IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

# International Journal of Advanced Research

## in Electrical, Electronics and Instrumentation Engineering

Volume 11, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.18

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 5, May 2022||

|DOI:10.15662/IJAREEIE.2022.1105032 |

# Use of Renewable Energy Systems to Ensure Energy Security in Supply System Failure Scenarios

**Vishal V. Mehtre, Udbhav Singh**

Assistant Professor, Department of Electrical Engineering , Bharati Vidyapeeth (Deemed To Be University) College of Engineering, Pune, Maharashtra, India

Student of Bachelors of Technology, Department of Electrical Engineering , Bharati Vidyapeeth (Deemed To Be University) College of Engineering, Pune, Maharashtra, India

**ABSTRACT :** The paper examines the role of security in energy sector as well as its implementation in renewable energy. The terms regarding energy security are introduced which are then followed by the implementation of mentioned terms in the renewable energy sector. We also discuss the future of the renewable energy sector & its future implications in terms of security. We also discuss mitigation techniques to ensure energy security & maintain maximum possible benefits both at the consumer end as well as the seller end while maintaining a balance between monetary benefits for both the consumer & the selller. We also discuss the climatic implications of the renewable energy sector.

**KEYWORDS :**- Security , Renewable Energy , Energy

## I.INTRODUCTION

Energy security plays an extremely important factor in our day to day lives directly or indirectly. Energy is required by us on a daily basis for basic living needs & even powering the appliances we use on a daily basis. On the other hand the industries responsible for fulfilling our basic needs also rely on the energy sector to function.
The energy security can be disrupted by factors both manmade or natural. In this current age of technology cyberattacks also pose a dangerous threat to energy security. The installation of smart systems in powerplants & grids opens up a new paradigm for malwares to infiltrate the systems & cause damage.
The definition of Energy Security according to International Energy Agency is “the uninterrupted availability of energy sources at an affordable price”. IEA also differentiates long term as well as short term energy security.

## II. NATURAL THREATS TO ENERGY SECURITY

Natural Disasters pose a threat to energy security. The damage done by natural disasters like floods , earthquakes , tsunamis etc are extremely dangerous & cause long term damage to power supply while at times posing a risk to people relying on the energy supply as well as people living around generation plants.
On 11$^{th}$ March , 2011 Japan was hit by Tohoku Eathquake & Tsunami. On detection of earthquake, [1]the computers automatically shut down the normal power generating reactors . But due to the shutdown & grid problems the reactors electrical supply failed & the emergency diesel generator was turned on. The generators powered the pumps that pumped coolants throughout the system to make sure that the decaying material was being cooled of as nuclear fuels by their very nature radiate heat energy even after fission has ceased.
But soon a tsunami hit the shores due to which the diesel generators that were supposed to pump the coolants failed . The result were three nuclear meltdowns , followed by three hydrogen explosions & release of radioactive compounds causing contamination. Reactor units 1-3 suffered from core meltdown while reactor 4 exploded. [7]

A large number of people were evacuated & an excluion zone was setup. The damaged reactors also caused an increase in environmental ionizing radiation which posed a serious threat of ARS , and long term risks such as cancer & birth defects amongst pregnant women.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 5, May 2022||

|DOI:10.15662/IJAREEIE.2022.1105032 |

A large amount of radioactive water was also released into the oceans which caused an increase in radio nuclides concentration of ocean water.
This disaster lead to the formation of anti-nuclear sentiments amongst people all around the world. Further, many countries around the world decreased construction of nuclear powered reactors & shifted to non-nuclear especially fossil fuel sources. These sources are extremely polluting & are also non-abundant.
Further post Fukushima the loss of reactors meant that the power requirements of the consumers that relied on those reactors were not being met. Emergency services also felt the brunt of power outages.
Using Renewable Energy for Energy Security means , that solar farms , wind farms , etc couldve been setup in order to bridge the supply gap that was created post disaster. Further , post disaster , the reliance on fossil fuels couldve been prevented & renewable sources couldve been used a replacement.
In 2021 a similar earthquake hit Fukushima causing power outage. This time 6 coal & gas fired production units were knocked out causing a supply gap of 3.6GW in the system.
Fukushima was marked Level 7 event on International Nuclear Event Scale.'

## III. MAN MADE THREATS TO ENERGY SECURITY

The man made threats can be broadly categorized into 3 parts :
3.1. Over Use & Over Reliance on Fossil Fuels & Non Renewable sources of energy
Fossil Fuels are by far one of the most widely used sources of energy. Majority part of the energy sector runs on fossil fuels to meet their energy requirement & fulfill domestic & industrial demands.
Use of fossil fuels has serious effects such as pollution which causes global warming. Further , our over reliance on these sources also implies that sooner or later we will end up depleting them out of our environment. This will lead to scarcity of fuel which would further push up the price of these fuels indirectly making the electricity more expensive for the consumers.
India faced a serious shortage of coal post Covid Lockdown wherein the reserve stockpile of coal at powerplants was reaching below the bottom threshold limit. This meant running out of fuel would lead to load shedding followed by power outages in regions which relied on the power plant. Not only that to overcome this shortage , the country would require to import coal from other countries , sometimes at a more expensive rate in order to fulfill its energy sector demands. This is a serious threat as large chunk of India's energy sector ie.59.1% still relies on fossil fuels for generation[6].
The supply demand gap can be compensated by setting up solar farms. Many corporate organizations as well as the government have shown interest in setting up solar farms to bridge the supply demand gap & also decrease the overall cost of generation & monetary burden on end consumers.
Further the AQI index of regions surrounding the coal plants will also be improved & load shedding wont be necessary to manage resources.

3.2. Man Made construction & Design Failures
One of the reasons disasters take place can also be traced to design flaws in system which can be done both on purpose for cost cutting or by due negligence of design & safety procedures. Constructions done by both government as well as private firms have the basic idea of maximizing profits , at times doing cost cutting into their designs. Further, poor regulation by governement over critical infrastructure , corrupt inspectors , officials & bureaucrats & complete ignorance of laws & safety procedures can become dangeous to lead to chain of events that can cause severe damage to energy sector.
One of the prime examples of such a disaster is the Chernobyl Nuclear Disaster which is the worst possible nuclear disaster in history till date.
The Reactor test to be conducted on Reactor 4 was done to make sure that the generator worked in case of meltdown of reactor or shutdown due to unforseen reasons. The diesel generators job was to pump coolant inside reactor to keep the decaying nuclear fuel cooled. The test procedure was written by authors who were not well versed with the working of RBMK reactors. The test had already been unsuccessfully carried out in 1982 , 1984 , 1985 & even 1986. Further the test authors didn't take required permission from chief design authority of reactors or Soviet Nuclear safety regulators.
The objective was to disable the emergency core cooling system & simulate a loss of coolant in the reactor.
Now in order to conduct the test the engineers were instructed to decrease the power output of the reactor. On 25$^{th}$ April 1986 , the power output was dropped to 50% of the normal output by the beginning of the day shift. But the tests had to be delayed to compensate for the peak power demands in the evening. The reactor was run 11 hours outside test without any safety measures.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 5, May 2022||

|DOI:10.15662/IJAREEIE.2022.1105032 |

On the 26th April , the power was further decreased according to the test requirements. But the decrease in output meant that the fission byproduct of xenon-135 had not burned off which under normal condition wouldn't compromise safety of the reactor.
Due to the ongoing reaction the xenon 135 [3] would absorb neutrons from ongoing reaction & become the stable xenon 136.
But once the power was further lowered , the reactor got into a near complete shutdown state. The xenon 135 prevented the rise of reactor power. In order to increase the reactivity the control rods were pulled out of the core. The core temperature & coolant flow was unstable too.
The power was then bumped up & even after multiple warnings from the SKALA system , the test was carried out. The control rods were out of the core. The steam to turbines was shut off & the diesel generator was started.
After looking at the unstable conditions , the emergency shutdown button called AZ-5 was pressed the button was meant to push the control rods back into reactor to control the reaction. But the control rods themselves had a major design flaw , the tips of the control rod were made up of graphite[2] which boosted reactor output. This meant the the output of the reactor increased exponentially.
The reactor output increased to 10 times the normal output. The steam boiler blew off & damaged the coolant lines & fuel channels. This further caused the explosion that destroyed the eactor casing. This explosion ejected hot graphite into the atmosphere as well as the radioactive core was open & spewed radiation in the atmosphere.
For a long time the Soviet Party denied the occurence of such an accident , further the party ignored the presence of reactor design flaws. The party failed to take immediate actions & the design bureaus hid the design flaws.
The people had no idea of the implications of such an explosion & continued to live normally , the soviet party didn't take necessary evacuation actions of evacuating the people out of the area & setting up an exclusion zone. It was only on 27th April that the first evacuation buses showed up. By this time people were already exposed to monumental amounts of radiation , especially the first responders.
On 28th April radiation alarms were set off in a power plant in Sweden 1000kms away from ground zero. The Soviets later filed a report with the International Atomic Energy Agency but only reporting it as a minor accident. The celebrations in Kyiv werent postponed either.
Soviet Liquidators were called on that consisted of soldiers & men who were tasked of removing debris from the top of the reactor in order to build a sarcophagus to contain the radiation exposure.
Further to prevent the meltdown of nuclear fuel into water bodies below the reactor , liquid nitrogen condenser was implemented to prevent the seeping down of nuclear fuel.
The soviets didn't rectify the problems present in RBMK reactors for a long time. Which meant the control rod issue was present in the reactors post chernobyl.
Post fall of USSR , Russia decreased the positive void coefficient of RBMK reactors & made them a lot safer.
The supply gap caused on 25th April which led to increase in power output coudve been mitigated by other non nuclear power sources thus preventing a delay in tests & the disaster couldve been prevented.

3.3. CyberSecurity risks to Energy Security

Most grids today have implemented smart technologies to ensure maximum efficiency of their grids. These include cloud based measures in order to control the power supply. Smart Grids that automatically bridge supply gaps by balancing the supply from grids with energy deficiancy to grids with excess energy supply.
But the use of computers & their applications comes at a risk of cyberattacks.
The recent example of Russian hackers taking over Ukraine power supply infrastructure & blacking out regions in Ukraine while russian attacks preventing proper defence from Ukrainian side. Denial of Service attacks are widely used to overload servers & cause a shutdown.[4]
Another example would be of StuxNet[5] worm that was created by CIA & NSA on the pretext of Iranian nuclear plant producing nuclear weapons grade fuel to be used in weapons of mass destruction . It was spread in the Iranian Nuclear Facilities that later on spread to power supply facilities in the region. The worm was aimed to infiltrate the Siemens PLC in the nuclear facility.
The worm was injected using USB sticks dropped around the facility. Sooner one of the employees inserted the USB stick inside one of the computers which later spread to the entire system. Sooner the worm started targetting all siemens controller around the power plant & reached US shores.
A cybersecurity analyst at Kaspersky lab realized the existence of such a worm & notified the US governement about it.
Siemens has updated the PLC firmware , but the original StuxNet script has then been used to create multiple worms & attack power plants around the world.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 5, May 2022||

|DOI:10.15662/IJAREEIE.2022.1105032 |

Over reliance on computers has its own security problems which can be only mitigated by implementing serious security systems & running simulations in controlled environments to be prepared for a real attack.

## IV. CONCLUSION

Implementation of renewable sources of energy would be a boon for the energy sector as well as climatic conditions. The entire sector is based on the implementation of smart technologies & so we need to make sure that the computers controlling the system are protected from outside interference. Further we also need to take serious action against organizations that sell exploits in the market that are used by hackers to target these systems.[8]

We need to ensure energy security & setup renewable power plants in order to bridge the supply demand gap in order to maintain the supply required by critical infrastructure.

We also need to predict future natural or man made calamities. Use of modern technologies like AI can be used to assess previous year data & predict the scenarios to pin point at the next similar disaster. Regular drills & cyber secuity measures should be implemented to ensure proper proterction.

Lastly, we also need to prevent cost cutting & corruption by bureaucrats & employees. Proper regulatory measures need to be implemented & laws should be formulated to prevent such disasters & severe punishment should be laid out for people that fail to uphold the same.

Distributed Generation & Storage facilities like domestic solar panels , mini-hydro plants should be setup , so that in case of collapse of central infrastructure, local back up supply is present to provide supply to critical infrastructure. These systems are heavily decentralized & are located close to loads.[9]

Further having distributed generation & storage would mean a smaller region will be affected should the system fail.

## REFERENCES

[1]. “Yukiya Amano , Director General , International Atomic Energy Agency” , ‘The Fukushima Daiichi Accident Report’

[2]. “Mikhail V. Malko , Joint Institute of Power and Nuclear Research, National Academy of Sciences of Belarus”, ‘The Chernobyl Reactor : Design Features & Reasons for Accident’

[3]. “International Atomic Energy Agency: International Consultative Group on the Nuclear Safety” , ’The Chernobyl Accident’ , Vienna, 1993.

[4].”Tim Krause , Raphael Ernst , Benedikt Klaer , Immanuel Hacker , Martin Henze” , ‘CyberSecurity in Power Grids : Challenges & Opportunities’ , Cyber Analysis & Defense, Fraunhofer FKIE, 53343 Wachtberg, Germany

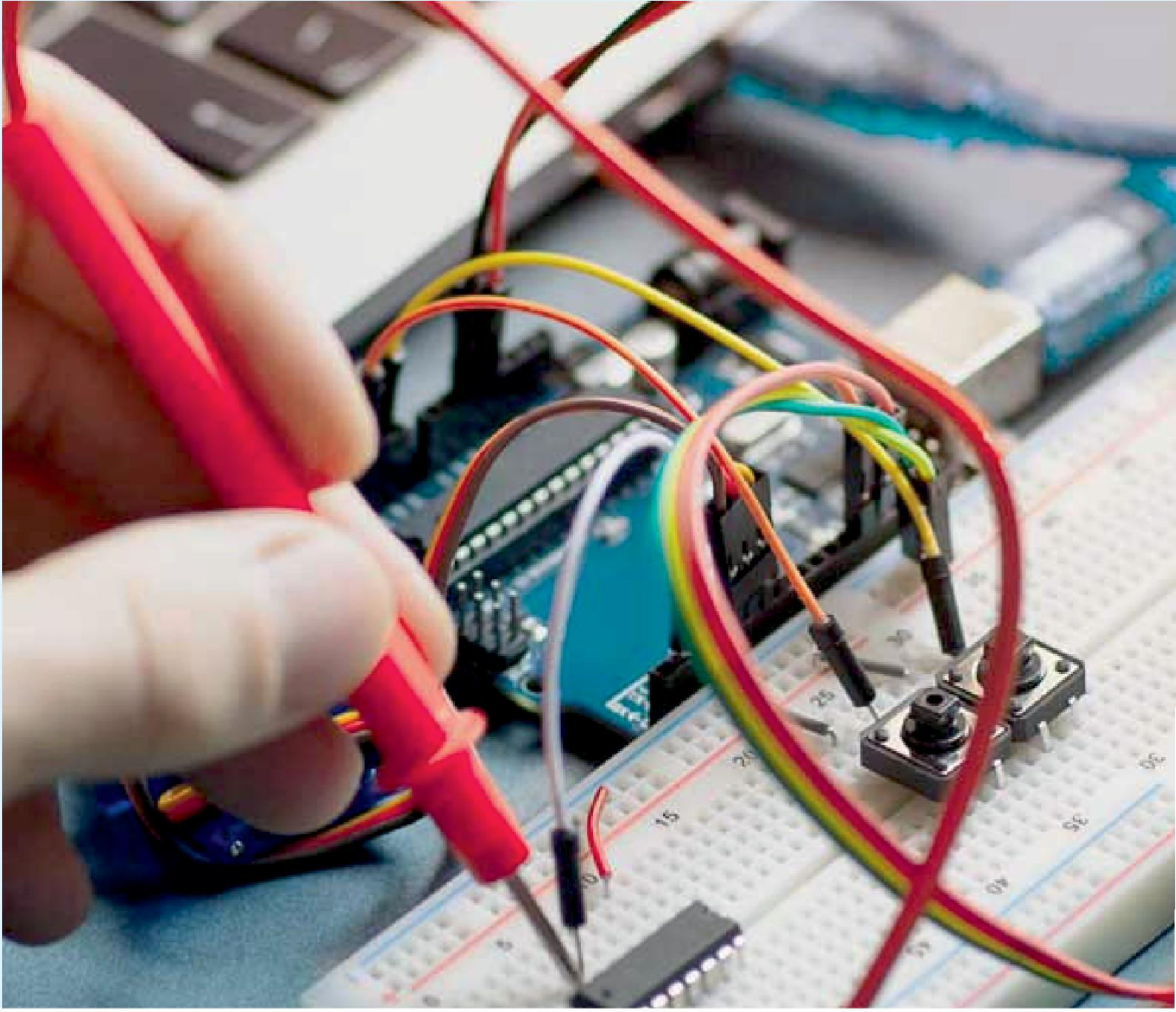
[5]. “Marie Baezner , Patrice Robin” , ‘Stuxnet’ , CSS Cyber Defense Project , 2018

[6]. “Ministry of Power” , ‘Power Sector at a Glance ALL INDIA’ , 2022

[7]. ”Atomic Energy Society of Japan” , ‘Overview of the Accident at the Fukushima Daiichi Nuclear Power Station’ , Springer , Tokyo , 2014

[8]. “Caroline Baylon” , ‘Lessons from Stuxnet & the Realm of Cyber & Nuclear Security : Implications for Ethics in Cyber Warfare’ , Springer , 2016

[9]. “G. Sree Lakshmi , Olena Rubanenko , G. Divya , V. Lavanya” , ‘Distribution Energy Generation using Renewable Energy Sources’ , IEEE India Council International Subsections Conference ,2020



INNO SPACE
SJIF Scientific Journal Impact Factor

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

**Impact Factor: 8.18**

# International Journal of Advanced Research

## in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

www.ijareeie.com

Scan to save the contact details