

EPT

ELECTRONIC PRODUCTS & TECHNOLOGY

NOVEMBER/DECEMBER 2020

CANADA'S
INFORMATION LEADER
FOR ELECTRONIC
ENGINEERS AND
DESIGNERS

EPT.CA

CYBER THREAT

Keeping converged IT/OT environments safe from cyber attack p.12

DATA BREACHES

Malicious hacks are costing Canadian businesses more than ever p.16

PROTECTING IP

More effective security solutions for corporate IP at the Edge p.18

SECURING THE DATASPHERE

An approach to data security in an increasingly connected world p.10

DIGIKEY.CA



Access to
9.7 Million+
Products
Online

In-Stock@Digi-Key

Reliability You Can Count On

1,200+ INDUSTRY-LEADING SUPPLIERS

1.9 MILLION+ PRODUCTS IN STOCK

NEW TECHNOLOGIES ADDED EVERY DAY

9.7 MILLION+ PRODUCTS ONLINE

**FREE
SHIPPING**
ON ORDERS OVER
\$100 CAD OR \$100 USD*

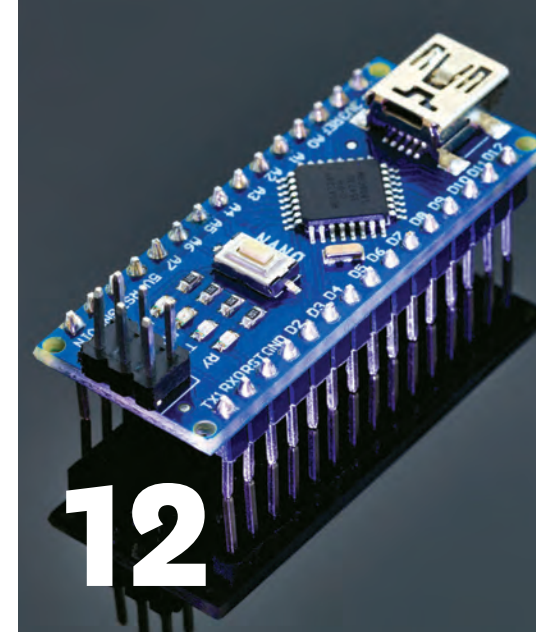


1.800.344.4539
DIGIKEY.CA



*A shipping charge of \$8.00 CAD will be billed on all orders of less than \$100.00 CAD. A shipping charge of \$20.00 USD will be billed on all orders of less than \$100.00 USD. All orders are shipped via UPS, Federal Express, or DHL for delivery within 1-3 days (dependent on final destination). No handling fees. All prices are in Canadian dollar or United States dollar. Digi-Key is an authorized distributor for all supplier partners. New products added daily. Digi-Key and Digi-Key Electronics are registered trademarks of Digi-Key Electronics in the U.S. and other countries.
© 2020 Digi-Key Electronics, 701 Brooks Ave. South, Thief River Falls, MN 56701, USA

ECIA MEMBER
Supporting The Authorized Channel



INSIDE

EP&T

NOVEMBER/DECEMBER 2020

Columns

4 EDITORIAL

Canada ups its game with educational initiatives in cybersecurity

8 WEST TECH REPORT

Woke Studios brings Elon Musk's artificial intelligence to life

In every issue

6 NEWSWATCH

22 NEW PRODUCTS

24 SUPPLY SIDE

25 PRODUCT SOURCE

25 AD INDEX

26 WOMEN IN ELECTRONICS

Fiona Leong, lead, procurement engineering with Clear Blue Technologies

COVER STORY

10 COVER STORY

Geotab puts focus on policies and best practices that help protect vital assets

12 CONVERGED ENVIRONMENTS

Security and business leaders require alignment to fend off cyber threats

16 CYBERSECURITY IN 2020

Securing more devices, systems and data than ever before

18 BEST SECURITY PRACTICES

Security-enabled IoT platforms are leading the way in countering threats



Cover photo: Getty Images/Stockphoto
Photos (this page, from top): Getty Images/Stockphoto



MSS1812T Series

Coilcraft

High Temperature Shielded Power Inductors



- Seven inductance values from 100 to 1000 μ H
- Excellent current handling with low DCR
- Low-loss ferrite drum core for flat inductance vs. current
- Cost-effective option for a variety of applications

Free Samples @ www.coilcraft.com

Canada takes bold steps in cybersecurity education



While Covid-19's 'new normal' forces companies to reconsider their existing plans, structures and processes and to seek out

new solutions, including in cybersecurity – it has become imperative for all nations to take steps to remain on the global forefront of research and security tech development.

Yes, cyber-threats are traditionally associated with password attacks. But, what about hardware? We currently live in an IoT-centric world where it seems that an increased amount of hardware devices have become wirelessly connected.

And, depending on the application, a lot of these devices can contain confidential information such as banking details, medical history, and other stored, personal details.

Fortunately, universities in Canada are joining the growing ranks of global cybercrime fighters. In fact, within the past year or so, four universities – the University of Waterloo and the University of New Brunswick, Ryerson and York Universities in Toronto – launched initiatives to increase this country's cybersecurity capacity.

University of Waterloo

Since opening its doors in September 2018, the University of Waterloo's Cybersecurity and Privacy Institute (CPI) has been tackling the emerging issues of cybersecurity and privacy head-on. By building on Waterloo's expertise in computer science, engineering, mathematics, cryptography and quantum computing the institute is creating a world-leading cybersecurity research and

technologies and increasing interdisciplinary collaboration across all faculties.

CPI's vision is to be internationally recognized as a leading interdisciplinary research institute making significant impact in improving information security and human privacy.

New Brunswick

Just over a year ago, the Canadian Institute for Cybersecurity (CIC) and the National Research Council of Canada (NRC) jointly opened the CIC-NRC Cybersecurity Collaboration Consortium (CNCCC) on the University of New Brunswick's Fredericton campus.

This innovative hub brings together more than 50 researchers and students to conduct cybersecurity research for critical infrastructure focusing on IoT, security, artificial intelligence, human-computer interaction, and natural language processing.

Today, the CNCCC is leading to discoveries and advances in cybersecurity including publications, patents, and the commercialization of technology, as well as providing training opportunities for graduate students and post-doctoral fellows.

The vision for the facility is to become one of the leading training and research institutes in Canada by 2021, renowned for its excellence in conducting cutting edge research in cybersecurity.

Already, its members' research is among the best in the world, with datasets that are used internationally for security testing and malware prevention.

Toronto's Ryerson & York U

Within the past year Ryerson University unveiled the SANS Institute, partnering with the Rogers Cybersecure Catalyst

to deliver much-needed cybersecurity training to women, new Canadians, and displaced workers. This unique training program – called the Accelerated Cybersecurity Training Program launched in the Greater Toronto Area (GTA), provides learners from diverse backgrounds the skills they need to launch careers in the cybersecurity sector.

Also in Toronto, the York University School of Continuing Studies launched an intensive format of its Cyber Security program this November to help address the critical and growing cyber security skills gap in Canada and worldwide.

In 12-weeks graduates can earn the Certificate in Cyber Security Fundamentals and the Certificate in Advanced Cyber Security. In addition, students will also be prepared to successfully write the exam for the CISSP designation.

In closing

With cyber threats growing in sophistication and magnitude across the world, the need for advancements and innovation in cybersecurity research has never been more critical.

Canada, it appears, is a prime target for cyber-attacks, as indicated by a 2019 study by Risk Based Security Inc. The report showed that Canada had the third most cyber incidents in the world, behind the US and UK at first and second place.

The good news is, as Canada continues to establish itself as a leader in developing cyber super-heroes, we won't have to look far for some help. **EP&T**

STEPHEN LAW

Editor
slaw@ept.ca

EP&T

ELECTRONIC PRODUCTS & TECHNOLOGY

Canada's information leader for electronic engineers and designers

NOVEMBER/DECEMBER 2020

Volume 42, Number 8

EDITOR Stephen Law
slaw@ept.ca · (416) 510-5208

WEST COAST CORRESPONDENT
Sohail Kamal · sohail@nextgear.ca

SENIOR PUBLISHER Scott Atkinson
satkinson@ept.ca · (416) 510-5207

MEDIA SALES MANAGER Jason Bauer
jbauer@ept.ca · 416-510-6797

ACCOUNT MANAGER Joanna Malivoire
jmalivoire@ept.ca · direct 866-868-7089

MEDIA DESIGNER Andrea M. Smith
asmith@annexbusinessmedia.com

CIRCULATION MANAGER Anita Madden
amadden@annexbusinessmedia.com
416-510-5183

ACCOUNT COORDINATOR Shannon Drumm
sdrumm@annexbusinessmedia.com

COO Scott Jamieson
sjamieson@annesbusinessmedia.com

EP&T is published eight times per year by

ANNEX BUSINESS MEDIA

111 Gordon Baker Road
Suite 400
Toronto, ON M2H 3R1
Tel (416) 442-5600
Fax (416) 510-5134
www.annexweb.com

SUBSCRIPTION RATES

Canada – \$58.50 one year;
\$94.00 two years
USA – \$134.00 (CAD) per year
International – \$183.50 (CAD) per year
Single copy – Canada \$15

CIRCULATION

amadden@annexbusinessmedia.com
Tel: 416-510-5183
Fax: 416-510-6875 or 416-442-2191

ISSN 0708-4366 (print)

ISSN 1923-3701 (digital)

PUB. MAIL AGREEMENT NO. 40065710

Return undeliverable Canadian addresses to: EP&T Circulation Department, 111 Gordon Baker Rd. Suite 400, Toronto, ON M2H 3R1



© 2020 EP&T. All rights reserved. Opinions expressed in this magazine are not necessarily those of the editor or the publisher. No liability is assumed for errors or omissions or validity of the claims in items reported. All advertising is subject to the publisher's approval. Such approval does not imply any endorsement of the products or services advertised. Publisher reserves the right to refuse advertising that does not meet the standards of the publication. Occasionally, EP&T will mail information on behalf of industry-related groups whose products and services we believe may be of interest to you. If you prefer not to receive this information, please contact our circulation department.

PRINTED IN CANADA

Funded by the Government of Canada



Connect with EP&T magazine

@EPTmagazine

facebook.com/EPTmag/

in/ept-magazine

info@ept.ca

ept.ca

Argentine, Australian, & Chinese Plugs—What's the Difference?



The Argentina plug is a Class I, 10A/250VAC which cycles at 50Hz. The standard plug rating in Australia is also 10A/250VAC. China's main grounded plug is also rated at 10A/250VAC. Are these sets compatible?

While China and Argentina have similar patterns, line and neutral contact pins for these plugs are reversed—the same for Australian and Argentinian plugs.

Australian and Chinese plugs and sockets have similar patterns—the Chinese pins are 1 mm longer than the Australian pins, and the plug sizes differ. Yet the Australian plug will mate with the Chinese socket.

Australia's plug and socket is described in AS/NZS 3112 and its standard rating is 10A. The set can be terminated with many IEC 60320 connectors.

China requires that their plugs, couplers, and cable be tested by the China Quality Certification (CQC) center to obtain the China Compulsory Certification's "CCC" mark.

Argentina requires cord sets be approved by IRAM (mark) and the Argentine product safety mark.

Australia requires approval of cord sets through a state testing agency, e.g., Department of Fair Trading. Instead of an approval mark, a file number is used.

Order Online! www.interpower.com

Business Hours: 7 a.m.–6 p.m. Central Time



MATERIALS

AIRCRAFT FLIES WITH 3D PRINTED HARDWARE COMPONENTS

Flight hardware components manufactured by a 3D printer were incorporated into the electronic design of supersonic aircraft, marking a turning point in commercial viability for high speed travel and demonstrates the power of additive manufacturing (AM), or 3D printing, while accelerating product development.

VELO3D, a Campbell CA-based digital manufacturer, recently announced that Boom Supersonic's XB-1 aircraft includes 21 flight hardware components that were manufactured by VELO3D's Sapphire 3D metal printer.

"Aviation hardware is especially difficult to manufacture with 3D metal printing, due to challenging aerodynamic designs that must be balanced with superior durability and high temperature requirements," says Benny Buller, CEO and founder of VELO3D.

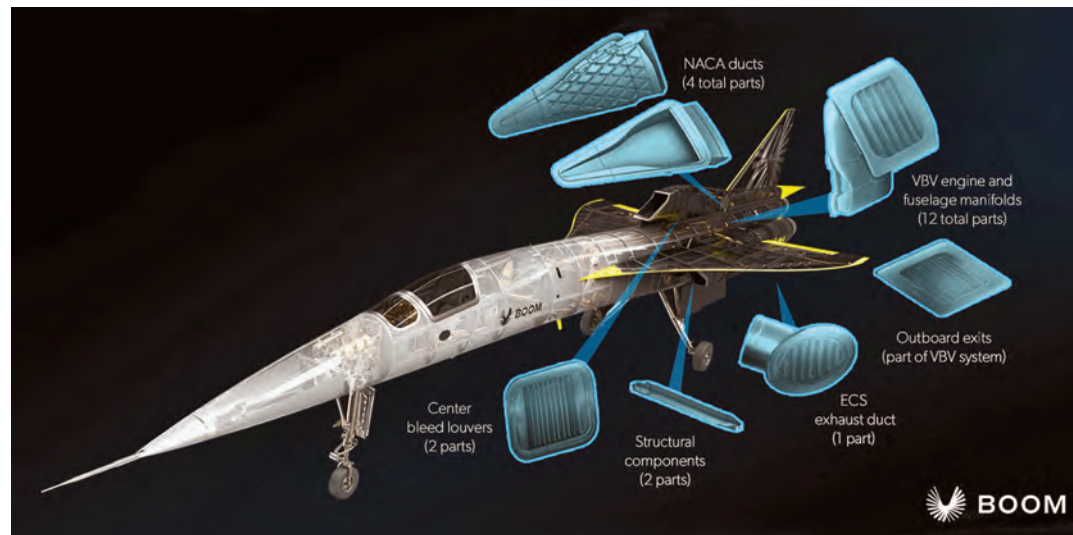
The printed Titanium parts are used for engine hardware, the environmental control system, and structural components. Characteristics of the geometric designs include tall, thin walls with high aspect ratios, which are inherently difficult to manufacture with either traditional processes such as welding and casting, or even most existing 3Dprinting technologies.

ELECTRONICS, AUTO SECTORS SPARK ADOPTION OF NEW CONDUCTIVE MATERIALS

Increasing demand for high-efficiency electronics and components such as electrical circuits is sparking innovation in the electrically conductive materials industry, according to recent analysis released by researchers Frost & Sullivan.

The demand for materials such as conductive polymers, conjugated polymers, quantum dots, metamaterials, conductive hydrogels, and shape memory alloys is expected to increase in the next five years. Extensive miniaturization efforts and anticipated electric vehicle penetration will result in the consumer electronics and automotive sectors securing the highest adoption potential for electrically conductive materials.

"Enhanced material properties such as thermal management improved electrical conductivity, and better



Boom's XB-1 will fly with Titanium 3D-printed components, most of which perform critical engine operations. All parts are manufactured using a 3D printing system.

mechanical properties will result in significant operational efficiency upgrades," says Aarthi Janakiraman, TechVision research manager at Frost & Sullivan. "The development of nanomaterials for manufacturing electrically conductive materials will open up new avenues for adoption. This will improve the application scope by addressing the key consumer demand for compact and energy-efficient devices."

AUTOMATION

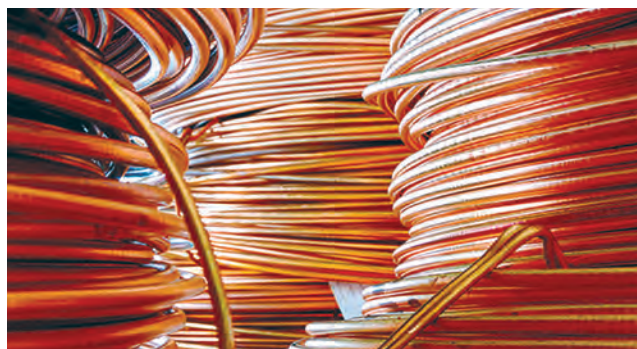
GERMAN TECHNOLOGY DAY PRESENTS ONLINE



Six prominent German-based players in automation and advanced manufacturing hosted Canada's second series of German Technology Days as a virtual event recently, attracting close to 500 registrations. Bosch Rexroth, EPLAN, Murrelektronik, PILZ, Rittal and WAGO, all with operations in Canada, delivered their seminar-styled presentations in an online approach.

The event incorporated many aspects that made the 2019 show successful into the new format.

The online trade show began with



The push for new electrically conductive materials is being driven by the electronics and automotive industries.

Source: Frost & Sullivan

a session that introduced attendees to each company and what they do.

"Rittal was pleased with the outcome of the German Technology Day Virtual Fair, with the theme of 'Collaboration and Connectivity.' Our digital platform truly enabled us to convey to the audience just how connected we are: from our IoT solutions to the integration with other partners in the industry," says Tim Rourke, president, Rittal Systems Ltd.

"Given its success, we hope to continue to enhance the event in the years to come, making it even more inclusive and keeping up with the latest trends in the manufacturing and electrical industry."

MANUFACTURING

M2S ELECTRONICS AMPS UP LOCAL MANUFACTURING



M2S Electronics, member of the Narvi consortium, a Quebec City-based designer and assembler of electronic & electromechanical systems, recently invested \$ 2.5-million into industry 4.0 infrastructure with the purchase of additional state-of-the-art production equipment.

As a result, the manufacturer can now provide enhancements in capacity and services for Quebec-based businesses – especially those that decide to relocate their electronic production in the province.

"On the strength of its financial health, M2S Electronics offers a real alternative to repatriate electronic productions from Quebec customers on our soil," says Jean-Daniel Binant, development executive director, M2S Electronics. "Moreover, for many of our own productions, for some in Asia

since the beginning of the 2000s, we have started more than two years ago to repatriate them to Quebec because automation 4.0 makes us competitive locally while reducing risk in the supply chain such as we have just experienced it with the Covid-19,” Binant continues.

AUTOMOTIVE

PROJECT ARROW VEHICLE DESIGN REVEALED

Automotive Parts Manufacturers’ Association (APMA) of Canada has officially unveiled its plans for the first, original, full-build, zero-emission concept vehicle named Project Arrow. An all-Canadian effort, it will be designed, engineered and built through the joint efforts of Canada’s world-class automotive supply sector and post-secondary institutions.



The winning design was selected from a field of three finalists and nine complete submissions. The winning team hails from Carleton University’s School of Industrial Design in Ottawa. The chosen vehicle design answered all the requirements of the competition brief and APMA says it represents a design that properly showcases Canada leadership in this space.

The global automotive market is entering a new era that is driven by the ‘ACES’ dynamic – autonomous, connected, electric, shared. Project Arrow is a lighthouse initiative that will showcase what Canada’s world-class automotive supply sector, its auto-tech SMEs and academic institutions can do on the global stage, according to APMA.

WEARABLES

HALIFAX WEARABLE FIRM CREATES COVID TOOL

Tenera Care, a Halifax-based wearable technology and data analytics firm, has created a tool for contact tracing in long term care facilities.

The wearable device pinpoints



Tenera Care created wearable device for contract tracing.

an individual’s location within 15cm, providing a highly effective level of accuracy in managing contact tracing when worn by all residents, staff, and visitors to a facility.

During a global pandemic, this technology provides a level of transparency and visibility and means only people who need to be quarantined, are quarantined.

A widespread installation of this platform presents an opportunity for

public health, as Tenera has been in discussions with provincial governments to finance the installation of the platform in long term care facilities. On top of the health benefits, the platform creates efficiencies in scheduling, with tangible savings to staffing costs.

Tenera sees the future of this platform in other industries like manufacturing.

Visit ept.ca for the latest new products, news and industry events.



The Engineer’s Guide to Who Makes What and How to Find It

As the engineer designing the future, you need resources that tell you not only where the future is headed, but also what components are available to manufacture that future. TTI can help. Our Markets and Technologies Resource Centers include:

- **Featured Product Data**
- **TTI and Supplier Literature**
- **White Papers and Articles**

It’s the place to find the information you need to innovate from TTI and the industry’s premier suppliers.

ttiinc.com/resourcecenters
1.800.CALL.TTI

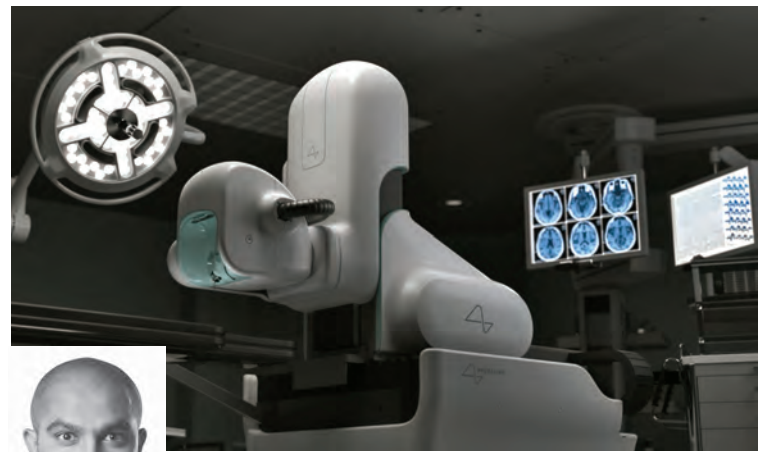


Woke Studios brings ELON MUSK's AI to life

The ascendancy of artificial intelligence is accelerating. Loudly asserted by tech icon Elon Musk, this trend poses existential threat risks to human life. The debate as to whether this progress is worth the inherent risks will continue, and in this article, we introduce an award-winning Vancouver design firm to fuel further debate.

The company is Woke Studios, which designs for Neuralink,

Musk's very own neural technology start-up. Neuralink recently released a presentation on their chip, which Musk described as "a Fitbit in your skull with tiny wires," that can read or write brain activity. The neural chip is a 'body ware' to be inserted surgically by a robot designed to implant the chip and wires with minimal damage to the brain or blood vessels. Musk says that



Afshin Mehin, CEO (left) of Woke Studios, assisted with the design of a surgical robot (above) for Elon Musk's Neuralink venture.

the process only takes hours, and leaves "just a small scar."

West Coast Report recently had the opportunity to interview Afshin Mehin, CEO and founder of Woke Studios, to find out how they have been able to stand out from the crowd, how they were discovered by Neuralink, and the role of AI in our future.

As an industrial design studio, Woke helps companies translate visionary technologies into products and services people will fall in love with.

"We are optimists at heart and believe that if new technologies are introduced into people's lives in the right way, that there is always a huge opportunity to improve quality of life," says Mehin.

Having won a RedDot design award for its Mio Slice wearable, and after supporting Recon Instrument's sunglasses, a product that led to Recon's acquisition by Intel, Woke was introduced to the team at Neuralink by Kindred (<http://www.kindred.ai>). As a member of the Recon team, Woke had to interface with electrical engineers and mechanical engineers to get their input and help to design the best 'experience' product for wearers. All three of these firms operate their HQ in Vancouver, illustrating the importance of being BC-based.

"Vancouver is a hotbed for soft goods companies. Being part of that ecosystem has always helped us be able to develop best in class close to body technologies," explains Mehin. "The challenges of having technology that has to be on your body, adapting to your bone and muscle structure, and giving and adjusting based on the human body's complex movements is something apparel designers have been dealing with

for centuries."

So where does this leave Woke with respect to AI? Interestingly, Mehin has a clear perspective.

"What is natural, what is unnatural? Wearing shoes is unnatural. With the Neuralink chip, one might see it as unnatural, see it like we are hacking the brain." On the other hand, says Mehin, "We might be able to harness this technology for people who can benefit from it, people who are paralyzed, who could not move a single muscle. They could learn to control a robotic arm to move a cup of water to their mouth so that they could drink from a straw."

This technology can help people, but it is important to be critical to ensure that we remain respectful, and Mehin is confident that technology can be used for good. Woke Studio excels at the thoughtful tailoring of products to end-user needs. Mehin concludes by suggesting to other entrepreneurs to set the bar high for creating a product or service that will leave your customer with a sense of delight and wonder in addition to providing a ton of value.

"Think about how design and design thinking can be applied more broadly across your business, whether it's designing your go to market strategy or designing your product's end of life strategy. The process of design is really powerful and can benefit companies well beyond styling a product." **EP&T**

Woke Studios <https://woke.com>

Neuralink <https://neuralink.com>



Sohail Kamal is EP&T's West Coast correspondent. sohail@nextgear.ca

Photo: Woke Studios



LECTRO®

CANADIAN BASED AUTHORIZED ELECTRONIC COMPONENT DISTRIBUTOR.

- ✓ Free shipping and sampling.
- ✓ Stocking program for 12 months.

CAPACITORS

(Film, Electrolytics, Ceramics, Tantalum, Super Caps)

CIRCUIT PROTECTION

(TVS, Varistors, PPTC, Fuses)

CONNECTORS

(Board to board, Wire to Board, IO / RF / USB type connectors)

DISPLAYS

(Alphanumeric, Graphic, TFT, OLED, Custom Glass)

EMBEDDED AND IOT

(RF Modules, SBC, HMI)

FREQUENCY CONTROL

(Crystals, Oscillators)

INDUCTIVE

(Transformers, Inductors, Chokes & Coils)

MEMORIES

(SSD and DRAM)

OPTOELECTRONICS

(Low-medium-high Power LEDs, 7 Segments, Detectors)

POWER

(AC-DC & DC-DC, PCB mount, Wall Mount, Rail Power supplies)

TERMINAL BLOCKS

(PCB and RAIL type)

THERMAL MANAGEMENT

(Fans, Blowers, Heatsinks)

Contact Ken for Specs, Pricing & Availability

✉ ken@dblectro.com ☎ 1-888-394-1424

Engineered to make life easier!



Tired of spending hours resolving radiated EMI issues? Use a power supply that actually meets Class B, even in a Class II construction (no earth ground).

CUS-M Series

High Performance Medical and Industrial AC/DC power supplies with low EMI

Features:

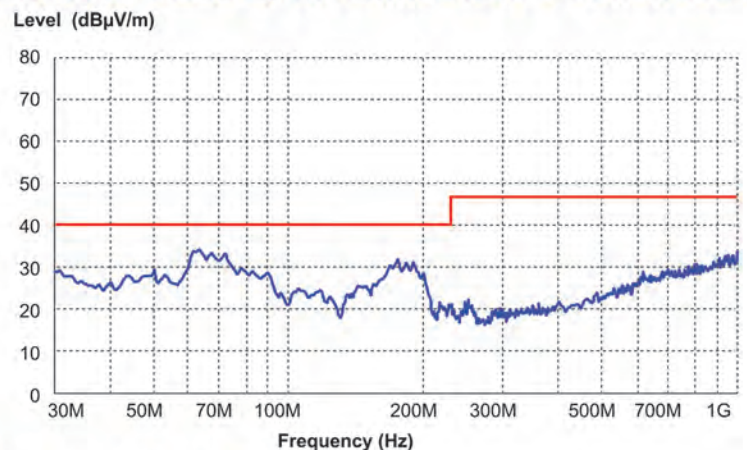
- Industrial and medical safety certifications
- Industry standard footprints
- Efficiencies up to 96%
- 4kVAC isolation and low leakage currents
- Suitable for B and BF rated equipment
- Class B conducted and radiated EMI

30-1500 Watt AC/DC Power Supplies

Model	Watts	Package	Size	Construction
CUS30M	30W	O, E, P*	2x3"	Class I / II
CUS60M	60W	O, E, P*	2x3"	Class I / II
CUS100ME	100W	O, E, B	2x4"	Class I / II
CUS150M	150W	O, E, B, F	2x4"	Class I / II
CUS200M	200W	O, E	3x5"	Class I
CUS400M	400W	O, E, B, F	3x5"	Class I / II
CUS600M	600W	O, E, F	3x5"	Class I / II
CUS1500M	1500W	E	5x2.5x10.3"	Class I

* E = Enclosed, O = open frame, P = pcb mount, F internal fan, B conduction cooling

EN55032 Class B, QP Limit Class II Construction



In stock for immediate purchase through our Distribution Partners:



For more information on how TDK-Lambda can help you power your unique applications, please visit our website at www.us.lambda.tdk.com or call 1-800-LAMBDA-4



Securing the Datasphere

An approach to data security in an increasingly connected world. **BY ALAN CAWSE**



There's an old saying: "Never let a good crisis go to waste." For cybercriminals, COVID-19 couldn't have provided a better opportunity to take advantage of organizations across the globe as they were scrambling to shift to a remote workforce. As if a massive disruption in business alone wasn't enough, corporate leaders were challenged with the task of securing enterprise perimeters that had suddenly vanished.

Now, as we near the end of 2020, organizations are moving forward, but are looking at enterprise security through a much different lens. As they chart a path toward ensuring that people, computers, networks and platforms are secured, many have adopted a zero-trust approach. And, for good reason. With data underpinning decision making in nearly every industry—finance, healthcare, retail and transportation—the ecosystem has become increasingly complex as the threat landscape expands.

For the past ten years, IDC has been calculating the amount of information the world collectively creates, captures, replicates and consumes in what it calls the global 'datasphere.' In a comprehensive study sponsored by Seagate, IDC experts predict our digital world will reach 175 zettabytes by 2025 to reflect a 61% increase from 45 zettabytes in 2019. Putting this into context, IDC senior VP David Reinsel explains that storing 175ZB of data would require 12.5-billion hard drives,

or so many Blue Ray discs that when stacked would climb the distance of the moon (238,900 miles)—23 times. (Then, correlate this volume of data to security vulnerability).

Security vulnerability

For decades, data has been essential to the transformation of the automotive industry, where on-board diagnostics (OBD) were introduced in the 1980s by the California Air Resources Board to track emissions in an effort to reduce pollution.

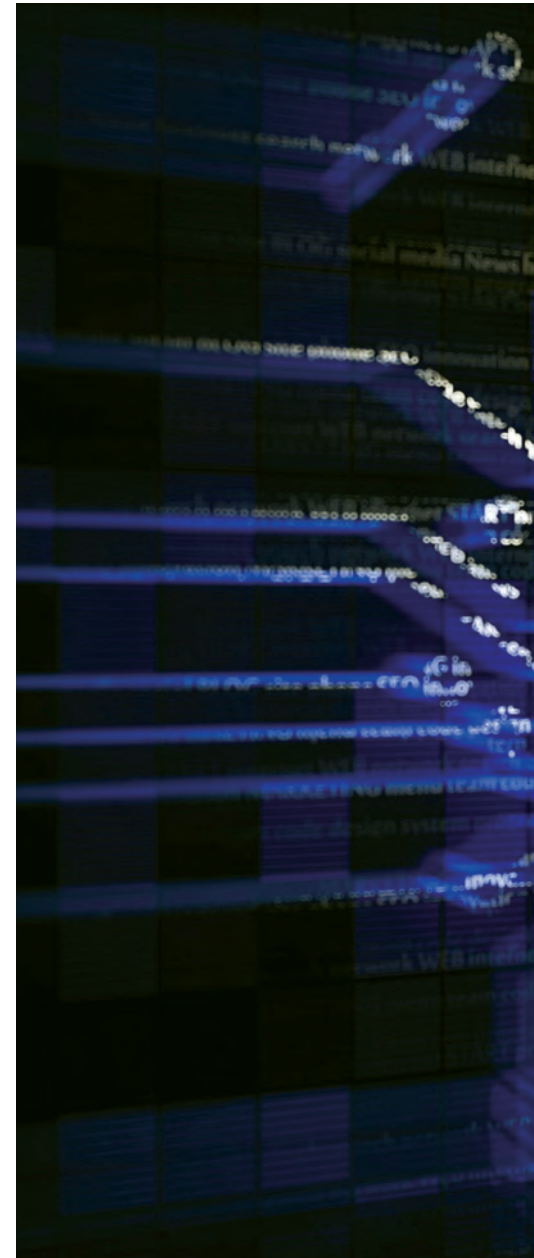
By 1996, when the OBD system was mandatory for all new vehicles, General Motors introduced OnStar, which connected drivers to roadside assistance and emergency services. Since then, OBD has become ubiquitous, not only giving vehicle owners insight to safety, maintenance, miles and driver behavior but also revolutionizing fleet management.

The presence of the OBD port allows GPS fleet tracking devices, widely referred to as telematics, to silently collect information such as fuel and electric usage, external weather conditions, road safety and traffic information, as well as provide insight into vehicle health and driver behavior. In fact, in the commercial and government sectors—where telematics solutions have been widely adopted among small, medium and mega-sized fleets—connected vehicles are a reality; businesses and governments could not operate without them.

We adopt a philosophy of vigilance, where reviewing, improving and validating security mechanisms and processes are key to ensuring systems remain resilient

ISO 27001

certification is essential to Geotab as it affirms that it is focused on following policies and best practices to protect the company's vital assets



According to Allied Market Research, the global automotive telematics market is projected to reach \$320.6-billion by 2026, reflecting a compound annual growth rate of 26.8% from 2019 to 2026. While the industry continues to experience explosive growth as data becomes increasingly invaluable, not only for fleets operators but also carmakers, insurance, logistics and supply chain companies, data security is more important than ever.

40-billion data points

As the top commercial telematics vendor, ranked #1 worldwide by ABI Research, Geotab Inc. takes a rigorous approach to security. With more than 40,000 customers around the world collectively deploying approximately 2.2-million Geotab GO devices, along with the MyGeotab platform to optimize fleet management, our firm processes more than 40-billion data points every day. Geotab's highest priority is to implement and maintain stringent security, technical and

Protecting converged IT/OT environments from cyber threats

Security and business leaders require alignment.



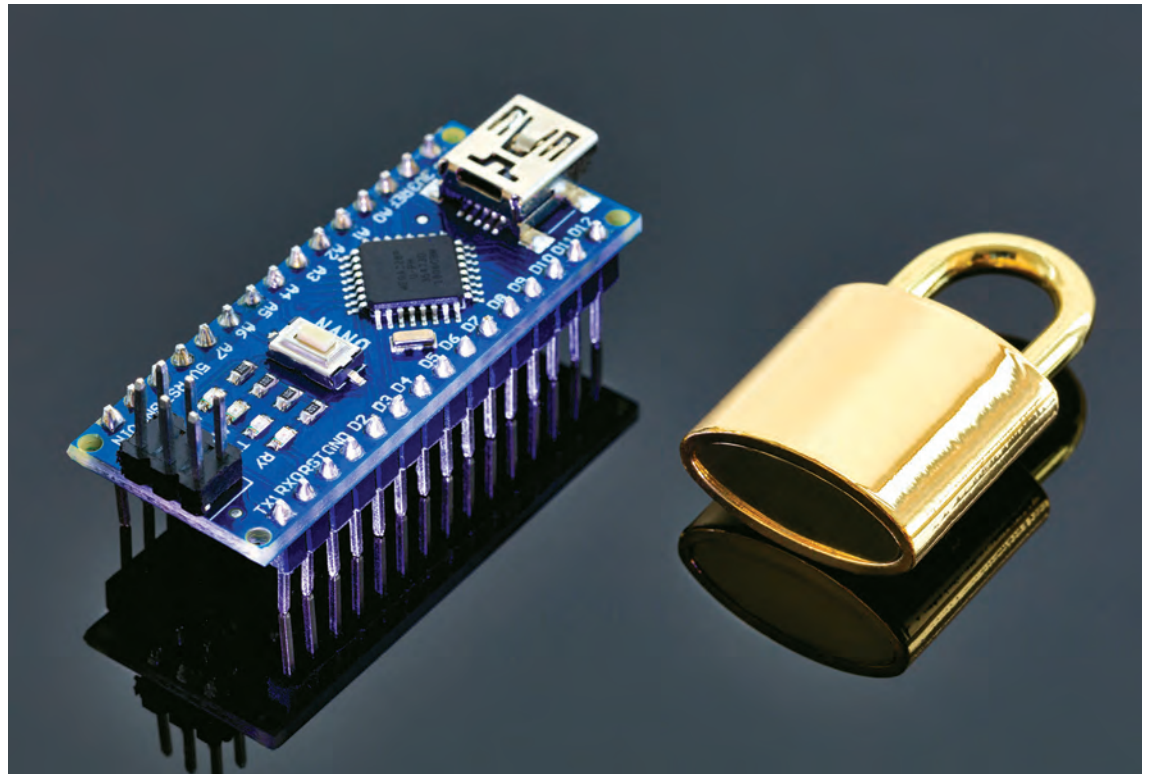
With the rise of digitized manufacturing and industrial internet of things (IIoT), the attack surface has expanded, converging the worlds of IT and operational technology (OT), while introducing new attack vectors that have allowed cyber threats to grow at alarming rates.

CISA recently warned about vulnerabilities in motion sensors in robotic controllers, commonly used in the critical manufacturing and healthcare sectors, and issued an advisory warning of rising threats to OT and control systems as OT assets become internet accessible.

In recent years we've seen a number of similar attacks, including the EKANS ransomware earlier this year that was designed to target industrial control systems. Despite the constant warnings and evidence of ongoing attacks, security teams often face challenges in aligning leadership to confront the issue of cyber risk.

The reality is that cyberattacks such as those designed to steal IP, disable networks or sabotage equipment can have serious consequences on critical infrastructure and essential services for entire countries.

The pandemic has underscored this threat as the heightened reliance on essential services continues to pique cybercriminals' interests. In fact, a recent study conducted by Forrester Consulting on behalf of Tenable found that, over the past year, 65% of organizations in the U.S. suffered business-impacting cyberattacks or compromises that involved OT systems. For these environments, bolting on a security solution alone is only fighting half of the battle. Organizations



need to integrate security into the business strategy and ensure close coordination between security leaders and business executives — particularly in industrial environments that often rely on 24/7 operations.

But, in most organizations, this isn't happening. The study, which surveyed over 800 global security and business executives in a variety of sectors, found that 75% of business and security leaders say their COVID-19 response strategies are, at best, only 'somewhat' aligned.

Align cyber strategies to business objectives

The good news is there are some concrete steps organizations can take to align leadership to take action and reduce cyber risk.

Just 54% of security leaders and 42% of business executives say their cybersecurity strategies

are completely or closely aligned with business goals. At its core, this is due to inconsistent communication among leadership, spurring a split in priorities and strategies. According to the study, fewer than half of security leaders consult business executives all the time or very frequently when developing their cybersecurity strategies. On the flip side, four out of ten business executives rarely — if ever — consult with security leaders when developing their organizations' business strategies.

The first step to correcting this is to begin a regular cadence of communication with business leadership to understand priorities and establish a coordinated strategy. In converged industrial environments, this will initially require both OT and IT security personnel to align on approaches. Historically, IT and OT security

teams held different priorities, with OT staff typically focused on stability, safety and reliability, and IT staff concerned about data, integrity, availability and confidentiality. Now that OT has been brought online, it has converged with IT, and IIoT devices have introduced even more interconnectivity, widening the playground for a cybercriminal in an attack scenario.

Position cyber risk as business risk

With IT/OT security teams on the same page, they are better poised to both strengthen communication with business leaders as well as address today's threats as a unified front.

A cyberattack can have devastating effects on business continuity, but these risks are often lost in translation when communicating with business leaders. In

fact, fewer than half of security leaders are framing the impact of cybersecurity threats within the context of a specific business risk. In order to drive effective communication, security leaders must speak the language of business risk.

To accomplish this, security leaders must be armed with business metrics that speak to how cyber risk can directly impact a business' value proposition. They should work to identify the potential cost of a business-impacting cyberattack to the organization's critical OT assets and express how this can affect revenue over time.

From there, they can illustrate how an attack on a business-critical device, such as a robot controller on a production line, can directly affect the efficacy of the organization's ability to deliver on its value proposition for customers.

Lastly, security leaders should show how other industrial organizations have been impacted, both monetarily and reputationally, and present recommendations for investments and processes their own organization can implement to strengthen security posture.

Focus on risk-based security

Once a mutual understanding and strategy is established among leadership, security leaders can demonstrate their alignment with business objectives by providing regular, risk-based insights into the organization's security posture.

Most of the time, a long-winded explanation of what the security team has done to remediate each and every vulnerability is neither realistic nor effective to resonate with business leadership. To fully communicate the true value-add that cybersecurity programs bring, security leaders should explain how their teams are assessing and reducing risk to the business' most critical assets.

For example, communicating the risk posed if a business-critical asset were to be taken offline due to a known vulnerability compared to the resource investment of remediating the vulnerability. These business-aligned

security metrics effectively communicate cybersecurity's role in overall business risk.

The study notes that business-aligned security leaders are eight times more likely to be highly confident in their ability to report on their organizations' level of security or risk. Plus, 85% of them have metrics to track cybersecurity ROI and impact on business performance versus just 25% of their siloed peers.

Taking a risk-based, business-aligned approach to cybersecurity can help industrial organizations evolve from "check-the-box" operations to a fortified, strategic cybersecurity program. With most industrial organizations operating mission-critical systems, there isn't room for poor security posture.

The global economy relies on critical infrastructure; locking arms between business and security leadership to proactively

address high-risk vulnerabilities can mean saving lives. With the right combination of technology, people and processes, industrial organizations can continue 24/7 with enhanced confidence in their ability to face the cyber threats of tomorrow. **EP&T**

*This article was submitted by **Tenable Inc.** a cybersecurity company based in Columbia, Maryland and creator of the vulnerability scanning software Nessus. www.tenable.com*

THINK
DESIGN SOLUTIONS

6 Volt 3 Volt

Compact Multi-Purpose Coin Cell Power Packs

Designers & Manufacturers of Electronic Components and Hardware

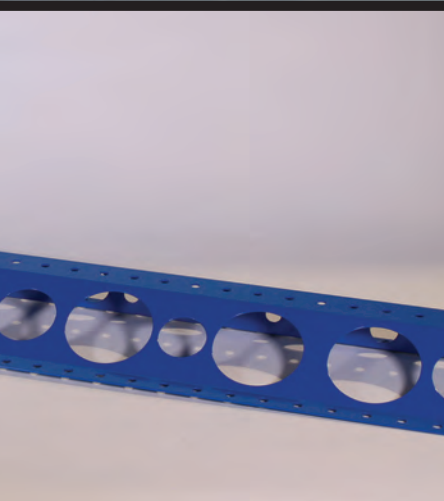
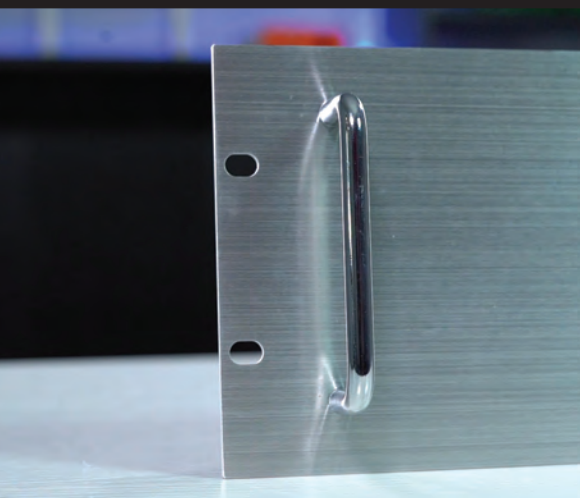
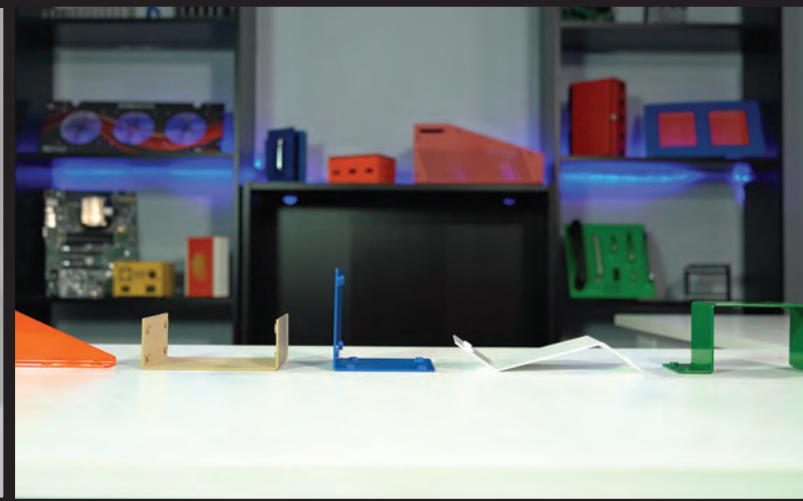
- Built-in on/off toggle switch for multi-purpose applications (safety, battery life extension, switchable power)
- Accepts all 2032 Coin Cells
- Available in Single (3 Volt) or Dual (6 Volt) battery configurations
- Polarized to prevent improper battery installation
- Designed for high shock and vibration applications
- Self-locking cover secures batteries within holder with retaining screws
- Supplied with 6" wire leads

IT'S WHAT'S ON THE INSIDE THAT COUNTS
KEYSTONE
ELECTRONICS CORP.

View our Dynamic Catalog M70 at www.keyelco.com
(516) 328-7500 [f](#) [t](#) [v](#) [in](#) [+](#) [b](#) (800) 221-5510

EMX EMX Enterprises Ltd Vancouver • Toronto • Montreal
Web: www.emx.ca • e-mail: sales@emx.ca

Design Custom Enclosures, Parts & Panels Yourself?

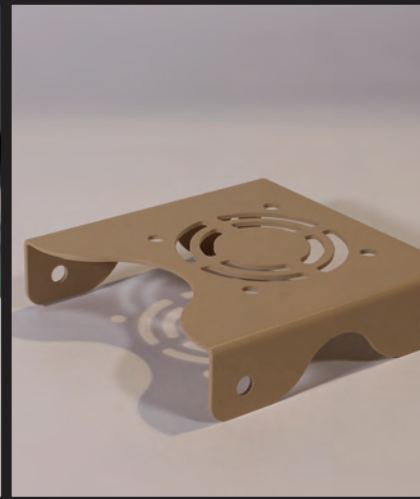


- Use Protocase Designer to design custom enclosures, parts and panels
- All template based, no mechanical engineering help needed
- Design for free, quote instantly

Made in Canada

1-866-849-3911

It's Easier With Protocase Designer



- Your design built and fully finished in 2-3 days
- No minimum order requirements - order just one if that's all you need
- 16,000 customers worldwide

protocase.com



Development testing for safety and security

Data breaches are costing Canadian businesses more than ever. **BY RAY BOISVERT**



COVID-19 has necessitated much of the global workforce to transition to a work-from-home model. This has forced organizational resources to access sensitive data via new remote pathways hastily built in early days of the pandemic crisis; yet, many remain captive of their legacy systems in lieu of a more ideal state of cloud-based business workloads.

As a result, there are more opportunities for critical security incidents especially if companies don't ensure the right tools and policies are in place.

During a time when businesses are expanding their digital footprint at an accelerated pace, while also battling a continuing talent shortage in the security industry, staff can be overwhelmed from securing more devices, systems and data than ever before.

Additionally, a recent IBM study found that more than half of surveyed employees new to working from home have not been provided with updated guidelines on how to handle customers' personally identifiable information. In fact, this gap in preparation has triggered 80% of data breaches which have been determined to be costliest breaches of all.

In the midst of these challenges, it is important for business leaders to understand the risks and costs they might face if customer or other sensitive data is exposed. IBM Security's just released Cost of a Data Breach report, conducted by the Ponemon Institute, sheds light on the financial damages that occur in the aftermath of a data breach.

According to the report, 70% of businesses that adopted remote working protocols due to the pandemic have indicated they expect future breach costs



to rise during this 'new normal'.

Based on an in-depth analysis of 500+ real world data breaches, the report found that these incidents cost companies \$3.86 million (USD) per breach on average, globally – and compromised employee accounts were the most expensive root cause. The average total cost of a data breach in Canada is \$6.35-million (CAD), an increase of 6.7% from 2019.

Other Canadian statistics from the report are:

- \$269 was the cost per lost or stolen record in the 2020 study, an increase of 7.2% from 2019.
- 42% of data breaches were caused by malicious attacks.
- The average time to identify a data breach decreased from 176 to 168 days.
- The average time to contain a data breach also decreased from 65 to 58 days.

Additional global findings include:

Smart Tech Slashes Breach Costs in Half: Companies studied who had fully deployed security automation technologies,

which leverage AI, analytics and automated orchestration to identify and respond to security events, experienced less than half the data breach costs compared to those who didn't have these tools deployed – \$2.45 million versus \$6.03 million on average.

Paying a Premium for Compromised Credentials:

In incidents where attackers accessed corporate networks through the use of stolen or compromised credentials, respondents saw nearly \$1 million higher data breach costs compared to the global average – reaching \$4.77 million per data breach. Exploiting third-party vulnerabilities was the second costliest root cause of malicious breaches (\$4.5 million) for this group.

Mega Breach Costs Soar by the Millions:

Breaches wherein more than 50 million records were compromised saw costs jump to \$392 million from \$388 million the previous year. Breaches where 40 to 50 million records were exposed cost studied companies \$364 million on average, a cost increase of \$19 million compared to the 2019 report.

Attackers Are Leveraging Employee Credentials and Misconfigured Clouds: The study also found that stolen or compromised credentials and cloud misconfigurations were the most common causes of a malicious breach for companies, representing nearly 40% of malicious incidents. Companies need to rethink their security strategy and reconsider how they authenticate users and the extent of access users are granted – especially now when so much of the workforce is working beyond traditional network parameters.

Advanced Security Technologies Can Save Companies Millions:

What can companies do to help minimize the impact of a breach? One major finding the study found was a growing divide in breach costs between businesses implementing advanced security technologies and those lagging behind. In fact, there's a cost-saving difference of \$3.58 million in the report for companies studied in the report with fully deployed security automation versus those that have yet to deploy this type of technology.

Security automation can also lead to a significantly shorter response time to breaches, which is a key factor shown to reduce breach costs – AI, machine learning, analytics and other forms of security automation enabled companies to respond to breaches an average of over 27% faster.

Without any advanced security tools in place, it can take an average of 74 additional days to identify and contain a breach. When longer breach cycles can surmount to millions of dollars more in costs to organizations, fully deployed security automation can slash costs by more than half, leading to a much quicker – and cheaper – breach response.

You can check out more detailed findings on this topic by downloading the full report at www.ibm.com/security/digital-assets/cost-data-breach-report/#/. **EP&T**



Ray Boisvert is associate partner at IBM Canada Security Services.

www.ibm.com/security/services



CONNECT

When technology and expertise come together

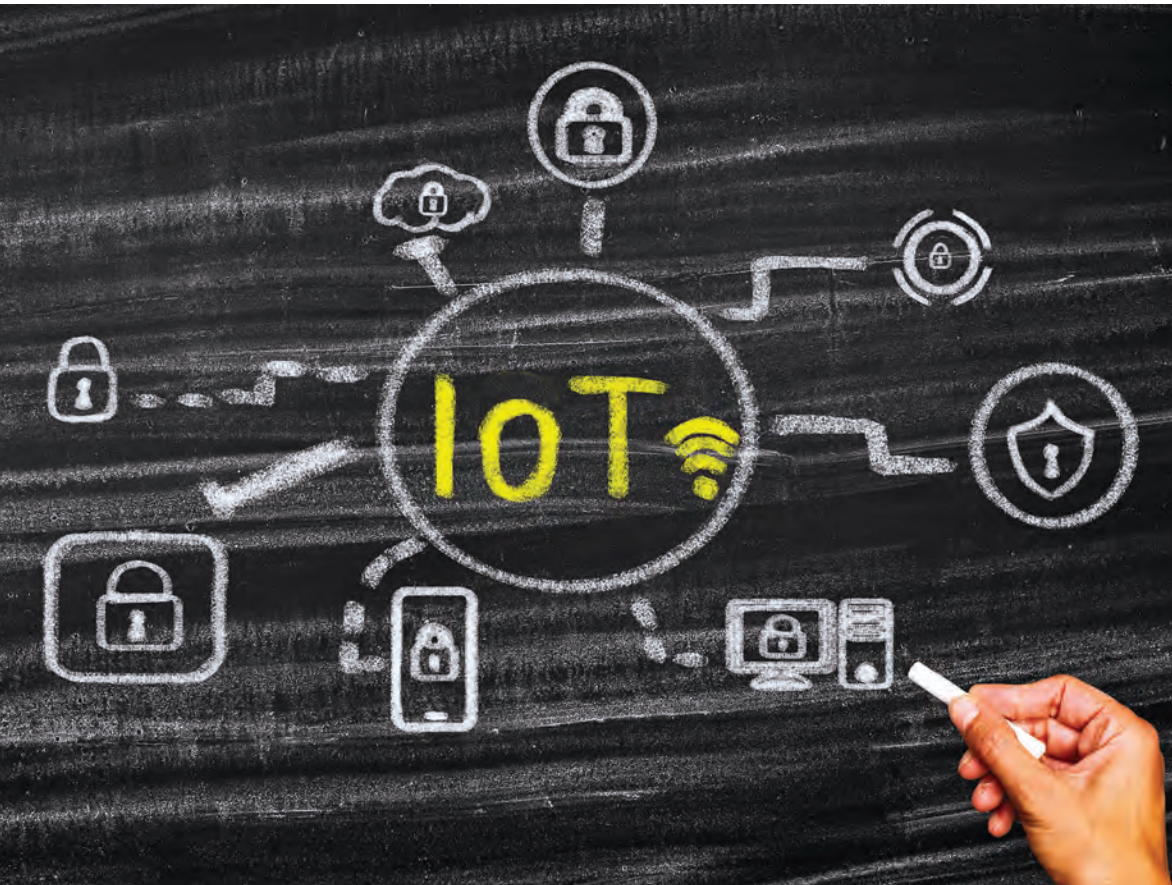
Phoenix Contact's expertise spans a wide range of applications so that you can make power, control, and network connections with absolute confidence. Single Pair Ethernet is the new standard (IEC 63171-5) shaping the future design of communication devices for industrial environments. With high-speed data transmission and up to 60 watts of power (PoDL), this new 2-wire technology increases density for connection points. From IP20 to IP6x solutions, you can trust Phoenix Contact for consistent quality, reliability, and high performance – every time.



www.phoenixcontact.ca/SPE



**PHOENIX
CONTACT**
INSPIRING INNOVATIONS



Best practices for protecting IoT devices

More effective security solutions for corporate IP at the Edge. **BY PHILIP ATTFIELD, CEO, SEQUITUR LABS**

➔ Over the last several years, humanity has seen significant technological innovation across nearly every business sector, including retail, manufacturing, consumer products, healthcare and more.

The adoption and integration of digital technologies into products at every level has become pervasive, with interconnectivity speeding the rise of IoT (Internet of Things). Practically every modern device we use today is now connected, allowing greater automation, control and analytics-based insights. The growth of this new area in device and computing interconnectivity is not only calling for better network and internet infrastructure, but also stronger and more effective security solutions.

The primary object of attention and

protection is the intellectual property in the form of Trusted Applications (TAs) that include artificial intelligence (AI) and machine learning (ML) algorithms at the edge. While the communication and management of devices from a single place has become possible, this has made it possible for IoT device vulnerabilities to be exploited – causing enormous damages to businesses worldwide as these TAs are stolen.

To confront this challenge, security-enabled IoT platforms are leading the way to counter this threat, providing the means to securely interface with and control a wide range of sensitive connected devices and systems such as home/business video camera and alarm systems, healthcare devices, as well as industrial systems that require secure supervisory control

and data acquisition (SCADA) environments such as utility switching and operations.

Many IoT products incorporate artificial intelligence (AI) or machine learning (ML) to conduct complicated tasks that require some level of intelligent functionality with access to sensitive code or data sets, allowing some level of decision making without pre-orchestrated programming.

The algorithms and models that deliver this functionality represent critical intellectual property (IP), and create significant value for the products and their vendors. While there are a vast number of potential IoT security threats designed by hackers for any number of reasons, not the least of which is financial gain, manufacturers and integrators remain focused on their search for best in class security strategies and products for locking down their products as these algorithms and models simply cannot be compromised. Such theft of the organization's intellectual property can create long-term damage to a company's revenue and brand and must be protected.

IoT security attacks

There are countless examples of IoT security attacks and their impacts on some of the most well-known brands in the world. In a case that occurred in March of 2020, criminal hackers cracked the Xbox Series X graphics code and AMD's future computer GPU's data and leaked the information on the Internet.

According to one report, "AMD has been having a particularly rough few months, apparently. The chip designer revealed that a hacker stole test files for a "subset" of current and upcoming graphics hardware, some of which had been posted online before they were taken down. While AMD was shy on details, the claimed intruder told TorrentFreak that the material included source code for Navi 10 (think Radeon RX 5700 series), the future Navi 21 and the Arden GPU inside the Xbox Series X."

A best practice for securing system applications is to move these trusted applications and housing them in a secure area with restricted access. One example involves using ARM TrustZone architecture, where a system-on-chip's (SOC) memory can be partitioned into a rich (non-secure) environment and a secure environment. The rich environment is larger in memory size—typically hundreds

ARM TrustZone

architecture is one option for a secure environment

“Major factors driving the growth of the IoT security market are the increasing number of ransomware attacks on the IoT devices across the globe, growing IoT security regulations and rising security concerns over critical infrastructures”

of Megabytes—and houses known (public) software, such as Linux kernels and open source supporting applications (e.g., OpenSSL). The secure environment has a small memory size—less than a Megabyte—and houses a Trusted Execution Environment (TEE) secure operating system. Applications that need to be protected are included here along with applications that support the securing process (e.g., key / certificate management and secure data storage). These are known as Trusted Applications (or TAs).

In such an architecture, the secure application process works

by allowing the IoT device’s application, running in the rich (non-secure) environment, to make a request to the Linux kernel to access the secure environment. The Linux kernel is suspended on one of the SoC’s cores, giving access to the TEE; The TEE then resumes from suspension and invokes the requested TA. The TEE then accesses the non-secure memory (RAM) and acquires data through the shared memory between the two environments. A layer of trusted applications can also reinforce security to further harden the environment, including:

- Cryptographic Trusted Applications: The deployment encryption and hashing algorithms
 - Certificate Management for Trusted Applications: for managing credentials
 - Secure Storage Trusted Applications: for storing critical data in the Secure Environment
 - TLS Trusted Applications: secure sockets for communication with external servers
- “Major factors driving the growth of the IoT security market are the increasing number of ransomware attacks on IoT devices across the globe, growing IoT security regulations, and rising security concerns over critical infrastructures,” noted analysts at Research and Markets in a recent report titled Global Internet of Things (IoT) Security Market Forecast to Grow to USD 36.6 Billion by 2025. “New variants of IoT threats, lack of awareness, costly

IoT security solutions, and budget constraints may limit the market growth.”

While the industry is becoming increasingly burdened by the growing number of threats, manufacturers and integrators are aware and incorporating next generation security into their products and solutions. This is the right move as it both enhances security and speeds time to market. These solutions bring IP protection to the edge while streamlining the design of manufacturing processes for a new era of solutions and devices that are connected and secure. **EP&T**

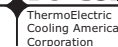


Philip Attfield is CEO of Sequitur Labs Inc. He brings a strong background in computing, networking, security and systems modeling. Attfield has more than 20-years of industry experience in large enterprises and small entrepreneurial firms. www.sequiturlabs.com



Choose thermoelectric technology for low maintenance.

Choose **teca**® for reliable quality.



**Control Cabinet
Cooling Solutions**

www.thermoelectric.com
773.342.4900
Call us today **MADE IN USA**
TECA offers safety-certified (UL/CSA & CE-mark) products.

How to secure tomorrow's connected industrial systems

BY ALAN GRAU, VP OF IOT/EMBEDDED SOLUTIONS, SECTIGO

There is a lot of chatter and concern about how to protect our smart homes and cities, our cars and planes, in short, all of our connected and IoT devices and systems against cyberattacks. The best way to protect these application spaces is by building security into the devices, starting at the factories and the assembly plants where these devices and sensors are developed and made.

Manufacturers of control systems for industrial systems have long been aware of the need to address safety in their designs, but the focus on security has often lagged. However, by ignoring security, safety is compromised.

Developers designing connected industrial systems and IoT devices face a host of challenges in addition to security. Which of the emerging IoT standards should they embrace? Which IoT protocols should be used? How can they distinguish their IoT and IIoT products in this competitive emerging field? How can they meet time-to-market challenges?

As a result of these basic connectivity and design challenges, and a lack of clear standards for cybersecurity, building security into the device is often just an afterthought. However, security need not be an overwhelming challenge. By including a few basic security capabilities, manufacturers can develop connected machines with essential security protections while establishing a strong security foundation on which additional security features can be added in the future.

VULNERABILITIES IN EMBEDDED DEVICES

Developers need to understand the basic types of security vulnerabilities, especially as they relate to embedded devices. Most vulnerabilities in embedded devices can be divided into one of three categories:

- implementation vulnerabilities



Implementation Vulnerability	Design Vulnerability	Deployment Vulnerability
<ul style="list-style-type: none"> • Buffer overflow • Improperly initialized random number generator 	<ul style="list-style-type: none"> • Storing or sending passwords in clear text • No secure boot 	<ul style="list-style-type: none"> • Using default password • Reusing password on multiple devices

Security vulnerabilities can result from implementation flaws, design flaws or failure to properly enable and use security features.

- design vulnerabilities
- deployment vulnerabilities

Deployment vulnerabilities pertain to issues introduced by the end user during the installation and operation of the device. These include not enabling security features, not changing default passwords, using weak passwords, and other similar errors. Unfortunately, for many connected devices, it is difficult for end-users to implement effective security solutions.

Implementation vulnerabilities occur when coding errors result in a weakness that can be exploited during a cyberattack. Buffer overflow attacks are a classic example of implementation vulnerabilities. Another common error is improperly seeding random number generators, resulting in security keys that are easy to guess.

3
The number of categories for vulnerabilities in embedded devices.

Adherence to software development processes, such as the OWASP Secure Software Development Lifecycle, or Microsoft's Security Development Lifecycle, along with thorough testing processes, help to address implementation vulnerabilities.

Design vulnerabilities are weaknesses that result from a failure to include proper security measures when developing the device. Examples of design vulnerabilities include use of hard-coded passwords, control interfaces with no user authentication, and use of communication protocols that send passwords and other sensitive information in the clear. Other less-glamorous examples include devices without secure boot, which allow unauthenticated remote firmware updates, or that include "back doors" intended to allow remote access for debugging and maintenance of the device.

FOUR ESSENTIAL COMPONENTS OF A SECURE CONNECTED DEVICE

Secure Boot

Secure boot utilizes cryptographic code signing techniques to ensure the device only executes code that was produced by the device OEM or other trusted party. In a device with secure boot capability, the bootloader computes a cryptographically secure hash on the firmware image prior to loading the image. This hash value is compared with a stored hash value to ensure the image is authentic. Cryptographic signing of the stored hash value prevents malicious third parties from spoofing the software load, ensuring that only software from the OEM is allowed to execute.

Secure Firmware Update

Secure firmware updates ensure that device firmware can be updated, but only with firmware from the device OEM or other trusted party. Like secure boot, cryptographically secure hash validation is used to verify the firmware before it is stored on the device. In addition, machine-to-machine authentication methods can be used by the IoT device to authenticate the upgrade server before downloading the new firmware image, thereby adding another layer of protection.

Secure Communication

IoT devices, by definition, support communication with other devices. The communication mechanisms will vary by device but may include

wireless protocols ranging from BLE and ZigBee to WiFi, cellular data, as well as Ethernet. Regardless of the transport mechanism and communication protocol, it is important to ensure that all communication is secured. Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) should be used when possible. For common wireless protocols, such as ZigBee or BLE, which have encryption built into the protocol, but that have known encryption vulnerabilities, encrypting at the application layer provide additional protections.

Data Protection

Engineers should consider encrypting any sensitive data stored on the device. Many large data breaches have resulted from data recovered from stolen or discarded equipment. Security protocols provide protection for data while it is being transmitted across networks but do not normally protect the data while it is

stored on the device.

Implementing Security for Sensor Networks

Implementing security in industrial networks presents some additional unique challenges. Many connected sensors are low-cost devices designed with the bare minimum resources required for the core device operation and do not have additional computing power to implement sophisticated cybersecurity solutions.

As these devices are often deployed 'in the field,' they may also be subject to physical and proximity-based attacks. Hackers can physically access the device, then attempt to attack it using available communication ports. Hackers can also physically acquire (buy or steal) a similar device, take it to their labs, and then tear it down or monitor communication buses looking for vulnerabilities. Proximity-based attacks target wireless protocols but require the attacker to be within the range of

the wireless protocol.

One alternative is to bite the bullet and utilize hardware platforms capability of supporting core security services in the sensor itself. While this will increase the cost of building the device, sacrificing security to save a few dollars is often a short-sited tradeoff.

In addition to securing sensor devices, manufacturers and suppliers must address the security of the overall network or factory. IoT sensors often communicate with a gateway or edge device that performs data collection or analysis. The gateway or edge device must provide high levels of security, both for itself and to provide protection for the sensors from which it collects data.

Summary

Security is a requirement for all connected machines and devices and must be prioritized during the initial development process, regardless of how small or seemingly insignificant the device or

the data it captures. By adding a few basic capabilities, including secure boot, secure firmware update, secure communication, data protection, and user authentication, the security of any device can be significantly increased.

A comprehensive security analysis will identify attack vectors and define security requirements. Engineers can then use this information to prioritize development of security features.

Only by including security into the devices themselves can we ensure that connected machines and IoT devices will be protected from cyberattacks. **EP&T**



Alan Grau has 30 years of experience in telecommunications and the embedded software marketplace. Grau

is VP of IoT/Embedded Solutions at Sectigo, a commercial certificate authority and provider of purpose-built, automated PKI solutions. www.sectigo.com

Working with Surtek Industries Inc. is like having your very own production facilities - without the overhead, staffing or production headaches. Our state-of-the-art facility has enabled us to gain recognition as a leader and innovator within the contract manufacturing industry.

If your project isn't ready for production yet, or if you require assistance at the design stages, we can assist you in achieving cost effective solutions.

We've got the technical expertise to help you solve complex assembly issues. Our supervisory staff and assemblers boast many years of experience in all aspects of assembly.

For our clients, that breadth of available resources translates into a superior level of quality, workmanship and reliability that is a cornerstone for the contract manufacturing industry.

**Address: #4-13018 84th Avenue
Surrey, BC V3W 1 L2
Canada
www.surtek.net**

Tel: 1.604.590.2235

Fax: 1.604.590.5852

E-mail: sales@surtek.net

ISO 9001:2015

Certified Registered Management System



IOT STARTER KIT BASED ON OPEN HARDWARE, PLUG & PLAY CONNECTIONS

ARDUINO

Explore IoT Kit is a gateway to the digital world of connected objects and people and helps students get started with the fundamental concepts of the Internet of Things (IoT) quickly and easily, as it's based on open hardware and plug-and-play connections. Kit includes 10 online activities that adopt a learning-by-doing approach, through which students acquire knowledge step-by-step by constructing fully functional solutions, including experiments, challenges, and building meaningful applications. <https://store.arduino.cc/usa/explore-iot-kit>

SILVER CONDUCTIVE SILICONE ADHESIVE MEETS NASA OUTGASSING SPECS

MASTER BOND



MasterSil 151S is an addition curing two-part silicone system that may be used as an adhesive, sealant, coating or form-in-place gasketing material.

Product's silicone chemistry passes NASA low outgassing specifications, and it retains improved electrical conductivity with a volume resistivity of 0.004 ohm-cm at 75°F. Product is suitable for low stress applications, as it is highly flexible across a wide service temperature range, and capable of resisting aggressive

thermal cycles and shocks. Product's mix ratio is 100 to 5 by weight, and it cures with the addition of heat. Upon mixing, it retains its smooth, paste consistency, and has a long working life of 6-12 hours for a 50 gram mass. www.masterbond.com

BACKSHELLS, ADAPTERS, BAND STRAPS COME IN MANY PLATINGS

TE CONNECTIVITY



Polamco BT series MIL-DTL-M38999 backshells, adapters and band straps offer a wide

selection of sizes, materials and platings to meet most application needs. The band strap termination system provides ease of installation and repair. The corrosion-resisting steel bands come in three styles to help meet shield termination needs and termination tool of user's choice. BT series backshells terminate the shield with a stainless steel band strap. Additional strain relief can be obtained with a heat shrink boot. bit.ly/3dZE2cb

ENCAPSULANT DELIVERS WARPAGE CONTROL

HENKEL

Loctite EccoBond LCM 1000AF encapsulation material leverages a



hydride-free resin platform to enable thorough protection, improved warpage control and fine gap filling for fan-in and fan-out wafer-level packages (FI WLPs, FO WLPs). REACH-compliant product has shown effective reliability-enhancing performance in internal evaluations of several wafer-level packaging configurations including FI WLPs, embedded wafer-level ball grid arrays (eWLBs), FO WLPs, and chip-on-wafer (CoW) encapsulation. Solvent-free encapsulant integrates fine particle fillers (average 3µm, upper cut 10µm), enabling high-yield, ultra-low warpage, improved flow properties.

www.henkel-adhesives.com/ca

RUGGED CIRCULAR LOCKING CONNECTORS DELIVER RELIABLE POWER

HEILIND ELECTRONICS



Amphenol ICC MRD series rugged circular locking

connectors provide reliable power or signal connections in harsh industrial, instrumentation and medical applications. The sealed devices provide IP67 protection against water and dust ingress and are rated for up to 10A and 500V to support high-power applications. Products come in 2, 3 and 4 position form factors to support design flexibility. www.heilind.com

HIGH-FREQUENCY MULTILAYER CERAMIC INDUCTORS SAVE SPACE

WÜRTH ELEKTRONIK

WE-MK range of SMT multilayer ceramic inductors with high self-resonant frequency (up to f_{RES} > 10GHz). WE-MK is available in three different sizes—0201, 0402 and 0603—as well as various inductance values from 1nH up to 470nH. Devices have very stable inductance over the entire operating temperature range from -55 to +125°C with inductance tolerances of ±5% or ±0.3 nH (depending on inductance value,



PUBLISHER'S PICK

AEC-Q200 CERTIFIED COMPACT DUAL INDUCTORS

TDK's extended range of EPCOS dual inductors cover an inductance range of 2 x 3.9 µH to 2 x 47 µH with maximum rated currents from 2.83 A to 7.05 A. These magnetically shielded AEC-Q200 certified inductors have low dimensions of only 12.5 x 12.5 x 10.5mm³ and high saturation currents up to 16.1 A.



Link for product info: www.tdk-electronics.tdk.com/en/529796/products/product-catalog/inductors-coils-/smt-power-inductors-epcos-



TDK Electronics Inc.

732-906-4300
www.tdk-electronics.tdk.com

higher inductance values are percentage based).

www.we-online.com

PIEZO ELECTRIC SWITCH COMES PRE-ASSEMBLED WITH CABLE

SCHURTER

PSE Piezo electric switch is installation-ready with its pre-assembled 15-meter-long cable. The potted polyurethane cable provides installation flexibility with high level IP67 protection according to IEC 60529 and IP69K according to DIN 40050-9. Device is waterproof from the switch surface to its electrical connections. The housing is made of 1.4462 stainless steel, resistant to corrosion and essential when used in areas with high humidity. Product provides a long lifetime of 20-million actuations, customary to the technology known for its robust performance.



www.schurter.com

**SIGNAL CONDITIONER
MODULE PROTECTS
NUCLEAR PLANTS**

ALLIANCE SENSOR GROUP



Model S2A DIN-rail mounting LVDT signal conditioner modules are microprocessor-based electronic smart modules used to protect power plants, especially

nuclear power utilities, against any potential vulnerabilities to any kind of cyber-attack. These inductive position sensors utilize specialized electronics known as signal conditioners for operation and to produce the required signals for the control system. Module's features include cybersecurity protection, system diagnostics, high module reliability, and real-time system recalibration capability. Colour coded plug-in screw terminal blocks facilitate pre-wiring a control system cabinet.

➤ alliancesensors.com

**WI-FI 32-BIT MCU
MODULE DELIVERS
ADVANCED PERIPHERAL
OPTIONS**

MICROCHIP TECHNOLOGY



WiFi32E01PC Wi-Fi microcontroller (MCU) module is a Trust&GO secured platform-enabled Wi-Fi MCU module that is pre-provisioned for cloud platforms. Designed with verifiable identity, the highly integrated device is compliant to Wi-Fi Alliance (WFA) specification and fully certified with the following world regulatory agencies: Federal Communications Commission (FCC), Industry Canada (IC) and European Radio Equipment Directive (RED). The Trust&GO platform inside the device streamlines the process of network authentication.

➤ www.microchip.com

**FPGAS SUPPORT
EXTENDED
TEMPERATURE RANGE
FOR RUGGED DESIGNS**

LATTICE SEMICONDUCTOR

MachXO3LF FPGAs are suitable for flexible deployment of robust automotive control applications and MachXO3D FPGAs for system security that support extended temperature operating ranges for automotive and other ruggedized applications. MachXO3D FPGAs



augment the popular system control capabilities of the MachXO FPGA architecture with

industry-leading security features, including hardware Root-of-Trust (RoT), platform firmware resilience (PFR), and secure dual-boot support. Both devices target control, bridging, and I/O expansion applications that must operate reliably in rugged environments.

➤ www.latticesemi.com/MachXO3

**MICROCONTROLLERS
DELIVER COMPLETE
IOT LIFECYCLE
MANAGEMENT**

INFINEON TECHNOLOGIES

Highly integrated IoT lifecycle management solution combines PSoC 64 Secure Microcontrollers with Trusted Firmware-M embedded security, the Arm Mbed IoT OS, and the Arm Pelion IoT platform to securely design, manage, and update IoT products without the need for custom security firmware. The Pelion-Ready and Mbed OS-Enabled solution demonstrates industry best practices for security, by reaching PSA Certified Level 1. Open-source software delivers configurable components that enable PSA Functional APIs and create a 'Secure Processing Environment'.



➤ www.infineon.com

Visit ept.ca for the latest new products, news and industry events.

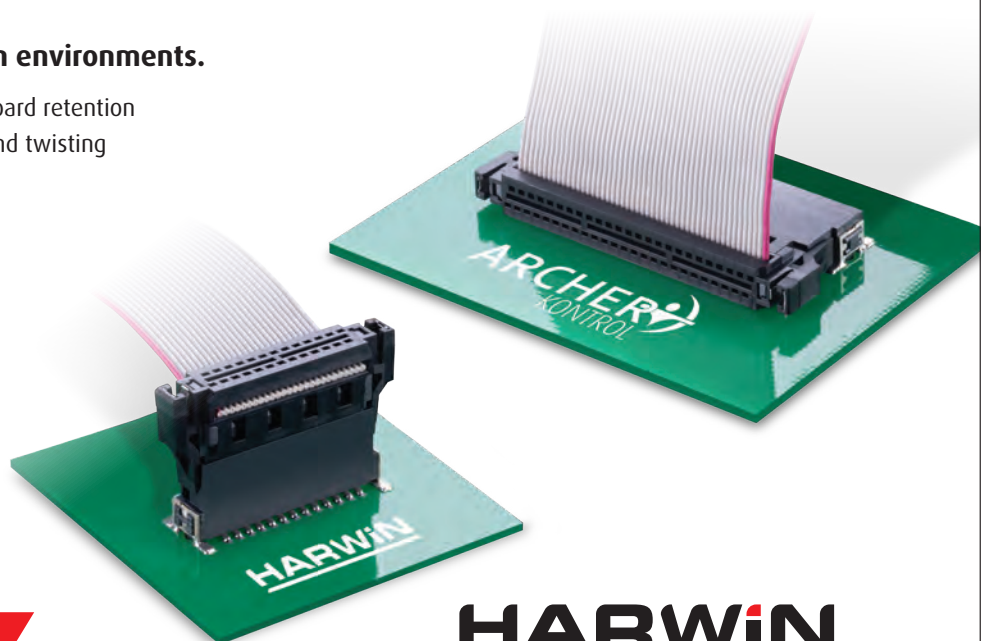
**Increased Performance
for Connected Hardware**

Designed to perform in high vibration environments.

With surface mount solder tabs for additional board retention strength, Archer Kontrol can withstand lateral and twisting forces in high vibration environments.

Ensuring reliability in the next generation of connected devices.

- Temperature range of -55°C to +125°C
- Assists with blind mating
- Fully shrouded connector system
- Tested to perform up to 500 operations
- Up to 3 Gbit/s data rate



**ARCHER
KONTROL**

harwin.com/archer-kontrol

HARWIN
Connect with confidence



Source: AMD EPYC Processors

ACQUISITIONS

AMD TO ACQUIRE XILINX

AMD entered into a definitive agreement to acquire Xilinx in an all-stock transaction valued at \$35 billion. The combination will create the semiconductor industry's leading high performance computing company, significantly expanding the breadth of AMD's product portfolio and customer set across diverse growth markets where Xilinx is an established leader.

The acquisition brings together two industry leaders with complementary product portfolios and customers. AMD will offer the industry's strongest portfolio of high performance processor technologies, combining CPUs, GPUs, FPGAs, Adaptive SoCs and deep software expertise to enable leadership computing platforms for cloud, edge and end devices. Together, the combined company will capitalize on opportunities spanning some of the industry's most important growth segments from the data center to gaming, PCs, communications, automotive, industrial, aerospace and defense.

"By combining our world-class engineering teams and deep domain

expertise, we will create an industry leader with the vision, talent and scale to define the future of high performance computing," says AMD president and CEO Dr. Lisa Su.

INTEL TO SELL NAND BUSINESS TO RIVAL

Intel has agreed to a \$9-billion deal to sell most of its memory business to South Korea's SK Hynix as it moves toward more diverse technologies while shedding a major Chinese factory at a time of deepening trade friction between Washington and Beijing.

Intel said it will keep its "Optane" business of more advanced memory products, which analysts say are mostly produced in the United States.



SK Hynix will acquire Intel's NAND memory chip and storage biz, including a related fab in China.

According to the plan, SK Hynix will acquire Intel's NAND memory chip and storage business, including a related manufacturing site in the northeastern

Chinese city of Dalian. SK Hynix said the companies expect to get required governmental approvals for the deal by late 2021. The transaction could reportedly make SK Hynix the world's second-largest provider of NAND flash memory chips behind Samsung Electronics, another South Korean chip giant.

Demand for flash memory has strengthened in recent months due to buying of personal computers and servers as the coronavirus pandemic forces millions to work from home.

HENKEL ADDS ADVANCED MATERIALS START-UP ACTNANO

Henkel Adhesive Technologies has co-invested in actnano, a Boston-based advanced materials start-up that provides a tailored conformal coatings technology for the protection of printed circuit boards (pcbs) in a variety of applications in growing electronics segments.

Founded in 2012, actnano has developed a commercialized technology for gel-based coatings with comprehensive waterproofing and environmental resistant properties. The materials are designed to provide superior protection to printed circuit boards including connectors, antennas, LED's and all mounted components and provide benefits in a broad variety of fast-growing automotive electronics and consumer electronics applications. The liquid applied coatings offer a drop-in solution for existing coating lines and enable customers to increase throughputs and to significantly reduce the production costs per device.

The actnano technology is hydrophobic, electrically insulating and allows electrical connection through the coating. Together with Henkel the start-up aims to further optimize waterproofing properties for tailored solutions in target markets.



Visit ept.ca for the latest new products, news and industry events.



ANNUAL ELECTROSOURCE DIRECTORY

Coming in **EP&T** February 2021

Make sure **your** business is included in Canada's electronics manufacturing supplier directory.

Check your listing in the digital edition at **EPT.ca** and ask your account manager how to ensure your business stands out!

Contact:

Joanna Malivoire | jmalivoire@ept.ca | 866-868-7089
Jason Bauer | jbauer@ept.ca | 416-510-6797

PRODUCT SOURCE GUIDE



A brilliant display of metal switches

- Electro-mechanical IP65, IK07
- Capacitive IP67, IK09
- Piezo IP69K, IK02

Diameters 16-30 mm
Illumination single or RGB 5-28 VDC
Lifetime 1.5, 5 or 20 million actuations

SCHURTER
ELECTRONIC COMPONENTS

BlockMaster's Medium Power Distribution Blocks

2 or 3 Poles / 50 Amps / 300 Volts

Termination: Screw Clamps, .250" Q.C., Ring/Spade



www.BLOCKMASTER.com
847-956-1680

Flat Pack Laser
Low Profile; Easy Mounting; Alignment Laser
Laser Head Rotates and Tilts for Exact Alignment



New Product

The "FLAT PACK" Laser from BEA Lasers
1.93" (L) x 1.26" (W) x 0.88" (H)
Aluminum Housing
Red or Green; Dot or Line Pattern
Power Supply Included

BEA LASERS

(847) 238-1420
www.bealasers.com

Are Your Cords Lost at Sea?

Why lose your cords overseas to quarantines and restrictions? Interpower® cords come with Value-Added options such as labeling and packaging—and ship FAST!




interpower
www.interpower.com

Visit our virtual trade show booth at
www.interpowertradeshow.com

UPGRADE YOUR KNOWLEDGE

Learn about **THERMAL DESIGN CONSIDERATIONS** in our latest ebook and streamline your PCB design process by preventing thermal issues before they happen.



Get the e-book:
go.ema-eda.com/LearnThermal

OrCAD COURTESY FOR PROGRESS

EMA Design Automation

UV CURING ADHESIVE with High T_g



UV26 Adhesive System

MASTERBOND
ADHESIVES | SEALANTS | COATINGS

+1.201.343.8983 • main@masterbond.com

POWER SUPPLIES

RUGGED INDUSTRIAL QUALITY

AC-DC Power Supplies
DC-DC Converters
DC-AC Inverters
Custom




ABSOPULSE
ELECTRONICS LTD. Tel: +1-613-836-3511

www.absopulse.com

Fast, Precise, and Cost Effective Fully Automatic Crimping Machine

The CrimpCenter 64 SP processes wires from 0.13 to 6 mm² and features all the latest quality assurance options, such as SmartDetect, WireCam and Guided Feasibility Study. These features, along with a number of performance enhancements, qualify the CrimpCenter 64 SP as a first-class machine for complex, high-precision production with high quality requirements.



Schleuniger

schleuniger.com | 905.827.1166

PANEL MOUNT BEEPERS & BUZZERS



High Audio Output!

In Stock! Competitive Prices! Free Samples!
IP65 RoHS High Audio / Lighted Output!
Listen to Our Product Selection Online!

(847) 956-1920
www.TUSAINC.com

AD INDEX

Absopulse Electronics	29
BEA Lasers	29
BlockMaster	29
Coilcraft	3
DB Lectro	8
Digi Key Corp.	FC & IFC
EMX Ent. Ltd.	13
Hammond Mfg.	31
Harwin	23
Interpower Corp.	5 & 29
Master Bond Inc.	29
Mouser Electronics	OBC
Phoenix Contact Ltd	17

Protocase	14-15
Schleuniger, Inc.	29
Schurter, Inc.	29
TDK Electric	22
TDK Lambda	9
TECA ThermoElectric Cooling	19
Transducers USA	29
TTI, Inc.	7

TO ADVERTISE in an upcoming issue of **EP&T**, contact **Scott Atkinson**, Publisher, satkinson@ept.ca or (416) 510-5207 or **Joanna Malivoire**, Account Manager, jmalivoire@ept.ca or direct 866-868-7089.

Canadian Women in Electronics Engineering

Exploring diversity through women in the Canadian electronics and industry profession



Fiona Leong is lead, procurement engineering with Clear Blue Technologies in Toronto. The firm provides smart

off-grid power technology and energy-as-a-service for cost-efficient power that can be installed anywhere, managed over the Internet, and deliver unmatched reliability and performance for use in telecom, industrial controls, street lights, security systems, emergency power and internet of things (IoT) devices.

How did you first become interested and involved in engineering?

I come from an extended family of mostly banking professionals, but I knew that I had no interest in that area from a very early age. Instead, ever since I was a young child, I have always liked math and wondered how things worked. My childhood was the start of the PC era and dial-up internet; there was this family friend that studied computer programming and he got my family our first PC. Whenever there were problems with it, he would come over and fix it, install new programs or hardware - and I would be very fascinated. When I got to high-school, I knew I wanted to study engineering and I started taking all the computer, technical shop, math and science classes, all of which I thoroughly enjoyed!



What is your message to female engineers seeking to take on leadership roles?

This one is a simple one. Don't be afraid to ask for an

opportunity and make your career goals known. Asking doesn't guarantee that you will get it, but if you don't ask and don't speak up for your own best interest, then people may never know and never consider it. Also, when you've been told "no", don't interpret it as meaning "you can't" but instead, interpret it as being given more time to become an even better

leader. Like the old saying goes - 'If at first you don't succeed, try, try and try again.'

Can gender imbalance in the engineering industry be solved?

If I was asked this question in my teenage years, my answer would probably have been "depends on whether or not females are going to be interested in engineering." This is because back then, engineering wasn't a common field for women and many didn't consider it, and so there wasn't enough females to create a balance even if we tried. To put things in perspective, I remember attending an Ontario-wide robotics competition at the University of Guelph (which is now called the Roboticon Competition) during my Junior year in high school when I had a lady come up to me and ask me "Did you know that you're the only girl in this competition?". Fast forward to today, I've seen so many more young women take on STEM programs, and engineering graduates have more and more women, my answer is, definitely, it's just a matter of time.

What key words of advice do you have for employers seeking to create a supportive environment for women?

Women work hard in their studies and take pride in their career achievements just like men, if not more. I believe women want to be recognized for their skills and abilities, so it is imperative that we be evaluated and considered for opportunities based on those attributes as equivalent candidates to our male counterparts. As hard as it may be to do, employers should aim to not consider whether female employees will be able to commit to the to the job and its responsibilities because of their family responsibilities. After all, the same worries do not typically arise when men are being considered for opportunities, so why should that be the case for women? If you are ever in doubt, be frank and have an open conversation to address any

concerns. This will show female employees that the workplace does care, and it is proactively trying to support our career growth.

Industry employers and associations have set some goals to achieve when it comes to equalization of genders within engineering circles. How do you think imposed gender initiatives will help women in their field?

A I believe that the imposed gender initiatives help women by having the workplace and management mindfully address unconscious biases in roles, which may traditionally be reserved for men. For example, roles that may require certain physical strength or may be in harsh work environments may seem more suited for males even if there are female candidates with the same credentials. However, if the workplace has set a goal to have at least 30% female representation in each function, female candidates will now be less likely to be overlooked for the role.

Women who graduate from engineering programs don't seem to stay in the industry, why do you think that happens?

I think that the reason here is two-fold. First of all, there is still the situation of more men being hired into technical roles than women - so the pool of women starting off their career in engineering is already less than that of men. Thereafter, as the natural course of life happens and personal goals and priorities change, women seem to fall into the role of the primary family caregiver and this responsibility presides over their career. You compound that with the unconscious bias of women not being equally considered for certain roles, it may make a career change decision easier. **EP&T**

 For more Women in Electronics, check out ept.ca.



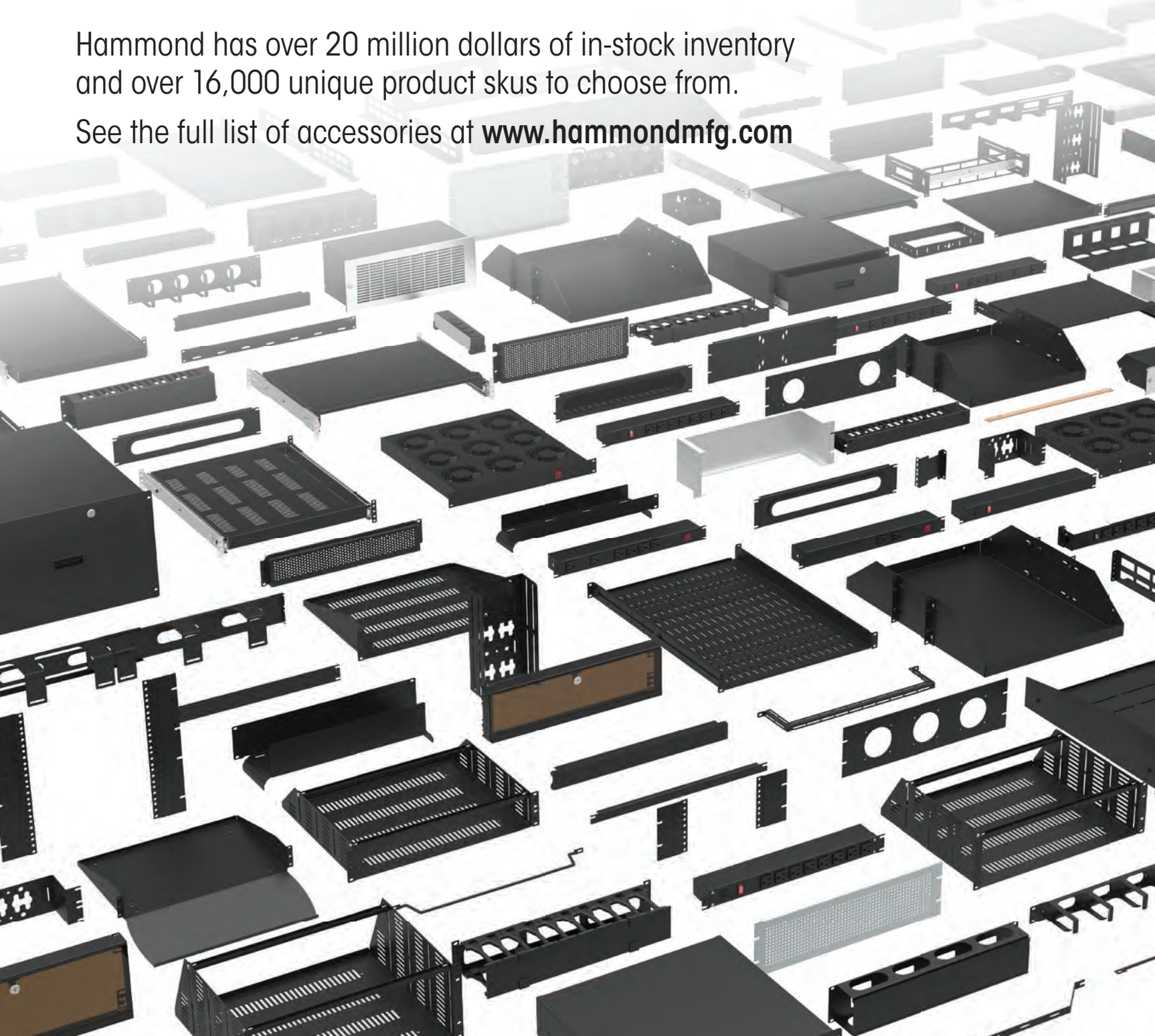
HAMMOND
MANUFACTURING®

85 MANUFACTURING
YEARS RACKS & CABINETS
SINCE 1934

THE LARGEST SELECTION OF RACK MOUNT ACCESSORIES

Hammond has over 20 million dollars of in-stock inventory and over 16,000 unique product skus to choose from.

See the full list of accessories at www.hammondmfg.com



Increase your engineering and buying confidence



Engineers and buyers find the leading brands and the widest selection of products in stock at [mouser.com](https://www.mouser.com)

