A NOVEL NON-DESTRUCTIVE ANTI-THEFT SYSTEM WITH LOW POWER AUTO SHUT-OFF AND WIRELESS REACTIVE-ABLE CIRCUITS FOR PHOTOVOLTAIC MODULE

WASIF ALI KHAN

MASTER OF ENGINEERING SCIENCE

LEE KONG CHIAN FACULTY OF ENGINEERING AND SCIENCE
UNIVERSITI TUNKU ABDUL RAHMAN
NOVEMBER 2018

A NOVEL NON-DESTRUCTIVE ANTI-THEFT SYSTEM WITH LOW POWER AUTO SHUT-OFF AND WIRELESS REACTIVE-ABLE CIRCUITS FOR PHOTOVOLTAIC MODULE

By

WASIF ALI KHAN

A dissertation submitted to the Department of Electrical and Electronic Engineering,
Lee Kong Chian Faculty of Engineering and Science,
Universiti Tunku Abdul Rahman,
In partial fulfillment of the requirements for the degree of
Master of Engineering Science
November 2018

ABSTRACT

A NOVEL NON-DESTRUCTIVE ANTI-THEFT SYSTEM WITH LOW POWER AUTO SHUT-OFF AND WIRELESS REACTIVE-ABLE CIRCUITS FOR PHOTOVOLTAIC MODULE

WASIF ALI KHAN

Solar farms are getting upgraded to overcome energy crisis. These solar farms are usually located at rural sites because of high land prices in urban areas and shading problems caused by buildings. In this regard, these solar farms are highly prone to theft due to limited procedures of protection and the photovoltaic modules used are valuable. Existing anti-theft methods implemented on solar farms are referred as to system based, instead of solar modules. These systems are used to alert the authorities about theft, but, at the same time, intruders will also be alerted by of alarms, and at times, security personnel might need a significant amount of time to reach the site to prevent the theft and the security guards at solar farms are not sufficient enough to tackle heavily armed robbers. Thus, these systems are not able to tackle theft issues effectively. In response, the Non-destructive anti-theft system (NODAS) has been developed to resolve theft issues in the growing industry of PV modules. It is a modular based system which does not require the integration of any

additional system. The NODAS constitutes of a low power position sensor, a high current auto shut-off switch and a wireless based microcontroller. The position sensor retrieves the location of the PV modules and stores it in a microcontroller as an authorized location. Upon detecting the modules' displacement, the microcontroller will then force the MOSFETs to interrupt the delivery of power to the PV modules. The PV modules can be replaced for maintenance purposes, and it can only be reactivated by authorized personnel using a wireless controller. The PV modules can also be reused after recovered from theft, making it non-destructive. Moreover, the MOSFETs play an important role in the circuitry as they interrupt the power to the load in the case theft. As the dissipated power in a MOSFET can damage itself and consequently, the PV modules, multiple MOSFETS are used in the circuit to distribute heat across each MOSFET. Experiments have been conducted to find the location on PV modules in which position sensor will get least affected by interconnections of PV modules. This experiment also helped to preset the tolerance of position sensor to avoid false alarms. The range for wireless controller was also observed to avoid delay in communication and loss of information. In this regard, it is important to note that NODAS does not entirely protect PV modules from theft, rather, it demotivates thieves from stealing the PV modules as displaced modules will not generate any power. The NODAS will be laminated inside PV module, but at this time, the project was only designed and developed to prove a concept. However, the components used for the project are readily available in miniature packages, so the same components can be used for the lamination of NODAS inside the PV modules.

ACKNOWLEDGEMENT

I would like to express the deepest gratitude for my supervisor Dr. Lim Boon Han for his timeless guidance throughout this project. His guidance was not only confined to the project besides that he also gave me advices to pursue my life towards right direction. He created an excellent environment to accomplish my goals without any obstacles. I would also like to thanks my co-supervisor, Dr. Lai An Chow to enhance my computing skills for the project. This project could not have done without their proficient guidance. I must have to admire the entire team of Universiti Tunku Abdul Rahman also that made this institution an extraordinary lively place to conduct interdisciplinary research. It gives open opportunities to students from all over the world to fulfill their temptations towards research. I would like to admire Universiti Tunku Abdul Rahman for granting me a fund to pursue my research.

I would also like to thanks my lovely family members including dad, mom, wife, brothers and sisters to keep faith in me and it could not be done without their continuous admiration and appreciation.

Last but not least, I would like to present my sincere gratitude towards my friends and fellow researchers that helped me to accomplish this task.

APPROVAL SHEET

This dissertation entitled **"A NOVEL NON-DESTRUCTIVE ANTI-THEFT SYSTEM WITH LOW POWER AUTO SHUT-OFF AND WIRELESS REACTIVE-ABLE CIRCUITS FOR PHOTOVOLTAIC MODULE"** was prepared by WASIF ALI KHAN and submitted as partial fulfillment of the requirements for the degree of Master of Engineering and Science at Universiti Tunku Abdul Rahman.

Approved by:

_____

(Dr. Lim Boon Han) Date:……
Supervisor
Department of Electrical and Electronic Engineering
Faculty of Engineering and Science
University Tunku Abdul Rahman

_____

(Dr.Lai An Chow) Date:……
Co-supervisor
Department of Electrical and Electronic Engineering
Faculty of Engineering and Science
University Tunku Abdul Rahman

FACULTY OF ENGINEERING AND SCIENCE

UNIVERSITI TUNKU ABDUL RAHMAN

Date: 07 November 2018

SUBMISSION OF DISSERTATION

It is hereby certified that **WASIF ALI KHAN** (ID No: **15UEM06591**) has completed this dissertation entitled "A NOVEL NON-DESTRUCTIVE ANTI-THEFT SYSTEM WITH LOW POWER AUTO SHUT-OFF AND WIRELESS REACTIVE-ABLE CIRCUITS FOR PHOTOVOLTAIC MODULE" under supervision of Dr. Lim Boon Han (Supervisor) from the Department of Electrical and Electronic Engineering, Faculty of Engineering and Science, and Dr. Lai An Chow (Co-supervisor) from the Department of Electrical and Electronic Engineering, Faculty of Engineering and Science.

I understand that the University will upload softcopy of my dissertation in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

_____

(WASIF ALI KHAN)

DECLARATION

I, Wasif Ali Khan hereby declare that the dissertation is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTAR or other institutions.

_____

(WASIF ALI KHAN)

Date: 07 November 2018

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

µA	Micro ampere
µW	Micro watt
A	Ampere
AC	Alternating current
ADC	Analog to digital converter
AES	Advanced encryption standard
AES 128	Advanced encryption standard 128 bit
APS	Application support
A/C	Air conditioner
CPU	Central processing unit
CCTV	Close circuit television
CSMA	Carrier-sense multiple access
DAC	Digital to analog converter
DC	Direct current
FCS	Frame checksum
FFD	Full functional device
GHz	Giga hertz
GPRS	General radio packet service
GPS	Global positioning system
GSM	Global system for mobile communication
HVAC	Heating, ventilation and air conditioning
IC	Integrated circuit
IEEE	Institute of electrical and electronics engineer

IrDA	Infrared device adaptor
I2C	Inter-integrated circuit
I/O	Input/Output
KBps	Kilo bit per second
LCD	Liquid crystal display
LED	Light emitting diode
m	Meter
mA	milli ampere
MAC	Medium access
MBps	Mega bit per second
mG	milli Gauss
MHz	Mega hertz
mm	millimeter
MOSFET	Metal oxide field effect transistor
MYR	Malaysia ringgit
NFC	Near field communication
NODAS	Non-destructive anti-theft system
NWK	Network
Op-amp	Operational amplifier
OSI	Open system interconnections
PAN	Personal area network
PBA	Printed board assembly
PER	Packet error rate
PHY	Physical
PV	Photovoltaic

QFN	Quad-flat no-leads
RFD	Reduced functional device
RFID	Radio frequency identification
RX	Receiver
SAP	Service access points
SCL	Serial clock
SDA	Serial data
SPI	Serial peripheral interface
SMD	Surface mount device
TV	Television
TX	Transmitter
USART	Universal synchronous asynchronous receiver transmitter
USB	Universal serial bus
V	Volt
W	Watt
WAN	Wide area network
Wi-Fi	Wireless fidelity
WSN	Wireless sensor network
ZCL	ZigBee cluster library
ZDO	ZigBee device object

CHAPTER 1

INTRODUCTION

1.1 Introduction

The use of alternative energy sources has been widely discussed as a measure to overcome the increased demand and price of energy caused by the growing world population. Solar energy is the one of the most accessible renewable energy and its use can help to reduce carbon footprint. In the meantime, numerous photovoltaic modules are required to receive a decent amount of energy, a huge area is required to install these modules, and it is difficult to find that area in the urban vicinity. Moreover, as the high cost of land is another issue that limits the number of solar farms in the urban area, rural areas are always preferred for installing solar power plants. At the same time, there are some barriers in installing photovoltaic modules in rural areas which need to be overcome.

The security of PV modules has always remained the primary concern as photovoltaic modules are left open in the field, and this creates security issues. A solar farm contains a large number of PV modules, making it an easy target for thieves. In this light, as shown by reports in Figure 1.1, theft cases have increased in line with the extensive use of PV modules (Lawson, 2012; Sawin, 2015).

Thieves can easily trespass into the property by using some tools and weapons and easily steal large numbers of PV modules within a short amount of time. (Gifford, 2014). In 2007, it was reported that up to 7,000 out of 60,000 PV modules were stolen from a solar farm located in Serre Persano, Italy in a period of just one year (Gualerzi, 2007). Different solutions are offered by academic institutions and commercial organizations but this issue remains un-preventive.

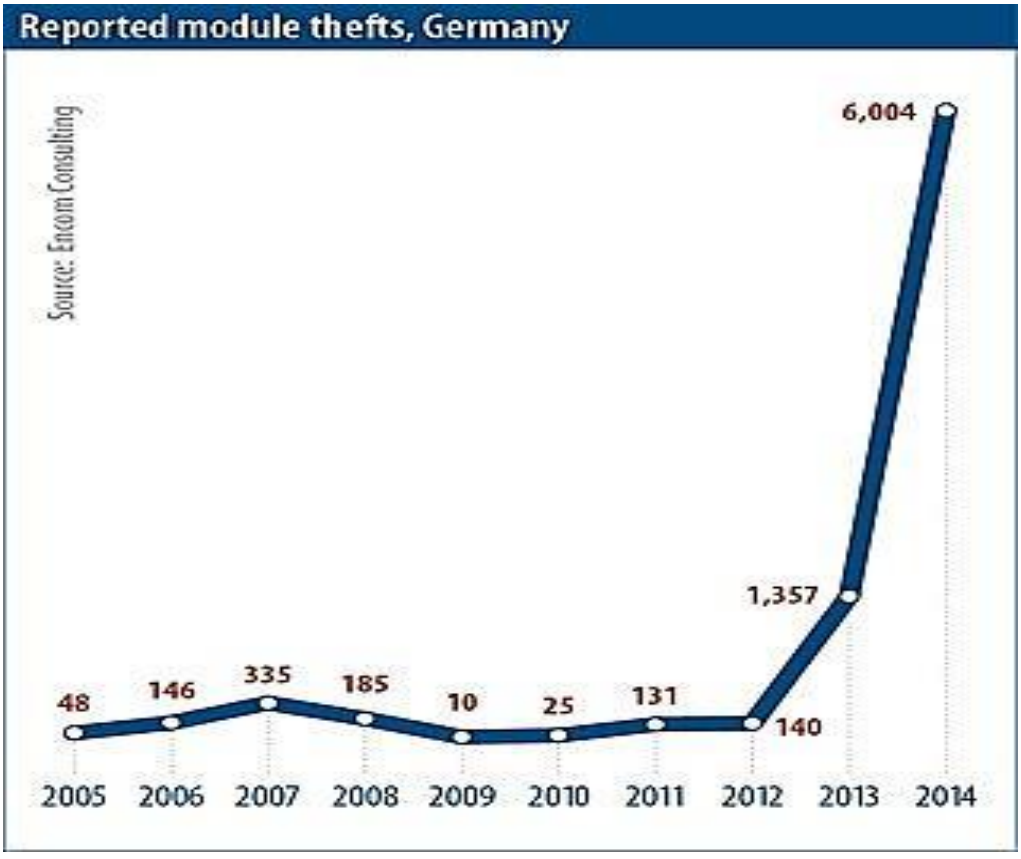


Figure 1.1: Exponential increment in theft cases from 2005 to 2014.

1.2 Problem Statement

The Existing anti-theft methods require PV modules to be installed with additional security systems, i.e. CCTV systems, wireless sensors and the GSM/GPRS systems to alert the authorities about theft. When theft is reported, authorities will follow conventional methods to catch the thieves or recover the stolen PV modules. So, it is least possible to tackle the theft effectively without any loss. This is the reason that the solutions implemented on the system level are non-preventive. Other challenges include the sounds of the alarm can alert the thieves that they are watched and prompt them to hasten their activities, and the security personals employed at solar farms could be insufficient to tackle heavily armed thieves.

As the security systems attached or installed into PV modules bring security issues as they can be easily modified or tampered by thieves, there is a significant need for a security system that can tackle theft issues in the fast growing industry of PV modules. After going through the anticipated problems, several research questions have been formulated:

- How can an anti-theft system, would be non-destructive with low power consumption, be developed within the module level?
- How can this anti-theft system be operated by an authorized person to resume its operation once it is displaced for maintenance purposes or recovered after theft?

- How does this developed system be reliable and will not generate any false alarm?

1.3 Research Objectives

1. To design an auto shut-off system using low-power position sensor for non-destructive anti-theft photovoltaic modules.

2. To design a wireless reactive-able device to resume operation of a non-destructive anti-theft photovoltaic module after auto shut-off.

3. To evaluate the performance of the non-destructive auto shut-off system.

1.4 Scope

The scope of this project covers the design, development and evaluation of a non-destructive anti-theft system. Initially, a position sensing circuit was designed to retrieve the position of the PV module. The reliability, repeatability and sensitivity of the position sensing circuit are tested to avoid triggering the false alarm. A shut-off switch is integrated with a position sensor that cut-off power to the load upon displacement of the PV module while a micro-controller is used to take effective decisions. It stores the position of PV module and controls generated power using shut-off switch. The wireless function of the micro-controller is used by an authorized person to reactivate generated power once the PV module needs to be reset again for maintenance purpose or after it has been recovered after theft.

The anti-theft system is developed to be embedded inside the PV module. However, at this time, this project is conducted to prove the concept, instead of developing a prototype. As the PV module does not have extra space for circuitry, the components used for the project are readily available in miniature package i.e. Surface Mount Devices (SMD). It remains the primary concern that the components will be laminated inside PV module in the future so it should sustain the temperature during the lamination process. At this stage, the modular based Integrated Circuits (IC) are used to prove the concept. These modules are integrated with an evaluation kit for development and evaluation purposes.

In the meantime, the study's scope does not cover small scale prototype development, as well as the lamination of anti-theft system inside the PV module. Thus, further research is suggested for lamination of the prototype which requires special debuggers, sockets etc., to program the IC and the micro-controller. Additionally, it does not cover outdoor performance and analysis as it requires lamination of the anti-theft circuit inside the PV module to proceed.

1.5 Contribution

The anti-theft system is a modular-based standalone system. Hence, it does not require the integration of any additional system. The anti-theft function will be triggered automatically as soon as the location of PV module changes. Moreover, the anti-theft system retrieves the location of a PV module after certain intervals only during day time. As it is only operational at daytime, it is powered by the PV

module itself and has no external battery. In this light, the anti-theft circuit operates at a very low power which is extracted from a PV module. Moreover, as the PV modules are operational only during the daytime, it is not required for the anti-theft circuitry to remain functional at night time which helps conserve the power consumption.

The anti-theft system is non-destructive as anti-theft circuitry can only be reset by an authorized personnel only after it has been recovered from theft or displaced for maintenance purposes. This anti-theft system will reduce theft cases related PV modules and reduce financial loss for society. The project has been presented at a conference and published in the conference proceedings for further system improvements by other researchers.

1.6 Dissertation Overview

The aims of this dissertation is to develop and evaluate a non-destructive anti-theft security system. The dissertation is organized as follows:

Chapter 1 discusses the essentiality of the project. It elaborates the problem and motivation to pursue the project, as well as the objectives of the project. Afterwards, it provides a bird's eye view of the system design and its block diagram to understand it in a better manner. Furthermore, it states the criteria to achieve the goal. The novelty and the scope of the project is highlighted in this chapter, and the contribution of the project towards the stakeholders is also prescribed.

Chapter 2 reviews the existing literature related to the project. The literature reviewed consists of theories, research papers, commercial products and patents on which the current systems are developed. It also presents a comparison of available products, technologies and methodologies, as well as the fundamental components used during the design and development phase. The basic mathematical calculations and architecture of wireless protocols are also discussed in this chapter.

Chapter 3 elaborates the methodology used to achieve the objectives. It provides a description of flow of a project that needs to be accomplished, and the major components of NODAS that are used during the development. This chapter also highlights the criterion for choosing the best available components for the project. Moreover, preliminary evaluation procedures and their findings, the problems faced during the design and development of the project and the approaches to solve it are highlighted in this chapter. Lastly, this chapter describes the software, hardware, wireless and security features used during the development of this project.

Chapter 4 presents the findings from the evaluation of different components, functionalities and NODAS as a whole. Furthermore, it details the tests conducted to ensure the reliability of components and NODAS and describes the sensitivity and tolerance of the project. This chapter also presents the results related to the robustness of the wireless functions.

Finally, Chapter 5 summarizes the project and deduce some conclusion out of it. The key innovations, the essentiality and outcomes of the project are also

illustrated in this last chapter. It also mentions the domain, limitations of the project and the findings of the experiments. In this regard, this chapter opens new horizons for researchers to make positive improvisations and remove discrepancies in the project.

CHAPTER 2

LITERATURE REVIEW

A literature review has been conducted prior to the design and development of this project. The literature reviewed comprised of research papers, patents, scholarly articles, books and commercially available products. Stolen PV modules have become prominent issues over the years and of researchers are working day and night to overcome theft issues. Consequently, researchers have produced numerous papers to solve the issue of theft in the fast growing industry of PV modules. Commercial organizations are also collaborating with academic research centers to develop the solution for the theft of PV modules as their investments are on stake too. Inventors are also contributing to the development of a viable solution. In this light, despite the commendable effort done by them, an economical and preventive solution has not been found until now.

For this study, theories, methods and experiments done by other researchers have been studied to avoid redundancy. The literature review has been very helpful in finding a novel solution to stop the theft of PV modules. The literature review is categorized into four sections, 1) Theories 2) Research papers 3) Commercial products and 4) Patents.

2.1 Background Study of Major Components

2.1.1 Photovoltaic Modules

Photovoltaic modules comprise up of various photovoltaic cells connected in series and parallel. The open circuit voltage V_{OC} is measured without connecting the load to PV cell while short circuit current I_{SC} is measured while creating a short circuit between positive and negative terminal of PV cell. The conventional PV cell shows an open circuit voltage of 0.6V. Voltages can be increased while connecting the PV cells in series while the current is increased when PV cells are connected in parallel (Walker, 2013). For series connection, the upper conductor of PV cell is connected with lower conductor of adjacent solar cell, as shown in Figure 2.1 below.

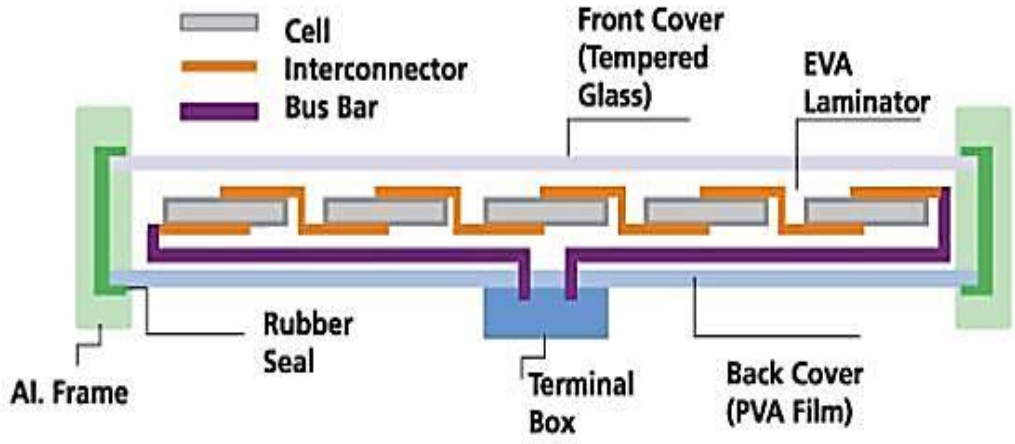


Figure 2.1: PV cells connected in series. Courtesy: Sanko Metal Industrial Co. Ltd.

2.1.1.1 IV Characteristics of PV Module

The IV curve of PV cell or PV array remains the same, however, as shown in Figure 2.2, its scaling is changed based on the number of cells connected in the series or parallel. Number of cells connected in parallel is indicated by ‘m’ while ‘n’ shows the number of cells connected in the series

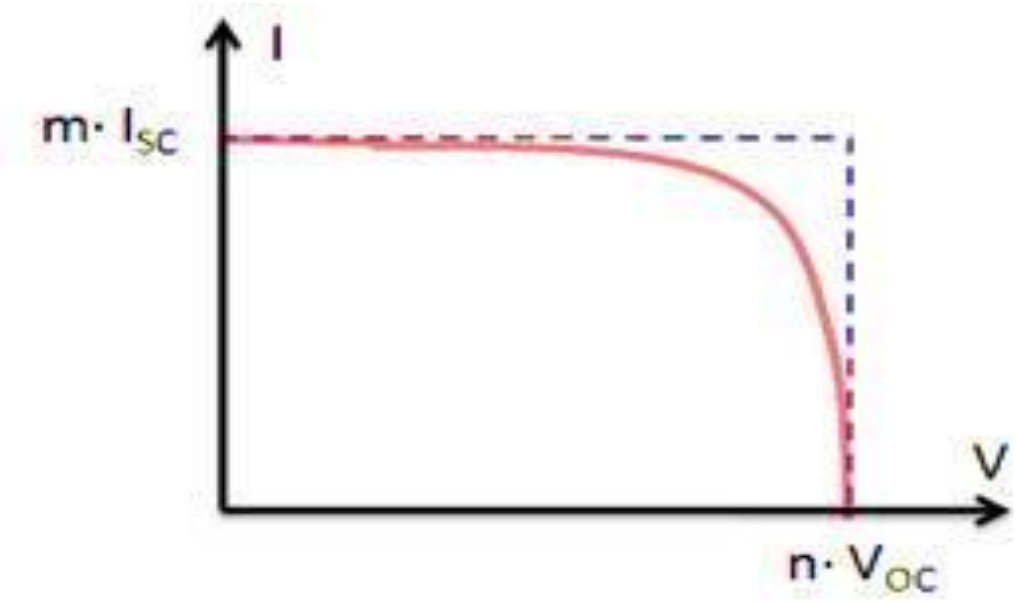


Figure 2.2: IV curve of PV module (Green, 2013).

V_{oc} is the open circuit voltage that reaches the maximum when the net current through PV cell or module reaches zero. On the other hand, the short circuit current I_{sc} reaches the maximum once the voltage across PV cell or module becomes zero, as illustrated in Figure 2.3.

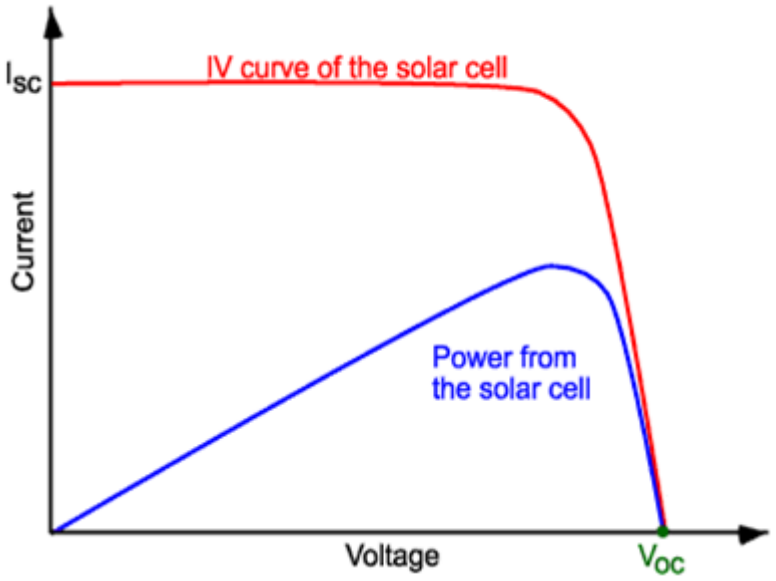


Figure 2.3: Short circuit current and open circuit voltage of a solar cell (Green, 2013).

The efficiency of PV cell can be calculated by using a simple equation shown below. Here, V_{mp} and I_{mp} denote the output power while P_{in} denotes the input power, which refers to sunlight. The fill factor, 'FF' represents the ratio of the output power to the product of V_{oc} and I_{sc}. It is used to estimate the non-linear behavior of the PV cell.

$$\eta = \frac{V_{mp}I_{mp}}{P_{in}} = \frac{V_{oc}I_{sc}FF}{P_{in}} \tag{2.1}$$

$$FF = \frac{V_{mp}I_{mp}}{V_{oc}I_{sc}} \tag{2.2}$$

In the meantime, the efficiency of PV module entirely depends on irradiation and temperature. So, maximum power point tracker MPPT is used to draw the maximum power from the PV module. Different techniques can be used

to track the maximum power point of the PV module. The maximum power point is illustrated in Figure 2.4.

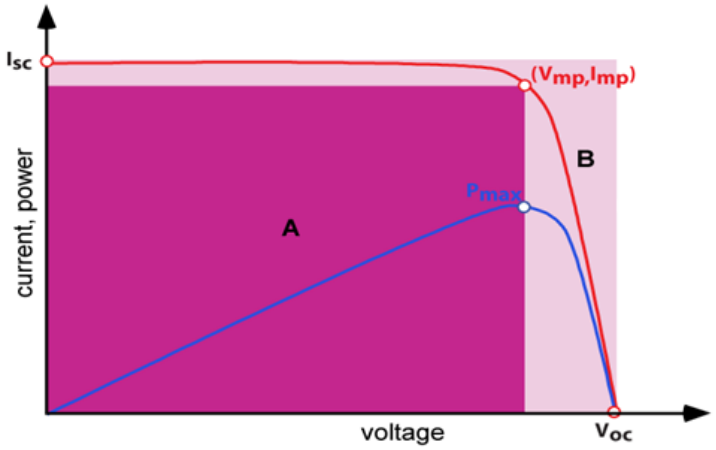


Figure 2.4: Maximum power point of a PV module (Green, 2013).

It is important to note that PV modules are very sensitive to temperature; the increase in the temperature of PV modules will cause a small increase to the short circuit current I_{sc}, and at the same time, it decreases the open circuit voltage V_{oc} as well as the fill factor, as shown in Figure 2.5 below. Consequently, the output power of PV module also decreases with the increase in temperature (Green, 2013).

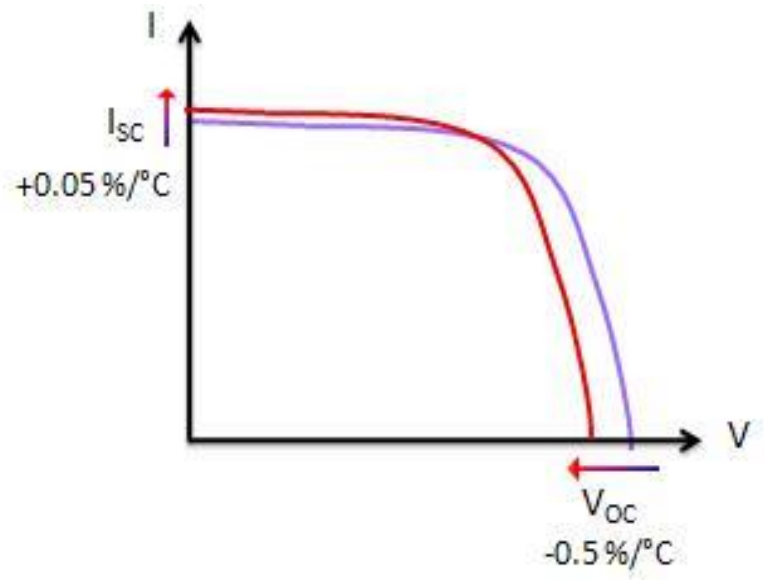


Figure 2.5: Temperature effect on PV module (Green, 2013).

2.1.2 Position Sensing

There are different sensors available in the market for position sensing. The Global positioning system (GPS) is the most common system for position sensing. However, GPS sensors are not very reliable because they could be affected by interferences and they rely on radio signals received by satellites. They need constant signals from satellites to keep track of the position of an object and as a result, GPS sensors consume more power during their operation.

A gyroscope is used to determine the orientation of an object. It is used for measure angular momentum. In this light, the reference of orientation will change as the orientation of the object changes. Hence, it is not suitable to be used for anti-theft application because thieves can bypass its system, making the PV module susceptible to theft. In some applications, an accelerometer is used together with a gyroscope for position sensing. This can be widely seen in cellular phones where

accelerometer and gyroscope sensors are used for orientation sensing and for gaming purposes, in addition to position sensing.

Tri-axes magnetometers are used to sense magnetic field in three different axes; these magnetometers are comprised of anisotropic magneto resistive sensors that detect magnetic fields in three different axes and convert them into differential voltages. These differential voltages are raw digital values that are converted into scaled values which are known as magnetic field values. These values are then stored in the micro-controller as reference positions. The heading angle can also be used for position sensing. The equations to calculate heading angle is shown below. (Honeywell, 1997)

If $y > 0$

$$\text{Heading Angle} = 90 - \tan^{-1}\left(\frac{x}{y}\right) \times \frac{180}{\pi} \tag{2.3}$$

If $y < 0$

$$\text{Heading Angle} = 270 - \tan^{-1}\left(\frac{x}{y}\right) \times \frac{180}{\pi} \tag{2.4}$$

If $y = 0$ & $x < 0$

$$\text{Heading Angle} = 180° \tag{2.5}$$

If $y = 0$ & $x > 0$

$$\text{Heading Angle} = 0° \tag{2.6}$$

2.1.3 Cut-Off Switch

A Cut-off switch prevents the flow of current to the load. Relays are also used for cutting off current supply, however, their size is not suitable to be used on PV modules because PV modules do not have the sufficient space to laminate the larger circuitry. Furthermore, a relay has a shorter life span due to its mechanical parts and it is impossible to replace any component after lamination of the PV modules. These components can downgrade the life expectancy of PV modules. In the meantime, a semiconductor-based cut off switch like a Metal Oxide Semiconductor Field Effect Transistor (MOSFET), is the best switch for the project as it is available in the SMD package. Furthermore, a MOSFET is a voltage-controlled device with a wide life latency as it has non-mechanical parts. There are few kinds of MOSFETs that are mentioned in the table below.

Table 2.1: Characteristics of depletion and enhancement type MOSFET (Theraja & Theraja, 2005).

V_{GS}	Depletion Type (Normally Closed)		Enhancement Type (Normally Open)	
	N Channel	P Channel	N Channel	P Channel
+ve	ON	OFF	ON	OFF
0	ON	ON	OFF	OFF
-ve	OFF	ON	OFF	ON

An N-channel enhancement MOSFET was used in NODAS. Normally, this kind of MOSFET is an open device by default. It requires 10V at the gate to fully drain the current. This control signal at the gate will be supplied by a micro-controller. Thus, the gate voltage should be sufficient to turn on the gate completely else or there would be power loss during the operation.

Power dissipation is another big issue as it could damage the PV modules. As mentioned earlier, due to space limitations, it is difficult to use heat sink in a PV module. Thus, calculating the power dissipation in MOSFET is important to develop a heat sink that is capable of sinking the heat without damaging the PV modules. Power dissipation is calculated by the mathematical equation shown below (Seshasayee, 2011).

$$P_{Dmax} = \frac{T_{Jmax} - T_A}{\Theta_{JA}} \qquad (2.7)$$

where:

Θ_{JA} = Thermal resistance

$\Theta_{JA} = \Theta_{JC} + \Theta_{CA}$

Junction to ambient = Junction to case + Case to ambient

T_J = Junction Temperature

T_A = Ambient Temperature

P_D = Power Dissipation (Seshasayee, 2011)

2.1.4 Microcontrollers

Microcontrollers are specific purpose mini computers that can be embedded to accomplish specific tasks with minimum hardware support. They have their own memory including ADC, DAC, serial I/O interface, parallel I/O interfaces. They only require an external clock to synchronize with external I/O devices (Dawoud & Peplow, 2010). Microcontrollers from different manufacturers including Texas Instruments, NXP Semiconductors, ST Microelectronics etc. were studied to filter out the best application.

However, microprocessors are deemed as more efficient than microcontrollers which need additional hardware supports, such as memory, ADC, Oscillators etc. to accomplish a task.

2.1.5 Wireless Technology

Wireless technology is used to reactivate the functionality of the PV modules once they are recovered after theft or after their locations were changed. Various technologies have been studied to find the best suited for anti-theft system. Figure 2.6 below presents a comparison of different wireless technologies in reference to distance range and data rate.

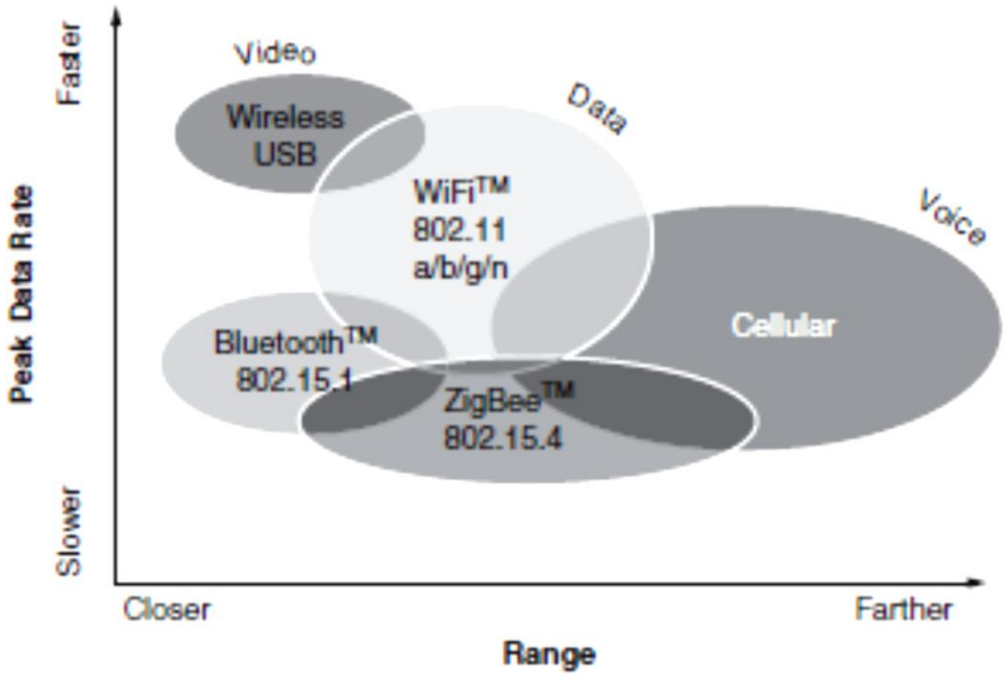


Figure 2.6: Comparison of different wireless technologies (Gislason, 2008).

Wireless technologies can be categorized into Wide Area Network (WAN) and Personal Area Network (PAN). WAN is used when communication over large distances is required while PAN is recommended for short distance communication. Satellite communication and telecommunication fall under WAN as communication spreads over a large distance.

PAN is recommended for solar farms as it does not require communication across a very large region. There are many new technologies related with PAN, such as Bluetooth, WiFi, ZigBee, IrDA, NFC etc. Table 2.2 presents several wireless technologies that fall under PAN.

Table 2.2: Features of wireless technologies (Gratton, 2011).

Technologies	Features
Bluetooth Recommended applications: Headsets, smart watches etc.	1Mbps data transfer rate 10m range Unlicensed spectrum 2.4GHz 60mA Tx mode Point to point communication Star topology Highly secured (Required pairing)
IrDA (Infrared Data Association) Recommended applications: TV, A/C, Fan, file transfer etc.	16Mbps data transfer rate 1m range No authentication required Point to point communication
Wi-Fi (Wireless Fidelity) Recommended applications: Internet sharing, files sharing etc.	11Mbps data transfer rate Up to 100m of range 2.4GHz & 5GHz Unlicensed spectrum 400mA Tx mode, 20mA Standby Point to multipoint communication Star topology Required authentication

NFC (Near Field Communication) Recommended application: Authorized access	0.1Kbps data transfer rate 5m range 13.56MHz spectrum Low power consumption Point to point communication
ZigBee Recommended applications: Home automation systems, WSN, ISM applications etc.	250Kbps data transfer rate 10 to 100meters 2.4GHz Unlicensed spectrum 25 – 35mA Tx mode, 3µA Standby Point to multipoint communication Mesh topology Untethered

2.1.6 ZigBee

ZigBee is an enhanced version of the IEEE 802.15.4 standard. ZigBee is best suited for home automation systems that only require monitoring and control. It consumes very less power as ZigBee will remain in an idle mode most of the time, unless it is interrupted to perform any operation. ZigBee is used for simple monitoring and control so it does not need much bandwidth so it could work efficiently with low data transfer rate.

Each node can be act as Full Function Device (FFD) or Reduced Function Device (RFD) in any network. In a ZigBee network, FFDs are referred as ZigBee coordinator that can communicate with any other devices in a network. ZigBee

routers are also FFDs and are responsible for routing. in a ZigBee network, RFDs are referred as ZigBee end device which can communicate only with the network coordinator. However, ZigBee end devices can only be used in star topology (Kumar, Sharma, & Grewal, 2014).

Unlike its counterparts, ZigBee is not affected by interference, making it highly reliable . In this light, ZigBee will auto-discover the shortest path to transmit data if there is any broken link between the two nodes, and has the ability to self-heal. The transmission range also gets extended in ZigBee using multi-hoping and multiple number of nodes can be deployed under star, mesh and tree topology.

ZigBee uses Carrier Sense Multiple Access Collision Avoidance (CSMA) to avoid collision while transmitting data. It checks the line before transmitting any data to ensure that the line is free at and to avoid collision of transmitted data. Furthermore, the packets sent from ZigBee consist of frame checksum (FCS) that assures the correction of data bits. Lastly, ZigBee achieves higher reliability and efficiency as it uses mesh topology and acknowledgements in a network.

2.1.6.1 ZigBee Architecture

ZigBee has almost the same architecture as the Open Systems Interconnect (OSI) layer network model, except the upper five layers (application, presentation, session, transport & network), which is covered in the ZigBee model i.e. ZigBee Device Object (ZDO) & Application Support (APS). Meanwhile, the lower layers physical (PHY) and medium access (MAC) layers are defined by Institute of

Electrical & Electronics Engineers (IEEE). The Service Access Point (SAP) separates each layer in ZigBee architecture where an SAP is used for data, while the other is used for management. ZigBee application consists of four frames in a packet; the differences in the OSI layer model and the ZigBee architecture can be seen in Figure 2.7.

1) MAC frame
    - Each MAC frame comprises of 16 bits.
    - The MAC is responsible for creating unique personal network.
    - It also contains information of nodes regarding acknowledgements and network formation.

2) NWK frame
    - The NWK frame also consists of 16 bits.
    - It contains information about multi-hop communication.
    - It establishes the mesh networks.
    - It is responsible for sending packets over a network and ensures that each packet is transmitted and received successfully.
    - The security is also implemented through the NWK frame.

3) APS frame
    - APS frame consists of 8 bits.
    - It is responsible for successful transmission between different applications i.e. applications of controlling device and controlled device.
    - It is responsible to filter duplicate messages.

- It is responsible to maintain data and transmission details of each node.

4) ZCL frame

- ZigBee cluster library consists of all functions for building ZigBee applications and profiles.
- An example of ZCL is the On/Off cluster for home automation application and Fan On/Fan Off for the HVAC systems.

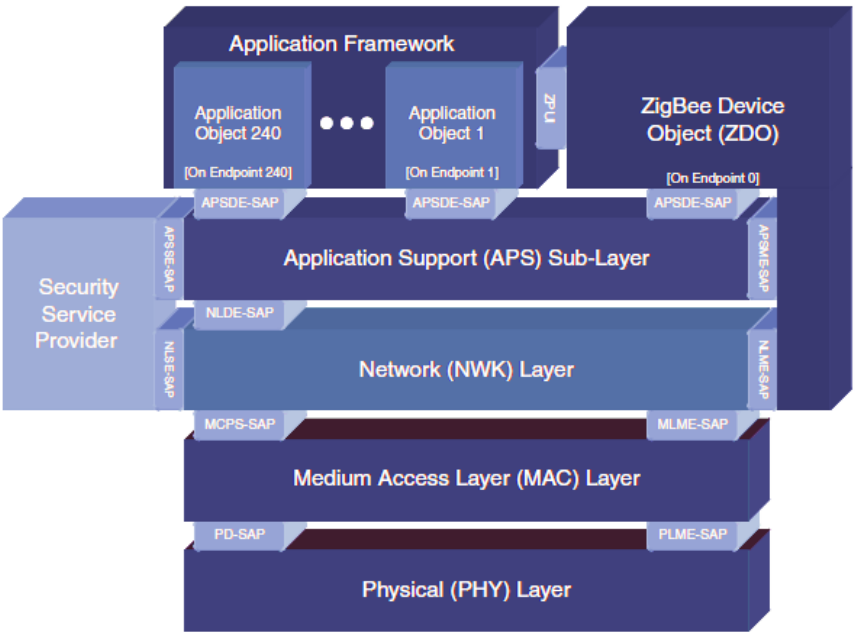


Figure 2.7: OSI layer model and ZigBee architecture (Gislason, 2008).

2.1.6.2 ZigBee Security

The nodes can only join the ZigBee network after they are validated by the coordinator. A common key is established to join a network, while each node has its own unique key for distinguishing the nodes. ZigBee uses the Advanced

Encryption Standard (AES) algorithm to secure the network from intruders (Gratton, 2011).

2.2 Research Papers

2.2.1 Power Monitoring of PV Module

Some researchers have proposed continuous monitoring of generated power and any unexpected drop in power is considered as theft. However, this unexpected loss of power can also be caused by malfunctioning which needs to be rectified to avoid power supply interruption . In this light, these solutions can solve the issue of theft, as well as of equipment malfunction. Visconti & Cavalera (2015) designed an electronic system to monitor efficiency of PV modules locally and remotely. The system detects malfunction and theft of PV modules by monitoring their efficiency. Different sensors and sun tracker are used to retrieve various parameters. The efficiency of the system is calculated and monitored consistently. The sudden drop of power is considered as theft, while progressive drop of power is considered as PV module malfunction.

2.2.2 Wireless Sensor Networks (WSN)

It is beneficial to use the wireless sensor networks (WSN) as they comprise of a number of sensors that are used to collect real-time data before they are passed to the central control unit for decision making. Bertoldo et al. (2012) designed an ad-hoc wireless sensor network to tackle theft issues in photovoltaic industry. In

this work, each PV module is equipped with an accelerometer that detects displacement in a PV module from its steady position. Computer generated short messages, e-mails and audial/visual alarm signals will be transmitted once the displacement exceeds the tolerance value. Here, the master and slave nodes communicate over the radio frequency link while the master transmits the signal to the computer via a serial communication link.

2.3 Commercial Products

Commercial organizations have realised the sensitivity of theft issues occuring in the PV industry as it brings financial costs to stakeholders. Consequently, corporate sectors are commissioning their research and development department to find a solution to the theft issues. They have been trying to develop new approaches to protect their products from theft. Some of their innovations are discussed below.

2.3.1 Tigo Energy

Tigo Energy (2015) introduced the smart PV modules with preinstalled security and monitoring system inside the junction box. These smart PV modules can be monitored and shut-off locally and remotely in the case of any emergency. These PV modules are used to connect in a string that passes through Tigo's monitoring unit. When there is an unexpected drop in power, the system will immediately send an alert to the authorities which activates locally connected devices such as lights, sirens or cameras to deter theft. However, the PV module

with monitoring system in the junction box can be tampered and can be installed to other sites. The system can be bypassed and the stolen PV modules could not be recovered. Moreover, the anti-theft system requires additional systems such as GPRS/GSM to alert the authorities, and as a result, this anti-theft solution is system based and does not tackle theft effectively.

Figure 2.8: Junction box of Smart PV module. Courtesy: Tigo Energy.

2.3.2 Solaris Energy Systems

Researchers working in Solaris Energy Systems Ltd. have introduced an innovative mechanical fasteners design which attaches two PV modules, as shown in Figure 2.9. This unique mechanical fasteners design require special tools and skills for them to be installed and dismantled, making it hard and time-consuming for these mechanical fasteners to be tempered. These special fasteners are named as Akraboot 4 which compose of three different blocks screwed together. A fiber

optics cable passes through each fastener and ends at an optical sensor.This optical sensor will continuously detect optical signals, while an alert will be sent to authorities when there is an attempt to remove or tamper the fasterners(Akraboot System, 2009). Akraboot fastens the PV modules together in such a manner that the removal of each fastener is very time consuming which demotivates thieves to enter these sites.

Figure 2.9: Akraboot 4. Courtesy: Solaris Energy Systems Ltd.

2.3.3 A Narnia Security

A Narnia Security previously known as Luceat, has offered a solution to protect PV modules from theft. Figure 2.10 shows special fasteners attached to each PV module and a plastic fiber cable, known as LiteWIRE, as shown in Figure 2.11 passes through each fastener and ends at the LiteSUN analyzer. A LiteSUN analyzer acts as a transceiver that generates and receives light signal through LiteWIRE. A LiteSUN analyzer detects bending and cutting of the LiteWIRE by

comparing incident and reflected light signal. A LiteSUN analyzer supports fiber optic cables which are approximately 300m in length, beyond that another LiteSUN is needed to be installed. A fiber optic cable can be start or end at the same LiteSUN device or the orientation can be change to increase distance covered by the anti-theft system using the multiple LiteSUN devices as shown in Figure 2.12 and Figure 2.13 (Naria Security, 2016).

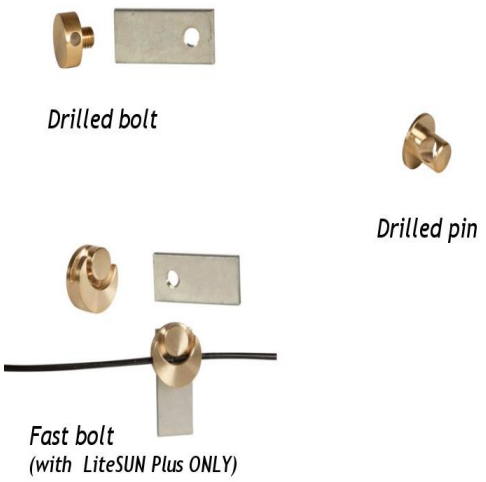


Figure 2.10: Mechanical fasteners. Courtesy: A Narnia Security.

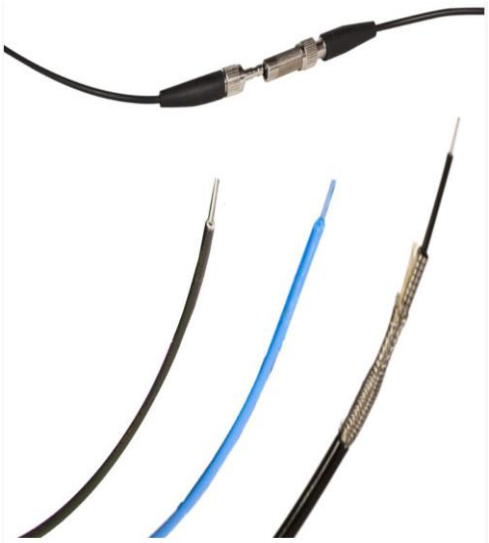


Figure 2.11: LiteWIRE Fiber Optic Cable. Courtesy: A Narnia Security.

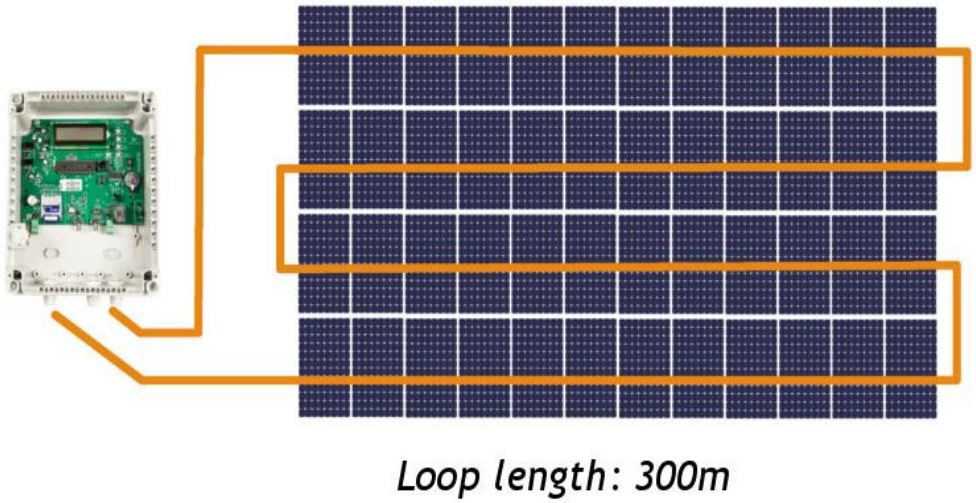


Figure 2.12: LiteWIRE and LiteSUN analyzer. Courtesy: A Narnia Security.

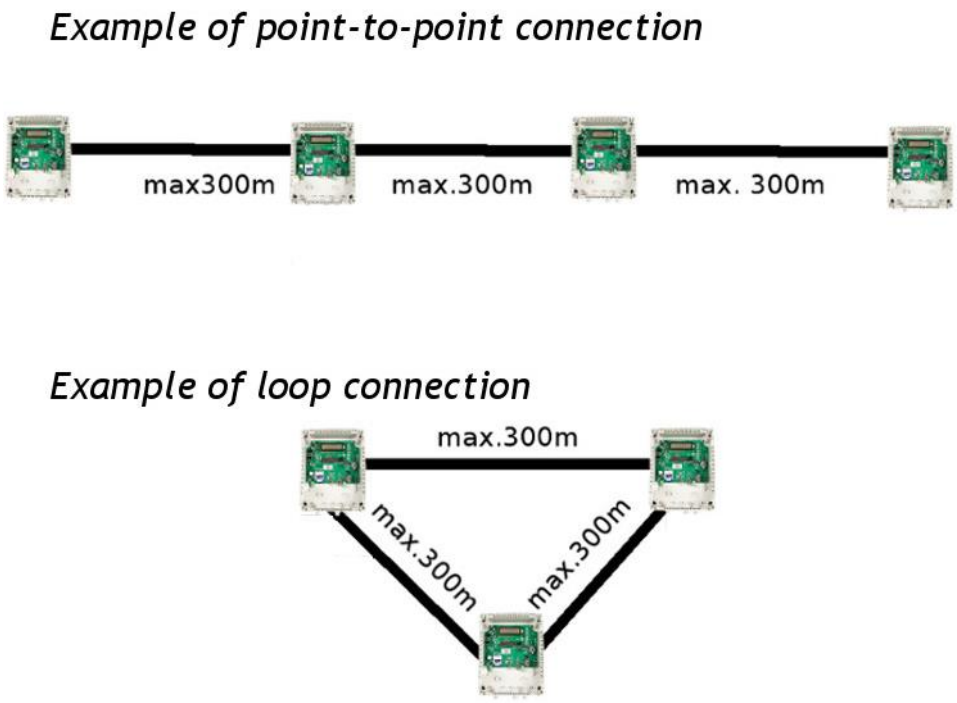


Figure 2.13: Different orientations to implement security system.

Courtesy: A Narnia Security.

2.3.4 SolteQ Europe

SolteQ was developed as an anti-theft solution for PV modules by using angle sensors that are connected to the central station via data cable. Each angle sensor has a unique identification and can be attached or tied to the PV module. Each sensor will be monitored periodically by a central station. An alarm signal will be transmitted when the angle sensor detects that the data cable was cut or when there is any unexpected twist. It also provides an option to count the modules before sending an alert signal to prevent it false alarm. This anti-theft can also be installed on fence poles around premises and will transmit an alert signal to the authority when it senses any trespassing and tampering. The company has also used close circuit television (CCTV) to monitor the PV modules and inverters (Berkay,

2013). The central station and angle sensor produced by the company is shown in Figure 2.14 below. The central station also has a wireless function to alert authorities.

Figure 2.14: The angle sensor and central station.
Courtesy: SolteQ Europe GmbH.

The anti-theft solutions from Solaris systems, Naria security and Solteq are quite similar as all of them are based on fiber cables that pass through each PV module and unexpected change in an optical signal is detected by the optical sensor. In this regard, it is important to note that these systems are not a complete solution as they only generate alarms/ signals to alert the authorities. These commercially available solutions are costly and require additional assembly procedures, especially for large-scale implementations. They also require additional power during implementation due to the need for continuous monitoring. This could generate higher power consumption and increase system cost even though they could not rectify the theft completely. Moreover, it is impossible to recover back the stolen PV modules once the system is bypassed.

Table 2.3: Comparison of different commercial solutions.

No.	Organization	Placement	Features	Technology	Discrepancies
1.	**SMART PV MODULES** Tigo Energy	Junction Box	• Monitoring • Security • Controlled locally and remotely. • Auto-shut off.	• GPRS/GPS.	• Additional cost required for GPRS/GSM. • Tampered easily.
2.	**Akrabot 4** Solaris Energy Systems	Frame of PV module	• Mechanical fastener. • Detects unusual movement or removal	• Optical sensor. • Fiber optics.	• Additional equipment is required to alert authorities. • Can't recover after theft.
3.	**A LiteSUN analyzer and a LiteWIRE** A Narnia Security	Frame of a PV module	• Mechanical fastener. • Detect bends and cutting of communication medium.	• Optical sensor. • Fiber optics.	• Additional equipment is required to alert authorities. • Can't recover after theft. • Limited to certain number of PV modules.
4.	**Solteq DSS** Solteq Europe GmbH	Frame of the PV module	• Detects unusual movement and twist. • ID based sensor is queried by central station. • Monitoring.	• Movement & angle sensor. • GSM.	• Swift action required to stop theft. • Numbers of armed officials required to tackle thieves. • Additional cost is required for equipment. • Can't recover after theft.

2.4 Patented Anti-Theft Solutions

Muhlberger & Protsch (2013) patented a solution for theft recognition of PV module. The anti-theft system resides in an inverter and the model of the anti-theft device is shown in Figure 2.15. The generated power from PV array is analyzed by a signal unit. The control unit is responsible to switch over the generated power. In this light, the power would not be fed to the consumer if the signal unit detects any deviation in expected generated power. A microcontroller or microprocessor acts as a control device to switch the alternating current (AC) or direct current (DC) supply to the consumer using DAC or DC-DC converter. Consequently, the data communication device will send an alert signal to the authorities in any case of theft.

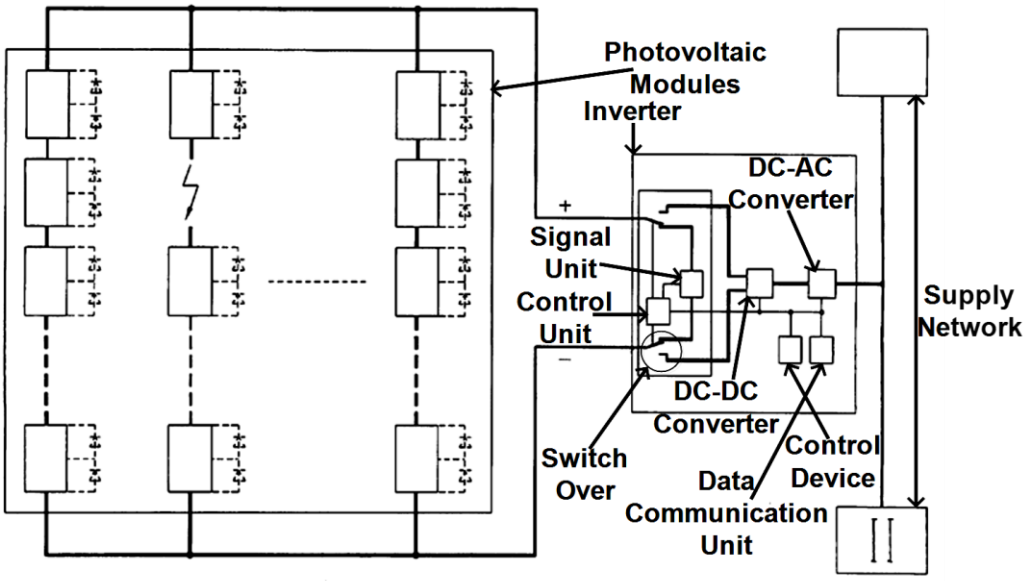


Figure 2.15: Schematic design of anti-theft model (Muhlberger & Protsch, 2013).

This model does not need any additional circuit for PV modules as theft is detected by the inverter. However, as this method is implemented on the system level instead of on the module level, the modules can be reused anywhere after they were disconnected. In this regard, this method is not preventive because the generated power varies from day to night and it is difficult to detect whether the deviation in power is caused by theft or variation in irradiance. Additionally, most solar farms are located in rural areas and the authorities need time to take action against thieves.

Sacchetti (2014) patented another unique solution to tackle theft issues. Electromechanical fasteners are used to fasten the junction box to the PV module. These fasteners are composed of axially hollow irreversible couplers that connect junction box and PV module mechanically and electrically. These fasteners and electrical contact will be broken if someone tries to detach junction box from PV module. The junction box consists of printed board assembly card. This electronic card in the junction box remains in wireless contact with external control unit that is physically connected to the personal computer (PC) to receive information. As this control unit also possesses a geo-referencing function, the alert signal is fired upon deviation in the distance between PV module and control unit. The removal of junction box will be detected by a control unit that generates an alert signal through the PC.

The PBA card is powered by PV module itself. The card , which consists of RFID reader tag, will read the information written on RFID tag attached to the PV

module. This shows that the specific junction box works for specific module only. Thus, besides the electromechanical fasteners, the anti-theft system also implements radio frequency identification. The invented anti-theft system is shown in Figure 2.16 below.

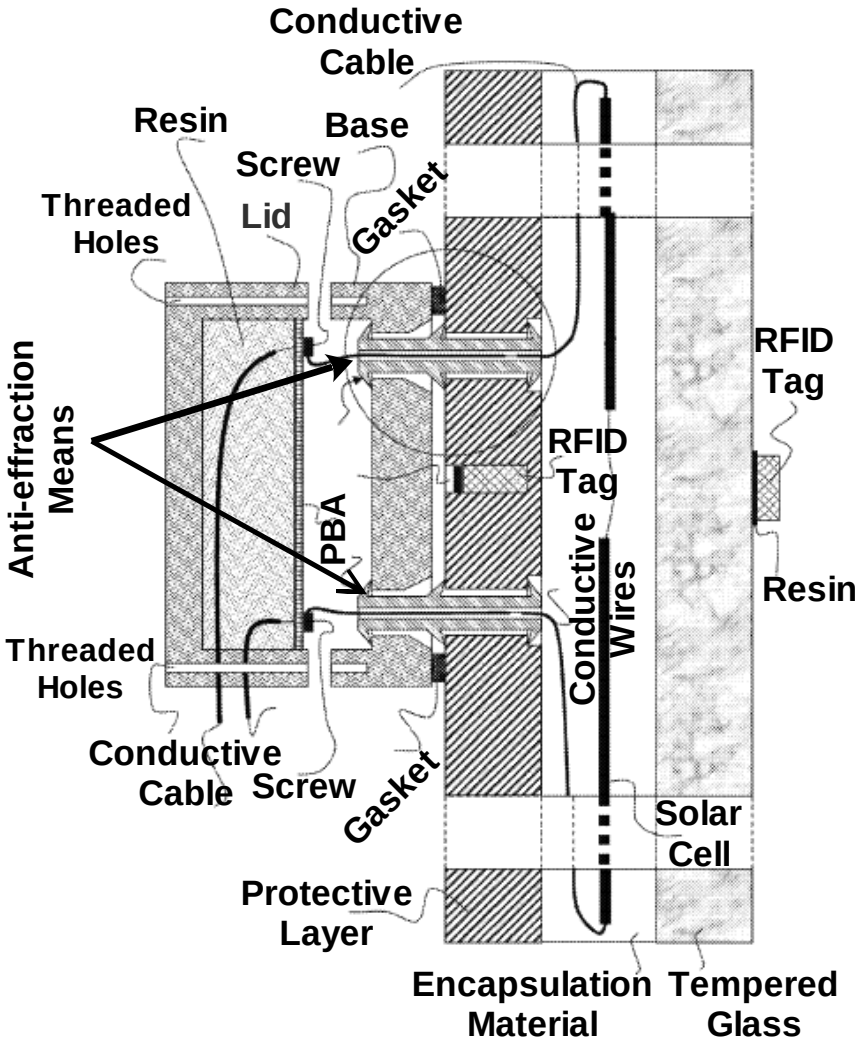


Figure 2.16: The anti-theft system for PV module (Sacchetti, 2014).

This anti-theft system has demonstrated impressive functions. However, similar to most other systems, the PV modules cannot be reused again even if they

are recovered back. As the PBA board in the junction box is powered by the PV modules, it requires significant power for additional security circuits and for continuous pooling by the external control unit. Additionally, this anti-theft system requires a complete setup of external devices which makes its implementation complex and expensive.

Goldack (2013) invented another model to secure PV module from theft. This model involves ‘handshake’ type scenarios before power is transferred to the load. In this model, a device that disables and enables power transfer is attached to the module end and consumer end respectively. The solar cells powered disabling device is embedded in the PV modules. It generates a specific pattern of a signal with the help of transistors and logic circuits. This specific signal is transferred to the enabling device at the consumer end via the same power transfer cables. If the received signal is acknowledged by the enabling device, then it will return the acknowledgement signal to the disabling device to allow power transfer to the consumer. However, if the enabling device at the consumer end does not recognize the received signal and does not return the acknowledgement signal, then the disabling device will not allow power transfer to the consumer. The invented model is shown in Figure 2.17.

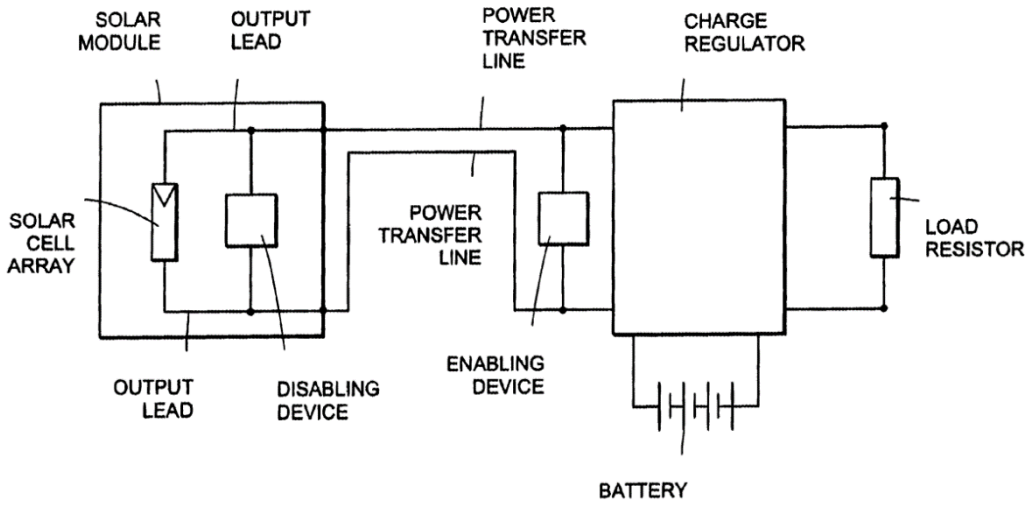


Figure 2.17: An anti-theft model (Goldack, 2013).

This model is quite impressive. However. it is only feasible with a small number of PV modules and small-scale installations. Meanwhile, it will be very complex to implement this system on large scale installations, for instance, it will be harder for the PV modules to communicate with enabling devices in a solar farm with a large number of PV as each PV module needs to have its own unique signal pattern and it is not feasible to feed all these patterns in real-time. Moreover, if the PV module is in the state of shut-off mode, the transistor will dissipate energy that can damage the embedded circuit, and inventor did not address the issue of heat dissipation. It is difficult to implement that kind of setup because solar farm has large number of PV modules and communication among PV modules and enabling device will become so complicated. Each PV module need have its own unique signal pattern and it is not feasible to feed all these patterns at a real-time.

The existing literature shows that there is a wide gap that needs to be filled to overcome theft of PV modules. In this review, we have chosen the most suitable methods, solutions, research papers and patents that can be applied to tackle theft issues effectively. It is revealed during literature review that the solution should not be system-based where it should not rely on auxiliary systems to accomplish the task. This is because auxiliary systems can be bypassed by intruders and there is no chance to recover back the stolen PV modules.

After going through available literature, it can be concluded that the modular based system will be more effective and preventive as it stands alone and does not require integration with any additional system to accomplish the task. Lastly, module-based anti-theft system cannot be tampered with, and it will not work after that. This could discourage thieves as there is no point to steal a PV module that will not work.

CHAPTER 3

METHODOLOGY

A modular based anti-theft system is developed to secure a PV module from theft activities. This anti-theft system is a complete standalone system that does not require external power for operation. Furthermore, it is modular based and can be embedded inside the PV module. This anti-theft system is named **NO**n-**D**estructive **A**nti-theft **S**ystem (NODAS). This system is non-destructive that requires unique credentials from authorized personnel to reset it. For this study, a prototype has been developed to prove the feasibility of the concept.

3.1 System Criteria

- The operation of PV module is controlled automatically and cannot be reactivated once it is stolen, hence, it can be sold to a new customer.

- The position sensor will be embedded inside a PV module and the power would be supplied through specially designed interconnections within the PV module. Hence, the PV modules need to be removed or reactivated which will the consequently destruct the PV modules.

- The PV module can only be reactivated by authorized personnel through a wireless controller.

- NODAS is non-destructive in nature as it can be reactivated after it is recovered from theft or removed for maintenance purposes.

- NODAS comprises of low power components and do not require any additional battery as the power will be supplied by the PV modules itself.

- It only operates at daytime and this could save the power consumption.

3.2 System Design

NODAS, or **NO**n-**D**estructive **A**nti-theft **S**ystem is designed to solve theft problems in solar power plants. It is designed and developed to be readily embedded inside PV modules, i.e., at the module level. It is impossible for thieves to access this security system and the PV modules will not generate any power once removed from their original position making it useless to steal these PV modules. NODAS comprises of three main blocks, 1) A position sensing block, 2) An auto shut off switching block and 3) A microcontroller with a wireless function block. Block diagram of NODAS is shown in Figure 3.1. NODAS detects the position of the PV module and stores it as a reference position in a microcontroller. The microcontroller keeps on comparing the instantaneous position with the reference position. The auto shut off switch is controlled by the microcontroller that shuts off the power supply of the PV module upon the mismatch between the instantaneous positions with the reference position. A Wireless communication system is used in NODAS for re-activation of the PV module and this has made the system non-

destructive. A unique key is required to reactivate the power supply in the case of reinstalling the PV module to another site or if it is recovered after being stolen.

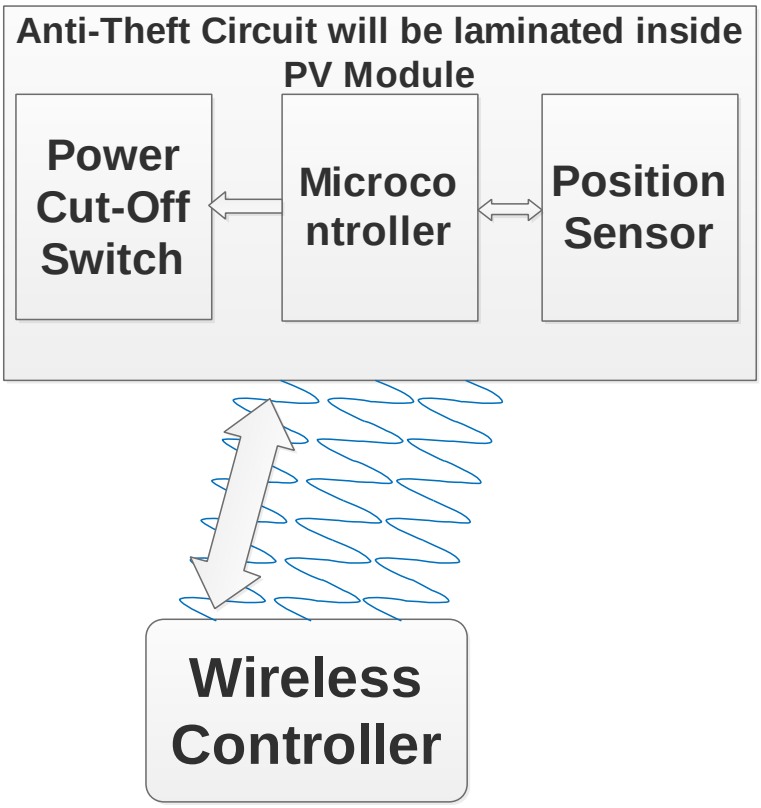


Figure 3.1: Block diagram of main components of NODAS.

The cost and power consumption of NODAS has been taken into serious considerations during the design and development process. Firstly, NODAS' circuitry needs to be economical because further increment in the price of PV modules will demotivate the consumers to buy PV modules with built-in security system. Second, as high power consumption will ultimately reduce the power at the supply end, components used in NODAS should consume less power. Moreover, an innovative algorithm stored in a microcontroller allows the anti-theft system to operate only during the daytime to reduce power consumption. It is also important

to mention that even though the system is only operating during the daytime, this does not demolish the function to prevent the module from theft. This design does not necessarily stop people from stealing PV modules, but it demotivates thieves in the long run as a stolen module will not be functional once it is relocated to a new unauthorized place.

3.3 Constituents of Methodology

The methodology involves all major components of NODAS, as shown in Figure 3.2. These main blocks are 1) Position sensor 2) Shut off switch and 3) A microcontroller. As each component has its own importance in accomplishing this project, all of them have gone through stringent selection criteria to avoid any shortcomings during its development. A position sensor is used to retrieve the position of a PV module before sending it to a microcontroller, subsequently, the microcontroller stores this initial position and keeps track of the instantaneous position of the PV module which will be matched with the initially stored reference position. A power shut-off switch is controlled by a microcontroller to cut-off power to the load when there is a mismatch between the reference and the instantaneous positions.

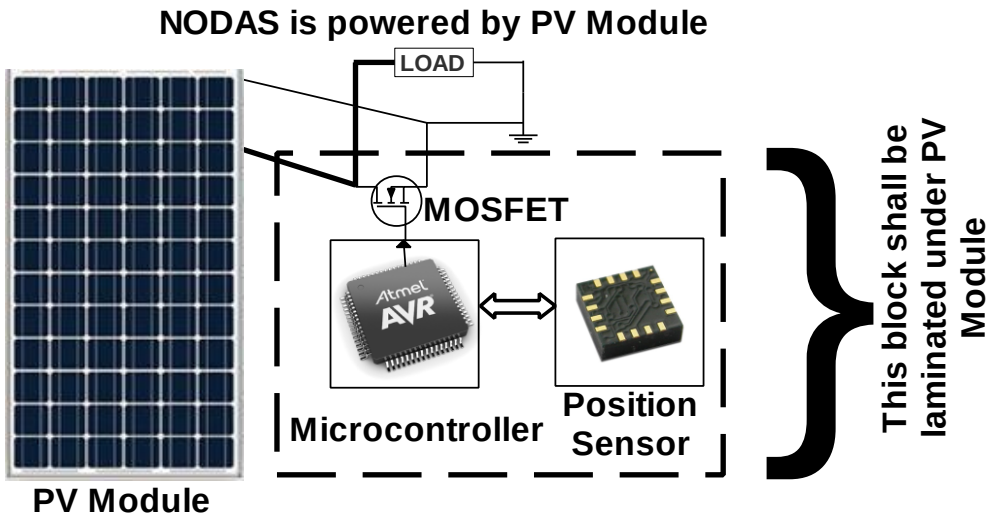


Figure 3.2: Schematic diagram of NODAS.

3.4 Position Sensing

Position sensing is considered as a major parameter to track down theft. The position of a PV module will be retrieved using a position sensor and stored in a microcontroller. In this light, the microcontroller also relies on a position sensor to determine whether the power to the load should be shut off. HMC5883L from Honeywell is used for position sensing in NODAS. As shown in Figure 3.3, the position sensor used during development is modular based, instead of chip based. As the project is developed to prove the validity of the concept, so the small-scale development of prototype will not be put under the scope.

Figure 3.3: HMC5883L in GY-273 module.

Position sensing is accomplished using a magnetometer, which detects magnetic fields that create differential voltage at three different axes. These differential voltages are in raw values which will be converted into scaled values to identify any magnetic field sensed in each direction. These scaled values are stored in a microcontroller. This form of position sensing is more reliable as all three axes are considered and it is nearly impossible to duplicate all three values at different locations. The raw and scaled values retrieved from the position sensor are shown in Figure 3.4 below.

```
Starting I2C Interface
Constructing New HMC5883L
Setting scale to +/- 1.3 Ga
Raw:    185   -226   -89        Scaled: 170.20   -207.92   -81.88
Raw:    189   -236   -90        Scaled: 173.88   -217.12   -82.80
Raw:    188   -235   -85        Scaled: 172.96   -216.20   -78.20
Raw:    185   -237   -89        Scaled: 170.20   -218.04   -81.88
Raw:    182   -235   -87        Scaled: 167.44   -216.20   -80.04
Raw:    185   -234   -87        Scaled: 170.20   -215.28   -80.04
Raw:    187   -234   -89        Scaled: 172.04   -215.28   -81.88
Raw:    186   -232   -93        Scaled: 171.12   -213.44   -85.56
```

Figure 3.4: The output of magnetometer shows raw and scaled values.

3.4.1 Selection Criteria of Position Sensor

After employing the selection criteria, the HMC5883L is found to be very appropriate for this project. The factors considered during the selection of a component are shown in Figure 3.5 below.

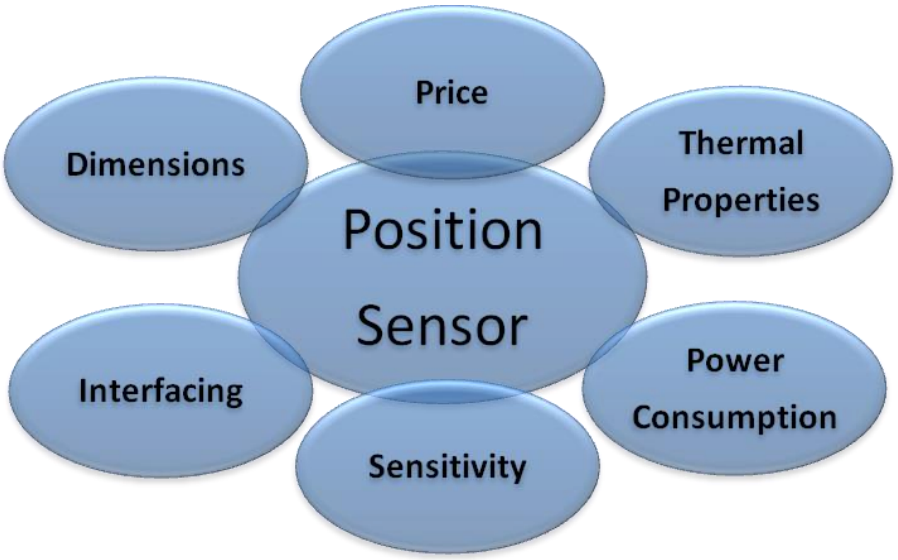


Figure 3.5: Criteria for selection of position sensor.

As PV modules are still very expensive, the components used for NODAS must be very economical. This is because the use of expensive components will consequently increase the cost for the PV modules that will demotivate consumers from buying PV modules with built-in security system. The price of selected position sensor is around 25MYR per unit and purchasing them in bulk will reduce the price.

NODAS is developed to laminate inside a PV module. In this regard, the module can go through the lamination process without any destruction as the position sensor used for NODAS can sustain temperature up to 125°C.

A solar farm consists of hundreds of PV modules which entails the security system to have minimal power consumption. The selected position sensor draws 2µA of current during idle mode and 100µA of current during the measurement mode, hence, the power consumed by position sensor is 7.2µW in idle mode while 360µW in measurement mode.

The position sensor is very sensitive as it is affected by magnetic field lines, which in turn, can be easily influenced by electromagnetic waves. For NODAS, the value of magnetic flux is retrieved at a particular location under the influence of magnetic field of surroundings and stored in a microcontroller. So, the position is considered as a displacement of PV module once the value of magnetic field is changed beyond the tolerance value. The PV module shut-off its power generation upon the displacement of a module, as well as when there is any disturbance created by a magnetic or ferrous material.

The position sensor used for NODAS has the simplest communication interface i.e. I2C. Only two wires are needed for communication with microcontroller, as shown in Figure 3.6.

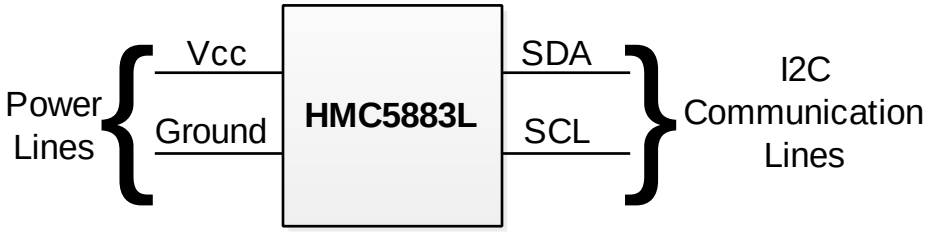


Figure 3.6: HMC5883L wiring schematic.

Meanwhile, as the PV module does not have any free space for additional circuit, the miniature components are used for NODAS; the HMC5883L comes in a 3mm×3mm×0.9mm (length × width × depth) of surface mount chip package. This can be easy be laminated inside the PV modules.

The HMC5883L has a built-in 12 bit analog to digital converter (ADC) that achieves 2mG of field resolution in full scale ±8 Gauss range, hence, it can detect 4096 discrete analog levels. The ADC to voltage value can be converted using expressions below.

Conversion of ADC value to voltage value

$$\frac{\text{Resolution of ADC}}{\text{System Voltage}} = \frac{\text{ADC reading (x)}}{\text{Measured Voltage}} \qquad (3.1)$$

Resolution of 12-bit ADC conversion 2^{12} = 4096 (Discrete levels of analog value)

So, equation 3.1 becomes

$$\text{Analog measured voltage} = \frac{4096}{\text{System voltage (5V)}} \times \text{ADC reading (x)} \qquad (3.2)$$

Or

$$\text{ADC reading}(x) = \frac{4096}{\text{System voltage}(5V)} \times \text{Analog measured voltage} \qquad (3.3)$$

The value of ADC can be determined using the equations mentioned above. Here, the default value for sensor field in the MC5883L is ±1.3 Gauss which could be increased up to ±8.1 Gauss accordingly. The gain settings are recommended to avoid issues related to register overflow.

3.4.2 Heading Angle Calculations

The heading angle is used for position sensing. It requires the calibration of magnetometer every time because the electromagnetic interference varies at different locations. The magnetometer needs to be rotated to capture the electromagnetic interference around the magnetometer and offset what required to be resolved to obtain the actual magnetic interference at a particular location. The heading angles can be calculated using Equations 2.3, 2.4, 2.5.and 2.6 and the pseudo code of magnetometer is stated in Appendix C. Consequently, the PV modules will not deliver any power to the load once they are displaced from their original position as the changes of magnetic field considers as the change in the position of PV module.

3.4.3 Integration of Position Sensor with Microcontroller

The position sensor is integrated with a microcontroller for further decision making. The position sensor retrieves the position and sends it to the microcontroller. The Arduino UNO kit was initially used to observe the behavior

of the position sensor. The position sensor is interfaced with a microcontroller using two wire interface (TWI), as shown in Figure 3.6 and Figure 3.7.

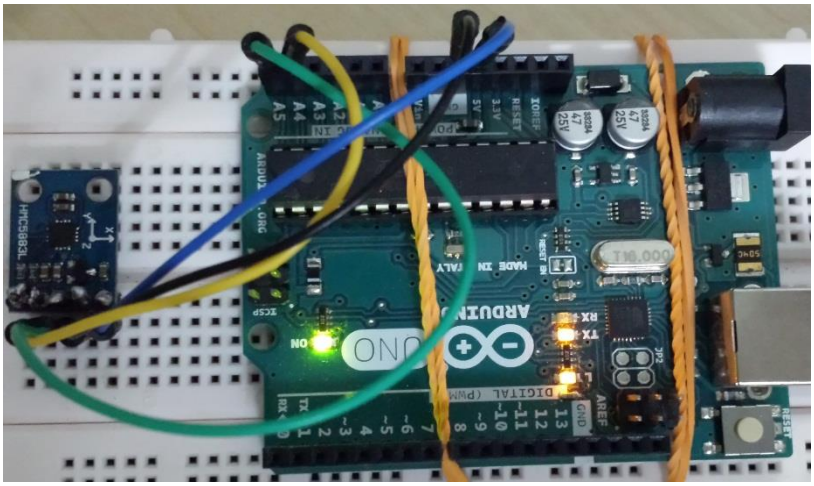


Figure 3.7: Magnetometer attached with Arduino Uno for testing.

3.5 A Cut-off Switch

A semiconductor based MOSFET (IRF640N) from International Rectifier is used in NODAS to interrupt the power supply to the load. The microcontroller sends a signal to the gate of MOSFET to cut-off the supply. The MOSFET is integrated with the Arduino UNO and position sensor for evaluation.

3.5.1 Selection Criteria of a Cut-Off Switch

The anti-theft circuit will be laminated inside PV module. The lamination will make it impossible for the components to be replaced without removing the lamination and will permanently destruct the PV module. In this light, the criteria for each component has been followed strictly to develop a robust system. The MOSFET is selected based on the criteria shown in Figure 3.8.

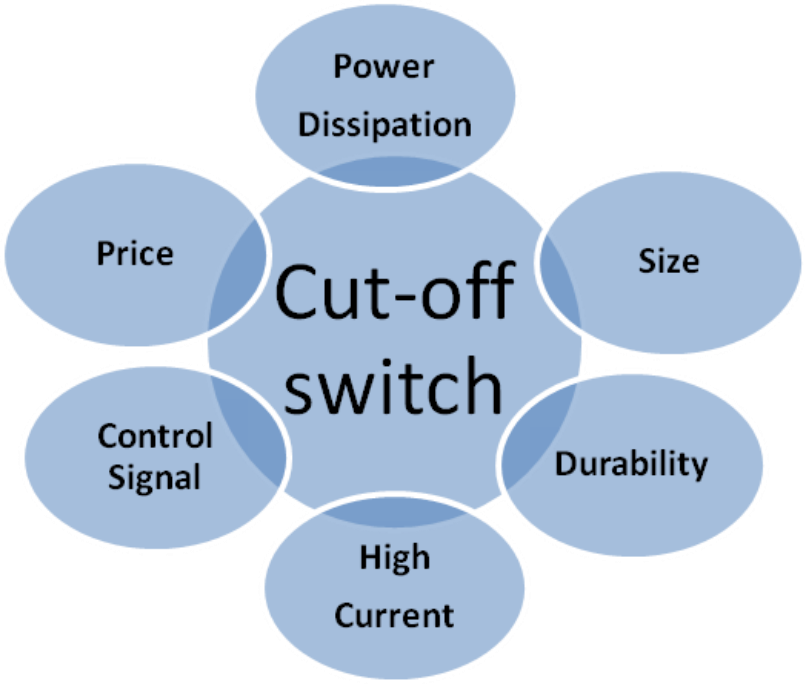


Figure 3.8: Selection criteria of cut-off switch.

The power dissipation of a cut-off switch is considered in selecting the best switch. Excessive power dissipation of MOSFET can damage the NODAS as well as the PV modules. The maximum current delivered by the PV module is assumed as 9A. Then according to datasheet, the MOSFET has 0.15Ω of drain to source resistance. So, a MOSFET dissipates maximum of 12.15W at 9A as calculated in Equation 3.4. The heat sink is required to handle that dissipated power to ensure that the NODAS and PV module would not be damaged by the dissipated heat.

$$P = I_D^2 \times R_{DS(on)} = 9^2 \times 0.15 = 12.15 \text{ W} \quad (3.4)$$

As NODAS will be laminated inside the PV modules. It is important to keep in mind that the PV modules have limited space, hence, the dimension of components should be kept small and minimal. MOSFETs are used in NODAS

instead of relays. Relays contain mechanical parts and can easily cause fatigue, meanwhile, as the MOSFETs do not contain any mechanical parts, they are more durable compared to other mechanical switches. MOSFETs are available in SMD packages and the dimension of each SMD based MOSFET is 16mm×10mm×5mm (length × width × depth).

According to the datasheet of IRF640N MOSFET, it can sustain 18A of current. In this regard, the NODAS was tested on 260W of commercial PV module that can draw up to 10A of current. Sufficient gate voltage is required to fully turn ON the MOSFET. The minimum voltage required at the MOSFET gate can be found in its datasheet i.e. 10V. The microcontroller supplies around 5V at I/O pins, while some MOSFETs require more voltage at the gate pin. Thus, when selecting which MOFSET to choose, the researcher had looked for the MOSFET that requires less voltage at the gate to avoid draining the current which dissipates the power inside the MOSFET. Furthermore, the researcher has considered the price of the MOSFET used; the individual price of MOSFET used for NODAS is around 6 Malaysian Ringgit and the price will be cheaper when they are bought in bulk.

3.5.2 Integration of Cut-off Switch with Position Sensor and a Microcontroller

The MOSFET was integrated with a microcontroller to observe its behavior. The MOSFET was tested in a laboratory using the Arduino UNO, as shown in Figure 3.9 and Figure 3.10. During the first test, the LED was connected as a load. Power to the LED and the microcontroller was supplied by an external power source because the small PV module does not generate adequate amount of power.

The position sensor retrieves the position of PV module and it is stored in a microcontroller. The LED is powered up when the stored position matches with the instantaneous position of PV module, while the MOSFETs will bypass the current, cutting off power to the LED if the reference position does not match with the current position of PV module.

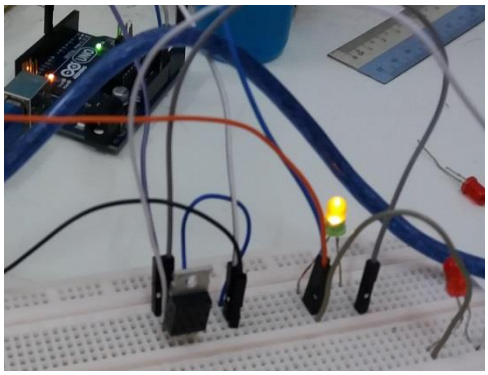


Figure 3.9: MOSFET in ON mode.

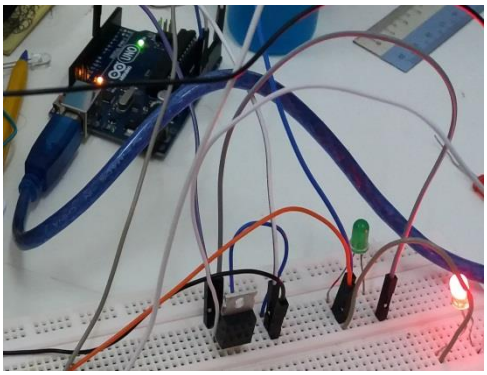


Figure 3.10: MOSFET in OFF mode.

In second experiment, a MOSFET was connected with the load (potentiometer) instead of an LED and the current flowing through the load was measured during the OFF and ON state. Because LEDs can withdraw less current while the potentiometer load can draw up to 9A of current. This time, the gate voltage was excited by a power supply in a laboratory to find the minimum voltage required to turn the MOSFET fully ON. It was observed that 10V are required to fully ON the MOSFET. This experiment was conducted to make sure that MOSFET is fully ON to avoid loss of the supplied power. It can be concluded that MOSFET requires 10V of excitation signal at the gate terminal. In this light, the components used for NODAS require 5V of supply, except for MOSFETs that require 10V of excitation signal. This indicates the need to design special interconnection inside

the PV modules to operate the MOSFETs. The newly designed interconnections of PV modules are illustrated in Figure 3.11 a) and 3.11 b).

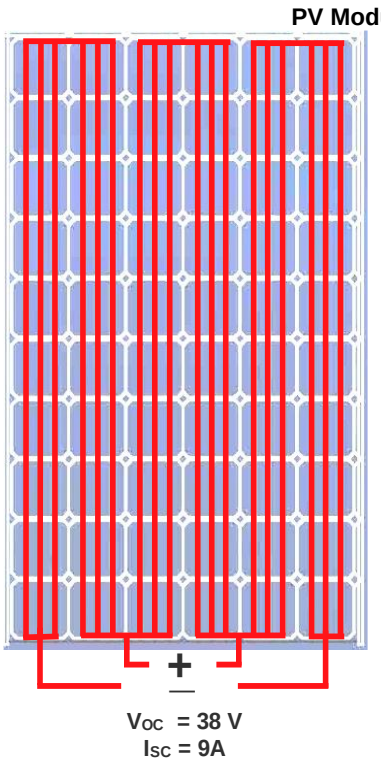


Figure 3.11a) : Conventional interconnections of PV module.

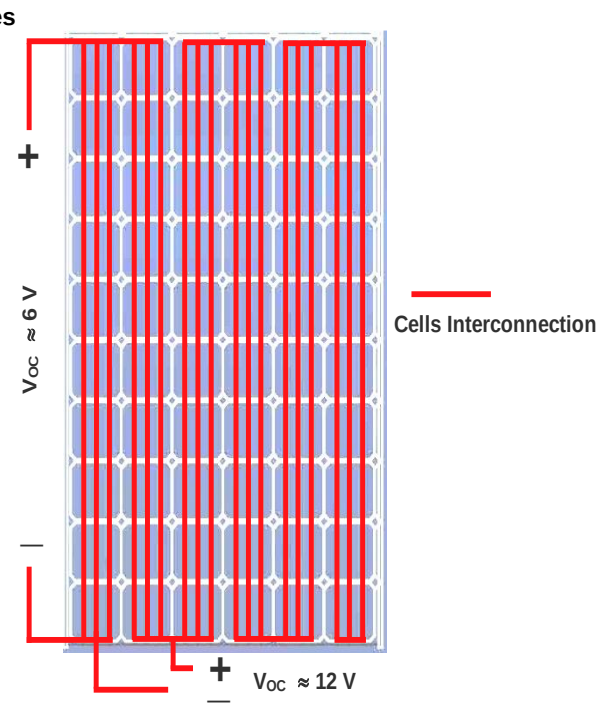


Figure 3.11 b) : Specially designed interconnections for NODAS.

The op-amp comparator is introduced in NODAS to provide an excitation signal at a gate terminal, as shown in Figure 3.12. As 10V is required at gate terminal, the op-amp is supplied 10V at V_{CC}^{+} through specially designed interconnections of PV modules. V_{CC}^{-} is connected to the ground while the non-inverting input is connected to the microcontroller that controls the output of op-amp to the MOSFET. The inverting input is connected to the PV module interconnection while it passes through the voltage divider circuit to reduce the voltage at inverting input. The schematic of the circuit is shown in Figure 3.12.

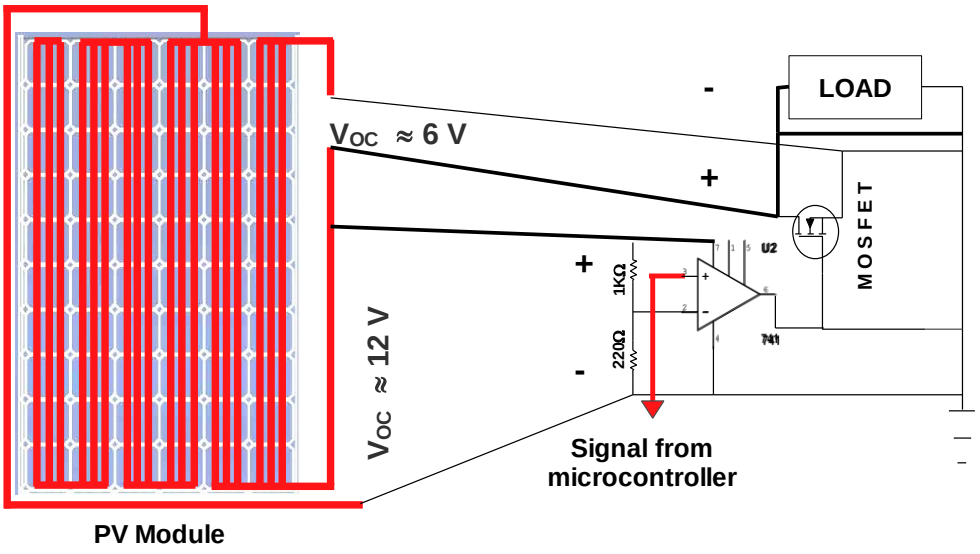


Figure 3.12: The schematic diagram of MOSFET with op-amp.

Two PV modules with different power ratings were used during development of NODAS. The Small PV module has the power rating of 10W while the larger PV module has the rating of 250W. The smaller PV module was used to prove the concept while the larger PV module was used for NODAS, but as mentioned earlier, the lamination does not come under the scope this a project. The larger PV module has a power rating of 250W and contains 60 PV cells. Each cell produces 0.5V. While designing special interconnections, the components that require 5V are supplied with power from 10 PV cells and components that require 10V are connected to 20 PV cells.

3.6 A Microcontroller

The NODAS uses an 8-bit AVR microcontroller from ATMEL. The microcontroller acts as a brain for the anti-theft system. The position sensor is integrated with the microcontroller and an intelligent algorithm is fed into the microcontroller. The algorithm retrieves the position of the PV module each morning and interrupts the deliverance of power when the location changes from the stored reference position. In this light, the microcontroller has a sufficient memory to store the algorithm which controls the operation of anti-theft system. The microcontroller used in NODAS also has a built-in wireless function and a security engine. The wireless function is used to reactivate NODAS without going close to every PV module while the security engine in used to secure data transmission and grant access to reset the anti-theft system.

The Atmel Studio 7.0 software was used for the development of ATMEL's microcontroller. ATMEL ATmega256RFR2 Xplained Pro shown in Figure 3.13 is a development kit that is used for debugging purposes. This development kit is used as a controller to demonstrate the operational functionalities of NODAS.

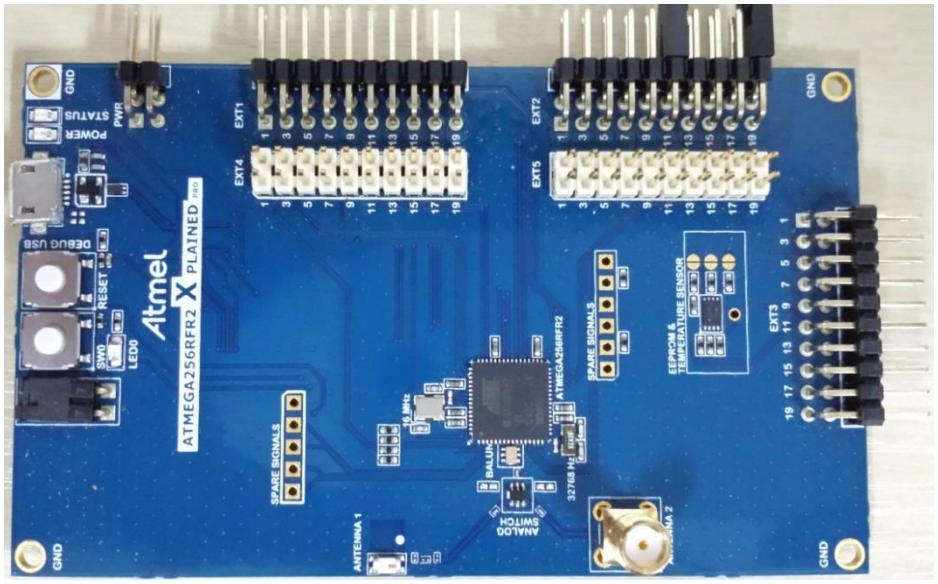


Figure 3.13: ATMEL's ATmega256RFR2 Xplained Pro development kit.

ATMEL's ZigBit extension board shown in Figure 3.14 also has the same onboard microcontroller. This extension board is attached with development kit for debugging purposes. The development kit is used as master device, while the extension board is used as a slave device. The position sensor, MOSFET, comparator and PV module are attached to the extension board while the controller triggers retrieval function of position sensor once the NODAS has to be reactivated.

Figure 3.14: ATMEL's Zigbit extension board.

3.6.1 Selection Criteria of Microcontroller

The microcontroller was selected based on the criteria shown in Figure 3.15.

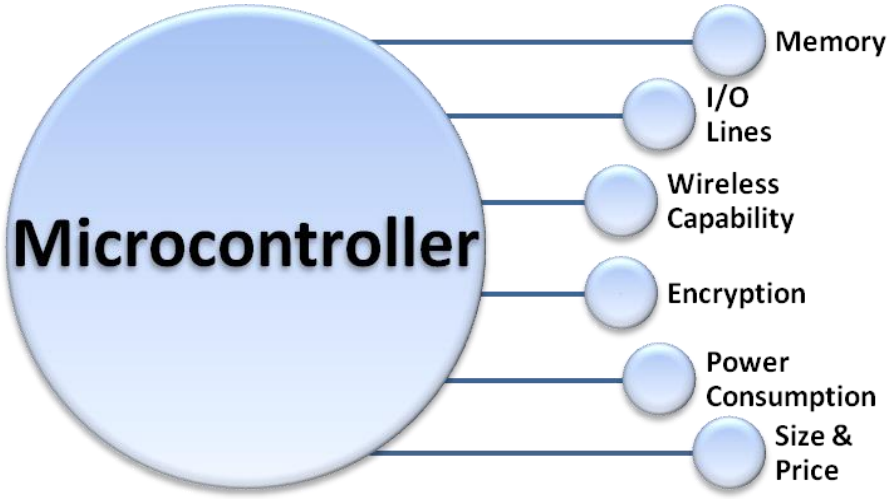


Figure 3.15: Selection criteria of microcontroller.

NODAS does not need to store a large amount of data as only the position retrieved from the magnetometer and the operational algorithm is needed to be stored in its memory. The ATMEL's ATmega256RFR2 contains an on-board 256K flash memory and 8K of electronically erasable programmable read only memory (EEPROM) that is quite sufficient for NODAS. The data endurance of microcontroller is up to 20K write/erase cycles at 125°C, and 50K write/erase cycles at 85°C.

As NODAS requires only position sensor to input data, only one port is needed for the position sensor. Meanwhile, the ATMEL's microcontroller has 38

programmable I/O lines for various interfaces, such as serial peripheral interface (SPI), universal synchronous/asynchronous receiver/transmitter (USART) and two wire interface (TWI). All ports in microcontroller are bidirectional and the available I/O ports in a microcontroller are quite sufficient for the anti-theft system, hence, the remaining I/O ports can be used for future development.

Solar farms constitute of a large number of PV modules and it is very hectic to approach each module to reactivate it. The ATMEL's microcontroller has a built-in low power 2.4GHz radio transceiver that is used to implement ZigBee application. NODAS also requires wireless communication to reactivate the PV modules after they are recovered from theft or after they are removed for maintenance.

It is important that only the authorized person can reactivate the PV module once it is in the shut-off mode, hence, encryption is used to make it safe from unauthorized access. The NODAS is claimed to be non-destructive. This is because it can be reactivated after it was removed by authorized personnel for any reason. The ATMEL's microcontroller offers advance encryption standard 128 bit AES-128 security engine to protect communication.

NODAS require components with ultra-low power consumption as it will be powered by the PV modules. The components that consume more power will end up decreasing the power of the PV module towards load. So, in a solar farm where there are large number of PV modules, the power consumed by NODAS in

each solar farm will become significantly high. In this regard, the ATMEL's microcontroller has a very efficient power consumption. It requires 1.8V to 3.6V of voltage supply whereas it draws a current of 10.1mA to 18.6mA in a transmission mode. The central processing unit CPU consumes 4.1mA of current at 16MHz while the CPU with 2.4GHz transceiver draws 6mA for reception and 14.5mA for transmission. It also has a deep sleep function that draws only 700nA of current.

It is crucial that the selected components for NODAS should be very compact in size as the PV module does not have sufficient space to integrate additional circuitry. The ATMEL's microcontroller is available in a quad flat no-lead QFN package with the dimension of 9mm×9mm×0.9mm (length × width × depth) and the price of the microcontroller is around 27MYR.

3.6.2 Integration of MOSFET and Position Sensor with a Microcontroller

The position sensor and the MOSFETs were integrated with ATMEL microcontroller for testing in the laboratory as shown in Figure 3.16 and 3.17. This experiment was conducted to observe the integration of the position sensor and the shut-off switch with the microcontroller. Power was supplied to the load by using small PV module with 10W of power. The position sensor retrieves the instantaneous position of PV module and stores it in a microcontroller. After the position has been stored, it can be seen from Figure 3.16 that the current drawn by the load is 198mA. At that moment, no current has been drawn by other three MOSFETs and shown by the three ammeters at the bottom. Figure 3.17 illustrates

that the PV module has been displaced and no current passed through the load so it was bypassed by the MOSFETs.

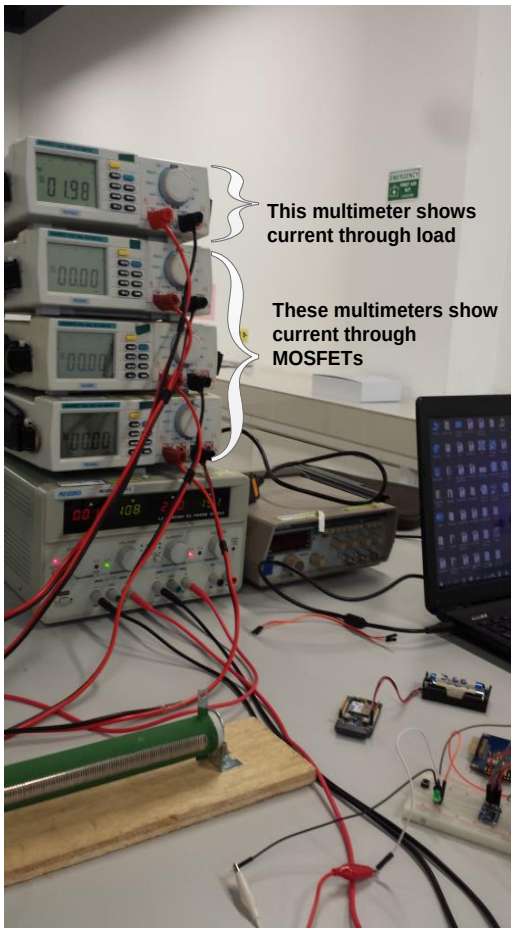


Figure 3.16: The current is drawn by the load (ON Condition).

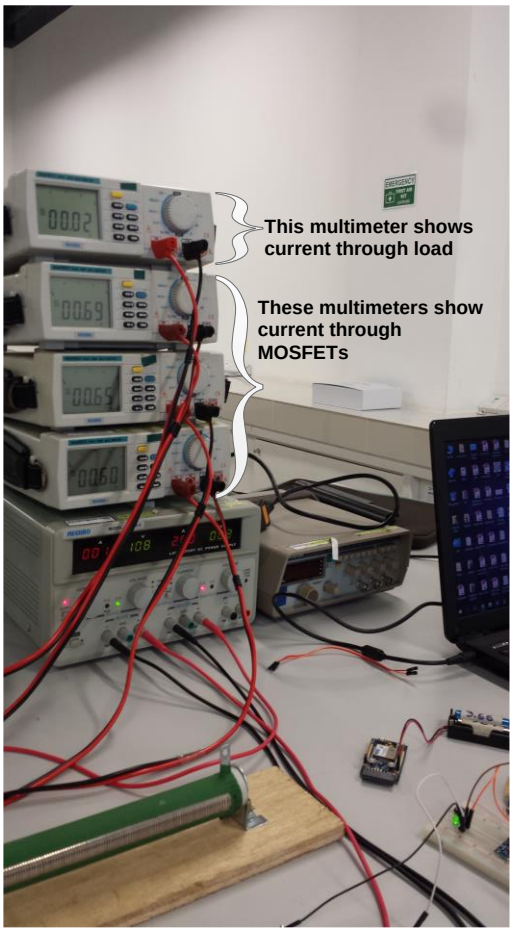


Figure 3.17: The current is by passed through MOSFETs (OFF Condition).

3.6.3 Wireless Function of a Microcontroller

The microcontroller is also incorporated with a wireless feature. It enables the user to operate the PV modules from several meters away. An authorized user can reactivate the operation of PV modules if they are displaced for maintenance purposes or recovered after theft. The authorization code can also be reset using wireless controller. This feature makes the PV modules indestructible.

NODAS comprises of two microcontrollers with the same features, the first microcontroller acts as a master (controller) while the second acts as a slave (controlled) device. The slave device is incorporated with the position sensor and the auto shut-off switch while master device acts independently. The circuitry on the controlled end is laminated inside the PV modules while the master is used to initialize, reactivate or deactivate the PV modules. The master board has its own external power supply, while the slave device is powered by the PV modules. As mentioned earlier, this paper is focused on proving a concept and the lamination of NODAS inside the PV modules does not come under scope of this research, so, at this time, the slave depends on external supply and small PV modules with 10W of power rating were used to prove the concept, as shown in Figure 3.18.

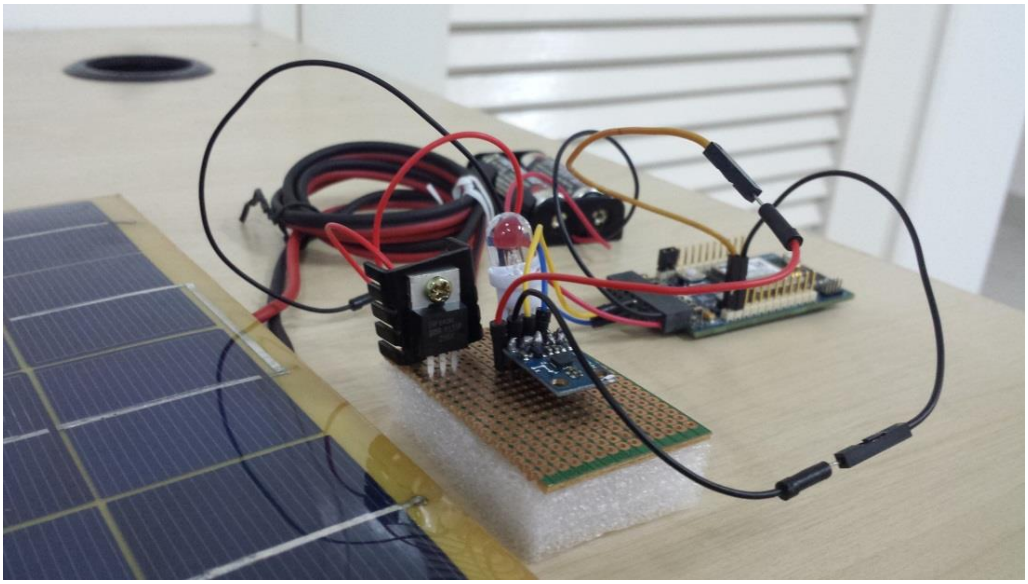


Figure 3.18: Integration of position sensor and shut-off switch with a microcontroller.

3.6.4 Security Implementation

Encryption has been implemented to prevent unauthorized access to the anti-theft circuitry. It only grants the permission to make changes for reactivation of PV module. The simple encryption was conducted during the experiment as shown in Figure 3.19. The 7 segment LCD, LED and a position sensor were integrated with ATMEL development kit to conduct this demonstration. The 7 segment LCD was used during the experiment to view the passcode. The digits changed between 0-9 by pressing push button which can be viewed through the 7 segment display. The re-activation of NODAS was done by inputting specific passcode during the initialization of the anti-theft system. Upon initialization, the position is retrieved and stored in the microcontroller. The LED attached during demonstration shows the status of activation, if the position changes, then the NODAS will stopped working and LED will be turned OFF. A touch button is

pressed until a preset digit can be viewed on the 7 segment display. If the digit matches with the stored digit, then the wireless controller will be allowed to reset the position, the LED will be turned ON and NODAS would remain inactive. The 7 segment display was only used or demonstration purpose only and it would not be laminate inside PV module. This test demonstrated security implementation and in the future, a keypad can be integrated with the wireless controller to allow the use of a longer password phrase to make the communication and authorization more secure.

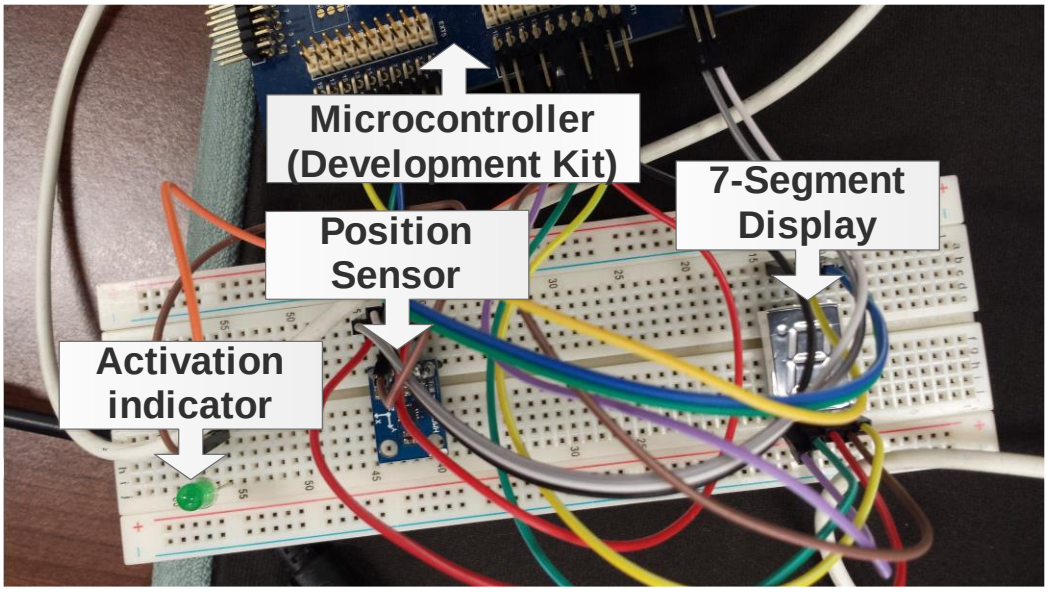


Figure 3.19: Demonstration of security encryption.

3.7 An Innovative Algorithm

An innovative algorithm has developed and stored in the microcontroller to reduce the power consumption of NODAS. An algorithm initializes the NODAS and makes the decision whether the PV modules should stop operating or resume normal operation. The NODAS remains operational only during daytime and at night time as no power is generated from PV module. The NODAS will initialize its operation after detecting sunlight and matches the current location with the stored reference location. The microcontroller would send a query to retrieve position after certain interval to continuously check the modules' instantaneous position. The PV modules will not generate any power if the current location does not match with the reference location. The algorithm fed into the microcontroller is illustrated in Fig 3.20.

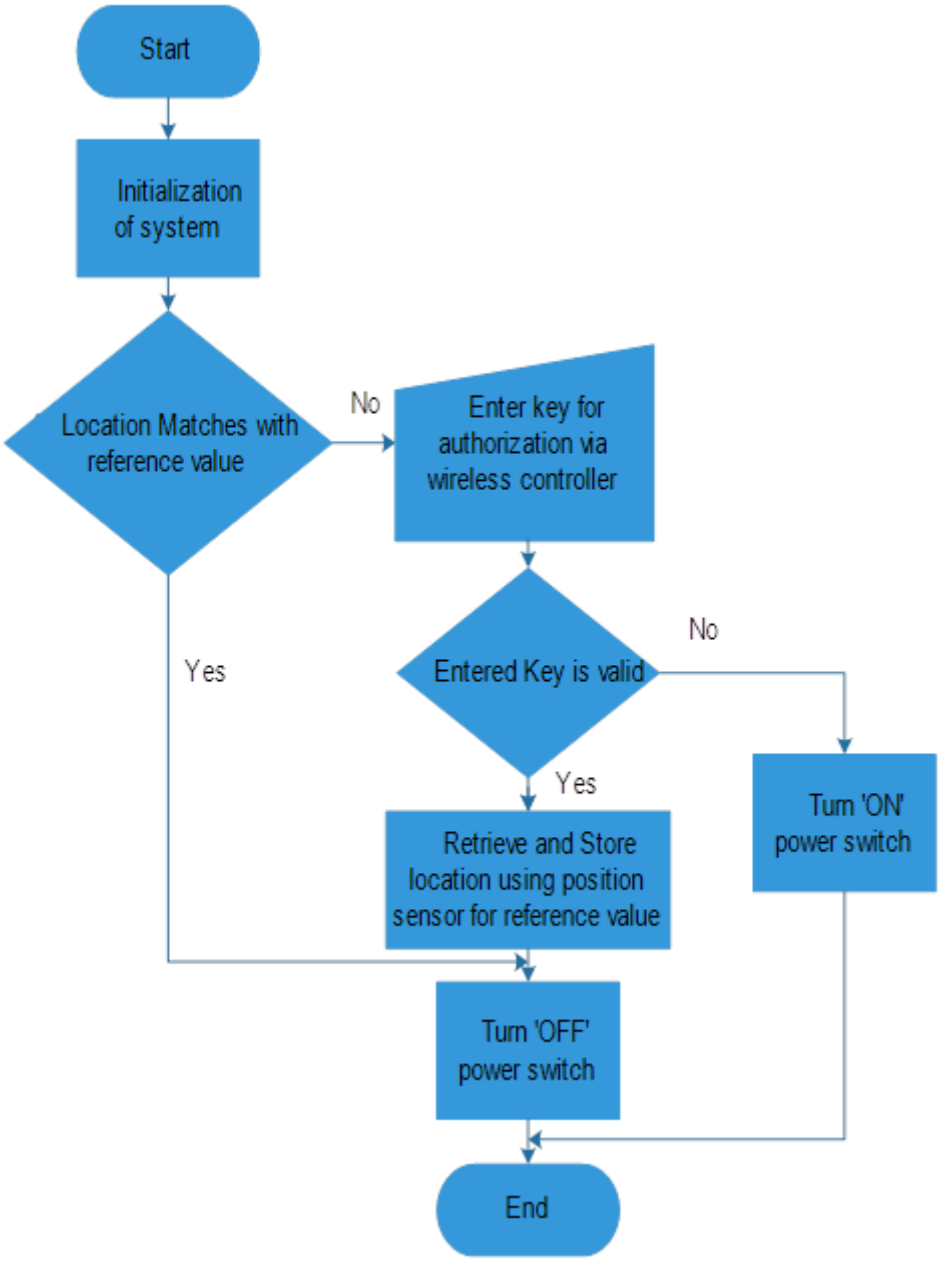


Figure 3.20: The algorithm stored in microcontroller of NODAS.

During the initialization, the position is retrieved from the position sensor and stored in a microcontroller as a reference position. The credentials are also stored in a microcontroller during the initialization of a system. After that, the system would turn OFF the power switch and NODAS will remain operational. The

microcontroller retrieves the position after certain interval to check the instantaneous position during daytime. Meanwhile, at startup, the position will be verified before power is delivered to the load. If someone tries to steal the PV modules or remove the PV modules for maintenance, then the microcontroller will shut off power supply to the load. The user will be asked for credentials if the position does not match with the reference position. If the user failed to provide the authorized credentials, the anti-theft system will activate the MOSFET to restrict the power supply to the load. On the other hand, if the credentials are verified, position sensor will be used to retrieve a new position and the new position will be saved as a new reference position in the microcontroller. The pseudo code of the algorithm can be viewed in Appendix E.

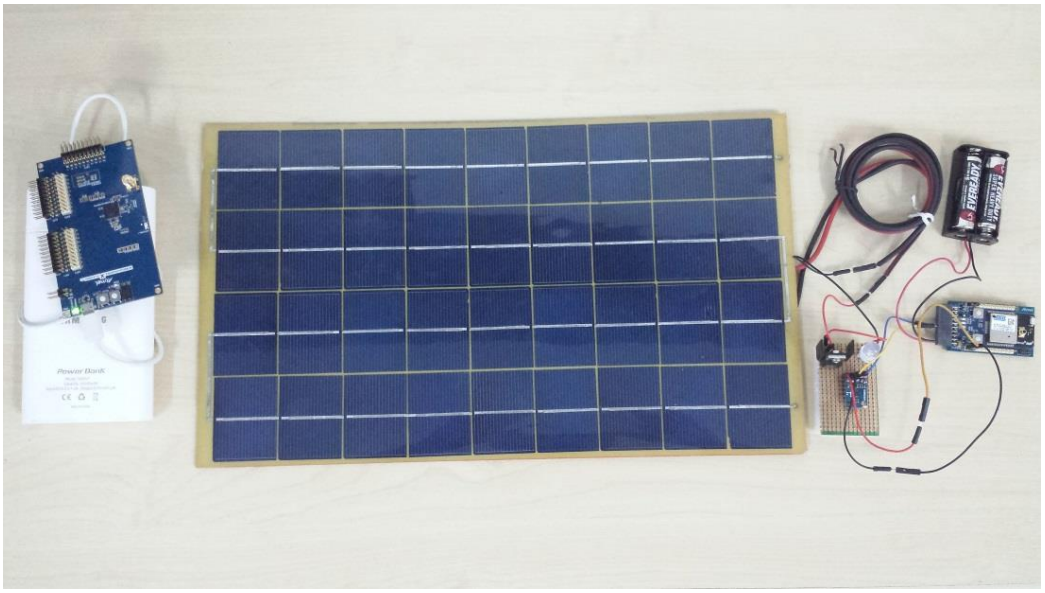


Figure 3.21: NODAS with wireless controller.

CHAPTER 4

RESULTS & DISCUSSIONS

The components used in NODAS were evaluated initially using Arduino UNO as well as the ATMEL's development kit. The microcontrollers used in both kits have different features but they came from same manufacturer. Two different PV modules were used during the laboratory tests and on the university's rooftop; the PV module used in the laboratory has the power rating of 10W while the larger PV modules used on the rooftop have the power rating of 260W. Each component has gone through various tests as discussed in the sections below.

4.1 Position Sensor

Various tests have been employed on the position sensor to determine the reliability and robustness of the system.

4.1.1 Electromagnetic Interference

As mentioned earlier, a magnetometer was used for position sensing of the PV modules. As the magnetometer is influenced by electromagnetic interferences, interferences caused by electromagnetic waves are evaluated to preset the tolerance level and avoid false triggering of the alarm. This test was conducted in two

locations, the laboratory and the rooftop after the integration of anti-theft circuitry with the larger PV modules to obtain real-time results.

The first experiment was conducted in the laboratory. The behavior of the position sensor was observed under influence of different intensities of electric fields i.e. from 1A to 9A. The distance of current carrying conductor was varied, such as 2mm, 5mm and 10mm, to find the least influential position. The current carrying conductor is placed in different orientations during the evaluation tests because position sensor could sense magnetic fields in three different axes. As shown in Figure 4.1, the current carrying conductor was placed in different orientations and distance between position sensor and current carrying conductor is also varied from 2mm to 10mm. Meanwhile, Figure 4.2 shows the least influential orientation of position sensor placed at the distance of 10mm from current carrying conductor. The influence in the interference is shown in points. The lowest number of points shows best suited orientation observed in the x-axis in Figure 4.2. The detailed results of other orientations and distances are tabulated in Appendix B.

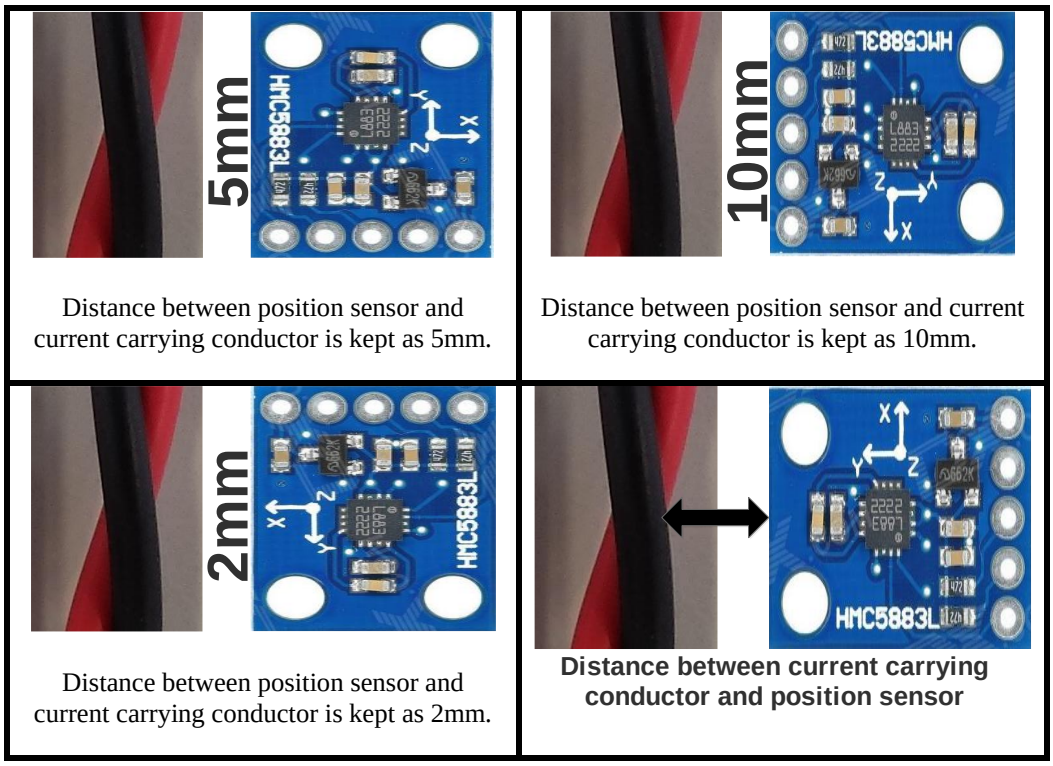


Figure 4.1: Electromagnetic interference test using different orientations.

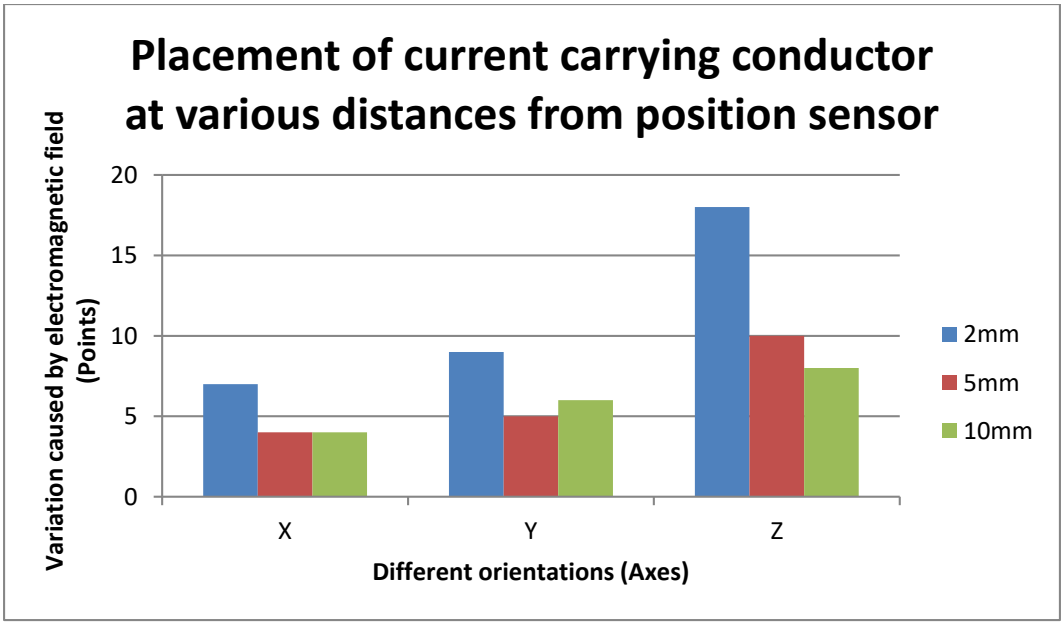


Figure 4.2: The deviation in magnetometer's reading while placing current carrying conductor near to x-axis of position sensor.

The second experiment was conducted while attaching the position sensor to the PV module. The anti-theft circuitry is developed to be laminated inside the PV modules, so it is necessary to study the effects of electromagnetic interference when the position sensor is attached to the larger PV modules. The position sensor can be affected by the interconnections of the PV module which carries up to 9A of flowing current. With the help of this experiment, the best location at PV module has also been found. In this position, the electromagnetic interference caused by the interconnections of PV module is minimal. This experiment has also helped to preset the tolerance of the position sensor. The repeatability of position sensor is also tested by redoing the experiment several times. Figure 4.3 below shows the unused location on PV module where the position sensor was attached during experiment. So, by using the results shown Figure 4.2, the position sensor would be placed within the unused area of PV module at a distance of 10mm.

Figure 4.3: PV module showing proposed place for lamination of anti-theft system.

4.2 Cut-Off Switch

The cut-off is evaluated for making the anti-theft system robust. Various tests have been conducted under different circumstances to avoid false alarming and other unexpected behavior.

4.2.1 Power Dissipation of MOSFET

The MOSFET has gone through various tests in the laboratory after integration with PV modules. It was observed that the shut-off switch dissipates power while in shut-off mode and gets heat up, consequently, evaluation has been done to avoid overheating of the MOSFET that can damage the circuit, as well as the PV modules.

It was observed during experiment that the MOSFETs could become overheated as heat sink was not used and the current passing through the MOSFET reached up to 4A. So, it is concluded that heatsink is required to dissipate heat without destructing the system, however, in real application, the NODAS will be laminated inside the PV modules that does not have sufficient space for a heat sink. As each PV module generates around 9A of current, there is a need to consider the issue of heat dissipation. Subsequently, another experiment was conducted to solve this problem. The next experiment used MOSFETs with switches and the number of MOSFETs with switches were increased from 3 up to 6 in the next round of the experiment while the temperature behavior was observed. The MOSFETs are connected in parallel as the current needs to be distributed to avoid over heating the

MOSFETs. The schematic of the circuit and the prototype designed for this experiment are shown in Figure 4.4 and Figure 4.5.

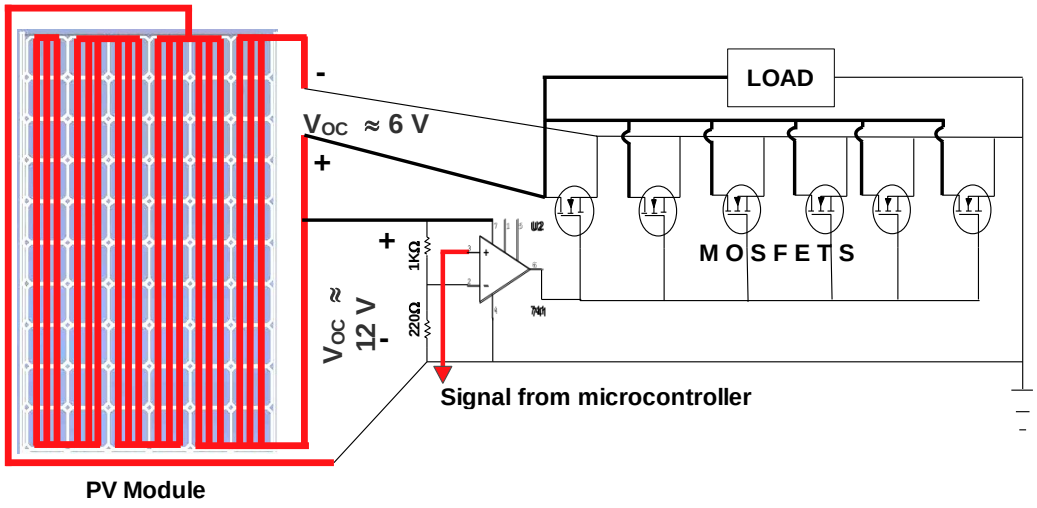


Figure 4.4: Schematic circuit of MOSFETs and Op-amp.

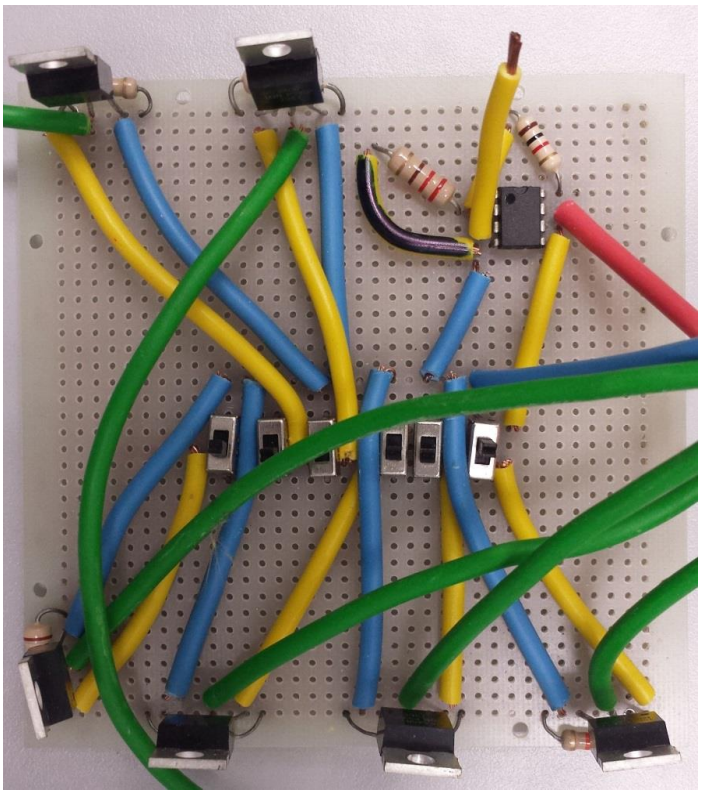


Figure 4.5: Prototype of 6 MOSFETs used to distribute heat dissipation in NODAS.

The same experiment was conducted again on the rooftop but this time, a PV module was used, instead of a power supply. The MOSFETs are connected between the PV module and the load to restrict power supply to the load. Initially, two MOSFETs were used for testing, subsequently, the number of MOSFETs was increased to distribute power across different MOSFETs. During the experiment, the MOSFETs were isolated in a paper box to minimize thermal interference caused by surroundings as shown in Figure 4.6. The results are presented in a table in Appendix A and graphical representation of the results is shown in Figure 4.7. The results show the decline in the MOSFET's temperature with the increasing number of MOSFETs. It was also observed that the temperature of MOSFETs remained under 50°C when there are 5 and 6 MOSFETs used and the current drawn by PV module was 9A. Thus, 6 MOSFETs are used in anti-theft circuitry to maintain NODAS' thermal stability. Moreover, as mentioned earlier, the MOSFETs used for NODAS come in SMD packages that do not require much space on the module. This makes the size and weight of the MOSFETs to remain feasible for the circuitry. The selected MOSFET costs around 2 to 3 Malaysian Ringgit when purchased in bulk. So, the price of circuitry will be higher by few Malaysian Ringgits.

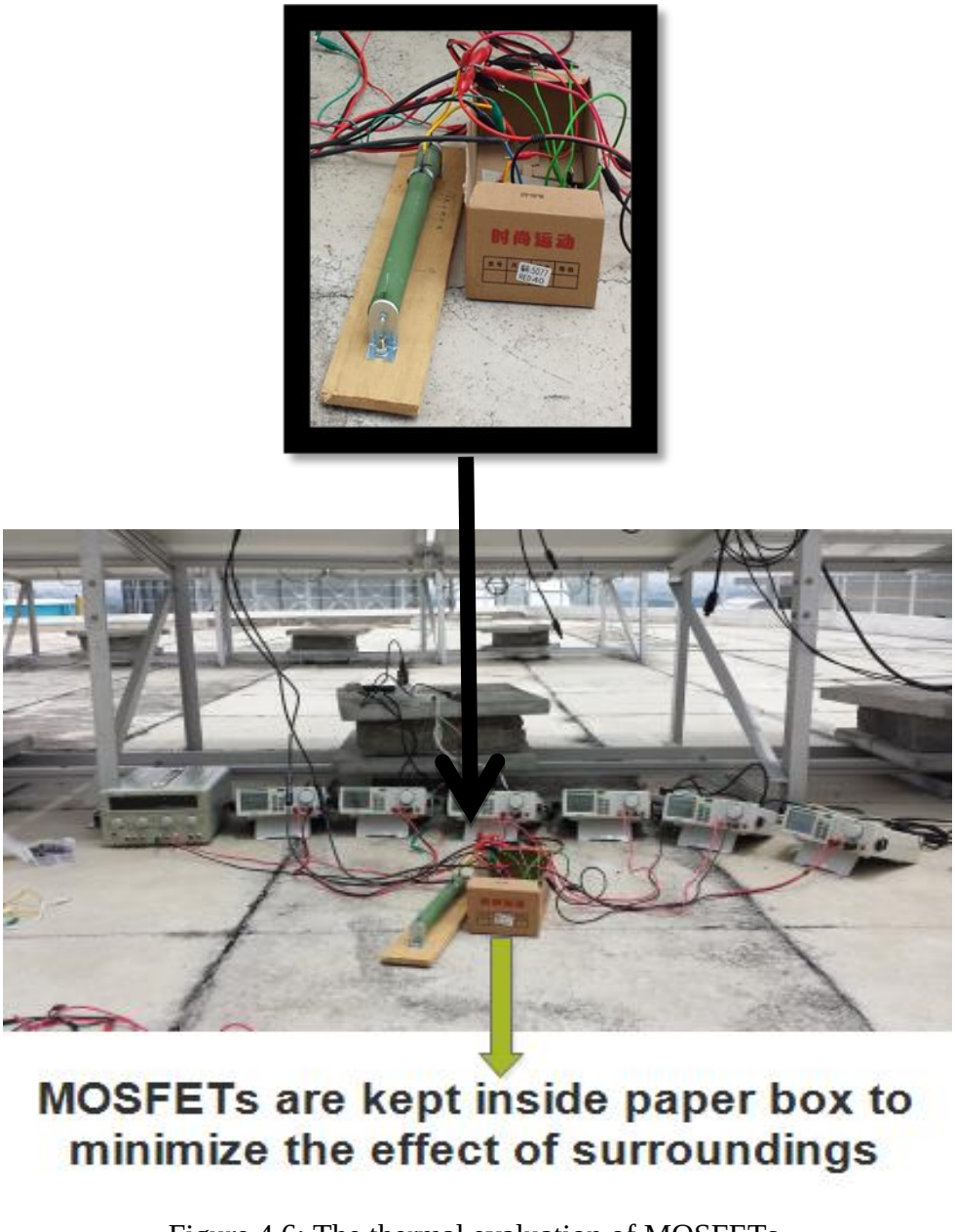


Figure 4.6: The thermal evaluation of MOSFETs.

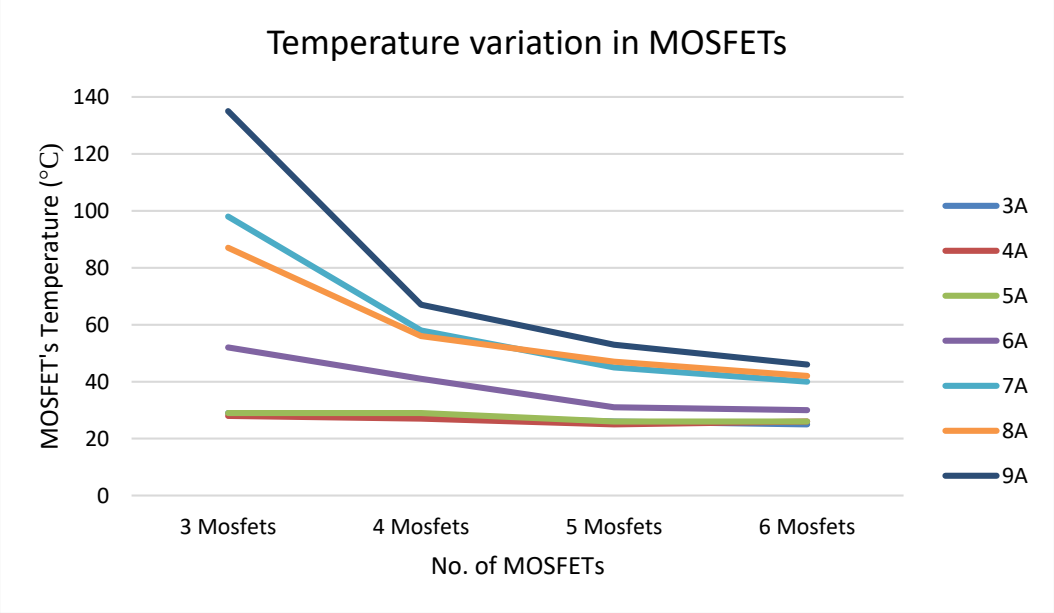


Figure 4.7: Variation of temperature under different number of MOSFETs and currents.

4.3 A Microcontroller

The microcontroller used for NODAS has a built-in wireless transmitter that allows wireless communication between any two nodes, hence, it is very important to test the wireless communication for lossless communication.

4.3.1 Wireless Capability

The wireless capabilities of the microcontroller are evaluated using ATMEL's hardware evaluation kit and a software development kit. The range of wireless communication has been evaluated in a clear path and by placing obstacle between the transmitter and receiver. This evaluation was done in both indoor and outdoor environments to observe the range of wireless communication in different conditions. Another test was conducted to study packet error rate (PER) in different scenarios. The PER is the ratio of transmitted and received packets during

communication. The PER depends on the interference, for instance, any obstacle that comes between the transmitter and receiver increases PER. In this regard, the increment in PER can cause delay in communication. The mathematical expression for calculating PER is shown below.

$$\text{Packet Error Rate (\%)} = (1 - \frac{\text{Frames transmitted}}{\text{Frames received}}) \times 100 \quad (4.1)$$

4.3.1.1 Wireless Range

The range of wireless communication has been tested in a clear path and also by bringing an obstacle in between transmitter and receiver. The test was conducted in the university's lobby and there was no obstacle between transmitter and receiver during the test. This means that the test was conducted in a clear path. The wireless range during the experiment was measured as 63.5m. However, at that distance, the packet error rate reached up to 50% that consequently increased the time interval to accomplish the transmission. Figure 4.8 presents a photo of the university's lobby where the experiment was conducted.

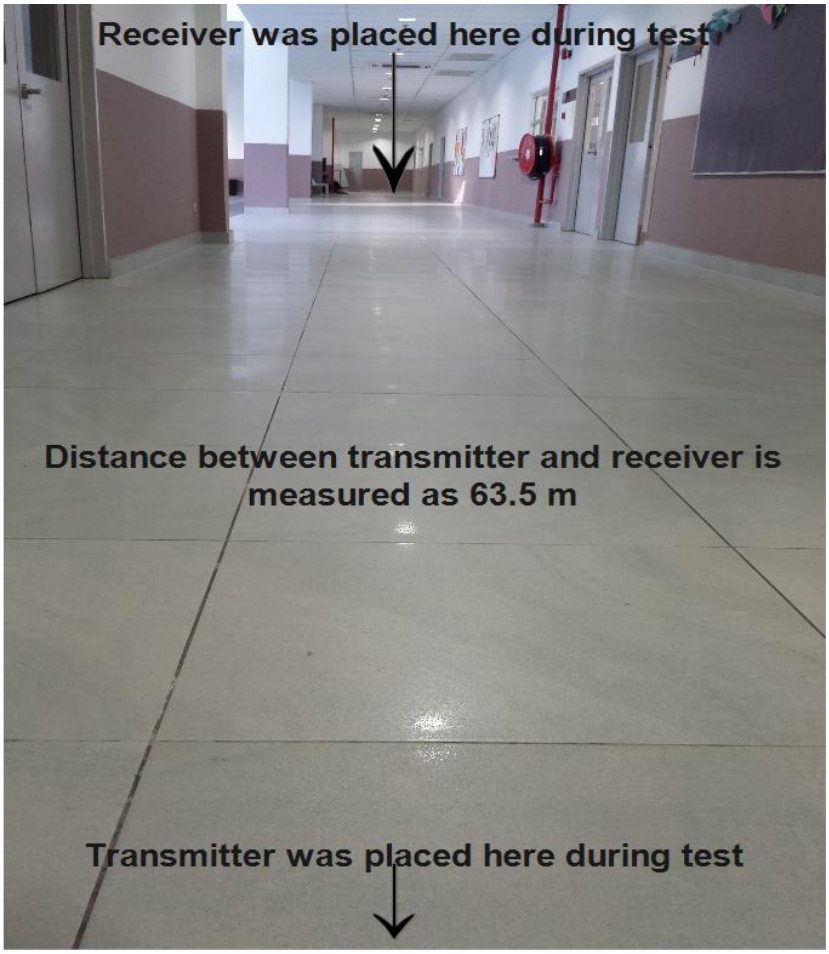


Figure 4.8: The range of transmitter and receiver is tested in university's lobby.

Another experiment has been conducted to observe packet error rate at various distance ranges from 10m to 50m. The graphical results of experiment are shown in Figure 4.9. The spike in PER was observed at the 64th packet which denotes the interference caused by someone passing through the area so it can be ignored. Besides that, the PER remained under 20%, which is considered as acceptable. The maximum PER (18%) was observed at the distance of 50m. It was mentioned earlier that the NODAS will have a controller that is used to reactivate the PV modules by authorized personnel. This controller can be used to control PV

modules and can work within the distance of 50m from the modules without any delay.

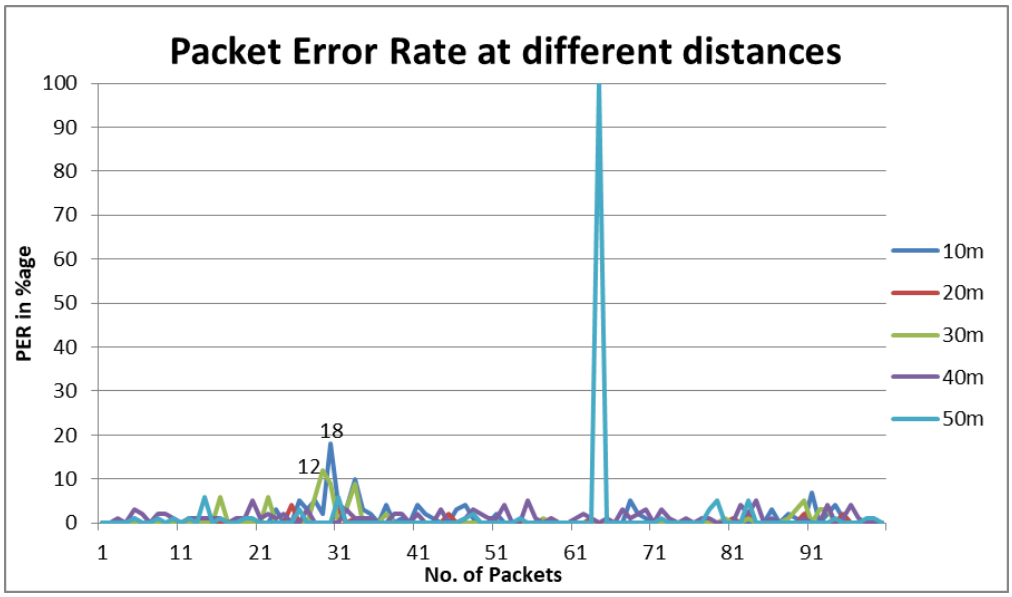


Figure 4.9: The PER at different distances.

4.3.1.2 Effect of PV Modules on PER

As the NODAS will be laminated in the PV modules in each application, another test was conducted on the rooftop of university in response to the fact that in real application, the interference created by the PV modules may affect wireless communication. Based on the small number of PV modules installed on rooftop, the transmitter and receiver were placed diagonally to the first PV module and last PV module as demonstrated in Figure 4.10. Another test was conducted when transmitter and receiver were placed straight before the first and last PV module as shown in Figure 4.11. In the straight setting, only two PV modules were present

between the transmitter and receiver while for the diagonal setting, there were around six PV modules between the transmitter and the receiver. That is how the interference caused by PV modules was observed during the experiment. The packet error rate PER was measured in both settings and shown in Figure 4.12. The graph topples around '1' and '0'. Here, '1' denotes 100% packet error while '0' means 0% packet error. During the experiment, it was noticed that the PER remains '0', indicating that PV modules did not cause any interference when they were placed between the transmitter and the receiver.

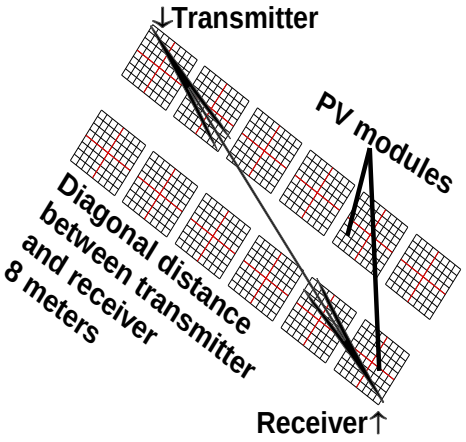


Figure 4.10: Diagonal placement of transmitter and receiver during test.

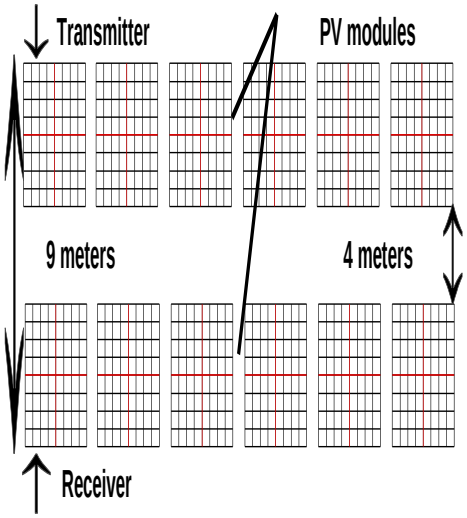


Figure 4.11: Straight placement of transmitter and receiver during test.

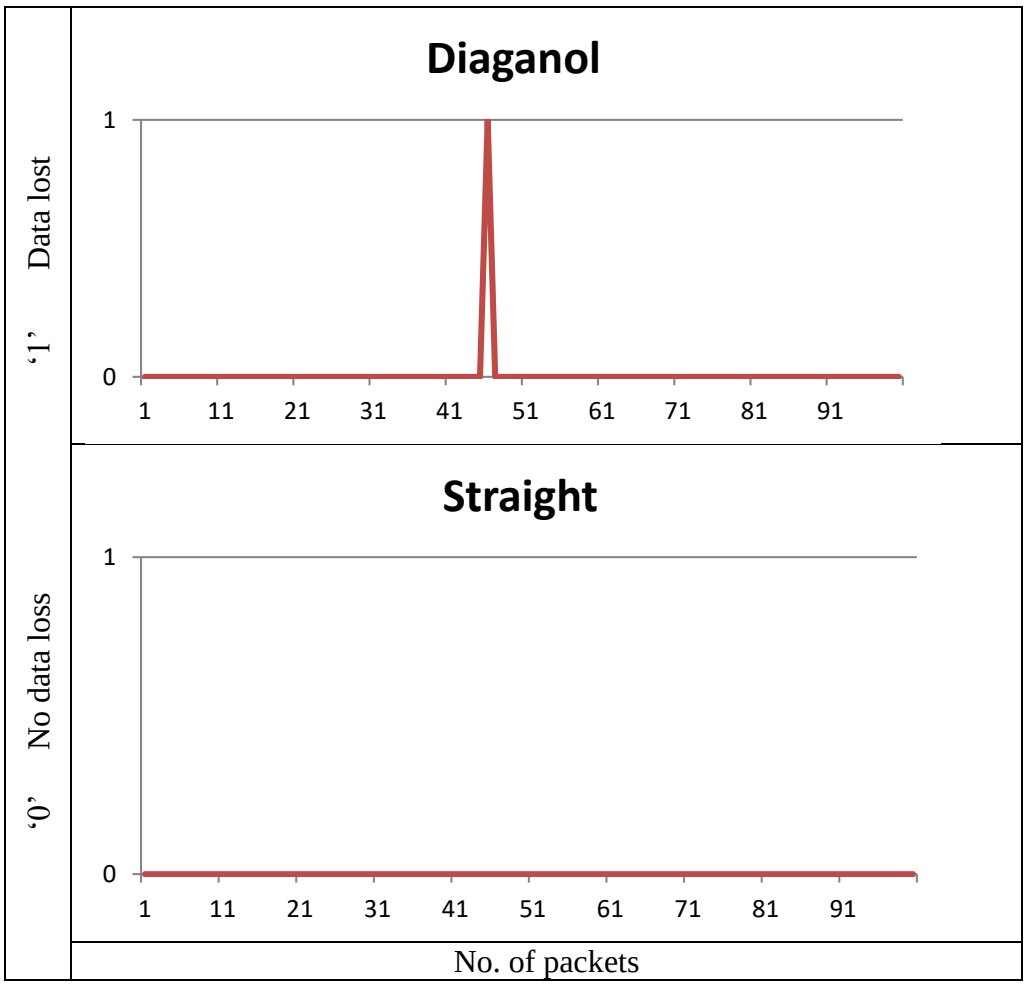


Figure 4.12: Packet Error Rate in different orientations.

CHAPTER 5

CONCLUSION

5.1 Novelty of NODAS

- Once it is stolen, the power generation function of a PV module shuts off internally and cannot be reactivated externally. The power cannot be resumed even it is sold to a new customer.

- Low power position sensor is used to detect the position of the PV module. This position sensor will be embedded inside a PV module and the power would be supplied through special interconnections within the PV module. Hence, the anti-theft system cannot be removed and re-activated by unauthorized person unless the PV module is broken up.

- The power generation of a PV module can be re-activated by using a pass key with a wireless controller. Encryption is used to ensure security of anti-theft system and to secure wireless communication.

- The anti-theft system is non-destructive as the PV module can resume its function once it is recovered from theft or removed for maintenance purpose.

- The anti-theft system consumes very low power, so no external or embedded battery is needed for the system. Battery usually has much shorter lifetime than the PV module.

- The anti-theft system operates only during daytime which saves power and makes it an ultra-low power consumable device.

5.2 Conclusion

The NODAS is a modular based anti-theft system which does not require additional components to tackle the theft. It is not required to alert the authorities to take any action upon theft because a PV module will become inactive once displaced from its original location. This demotivates thieves from stealing the PV module as the PV module will be useless once it is displaced from its location. It is worth mentioning that this project is designed and developed at a small scale for this study to prove this concept, hence, the actual lamination of the circuit was not covered. In this regard, the NODAS energy source is supplied by external batteries as the smaller PV modules with lower power ratings are not capable of generating enough power for NODAS. Fortunately, the components used for NODAS are readily available in a miniature size as PV module does not have sufficient space for laminating large components.

The NODAS has been designed and developed using low power position sensor. The position sensor was tested in the laboratory to determine its tolerance that is preset in the algorithm to avoid false alarm triggering. Meanwhile, the

position sensor detects magnetic field around it in three different axes. So, it is observed during the experiment that the position sensor shows less deviation, while a high current carrying conductor is placed perpendicular to x-axis of position sensor. The distance of current carrying conductor was also changed and it was observed that the position sensor show minimum deviation, if the current carrying conductor is placed at a distance of 10mm from position sensor. The number of MOSETs used for NODAS have also been evaluated through experiments to limit the power dissipation within the range that can cause damage of NODAS and eventually, the PV module. It has been observed that 6 or more MOSFET are suitable for NODAS to dissipate around 9A of current. Separate interconnections are proposed for components that need 5V while 10V is supplied to the MOSFETs to turn in on fully.

A wirelessly reactive able device has been set up to resume NODAS' operation after recovery from theft and also for other conditions. Experiments has been conducted to show that the wireless function of NODAS can work effectively around the radius of 50 meters without losing any information. The basic encryption has been done also for securing communication between transmitter and receiver.

The NODAS has gone through different evaluation processes to make it sure the robustness of the developed system. Several experiments have been conducted after integrating NODAS to the PV module with 260W of power rating while other experiments are conducted in a laboratory. The components used in

NODAS are tested with basic hardware kit i.e. Arduino UNO and later tested with selected micro-controllers, i.e. ATmega265RFR2.

The estimated price of components used for NODAS lies around 70 Malaysian Ringgits while it would be reduce further once the purchasing will be done on a large scale.

5.3 Recommendations

The NODAS can be improvised further after doing deep research about lamination process. In this project, the modular based ICs and evaluation kits are used whereas the lamination of NODAS in the PV module requires the circuit design and development to integrate all the components on a printed circuit board. In the developed system, the wireless controller is used within the personal area network. The range can also be extended further to wide area network by introducing the mesh topology in the system. Using the router, the PV modules can be reactivated from anywhere by using internet. The wireless controller can also be improvised further by adding keypad to generate strong passwords. The keypad could also allow adding plenty of functions to anti-theft system such as selecting specific module or multiple PV modules within the network to reset all at the same time.

LIST OF PUBLICATION

1) Wasif Ali Khan, Boon-Han Lim, An-Chow Lai, Kok-Keong Chong. “A novel anti-theft security system for photovoltaic modules”, AIP Publishing, 2017

REFERENCES

Abdul Hamid, S. B., Rosli, A. D., Ismail, W. & Rosli, A. Z., 2012. Design and Implementation of RFID-based Anti-Theft System. Penang, *IEEE International Conference on Control System, Computing and Engineering*, pp. 452-457.

B., 2013. *Flyer SolteQ.* [Online] Available at: http://www.solteq.eu/Flyer_SolteQ_DSS01_ENG.pdf [Accessed 9 April 2016].

Bertoldo, S., Rorato, O., Lucianaz, C. & Allegretti, M., 2012. A Wireless Sensor Network Ad-Hoc Designed as Anti-Theft Alarm System for Photovoltaic Penels. *Wireless Sensor Network,* 14 March, Volume 4, pp. 107-112.

Dawoud, S. & Peplow, R., 2010. *Digital System Design - Use of Microcontroller.* 1st ed. Aalborg: River Publishers.

Gifford, J., 2014. *Protecting components from theft.* [Online] Available at: https://www.pv-magazine.com/magazine-archive/protecting-components-from-theft_100016953/
[Accessed 23 May 2017].

Gislason, D., 2008. *ZigBee Wireless Networking.* 1st ed. New York: Newnes.

Goldack, D., 2003. *Protective system for a solar module.* United States of America, Patent No. US6650031B1.

Gratton, D. A., 2011. *Developing Practical Wireless Applications.* 1st ed. Burlington: Elsevier Science & Technology.

Green, M. A. (2013). *Solar Cells - Operating Principles, Technology and System Applications* (2nd Edition ed.). (N. Holonyak, Jr., Ed.) NJ: Prentice Hall Publisher.

Gualerzi, V., 2007. *Now the solar is tempting even thieves stolen from Enel thousands of panels.* [Online] Available at: http://www.repubblica.it/2006/11/sezioni/ambiente/solare/furti-pannelli/furti-pannelli.html
[Accessed 22 November 2017].

Kumar, A., Sharma, A. & Grewal, K., 2014. Resolving the paradox between IEEE 802.15.4 and ZigBee. Faridabad, *IEEE Conference on Reliability Optimization and Information Technology*, pp. 484-486.

Lawson, J., 2012. *The PV industry tackles solar theft.* [Online] Available at: http://www.renewableenergyworld.com/articles/print/special-supplement-large-scale-solar/volume-2/issue-1/solar-energy/the-pv-industry-tackles-solar-theft.html
[Accessed 30 March 2016].

Muhlberger, T. & Protsch, R., 2013. *Method for theft recognition on a photovoltaic unit and inverter for a photovoltaic unit.* United States of America, Patent No. US8466789B2.

Naria Security, 2016. *Anti-theft system for photovoltaic panels over plastic fiber.* [Online]
Available at: http://www.nariasecurity.it/en/applications/anti-theft-system-for-solar-panels/

Sacchetti, A., 2014. *Antitheft system for photovoltaic panels.* United States of America, Patent No. US8736449B2.

Sawin, J. L., 2015. *Global Status Report.* [Online] Available at: http://www.ren21.net/wp-content/uploads/2015/07/REN12-GSR2015_Onlinebook_low1.pdf
[Accessed 6 March 2016].

Seshasayee, N., 2011. *Understanding Thermal Dissipation and Design of a Heatsink,* Dallas: Texas Instruments Incorporated.

Tigo Energy, 2015. *Products.* [Online] Available at: http://www.tigoenergy.com/products/#Smart-Modules [Accessed 19 March 2016].

Visconti, P. & Cavalera, G., 2015. Intelligent System for Monitoring and Control of Photovoltaic Plants and for Optimization of Solar Energy Production. Rome, *IEEE 15th International Conference on Environmental and Electrical Engineering*, pp. 1933-1938.

Walker, A., 2013. *Solar Energy.* 1st ed. New Jersy: John Wiley & Sons Inc.

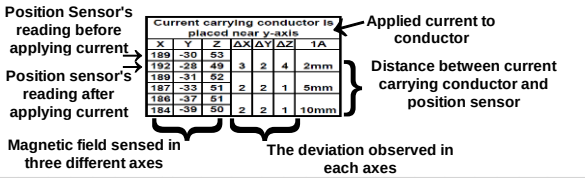
APPENDIX A

Thermal Evaluation of MOSFETS

	3A	4A	5A	6A	7A	8A	9A
3 Mosfets	29°C	28°C	29°C	52°C	98°C	87°C	135°C
4 Mosfets	28°C	27°C	29°C	41°C	58°C	56°C	67°C
5 Mosfets	26°C	25°C	26°C	31°C	45°C	47°C	53°C
6 Mosfets	25°C	26°C	26°C	30°C	40°C	42°C	46°C

APPENDIX B

Data of Magnetic Interference Experiment



X	Y	Z	ΔX	ΔY	ΔZ	1A
189	-30	53				
192	-28	49	3	2	4	2mm
189	-31	52				
187	-33	51	2	2	1	5mm
186	-37	51				
184	-39	50	2	2	1	10mm

Current carrying conductor is placed near X-axis

X	Y	Z	ΔX	ΔY	ΔZ	1A
-23	173	79				
-26	178	83	3	5	4	2mm
-24	176	80				
-22	178	82	2	2	2	5mm
-17	179	82				
-15	182	84	2	3	2	10mm

X	Y	Z	ΔX	ΔY	ΔZ	2A
-6	179	103				
-12	182	105	6	3	2	2mm
-18	178	81				
-15	181	84	3	3	3	5mm
-25	170	43				
-23	167	42	2	3	1	10mm

X	Y	Z	ΔX	ΔY	ΔZ	3A
-13	166	38				
-9	161	32	4	5	6	2mm
-25	166	43				
-31	163	41	6	3	2	5mm
-26	169	44				
-23	167	42	3	2	2	10mm

X	Y	Z	ΔX	ΔY	ΔZ	4A
-3	179	92				
-13	187	99	10	8	7	2mm
-10	175	58				
-2	171	56	8	4	2	5mm
-5	173	52				
-3	170	50	2	3	2	10mm

X	Y	Z	ΔX	ΔY	ΔZ	5A
-2	170	50				
9	164	46	11	6	4	2mm
-2	171	53				
3	165	49	5	6	4	5mm
-5	174	52				
-4	171	50	1	3	2	10mm

X	Y	Z	ΔX	ΔY	ΔZ	6A
-6	176	82				
-22	190	98	16	14	16	2mm
-6	178	66				
3	175	74	9	3	8	5mm
-6	182	91				
1	186	94	7	4	3	10mm

X	Y	Z	ΔX	ΔY	ΔZ	7A
-8	177	87				
-23	189	101	15	12	14	2mm
-8	178	89				
-5	185	96	3	7	7	5mm
-6	180	91				
2	184	95	8	4	4	10mm

X	Y	Z	ΔX	ΔY	ΔZ	8A
21	168	128				
1	164	122	20	4	6	2mm
-27	166	32				
-30	161	23	3	5	9	5mm
-27	165	32				
-33	164	33	6	1	1	10mm

X	Y	Z	ΔX	ΔY	ΔZ	9A
-27	166	35				
-20	157	17	7	9	18	2mm
-26	166	33				
-30	161	23	4	5	10	5mm
-26	167	31				
-30	161	23	4	6	8	10mm

Current carrying conductor is placed near Y-axis

X	Y	Z	ΔX	ΔY	ΔZ	1A
189	-30	53				
192	-28	49	3	2	4	2mm
189	-31	52				
187	-33	51	2	2	1	5mm
186	-37	51				
184	-39	50	2	2	1	10mm

X	Y	Z	ΔX	ΔY	ΔZ	2A
189	-43	45				
191	-36	41	2	7	4	2mm
186	-36	44				
190	-34	41	4	2	3	5mm
185	-42	42				
187	-40	41	2	2	1	10mm

X	Y	Z	ΔX	ΔY	ΔZ	3A
188	-33	43				
191	-10	51	3	23	8	2mm
189	-30	53				
194	-25	45	5	5	8	5mm
186	-35	49				
189	-38	50	3	3	1	10mm

X	Y	Z	ΔX	ΔY	ΔZ	4A
189	-42	44				
195	-32	38	6	10	6	2mm
188	-42	43				
190	-39	40	2	3	3	5mm
183	-44	41				
186	-42	39	3	2	2	10mm

X	Y	Z	ΔX	ΔY	ΔZ	5A
191	-32	50				
197	-25	38	6	7	12	2mm
188	-36	49				
192	-38	44	4	2	5	5mm
186	-31	48				
189	-34	46	3	3	2	10mm

X	Y	Z	ΔX	ΔY	ΔZ	6A
189	-31	50				
195	-22	37	6	9	13	2mm
189	-31	50				
194	-32	42	5	1	8	5mm
185	-34	47				
187	-36	45	2	2	2	10mm

X	Y	Z	ΔX	ΔY	ΔZ	7A
188	-28	52				
196	-16	35	8	12	17	2mm
186	-35	50				
193	-38	41	7	3	9	5mm
188	-36	49				
191	-40	46	3	4	3	10mm

X	Y	Z	ΔX	ΔY	ΔZ	8A
100	-54	140				
108	-47	123	8	7	17	2mm
97	-54	136				
102	-50	128	5	4	8	5mm
95	-62	130				
96	-56	129	1	6	1	10mm

X	Y	Z	ΔX	ΔY	ΔZ	9A
193	-31	55				
202	-16	31	9	15	24	2mm
193	-27	55				
198	-32	45	5	5	10	5mm
189	-30	50				
194	-32	49	5	2	1	10mm

Current carrying conductor is placed near Z-axis

X	Y	Z	ΔX	ΔY	ΔZ	1A
191	-34	57				
195	-24	55	4	10	2	2mm
195	-35	55				
197	-32	56	2	3	1	5mm
195	-37	54				
198	-35	55	3	2	1	10mm

X	Y	Z	ΔX	ΔY	ΔZ	2A
191	-33	57				
196	-19	52	5	14	5	2mm
193	-35	56				
198	-31	58	5	4	2	5mm
197	-37	54				
198	-35	56	1	2	2	10mm

X	Y	Z	ΔX	ΔY	ΔZ	3A
188	-33	43				
192	-10	51	4	23	8	2mm
201	-34	42				
205	-30	50	4	4	8	5mm
205	-36	41				
203	-35	44	2	1	3	10mm

X	Y	Z	ΔX	ΔY	ΔZ	4A
188	-34	44				
193	0	57	5	34	13	2mm
199	-34	42				
202	-31	50	3	3	8	5mm
204	-38	41				
205	-37	45	1	1	4	10mm

X	Y	Z	ΔX	ΔY	ΔZ	5A
190	-27	51				
202	22	68	12	49	17	2mm
203	-32	49				
208	-27	61	5	5	12	5mm
209	-49	45				
212	-45	48	3	4	3	10mm

X	Y	Z	ΔX	ΔY	ΔZ	6A
190	-29	51				
202	22	68	12	51	17	2mm
204	-30	50				
208	-28	60	4	2	10	5mm
209	-51	45				
211	-46	49	2	5	4	10mm

X	Y	Z	ΔX	ΔY	ΔZ	7A
192	-34	64				
202	-22	44	10	12	20	2mm
201	-34	62				
205	-28	67	4	6	5	5mm
203	-47	62				
205	-42	65	2	5	3	10mm

X	Y	Z	ΔX	ΔY	ΔZ	8A
193	-41	65				
204	-5	38	11	36	27	2mm
199	-41	63				
206	-25	57	7	16	6	5mm
203	-47	62				
206	-43	65	3	4	3	10mm

X	Y	Z	ΔX	ΔY	ΔZ	9A
193	-18	52				
203	40	42	10	58	10	2mm
190	-20	52				
213	-13	60	23	7	8	5mm
190	-16	50				
208	-41	58	18	25	8	10mm

APPENDIX C

Pseudo-Code for Position Sensor (Arduino UNO)

```
#include <Wire.h>
#include <HMC5883L.h>

HMC5883L compass;
int error = 0;

void setup()
{
	Serial.begin(9600);
	Serial.println("Starting I2C Interface");
	Wire.begin();
	Serial.println("Constructing New HMC5883L");
	compass = HMC5883L();
	Serial.println("Setting scale to +/- 1.3 Ga");
	error = compass.SetScale(8.1);

	if(error != 0)
		Serial.println(compass.GetErrorText(error));

	Serial.println("Setting measurement mode to continuous");
	error = compass.SetMeasurementMode(Measurement_Continuous);
	if (error != 0)
		Serial.println(compass.GetErrorText(error));
```

```
	pinMode(4,OUTPUT);
}

void loop()
{
	MagnetometerRaw raw = compass.ReadRawAxis();
	MagnetometerScaled scaled = compass.ReadScaledAxis();
	int MilliGauss_OnTheXAxis = scaled.XAxis;

	float heading = atan2(scaled.YAxis,scaled.XAxis);
	float declinationAngle = 0.0457;
	heading += declinationAngle;

	if(heading < 0)
		heading += 2*PI;
	if (heading > 2*PI)
		heading -= 2*PI;

	float headingDegrees = heading * 180/M_PI;

	Output(raw,scaled,heading,headingDegrees);

	delay(2000);

	if(heading > 4)
		digitalWrite(8,HIGH);
	else
```

```
                digitalWrite(8,LOW);
}

void Output(MagnetometerRaw raw, MagnetometerScaled scaled, float heading, float headingDegrees)
{
        Serial.print("Raw:\t");
        Serial.print(raw.XAxis);
        Serial.print("   ");
        Serial.print(raw.YAxis);
        Serial.print("   ");
        Serial.print(raw.ZAxis);

        Serial.print("   \tScaled:\t");
        Serial.print(scaled.XAxis);
        Serial.print("   ");
        Serial.print(scaled.YAxis);
        Serial.print("   ");
        Serial.print(scaled.ZAxis);

        Serial.print("   \tHeading:\t");
        Serial.print(heading);
        Serial.print(" Radians   \t");
        Serial.print(headingDegrees);
        Serial.println(" Degrees   \t");
 }
```

APPENDIX D

Pseudo-Code for Position Sensor (ATMEL)

```
#define F_CPU 1600000UL
#include <asf.h>
#include <util/delay.h>
#include <avr/io.h>

#define USART_SERIAL                    &USARTA1
#define USART_SERIAL_BAUDRATE           9600
#define USART_SERIAL_CHAR_LENGTH        USART_CHSIZE_8BIT_gc
#define USART_SERIAL_PARITY             USART_PMODE_DISABLED_gc
#define USART_SERIAL_STOP_BIT           false

#define SLAVE_BUS_ADDR 0x1E

#define status0x08      "TWI: START transmitted.\r\n"
#define sizeof0x08      sizeof(status0x08)
#define status0x10      "TWI: REPEAT START transmitted\r\n"
#define sizeof0x10      sizeof(status0x10)
#define status0x18      "TWI: SLA+W transmitted, ACK received.\r\n"
#define sizeof0x18      sizeof(status0x18)
#define status0x20      "TWI: SLA+W transmitted, NACK received.\r\n"
#define sizeof0x20      sizeof(status0x20)
#define status0x28      "TWI: Data byte transmitted, ACK received.\r\n"
#define sizeof0x28      sizeof(status0x28)
#define status0x30      "TWI: Data byte transmitted, NACK received.\r\n"
```

```
#define sizeof0x30     sizeof(status0x30)
#define status0x40     "TWI: SLA+R transmitted, ACK received.\r\n"
#define sizeof0x40     sizeof(status0x40)
#define status0x50     "TWI: Data byte received, ACK has been returned.\r\n"
#define sizeof0x50     sizeof(status0x50)
#define statusstop     "TWI: Stop Transmitted.\r\n"
#define sizeofstop     sizeof(statusstop)

int k;

int x_axis,y_axis,z_axis;

int tempx[1000],tempy[1000],tempz[1000];

int tempmx,templx,tempmy,temply,tempmz,templz;

UsartPrintStatus (int status)
{
        if (status==0x08)
        {
                for(int i=0;i<sizeof0x08;i++)
                {
                        usart_putchar(USART_SERIAL, status0x08[i]);
                }
        }
        if (status==0x10)
        {
```

```
        for(int i=0;i<sizeof0x10;i++)
        {
                usart_putchar(USART_SERIAL, status0x10[i]);
        }
}
if (status==0x18)
{
        for(int i=0;i<sizeof0x18;i++)
        {
                usart_putchar(USART_SERIAL, status0x18[i]);
        }
}
if (status==0x20)
{
        for(int i=0;i<sizeof0x20;i++)
        {
                usart_putchar(USART_SERIAL, status0x20[i]);
        }
}
if (status==0x28)
{
        for(int i=0;i<sizeof0x28;i++)
        {
                usart_putchar(USART_SERIAL, status0x28[i]);
        }
}
if (status==0x30)
```

```
{
        for(int i=0;i<sizeof0x30;i++)
        {
                usart_putchar(USART_SERIAL, status0x30[i]);
        }
}
if (status==0x40)
{
        for(int i=0;i<sizeof0x40;i++)
        {
                usart_putchar(USART_SERIAL, status0x40[i]);
        }
}
if (status==0x50)
{
        for(int i=0;i<sizeof0x50;i++)
        {
                usart_putchar(USART_SERIAL, status0x50[i]);
        }
}
if (status=="s")
{
        for(int i=0;i<sizeofstop;i++)
        {
                usart_putchar(USART_SERIAL, statusstop[i]);
        }
}
```

```
}

void usart_init(void)
{
	static usart_rs232_options_t USART_SERIAL_OPTIONS = {
		.baudrate = USART_SERIAL_BAUDRATE,
		.charlength = USART_SERIAL_CHAR_LENGTH,
		.paritytype = USART_SERIAL_PARITY,
		.stopbits = USART_SERIAL_STOP_BIT
	};

	usart_init_rs232(USART_SERIAL, &USART_SERIAL_OPTIONS);
}

TWI_Start()
{
	TWCR |= (1<<TWINT) | (1<<TWSTA) | (1<<TWEN);
	TWInterrupt TWStart TWEnable
	while (!(TWCR & (1<<TWINT)));
}

TWI_SendByte(int WMem)
{
	TWDR = WMem;
	TWCR = (1<<TWINT) | (1<<TWEN) | (1<<TWEA);
	while (!(TWCR & (1<<TWINT)));
}
```

```
TWI_SendByte_NACK(int WMem)
{
        TWDR = WMem;
        TWCR = (1<<TWINT) | (1<<TWEN) | (0<<TWEA);
        while (!(TWCR & (1<<TWINT)));
}

TWI_Read(int RMem)
{
        TWDR = RMem;
        TWCR = (1<<TWINT) | (1<<TWEA);
        while (!(TWCR & (1<<TWINT)));
}

TWI_Stop()
{
        TWCR = (1<<TWINT) | (1<<TWEN) | (1<<TWEA);
        _delay_ms(600);
}

int main (void)
{
                board_init();
                sysclk_init();
                usart_init();
                int k=0;
```

```
while(1)
{
        MCUCR = (0<<PUD);
        DDRD = (0<<PD1) | (0<<PD0);
        PRR0 = (0<<PRTWI);

        TWBR = 72;
        TWCR = (0<<TWIE);
        TWSR = ((0<<TWPS0) | (0<<TWPS1));

TWI_Start();
TWI_SendByte(0x3C);
TWI_SendByte(0x00);
TWI_SendByte(0x70);
TWI_Start();
TWI_SendByte(0x3C);
TWI_SendByte(0x01);
TWI_SendByte(0xA0);
TWI_Stop();

TWI_Start();
TWI_SendByte(0x3C);
TWI_SendByte(0x02);
TWI_SendByte(0x01);
TWI_Stop();
```

```
TWI_Start();
TWI_SendByte(0x3C);
TWI_SendByte(0x02);
TWI_Stop();

TWI_Start();
TWI_SendByte(0x3D);
TWI_SendByte(0x3D);
int xmsb = TWDR;
TWI_SendByte(0x3D);
int xlsb = TWDR;
x_axis = (xmsb<<8) | (xlsb);
uint8_t bufferx[16];

tempx[1000];
tempx[k]=x_axis;

itoa(x_axis,bufferx,10);

tempmx=tempx[10]+5;
templx=tempx[10]-5;

TWI_SendByte(0x3D);
int zmsb = TWDR;
TWI_SendByte(0x3D);
int zlsb = TWDR;
z_axis = (zmsb<<8) | (zlsb);
```

```
uint8_t bufferz[16];

tempz[1000];
tempz[k]=z_axis;

itoa(z_axis,bufferz,10);

tempmz=tempz[10]+5;
templz=tempz[10]-5;

TWI_SendByte(0x3D);
int ymsb = TWDR;
TWI_SendByte(0x3D);
int ylsb = TWDR;
y_axis = (ymsb<<8) | (ylsb);
uint8_t buffery[16];

tempy[1000];
tempy[k]=y_axis;
itoa(y_axis,buffery,10);
tempmy=tempy[10]+5;
temply=tempy[10]-5;

if(x_axis<tempmx && x_axis>templx && y_axis<tempmy &&
y_axis>temply && z_axis<tempmz && z_axis>templz)
{
        DDRB = 0xFF;
        PORTB = 0x00
```

```
}
_delay_ms(100);
}
else
{
        DDRB = 0xFF;
        PORTB= 0xFF;
        while(!(PINE & (1<<PINE4)))
        {
                k=0;
        }
}
k++;
usart_putchar(USART_SERIAL, 'x');
usart_putchar(USART_SERIAL, '=');
for (int i=0;i<sizeof(bufferx);i++)
{
        usart_putchar(USART_SERIAL, bufferx[i]);
}
usart_putchar(USART_SERIAL, 32);
usart_putchar(USART_SERIAL, 'y');
usart_putchar(USART_SERIAL, '=');

for (int i=0;i<sizeof(buffery);i++)
{
        usart_putchar(USART_SERIAL, buffery[i]);
}
```

```
                usart_putchar(USART_SERIAL, 32);
                usart_putchar(USART_SERIAL, 'z');
                usart_putchar(USART_SERIAL, '=');
                for (int i=0;i<sizeof(bufferz);i++)
                {
                        usart_putchar(USART_SERIAL, bufferz[i]);
                }

                usart_putchar(USART_SERIAL, 10);
                usart_putchar(USART_SERIAL, 13);



                TWI_Stop();
                _delay_ms(10);

        }
}
```

APPENDIX E

Pseudo-Code for Wireless Controller (ATMEL)

```
#include "astudio/includes.h"

int x_axis, y_axis, z_axis, ux, uy, uz, lx, ly, lz;
int temp = 0;
int count = 1;
unsigned short ee_x, ee_y, ee_z;
unsigned char ee_xmsb, ee_xlsb, ee_ymsb, ee_ylsb, ee_zmsb, ee_zlsb;
int xmsb, xlsb, ymsb, ylsb, xlsb, zmsb, zlsb;

#if defined(PLATFORM_ZIGBIT)
HAL_GPIO_PIN(LED, B, 5);
HAL_GPIO_PIN(BUTTON, E, 6);

#elif defined(PLATFORM_ZIGBIT_X0)
HAL_GPIO_PIN(LED, A, 5);
HAL_GPIO_PIN(BUTTON, E, 5);

#elif defined(PLATFORM_RCB128RFA1) ||
defined(PLATFORM_RCB256RFR2)
HAL_GPIO_PIN(LED, E, 2);
HAL_GPIO_PIN(BUTTON, E, 5);

#elif defined(PLATFORM_XPLAINED_PRO_ATMEGA256RFR2)
HAL_GPIO_PIN(LED, B, 4);
```

```
HAL_GPIO_PIN(BUTTON, E, 4);

#elif defined(PLATFORM_XPLAINED_PRO_SAMD20_RZ600) ||
 defined(PLATFORM_XPLAINED_PRO_SAMD20_REB)
HAL_GPIO_PIN(LED, A, 14);
HAL_GPIO_PIN(BUTTON, A, 15);

#elif defined(PLATFORM_XPLAINED_PRO_SAMR21)
HAL_GPIO_PIN(LED, A, 19);
HAL_GPIO_PIN(BUTTON, A, 28);

#else
  #error Unsupported platform
#endif

typedef enum AppState_t
{
        APP_STATE_INITIAL,
        APP_STATE_IDLE,
        APP_STATE_WAIT_CONF,
} AppState_t;

typedef struct AppMessage_t
{
        uint8_t buttonState;
} AppMessage_t;
```

```
static AppState_t appState = APP_STATE_INITIAL;
static AppMessage_t appMessage;
static NWK_DataReq_t appNwkDataReq;
static bool appButtonState = false;

static void appDataConf(NWK_DataReq_t *req)
{
	appState = APP_STATE_IDLE;
	(void)req;
}

static void appSendMessage(uint8_t state)
{
	appMessage.buttonState = state;

	appNwkDataReq.dstAddr = 1 - APP_ADDR;
	appNwkDataReq.dstEndpoint = APP_ENDPOINT;
	appNwkDataReq.srcEndpoint = APP_ENDPOINT;
	appNwkDataReq.options = NWK_OPT_ACK_REQUEST |
	NWK_OPT_ENABLE_SECURITY;
	appNwkDataReq.data = (uint8_t *)&appMessage;
	appNwkDataReq.size = sizeof(appMessage);
	appNwkDataReq.confirm = appDataConf;

	NWK_DataReq(&appNwkDataReq);

	appState = APP_STATE_WAIT_CONF;
}
```

```
static bool appDataInd(NWK_DataInd_t *ind)
{
	AppMessage_t *msg = (AppMessage_t *)ind->data;
	if (msg->buttonState)
	{
		PORTB ^= (1 << PINB4);
	}

	return true;
}

static void APP_TaskHandler(void)
{
	switch (appState)
	{
		case APP_STATE_INITIAL:
		{
			HAL_GPIO_BUTTON_in();
			HAL_GPIO_BUTTON_pullup();

			NWK_SetAddr(APP_ADDR);
			NWK_SetPanId(APP_PANID);
			PHY_SetChannel(APP_CHANNEL);
			PHY_SetRxState(true);
			NWK_SetSecurityKey((uint8_t *)"Security12345678");
			NWK_OpenEndpoint(APP_ENDPOINT, appDataInd);
```

```
        appState = APP_STATE_IDLE;
} break;

case APP_STATE_IDLE:
{
        if (appButtonState != PINE & (1<<PINE4))
        {
                appButtonState = HAL_GPIO_BUTTON_read();
                appSendMessage(appButtonState);
        }

        if(!(PINE & (1<<PINE4)))
        {
                appSendMessage(1);
                _delay_ms(20);
        }

        if(TCNT1 > 31250)
        {
                TCNT1 = 0;
                PORTB ^= (1 << PINB4);
        }
} break;

case APP_STATE_WAIT_CONF:
break;
```

```
        }
}

int main(void)
{
        SYS_Init();

        DDRB |= (1 << PINB4);
        PORTB &= ~(1 << PINB4);

        TCCR1B = 0x03;
        TCNT1 = 0x0;

        while (1)
        {
                SYS_TaskHandler();
                APP_TaskHandler();
        }
}
```

APPENDIX F

Pseudo-Code for NODAS (ATMEL)

```
#include "astudio/includes.h"

int x_axis, y_axis, z_axis, ux, uy, uz, lx, ly, lz;
unsigned short ee_x, ee_y, ee_z;
unsigned char ee_xmsb, ee_xlsb, ee_ymsb, ee_ylsb, ee_zmsb, ee_zlsb;
int xmsb, xlsb, ymsb, ylsb, xlsb, zmsb, zlsb;
int count = 0;
char disabled = 0;

#if defined(PLATFORM_ZIGBIT)
        HAL_GPIO_PIN(LED, B, 5);
        HAL_GPIO_PIN(BUTTON, E, 6);

#elif defined(PLATFORM_ZIGBIT_X0)
        HAL_GPIO_PIN(LED, A, 5);
        HAL_GPIO_PIN(BUTTON, E, 5);

#elif defined(PLATFORM_RCB128RFA1) ||
defined(PLATFORM_RCB256RFR2)
        HAL_GPIO_PIN(LED, E, 2);
        HAL_GPIO_PIN(BUTTON, E, 5);

#elif defined(PLATFORM_XPLAINED_PRO_ATMEGA256RFR2)
        HAL_GPIO_PIN(LED, B, 4);
```

```
        HAL_GPIO_PIN(BUTTON, E, 4);

#elif defined(PLATFORM_XPLAINED_PRO_SAMD20_RZ600) ||
defined(PLATFORM_XPLAINED_PRO_SAMD20_REB)
        HAL_GPIO_PIN(LED, A, 14);
        HAL_GPIO_PIN(BUTTON, A, 15);

#elif defined(PLATFORM_XPLAINED_PRO_SAMR21)
        HAL_GPIO_PIN(LED, A, 19);
        HAL_GPIO_PIN(BUTTON, A, 28);

#else
        #error Unsupported platform
#endif

typedef enum AppState_t
{
        APP_STATE_INITIAL,
        APP_STATE_IDLE,
        APP_STATE_WAIT_CONF,
} AppState_t;

typedef struct AppMessage_t
{
        uint8_t buttonState;
} AppMessage_t;
```

```
static AppState_t appState = APP_STATE_INITIAL;
static AppMessage_t appMessage;
static NWK_DataReq_t appNwkDataReq;
static bool appButtonState = false;

static void appDataConf(NWK_DataReq_t *req)
{
	appState = APP_STATE_IDLE;
	(void)req;
}

static void appSendMessage(uint8_t state)
{
	appMessage.buttonState = state;

	appNwkDataReq.dstAddr = 1 - APP_ADDR;
	appNwkDataReq.dstEndpoint = APP_ENDPOINT;
	appNwkDataReq.srcEndpoint = APP_ENDPOINT;
	appNwkDataReq.options = NWK_OPT_ACK_REQUEST |
	NWK_OPT_ENABLE_SECURITY;
	appNwkDataReq.data = (uint8_t *)&appMessage;
	appNwkDataReq.size = sizeof(appMessage);
	appNwkDataReq.confirm = appDataConf;

	NWK_DataReq(&appNwkDataReq);

	appState = APP_STATE_WAIT_CONF;
}
```

```
static bool appDataInd(NWK_DataInd_t *ind)
{
	AppMessage_t *msg = (AppMessage_t *)ind->data;
	if (msg->buttonState)
	{
		LCDclear();
		LCDsetCursor(0,0);
		LCD_Write_Str("New position set");
		LCDsetCursor(0,1);
		LCD_Write_Str("and saved!!");
		PORTD ^= (1 << PIND6);
		PORTG ^= (1 << PING2);
		EEPROM_atomic_write(0x0000, xmsb);
		EEPROM_atomic_write(0x0001, xlsb);
		EEPROM_atomic_write(0x0002, ymsb);
		EEPROM_atomic_write(0x0003, ylsb);
		EEPROM_atomic_write(0x0004, zmsb);
		EEPROM_atomic_write(0x0005, zlsb);

		set_upper_lower();
		beep_buzzer();
		_delay_ms(400);
		disabled = 0;
		LCDclear();
		LCDsetCursor(0,0);
		LCD_Write_Str("PV RE-ENABLED!");
```

```
                _delay_ms(400);
                LCDclear();
                LCDsetCursor(0,0);
                LCD_Write_Str("x=");
                LCDsetCursor(0,1);
                LCD_Write_Str("y=");
                LCDsetCursor(7,1);
                LCD_Write_Str("z=");
        }

        return true;
}

static void APP_TaskHandler(void)
{
        switch (appState)
        {
                case APP_STATE_INITIAL:
                {
                        HAL_GPIO_BUTTON_in();
                        HAL_GPIO_BUTTON_pullup();

                        HAL_GPIO_LED_out();
                        HAL_GPIO_LED_set();

                        NWK_SetAddr(APP_ADDR);
                        NWK_SetPanId(APP_PANID);
```

```
        PHY_SetChannel(APP_CHANNEL);
        PHY_SetRxState(true);
        NWK_SetSecurityKey((uint8_t *)"Security12345678");
        NWK_OpenEndpoint(APP_ENDPOINT, appDataInd);

        appState = APP_STATE_IDLE;
} break;

case APP_STATE_IDLE:
{
        if (appButtonState != (PINE & 0x01))
        {
                appButtonState = HAL_GPIO_BUTTON_read();
                appSendMessage(appButtonState);
        }

        if (disabled != 1)
        {
                if(TCNT1 > 31250)
                {
                        TCNT1 = 0;
                        mag_single_measurement();
                        LCDsetCursor(2,0);
                        LCD_Write_Int(x_axis);
                        LCDsetCursor(2,1);
                        LCD_Write_Int(y_axis);
                        LCDsetCursor(9,1);
```

```
                                        LCD_Write_Int(z_axis);
                                    }
                                }
                            } break;
                            case APP_STATE_WAIT_CONF:
                            break;
                    }
}

int main(void)
{
        SYS_Init();
        TWI_init();
        LCD_Init();
        DDRD |= (1 << PIND6);
        DDRG |= (1 << PING2);
        DDRE |= (1 << PINE2);
        PORTD = (0 << PIND6);
        PORTG = (0 << PING2);

        DDRD |= (1<<PIND4);

        DPDS0 = 0xFF;

        TCCR1B = 0x03;
        TCNT1 = 0x0;
```

```
set_upper_lower();
if(check_location())
{
        LCDclear();
        PORTE &= ~(1 << PINE2);
        LCDsetCursor(0,0);
        LCD_Write_Str("Location Match");
        _delay_ms(500);
        LCDclear();
        LCDsetCursor(0,0);
        LCD_Write_Str("x=");
        LCDsetCursor(0,1);
        LCD_Write_Str("y=");
        LCDsetCursor(7,1);
        LCD_Write_Str("z=");
}
else
{
        PORTE |= (1 << PINE2);
        LCDclear();
        LCDsetCursor(0,0);
        LCD_Write_Str("Location Wrong!!!");
        disabled = 1;
        _delay_ms(500);
        LCDclear();
        LCDsetCursor(0,0);
        LCD_Write_Str("PV DISABLED!");
```

```
        }


        while (1)
        {
                SYS_TaskHandler();
                APP_TaskHandler();
        }
}
```

APPENDIX G

Datasheet of MOSFET IRF640N

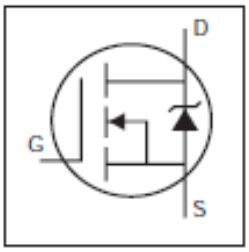
International
IOR Rectifier

PD - 94006A

IRF640N
IRF640NS
IRF640NL

HEXFET® Power MOSFET

- Advanced Process Technology
- Dynamic dv/dt Rating
- 175°C Operating Temperature
- Fast Switching
- Fully Avalanche Rated
- Ease of Paralleling
- Simple Drive Requirements



V_{DSS} = 200V

$R_{DS(on)}$ = 0.15Ω

I_D = 18A

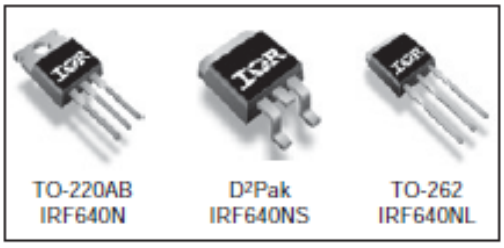
Description

Fifth Generation HEXFET® Power MOSFETs from International Rectifier utilize advanced processing techniques to achieve extremely low on-resistance per silicon area. This benefit, combined with the fast switching speed and ruggedized device design that HEXFET Power MOSFETs are well known for, provides the designer with an extremely efficient and reliable device for use in a wide variety of applications.

The TO-220 package is universally preferred for all commercial-industrial applications at power dissipation levels to approximately 50 watts. The low thermal resistance and low package cost of the TO-220 contribute to its wide acceptance throughout the industry.

The D^2Pak is a surface mount power package capable of accommodating die sizes up to HEX-4. It provides the highest power capability and the lowest possible on-resistance in any existing surface mount package. The D^2Pak is suitable for high current applications because of its low internal connection resistance and can dissipate up to 2.0W in a typical surface mount application.

The through-hole version (IRF640NL) is available for low-profile application.



TO-220AB IRF640N | D^2Pak IRF640NS | TO-262 IRF640NL

Absolute Maximum Ratings

	Parameter	Max.	Units
I_D @ T_C = 25°C	Continuous Drain Current, V_{GS} @ 10V	18	A
I_D @ T_C = 100°C	Continuous Drain Current, V_{GS} @ 10V	13	
I_{DM}	Pulsed Drain Current ①	72	
P_D @T_C = 25°C	Power Dissipation	150	W
	Linear Derating Factor	1.0	W/°C
V_{GS}	Gate-to-Source Voltage	± 20	V
E_{AS}	Single Pulse Avalanche Energy②	247	mJ
I_{AR}	Avalanche Current①	18	A
E_{AR}	Repetitive Avalanche Energy①	15	mJ
dv/dt	Peak Diode Recovery dv/dt ⑤	8.1	V/ns
T_J T_{STG}	Operating Junction and Storage Temperature Range	-55 to +175	°C
	Soldering Temperature, for 10 seconds	300 (1.6mm from case)	
	Mounting torque, 6-32 or M3 srew④	10 lbf•in (1.1N•m)	

Electrical Characteristics @ T_J = 25°C (unless otherwise specified)

	Parameter	Min.	Typ.	Max.	Units	Conditions
$V_{(BR)DSS}$	Drain-to-Source Breakdown Voltage	200	—	—	V	V_{GS} = 0V, I_D = 250µA
$\Delta V_{(BR)DSS}/\Delta T_J$	Breakdown Voltage Temp. Coefficient	—	0.25	—	V/°C	Reference to 25°C, I_D = 1mA
$R_{DS(on)}$	Static Drain-to-Source On-Resistance	—	—	0.15	Ω	V_{GS} = 10V, I_D = 11A ③
$V_{GS(th)}$	Gate Threshold Voltage	2.0	—	4.0	V	V_{DS} = V_{GS}, I_D = 250µA
g_{fs}	Forward Transconductance	6.8	—	—	S	V_{DS} = 50V, I_D = 11A ③
I_{DSS}	Drain-to-Source Leakage Current	—	—	25	µA	V_{DS} = 200V, V_{GS} = 0V
		—	—	250		V_{DS} = 160V, V_{GS} = 0V, T_J = 150°C
I_{GSS}	Gate-to-Source Forward Leakage	—	—	100	nA	V_{GS} = 20V
	Gate-to-Source Reverse Leakage	—	—	-100		V_{GS} = -20V
Q_g	Total Gate Charge	—	—	67	nC	I_D = 11A
Q_{gs}	Gate-to-Source Charge	—	—	11		V_{DS} = 160V
Q_{gd}	Gate-to-Drain ("Miller") Charge	—	—	33		V_{GS} = 10V, See Fig. 6 and 13
$t_{d(on)}$	Turn-On Delay Time	—	10	—	ns	V_{DD} = 100V
t_r	Rise Time	—	19	—		I_D = 11A
$t_{d(off)}$	Turn-Off Delay Time	—	23	—		R_G = 2.5Ω
t_f	Fall Time	—	5.5	—		R_D = 9.0Ω, See Fig. 10 ③
L_D	Internal Drain Inductance	—	4.5	—	nH	Between lead, 6mm (0.25in.)
L_S	Internal Source Inductance	—	7.5	—		from package and center of die contact
C_{iss}	Input Capacitance	—	1160	—	pF	V_{GS} = 0V
C_{oss}	Output Capacitance	—	185	—		V_{DS} = 25V
C_{rss}	Reverse Transfer Capacitance	—	53	—		f = 1.0MHz, See Fig. 5

Source-Drain Ratings and Characteristics

	Parameter	Min.	Typ.	Max.	Units	Conditions
I_S	Continuous Source Current (Body Diode)	—	—	18	A	MOSFET symbol showing the integral reverse p-n junction diode.
I_{SM}	Pulsed Source Current (Body Diode)①	—	—	72		
V_{SD}	Diode Forward Voltage	—	—	1.3	V	T_J = 25°C, I_S = 11A, V_{GS} = 0V ③
t_{rr}	Reverse Recovery Time	—	167	251	ns	T_J = 25°C, I_F = 11A
Q_{rr}	Reverse Recovery Charge	—	929	1394	nC	di/dt = 100A/µs ③
t_{on}	Forward Turn-On Time	Intrinsic turn-on time is negligible (turn-on is dominated by L_S+L_D)				

Thermal Resistance

	Parameter	Typ.	Max.	Units
$R_{\theta JC}$	Junction-to-Case	—	1.0	°C/W
$R_{\theta CS}$	Case-to-Sink, Flat, Greased Surface ④	0.50	—	
$R_{\theta JA}$	Junction-to-Ambient④	—	62	
$R_{\theta JA}$	Junction-to-Ambient (PCB mount)⑤	—	40	

APPENDIX H

Datasheet of Microcontroller ATmega256RFR2

Features

- Network support by hardware assisted Multiple PAN Address Filtering
- Advanced Hardware assisted Reduced Power Consumption
- High Performance, Low Power AVR® 8-Bit Microcontroller
- Advanced RISC Architecture
  - 135 Powerful Instructions – Most Single Clock Cycle Execution
  - 32x8 General Purpose Working Registers / On-Chip 2-cycle Multiplier
  - Up to 16 MIPS Throughput at 16 MHz and 1.8V – Fully Static Operation
- Non-volatile Program and Data Memories
  - 256K/128K/64K Bytes of In-System Self-Programmable Flash
    - Endurance: 10'000 Write/Erase Cycles @ 125°C (25'000 Cycles @ 85°C)
  - 8K/4K/2K Bytes EEPROM
    - Endurance: 20'000 Write/Erase Cycles @ 125°C (100'000 Cycles @ 25°C)
  - 32K/16K/8K Bytes Internal SRAM
- JTAG (IEEE std. 1149.1 compliant) Interface
  - Boundary-scan Capabilities According to the JTAG Standard
  - Extensive On-chip Debug Support
  - Programming of Flash EEPROM, Fuses and Lock Bits through the JTAG Interface
- Peripheral Features
  - Multiple Timer/Counter & PWM channels
  - Real Time Counter with Separate Oscillator
  - 10-bit, 330 ks/s A/D Converter; Analog Comparator; On-chip Temperature Sensor
  - Master/Slave SPI Serial Interface
  - Two Programmable Serial USART
  - Byte Oriented 2-wire Serial Interface
- Advanced Interrupt Handler and Power Save Modes
- Watchdog Timer with Separate On-Chip Oscillator
- Power-on Reset and Low Current Brown-Out Detector
- Fully Integrated Low Power Transceiver for 2.4 GHz ISM Band
  - High Power Amplifier support by TX spectrum side lobe suppression
  - Supported Data Rates: 250 kb/s and 500 kb/s, 1 Mb/s, 2 Mb/s
  - -100 dBm RX Sensitivity; TX Output Power up to 3.5 dBm
  - Hardware Assisted MAC (Auto-Acknowledge, Auto-Retry)
  - 32 Bit IEEE 802.15.4 Symbol Counter
  - SFD-Detection, Spreading; De-Spreading; Framing ; CRC-16 Computation
  - Antenna Diversity and TX/RX control / TX/RX 128 Byte Frame Buffer
  - Phase measurement support
- PLL synthesizer with 5 MHz and 500 kHz channel spacing for 2.4 GHz ISM Band
- Hardware Security (AES, True Random Generator)
- Integrated Crystal Oscillators (32.768 kHz & 16 MHz, external crystal needed)
- I/O and Package
  - 38 Programmable I/O Lines
  - 64-pad QFN (RoHS/Fully Green)
- Temperature Range: -40°C to 125°C Industrial
- Ultra Low Power consumption (1.8 to 3.6V) for AVR & Rx/Tx: 10.1mA/18.6 mA
  - CPU Active Mode (16MHz): 4.1 mA
  - 2.4GHz Transceiver: RX_ON 6.0 mA / TX 14.5 mA (maximum TX output power)
  - Deep Sleep Mode: <700nA @ 25°C
- Speed Grade: 0 – 16 MHz @ 1.8 – 3.6V range with integrated voltage regulators

Applications

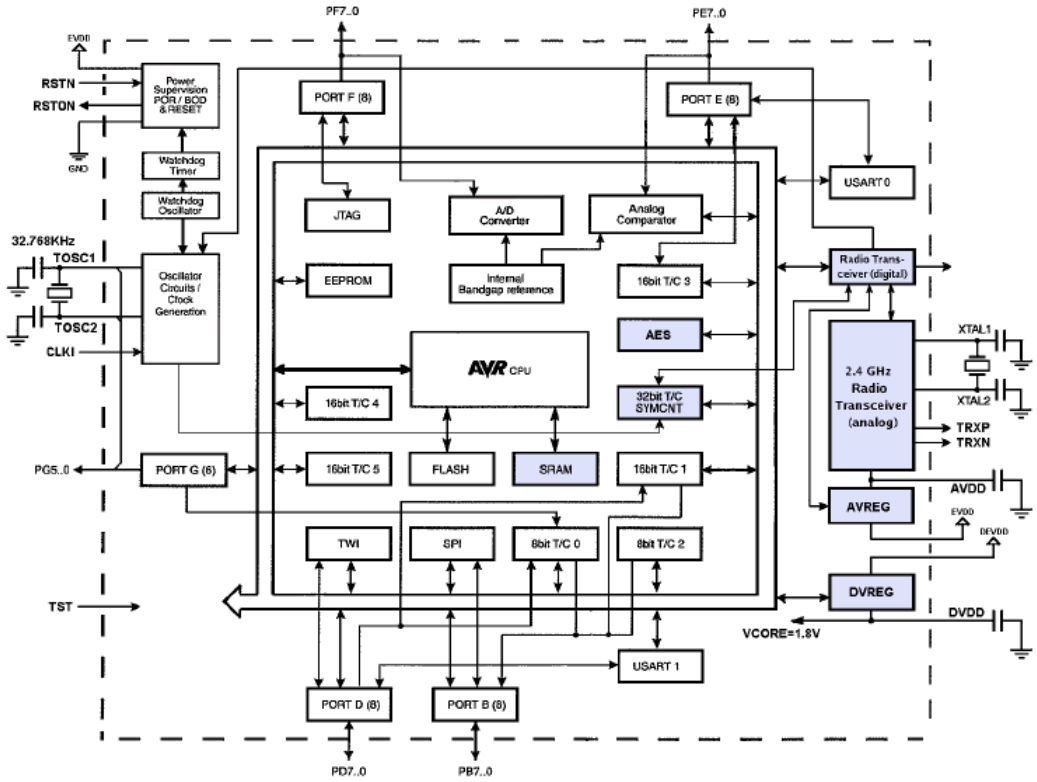
- ZigBee® / IEEE 802.15.4-2011/2006/2003™ – Full and Reduced Function Device
- General Purpose 2.4GHz ISM Band Transceiver with Microcontroller
- RF4CE, SP100, WirelessHART™, ISM Applications and IPv6 / 6LoWPAN

Atmel

8-bit AVR® Microcontroller with Low Power 2.4GHz Transceiver for ZigBee and IEEE 802.15.4

ATmega256RFR2
ATmega128RFR2
ATmega64RFR2

8350C-MCU Wireless-09/14


PF7..0
PE7..0
EVDD
RSTN
RSTON
GND
Power Supervision POR / BOD & RESET
Watchdog Timer
Watchdog Oscillator
32.768KHz
TOSC1
TOSC2
CLKI
Oscillator Circuits / Clock Generation
PG5..0
PORT G (6)
TST
PORT F (8)
PORT E (8)
JTAG
A/D Converter
Analog Comparator
USART 0
EEPROM
Internal Bandgap reference
16bit T/C 3
Radio Trans-ceiver (digital)
AES
AVR CPU
16bit T/C 4
32bit T/C SYMCNT
2.4 GHz Radio Transceiver (analog)
XTAL1
XTAL2
TRXP
TRXN
16bit T/C 5
FLASH
SRAM
16bit T/C 1
AVDD
AVREG
EVDD
DEVDD
TWI
SPI
8bit T/C 0
8bit T/C 2
DVREG
DVDD
VCORE=1.8V
USART 1
PORT D (8)
PORT B (8)
PD7..0
PB7..0

35 Electrical Characteristics

35.1 Absolute Maximum Ratings

Note that stresses beyond those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification are not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
T_{STOR}	Storage temperature		-50		150	°C
T_{LEAD}	Lead temperature	T = 10s (soldering profile compliant with IPC/JEDEC J-STD-020B)			260	°C
V_{ESD}	ESD robustness	Compliant to [4]	4			kV
P_{RF}	Input RF level				+14	dBm
V_{DDMAX}	Maximum voltage	Maximum voltage from any pin to ground	-0.3		3.6	V
V_{DMAXEV}	Maximum voltage difference between DEVDD and EVDD		-0.3		0.3	V
V_{DIG}	Voltage on all pins	except pins 8,9,21,22,60,62	-0.3		V_{DDMAX}	V
V_{ANA}	Voltage on pins 8,9,21,22,60,62		-0.3		2.0	V
V_{COMP_IN}	Comparator input voltage	Pins with Comparator input connected by the analog multiplexer	-0.3		V_{DDMAX}	V
V_{PGA_IN}	PGA input voltage	Pins with PGA input connected by the analog multiplexer	-0.3		V_{DDMAX}	V
V_{ADC_IN}	ADC input voltage	Pins with ADC input connected by the analog multiplexer (PGA bypassed)	-0.3		2.0	V

35.2 Recommended Operating Range

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
T_{OP_ZU}	Operating temperature range		-40		+85	°C
T_{OP_ZF}	Operating temperature range		-40		+125	°C
V_{DD}	Supply voltage	Voltage on pins 23,34,44,54,59[2]	1.8	3.0	3.6	V
V_{DEV}	Voltage difference between DEVDD and EVDD	EVDD and DEVDD should be tight together on the PCB		0.0		V
$V_{DD1.8}$	Supply voltage (on pins 21,22,60)	External voltage supply[1]	1.7	1.8	1.9	V
V_{OVRDRV}	Pin Overdrive voltage	Pin Voltage exceeding supply voltage except pins 8,9,21,22,60,62			+0.3	V