CEEAMA™
Consulting Electrical Engineers Association of Maharashtra

CEEAMA LiveWire

E-NEWSLETTER

Published by Consulting Electrical Engineers Association of Maharashtra

Celebrating Engineer's Day on September 15,
as a tribute to a great Indian Engineer
Bharat Ratna Mokshagundam Visvesvaraya.

India's Chandrayaan 3 succesfully lands on the Moon,
making India the third fourth country in the moon race
and first country to land on the lunar South Pole..

Electrical Consultants Newsletter
Volume No. 4 Issue #32
September 2023

CEEAMA Governing Council
Directors

Mr. Veejhay Limaye
Hon. President

Mr. Chidambar Joshi
Hon. Secretary

Mr. Ulhas Vajre
Hon. Treasurer

Directors

Mr. Narendra Duvedi

Mr. Mohan Kelkar

Mr. Anil Bhandari

Mr. Krishna S. Chandavar

Mr. Arvind Gadre

Mr. Ambuj Rastogi

Mr. Subhash L. Bahulekar
Chief Editor - CEEAMA LIVEWIRE

From the Editors Desk,

The change of guards at CEEAMA, the new TRIDEVs – Mr. Veejhay Limaye (Hon. President), Mr. Chidambar Joshi (Hon. Secretary) & Mr. Ulhas Vajre (Hon. Treasurer) had a great kick-start at CEEAMA's GCs conducted at Pune and then online respectively on 6th & 26th August 2023.

While it was a gracious moment expressing our gratitude to all the retiring team, the new zeal of the new team was quite assuring of its ability to set the bench-mark to greater heights. We all wish them great term ahead and look forward to gain immensely from their vast experience and knowledge.

While the new electrifying team has rechristened the E-NEWS as LIVEWIRE, we are also glad to bring "Mann ki Baat" of our President & Secretary to create a greater connect and belongingness with all our members. I am sure you will enjoy this special issue with equal or even better spirit and response.

Wishing you all a very "Lively Wired" safe journey in your life! Read on...

Subhash L. Bahulekar

Chief Editor – CEEAMA

From the President's desk:

Dear Readers,

Thank you for showing your faith in me to work as the President for the next two years. I have taken charge from 1st August 2023 along with a wonderful team comprising of dynamic secretary Mr. Chidambar Joshi & treasurer Mr. Ulhas Vajre, an epitome of knowledge. The precedent set by the previous team led by Mr. Narendra Duvedi has set the bar high. I congratulate them for sailing through tough times and coming out with flying colors.

CEEAMA E-news is now renamed as 'CEEAMA LiveWire'. A "livewire" person is a colloquial expression used to describe someone who is highly energetic, dynamic, enthusiastic, and full of vitality. This term is often used to characterize individuals who have a lively and engaging personality, are quick-witted, and exude a sense of excitement in their interactions and activities. CEEAMA Livewire, the new committee and GC included, hope to achieve that as well as be full of energy. The CEEAMA Livewire proposes to be a spark to help its readers stand out in a crowd. We have not just changed the name, but also added some new features that will help focus on particular topics and generate a buzz. We endeavor to publish the CEEAMA LiveWire issue in first week of every month. As the name implies, we are expecting it to be fully charged with articles and case studies from field experts and members.

We are drawing up an annual calendar for one topic per month. This is aimed at providing in-depth as well as broad knowledge sharing on respective topics. I urge you to participate in the topic of your expertise and enlighten the readers. We are ready to accommodate as many and any number of articles, so as long far as they provide new insights into the subject. The editorial team is all geared up to make this a grand success.

We will also be carrying out technical programs on the above topics, as well as other electrical subjects - either online, or off-line based on the subject. I look forward to your full participation in this. I am certain this will help in enhancing knowledge as well as skills for the electrical fraternity.

Your participation at CEEAMATECH 2023 (Subject:- EV Charging Infrastructure) at Lonavala was heartwarming. We are looking forward to conduct more such programs on different topics on a grander scale.

We will be having our AGM in September and would request all members to be present, so that we can make an emphatic re-connect. I would encourage all to take this opportunity to present new and out-of-the-box ideas so as to make CEEAMA great again.

Veejhay B Limaaye

Hon. President

CEEAMA

From the Secretary's desk:

Dear Readers,

We welcome you to the September '23 issue of CEEAMA LiveWire.

The new GC committee met in the 1st week of August and proposed a number of changes including thematic periodicals, better engagement with the members as well as the industry, reaching out to more and growing community in general. Every month we propose to focus on a particular topic. With the help of CEEAMA members and the past leadership, we hope to make this mission possible. There are opportunities for sponsorship too, which will help ensure that the advertisements stay in the Archives forever. An yearly timetable for various themes is as follows:

Sr. No.	Month	Theme
1	Sep-23	Cyber Security in Power Systems
2	Oct-23	Cables
3	Nov-23	Power Quality and Capacitors
4	Dec-23	Solar Power
5	Jan-24	Lighting
6	Feb-24	UPS
7	Mar-24	Transformers
8	Apr-24	Earthing & Lighting Protection
9	May-24	Electrical Vehicles
10	Jun-24	Motors
11	Jul-24	Building Automation
12	Aug-24	Switchgear

Not withstanding the above, we welcome articles on other diverse issues, like before, so that they too can be published as earlier as possible. We hope the above will help all of us to plan better and keep our experience-sharing ready.

Earlier this month, Govt. of India came out with a GR with new policy condition restricting the import of laptops, tablets, all-in-one PCs, and Servers. This will affect the IT landscape in India in a big way, ushering in tremendous growth of IT equipment manufacture within India – an opportunity for many new budding engineers to set up new electronics manufacturing facilities as well as assembly shops.

On 15th August, the 77th Independence Day was celebrated with great pomp and fervor.

Talking about computers and "Desh Prem", in July we had the latest Mission Impossible movie featuring the secret agent Ethan Hunt grapple with Artificial Intelligence and the threat to all nations. Usually in any Mission Impossible film, Ethan Hunt is tasked with infiltrating a high-tech enemy base that's protected by a labyrinth of electrified fences, voltage-laden traps, and security systems that would make any engineer's head spin. As he faces off against hordes of enemy agents, Ethan's quick thinking and engineering prowess comes to the forefront. For example, when confronted with a locked door, he doesn't waste time searching for keys; instead, he carefully analyzes the electronic lock's wiring, bypasses the security protocols, and gains access in seconds. It's like a high-stakes game of "Guess the Resistor Value" – and Ethan always wins. Such movies do prove that when it comes to espionage, gadgets are cool, but a solid understanding of electrical engineering on the hero's part is truly electrifying!

Taking cue from the above, we focus this month on Cyber Security in Electrical Power Systems. I would request all readers to take a moment out to think about life without the presence of the cyber world. This would be like achieving Nirvana, alas, it will not let us live peacefully in this fully wired world with data, streaming, blogs, in-feeds and emails with their bulky attachments.

Wishing you all a happy Ganesh Chaturthi in advance.

Ganpati Bappa Moraya, Mangal Murti Moraya!!

Chidambar Joshi

Hon. Secretary

CEEAMA

CHANDRAYAAN - 3

The entire CEEAMA community takes this opportunity to congratulate the entire staff along with the Scientists, Engineers and Astro-Physicists at ISRO for their historic achievement of soft landing of Chandrayaan-3 on the South Pole of the Moon. August 23, the day the Chandrayaan-3 lander touched down on the lunar surface, would be celebrated as “National Space Day” from now on.

Chandrayaan-3 is a follow-on mission to Chandrayaan-2 to demonstrate end-to-end capability in safe landing and roving on the lunar surface. It consists of Lander and Rover configuration. It was launched by LVM3 from SDSC SHAR, Sriharikota. The propulsion module carried the lander and rover configuration till 100 km lunar orbit. The propulsion module has Spectro-polarimetry of Habitable Planet Earth (SHAPE) payload to study the spectral and Polari metric measurements of Earth from the lunar orbit.

Chandrayaan-3 consists of an indigenous Lander module (LM), Propulsion module (PM) and a Rover with an objective of developing and demonstrating new technologies required for Inter planetary missions. The Lander will have the capability to soft land at a specified lunar site and deploy the Rover which will carry out in-situ chemical analysis of the lunar surface during the course of its mobility. The Lander and the Rover have scientific payloads to carry out experiments on the lunar surface. The main function of PM is to carry the LM from launch vehicle injection till final lunar 100 km circular polar orbit and separate the LM from PM. Apart from this, the Propulsion Module also has one scientific payload as a value addition which will be operated post separation of Lander Module.

Chandrayaan-3 is the third lunar mission by the Indian Space Research Organisation (ISRO) and it has several potential benefits for the public and the nation:

1. Advancement in Science and Technology: Chandrayaan-3 will help to advance the scientific knowledge and technological capabilities of India, allowing the country to keep pace with other leading space-faring nations. The data collected during the mission will provide new insights into the lunar geology, mineralogy, and helium deposits.

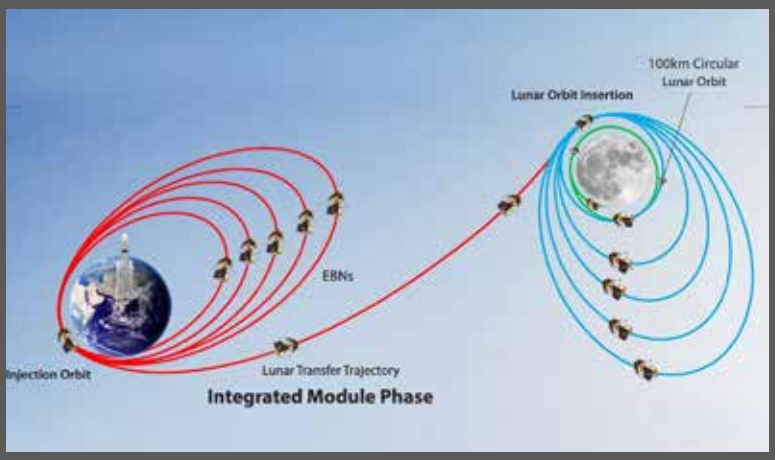
2. Economic Development: The scientific data collected by Chandrayaan-3 will also have economic benefits, such as identifying valuable mineral resources that could be used for commercial purposes. This could help to boost the country’s economy and create jobs.

3. National Defence: The launch and success of Chandrayaan-3 will help to reinforce India’s capabilities in space technology. This can play a significant role in enhancing the country’s national security and defence.

4. Technological Advancements: Chandrayaan-3 will also help to pave the way for future lunar missions by ISRO and contribute towards the development of more advanced technologies and research capabilities.

5. International Recognition: A successful mission by ISRO will bring international recognition and prestige to the country, showcasing its technological advancements and capabilities on the global stage.

Chandra's Surface Thermophysical Experiment (ChaSTE) to measure the thermal conductivity and temperature; Instrument for Lunar Seismic Activity (ILSA) for measuring the seismicity around the landing site; Langmuir Probe (LP) to estimate the plasma density and its variations. A passive Laser Retroreflector Array from NASA is accommodated for lunar laser ranging studies.



It is a convention to name the spot of the touchdown on the moon. And India too has now decided to name the point where Vikram lander touched down. That point will now be known as 'Shiv Shakti Point. The 'Shakti' in the name 'Shiv Shakti' comes from the hard work, inspiration and empowerment of the women scientists.

India has decided to also name the point where Chandrayaan-2's Vikram lander crash-landed. Since we now have "Har Ghar Tiranga" and the Tiranga is even there on the Moon, it is only apt to name the point 'Tiranga Point' - India's first contact with the surface of the Moon.

https://www.isro.gov.in/Chandrayaan3_Details.html

https://www.thehindubusinessline.com/news/chandrayaan-3-touchdown-point-to-be-known-as-shiva-shakti-point-pm-modi/article67237772.ece

https://www.ndtv.com/india-news/chandrayaan-3-landing-site-to-be-called-shiv-shakti-point-says-pm-modi-4330959

Contributed by

Chidambar Joshi

Hon Secretary,

CEEAMA

National Engineers Day - 15th September

On March 4th each year, people all over the globe celebrate World Engineering Day. It is a day that reminds us of all the great things engineers have done to get us to where we are today. That's a lot of things when you think about it. The theme of World Engineering Day for Sustainable Development 2023 was "Engineering innovation for a more resilient world".

In India, we celebrate Engineer's Day on September 15, as a tribute to the greatest Indian Engineer Bharat Ratna Mokshagundam Visvesvaraya.

He did excellent work in the field of engineering (dams, reservoirs and hydro-electric projects) education and administration. In 1899, Visvesvaraya was invited to join the Indian Irrigation Commission where he implemented an intricate system of irrigation in the Deccan Plateau and designed and patented a system of automatic weir water floodgates that were first installed in 1903 at Khadakwasla Dam near Pune. These floodgates were initially installed at the Khadakvasla Reservoir near Pune in 1903. Later with successful implementation, similar floodgates were designed and installed at Tigra Dam and Krishna Raja Sagara Dam. He was one of the chief engineers of the flood protection system for the city of Hyderabad who suggested flood relief measures for the city, which was under constant threat by the Musi river. He achieved celebrity status when he designed a flood protection system for the city. He was instrumental in developing a system to protect Visakhapatnam port from sea erosion. This dam created the biggest reservoir in Asia at the time of its construction.

Visvesvaraya was appointed a Companion of the Order of the Indian Empire (CIE) in 1911 by King Edward VII. In 1915, while he was Dewan of Mysore, Visvesvaraya was knighted as a Knight Commander of the Order of the Indian Empire (KCIE) by King George V for his contributions to the public good. After India attained independence, Visvesvaraya received the Bharat Ratna, India's highest civilian honour, in 1955. In addition to a number of Government postings, he represented the Board of Directors of Tata Steel from 1927–1955. The College of Engineering, Pune, his alma mater, erected a statue in Visvesvaraya's honour.

Happy Engineers Day to all.

References:

- http://timesofindia.indiatimes.com/articleshow/94214101.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- https://en.wikipedia.org/wiki/M._Visvesvaraya

Contributor

Chidambar Joshi

Hon Secretary,

CEEAMA

Cybersecurity Issues Related to Electrical Networks

1. Introduction

Electrical networks are critical infrastructures that power modern societies. Modern electrical networks are augmented with digital auxiliary equipment and infrastructure. With increasing reliance on digital technologies, these networks too are becoming vulnerable to cyber threats. Cybersecurity issues related to electrical networks pose significant risks to their reliability, safety, and operational efficiency.

In an era defined by unprecedented technological advancement and rapid digitization, the role of electrical networks has evolved beyond their conventional purpose. These networks are no longer limited to the transmission and distribution of power; they now serve as the backbone of an interconnected world, facilitating the seamless flow of data, communication, and automation. However, as our reliance on these networks deepens, so does the urgency to fortify their security.

The evolution of electrical networks into intricate cyber-physical systems has ushered in unparalleled efficiency and convenience. Smart grids, intelligent substations, and distributed energy resources have revolutionized the way we generate, distribute, and consume electricity. Yet, with great innovation comes great vulnerability. The possibility of cyber threats looms larger than ever, with potential consequences ranging from minor disruptions to catastrophic outages and even compromised public safety.

The rapid digitization of electrical networks has introduced a myriad of entry points for malicious actors to exploit. From ransomware attacks targeting utilities' operational systems to the manipulation of demand-response mechanisms, the threats are both diverse and daunting. It is important to bolster network resilience through proactive measures such as real-time monitoring, robust encryption, and anomaly detection. (Acknowledgement [h])

This article discusses various cybersecurity challenges faced by electrical networks and highlights the importance of implementing robust security measures.

2. Examples of cyber-attacks on electrical power networks

To drive the point home and to gauge the implications of the cyber-attacks in history, let us look at a few examples:

2.1 Stuxnet (2010): While not directly targeting power networks, Stuxnet is a notorious worm that targeted industrial control systems, including those used in power plants. It was discovered to have been designed to disrupt Iran's nuclear program by targeting centrifuges used for uranium enrichment.

2.2 Dragonfly/Energetic Bear (2011-2014): A cyber espionage group believed to be sponsored by a nation-state targeted energy companies in Europe and the United States. They gained access to critical systems and potentially had the capability to disrupt power distribution.

2.3 BlackEnergy Attacks on Ukraine (2015): The BlackEnergy malware was used in a series of cyber-attacks on Ukrainian energy companies in 2015, which led to significant power outages in some regions. The attacks were coordinated with other malware like KillDisk.

2.4 Ukraine Power Grid Attack (2015 and 2016): In December 2015 and again in December 2016, parts of Ukraine experienced significant power outages due to cyber-attacks. The attackers used malware to compromise the power distribution systems, resulting in widespread blackouts and disruptions.

2.5 CrashOverride / Industroyer (2016): This malware was used in an attack on Ukraine's power grid in 2016. It targeted industrial control systems and could potentially be modified to target other types of critical infrastructure.

2.6 NotPetya (2017): While primarily a ransomware attack, NotPetya also caused disruption to power networks in Ukraine and other countries. It spread quickly through corporate networks, affecting various industries.

2.7 Colonial Pipeline Ransomware Attack (2021): While not targeting power networks directly, this attack on a major U.S. pipeline operator highlighted the vulnerability of critical infrastructure to cyber-attackcyber-attacks. The attack led to a temporary shutdown of the pipeline and fuel shortages in parts of the United States.

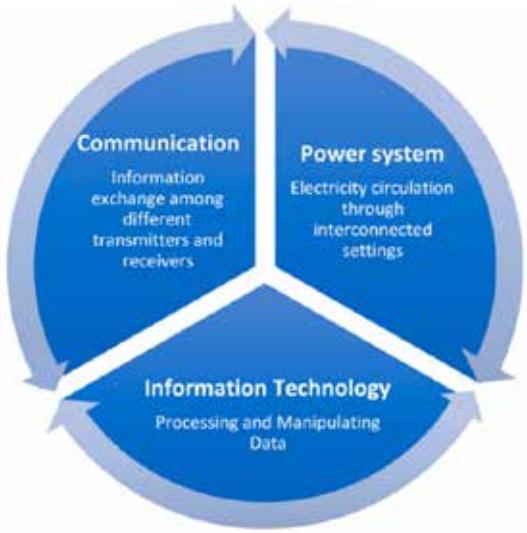
2.8 Iran Nuclear Facility Incident (2021): In April 2021, an incident occurred at Iran's Natanz nuclear facility, reportedly involving a cyber-attackcyber-attack that damaged centrifuges used for uranium enrichment. While the details remain somewhat opaque, it highlighted the potential impact of cyber-attackcyber-attacks on critical infrastructure.

2.9 India Power Outage (2020): In July 2020, large parts of Mumbai and surrounding areas experienced a major power outage, which was attributed to a cyber-attack on the state's electricity infrastructure. (Acknowledgement [i])

3. Setting up cybersecurity in electrical networks

A digitally controlled electrical power system is a modern and sophisticated infrastructure designed to manage and regulate the flow of electricity in various applications. It utilizes digital technology and advanced algorithms to monitor, control, and optimize power generation, distribution, and consumption. Key components of such a system include digital controllers, sensors, communication networks, and intelligent software. These elements work together to ensure efficient and reliable electricity supply while responding dynamically to changes in demand and external conditions.

The advantages of a digitally controlled electrical power system include enhanced reliability, improved energy efficiency, reduced downtime, and better control over power quality. It also facilitates remote monitoring and management, allowing operators to optimize performance and respond promptly to any abnormalities or emergencies. Overall, the shift towards digitally controlled electrical power systems represents a significant advancement in the power industry, paving the way for a more resilient, flexible, and sustainable electrical grid.



The triad of confidentiality, integrity, and availability (CIA) as the fundamental concept of information security has to be interpreted slightly differently in the energy sector. In traditional cybersecurity, it is generally preferable to ensure confidentiality and integrity and possibly sacrifice (some) availability. In power grids, however, availability is by far the most important measure of the triad, as the consequences of downtime can be severe. The longer a blackout lasts and the more of the grid is affected, the harder it is to rebuild the grid.

Through real-time data acquisition and analysis, the digital control system can adjust power generation levels, manage energy storage, and balance the distribution of electricity to meet the needs of consumers and maintain grid stability. Moreover, it enables integration with renewable energy sources, such as solar and wind, promoting cleaner and sustainable power generation. Now a days it is crucial to protect critical infrastructure from cyber threats and potential attacks. Some essential steps taken to enhance cybersecurity in electrical networks are as follows:

3.1 A comprehensive Risk Assessment is conducted for the electrical network. Potential vulnerabilities, critical assets, and possible threats are identified. Understanding the risks is the foundation for developing an effective cybersecurity strategy.

3.2 A clear and well-defined cybersecurity policy that outlines the objectives, roles, responsibilities, and protocols for securing the electrical network is created. It is ensured that all employees and stakeholders are aware of and adhere to this policy.

3.3 Hardware security is achieved by installing firewalls and provision of network segmentation to separate out the critical assets and systems from non-critical ones. This prevents lateral movement of cyber threats and limits the potential breaches.

3.4 Regular software updates and patches are required to keep all software, operating systems, and firmware up to date. Network Monitoring and Intrusion Detection tools help identify suspicious activities and potential cyber threats in real-time, allowing for timely responses. If remote access is necessary, it is ensured that it is done through secure channels like Virtual Private Networks (VPNs) and multi-factor authentication (MFA). Limit the access of privileges to only those who require it.

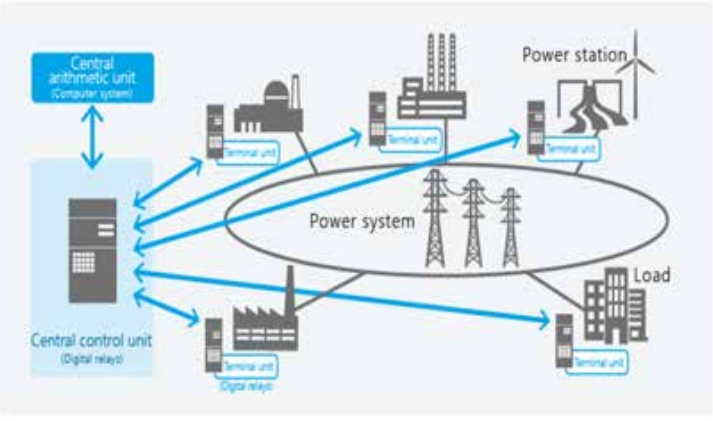
3.5 Employee training and awareness is vital to ensure employees and personnel are aware of cybersecurity best practices, common threats, and social engineering techniques. Employees are often the first line of defence against cyber-attacks. Ensuring that all devices connected to the network have strong passwords and are configured securely helps network maintain its safety. Removing or disabling unnecessary services and ports are required to minimize potential attacks.

3.6 Sensitive data encryption adds an extra layer of protection to data, making it more challenging for unauthorized users to access or manipulate it. Regular audits are conducted including periodic penetration testing and cybersecurity audits to identify weaknesses and potential vulnerabilities in the system. Ethical hacking and plugging the loopholes promptly helps in improving overall security.

3.7 Development of a detailed incident response plan that outlines the steps to be taken in the event of a cyber incident is important. This plan should cover containment, eradication, recovery, and lessons learned. This plan could differ from state to state or industry to industry. Engagement with industry peers, government agencies, and cybersecurity experts to stay updated on the latest threats and best practices is required. Participation in information-sharing initiatives to collectively strengthen cybersecurity in critical infrastructure sectors helps fight the menace together.

4. Challenges faced

4.1 One of the primary concerns in electrical networks is unauthorized access. Hackers or unauthorized individuals gaining access to Supervisory Control and Data Acquisition (SCADA) systems or Industrial Control Systems (ICS) can disrupt power generation, transmission, or distribution processes. By exploiting vulnerabilities, attackers can manipulate critical systems, leading to power outages, equipment damage, or even physical harm.



4.2 Electrical networks are susceptible to malware and ransomware attacks. Malicious software can exploit system vulnerabilities or employ social engineering techniques to compromise the network. Malware can disrupt network operations, compromise data integrity, or encrypt critical files, demanding ransom payments for their release. Such attacks can cause significant disruptions and financial losses like the one in Mumbai in October 2020.

4.3 Electrical networks rely on a complex supply chain involving components and equipment from multiple vendors. Supply chain vulnerabilities can arise from compromised components, counterfeit hardware, or insecure software/firmware embedded in devices. Attackers can exploit these weaknesses to gain unauthorized access or compromise the integrity of the network.

4.4 Inadequate network segmentation within electrical networks can increase the risk of cyberattacks. Interconnected systems without proper segmentation allow attackers to move laterally within the network, compromising multiple systems or gaining unauthorized control over critical infrastructure. Implementing strong network segmentation and access controls is essential to limiting the impact of potential breaches.

4.5 Cyber-attacks on power grids specifically exploit human behaviour either through spear-phishing, most prominently using emails, or manipulated downloads. These problems cannot solely be solved by using more sophisticated security technology. Consequently, employees need to be trained to increase awareness towards security-related behaviour.

4.6 Weak authentication mechanisms and access controls make electrical networks more vulnerable to cyber threats. Weak passwords, default credentials, or the absence of multi-factor authentication can expose critical systems to unauthorized access. Strengthening authentication processes and implementing robust access controls are vital to reducing these risks.

4.7 Failure to apply security updates or patches promptly leaves electrical networks exposed to known exploits and vulnerabilities. Without regular updates, systems remain susceptible to attacks that have already been addressed by the vendor. Effective patch management practices are essential to maintaining the security and integrity of the network.

4.8 Insufficient monitoring and incident response capabilities delay the detection and response to cyber threats in electrical networks. Without proper monitoring, anomalies or malicious activities may go unnoticed, prolonging the potential impact of an attack. Implementing robust security monitoring tools and establishing well-defined incident response procedures are crucial to minimizing the impact of cyber incidents.

4.9 Physical security risks present a significant challenge to the cybersecurity of electrical networks. Unauthorized access to substations, control rooms, or other critical infrastructure can lead to tampering with equipment, manipulation of controls, or the installation of malicious devices. Integrating physical security measures with cybersecurity protocols is essential for comprehensive protection.

4.10 Inadequate cybersecurity awareness and training among employees and personnel increase the vulnerability of electrical networks to social engineering attacks, phishing attempts, or inadvertent security breaches. Regular training programs on cybersecurity best practices, policies, and incident response protocols are essential to enhance the human factor in security.

4.11 Weakest link problem (Acknowledgement [b]) - For attacks to have devastating consequences, an attacker does not have to target the largest grid operator. As long as the victim of an attack has control over enough power to affect the grid frequency, the attacker can leverage cascading effects to affect the whole power grid. As smaller operators often lack the means to harden their systems as much as larger operators, such targets may be more attractive to attackers. Furthermore, attacks do not have to be limited to grid operators: An attacker controlling a larger number of consumer electronics, e.g., solar power cells, might still be able to influence the frequency within the grid. As a result, there is a need to develop solutions which can be used by all relevant actors in interconnected power grids and are not only deployable by larger grid operators.

4.12 Cascading Effects (Acknowledgement [b]) - Instead of having to compromise the network of one or more grid operators, an attacker may leverage cascading effects in the power grid to cause a power outage For example, by remotely gaining control over a large number of consumer electronics, such as solar power cells, an attacker can take advantage of the mechanics of the operating reserve to influence the frequency within the grid. There are also companies that centrally manage many distributed solar or wind plants, e.g., within the scope of a virtual power plant. A compromise at one of these service providers may allow attackers to leverage similar effects. An attack exploiting cascading effects could be global in scale with a medium to high impact (depending on the amount of power under the attackers' control) but has a high technical difficulty, as a comparably large number of devices has to be exploited and controlled simultaneously. However, already today, larger botnets, e.g., Conficker, Hajime, or WannaCry, control hundreds of thousands to millions of devices making such attacks less likely than it appears. The problem might further exaggerate with the rise of electric mobility, as electric cars, as well as their charging infrastructure, will be networked, facing their own cybersecurity risks combined with a high amount of energy consumption under their control.

4.13 Insider threats pose a significant cybersecurity risk to electrical networks. Insiders, including disgruntled employees or contractors with privileged access, may intentionally sabotage systems, steal sensitive information, or cause disruptions from within the organization. Effective access controls, employee monitoring, and periodic security audits are crucial to mitigating this risk.

5. Case Study: Cybersecurity Threat to Electrical Network and Mitigation

In 2016, a major cybersecurity incident occurred, targeting an electrical network in a metropolitan area in the United States. (The name of the distribution company, the personnel involved and the details of network are withheld due to the sensitive nature of the data.) The attack was aimed to disrupt the power supply and create widespread chaos and inconvenience. This case study highlights the nature of the threat and the mitigation measures employed to safeguard the electrical network.

Incident Overview

The attack was initiated through a sophisticated spear-phishing campaign that targeted key personnel within the electricity distribution company. Malicious actors sent convincing emails containing attachments with embedded malware. Once opened, the malware exploited vulnerabilities in the recipients' systems, allowing unauthorized access and control over critical infrastructure. The attackers gained access to the Supervisory Control and Data Acquisition (SCADA) systems, which controlled the operation of substations, circuit breakers, and other network components. They attempted to manipulate the power generation and distribution processes, aiming to cause widespread power outages.

Response and Mitigation

Upon detecting the attack, the electricity distribution company activated its well-prepared incident response plan.

The incident response team, comprising cybersecurity experts, network engineers, and relevant stakeholders, coordinated the response efforts. Their primary objective was to contain the attack, minimize disruptions, and restore normal operations swiftly.

Network Segmentation

To limit the attackers' ability to move laterally within the network, network segmentation was implemented. This involved dividing the network into isolated zones or segments, with controlled access between them. By implementing strict access controls and isolating critical components, the impact of the attack was contained, preventing the compromise of the entire electrical network.

Patch Management and Updates

The distribution company did not have any patch management philosophy. The incident prompted a thorough review of the network's infrastructure and software. Security patches and updates were promptly applied to address known vulnerabilities and strengthen the overall security posture. This included updating SCADA systems, network devices, and associated software to ensure that the latest security patches were in place.

Employee Training and Awareness

Recognizing the importance of human factors in cybersecurity, the distribution company implemented comprehensive employee training and awareness programs. Staff members received training on identifying phishing attempts, handling suspicious emails and attachments, and practicing good cybersecurity hygiene. Regular awareness campaigns were conducted to reinforce best practices and promote a culture of security throughout the organization.

Enhanced Network Monitoring

To improve threat detection capabilities, the distribution company deployed advanced security monitoring tools and techniques. This included implementing Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) systems, and anomaly detection mechanisms. Real-time monitoring of network traffic, system logs, and unusual behaviour patterns allowed for early detection and timely response to potential threats.

Collaboration with Cybersecurity Experts

The distribution company collaborated with external cybersecurity experts and consultants to assess the network's vulnerabilities and identify areas for improvement. These experts conducted thorough security audits, penetration testing, and vulnerability assessments to identify potential weaknesses. Recommendations were made to further enhance security controls and strengthen the resilience of the electrical network.

Results and Outcomes

Through a coordinated response and the implementation of robust mitigation measures, the distribution company successfully thwarted the attack and prevented widespread power outages. The incident highlighted the critical importance of cybersecurity in the energy sector and led to significant improvements in the network's security posture.

Lessons Learnt:

i. Continuous Improvement: Regular security assessments, updates, and employee training are essential for maintaining a strong cybersecurity posture.

ii. Collaboration: Engaging external cybersecurity experts can provide valuable insights and ensure a comprehensive approach to mitigating threats.

iii. Network Segmentation: Implementing network segmentation can limit the lateral movement of attackers and minimize the impact of a potential breach.

iv. Incident Response: Having a well-prepared incident response plan and a trained response team is crucial for minimizing the impact of cyber-attacks.

v. Employee Awareness: Building a culture of cybersecurity awareness among employees is essential for preventing successful phishing and social engineering attacks.

The distribution company realised that Cybersecurity is an ongoing process, and the landscape of cyber threats is constantly evolving. Regular -assessment and updating the cybersecurity measures to stay ahead of potential risks is the need of the hour.

6. Conclusion

Many industries incorporate security considerations throughout the entire product development lifecycle. Security is not an afterthought but an integral part of their design and engineering processes.

Cybersecurity issues in Electrical networks pose significant risks to the reliability and safety of electrical networks. Unauthorized access, malware and ransomware attacks, insider threats, supply chain vulnerabilities, lack of network segmentation, weak authentication and access controls, inadequate patch management, insufficient security monitoring, physical security risks, and lack of cybersecurity awareness are critical concerns.

The case study presented underscores the evolving nature of cyber threats targeting electrical networks. By implementing a robust incident response plan, network segmentation, regular patch management, employee training, enhanced monitoring, and collaboration with cybersecurity experts, the distribution company successfully mitigated the attack and fortified the security of their electrical network. This incident

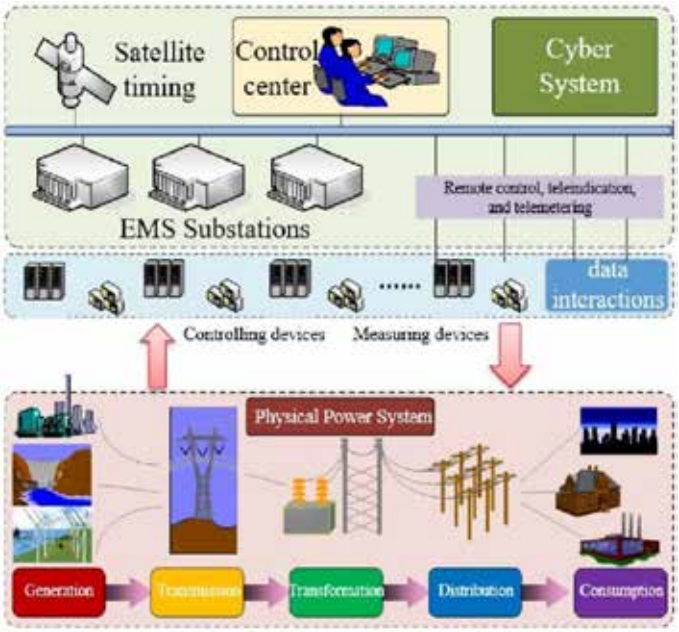
highlights the critical role of proactive cybersecurity measures in safeguarding critical infrastructure and the need for constant vigilance in an increasingly interconnected digital landscape.

By prioritizing cybersecurity, electrical networks can enhance their resilience and protect against ever evolving cyber threats.

7. The Future Landscape

7.1 A futuristic model of Cyber System for electrical power networks is seen in the adjoining figure. With ever growing complex nature of the electrical networks and its reliance on digital systems, the role of Cybersecurity will be ever evolving.

7.2 Traditional security paradigms no longer suffice in an era where perimeter defences are constantly eroding. Zero-Trust Architectures have emerged as a promising solution, requiring stringent identity verification and continuous monitoring regardless of location or user role. We explore the implementation of zero-trust principles within electrical networks, highlighting the role of micro-segmentation, least-privilege access, and multi-factor authentication in fortifying critical infrastructure.



7.3 The convergence of artificial intelligence and electrical network security has given rise to a new era of proactive defence termed as AI-Powered Threat Detection. Machine learning algorithms are now capable of analyzing vast volumes of network data to identify anomalies and potential breaches. We investigate the successful integration of AI-driven threat detection tools, examining their role in thwarting cyberattacks and enhancing incident response times.

7.4 The interconnected nature of modern power systems necessitates Collaborative Defence Strategies - a collective approach to security. Public and private sector collaboration is paramount, with utilities, government agencies, and cybersecurity firms working in unison to share threat intelligence and best practices.

7.5 A chain is only as strong as its weakest link, and in the realm of electrical network security, human factors cannot be overlooked. We delve into the importance of comprehensive cybersecurity training for utility personnel, equipping them with the skills to identify and respond to potential threats effectively. Moreover, we investigate the role of robust insider threat prevention mechanisms in safeguarding critical infrastructure.

As we stand on the precipice of a future dominated by smart cities, renewable energy integration, and IoT-driven automation, the imperative to secure our electrical networks has never been clearer. Through informed insights, expert analysis, and a commitment to collaborative action, we can navigate the evolving threat landscape and ensure a connected world that is both efficient and secure.

8. Government of India initiative

Government of India has set up the Indian Computer Emergency Response Team (CERTIn) for Early Warning and Response to cyber security incidents and to have collaboration at National and International level for information sharing on mitigation of cyber threats. CERT-In regularly issues advisories on safeguarding computer systems and publishes Security Guidelines which are widely circulated for compliances.

All Central Government Ministries/ Departments and State/Union Territory Governments have been advised to conduct cyber security audit of their entire Cyber Infrastructure including websites at regular intervals through CERT-In empanelled Auditors so as to identify gaps and appropriate corrective actions to be taken in cyber security practices.

CERT-In extends supports to enable Responsible Entity in conducting cyber security mock drills and in assessment of their preparation to withstand cyber-attacks. The Responsible Entity must submit Reports of Cyber Audit of cyber security controls, architecture, vulnerability management, network security and periodic cyber security drills to sectoral CERT as well as CERT-In. Teams of experts review these reports and shortcomings, if any, in the compliances, are flagged by them. CERT-In also conducts workshops and training programs on a regular basis to enhance Cyber awareness of all Stakeholders.

9. Acknowledgement

a. Siemens network management

b. Paper - Cybersecurity in Power Grids: Challenges and Opportunities by Tim Krause, Raphel Ernst, et al., 21 September 2021

c. Paper - Microgrid Cyber-Security: Review and Challenges toward Resilience by Bushra Cannan, Bruno Collichio, Djaffer Ould, IRIMAS Lab., France

d. Paper - Analyzing the Impact of Cybersecurity on Monitoring and Control Systems in the Energy Sector by Mohammed Alghassab

e. Google and Wikipedia

f. CEA (Cyber Security in Power Sector) Guidelines, 2021

g. Paper - Cyber Security and Power System Communication — Essential Parts of a Smart Grid Infrastructure - Göran N. Ericsson

h. https://www.electricity-cybersecurity.com/

i. https://www.indiatoday.in/india/story/maharashtra-cyber-cell-mumbai-power-outrage-1774522-2021-03-01

Contributed By

Chidambar V Joshi

ME (Electrical Power Systems), MIE, MIETE, CEng.

Variable Frequency Drives – A holistic overview – Use in India.

Synopsis: My generation is witness to the growth of power electronics, digital electronics, and its effect on electrical engineering for the last 42 years. We have seen clean grids with very limited nonlinear load, and now grids feeding more than 50% nonlinear loads. As a power quality enhancement and energy optimization enthusiast, I come across many Variable Frequency Drive (VFD) installations impacting internal power quality affecting electrical equipment and digital controls. This article is an attempt to take overview of VFD installations done in the industry for a justified cause, and otherwise along with their impact on power quality, reactive power compensation etc. A brief history of technology progress over the last 40 years is also discussed.

History of VFDs

Era of DC drives

During the 1980s, DC motors had good acceptance for generating various torque speed characteristics as required by loads. The popular applications were ranging from precision machine tools, to high power applications in steel and cement industry, to name a few.

An electrical motor rotates due to interaction between two fluxes. DC motor uses field flux and armature flux. It was easily possible to control these fluxes independently with the then available Thyristors or controlled rectifiers. However, DC motor had its own drawbacks of high maintenance due to commutator and brushes. High power DC drives used to have 12 pulse / 24 pulse transformers at input, leaving very little impact on grid side power quality by limiting primary side current harmonics.

Many steel and cement industries used to have sufficient source side derating to accommodate this abuse without affecting upstream power quality. The applications were limited to high end processes, where speed variation was unavoidable. This option did not become popular in low ratings because of high costs and high maintenance requirements.

Advantages and reliability of AC motors

AC squirrel cage induction motor, on the other hand, is maintenance free and offers almost constant speed, the speed being only dependent on frequency (120f/P). All applications which tolerate about 5% speed variation (decided by slip) use squirrel cage induction motors.

Speed variation of induction motor needs frequency variation while maintaining V/f ratio constant (V being the applied voltage). To achieve this, applied voltage also must be varied in proportion with frequency. Commercially available AC power has fixed frequency. So AC to DC and again DC to AC conversion is required. This involves the use of inverters. Thyristors had a drawback that their commutation (switching off) on DC voltage requires forced commutation, which is a complex design and performance deteriorates with aging of passive components like inductors and capacitors. Another power semiconductor available initially was “Darlington pair transistor”. This proved to be fragile for dynamic motor loads and had limitations of Peak Inverse Voltage withstand capacity. Inverters with this technology never became popular.

Entry of new, easy to use Power semiconductors

During 1990s, power MOSFETS were introduced, which initiated high frequency DC - AC power conversion with ease – forced commutation was not required. Subsequent introduction of IGBTs helped in overcoming all reliability barriers. Side by side with microcontrollers and DSPs entering the control of power conversion area, they took reliability to further heights as compared to analog days.

AC Drives and digital controls:

After 2010, “cost effective variable frequency drives” became a reality and the work horse of engineering and process industry. “The Squirrel Cage” induction motor became a true variable speed motor. This gave rise to various variable speed applications which became techno-commercially feasible. Digital controls further gave birth to Vector Control of AC drives. Vector Control is achieved by supplying the motor stator with a current which is the

vector sum of magnetizing component and load torque component. Digitally, it became possible to control both independently. Modern day VFDs when connected to induction motor, run a special algorithm and test the motor under various conditions automatically, collect input parameter readings, use name plate data, and generate a model of the motor equivalent circuit inside the drive memory. This then is used to generate various torque speed characteristics, as required by the load, including staring current requirements / breaking requirements etc. Complex applications like using cranes to shift heavy material in factories with very little sway, positioning oil rigs in sea by holding the anchors etc are now possible using high end VFDs. VFDs have started powering electric vehicles in bulk and are capable of operating in motoring and regenerating modes.

Modern day VFDs also offer on board PLC with digital / analog inputs, programming and communication facility using standard protocols. With This, the installation can be easily converted into an IOT node.

Use of VFDs and Power Quality issues.

Traditional VFDs (very commonly used in India even today in industries) use a 6-pulse thyristor rectifier to convert AC to DC and then use IGBTs to convert this DC to AC. As a result of unhealthy market competition, such VFDS with 800 / 900kW capacity are also supplied with 6-pulse rectifiers and work on 433V supply. Specifications and commercials of such machines are usually finalized by the senior management and the process owners, who are rarely electrical engineers and informed about power quality issues. The transformers feeding such drives are usually “Distribution Transformers” and very rarely selected with “K Factor derating” to support harmonic currents. This is where the issue of power quality deterioration begins.

Now let us look at application classes and salient facts about VFDs.

1. In class 1 we see that motor is ordered with VFD, and VFD is used as most reliable starter with protections. In such applications, there is no need for speed variation.

2. In class 2 of VFD installations, VFDs are installed, but are not in closed loop control and motor speed is varied once in six months or a year.

3. In class 3, VFDs are used in closed loop, and the speed is varied to control some output parameter like flow / pressure / position etc.

4. In class 4 VFDs / Servo drives are used in machine tool applications, where 99% VFDs work in closed loop.

There is a myth prevailing in the field which says **“VFDs save energy”. The fact is speed reduction in case of centrifugal machines saves energy.** Energy consumption reduces in cube proportion of speed reduction in such cases. The classes 1,2,3 above hardly save any energy and in fact contribute most in creating power quality problems. We see that even 2HP/3HP motors also are fed through VFDs unnecessarily in this category.

Avoiding / limiting misuse of VFDs.

Demand quantification in real time needs to be done during plant design to know quantity of various utilities like compressed air, water, chilled water etc. This results in correct recommendation of equipment size and then VFDs can be used with utmost advantage to accommodate daily load and seasonal load variations while the equipment delivering required output at best efficiency. This is done very seriously in developed world, whereas the same is done very loosely in India. Pumps and compressors are added without calculation to cover even wastage.

It may be noted here that an energy efficient pump and motor, if coupled together, may not form an energy efficient pumping system overall, if the pump operating point does not fall in best efficiency zone of its characteristics. If required duty from pump is same throughout the day and year, a proper selection can give the most efficient system without the requirement of a VFD. In such case, if variable flow or pressure is required from pump as part of process requirement, then a VFD may be required. This can shift the best efficiency zone across various flow requirements by adjusting motor speed rather than throttling the line for flow reduction. The best performance in this situation will be possible by using a true closed loop control.

Power quality issue and mitigation techniques related to VFDs.

1. Excessive draw of harmonic currents from transformers / grid can result in:Voltage distortion at source
   a) Associated EMI/RFI can disturb the working of other sensitive loads.
   b) Due to voltage distortion, linear loads also start taking nonlinear currents.
   c) Overheating, nuisance tripping
   d) Mechanical misalignments of rotating machines, excess vibrations.
   e) Violation of statutory requirements at the point of common coupling for harmonics.

2. A 6-pulse rectifier input current predominantly contains 5th and 7th harmonic current, the total distortion being around 46%. These are the characteristic current harmonics of this type of rectifier. Each harmonic current will have its respective phase with harmonic voltage and angle will depend upon the respective system impedance at that frequency.

3. If 10 such VFDs get connected to a single bus, the resultant current will be the vector sum of all these currents. If there are any other linear loads working on the same bus, their current gets added vectorially to decide resultant current.

4. Usually, it is found that due to **phase cancellation effect** at the upstream bus, the resultant current will have reduced content of harmonic currents. The phase of this current with respect to voltage will decide the power factor. If the loads are dynamic in nature, the power factor and harmonic contents both vary with respect to time. It is difficult to suggest cost optimized power factor improvement and harmonic mitigation solutions unless this pattern with respect to time is known.

5. Use of only capacitors, use of wrongly tuned filters can cause resonance between them and the system impedance, which results in amplifying current distortion in transformer circuit. If source capacity is insufficient, this will give rise to voltage distortion. As explained earlier, these harmonic currents unnecessarily increase if VFDs are used without justifying their advantages.

6. Tuned passive filters are not recommended, as they may introduce short-circuit if harmonic voltages of tuned frequency are present in the system. Detuned filters tuned to a frequency close to (but not equal to) a current harmonic frequency present in current, help in shunting some harmonic current and keep it circulating between load circuits. The filtering capacity of such filters is effective if the bus power factor is between 0.8 to 0.85. These filters are designed to give capacitive correction at fundamental frequency, and can connect more blocks (if power factor is low) to filter harmonics and simultaneously correct power factor.

7. Active harmonic filters are electronic systems – they analyze real time harmonic spectrum and draw antiphase harmonic currents from source so that resultant harmonic currents drawn from source get nullified to the extent the filter is programmed. Such filters have facility for onsite programming to mitigate selective harmonics. They also can correct lagging or leading power factor through a dedicated small portion of the total capacity. The internal losses of these filters are relatively high as compared to passive filters. Further, high maintenance costs and threat of “technology obsolescence” also is present.

8. Some vendors combine 6 plus 7 and offer hybrid solution to get the best of both techniques along with optimized cost.

9. Purchasing harmonic compensated drives. “Active Front End Rectifier” technology is being extensively used in VFDs, UPS systems, other rectifier applications to keep the harmonic current draw within specified limits. Make “equipment acceptance standards” at national level, and force manufacturers and users to strictly follow them.

Summary:

1. Use of VFDs with induction motors is a boon to the industry. Adjustable torque speed characteristics are available with robust and reliable equipment to suit almost every load profile.
2. All passive techniques like demand quantification, understanding real time load profile etc should be used to justify the use of VFD and selection of a particular model.
3. If VFD ratings, models and power system details are known, system simulation tools like ETAP can be used

for a detailed harmonic analysis at various buses and the effect of proposed solutions. These software tools also facilitate design of filters.

4. It is high time India should frame product standards with detail specifications of input parameter compliances. The products should include (not limited to) SMPS, VFDs, UPS systems, EV chargers, Process rectifiers etc.
5. The compliance limits should stipulate how much harmonic currents an equipment can draw from source – may be above a particular wattage (such limit is 400W in developed countries).
6. Thus, VFD is a good TOOL. If used wisely, it can save a lot of energy, and impart a lot of process flexibility.

Contributed by:

Narendra Duvedi

Immediate past President CEEAMA

WINNERS OF QUIZ
JULY 2023

SAGAR JAGADALE
LFM - 202
M/S CHIYODA CORPORATION, JAPAN

SUBRAMANYAN
LFM-096
M/S S. G. ENGINEERS PVT. LTD.

UDAY D SATHE
LFM - 211
M/S UDAY D SATHE

RUPESH JOSHI
P-025
M/S SWATI ENTERPRISES

ULHAS VAJRE
LFM-117
M/S SUMIT ENGINEERING SERVICES

Congratulations

WINNERS OF QUIZ
JULY 2023

VEEJHAY LIMAYE
LFM-037
M/S V. L. ENGINEERS

SANDIP KHANDGE
BITWISE WORLD

SAMIT THORAT
M/S - TATA MOTORS LIMITED

INFINITY ENGINEERING COMPANY
AM-148

Congratulations

QUIZ SEPTEMBER 2023

1. Which of the following power system is possible to be presented on a Single line diagram?
    a) Power system with LG fault
    b) Balanced power system
    c) Power system with LL fault
    d) Power system with LLG fault

2. A V-V connected transformer can be connected in parallel to delta-delta connected transformer but not to _____
    a) delta-star
    b) star-delta
    c) star-V
    d) all of the mentioned

3. The magnitude of electromagnetic or interaction torque, in all rotating machines, is given by _____
    a) Te ∝ (stator field strength)sinδ
    b) Te ∝ (rotor field strength)sinδ
    c) Te ∝ (stator field strength)(rotor field strength)sinδ
    d) Te ∝ sinδ

4. A control system working under unknown random actions is called _____
    a) Adaptive control system
    b) Stochastic control system
    c) Computer control system
    d) Digital data system

5. Standing waves along the transmission line occurs due to
    a) Impedance match
    b) Impedance mismatch
    c) Reflection
    d) Transmission

6. For a single phase, 50 Hz transformer, if the open circuit test is conducted at 40 Hz, what is the variation in the no-load power factor of the transformer?
    a) Decreases
    b) Increases
    c) Remains constant
    d) None of the mentioned

7. A 220pF capacitor and a 330pF capacitor are each connected across a 6VDC source. The voltage across the 220pF capacitor is
    a) 3V
    b) 6V
    c) 4V
    d) 0V

8. The voltages of the two healthy phases will _____ if the 3-ph system is not grounded and if the single line to ground fault occurs.
    a) Increase
    b) Decrease
    c) Unchange
    d) None of the above

9. Temporary magnets are used in which of the following?
    a) Hoist.
    b) Generators.
    c) Motors.
    d) All of these.

10. Candela is the unit of _____?
    a) Wavelength.
    b) Luminous intensity.
    c) Luminous flux.
    d) Frequency.

Rules for the QUIZ:

- The Quiz will be open for 10 days from the date of EMAIL.
- Each correct answer received on DAY 1 will get 100 points
- Next days the points will reduce as 90 – 80 – 70 and on 10th day points will be ZERO even if the
- answer is correct.
- All participants will receive E certificate signed by CEEAMA President with the points earned
- mentioned on the same.

Please use following google form link to participate in the QUIZ.

https://forms.gle/WYihV6tVfgd2hT1X7

"Thank you all for the overwhelming response to the E-NEWS in general and E-Quiz in particular. MCQ based quiz is always tricky and surprisingly can take us aback when we realise our conceptions (misconceptions) about the subject / system / product.

The aim of the feature was to create inquisitiveness in your mind and help you check your technical quotient

quickly. The response will also help us to present articles and webinars on subjects which are important, but which

lack enough awareness / knowledge in general.

It can open a pandora box for our discussions and arguments and probable solutions. Engineering evolves with conception. It gets fuelled with community discussions and capitalist actions. All stakeholders start realising the need to take a closer look and help improve standards as we have seen in the past century. Surely it makes the world a better place.

Wish you all a better luck this time.

Do spread the word.

July 2023 Quiz Answers

1.	D – Any of these	6.	D - All of the above
2.	A – Zero	7.	B - 65.18
3.	B – Maximum	8.	D - Both A & C
4.	A - Energy reduction programs	9.	A - Detects leakage
5.	A - Act as Motor starter	10.	D - All of the above

NEW REGISTERED MEMBERS IN 2023

Welcome

MR. UMESH SHASHIKANT PHATAK

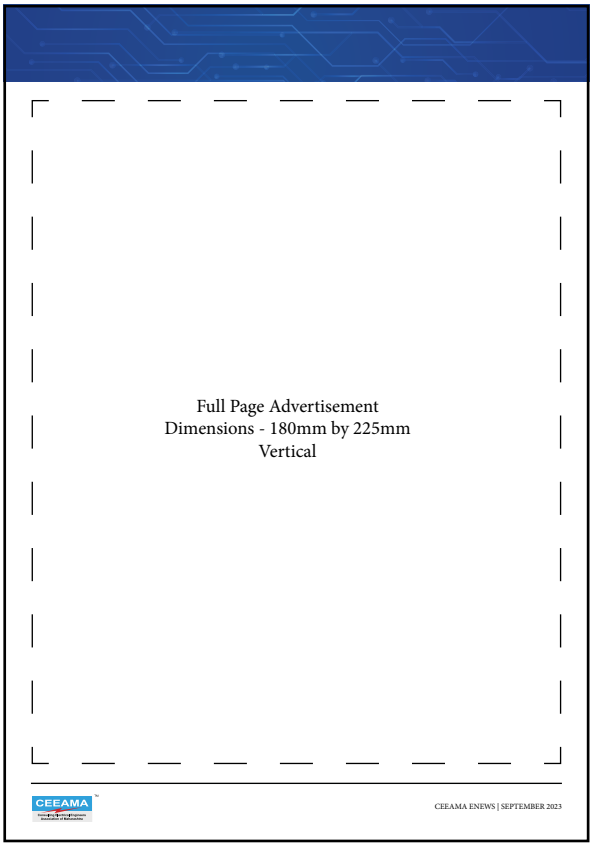
MR. SHRIKANT SATHE
SATHE ASSOCIATES

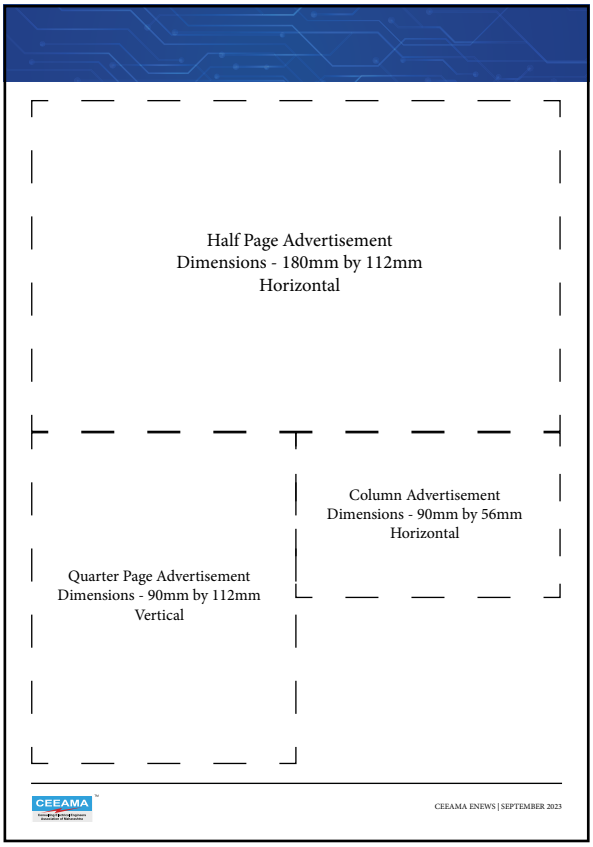
M/S FORTUNEARRT LED LIGHTING PRIVATE LIMITED
MR. NAVEEN KUMAR GOLLEN

M/S RISHABH TECHNOLOGIES PRIVATE LIMITED
MR. VIKAS SRIMAL
MR. NAVEEN GOLLEN

M/S COSPOWER ENGINEERING LTD.
DIRECTOR - PATHIK SHAH
REPRESENTATIVES - SURYAKANT PATIL

ADVERTISEMENT RATES





Above given layouts are only for understanding the advertisement sizes. Actual positions of ads may vary as per space available in the issues.
Below given rates are for advertisement size and number of issues published monthly.

E-Newsletter Ad	3 months	6 months	9 months	12 months
Full Page Ad	INR 1000/-	INR 2000/-	INR 2700/-	INR 3300/-
Half Page Ad	INR 800/-	INR 1600/-	INR 2200/-	INR 2800/-
Quarter Page Ad	INR 600/-	INR 1200/-	INR 1600/-	INR 2100/-
Column Ad	INR 400/-	INR 800/-	INR 1000/-	INR 1400/-
Website Ad	INR 1000/-	INR 2000/-	INR 2700/-	INR 3300/-

GST @18% will be additional on all the above rates.

Please send the E-Newsletter Advertisement in PDF or JPG format ONLY.
Please send the Website Advertisement in JPG or PNG format ONLY.

CEEAMA™

Consulting Electrical Engineers Association of Maharashtra

CEEAMA *LiveWire*

E-NEWSLETTER

Published by Consulting Electrical Engineers Association of Maharashtra

Electrical Consultants Newsletter
Volume No. 4 Issue #32
September 2023

A-103. Sanpada Railway Station Building, 1st floorSanpada East, Navi Mumbai – 400705
Email: admin@ceeama.org