grid.
4. To develop the skills in Students of analyzing the issues with the transition towards the smart grids and evaluate and propose solutions for smart power grid.

**Learning outcomes**

Upon successful completion of this course, students should be able to:

1. Analyze the current power grid operations and identify the current issues.
2. Identify and address the issues related to renewable energy integration, demand side management, and energy efficiency.
3. Design architectures for the electrification of transportation and transportation networks.
4. Understand the operation principles and the role of different control, optimization, and communication technologies in developing smart energy grids.
5. Identify control-room technologies for system-wide remote monitoring, protection, and risk management of smart grid cyber security
6. Conduct basic economic analysis to quantify and evaluate the smart grid benefits.
7. Analyze the role of electricity in sustainable development and energy security.
8. Analyze the enabling communication and sensing technologies for cyber-physical systems.

**Teaching methods**

Teaching will be through taught lectures, tutorial discussions.

**Topical Coverage**

i Introduction to Cyber-Physical Systems (CPS)

a. The Power Grid, Grid Sensing and Data collection Methods: SCADA, PMU, What is Cybersecurity in the context of power systems? Is this a real threat?, Operations: Computation/Cyber Aspects of the Grid –State Estimation (SE), Real- time Contingency Analysis, Security-constrained Economic Dispatch.

ii Introduction to Smart Power Grids and Post Carbon Economy.

a. Smart Grid Applications, Government, Industry, Standardization

iii Enabling Technologies:

a. Smart Grid Communications. Network Architectures, Power Line Communications, Advanced Metering Infrastructure, Sensor Technologies. Distributed Generation. Stochastic Models, Forecasting, Carbon Footprint, Microgrid Architecture.

iv Automation networks:

a. Types of networks and their attributes, Different network protocols, ISO-OSI reference model, Industrial automation networks with LonWorks as a case study, Automation network security

v Power System Dynamics (PSD):

a. Emphasizing the structure and information needed to solve optimal power flow (OPF) problems. also, the application of these OPF solutions to evaluate the performance of systems with renewable energy sources; Understand and classify types of power system stability phenomena; Analyze two major types of stability: voltage and frequency stability; Understand active power balance and frequency control

vi Wide Area Monitoring Protection and Control (WAMPAC):

a. Energy Management System (EMS), Digital substations, Synchronized Measurement Technology, Cyber Security in an EMS

vii Smart Grid Cyber Security:

a. Cyber security risk assessment, Security index computation, Use of RTDS and simulation tools for analyzing the impact of an attack

viii Machine Learning Countermeasures/Analytics:

a. The need for better bad data detectors, using machine learning methods such as SVM, nearest neighbor, recurrent neural networks, and LSTMs to design enhanced BDDS that include anomaly detectors for real-time situational awareness

**h) Mode of assessment**

This course will be assessed through assignments and class tests (40%) and the final written examination (60%).

**(h) Reading List**

(1) Smart Grids - Fundamentals and Technologies in Electricity Networks, Bernd M. Buchholz, Zbigniew Styczynski, 1st Edition,ISBN- 13: 978-3642451195.
(2) Peak Energy Demand and Demand Side Response, Jacopo Torriti, 1st Edition, ISBN: 978 1138016255
(3) Plug-in Electric Vehicle Grid Integration, I.S. Bayram and A. Tajer, 1 st edition, ISBN-13: 978-1630810511.
(4) Electric Power System Basics, Steven W. Blume, 1st edition, ISBN: 978 0470129876
(5) The Advanced Smart Grid: Edge Power Driving Sustainability, Andres Carvallo, John Cooper, 1st Edition, ISBN-13: 978-1608071272

## 6.4. DETAILED COURSE DESCRIPTION YEAR 2: SEMESTER 1

### 6.4.2 CPS82102: Seminar Series

**(a)Course Description**

This course will help students to strengthen their ability to do guided research. Through class presentations, students will provide progress on their master'sresearchplans. This course will also help students to be equipped with scholarly writing and presentation skills. However, what is expected out of the students will be explicitly given to them and examined.

**(b) Course Objectives**

The main objectives of this course are:

1. Equip students with the ability to search for and internalize scientific academic material.
2. Develop the students ability in technical writing.
3. Develop the students' presentation skills.

**(c) Learning Outcomes**

At the end of this course students should be able to:

1. Read and internalize scientific academic material in their area of specialization.
2. Developed appropriate conceptual and methodological approaches to their research.
3. Have developed a full research plan for their research-based dissertation.
4. Learned how to offer and received constructive comments on their work in progress.
5. Competently present scientific findings.

**(d) Mode of Study**

Students will be given broad areas of study together with research questions to address by the beginning of the second semester. Each student will be given a senior staff who will be their

supervisor and from whom they will get advice and guidance. The student will then be required to address one research problem and make a write up on it. The student will then be required to present their research proposal to the staff members in the department. As part of the course, the student will also be obliged to attend all (weekly) research talks in the school for the entire semester.

**(e) Detailed Course Content**

Teaching of this course will be in four modules. Each module will be a complete unit of teaching and will be assessed at independently during continuous assessments. The content of the modules will include:

*i.* Module One: Scientific paper writing *(6 hours)*
*ii.* Module Two: Scientific paper presentation *(6 hours)*
*iii.* Module Three: Presentation of research plan *(9 hours)*
*iv.* Module Four: Presentation and discussion of research progress *(9 hours)*

**(f) Study Materials**

Journal articles, conference proceedings, projector and laptop.

**(g) Mode of Assessment**

Students are expected to attend class every week, participate in discussions, and prepare and deliver presentation(s) during the semester.
The method of assessment will be categorized as:

- Attendance of weekly research seminars (10%)
- Scientific paper write up and presentation (40%)
- Research proposal presentation (40%)
- Knowledge of subject matter (10%)

**(h) Reading List**


1. J. Zobel *Writing for Computer Science* Springer, 8, 2014.
2. S. Keshav *How to Read a Paper* ACM SIGCOMM Computer Communication Review, 37(3), 83-84, 2007
3. How to Present a Paper in Theoretical Computer Science: A Speaker'sStudentsGuide. f https://larc.unt.edu/ian/pubs/speaker.pdf
4. Giving a Talk: Guidelines for the Preparation and Presentation of Technical Seminars. http://www.comm.toronto.edu/%7Efrank/guide/guide.pdf
5. The Paper Reviewing Process. http://greatresearch.org/2013/10/18/the-paper-reviewing-process/


**6.4.3 CPS82103 Scholarly Writing**
**Course Description**

The course is designed to cover techniques that can be applied to different types of academic writing including essays, reviews, research papers, grant proposals and thesis writing. The Learners will practice these techniques by drafting a research article with support from other class members and the instructor.

**Objectives**

The purpose of this course is to

provide Learners with the opportunity to improve their skills in writing a research article and other academic texts.

**Learning Outcome**

Upon completion of the course the students should be able to: -

1. Write a research article, review article, thesis chapter and - other related academic research text
2. . Demonstrate and apply knowledge of basic essay structure, including introduction, body and conclusion;
3. Demonstrate understanding of the ways in which writers, - texts and readers interact
4. Make appropriate grammatical and lexical choices in their text,
5. Make appropriate choices about register and - Structure information effectively.
6. Employ correct citation style, including parenthetical, in-text citation and works-cited pages.

**Course Content**

i Paragraph structure (topic sentence, supporting examples, transition sentence)

ii Basic rhetorical modes (narration, description, exposition)

iii Writing process (pre-writing, writing, re-writing)

iv Effective use of quotation, paraphrase and summary

v Stylistics (vocabulary, conciseness)

vi Correct paper formatting

vii Grammar & mechanics as needed

viii Reading and responding to assigned readings

**Teaching Methods**

Seminars, writing assignments, peer reviews, presentations.

**References**


1. Hairston, et al. The Scott, Foresman Handbook for Writers (San Francisco: Longman 2002 or latest edition)
2. Swales, J. M. and Feak, C. B. (2012) Academic Writing for Graduate Students. Third edition. Ann Arbor: University of Michigan Press (415 pages).
3. Graff, G, and Birkenstein, C. They Say, I Say: The Moves that Matter in Academic Writing. 4th edition, Norton, 2018.


**APPENDIX A: PROGRAMME FUNDING**

The Master of Science in Cyber Physical System Engineering will be funded through:

**i. Tuition fees.**
*S*ee Table 2 below

**ii. Government funding.**

Presidential initiative proposal has incorporated into funding to the programme.

**iii. Development partners**

- Project Proposals to donor agencies
- Position the programme for the upcoming Africa Mobility Scheme proposals later this year.
- Engage SIDA for possible support of MSc and PhD in Cyber Physical Systems Engineering.

The budget for the MSc in Cyber Physical has been developed based on costs chargeable to Uganda students admitted to the course. The budget is based on the assumption that 15 students are admitted to the course. Each of the budgets includes recurrent expenditures and projected staff costs (both academic, administrative and support staff), as well as capital expenditure and other running costs.

**Table 2. Proposed programme budget**

| ***Assuming intake of 15 students*** | | |
|---|---|---|
| **A. REVENUE PER SEMESTER** | **Semester I** | **Semester II** |
| Tuition fees | Amounts (UGX) | Amounts (UGX) |
| Students'fees | 2,000,000 | 2,000,000 |
| (UGX 30,000,000 per annum) | | |
| Tuition fees for 15 students @UGX 1,800,000 | 30,000,000 | 30,000,000 |
| *Total* | ***30,000,000*** | ***30,000,000*** |
| | | |
| **B. EXPENDITURE PER SEMESTER** | | |
| University Council 5% | 1,750,000 | 2,750,000 |
| Teaching Expenses 30% | 10,500,000 | 10,500,000 |
| Administrative Expenses 5% | 1,500,000 | 1,500,000 |
| Office Expenses 3% | 9000,000 | 900,000 |
| Library Materials 2% | 600,0000 | 600,0000 |
| Faculty levy 5% | 1,500,000 | 1,500,000 |
| Utilities/Furniture 2% | 600,000 | 600,000 |
| Staff Development 2% | 600,000 | 600,000 |
| Repair/reinforcement of Materials lab 7% | 2,400,000 | 2,400,000 |
| Air ticket for visiting professors 8% | 2,800,000 | 2,800,000 |
| | | |
| ***Total 64%*** | ***24,350,000*** | **24,350,000** |
| ***Expected Revenue 36%*** | ***5,650,000*** | **5,650,000** |

**APPENDIX B: LIBRARY RESOURCES**

| SN | DATABASE | URL FOR LOGIN |
|---|---|---|
| 1 | Emerald Insight | http://www.emeraldinsight.com |

| | | |
|---|---|---|
| 2 | Libhib | http://libhub.kiox.org |
| 3 | Ebrary | http://site.ebrary.com/lib/busitemau |
| 4 | Edudonor Index | www.edudonorindex.com |
| 5 | ARDI (Access to Research for Development and Innovation) | http://ardi2.wipo.int |
| 6 | CTA Publishing | http://publications.cta.int/en/ |
| 7 | TEEAL (The Essential Electronic Agricultural Library) | |
| 8 | Research4Life (This is a Gateway to other Databases) such as HINARI | http://www.who.int/hinari/en/ |
| 9 | INASP: International Network for Availability of Scientific Publications | http://www.inasp.info/en |
| 10 | EIFL: Electronic Information for Libraries | http://www.eifl.net |
| 11 | AGORA (Access to Global Research in Agriculture) | www.fao.org/agora/en |
| 12 | OARE (Online Access to Research in the Environment) | http://www.unep.org.oare |

APPENDIX C: HUMAN RESOURCES

**Table A1-1: Academic Staff available to Teach Masters Science in Cyber Physical Systems Engineering.**

| SN | NAME | POSITION | Current course load | Proposed Courses | Qualification |
|---|---|---|---|---|---|
| 1 | Dr. Musinguzi Wilson Babu | Assoc. Prof. | • Fluid Dynamics<br>• Electrical Technologies | • Research Seminar Series<br>• Smart Grid | • PhD Energy Engineering (Makerere University, Uganda)<br>• MSc. Sustainable Energy Engineering (The Royal Institute of Technology, Sweden)<br>• BSc Mechanical Engineering (Makerere University, Uganda) |
| 3 | Prof. Twaib Semwogere | Assoc. Prof. | •Engineering Mathematics<br>•Research Methods | •Scholarly writing<br>•Research Methods | • PhD Mechanical Engineering (MAK,)<br>• MSc. Mathematics, BSc. Mathematics ( MAK) |

| | | | | | |
|---|---|---|---|---|---|
| 4 | Dr. Matovu Davis | Lecturer | • Cloud and IoT forensics<br>• Enterprise Networks | • Internet of Things<br>• Cloud Technologies and Architectures | • PhD IT (Masinde Muliro University of Science and Technology-Kenya)<br>• MSc. Computer systems and Networks Engineering (Kharkov National University of Radio Electronics-Ukraine)<br>• BSc. Computer Engineering (Kharkov National University of Radio Electronics-Ukraine) |
| 5 | Mr. Arineitwe Joshua | Lecturer | • Circuit Theory<br>• Electricity and Magnetism | • Modeling of CPS<br>• Embedded System design | • MSc (EE), MSc. (Physics), BSc(Ed)– Physics/Mathematics (MAK)<br>• |
| 6 | Mr. Alunyu Andrew | Lecturer | • Database Systems<br>• Mobile Application Development<br>• File Systems Forensics | • Business Process Modeling and Analysis<br>• Real Time OS | • PhD in information systems (ongoing) MAK<br>• MSc (Data Communication & Networks) (MAK)<br>• BSc. Education (Physics/Maths) MUST |
| 7 | Dr. Gilbert Gilibrays Ocen | Senior Lecturer | • Cybercrime & Digital Forensic<br>• IT Audit<br>• Systems Security | • Network and distributed control systems<br>• Privacy in Digital age | • PhD. In information technology. Masinde Muliro University of Science and Technology- Kenya)<br>• MSc. Information Technology (CUU)<br>• BSc. Computer Engineering (Kharkov National University of Radio Electronics-Ukraine) |
| 8 | Dr. Odongtoo Godfrey | Senior Lecturer | • Cyber Incidence Response<br>• Data Communication &Networks<br>• Project | • Network Security<br>• Embedded IoT Systems | • PhD. Information Technology (MAK)<br>• MSc (Information Technology) (UCU)<br>• PGD Data communication & |

| | | | | | |
|---|---|---|---|---|---|
| | | | Management | | Software Engineering (MAK)<br>• BSc. Education (Physics/Maths) MUST |
| 9 | Dr. Godliver Owomugisha | Senior Lecturer | • Artificial Intelligence<br>• Data mining<br>• Digital Image Processing | • Learning decision Making<br>• Digital signal processing | • PhD in Computer Science, University of Groningen, The Netherlands.<br>• MSc. Computer Science, Makerere University<br>• BSc. Computer Science, Makerere University |
| 10 | Mr. Lusiba Badru | Lecturer | • User interface Design<br>• Object oriented Programming<br>• | • Cryptography and communicatio n security | • PhD. In information technology (*ongoing*) Masinde Muliro University of Science and Technology-Kenya)<br>• Master of Science (Computer Science), Gadjah Mada University, Yogyakarta, Indonesia, 1997.<br>• B.Sc. (Economics & Mathematics) with Education, Islamic University In Uganda, Mbale, Uganda 1992. |
| 11 | Dr. Rose Nakasi | Senior Lecturer | • Structured Programming<br>• Web development | • Embedded System Design | • PhD in Computer Science, Makerere University.<br>• MSc. Computer Science, Makerere University<br>• BSc. Computer Studies, Busitema University |
| 12 | Ms. Asingwire Barbra | Lecturer | • | • Network Security | • PhD. in IoT and Network Security (*ongoing*)<br>• MSc (Data Communication & Networks) (MAK)<br>• Bachelors of Computer Engineering (BU) |
| 13 | Dr. Mirondo Geofrey | Lecturer | • Communication theory | • Design and Analysis of | • PhD Technical University of |

| | | | | | |
|---|---|---|---|---|---|
| | | | ● Signal Processing<br>● Circuit Theory | CPS<br>● Cloud technologies and Architecture | Catalonia, Barcelona, Spain<br>● Msc. Telecommunication<br>● Bsc. Telecommunication (KyU) |