ARIHANT

Arihant स्पर्श Newsletter

A Touch of Excellence, Every Month

M A Y 2 0 2 5

TABLE OF CONTENTS

DIRECTOR'S MESSAGE

Power of Team Work

"Teamwork makes the dream work." It's a phrase we've all heard, but what does it really mean in practice? And how can we nurture a culture where teamwork and collaboration thrive?

A strong culture of teamwork empowers individuals by recognizing and valuing their unique strengths. It creates an environment where everyone feels heard where people are encouraged to ask questions, raise concerns and share ideas. Supporting individuals for who they are and helping them become the best version of themselves is at the heart of true collaboration.

When teamwork becomes the foundation of a company's culture, it leads not only to greater cohesion and efficiency but also sparks innovation. It invites a diversity of thought, encourages a proactive attitude, and fosters creativity. This collaborative spirit strengthens problem-solving and leads to faster, more effective decision-making.

Teamwork must be woven into the very fabric of an organization—reflected in our people, our processes, and our everyday actions. It's not just about saying the right things; it's about living them. We must walk the walk and talk the talk.

To build this culture, trust is essential. Clear communication and collaboration must exist not only within teams but also across all levels of the organization—from colleagues to managers to leaders. There must be a shared sense of purpose and unity in both thought and action.

"I can do things you cannot, you can do things I cannot; together we can do great things."

Best Regards
Hemang Jain
Director, Arihant Electricals

SPOTLIGHT OF THE MONTH

Featured Articles

Dive into this month's insightful articles, covering industry trends, innovations, and expert perspectives. Stay informed, stay inspired, and explore ideas that drive excellence at Arihant Electricals.

1 Strategic Roadmap for Growth in 2025-26

ARUN SHARMA
(VP)

As we step into the new financial year 2025-26, we find ourselves at a pivotal juncture for our organization and our nation. This year presents unique challenges and opportunities, driven by rapidly advancing technologies, stiff competition, and the shared vision of transforming India into a "Viksit Bharat" (Developed India) by 2047, the centenary of our independence. Aligning our organizational goals with national progress is not just a responsibility but a privilege. This is the time to delve into a comprehensive roadmap on goals, strategy, planning, and execution to propel our organization forward while contributing to India's growth story.

The foundation of our success lies in defining clear, measurable, and time-bound goals. These should reflect the organization's vision while staying attuned to market dynamics and technological innovations. Goals should prioritize enhancing efficiency, fostering innovation, and maximizing customer satisfaction. It is imperative that the national initiatives like "Digital India" "Make in India" and "Skill India" are put into practical use within the organization, within the departments and teams.

The financial year 2025-26 marks an era of unprecedented technological innovation. Artificial Intelligence, Blockchain, Internet of Things (IoT), and 5G connectivity are reshaping industries. To stay competitive, adopting cutting-edge technologies to enhance operational efficiency and customer experience is indispensable. We should upskill our workforce to ensure proficiency in emerging tech trends, leverage data analytics for informed decision-making and personalized solutions.

Innovation is the lifeblood of progress. So, we have to encourage a culture where every employee feels empowered to propose new ideas and solutions. As India aspires to become a global technology hub, our investments in R&D is a powerful catalyst to contribute our part in nation development.

In an unpredictable economic landscape, resilience is key. This can only be done through radically innovative strategies, diversifying revenue streams, and maintaining financial prudence to weather any uncertainties about cash flows and funding. For planning and seamless execution, each one of us should generate a comprehensive action plan with detailed timelines, resource allocation, accountability structures and spirit to coordinate with other departments. Instilling mechanisms for progress tracking, Monitoring and Evaluation of KPIs are the vehicles to stay on track.

The financial year 2025-26 will be marked by intense competition across industries. To stay ahead, strategies must factor in comprehensive market analysis to anticipate trends and customer needs. Customer relationship management (CRM) systems will deepen customer engagement and loyalty.

Let us embark on this journey with determination, innovation, and collaboration. Together, we can turn aspirations into achievements and challenges into milestones of success.

2 The Internet of Things, Current Emerging Trend

PRASHANT AWASTHI
(Sales & Mkt.)

The Internet of Things (IoT) describes the network of physical objects "things" that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools.

Ranging from smart home gadgets to personal health devices to industrial machinery equipped with sensors, Internet of Things technology is transforming how people and businesses carry out their daily activities. As the IoT expands and is enhanced with technologies like AI, it offers companies innovative ways to study and serve their customers and provides consumers with more robust, personalized services and new ways to interact with the world around them.

IoT Trend to look out in Current Scenario

Today, most major enterprises have already integrated IoT into their core systems and initiatives to drive digital businesses. From smart city to smart mobility, IoT exist at every inch. The IoT marketplaces are like gateways that offer companies the option to connect and interact with a wide range of vendors, without having to create or change existing platforms.

As we rely on connected devices to make our lives better, security would play a major role. IoT security requires a multi-layered approach where all participants in the IoT ecosystem are responsible for the security of the devices, data and solutions.

IoT is a promising technology which tends to revolutionize and connect the global world via heterogeneous smart devices through seamless connectivity. It will also force mobile providers to move faster than ever.

Another sector to look out for is automotive. The connected automotive sector is a growing sector in India and expected to grow exponentially in the coming years. Usage of IoT within truck, car rental and other companies would see exponential usage of IOT.

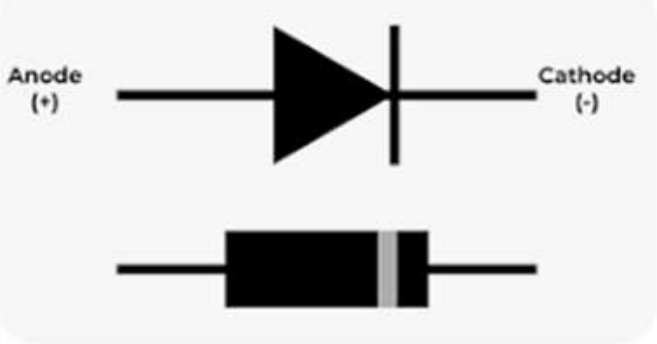
Smart utility-key sector to focus on, energy today is much more than a mere natural resource, increasing population & pollution led to uncontrolled energy consumption. Smart grid is a solution that allows generators, suppliers and consumers to be integrated by intelligent control, monitoring and communication of energy consumption.

Examples of IOT in Every Day Life

- Smart Wearables
- Smart Toll Collection
- Smart Home –Smoke Detector, Smart Lights
- Smart Meters
- Voice assistance devices-Amazon Echo

3 Brief of Diode

ROHIT JHA
(Sales- Lighting Division)



A diode is a semiconductor device that allows current to flow in one direction only. It acts as a one-way switch for electrical current, making it a fundamental component in electronics.

Structure and Symbol

A diode typically consists of a p-n junction, where the "p" side contains an excess of holes (positive charge carriers), and the "n" side contains an excess of electrons (negative charge carriers). The symbol of a diode resembles an arrow pointing in the direction of conventional current flow, with a line representing the cathode.

Working Principle

When a diode is forward-biased (positive voltage to the anode and negative to the cathode), it conducts electricity. In reverse bias, it blocks current, except for a very small leakage current. If the reverse voltage exceeds a certain limit (breakdown voltage), it may conduct suddenly, depending on the diode type.

Types of Diodes

1. Standard (PN) Diode – Basic one-way current control.
2. Zener Diode – Designed to conduct in reverse once a specific voltage is reached; used in voltage regulation.
3. Light Emitting Diode (LED) – Emits light when current flows through it.
4. Schottky Diode – Offers fast switching and low forward voltage drop.
5. Photodiode – Converts light into current; used in sensors.
6. Varactor Diode – Used in tuning circuits, changes capacitance with voltage.

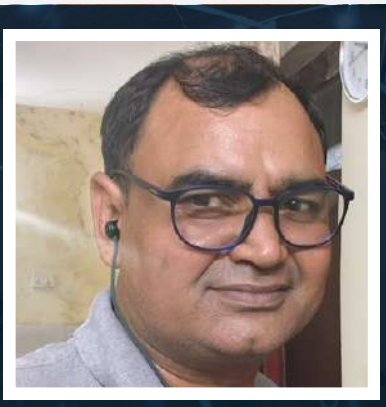
Applications

- Rectification in power supplies (converting AC to DC)
- Voltage regulation
- Signal demodulation
- Circuit protection (surge protectors)
- Light emission in LEDs
- Clipping and clamping in signal processing

Conclusion

Diodes are simple yet crucial devices in modern electronics. Their ability to control the direction of current makes them invaluable in a wide range of applications, from power supplies to communication systems and consumer electronics.

4 Cybersecurity in Industrial Environments



RAVINDAR SINGH
(IT)

Cybersecurity in industrial environments, often referred to as Industrial Control Systems (ICS) security, is the protection of critical infrastructure and operational technology (OT) used in industries such as manufacturing, energy, transportation, and utilities. Unlike traditional IT systems, ICS systems manage and control physical processes and machinery, making them vulnerable to cyberattacks that could have significant safety, economic, and operational impacts.

Key Aspects of Cybersecurity in Industrial Environments

1. ICS and OT Security:
Industrial systems often rely on SCADA (Supervisory Control and Data Acquisition) systems, PLC (Programmable Logic Controllers), and DCS (Distributed Control Systems) to monitor and control physical equipment. These systems were originally designed with little regard for cybersecurity and often use proprietary protocols that may not be secure by modern standards.

2. Risk and Threat Landscape:
Industrial environments face specific threats, including:

- Cyberattacks: Hacking groups, ransomware, and advanced persistent threats (APTs) targeting OT.
- Insider Threats: Employees or contractors with access to critical systems could intentionally or unintentionally compromise security.
- Physical Attacks: Cyberattacks could be used to damage physical assets or disrupt production.

3. Safety vs. Security:
A significant challenge is balancing cybersecurity with safety. Industrial systems often have high safety standards to prevent physical harm to employees, equipment, or the environment. Cybersecurity efforts must ensure that safety protocols are not compromised while defending against cyber threats.

4. Legacy Systems:
Many industrial environments still use outdated or legacy systems that were not designed with cybersecurity in mind. These systems may not receive regular software patches, and replacing them is often expensive and time-consuming. Attackers often exploit vulnerabilities in these legacy systems.

5. Network Segmentation:
A critical cybersecurity measure is network segmentation, which divides the network into separate zones with different levels of trust. This helps limit the spread of an attack from IT systems to OT systems. ICS networks should be isolated from corporate IT networks as much as possible.

6. Access Control and Authentication:
Securing access to industrial systems is essential. Strong authentication measures, including multi-factor authentication (MFA), should be used. Access controls should ensure that only authorized personnel can interact with critical systems.

7. Monitoring and Detection:
Continuous monitoring of both IT and OT environments is crucial. This includes network traffic analysis, anomaly detection, and intrusion detection systems (IDS) designed to identify unusual behaviours that could indicate a cyberattack.

8. Incident Response and Recovery:
Organizations need a robust incident response plan that covers how to quickly and effectively respond to cyberattacks. This plan should include both IT and OT teams, and there should be contingency plans for restoring operations after a security breach.

9. Supply Chain Security:
The security of third-party vendors and contractors is also crucial, as many industrial systems rely on external providers for software, hardware, and services. Compromised third-party software or hardware can serve as a vector for attack.

10. Regulatory Compliance and Standards:
Different industries and countries have regulatory standards for ICS cybersecurity. Some common frameworks include:

- NIST (National Institute of Standards and Technology) Cybersecurity Framework.
- IEC 62443: International standard for securing industrial automation and control systems.
- NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection): Specifically for the energy sector.
- ISO/IEC 27001: Information security management systems standard, applicable to both IT and OT.

Challenges in ICS Cybersecurity

- Lack of Awareness: Many industrial operators may not fully understand the cybersecurity risks involved with their systems and may prioritize operational efficiency over security.
- Integration with IT: As industries become more digitalized, the integration of IT and OT creates new attack surfaces and challenges in securing systems.
- Downtime Concerns: Cybersecurity measures, such as system updates or patching, can disrupt production. The cost of downtime in industrial environments is often high, making it harder to implement security measures.
- Legacy Equipment: Updating or replacing legacy equipment with modern, secure systems is a significant financial burden and may disrupt operations.

Best Practices for Enhancing ICS Cybersecurity

1. Risk Assessment: Regularly assess the risk to ICS and OT systems, identifying potential vulnerabilities and threats.
2. Patching and Updates: Ensure that all systems (where possible) receive timely security patches and updates.
3. Security Audits: Regularly audit systems for vulnerabilities and implement remediation actions.
4. Training and Awareness: Provide cybersecurity training to employees, especially those with direct access to ICS.
5. Data Encryption: Encrypt sensitive data, both at rest and in transit, to protect it from unauthorized access.
6. Backup Systems: Ensure robust backup and recovery processes to maintain continuity in case of a cyberattack.

Emerging Trends in ICS Cybersecurity

- Artificial Intelligence (AI): AI and machine learning are increasingly being used for anomaly detection and identifying potential security threats in real time.
- Zero Trust Security Models: The adoption of zero-trust architectures, where every device and user is treated as untrusted by default, is becoming more common in OT environments.
- Collaboration Across Sectors: Governments, private sectors, and industrial organizations are increasingly collaborating to enhance cybersecurity across critical infrastructure industries.

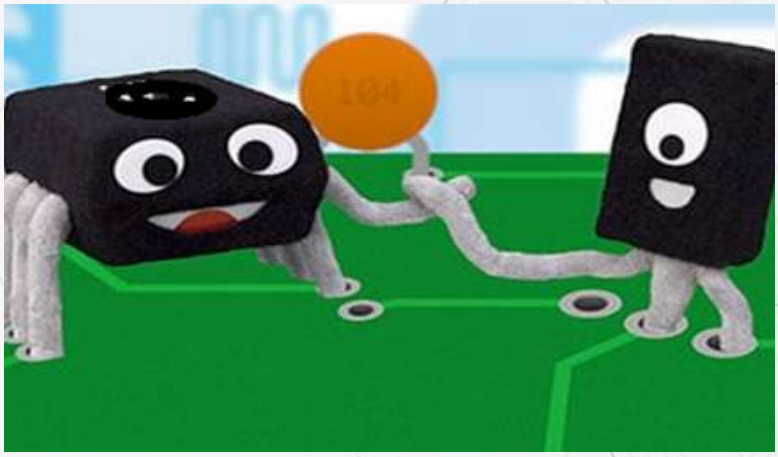
Cybersecurity in industrial environments is a growing concern, as cyberattacks on OT systems can lead to severe consequences, including production downtime, environmental damage, and even harm to human life. Therefore, ensuring the safety and security of these environments is a continuous process that requires careful planning, investment in technology, and a proactive security posture.

5 Dr. Mos

SHIVAM SRIVASTAVA
(Technical Marketing)

Dr. Mos sounds like a Mosfet that went and got itself a PhD! Is it for real, though? Well, it's actually short for Driver Mosfet, an energy-efficient tech Intel cooked up in 2004. It combines a Mosfet and a Mosfet driver IC into one neat little package, making things smaller and more efficient—talk about brainy tech!

Compared to separate Mosfets, an integrated Mosfet will shrink the PCB size by a factor of four and boost power density threefold. Dr. Mos can supply greater current at the same voltage when paired with multiphase controllers, allowing for more efficient switching performance. This makes it ideal for low-voltage, high-power applications. Initially, it was used in server motherboards with two Mosfets and one driver. Now, it has also been developed for wireless charging. For wireless charging, it uses four Mosfets —two on the high side and two on the low side. The high side connects to the power source, and the low side connects to ground, forming a complete full-bridge topology.



Some examples of Dr. Mos ICs and respective manufactures with part numbers

S. No.	Company Name	Part No.
1	South chip	SC5001
2	South chip	SC5003
3	South chip	SC5008
4	I smartWare	SW5006
5	Chipown	PN7727
6	NuVolta	NU1020
7	Wpinno	WP8012

HIGHLIGHTS FROM EVENTS AND CONFERENCES

1. Startup Mahakumbh 2025 at Bharat Mandapam

Arihant Electricals was proud to be part of the world's largest Startup Conference and Exhibition Startup Mahakumbh 2025. This landmark event brought together thousands of startups, corporates, and government bodies, creating a dynamic space for collaboration and growth.

For Arihant, it was more than just participation — it was an opportunity to showcase our capabilities, explore strategic B2B partnerships, and contribute to India's thriving entrepreneurial ecosystem.

From groundbreaking innovations to meaningful exchanges, Startup Mahakumbh 2025 reinforced our commitment to driving progress and shaping the future of electrical engineering and turnkey solutions.

2. Strengthening India's Defence Backbone: Arihant Electricals at PHDCCI Industry Interactive Session

Arihant Electricals participated in the Industry Interactive Session on Revenue Requirements of the Indian Army, held on 21 April 2025 at PHD House, New Delhi, and hosted by PHDCCI.

This high-level session served as a crucial platform for dialogue between the defence industry and the Indian Army, with discussions focused on:

- Industry perspectives on revenue procurement
- Insights into ongoing and upcoming procurement plans of the Indian Army
- Procurement procedures and strategic focus areas
- Direct interaction with senior Army officials and key decision-makers
- Opportunities for collaboration and partnerships
- The Army's expectations from Indian industry players

The event featured distinguished speakers from the MGS Branch and leading voices from the defence manufacturing ecosystem, offering invaluable insights into the evolving needs and opportunities within India's defence sector.

3. Empowering Innovation & IP Excellence: Arihant Electricals at the Global IP Summit 2025

Arihant Electricals was proud to be part of the 15th Global Innovation & Intellectual Property Summit, held on 29 April 2025 at Hotel The Lalit, New Delhi.

Organized by CII and the Office of the Principal Scientific Adviser to the Government of India, the summit featured thought-provoking discussions on emerging technologies, IP commercialization, and building future-ready innovation ecosystems.

A key highlight was the launch of the Innovation Excellence Evaluation Report for public-funded R&D organizations — a landmark initiative shaping India's innovation roadmap.

PEOPLE & CULTURE

ARIHANT

At Arihant Electricals, our people are our greatest strength. This month, we celebrated birthdays, welcomed new team members, and fostered a positive workplace culture. Through these moments, we continue to build a collaborative and engaging work environment where everyone thrives!

April Birthday Celebrations

Celebrating our incredible team members and wishing them joy, success, and prosperity!

Birthday celebration of Priya

Upcoming May Birthdays

Wishing you joy, success, and a fantastic year ahead!

Shankaraiah Gajam (Sales)	May 8
Devendra Singh Mehta (Mkt.)	May 10
Devinder Kumar	May 10
Sandeep Kumar Verma (Manuf.)	May 16
Vineet Kumar (R&D)	May 18

PEOPLE & CULTURE

ARIHANT

Welcome Aboard! (New Joinees - April 2025)

Excited to have new talents join the Arihant family as we grow together!

Rajdeep	April 7, 2025	Sr. Manager Biz. Dev.
Niti Sharma	April 14, 2025	Trainee (CSR)
Himanshu	April 21, 2025	Executive Purchase
Praween Kumar	April 7, 2025	GET
Anuj Kumar Gautam	April 23, 2025	Technician
Vivek Kumar	April 28, 2025	Engineer (Motor Winding)

MOMENTS OF LAUGHTER & FUN

ARIHANT

LIGHTENING THE LOAD:
INDUSTRY HUMOR AT ARIHANT

At an industrial expo, a CEO walks up to an electrical engineer at Arihant Electricals and asks,
"So, what makes your solutions different?"

The engineer smiles and says,
"Well, we don't just conduct electricity...
we conduct results!"

The CEO laughs, "Impressive! But can you handle high pressure?"

Engineer replies,
"We work with transformers daily.
Pressure is just another voltage level to us!"

The CEO nods, "Shocking... but in a good way!"

And just like our circuits – the conversation stayed current!

CONTACT US

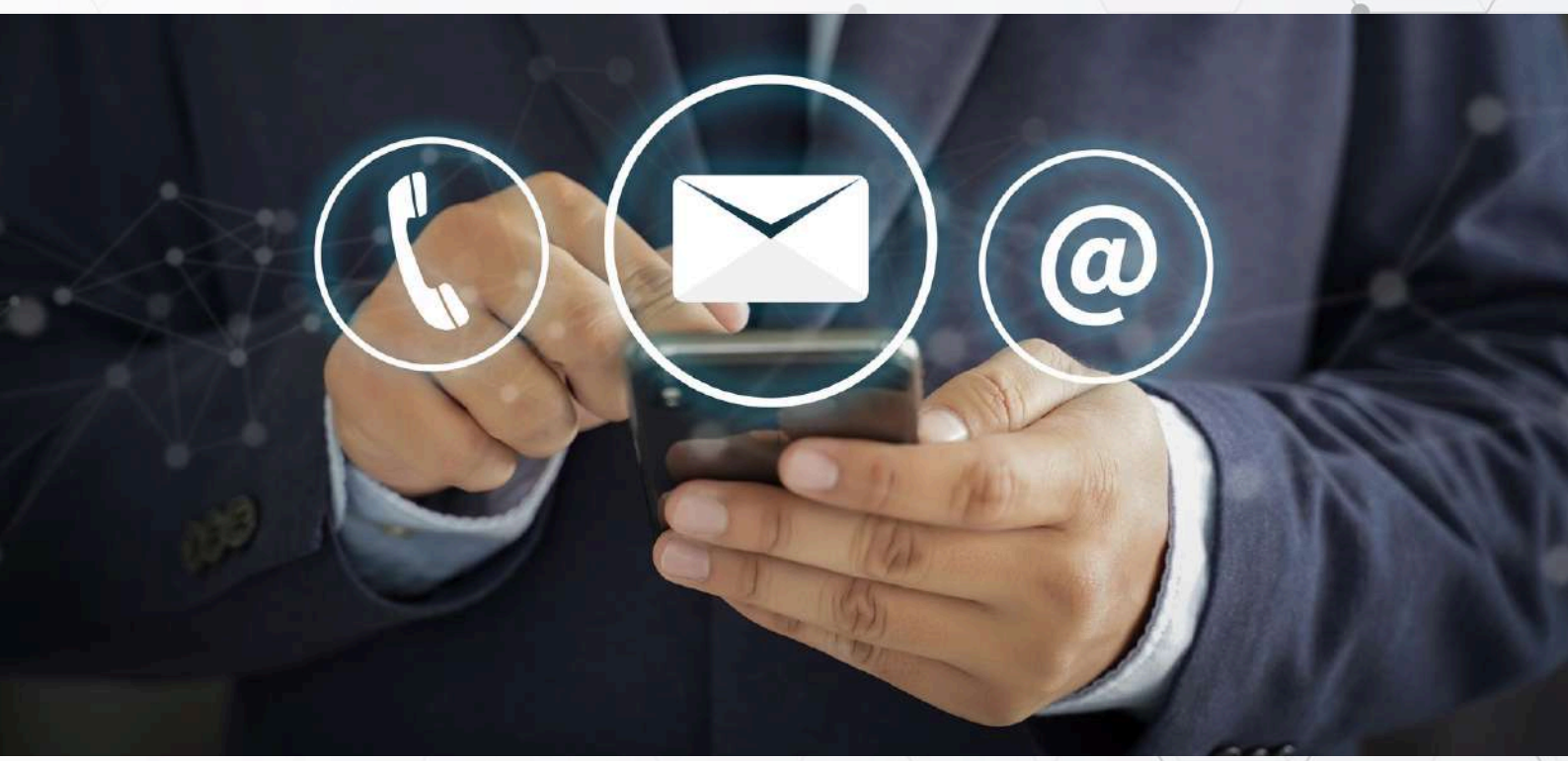
E-mail
info@arihantelectricals.com

Phone
+91 – 120 – 6256192

Social Media
arihantelectr
arihantelectr
arihantelectricals

Website
www.arihantelectricals.com
www.arisysel.com

HQ Address
Plot No. 60, Ecotech 12, Greater Noida,
Gautam Budh Nagar – 201 318, UP, India



We solicit your valuable suggestions and feedback to enhance this newsletter for future editions.