Design and Implementation of a Smart Transducer System Prototyping of a Micro-controller Based Intelligent Electrical Equipment Theft Detection Methodology

Malebo L.G Maboko
M.Sc (Eng) Student
School of Mechanical, Industrial and Aeronautical Engineering
University of the Witwatersrand (Wits)
Johannesburg, South Africa
672871@students.wits.ac.za

Mncedisi Dewa, Ph.D.
Senior Lecturer
School of Mechanical, Industrial and Aeronautical Engineering
University of the Witwatersrand (Wits)
Johannesburg, South Africa
mncedisi.dewa@.wits.ac.za

Abstract

This paper presents the design and implementation of a smart transducer system for electrical cabinet equipment theft. The system consists of a sound sensor module, an ultrasonic distance sensor element and an ATMega328p micro-controller. The solution was designed to operate in a zone 2 hazard area. The raw sound sensor output signal was preprocessed using appropriate signal transformations. The prototype was tested on HUAWEI's 5G Telecommunications cabinet, connected to an SMU on the rectifier via USB for main power. Alarms are displayed on HUAWEI'S NetEco site energy monitoring software noise threshold and/or door movement detected. This solution can easily integrate to any IoT system with minimal or no modifications. A low cost, low power consumption, real-time, high accuracy solution was realised. The prototype implemented achieves an average response time of 4 over 6 samples.

Keywords
Arduino, ATMega328p, Sound Detector, Ultrasonic Distance Detector and IoT.

1. Introduction
According to Smith (2004). Electricity theft within the power distribution network mainly takes place in two ways, by bypassing the energy meter and by hooking of the energy line, This paper focusses of electricity equipment theft in enclosed areas such as electrical and network cabinets. Enclosed electrical equipment such battery modules and energy meters can be secured from theft and tempering.

In South Africa and most countries around the globe cabinet intuition is illegal according to Eskom Holdings SOC Ltd (2022). This crime leads to:

- Removal of the energy meters and other vital electrical equipment.
- Illegal connections.
- Vandalism and
- Tempering of the energy meters.

Illegal removal of the energy meter and other electrical components is global problem. This form of electricity equipment theft can lead to power cuts in the community. Customers will not get power services in their households as this causes electrical voltage discontinuity. Additionally, this crime of removal of vital power equipment such as power backup batteries leads to a non-resilient, poor energy network infrastructure for example, it results in immediate power loss during load shedding. Illegal connections are a form of electricity theft that can lead to unknown power usage by electricity distribution companies. Vandalism (destruction of electricity equipment) can lead to incorrect meter readings, billing irregularities and inconsistent energy metering communication. Tempering of the energy meter such as bypassing the energy meter is a fraudulent act that leads to electricity theft as zero-meter readings can be recorded although the customers are using electricity. These societal issues are influenced largely by the lack of action by the law pertaining electricity equipment theft. Current tariff prices and the economic state of the country also contribute to this, according to Glauner et al (2017).

The massive financial losses due to electricity equipment theft can lead to bankruptcy. The funds needed to maintain the existing power systems, as well as funds to upgrade the existing power systems for more capacity are exhausted. This is the current predicament in South Africa according to Glauner et al (2017). There is lack of maintenance of equipment and no upgrades made in response to the increase in electricity demand. Most countries around the globe experience the challenge of electricity equipment theft according to Elisan (2022).

In South Africa, there is a rampant theft of back-up batteries used to power telecommunication towers during power cuts according to Elisan (2022). MTN network service provider reported losing 200 batteries (48V-100Ah Lithium Iron Phosphate) in a month. Vodacom records at-least 700 batteries including vandalism per month. Cell C also recorded over 800 sites intrusions and 2300 batteries stolen in 11 months. Similarly, rain networks report a total of 80-110 site vandalism and battery theft every month. On battery costs R 28 000.00, MTN has reported more than R300 million worth of stolen batteries in 2018. Since then, a 35% increase of battery theft has been recorded across the telecommunications networks. R 130 million is spent on vandalism only. Vodacom reports that a total of R 10 million on 100 sites is a minimum requirement to replace the batteries according to Elisan (2022) and Ahmad (2010).

In South Africa total of R 3 billion has been recorded in 2019 only due to equipment theft and electricity equipment theft in Gauteng Province municipalities namely, Tshwane, Johannesburg and Ekurhuleni. In the rest of the world Pakistan suffers total losses of around R 15,9 billion, in Brazil a total of R 188 billion, and a total of 107 billion in USA and R286 billion in India in 2018 according to Ahmad (2010).

1.1. Objectives

The main objective of this research is to develop an efficient and cost-effective electricity equipment theft detection technique that could response in real time. This will be realised by:

- Investigation and evaluation of existing electricity equipment theft detection schemes.
- Design and implementation of a new electricity equipment theft technique.

1.2 Problem statement

Electricity equipment theft in electrical and network cabinets within the electrical power network negatively affects the quality of power supply, power systems maintenance as well as tariff prices on genuine consumers. This consequently degrades the quality of electrical power services to the community.

1.3 Requirements

A real-time smart transducer measurement system must be developed for cabinet power equipment theft detection. The solution must integrate with HUAWEI's Telecommunications network cabinet for signaling when triggered and send alarm information to NetEco HUAWEI's a centralized remote Operations Support System (OSS) solution for site energy for notifications. Furthermore, the solution should be robust enough to integrate with any Internet of Things (IoT) platform with no minimal design alterations.

1.4 Assumptions and Constrains

It is assumed that the system will always be mounted in the cabinet. So, it will rely on the intrinsic safety of the cabinet. The system will have an operating temperature range of -40°C to 40°C. Any mechanical components that may affect the functionality of solution and instability are not considered in the design. This solution will not work for non-enclosed electrical components such transmission lines.

1.5 Success criteria

The design is deemed a success if the measurement system designed meets the stated requirements with acceptable response time. The data output from the microphone sensor should be in the decibel meter audible (dBA) range. The model should be standalone and be powered by a 5V power Universal Serial Bus (USB) source.

2. Literature Review

The Industrial Internet of Things (IIoT) and IoT have recently become more popular. Different solutions have been presented to address the issue of theft in general, specifically by means of object detection. Home automation is the most discussed topic in IoT. Techniques used to detect electricity equipment theft can be classified as follows:

- Theoretical studies
- Hardware solutions
- Combined hardware and software solutions
- Manual checking of equipment tempering, and components ceil checks.

Ahmad (2010) implemented a noise detection system using the 8-bit AVR microcontroller of the ATMEL family. This runs assembly code, and the solution could measure between 58 dBA and 95 dBA, The system categorized nose in three conditions. The safety, danger threshold and very dangerous. According to Rancang et al (2011) a noise detection using ATMega microcontroller16 running C code and a microphone element with a detection range of 56 dBA-75 dBA.

Rajagukguk and Sari (2018) presented a scientific study, a noise level monitoring tool using Arduino uno running C code as data processing input from the microphone sound sensor. The operating principle of the tool is that it detects noise and displays it on an LCD in dBAs. Then when the tool detects noise above 75 dBA red LED switches on and buzzer will beep indicating danger. For sound greater than 56 dBA an orange LED will switch on and a buzzer would beep. Lastly for sound levels less than 55 dBA. This tool was able to detect and display sound between 50 dBA and 100 dBA. Thillai et al (2019) developed a security system (knock detector) which was a distinctive way to open a door without a key. This uses a piezo-electric sensor programmed on with an Arduino microprocessor using C programming language. Vanitha et al (2021) presented a model of automated noise detection system using Arduino Nano and C programming language. The system was used to identify the source of noise in closed areas such as a library so that necessary actions can be taken.

Wahl et al. (2012) developed a distributed Pyroelectric Infra-Red (PIR) sensor-based methodology for counting people. The prototype functions such that binary output from PIR sensors is used to reduce the over-head of continuous sampling and in turn reduce the energy consumption. Nazaar et al (2021) developed a motion detection security system using Arduino uno. The system detects the motion of an intruder using PIR motion sensor. This type of system specifically detects humans and animals using the radiation of their body heat. The system was designed with an electronic buzzer for sound as notification in case intrusion. The application was a home-based bell system where the PIR reads human proximity to the door and automates a sound notifying people in the household that there is someone the near proximity of the door.

Palayo (2021) from techmemicro uses intelligent camera object-based detection method using pixy camera and Arduino uno to detect objects using image processing. The camera module's image processing functions by identifying different sections of an object using width and height, colour and other characteristics. This detection method for an intrusion system is a hardware based simplified image detection and tracking system no signal processing will be needed as required in deep learning and machine learning algorithms. Prasetyo et al (2018) developed a GSM system-based model using Arduino Nano and C programming language to achieve a chainsaw sound and vibration sensor for timber theft in the forest. The vibration sensor is used to detect falling trees and the sound detector detects sound with threshold of 63.4 dB.

This work developed in this paper was inspired by Rajagukguk and Sari (2018). To come up with this solution, an additional proximity sensor as presented in Wahl et al was combined with the sound sensor to achieve a more intelligent system. The focus of the paper is on an amalgamated software and hardware solution. These types of solution include: Microprocessor based solution running C or assembly code, Micro controller running Python or C code, Programmable Automation Controller (PAC) running C++ or C code, Programmable Logic Controller (PLC) running Ladder Diagram (LD), Structured Text (ST), Functional Block Diagrams (FBD), Instruction List (IL) and/or Sequential Function Charts (SFC).The presented work uses a microcontroller ATMega328p based C code detection solution was chosen due to it's power efficiency consumption, portability, low cost, accuracy and Realtime capabilities. C code was chosen as it is recommended by the Arduino community which is well documented.

3. Methods

All source code sketches used for this project can be found on this platform: https://drive.google.com/drive/folders/1QYo3AGd2fIBOOP4K6W-8pz3UlK1e8aFw.

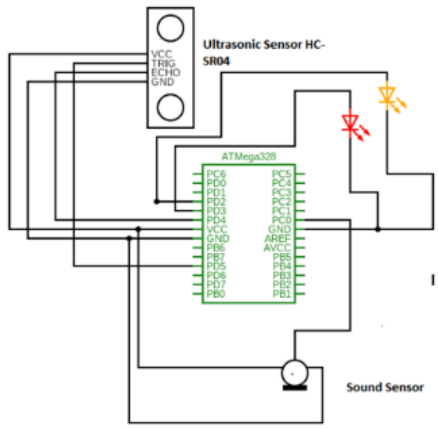

Figure 1. System Design Schematic.

Figure 1 shows the overall system schematic diagram. The data acquisition was achieved using KY-037 microphone sound sensor and an HC-SR04 ultrasonic distance sensor. The data processing as well as control and initial system testing was achieved using Arduino Uno as shown in Figure 2, and later the functionality was loaded to the ATMega328p micro-controller for more portability, reduced size and less costs. The system's power supply will be through a 5V USB from the System Management Unit (SMU) to the VCC and GRD pins of the ATMega328p chip. The digital information pins PD2 and PD3 of the ATMega328p are the system's output that trigger the digital input of the ratifier when activated. PC0 is an analog input pin connected to the sound detector module and PD5 is a digital input pin connected to the Ultrasonic sensor module.

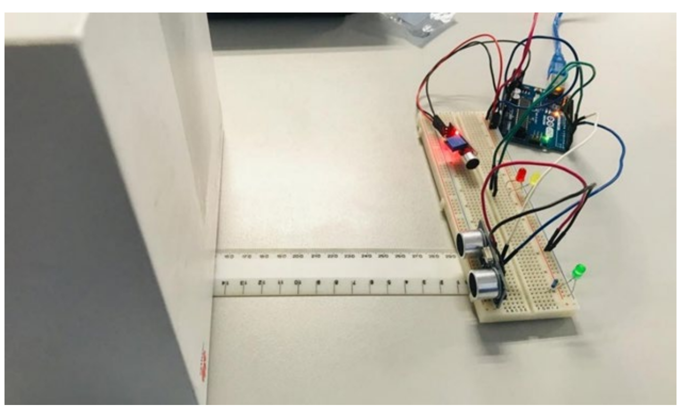

Figure 2. Picture of testing system.

3.1. Functionality

The smart transducer system detects theft based on three different scenarios:

- When sound greater than 80 dBA is detected and within 15 minutes the distance between the sensor system and the cabinet door is greater than 15 cm we have theft detected. The red LED switches on and sends a high signal to the digital input dry contact of the rectifier. The alarm then displays on NetEco platform.
- When sound is less than 80 dBA but distance between the sensor system and the cabinet door is greater than 15 cm we have theft suspected/a normal site visit. The Orange LED switches on and sends a high signal to the digital input dry contact of the rectifier. The alarm then displays on NetEco platform.
- If sound is greater than 85 dBA probably theft. The Orange LED switches on and sends a high signal to the digital input dry contact of the rectifier. The alarm then displays on NetEco platform.

4. Data Collection

All noise data was generated by physical banging of the cabinet door with a hammer to imitate intrusion. A single bang and multiple bangs were created. A continuous noise data such as a one produced by a grinder cutting metal was also recorded. All tests were done in the field on an intrinsically safe HUAWEI's 5G telecommunications outdoor cabinet with IP55 protection ratings.

The raw signal detected by the sound sensor module required preprocessing as it was unstable with a fluctuating amplitude. Application of appropriate logarithmic transformations indicated in equation 1 assisted in the stability of the signal. Further correction of the signal's amplitude was done by an iterative method to achieve the correct amplitude. The sound sensor module has a variable resistor of x ohms which was maximized to achieve less sensitivity for to avoid false positives. The dBA value achieved the sound sensor was then compared with dBA values achieved using smart phone application called DecibelX running on iOS app 15 on iPhone 7 Plus. More accurate results we obtained. The ultrasonic sensor has an accurate raw data reading as no preprocessing was needed.

$$OutputSoundSignal = Alog(raw\_soundsignal)$$

Where A is the desired amplitude, raw_soundsignal is the non-processed input signal and OutputSoundSignal is the sound signal converted to dBA.

Figure 3 shows the output signal before data processing and Figure 4 shows the system's behavior recording cabinet sound after data processing. The signal achieved is stable. All graphs were plotted using Arduino's serial plotter monitor.

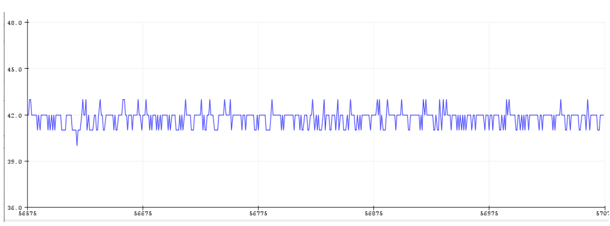

Figure 3. Signal output before data processing.

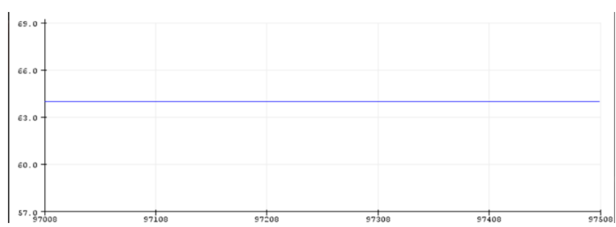

Figure 4. Signal output after data processing.

5. Results and Discussion

The prototype implemented achieves an average response time of 4s over 6 samples as show in Figure 5 below shows alarms displayed on HUAWEI's NetEco site energy monitoring software. For testing purposes all alarms we set to minor alarms. At a later stage critical stages will be renamed and configured as required. Table 1 shows the tabulated results during testing with the corresponding response time.

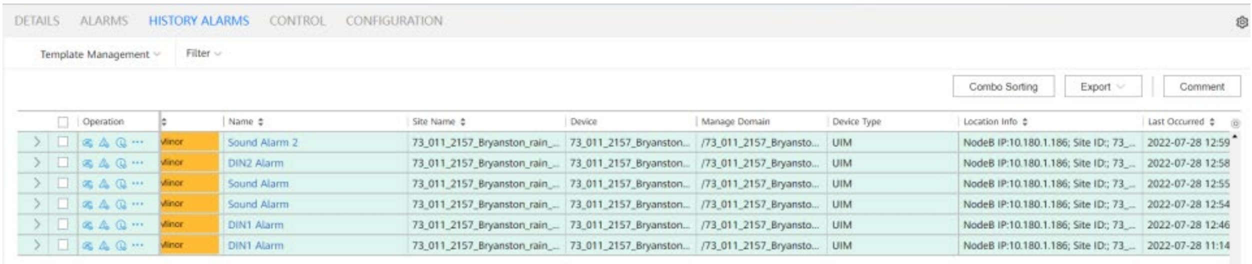

Figure 5. Alarm history on NetEco platform.

Table 1. Test sample and response times.

Test Samples	Response time (s)
Test sample 1	3.8
Test sample 2	3.3
Test sample 3	4.2
Test sample 4	3.7
Test sample 5	4.1
Test sample 6	3.9
Total sum	**4.0**

Figure 6, 7, and 8 shows results graphical representation of the system when noise is generated by banging the cabinet. Figure 9 shows a snapshot of Arduino's object distance detection in cm and sound in dBA.

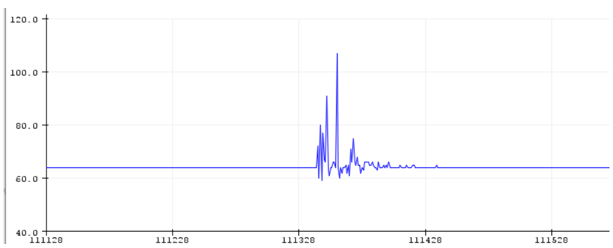

Figure 6. Single loud noise generated.

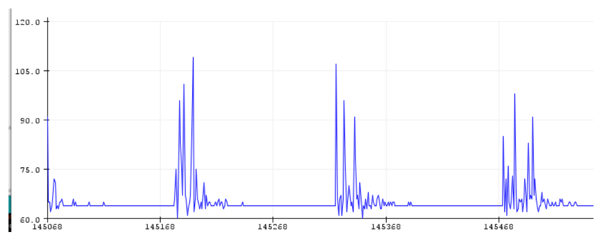

Figure 7. Multiple loud noise generated.

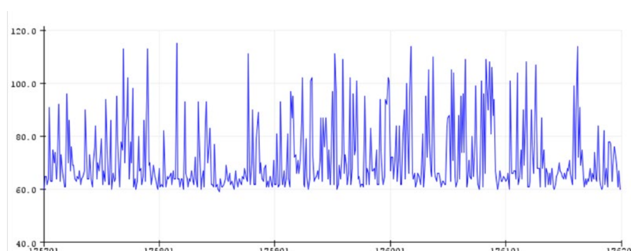

Figure 8. Continuous loud noise generated (grinder) monitoring.

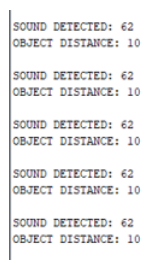

Figure 9. Sound Detected and Object distance.

Finally, the was calibrated to have a dBA range 64dBA (maximum lower threshold sound of an operating cabinet) to 120 dBA.

5.3 Critical analysis and Proposed Improvements

The circuit is currently powered by a USB connect to the rectifiers SMU. The SMU's power output is rated at 5W, 5V at 1A. However, an LM805 voltage regulator can be used to protect the circuit from any possible voltages higher than 5V. The output signal of the circuit is connected to the rectifier's digital input. A relay between the circuit's output and the rectifiers digital input would be provide a more efficient solution.

The product developed consists of sensitive electronic devices, these devices are sensitive when exposed to mechanical harm and humidity. Development of and intrinsically safe encapsulation may extend the operation lifetime of the product. For this investigation it is enough that the product will rely on the intrinsic safety the cabinet.

The system's static characteristic temperature is the limiting property of the solution. The Arduino, ATMega328p, currently has a maximum operating temperature of 85°C. However, the microphone and the ultrasonic sensor detector have a maximum operating temperature of 40°C. Therefore, this limits the system to function in environments with temperatures below 40°C. More temperature resilient components should be investigated later.

An electronic relay is an electromechanical device that is used a switch. This device consists of multiple contacts input terminal and multiple contact output terminals. Configured as Normally Closed (NC) or Normally Open (NO) upon coil energization. Multiple input-output contacts would help the solution in terms of scalability as well as efficient logical programming.

6. Conclusion

This paper presented the development of a custom smart transducer system for electrical cabinet equipment theft. The system consists of a sound sensor module, an ultrasonic distance sensor element and an ATMega328p micro-controller. The solution was designed to operate in a zone 2 hazard area. The raw sound sensor output signal was preprocessed using appropriate signal transformations. Testing results and critical analysis were documented. The prototype was tested on HUAWEI's 5G Telecommunications cabinet, connected to an SMU on the rectifier via USB for main power. Alarms are displayed on HUAWEI'S NetEco site energy monitoring software noise threshold and/or door movement detected. This solution can easily integrate to any IoT system with minimal or no modifications. A power efficient low cost, real-time, high accuracy solution was realised. The prototype implemented achieves an average response time of 4s over 6 samples, with an operating range of 64 dBA to 120 dBA.

References

Smith, T.B., Electricity Theft: A Comparative Analysis. Energy Policy, 32, 2067-2076, 2004.

https://www.eskom.co.za/distribution/customer-service/public-safety/, *Electricity Safety Tips*, Accessed 29/09/2022

P. Glauner, J. A. Meira, P. Valtchev, R. State, and F. Bettinger, "The challenge of non-technical loss detection using artificial intelligence: A survey," *International Journal of Computational Intelligence Systems*, vol. 10, no. 1, p. 760–775, 2017.

Miguel Enzo Elisan, https://intelli-tower.com/tower-monitoring/cell-tower-battery-theft-in-africa/, Cell-Tower Battery Theft in Africa, Accessed 29/09/2022

Suyatno dan H. Ahmad, Perancangan dan Pembuatan Alat Pendeteksi Tingkat Kebisingan Bunyi Berbasis Mikrokontroler, Jurnal Fisika dan Aplikasinya, Vol. 6, No. 1, 1- 4, 2010.

P. de Wet, "Gauteng metros lost r5 billion in electricity last year –but ekurhuleni is doing a lot better than joburg and tshwane," Feb 2019. [Online]. Available: http://www.businessinsider.co.za/Gautengcities-water-and-electricity

Krstovski, S., Quality index, www.ieomsociety.org/newsletter/. Accessed May 21, 2020.

P. de Wet, "Gauteng metros lost r5 billion in electricity last year –but ekurhuleni is doing a lot better than joburg and tshwane," Feb 2019. [Online]. Available: http://www.businessinsider.co.za/Gautengcities-water-and-electricity

Kharis Rancang, Bangun Sistem and Deteksi Kebisingan sebagai, Media Kontrol Kenyamanan Ruangan Perpustakaan, Skripsi, Fakultas Sains dan Teknologi, Fisika, Universitas Islam Negeri Sunan Kalijaga, Yogyakarta.Juniastel Rajagukguk and Nurdieni Eka Sari, Detection System of Sound Noise Level (SNL) Based on Condenser Microphone Sensor Journal of Physics: Conf. Series 970 (2018) 012025, 2010.

T. J. Salai Thillai, T. Sarath Babu and B. S. Reddy, "Arduino based safeguarding system by using sound," *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 765-769. 2019.

C. N. Vanitha, K. L. Sridhar and R. Dhivakar, "Automation of Noise Detection Using Internet of Things," *2021 6th International Conference on Inventive Computation Technologies (ICICT),* pp. 184-189, 2021.

F. Wahl, M. Milenkovic, and O. Amft. A distributed pir-based approach for estimating people count in office environments. In IEEE 15th International Conference on Computational Science and Engineering, CSE '12, pages 640–647, 2012. Washington, DC, USA, IEEE Computer Society.

Mohammad, Nazeer, Motion Detection Security Alarm Using Arduino, 2021.

Roland Palayo, https://www.teachmemicro.com/detect-objects-camera-arduino/, Detect Objects with Camera and Arduino, last accessed 29/09/2022

D. C. Prasetyo, G. A. Mutiara and R. Handayani, "Chainsaw Sound and Vibration Detector System for Illegal Logging," *International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*, 2018, pp. 93-98, 2018.

Biographies

Malebo Maboko is currently a Special Project Research Engineer at rain Networks, South Africa. He is an M.Sc in Engineering specialising in Artificial Intelligence student at the School of Mechanical, Industrial and Aeronautical Engineering, University of the Witwatersrand. He currently holds a B.Sc in Engineering in Electrical Engineering: (Information Engineering) form the School of Electrical and information Engineering, University of the Witwatersrand. He previously served as a Candidate Control, Instrumentation and Automation Engineer at BBE and Proconics Groups. His research interested are in Telecommunications Engineering, IoT, Data Analytics and Machine Learning. He is currently a registered as a Candidate Engineer with the Engineering Council of South Africa (ECSA).

Mncedisi Dewa holds a PhD in Industrial Engineering from Stellenbosch University, a Master of Engineering degree in Manufacturing Systems and Operations Management and BEng degree in Industrial and Manufacturing Engineering from the National University of Science and Technology, Zimbabwe. He is currently a Senior lecturer in the School of Mechanical, Industrial and Aeronautical Engineering at the University of the Witwatersrand. Within the School, he conducts teaching, learning, postgraduate supervision, academic consultation and collaborative research. He has served as an academic for over twelve years now, with seven of those years in the Higher and Tertiary education sector in South Africa. His research interested are in the areas of E-learning, Digital Assistance Systems, system modelling, simulation and Engineering Education. He is a registered member of the South African Institute of Industrial Engineers (MSAIIE), the South African Society for Engineering Education (MSASEE) and a registered Candidate Engineer with the Engineering Council of South Africa (ECSA).