Integrating Technology, Driving Growth

TechTalk

GALAXY
Integrating Technology | Driving Growth

GALAXY OFFICE AUTOMATION PVT. LTD. Issue No. 94 April 2020

Without an emergency business plan, you could be out of business!

The COVID-19 pandemic is a human tragedy, something of likes not seen since World War II. To minimize the spread, most parts of the world have practically locked down leading to employees not being able to attend offices. This has fast tracked technology to reshape the way we live, the way we work and enable us to perform our office work remotely. This is a wake-up call to organizations that focus on daily operational needs at the expense of investing in digital business and long-term resilience.

As organizations of all types shift to work from home—government, healthcare, financial services, customer support, and others—they need to enable employee access to the specific desktop and application configurations necessary to perform their roles remotely. IT leaders are witnessing challenges on Business Continuity, including infrastructure breakdowns, denial-of-service attacks, and sites going down because of traffic load, access to End Points etc. The onus of ensuring secure remote work by employees in times of crises, is definitely on the IT teams.

Galaxy can help your organization design and implement a technology infrastructure that will ensure the continuity of your key operations with solutions that are customizable, scalable and cost-efficient.

Galaxy's BCP Services enables a highly resilient business amidst the proliferation of cloud-based IT services, constant threats to your most critical information, and increasing expectations from stakeholders and regulators. Our expert solution consultants work with you every step of the way to transform how you approach business resiliency by optimizing existing programs and introducing new approaches. Our methodologies apply industry best practices to the IT infrastructure, security, application access and availability of your business resiliency programs to optimize them for your unique specifications.

Contact our experts by dropping an email at marketing@goapl.com to start planning right now!

Free Security for Times of Uncertainty

Let's work together to keep everyone safe

To help keep your employees safe and secure, we'd like to help your organization stay secure and without interruptions. To achieve this, we'd like to offer you CheckPoint's 60-day free licenses for three products that can ensure secure remote connectivity for all your employees:

Remote Access VPN | **Mobile Security** | **Endpoint Security**

To obtain this offer, please email us at marketing@goapl.com

MD SPEAKS

Anoop Pai Dhungat
Chairman & MD

Dear Readers,

As I am writing this article from home, my worst fears about the COVID-19 are coming true. Indeed, this virus is causing an enormous loss of lives and livelihoods and it will take a really brave and hardworking society to bounce back swiftly. I am very happy at the way our local administration has handled the situations on the ground. From introducing social distancing and only 50% of the staff being allowed to work in the office, to a complete lockdown once they realised that this was not being followed. I think everyone would have learnt the bitter lesson that if social distance cannot be followed voluntarily then lockdowns are the only option. Lockdowns, hurt everyone economically so it may well be in everyone's interest to absolutely follow social distancing and working from home wherever possible. When the lockdown will be removed is anybody's guess, but whenever that is we must remember that the virus will still be around.

I am really proud of my team that was able to ensure that most of our customers had the infrastructure in place to carry out their work remotely thus minimising the operational impact that the lockdown had on their businesses. I hope that this period passes quickly and we are able to collectively recoup and carry on as before.

Stay Home & Stay Safe

Future Is Now

‘World-first’ socially assistive robot under development in Scotland

Artificial intelligence experts in Scotland are working on what is believed to be the world’s first multi-user conversational robot for healthcare.

The Spring (Socially Pertinent Robots in Gerontological Healthcare) project at Heriot-Watt University is part of a multimillion-pound collaboration involving teams from eight European and Asian institutions.

It is the first research project to be announced by the National Robotarium – due to open at the university’s Edinburgh campus in 2021, and will develop socially assistive robots (SARs).

Working with existing robots such as the iCub, the research will develop the technology to perform multi-person interactions and open social conversation for the first time in a healthcare setting.

Professor Oliver Lemon at Heriot-Watt said: “Research shows that the careful use of robots in group settings can have a positive impact on health, such as decreased stress and loneliness, and improved mood and sociability.

“Healthcare practitioners have been supportive of the use of robots during the non-medical phases of time in hospital, because social robots can help explain complex concepts to patients with limited medical knowledge.

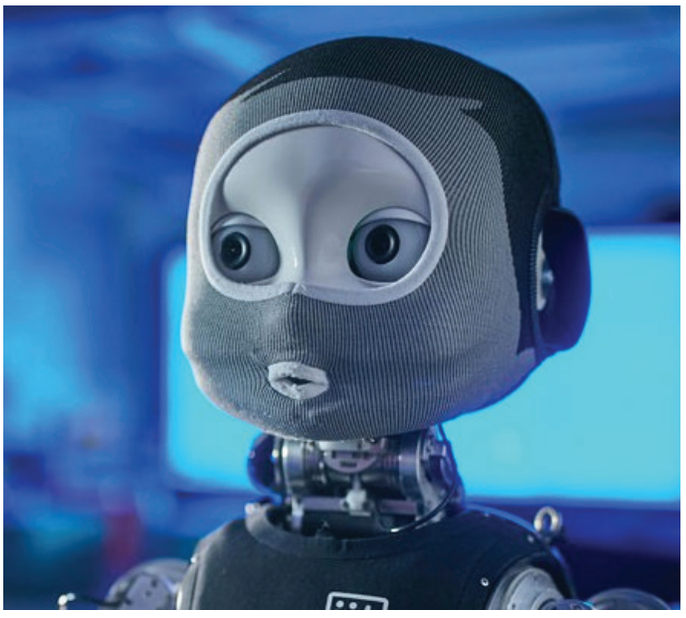
“Social robot technology is of interest for elder care, because robot companionship has the long-term potential to better connect people with each other. Social robots could improve both psychological well-being and the relationship between patients and hospital professionals.”

Research will focus on supporting elderly patients by combining scientific findings and technological developments.

The work will then help the robots understand various individuals and group situations to make appropriate decisions, such as identifying patients who have been waiting alone for a long time or who might be anxious.

Professor Lemon added: “While overcoming the limitations of current social robots raises numerous scientific and technological challenges, it has the potential to create tremendous social impact and economic value.

“The National Robotarium’s focus on creating societal benefits is ideally aligned to addressing such challenges. This type of technology is touch-free and hands-free so will be in great demand in the future as it will reduce the risk and spread of infection.”



https://bit.ly/2QTkVWE

Design of inorganic materials for brain-like computing

Ever wish your computer could think like you do or perhaps even understand you?

That future may not be now, but it's one step closer, thanks to a Texas A&M University-led team of scientists and engineers and their recent discovery of a materials-based mimic for the neural signals responsible for transmitting information within the human brain.

The multidisciplinary team, led by Texas A&M chemist Sarbajit Banerjee in collaboration with Texas A&M electrical and computer engineer R. Stanley Williams and additional colleagues across North America and abroad, has discovered a neuron-like electrical switching mechanism in the solid-state material β'-CuxV2O5 -- specifically, how it reversibly morphs between conducting and insulating behaviour on command.

The team was able to clarify the underlying mechanism driving this behaviour by taking a new look at β'-CuxV2O5, a remarkable chameleon-like material that changes with temperature or an applied electrical stimulus. In the process, they zeroed in on how copper ions move around inside the material and how this

subtle dance in turn sloshes electrons around to transform it. Their research revealed that the movement of copper ions is the linchpin of an electrical conductivity change which can be leveraged to create electrical spikes in the same way that neurons function in the cerebral nervous system -- a major step toward developing circuitry that functions like the human brain.

In their quest to develop new modes of energy efficient computing, the broad-based group of collaborators is capitalizing on materials with tunable electronic instabilities to achieve what's known as neuromorphic computing, or computing designed to replicate the brain's unique capabilities and unmatched efficiencies.

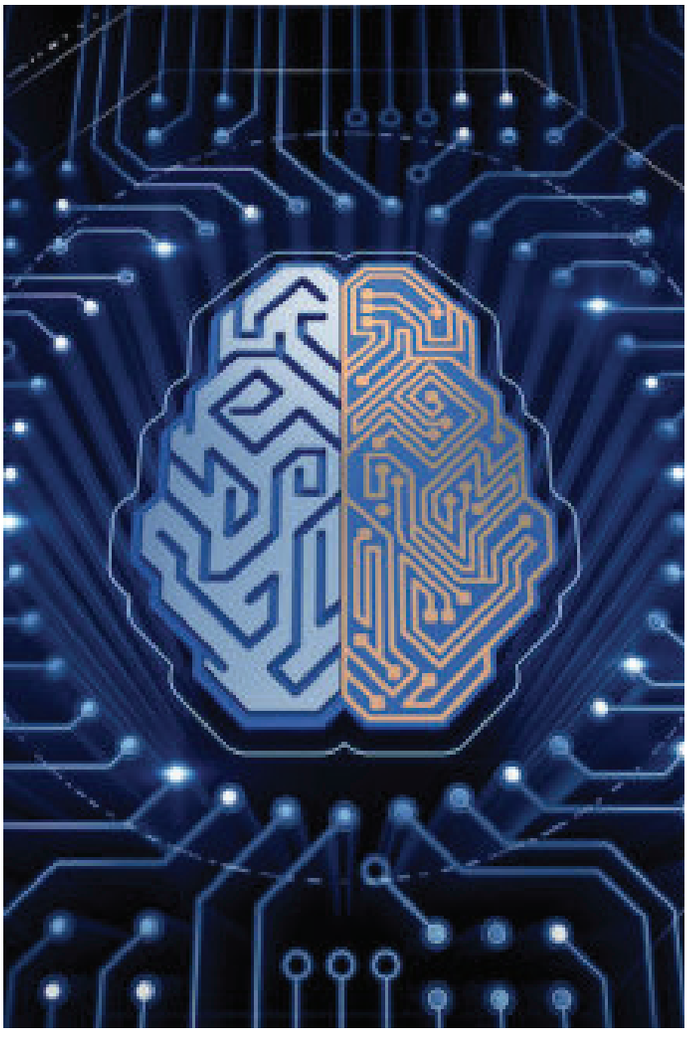
While smart phones and laptops seemingly get sleeker and faster with each iteration, Parija notes that new materials and computing paradigms freed from conventional restrictions are required to meet continuing speed and energy-efficiency demands that are straining the capabilities of silicon computer chips, which are reaching their fundamental limits in terms of energy efficiency. Neuromorphic computing is one such approach, and manipulation of switching behaviour in new materials is one way to achieve it.

By using an extensive combination of computational and experimental techniques, Handy said the team was able to demonstrate not only that this material undergoes a transition driven by changes in temperature, voltage and electric field strength that can be used to create neuron-like circuitry but also comprehensively explain how this transition happens. Unlike other materials that have a metal-insulator transition (MIT), this material relies on the movement of copper ions within a rigid lattice of vanadium and oxygen.

Transmitting, storing and processing data currently accounts for about 10 percent of global energy use, but Banerjee says extrapolations indicate the demand for computation will be many times higher than the projected global energy supply can deliver by 2040. Exponential increases in computing capabilities therefore are required for transformative visions, including the Internet of Things, autonomous transportation, disaster-resilient infrastructure, personalized medicine and other societal grand challenges that otherwise will be throttled by the inability of current computing technologies to handle the magnitude and complexity of human- and machine-generated data. He says one way to break out of the limitations of conventional computing technology is to take a cue from nature -- specifically, the neural circuitry of the human brain, which vastly surpasses conventional computer architectures in terms of energy efficiency and also offers new approaches for machine learning and advanced neural networks.

Because the various components that handle logic operations, store memory and transfer data are all separate from each other in conventional computer architecture, Banerjee says they are plagued by inherent inefficiencies regarding both the time it takes for information to be processed and how physically close together device elements can be before thermal waste and electrons "accidentally" tunnelling between components become major problems. By contrast, in the human brain, logic, memory storage and data transfer are simultaneously integrated into the timed firing of neurons that are densely interconnected in 3-D fanned-out networks. As a result, the brain's neurons process information at 10 times lower voltage and an almost 5,000 times lower synaptic operation energy in comparison to silicon computing architectures. To come close to achieving this kind of energetic and computational efficiency, he says new materials are needed that can undergo rapid internal electronic switching in circuits in a way that mimics how neurons fire in timed sequences.

Handy notes that the team still needs to optimize many parameters, such as transition temperature and switching speed along with the magnitude of the change in electrical resistance. By determining the underlying principles of the MIT in β'-CuxV2O5 as a prototype material within an expansive field of candidates, however, the team has identified certain design motifs and tunable chemical parameters that ultimately prove useful in the design of future neuromorphic computing materials, a major endeavor that has been seeded by the Texas A&M X-Grant Program.



https://bit.ly/39x8INP

5 Ways to Keep Your Data Safe While Working from home

As more and more organizations implement company-wide work from home policies as a way to protect the health of employees in the wake of COVID-19, they are also considering how to continue business as usual under a whole new networking situation

As more and more organizations implement company-wide work from home policies as a way to protect the health of employees in the wake of COVID-19, they are also considering how to continue business as usual under a whole new networking situation.

Many employees beginning a remote work situation for the first time may not be up to date on how to keep their devices safe, confidential information private and networks secure.

We asked IEEE Impact Creators and cybersecurity experts to weigh in and share their tips for staying safe online while working, as well as practicing social distancing:

Ensure Your WiFi and Router Passwords Are Secure

"One of the simplest things you can do to secure your home network is to ensure your WiFi and router passwords are secure," advised IEEE member Carmen Fontana.

It's important that your home network has a strong password that contains a variety of characters and symbols to prevent cyber attackers from easily breaking into your network. Keeping an industry-set password or not having a strong password is like leaving the door open for someone to walk into your house. Changing your password regularly is also a great way to keep the door locked on your devices.

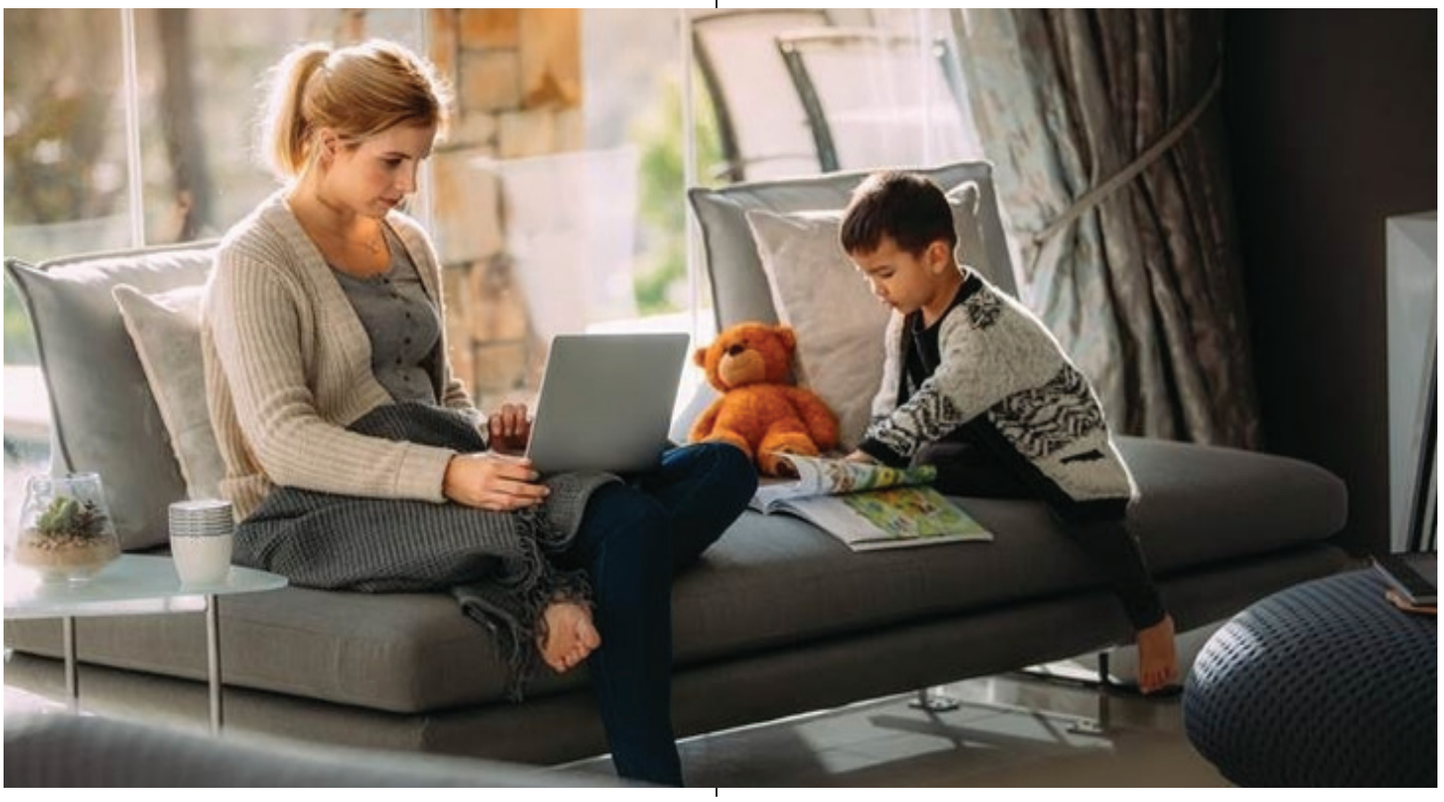
"Consider using separate security for your guest/family/IoT devices than your work WiFi," says Fontana. "If you want to go even further, think about implementing a firewall and/or Domain Name System (DNS) server."

Check In With Your IT Department

Spending more time working from home may expose new privacy vulnerabilities and information to bad actors — your IT department can be the first line of defense.

"Unfortunately, nefarious actors use situations like this to prey on our insecurities," says Fontana. "Your company's IT support team should never unexpectedly email you to ask for account information, home networking information, etc. Exercise excessive caution if you are contacted in this manner."

If you do encounter a situation you are unsure of,



contact your IT department to see if this was a company-approved initiative.

"If you receive a call purportedly from your helpdesk, call them back on the number listed in your corporate directory," reiterates IEEE member Kayne McGladrey. "Threat actors are actively calling employees in the hopes that they are unfamiliar with working from home."

Only Use Employer-Provided Devices

"Employees should only use employer-provided and approved hardware to connect to the corporate infrastructure when working remote," says McGladrey. "This is to limit the risk of accidental or unintentional data loss or exposure when using a personal device."

It might be tempting to use your personal device if you were not able to take home all of your hardware or if you feel your devices are easier to navigate. Your IT department has worked hard to set up infrastructures to protect you and your company from unintentionally sharing confidential information. It's safer to continue using the devices your company has provided.

Keep Your Software Up-To-Date

"Running the most recent versions of your mobile operating system, security software, apps and web browsers is among the best defenses against malware and other threats," says IEEE Senior member Kevin Curran. "When you see a message on your computer or mobile to update, then do so immediately. These updates often contain security patches which protect against new vulnerabilities."

As mentioned before, if you are feeling uneasy about updating anything — check in with your IT department before you hit download. They can confirm what seems suspicious and what is necessary for the health of your device.

Be Patient with Slower Network Servers

Remember to allow extra time as you navigate this new remote-only world of work. Network servers are expected to be a little slower as more people all take to their computers to get all necessary work done.

"With many people now working from home, we can anticipate some service outages and slowdowns," says McGladrey. "Be patient. We're all in this together."

https://bit.ly/2UFrBJm

Special Focus

Forcepoint Web Security Cloud is a flexible web protection solution that provides fine-tuned control over your users' web access, while providing comprehensive protection against web threats such as viruses, malware, data loss, and phishing attacks.

Forcepoint Web Security Cloud is intuitive to use and works out of the box with a default policy that applies common web filters. To make full use of its features, you can customize this default policy and configure your own policies to meet the needs of your organization.

This guide outlines the setup tasks required to get Forcepoint Web Security Cloud managing your web traffic. It also contains information on how to work with roaming users, and tips on tailoring policies for your organization. In the appendix you can find tips for preparing your end users for their new web protection system.

How Forcepoint Web Security Cloud works?

Forcepoint Web Security Cloud operates as a proxy server for HTTP and HTTPS traffic, as well as FTP over HTTP. When users request a web resource, their browsers do not connect directly to Internet web servers (shown in the following diagram as origin servers), but instead connect to the cloud proxy, which in turn relays requests to the origin server. This allows the cloud service to apply filtering rules and perform

content scanning, providing protection against security threats, data loss, and inappropriate content.

The service can use various methods to identify and authenticate users: The Forcepoint Web Security Endpoint, a third-party single sign-on identity provider, NTLM transparent identification, or manual authentication with a user name and password.

Roaming users (those connecting from an unknown IP address) can be identified via the Forcepoint Web Security Endpoint, via a single sign-on provider, or they are required to authenticate.

For a free consultation,
please email us at marketing@goapl.com

What is VMware Horizon?

VMware Horizon® 7 is a solution that simplifies the management and delivery of virtual desktops and apps on-premises, in the cloud, or in a hybrid or multi-cloud configuration through a single platform to end-users. By leveraging complete workspace environment management and optimized for the software-defined data center, Horizon 7 helps IT control, manage, and protect all of the Windows resources end users want, at the speed they expect, with the efficiency business demands.

What VMware Horizon Does

Delivers Desktops and Applications through a Single Platform

Transform static desktops into secure, digital workspaces that can be delivered on demand. Provision virtual or remote desktops and applications through a single VDI and app virtualization platform to streamline management and easily entitle end users.

Dramatically Improves ROI

Dynamically allocate resources with virtual storage, virtual compute and virtual networking to simplify management and drive down costs. Reduce day-to-day operations costs with a single platform that allows you to extend virtualization from the data center to your devices.

Secures Data and Simplifies Compliance

Consolidate control, delivery and protection of end user compute resources with policies that dynamically adapt to the end user's computing environment. Leverage virtual networking to simply and dynamically protect data center infrastructure and workloads.

Simplifies Management across On-premises and the Cloud

Take advantage of a modern desktop and application delivery architecture that delivers desktops in seconds, reduces storage and operational costs with truly stateless desktops and ensure painless application packaging and installation.

Supports a Rich, Adaptive User Experience

Provide a consistently great end user experience for knowledge workers, mobile workers and even 3D developers across devices, locations, media and connections.

We have a special offer for Horizon VMC on AWS use case and Horizon 7, to know more contact us at marketing@goapl.com

GALAXY
Integrating Technology | Driving Growth

A-23/24, Ambika Towers, Ground Floor,
Off. Jijamata Road, Nr, Pump House, Andheri (E),
Mumbai - 400 093, India.

91-22-42187777
marketing@goapl.com
www.goapl.com