Vidya Vikas Education Trust's
Universal College of Engineering
Approved by AICTE, DTE, Maharashtra State Goverment and Affiliated to Mumbai University
Accredited with B+ Grade by NAAC | Recognised as Linguistic (Gujarati) Minority Institution

COMPILED AND DESIGNED BY:

Ms. Sampada Pimpale

VOLUME 03 EDITION 04

OCTOBER 2020

Department Vision:

To be recognized for practicing the best teaching-learning methods to create highly competent, resourceful and self-motivated young electronics engineers for benefit of society.

Department Mission:

- To nurture engineers who can serve needs of society using new and innovative techniques in electronics.
- To improve and apply knowledge of electronics subjects through participation in different technical events.
- To enhance carrier opportunities of electronic students through industry interactions and in plant training.
- To install the passion and spirit among students to pursue higher education in electronics and entrepreneurship.

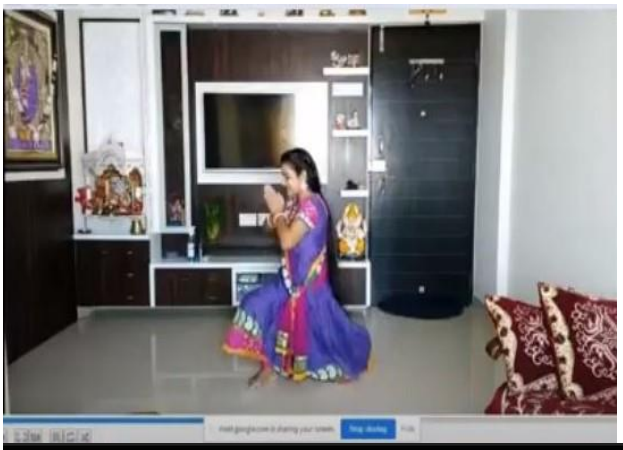
Teachers' Day Celebration

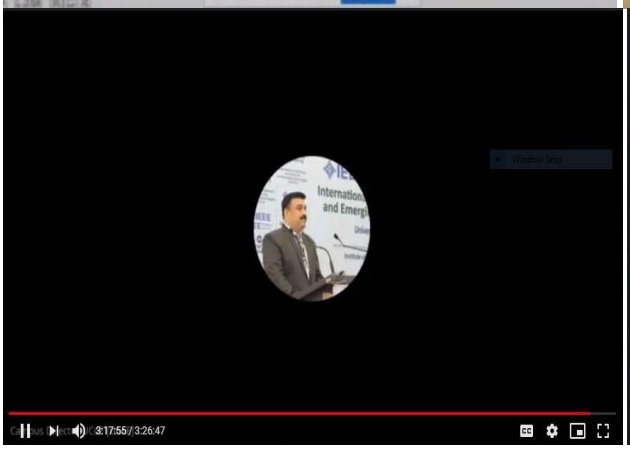
Celebrated on September 5 every year, this day marks the birth anniversary of Dr Sarvepalli Radhakrishnan, India's second President.

Across the country every year on September 5, Teachers' Day is celebrated. The day is dedicated to teachers and acknowledges their contribution in shaping one's life; something that Dr. S Radhakrishnan always wanted. Dr Sarvepalli Radhakrishnan, author, scholar, Bharat Ratna recipient and the first Vice President and second President of independent India, was born on September 5, 1888. Born into a Telegu family, a stark record in academics ever since he was young, Dr Radhakrishnan played into almost all fields of social sciences.

He was a philosophy academic, very respected in his field; and was responsible for garnering worldwide attention towards Indian Philosophy. His teaching career spanned for many years, teaching at Chennai's Presidency College and Calcutta University; then the Vice Chancellor of Andhra Pradesh University from 1931-36. He was then called by Oxford to teach the subject "Eastern Religions and Ethics" in 1936. He taught there for about 16 years.

This year due to Covid-19 pandemic, as all the colleges are temporarily shut-down, our college has celebrated the teachers' day through virtual platform. Below are the few glimpses for unique celebration of teachers' day celebration.





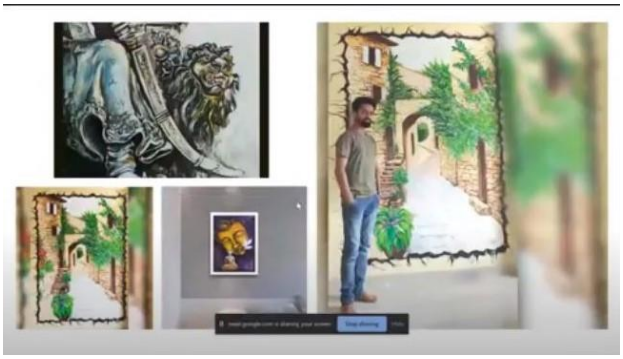
NSS Day Celebration

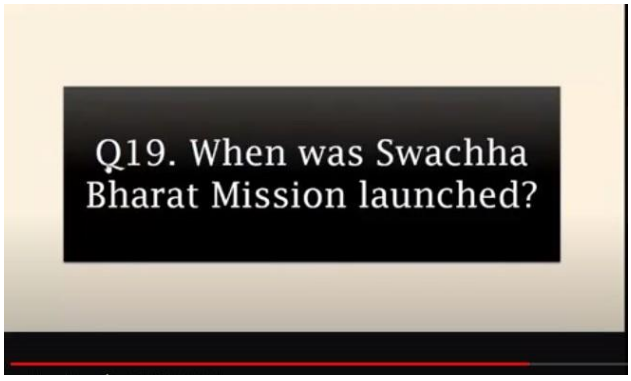
The National Service Scheme is a public service program conducted by the Ministry of Youth Affairs and Sports. Every year, NSS day is observed on September 24 across India.

The University Grants Commission (UGC) that was headed by S Radhakrishnan, had recommended the introduction of voluntary national service in academic institutions post-independence. In the year 1952, the government emphasized the requirement of social and labour service by Indian students for a year.

The National Service Scheme (NSS) is a central sector scheme of the government of India, Ministry of Youth Affairs & Sports. It allows the students of 11th & 12th Technical Institutions, graduate & post-graduate at colleges and university level of India to be a part of various government-led community service activities & programmes.

This year, the NSS day is celebrated on virtual platform. Some of glimpses of the event are shown pictures below.





The keys to secure embedded software development

In the last decade billions of connected devices have been created and adopted presenting an endless number of security challenges each day.

With Internet of Things (IoT) devices being integrated into homes, businesses, healthcare, factories and wearable technologies, there are a growing number of risks to our connected modern economy. With billions of new connected devices expected to enter the market in the next decade, the number of security risks is growing at an exponential rate and we need to address them

The landscape has changed for embedded system developers who have to manage an increasing number and variety of embedded systems in the form of IoT devices that are connected to the network, internet or cloud.

With IoT devices being used in many different environments for different purposes, there are a host of use cases for embedded systems which provide a wealth of attractive opportunities for hackers. The opportunities are also present in vast quantities as IoT manufacturers are producing IoT devices at a rapid rate as they race to provide the best products to the market at competitive prices. This means that the consideration of security in the design often takes a back seat, creating an environment of growing, large quantities of connected devices with poor security levels.

As a result, a whole new class of attacks, are now possible on smart home equipment such as home security systems and baby monitors which, while seemingly mundane, are a target for hackers. These types of devices present a vast array of risks to an opportunist who knows how and wants to gain access to private data on the network.

Smart connected fridges that automatically order the food vacant in a fridge, as well as home security cameras, have previously been a target for attackers to spy on victims or gain access to financial information. The only way to mitigate these risks is to ensure smart devices are properly secured and are reliable and safe to use. If embedded systems are not secured, they can easily become infected and used as a botnet for malicious purposes.

Learning from the past

Identifying what can go wrong in each use case of a device is key to understanding what is needed to increase security to prevent the attacks from happening in the first place.

With the use of technology growing at a rapid rate and with security developers struggling to keep up with the levels of protection needed, there have been multiple successful attacks over the years

which we have learnt key lessons from. For example, the Stuxnet virus in 2010 was a serious attack on critical infrastructure which compromised computer software in the Programmable Logic Controllers in the Iranian nuclear programme.

Similarly, 5 years later in 2015 hackers gained access to the firmware within the Ukrainian power grid which resulted in a temporary loss of power to 225,000 individuals. In both cases, the security of the systems involved were adequate at the time of design, however when attacked the systems were compromised as they no longer matched the sophistication of these cyber-attacks. With significant consequences possible, it is vital to understand what is necessary to prevent these attacks from happening today and in years to come.

With attacks becoming more sophisticated and more devices providing more opportunities for hackers, embedded systems must stay up to date to be the most secure. In order to reduce these vulnerabilities, embedded systems need to have secure updates integrated into the lifecycle of the software to protect the integrity of the device now and into the future.

Overcoming challenges

Embedded software developers play a critical role in mitigating the many risks possible in IoT devices by managing and protecting the integrity of its embedded systems and components.

In order to properly secure embedded systems, those systems must be designed with consideration of the needs of the device and the potential risks in mind. The level of risk must be identified first because the greater the level of risk, the greater level of security is needed. With every device being unique, there is not one solution that can be applied to address the many types of attacks that are possible with IoT embedded systems. In addition, one solution cannot be relied on during an embedded system's lifecycle. System updates will be needed throughout the life of the device and a process must be followed to ensure remote management of the integrity of the device.

An adaptive process

To secure software and firmware during the embedded system development process, there are a series of practices that Trusted Computing Group (TCG) recommends for a variety of unique devices.

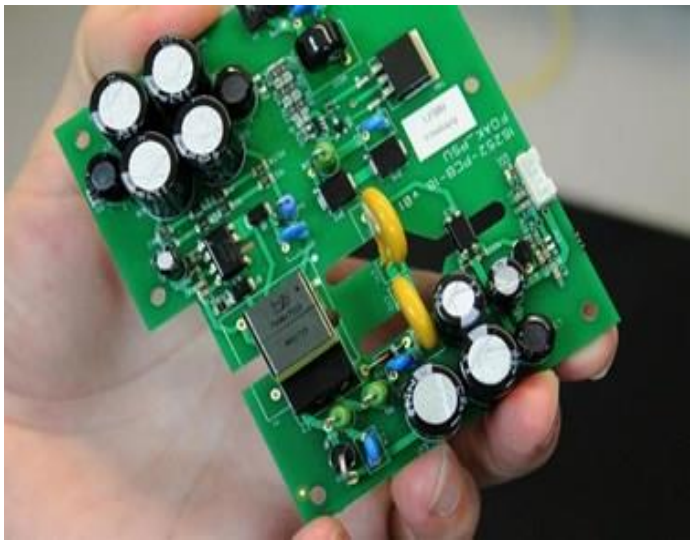
Firstly, security must be built into all steps of the development process so that all potential weak points are considered. From there, a thorough threat analysis is recommended to identify which countermeasures will be needed during the design and maintenance of their embedded system. With new and emerging threats constantly appearing, a consistent approach to applying best practices for security and improving them over time will ensure the integrity of the device is maintained through its lifetime.

Using the latest technology and solutions, such as the TCG Trusted Platform Module (TPM), enables embedded system managers to identify the integrity of device software remotely with 100 commands in each TPM available to take appropriate action when needed. The TPM can safeguard cryptographic keys and decrypt payloads to symmetrically encrypt the transportation of data between the distribution server and the device. This is essential to performing secure firmware updates to maximize device integrity and ensure that a high level of security is provided.

Source:https://www.newelectronics.co.uk/electronics-technology/the-keys-to-secure-embedded-software-development/231070/

A partnership in design

Although most electronics engineers understand the principles of an AC to DC power supply (PSU) and could probably design one to work, it takes specialist knowledge and skills to fully optimize it



for cost, size and performance. And in some cases, to develop a solution that might otherwise almost seem impossible. As a product design consultancy, 42 Technology is often asked to design PSUs either as a standalone project or part of a complete product design. Some of these projects can have particularly challenging requirements, not easily achievable using standard components, and to help with this the company regularly collaborates with the custom magnetic division of Würth Elektronik. Having identified the need for a bespoke transformer, the process usually starts by first listing the required electrical specifications – such as input/output voltages, primary inductance and so on – as well as details on relevant safety standards, mounting preference, manufacturing volume and cost target.

However, Martin Romero, one of Würth Elektronik's custom magnetic design engineers says some design teams do not always consider safety requirements or production volumes from the start. But these factors make a significant difference to other design trade-offs such as size, reliability, efficiency and cost. "Würth Elektronik is not only a transformer design house, developing over 100 new custom part numbers per month, but also a manufacturer. If we are told about target production volumes, we can adapt our designs to more easily fit into existing production lines to help reduce costs," says Romero.

"Also, it really helps if we are able to choose the transformer size and pin outs rather than them being pre-determined upfront." The bobbin and core are the two largest drivers behind transformer cost and size so they usually feature heavily in follow-up discussions to determine where design compromises can be made.

For example: if the specified windings are too thick to fit into the target bobbin they can be reduced at the expense of efficiency. Alternatively, the core size can be increased but this adds cost and increases the transformer footprint. Würth Elektronik typically takes around a week to develop a detailed design, then an additional week to supply test samples that can be evaluated by building and testing a prototype PSU. Samples are supplied with a specification sheet listing electrical parameters, package outline and pin outs, and a test data report When the design has been finalized, the transformer is then assigned a part number, allowing it to be ordered.

Source: https://www.newelectronics.co.uk/electronics-technology/a-partnership-in-design/230270/

ON Semiconductor Introduces High-Performance CMOS global shutter Image Sensor

ON Semiconductor, driving energy efficient innovations, has introduced the AR0234CS 2.3 Mp CMOS image sensor with global shutter technology. The high-performance sensor is designed for a variety of applications including machine vision cameras, AR/VR/MR headsets, autonomous mobile robots (AMRs) and barcode readers.

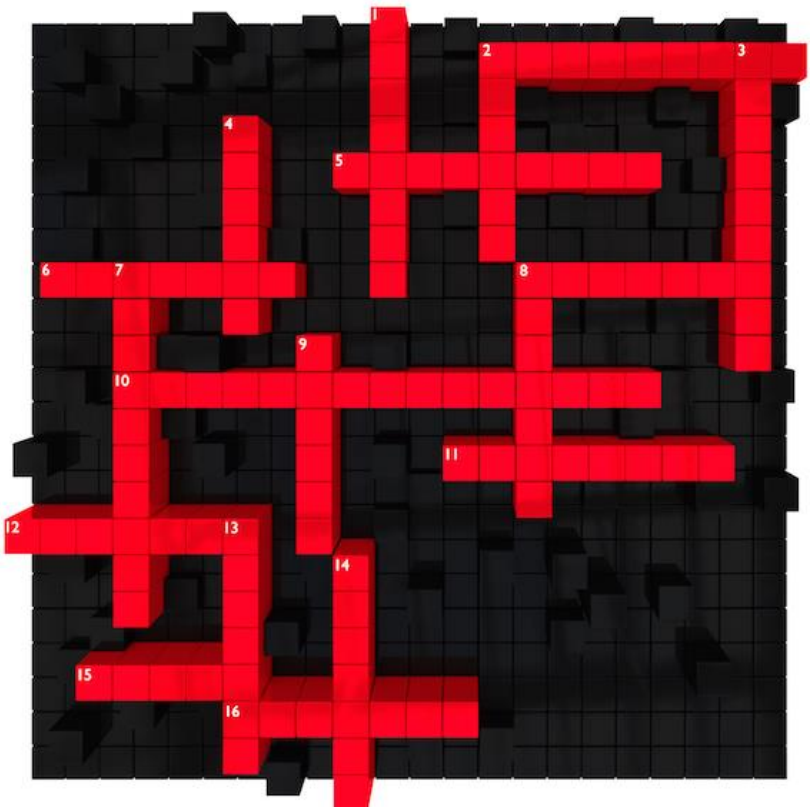
The AR0234CS captures 1080p video and single frames operating up to 120 frames per second (fps). With its industry-leading shutter efficiency, the 2.3 Mp sensor produces crisp and clear images by minimizing frame-to-frame distortion in high-speed scenes and reducing the motion artifacts other image sensors experience. The AR0234CS sensor's innovative pixel architecture delivers high dynamic range needed to support lighting conditions from the darkness of night to bright sunlight. The low noise and improved low-light response makes it suitable for applications spanning across consumer, commercial & industrial IoT, and the extended operating temperature range makes it deployable in challenging outdoor conditions.

"The need for quality image sensing is increasing, as more manufacturers are automating with vision-based expert systems," said Gianluca Colli, vice president and general manager, Industrial and Consumer Sensor Division (ICSD) Group at ON Semiconductor. "That demand requires optimizing size, performance and power of the image sensor. ON Semiconductor is one of the first manufacturers to recognize and respond to this need with the AR0234CS."

Other advanced features of the AR0234CS include: programmable regions of interest with on-chip histogram, auto exposure control and 5 x 5 statistics engine, fully integrated strobe illumination control, a flexible row and column skip mode, along with horizontal and vertical mirroring, windowing and pixel binning. Together with the AP1302 Image Signal Processor (ISP), the AR0234CS delivers a comprehensive camera system that can be designed and developed quickly for fast time-to-market. Additionally, system designers can access the DevSuite software to evaluate features and capabilities, configure and tune the sensor, and provide a ready-made output that is usable for further image processing.

Source: https://www.eletimes.com/on-semiconductor-introduces-high-performance-cmos-global-shutter-image-sensor

Technical Puzzle



Across

2. A diagram that shows the electrical connections of the electronic components
5. Current is considered to be the movement of _____.
6. A voltage source that converts chemical energy to electrical energy
8. A flow of electric charge
10. A characteristic of a secondary cell
11. A material that is composed of a mixture of elements
12. The term used to designate electrical pressure
15. A short circuit will have a _____ current flow.
16. The part of an atom that has no electric charge

Down

1. A voltmeter is used in _____ with the circuit.
2. A device that opens or completes an electrical path
3. A material that opposes the movement of free electrons
4. One coulomb passing a point in one second
7. A resistive component that is designed to be temperature sensitive
8. A unit of charge that contains 6.25 × 10^18 electrons
9. An atom's atomic number is determined by its number of _____.
13. A substance that is found only in its pure form
14. It is used to measure current.