IMELCO
International Marketing Electrical Corp.

GLOBAL CIRCUIT

A PUBLICATION OF THE WORLDWIDE IMELCO NETWORK
DEDICATED TO THE MEN AND WOMEN THAT ARE SERVING THE NEEDS OF THE ELECTRICAL CONSTRUCTION PROFESSIONAL ALL OVER THE WORLD

2020 ISSUE 11

MARKETING

DIGITAL ALTERNATIVES TO FACE-TO-FACE EVENTS

OPPORTUNITIES

PROTECTED AGAINST MANIPULATION: ACTUATORS OF THEBEN

NETWORKING

OUR PROVISIONAL MEETINGS' SCHEDULES 2020 - 2021

BUSINESS

SMALL BUSINESS: THE BIGGEST OPPORTUNITY FOR CYBER CRIMES

IN THIS ISSUE

MARKETING

BUSINESS

OPPORTUNITIES

NETWORKING

Global Circuit would love to **picture your organisation in the next issue.**
If you are interested or wish to contribute to the editorial content of the Global Circuit's next issue, please contact us at **marketing@imelco-solutions.com**

PERSPECTIVES

ARE YOU READY FOR 5G?

The pace of innovation has effects on people and business, it constantly puts us in front of new challenges. As ever, these may be seen as a threat and an opportunity.

The new 5G mobile network is scheduled to become reality this year. While network operators and the governments are still in the tendering procedure, industry and mobile phone users long for the new network to be in place as soon as possible: the new standard promises a multiple of the speed that UMTS or LTE offer today.

The technology also stands for a faster connectivity what IoT is concerned, which is important for manufacturers of connected industrial systems and solutions, not to forget those producers of transmission masts, accessory equipment or driverless cars.

However, there are also some concerns in how the beamforming and a higher exposure to radiation may affect populations' health. Likewise, the overall excitement about the benefits of the new technology decreases when it comes to the topic of the cyber security: a 5G-powered world will be increasingly connected as more data will be exchanged between devices and applications. This significantly enhances the number of the entry points for potential cyberattacks.

5G: opportunity or threat?... Either way, a subject to be treated by decision-makers with due care and diligence.

E Reignier

Elena Reignier,
Managing Director, IMELCO

Electrical distributors: FUTUREPROOF YOUR BUSINESS!

In the last half-century, electrical distributors have played a vital role in the success and growth of the power industry. Through established distribution networks, brands such as Schneider Electric have been able to engage with electricians and contractors worldwide, providing solutions and services to help them meet the demands of their customers. Electrical distributors have also been able to adapt to changing industry trends to keep their business models competitive despite varying market cycles and evolving technology.

The last five years, however, have been particularly challenging. Digitization has been a game changer for all players involved – from manufacturers and distributors to electricians and end-users. In countries such as Switzerland, Netherlands, and Denmark, more than 50% of electrical distribution is now conducted online, which has forced distributors to recast their business model significantly.

Transformation drivers beyond digitization

Along with digitization, several other factors are re-shaping the landscape of the electrical distribution marketplace:

- **Market concentration.** Through mergers and acquisitions, dominant players are consolidating with an eye toward increasing market share, adding technical expertise, and/or expanding value-added service offerings.
- **Pricing transparency.** E-commerce is driving price transparency regardless of purchase channel, putting pressure on traditional distributor margins as offline and online prices converge.
- **New technologies and IoT.** Customers are looking for more sophisticated and technically complex solutions, necessitating that distributors and the electricians they serve develop new competencies.

Bottom line: distributors have had to reevaluate their business models, adding more services and solutions to strengthen their value proposition and reduce the importance of price as a choice factor.

Growing with green products

Electrical distributors are expanding their offerings with a focus on green products, reflecting a larger, cross-industry trend worldwide. Electric vehicles (EVs) are one emerging category where distributors see potential for future growth.

For example, Audi has teamed with Amazon and Electrify America to help kickstart its EV ecosystem.

When you look at what's down the road – by 2040, there will be 530 million EVs in service compared with 2.8 million in 2017, and 560 million charging points compared with 3.1 million – it's easy to understand the trend toward green products distribution.

The proliferation of solar and storage solutions in the residential market represents another promising opportunity for electrical distributors.

Many have established divisions dedicated to green solutions in order to capitalize on their potential to provide incremental growth. The first movers will have an advantage as green products become mainstream in the coming decade.

Supporting the Winners of Tomorrow

Schneider Electric recognizes the challenges distributors face in their transformation journeys

and is committed to helping them become futureproof players amid all the change. To guide and support its partners as they evolve their business model, the company offers the following recommendations:

- **Understand your customers' needs.** Identify the main pain points for your customers – electricians, panel builders, contractors, OEMs – and align your internal processes, including IT, with these needs so you can be efficient and agile in providing solutions to real problems. Invest in a robust CRM tool to gather the data you need to understand and respond to the marketplace.
- **Take an omnichannel approach.** Combine your physical and digital models to cater to different customer preferences. Apply digital marketing strategies based on data generated by your CRM to respond better to market needs and opportunities.
- **Bolster your digital presence.** Improve your digital visibility throughout the customer journey with tools such as online catalogs, configurators, quality content – photos, videos, tutorials, etc. – and, especially, apps.
- **Specialize to add value.** Create more value for your customers – and greater profits for your business – by developing new competencies in areas such as industrial automation, energy efficiency, smart homes and buildings, project management, custom logistics, training, and predictive and corrective maintenance.
- **Reinforce your core values.** Don't lose the traditional values you've always offered your customers – local service, product knowledge and availability, and your understanding of their business. Amid all the industry change, these remain as key differentiators.
- **Prepare for the future.** Get the training you need to navigate the digital transformation and provide more value to your customers.
- **Build a partner ecosystem.** Create alliances and partnerships with companies and brands that complement your offering and provide the innovation and support you'll need to succeed in the future.

To the future, together

The future is promising for those electrical distributors who are transforming their business to respond to emerging industry trends and the changing needs of their customers. And because implementing some or all of the above recommendations can be challenging, Schneider Electric is ready to support its distributor partners on every step of their journey, providing them with:

- The best solution portfolio in the industry
- Innovative and efficient technology that fulfills the demands and requirements of today's marketplace
- Programs and training that let distributors become more specialized
- Content and materials to speed the digitization of their business
- Expert technical and consultative support whenever they need it

To learn more about how Schneider Electric is forging special partnerships with distributors to enhance their productivity and futureproof their business in the digital age, visit:

schneider-electric.com/en/partners/distributors

THE DIGITAL TRADE THE SHORT-TERM ALTERNATIVE

In times of Covid-19 you have to get creative. MITEGRO thought so too and quickly set up a digital trade fair.

By postponing Light and Building, the world's leading trade fair for light and building technology, many manufacturers were confronted with the question, how to inform about new products?

Many "trade fair" visitors were faced with the challenge of simply getting information about new products from the suppliers.

Because the digital alternative should ideally also take place at the planned time of the real trade fair, time was short.

After the first positive feedback from the contacted manufacturers, great interest emerged across the board. The wholesale trade also showed lively sympathy and promised to support in marketing.

There were lot of phone calls and organization within 7 days, so 46 manufacturers finally came together. (Including a waiting list).

In form of LIVE webinars, each manufacturer now had a time window of 30 minutes for the presentation of the trade fair innovations.

A new webinar started every hour of the trade fair week. The virtual participants were muted, but were always able to ask questions, that were answered live and directly.

Many manufacturers showed high sense of creativity in their ideas for the LIVE webinars. From a product presentation with Power Point, over the use of the camera to show the new products up to the construction of the exhibition stands, to give the participant the feeling of being live at the exhibition.

The virtual trade fair visitors were also very enthusiastic. Almost 3000 participants were reached live and the feedback was consistently positive. Even today it is still possible to see all webinars, because all 46 manufacturer webinars have been recorded. And this service is accepted with high interest.

After **so much positive** feedback, the **next digital** fair is already being discussed. **We are excited** and look forward to the **creativity of the electrical industry.**

live.mitegro.de

A NEW DECADE A NEW DEVELOPMENT

The last decade has been dominated by the smartphone. It has been a dazzling trend in many aspects. The usage of the smartphone in the world has a higher adaption rate per capita than the use of toilet paper.

Furthermore, the possibilities and applications offered by the smartphone has been incredible. From a normal phone to call people it has become a multi-disciplined device. It is still possible to use it as a phone but also as a photo camera, a video camera, a scanner, a fax, a mini laptop, a games player, a navigation system, a music player, flashlight, an alarm clock, an agenda, a calculator, a compass, a dictaphone, a video conferencing device, for wireless payment and internet access device. It does not matter if one is 3 years old or 99 years of age, the smartphone is an indispensable part of many lives every second of every day.

All of this has happened in an amazingly short period of time. It's hard to believe that the iPhone was introduced only thirteen years ago.

In a recent issue of Global Circuit, we talked about the effective use of business data and artificial intelligence (AI). We may expect the same extremely rapid development from these technological newcomers. Due to the continuous improvement in power and speed of computers more powerful and intelligent algorithms will be used which will support us in business.

The reason the smartphone has been so successful is convenience. It is such a multi-disciplined device that it helps everybody with something. We don't get lost, are not bored anymore, can pay easily etc. There is a back side to this, the smartphone contains an enormous amount of data which influence our privacy and can be used to manipulate us. The creation and mining of data is and will be a part of our personal and business lives. It is necessary that there will be good constructive regulation on the mining, usage and selling of data.

Co Braber,
President IMELCO

However, experience teaches that creating international regulations is a syrupy process. The technological developments on the other hand will be lightning fast. In our industry we should define which is the convenience trigger of our customers. How can we help them by using the new technologies and use it in an ethical and productive way? Project planning, pre delivering, stock optimization, consulting and many more aspects of the business can become premium assets in the relationship with our partner-suppliers and customers.

A final note we do not need to be afraid of the new technologies. Even AI is not a danger to mankind. AI will become more and more intelligent but it will never develop a conscience or feelings so it will never get in conflict with humans. We should look at the new decade with electrification and the new technologies as yet another chance for all of us to stand out for the betterment of our industry.

IT SECURITY IN PRODUCTION PERMANENTLY HIGH SECURITY LEVEL

Due to several security breaches the topic of IT security is currently receiving a great deal of attention. Studies have documented that production has already been affected by IT security problems within a significant number of companies. Despite this, only around half of the companies questioned as part of a survey conducted by ZVEI, the German Electrical and Electronic Manufacturers' Association, had completed a risk analysis of their production sector.

A major challenge is being able to assess the risk of potential future attacks for which there are no documented incidents. There is practically no reliable information that companies could use to assess the threat level. If security measures are to be introduced into production, the "top-down" and "bottom-up" concepts implemented in standard engineering processes could be a possible solution:

- **Best practices (bottom-up)**

There are a number of measures that will always increase security levels regardless of a specific threat analyses. These include segmenting networks and protecting them with firewalls, introducing a user and password management system, as well as recording and evaluating events. These activities will quickly ensure that a basic security level is established. However, any subsequent targeted improvement to the security level requires a systematic approach. The German Federal Office for Information Security (BSI) supports systematization using the LARS tool (Light and Right Security).

- **Information security management (top-down)**

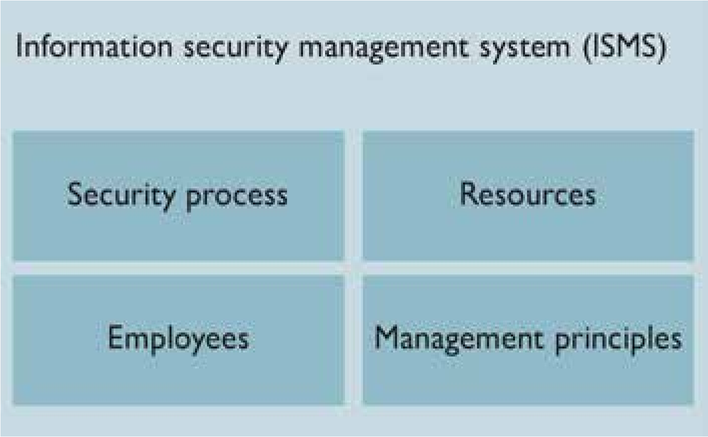
A target-oriented approach is detailed in the ISO/IEC 27000-series and ISO/IEC 62443 standards. The initial assessment determines the protection requirements: what needs to be protected against which threat? Organizational and technical measures can then be implemented based on these considerations.

Further development measures

While automation systems were isolated in the past, nowadays they are closely linked to the company's IT infrastructure. Thanks to the development of digitalization, networking is becoming increasingly important and now also includes inter-company aspects and cloud services. IT security must therefore be developed accordingly.

- **Information security management system (ISMS)**

An ISMS will examine all aspects of IT security. A continually high level of security can only be implemented in an organizational context.



Information security management system (ISMS)

Security process

Resources

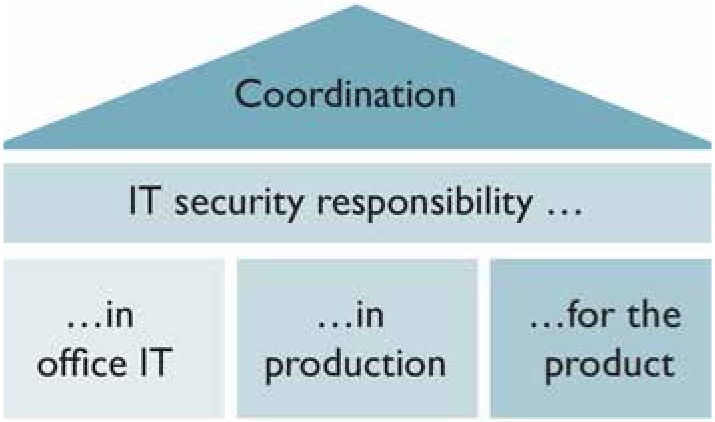
Employees

Management principles

The general ISMS detailed in the ISO/IEC 27000-series is currently being introduced in IT systems at larger companies. However, automation differs from IT in a large number of criteria and must therefore be given special consideration in an ISMS, as is the case in section 2-1 of ISO/IEC 62443.

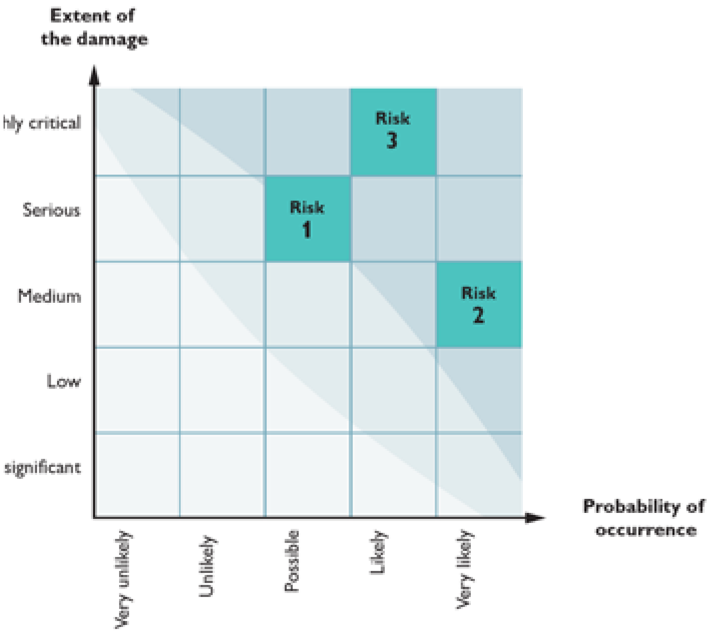
- **Controlling responsibilities**

In order to ensure that the specified characteristics and different perspectives are taken into consideration, the responsibilities must be controlled accordingly. One of the suggestions for realizing this was developed as part of the Industrie 4.0 platform. The overall coordination of the activities is an important part of this concept, because the desired security level can only be achieved by means of an agreed approach.



- **Identification and classification of company values**

To effectively and efficiently implement IT security, the company's assets that are to be protected, i.e. systems, plants and processes, must be identified and rated according to their criticality such that a threat analysis can be implemented. Potential threats must be determined first, before any resulting risks can be evaluated. This risk assessment, which takes the extent of the damage and probability of occurrence into consideration, is particularly challenging.



While accidents and technical faults can be assigned high levels of probability, targeted attacks cannot be based on statistical estimates. The ISO/IEC 62443 therefore uses security levels 1 to 4, which are based on the capabilities of possible attackers. Even if the threat analysis needs to be completed by external specialists, it provides a basis for subsequent prioritizations and is thus a sensible economic investment. Technical and organizational measures are then to be selected and implemented based on the results of the risk evaluation.

Areas of action in the automation sector

Different areas of action can be defined in the automation sector:

- **Formation of zones**

The automation system should be split into zones that are arranged by tasks, classification or protection requirements. Particular attention must be paid to the transitions between the individual zones.

- **Network security**

Separating the automation networks into different segments that can be based on the zones is recommended. The use of firewalls ensures that the flow of information between segments can be controlled.

- **Selection of secure systems and components**

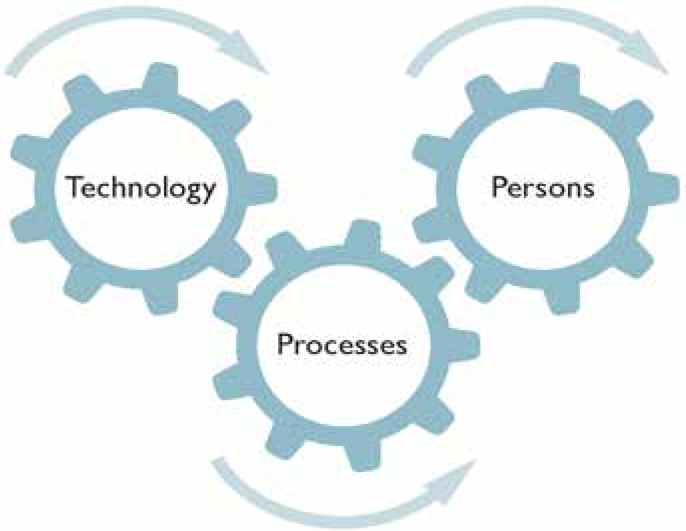
The selected systems should comprise the necessary security characteristics.

- **Patch management**

Total IT security cannot be achieved. It is therefore necessary that available software updates/patches are assessed according to their criticality and are installed accordingly.

- **Prevention and response**

Records must be collated and evaluated to be able to detect attacks. An emergency plan to safeguard and restore the system should also be created.



Supplier support

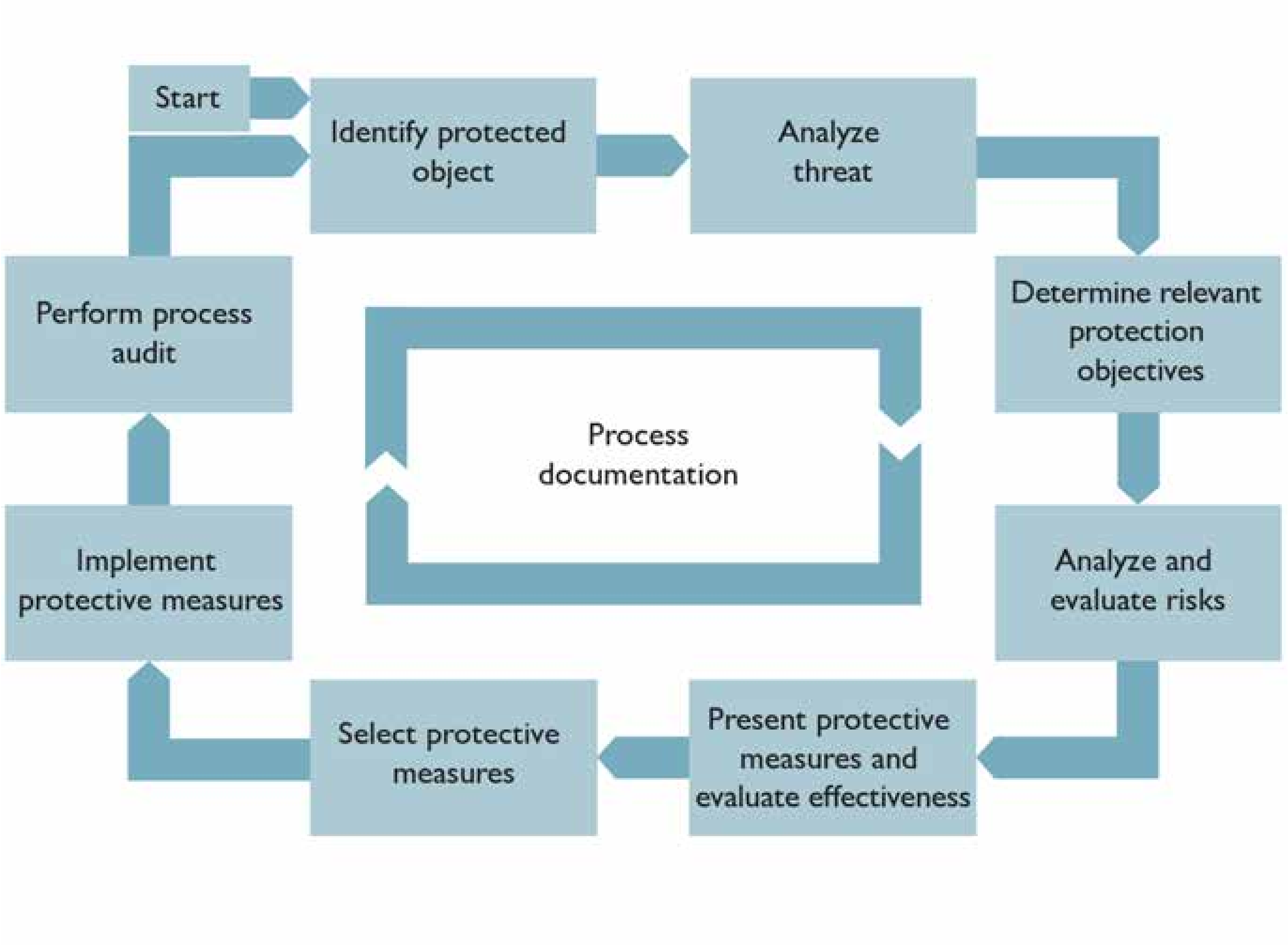
Implementation of the protective measures is dependent on the support of the relevant suppliers. Machines and plants are to be equipped with the necessary security functions such that they can be securely integrated into the operator's systems. This includes a user and right management system, secure reports and the recording of events. Section 3-3 of the IEC 62443 describes these functions from a system viewpoint. The effectiveness of the technical functions is ensured by guaranteeing the necessary specialist knowledge and continuous maintenance as part of the planning and operating processes in accordance with IEC 62443 section 2-4.

Related sections 4-1 and 4-2 of IEC 62443 must be taken into consideration when selecting which components to use. The functions in accordance with section 4-2 relate to supporting system features. Endpoint security is achieved by means of development and maintenance processes in accordance with section 4-1 (Security Development Lifecycle, SDL). The maintenance process includes the supply of patches for security weaknesses in the product. The provision of specified security functions and processes should already be considered when selecting suppliers.

Summary

IT security in the automation sector is based on an integrated approach. An excellent level of protection can only be achieved by ensuring that organizational and technical measures within the company interact and by working in close collaboration with suppliers. Security concepts can either be developed and implemented internally or by enlisting external advisors.

Phoenix Contact will support its customers throughout the entire process. A range of services including an assessment and threat analysis form the basis for establishing a security concept. Networks with secure access can then be implemented with the relevant components.


Start
Identify protected object
Analyze threat
Determine relevant protection objectives
Analyze and evaluate risks
Present protective measures and evaluate effectiveness
Select protective measures
Implement protective measures
Perform process audit
Process documentation

CYBER RISKS IN 5G

5G is the wireless fabric that connects everything, including autonomous vehicles, enable a surgeon to operate remotely a patient in real-time, and enable the realization of smart factories, homes, and cities. However, 5G raises more concerns over the previous cellular standards for the following reasons:

- **Architecture:** 5G networks are based on a software-defined network where activities will be pushed towards routers that are spread throughout the entire network. As a result, it will be impossible to identify or allow the deployment of chokepoints to be used in security inspection and control.
- **Virtualization:** In 5G most of the activities are developed and performed based on the Internet Protocol as well as popular operating systems. As a result, it will be easier to attack the software and manipulate it.
- **IoT proliferation:** Even before 5G networks will be deployed, IoT is already being deployed in a diverse range of use cases such as: military operations, transportation, public safety, healthcare, and smart urban centers. The devices will permit individuals and organizations alike to run critical processes. However, adding billions of IoT devices also introduces increasing vulnerabilities.

It's clear that the vulnerabilities in 5G go beyond wireless, introducing risks around virtualized and cloud-native infrastructures. These and other security challenges are significant reasons why the cybersecurity industry will undergo tremendous changes to match the level of the cyber risk environment the 5G network deployment will cause.

What are the measures that can be taken to mitigate cyber risks in 5G networks?

Since cyberattacks on 5G will be software ones; they must be combatted with software protections. For that, AI-powered solutions ensure that the security products will continue self-learning and updating adapting to an ever-changing environment.

As all businesses are aware of the 5G cyber risks, they will expect companies providing the network's services to demonstrate sufficient cybersecurity defenses that can sustain 5G network security. Whether small local ISPs or renowned brand names, they must implement successful cybersecurity programs.

Security should be considered in every aspect throughout the entire development life cycle rather than incorporating it in an already finished product. Since 5G is expected to be software-driven, it is more important than ever to integrate security, not only in the software but also in hardware and firmware development. This might see regulatory bodies to enforce the minimum-security requirements in all 5G hardware and software.

With its software operations per se vulnerable, and a distributed topology that precludes the kind of centralized chokepoint afforded by earlier networks, 5G networks will be an invitation to attacks. Given that the cyber threat to the nation comes through commercial networks, devices, and applications, the 5G cyber focus must begin with the responsibilities of those companies involved in the new network, its devices, and applications.

AUNA distribución

AUNA EMAIL AND APP PROTECTION SONIC WALL

The group trusts SonicWall to detect and dissipate new attack vectors

Business need

A so-called 'CEO attack,' which targeted one of the Group's partners, highlighted the need to update its email solution and anti-spam engine to protect itself against new threats.

Solution

The company deployed SonicWall TZ Series firewalls and SonicWAVE wireless access points, with advanced security features, including DPI-SSL inspection of encrypted threat traffic, SonicWall Capture Client endpoint protection, Capture Advanced Threat Protection (ATP) sandboxing, and Cloud App Security (CAS) service.

Capture ATP stops unknown and zero-day attacks before they execute. Capture Client offers zero-touch deployment of endpoint security. It applies Capture ATP to stop suspicious files from entering the network, and provides automatic rollback of compromised systems.

CAS protects cloud-based email, applications and file sharing.

Results

The solution has resulted in a 99% reduction in the number of calls related to fraudulent emails to the technical department.

Benefits

- The time dedicated to resolve any incidents was significantly shortened
- The number of calls related to fraudulent emails was reduced by 99%
- Greater control over email accounts and visibility into the applications users are using (Shadow IT)
- Easy and transparent integration of the CAS solution thanks to its API

Solutions at a Glance

- TZ Series Firewalls
- SonicWAVE Wireless Access Points
- Cloud App Security Advanced
- Capture Client Advanced

> **"We have found in SonicWall solutions that are simple to install and manage and very affordable, so they are very easy to justify to management. We're talking about an increase in investment of 1.5€ per user account, which gives us a level of responsiveness that, at the time of the project, had no competition."**
>
> **Raúl Campomar Bueno - IT Systems Department**

AUNA Distribución is the largest group of independent distributors of electrical material, renewable energies, plumbing and HVAC in Spain, with more than 450 points of sale in the Iberian Peninsula, the Balearic Islands, the Canary Islands, Ceuta and Melilla.

www.aunadistribucion.com

SCHNEIDER ELECTRIC JOINS CYBERSECURITY TECH ACCORD

Schneider Electric, the leader in the digital transformation of energy management and automation, has joined the Cybersecurity Tech Accord, a watershed agreement among its signatories to enhance the cybersecurity ecosystem and to defend the digital economy from cyberattacks.

The Cybersecurity Tech Accord is a public commitment among 144 global companies to protect and empower civilians online and to improve the security, stability and resilience of cyberspace. As a digital transformation leader operating in more than 100 countries, Schneider Electric is committed to upholding the Accord's core principles and will continue to work closely with governments, customers, and partners to confront cybersecurity risks and challenges.

- **Largest-ever cybersecurity alliance advances industry collaboration to defend digital economy**
- **Improves the security, stability and resilience of cyberspace in an increasingly digital world**
- **Supports the commitment to an open, transparent and collaborative culture that focuses on people, processes and technology**

"We are facing a new reality and geopolitical climate where malicious actors have unlimited time, resources and funding to carry out cyberattacks. Taking on newer, more innovative and increasingly dangerous threats can't be limited to a single company, industry or region," said Christophe Blassiau, Senior Vice President, Digital Security and Global CISO, Schneider Electric. "In joining the Cybersecurity Tech Accord, we're proud to continue our collaboration with industry leaders around the world to help detect, prevent and respond to cyberattacks."

Schneider Electric and fellow Cybersecurity Tech Accord signatories, including prominent partners such as Cisco and Microsoft, secure critical aspects of the world's online environment, including telecommunications, data centers and industrial control systems.

Schneider Electric and its partners have repeatedly worked together on digital innovation projects that ensure cybersecure measures are engrained at each level of the development journey, from edge to cloud.

"It is paramount for the digital ecosystem to have open and productive conversations, be transparent about attacks and collaborate on the development of new approaches to ensure both legacy and new technologies can withstand the most sophisticated cyber threats," Blassiau said.

"The evolution of ongoing conversations between governments, civil society and industry on the importance of cybersecurity at the international level exemplifies the need to work together across stakeholder groups to combat escalating threats online," said Annalaura Gallo, Cybersecurity Tech Accord. "We are pleased to welcome Schneider Electric as a signatory to the Cybersecurity Tech Accord, and we look forward to leveraging their unique expertise and experience as we collectively strengthen the security of the global, digital economy."

"Cybersecurity relies on partnership and collaboration, which have been central to the Cybersecurity Tech Accord from the beginning. Microsoft is delighted to see an increasing number of companies, including global heavy weights such as Schneider Electric, sign up to the principles that are pivotal to the long-term security and stability of cyberspace and that form the heart of the Cybersecurity Tech Accord," added Tom Burt, Corporate Vice President, Microsoft Customer Security and Trust.

In addition to the Cybersecurity Tech Accord, Schneider Electric is also a member of the Cybersecurity Coalition, as well as a founding member of the ISA Global Cybersecurity Alliance, which advances cybersecurity readiness and awareness in manufacturing and critical infrastructure facilities and processes.

To learn more about Schneider Electric's collaborative, three-pronged approach to cybersecurity, please read the blog (follow this link) : https://bit.ly/GC11-B4

About Schneider Electric

At Schneider, we believe access to energy and digital is a basic human right. We empower all to do more with less, ensuring Life Is On everywhere, for everyone, at every moment.

We provide energy and automation digital solutions for efficiency and sustainability. We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an open, global, innovative community that is passionate with our Meaningful Purpose, Inclusive and Empowered values.

www.se.com

CYBERCRIME IN SMALL BUSINESSES

“Hello friend! I have some bad news for you. Your files have been encrypted!”

If you or your business has ever been on the receiving end of a message like this, you’ve probably felt a number of emotions and had many thoughts. First, your blood runs cold.
Then you think it’s got to be a hoax, and then you check your files to find that, yes, they’re encrypted. Blind panic ensues, and you feel sick in the pit of your stomach.

If you’ve been in this situation, you’re definitely not alone – cybercrime is a fast-growing, complex problem that costs the Australian economy more than $1bn annually, and affects more than 500,000 small businesses. At its most basic level, cybercrime involves using computers and the internet to break the law, and common occurrences include identity theft and fraud, online scams and attacks on your computer systems or websites.

Regardless of the form of the attack, one thing is certain: Australians are losing huge sums of money to cyber criminals. In 2018, almost half a billion dollars ($489 m) in losses was reported to the ACCC, the Australian Cybercrime Online Reporting Network (ACORN), and other state and territory government agencies. Worryingly, these losses are up 44% on the $340m reported in 2017, hammering home the ever-growing impact of scams on the Australian public – and business community.

SMALL BUSINESS: THE BIGGEST OPPORTUNITY FOR CYBER CRIMES

Online security is a major concern for most Australian organisations, but there’s a widely held misconception that cybercrime only affects big companies. In reality, small businesses represent big opportunities for hackers, as these businesses typically have lower budgets and less resources they can invest into their online security.

According to the 2018 Verizon Data Breach Investigations Report, 58% of cyber attack victims worldwide were small businesses. Here in Australia, small businesses are aware of the threat of cybercrime yet remain largely unprotected and unprepared. A recent survey found that more than half (56%) of Australian small businesses either don’t have cybercrime protection or assume it is covered through their business insurance. “Roughly, 60% of small businesses every year will experience a cyber attack,” says Roger Smith, cybersecurity industry veteran and author of Cybercrime, a Clear and Present Danger, who, alongside running his own ICT consultancy, delivers the Australian Defence Force Academy’s compulsory undergraduate course in cybersecurity. He details the importance of small businesses waking up to this ‘clear and present danger’ or risk having to shut their doors. “We’ve worked with clients who have been devastated – they’ve lost their entire database and not had backup, which takes a thriving business to one that is severely struggling,” he says.

After a cybercrime event, businesses will often have to suspend their operations and many never restart, with the lost revenue due to downtime, the cash spent attempting to remediate the breach and the reputational damage creating an insurmountable challenge.

HOW CYBER CRIMINALS GET INTO YOUR BUSINESS

While there are a number of ways cyber criminals can attempt to infiltrate an organisation, the number one way your business can be exposed to cyber criminals is via email. “Email is a common way scammers can infiltrate your business with ransomware — a malicious software that criminals use to lock up their victims' computers so they can extort money from them," says Smith. This occurs when innocent looking attachments on messages are loaded with malware (malicious software) so that when the recipient opens them the bugs infect their computers. "Once inside your network, the attackers can do things such as steal or encrypt your data," says Smith.

Unfortunately, the malware doesn't necessarily only affect the computer of the person who actually opens the email. Malware can quickly spread throughout a company and infect multiple machines or even take hold of a company's server system.

FIRST THINGS FIRST : ASSUME THE WORST

As a busy electrical contractor, a lot of your business – from communication to banking, data collection to ordering – may be conducted online. So, how do you or your employees differentiate between a regular invoice or quote attachment from a client or wholesaler and one designed to infect your system? "Be paranoid and be prepared," says Smith. "Two key mistakes small companies make that leave them vulnerable to cyber attacks are firstly, they assume they won't be targeted, and secondly, they don't provide any cybersecurity training for their employees," says Smith.

This 'she'll be right' attitude is leaving small businesses at risk. Instead, Smith highlights that we need to apply a level of distrust to everything we do online. "If you receive an email from a client that doesn't seem right - perhaps the language is different to that which they would usually use, or perhaps it is asking you to change over their payment details – double check with your client in person or over the phone, using a number for their business that you know is correct," says Smith.

He also highlights the importance of employee training as paramount to staying vigilant against threats. "You need to assume you are, or will be, a target. Make sure your employees are trained and aware of the possible risks and threats that exist online so they can be vigilant," says Smith.

A MULTI-LAYERED APPROACH

Worryingly, 87% of small businesses believe their business is safe from cyber attacks simply because they use antivirus software.

Antivirus software, while important, is not enough – unfortunately, there is no one single fix for cybersecurity.

CYBERCRIME:
UNMASKED
EACH YEAR, 60% OF SMALL BUSINESSES WILL BE THE VICTIM OF AN ATTACK FROM A CYBER CRIMINAL. OF THAT NUMBER, 40% WILL GO OUT OF BUSINESS AS A RESULT. IF YOU'VE NOT THOUGHT SERIOUSLY ABOUT CYBERSECURITY BEFORE, YOU'D BETTER START NOW.

"You can't solely rely on antivirus software to keep you safe from attack," says Smith. "One thing we are most interested in is prevention – that idea of having a 'Plan B'. I stress to every business owner that they not only have a decent disaster recovery plan, but also a business continuity plan. "That way, if something does happen, you've already got your roadmap for how to get back to business as normal."

Alongside implementing some cybersecurity basics – a backup system, an antivirus system and a firewall (a network security system that essentially acts as a gatekeeper to monitor and control incoming and outgoing network traffic) – it's also important to protect your website by making sure all your online systems are regularly 'patched' (applying updates, fixes and improvements). "Make sure all your systems are patched to fix any security vulnerabilities and other bugs – scammers use malware to target systems and software that haven't been patched or updated and are therefore vulnerable to attack," says Smith.

In addition, he recommends using a password manager that generates complex passwords for every component you use in the digital world –think email, ordering portals, Google Drive, your company database – along with implementing two-factor authentication for all your passwords. "Two-factor authentication means that not only do you need a login and password, you also need a code. So, if someone tries to use your login details, a message will be sent to your mobile.

"Being aware that someone is attempting to access your account allows you to go in and change your details, booting them out and keeping your network secure," says Smith.

I'VE BEEN HACKED. WHAT SHOULD I DO?

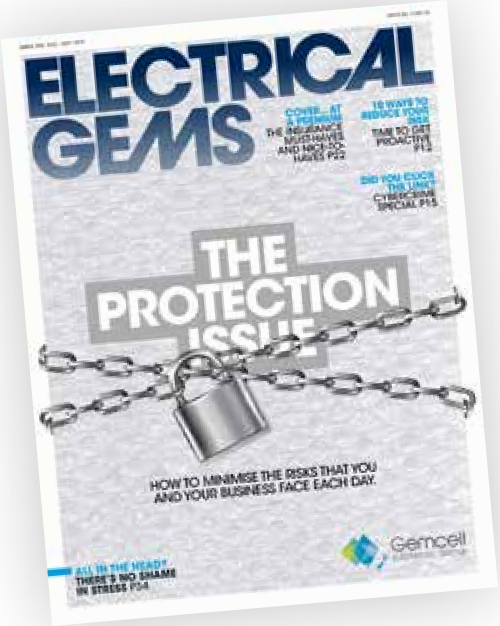
Should the worst happen, Smith's surprising advice is: do NOT turn off your computer. "A ransomware attack takes between two and five hours to encrypt your files. If you think something has happened and you catch it early enough, the first thing to do is not turn off your computer, but disconnect from your network. "You can then give your computer to a forensic expert, who may be able to halt the encryption process. If you simply turn off your computer, the malware will just continue to do its thing as soon as you turn it on again," says Smith. He also highlights that you have certain responsibilities as a business owner if your business experiences a cyber event. "If your customers' financial data or personal data, such as their licence numbers or physical addresses have been compromised, you have a responsibility to inform your customers," says Smith.

CHANGING THE CONVERSATION AROUND CYBERCRIME

There's something about the digital world that can feel a little like a lawless frontier—there's a perception that what we do online doesn't count in the real world. Smith uses the example of pirated video content, saying "people don't associate breaking the law with the digital world. So we don't think about laws being broken when we pirate a video, yet no one would think about walking into a store and not paying for a DVD."

He also points to the stigma that prevents many people from talking about these attacks, which makes it not only harder to recuperate from – financially and emotionally – but also leads to cybercrime being underreported. "If you are hacked, of course you feel violated, yet there is a stigma around cybercrime that prevents many people from talking about it. They feel naïve and stupid, and therefore don't share their experience. But the fact is, these are sophisticated attacks. "If someone robbed you while walking down the street, you'd get sympathy and support. Why should being a victim of cybercrime be any different?" says Smith.

Editorial featured in Electrical Gems Issue 152


ELECTRICAL GEMS
THE PROTECTION ISSUE
HOW TO MINIMISE THE RISKS THAT YOU AND YOUR BUSINESS FACE EACH DAY.
Gemcell

signify

DATA SECURITY IN CONNECTED SYSTEMS

1.1 The Internet of Things and connected devices

The Internet of Things (IoT) has been called the next industrial revolution. It is already transforming the way businesses, governments, and consumers interact with the physical world. By blending the physical and digital realms, the IoT is profoundly changing the way we relate to our environment, to each other, and to information. It is revolutionizing the way we live, work, travel, heal, and relax.

According to Gartner, the IoT is "a network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."[1] The sensing is done by sensors of various types—whether these are motion sensors in the ceiling of an office space, noise- level sensors on a city street, or sensors that can detect physiological states and changes in an individual. The communication is handled by standard wired or wireless communications methods embedded in connected physical devices.

Connected physical devices range from thermostats to energy meters to tractors to wearables for monitoring personal fitness and vital signs. Any digital device that can collect or share meaningful data about itself, its usage, and its environment is a candidate for participation in the IoT.

Connected devices generate data of various kinds. In IoT applications, this data is often aggregated in the cloud. This aggregated data can be processed and analyzed to extract knowledge and actionable insights that businesses, municipalities, and individuals can use to achieve their goals.

The IoT is still a fairly young technology, and its infrastructure is still developing, but its potential impact is enormous. The McKinsey Global Institute (MGI) predicts that "the Internet of Things has a total potential economic impact of $3.9 trillion to $11.1 trillion per year in 2025… equivalent to about 11% of the world economy."[2] Business Insider predicts that 24 billion devices will be connected to the Internet by 2020- in other words, "four devices on average for every human on Earth."[3]

The sheer volume of data now being collected from these billions of connected devices requires a special combination of technologies, analytical approaches, software platforms, and computing power. This combination is known as Big Data. Big Data poses novel data management challenges that can't be resolved with traditional approaches. It therefore poses novel risks, especially while enterprises are still learning how to avoid pitfalls and adopt emerging best practices.

1.2 System security and data management

Some security experts have said that the only way to ensure that data is safe is not to save it in the first place.

Others, like CTO of IBM Resilient Bruce Schneier, consider data a "toxic asset" that must be treated "as we would any other source of toxicity."[4]

While these might be extreme views, leading analysts and researchers agree that security is among the top challenges facing the IoT today. In a study that McKinsey conducted in 2015 in collaboration with the Global Semiconductor Alliance (GSA), respondents most frequently cited security as their greatest concern about the IoT.[5] Similarly, in Gartner's 2016 Internet of Things Backbone Survey, which studied important geographic regions around the world, including China, Germany, India, Japan, the United Kingdom and the United States, "security emerged as the top concern" from a technology and administration perspective.[6]

With so much connectivity and data flowing through so many interconnected systems, how do you keep everything secure? How do you protect the enormous and growing range of invaluable digital assets—including company- confidential data, city infrastructure, information on private individuals, transactional data, and home devices?

The two main aspects of security are system security and data management. System security includes both physical security and cybersecurity—the physical network, connected devices, applications, communications operations, and so on. Data management comprises all the disciplines needed to manage data as a valuable resource. The Data Management Association (DAMA) Data Management Body of Knowledge defines data management as "the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets."[7] Data governance, data security, and data privacy are all aspects of data management.

1.3 Connected lighting in the IoT

The LED lighting revolution began in the late 1990s, when companies such as Philips Color Kinetics designed and brought to market best-of-breed digital lighting systems and luminaires for professional and home use across the entire range of lighting applications. White-light LED luminaires with light output and quality equivalent to or better than comparable conventional luminaires began to appear in the mid-2000s, along with color-changing LED lighting for architectural applications, which optimized and improved upon approaches and control solutions adapted from entertainment and stage lighting. Recent innovations in the digital lighting space include spectrally tunable LED luminaires that support new human-centric lighting approaches in wellness and productivity applications.

Within the last five years, leading-edge companies have been applying their expertise in LED lighting to developing connected lighting systems, both in the consumer realm and in the professional lighting space. Connected lighting is the intersection of digital lighting and the IoT. In a connected lighting system, LED luminaires are enabled with two-way data communications, allowing them to participate in the IoT by sharing data about their own status and operations.

Since lighting is already installed, or has to be installed, everywhere that people work and live, and everywhere that they go in urban environments, it serves as a natural platform for sensor networks and other physically distributed systems. If the lighting system is connected, it can serve as an enabling platform for delivering IoT applications wherever lighting is used. In Cisco's view, lighting is the first step in creating a single converged IP network that can integrate disparate networks-HVAC, metering, lighting, CCTV, physical security, scheduling—into one network. This converged and connected network provides building intelligence that delivers "new and innovative experiences for building occupants while providing granular energy management, control, analytics, and integration capabilities for building owners and operators."[8] Similarly, smart cities increasingly rely on converged infrastructures to deliver better experiences and outcomes for citizens.

Connected street lighting serves a similar role as the digital ceiling, creating a platform for distributing sensors, broadband communications equipment, and other connected devices throughout a municipality, and offering APIs for integrated monitoring and management of disparate city services networks.

Each of these applications represents new sources of data that must be managed. For example, LED luminaires can collect and share data collected from any sensors that may be integrated into the system. These typically include daylight, occupancy, motion, noise, and air quality sensors, but there's no inherent limitation on the type of sensors that can be added to the system. Communications from the lighting system, via visible light communications or other means, enables location-based applications that typically make use of ubiquitous smartphone apps and wireless connectivity.

These have many advantages for the users and managers of spaces, and represent additional data streams that a cloud-based system can store for processing and analysis.

Interact systems use the connected lighting infrastructure to offer IoT applications in several key application areas. Via partnerships with other leading technology and communications providers, such as Cisco and Ericsson, Interact systems offer end-to- end connected lighting solutions for smart cities, smart buildings, and smart retail. While specifics differ from system to system, all systems share a general architecture that includes:

- Lighting instrumentation, including connected luminaires, sensors, and lighting controls
- Networking hardware and software, including gateways, servers, switches, cabling, and data communications
- Management and monitoring software for the lighting system and IoT applications that the lighting system hosts
- Cloud services for hosting software applications and for gathering data from illuminated environments
- APIs for integrating Interact applications with other facilities and management applications in the digital ecosystem, and for building mobile apps and other software components, such as dashboards
- A data analytics platform for turning the raw data collected from connected systems into actionable knowledge and wisdom

Each of these aspects of an IoT system presents its own challenges to data privacy, data and system security, and data governance.

1. "The Internet of Things." IT Glossary, Gartner: http://www.gartner.com/it-glossary/internet-of-things/
2. Manyika, James, et al. "Unlocking the potential of the Internet of Things." McKinsey Global Institute, June 2015: http://www.mckinsey.com/businessfunctions/digital-mckinsey/our-insights/the-internet-of-things-thevalue-of-digitizing-the-physical-world
3. "There will be 24 billion IoT devices installed on Earth by 2020." Business Insider, 9 June 2016: http://www.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-5
4. Schneier, Bruce. "Data Is a Toxic Asset." Schneier on Security, 4 March 2016: http://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html
5. Bauer, Harald, Burkacky, Ondrej, and Knochenhauer, Christian. "Security in the Internet of Things." McKinsey & Company, May 2017: http://www.mckinsey.com/industries/semiconductors/our-insights/security-in-theinternet-of-things
6. Nuttall, Nathan, Goodness, Eric, Hung, Mark, and Geschickter, Chet."Survey Analysis: 2016 Internet of Things Backbone Survey." Gartner, 5 January 2017: http://www.gartner.com/doc/3563218/survey-analysis--internet-things
7. DAMA-DMBOK: Data Management Body of Knowledge (2nd Edition). Technics Publications, 2017: p. 17.
8. Huijbregts, Rick. "Re-imagining business value in a digital world." Cisco, May 2016.

Data management, privacy, and security in connected systems

www.interact-lighting.com

International Standard: DATA SECURITY

Unified database is a successful project of the Russian Association of Electrotechnical Companies. Target audience: distributors and suppliers, both members of the RAEC and non-members of the association, covering the whole industry.

The RAEC Nomenclature and ETIM Center, which maintains and develops the database, ensures the security, stability and relevance of its data.

The key priority in data security is to ensure its integrity and, at the same time, its "freshness", completeness, and accuracy. All of that in online mode.

Unified database in numbers:

- **1.4 million products**
- **760 brands**
- **4,161 classes**
- **12.5 million properties filled**

Maya Avdonina, Head of the RAEC Nomenclature and ETIM Center

The fundamental elements of the architecture of the security system as presented by Maya Avdonina, Head of the RAEC Nomenclature and ETIM Center:

Data confidentiality

We ensure confidentiality of information, which constitutes a competitive advantage for the vendor. Only distributors have access to it, while third-party manufacturers cannot use it

Confidentiality of prices and left over stocks

These attributes can be conveyed only to the distributor. Competing vendors cannot view each other's data in this category

Ensuring safe access.

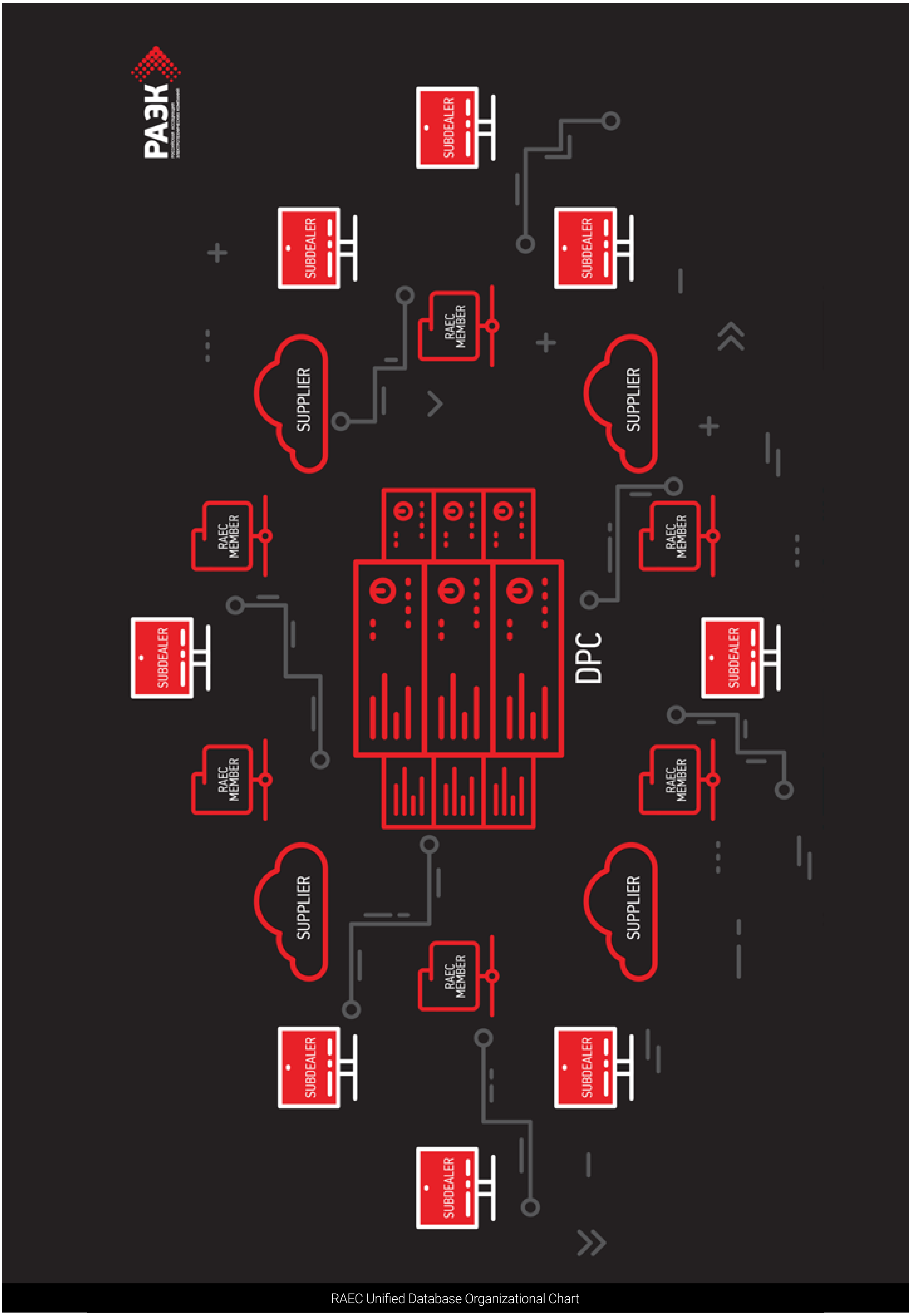
All our keys (accounts) are personalized, and a specific operator is responsible for each point of entry. There is a role, a position, and a scope of authority defined for each key. When unauthorized access is attempted, a verification algorithm is triggered which protects data from leaks.

Hybrid verification system: notification of the system when the incident is detected and verification by a technician.

Ensuring the stability of our system

The Unified RAEC Database servers are located in several locations of the certified Data Center with a system of emergency recovery and regular backup.

The sizing policy allows us to automatically calculate the required capacity based on the needs of the database.



RAEC Unified Database Organizational Chart

ABB

Unlock
THE POTENTIAL OF 5G

The rollout of 5G networks is going to see an explosion in the number of new devices connected to the internet, all communicating with each other at incredibly fast speeds. This increase in connectivity will create huge possibilities for consumers, businesses and society, driving the potential for everything from self driving cars to robots performing surgery.

It will also lead to a seismic shift in the amount of data processed worldwide. And, as we generate more data, we will also see greater concerns around cyber security.

According to Accenture's '2019 Cost of Cybercrime Study', the global business value at risk over the next five years is US$5.2 trillion. As ABB Electrification's Chief Technology Officer, Amina Hamidi, explains: "In our increasingly connected world, data is the lifeblood of any industry and the need to protect that data is a key part of ABB's DNA. Providing maximum security risk mitigation is an exercise in patience and continuous executions of the basics, while always pursuing security innovations. There is no one simple solution to keeping our data safe."

ABB views security as a continuous process that needs to be front of mind for all businesses that handle data.

Our experts have some simple tips for distributors whose customers are concerned about cyber security:

- **Know your assets:** Complete an asset inventory of every element of an organization – from data to software systems. Without this, you won't be able to identify where the potential gaps are
- **Test and test again:** Perform regular back and test restore cycles to make certain that any backups are protecting as they should
- **Check your vulnerabilities:** Do a software vulnerability analysis so you know the state and version of every software asset
- **Flex your approach depending on your Operation Technology (OT):** Patching is automatic in IT but can be more complex in industrial OT. In some case, patching OT can make things worse. For older OT systems, we would recommend a threat analysis to identify vulnerabilities and minimize risk
- **Keep your logging central:** Enabled centralized logging, so that security managers know why something is failing, not just how. It consolidates, manages and analyzes logs so security teams can fully understand their environments, identify threats early and optimize defences

ABB

ABB is constantly improving its solutions to guarantee 360° security in product design, implementation and operation. It is also leveraging best in class technology partners, such as Microsoft, Ericsson and HPE to monitor for possible new threats and react quickly to keep systems as secure as they can be. With current estimates forecasting the number of 5G connections to reach anywhere between 20 million and 100 million by 2021, the rollout will unlock tremendous opportunities for distributors and partners.

Key benefits of improved connectivity include:

- **Spare part planning:** it will be easier to provide near real time device status to plan maintenance more effectively. Distributors will be able to forecast spare part availability and shorten the lead time to repair faults.
- **Condition and predictive maintenance:** it will become easier to acquire data with higher frequency and run even more accurate analytics to identify more precisely the type of fault and possible cause. This gives distributors the opportunity to offer Smart Maintenance and Repair services to end users.
- **Reducing the need for cabling and complex configurations:** mobile networks will make installation even easier as it will remove the need for cabling to connect devices.
- **Stronger energy management:** energy management is a key tool to make sure that solutions only use energy where and when they need it. Solutions like ABB Ability™ Electrical Distribution Control System already provide a huge amount of information to implement and maintain certification like LEED and ISO5001. However, power quality issues and electrical network analysis can only be performed locally because of the massive quantity of information needed for troubleshooting. As Amina Hamidi from ABB concludes: “It is hard to believe that it is 18 years since the first commercial 3G network went live in South Korea. Since then we have seen dramatic changes in the way we connect with each other."

“The rollout of 5G will continue this dynamic shift. Alongside our distributors and suppliers, we need to use this to our advantage, to not only offer greater benefits like energy management and predictive maintenance, but to also ensure that we keep our customers as safe as possible in this brave new world.”

More informations
https://new.abb.com/about/our-businesses/electrification

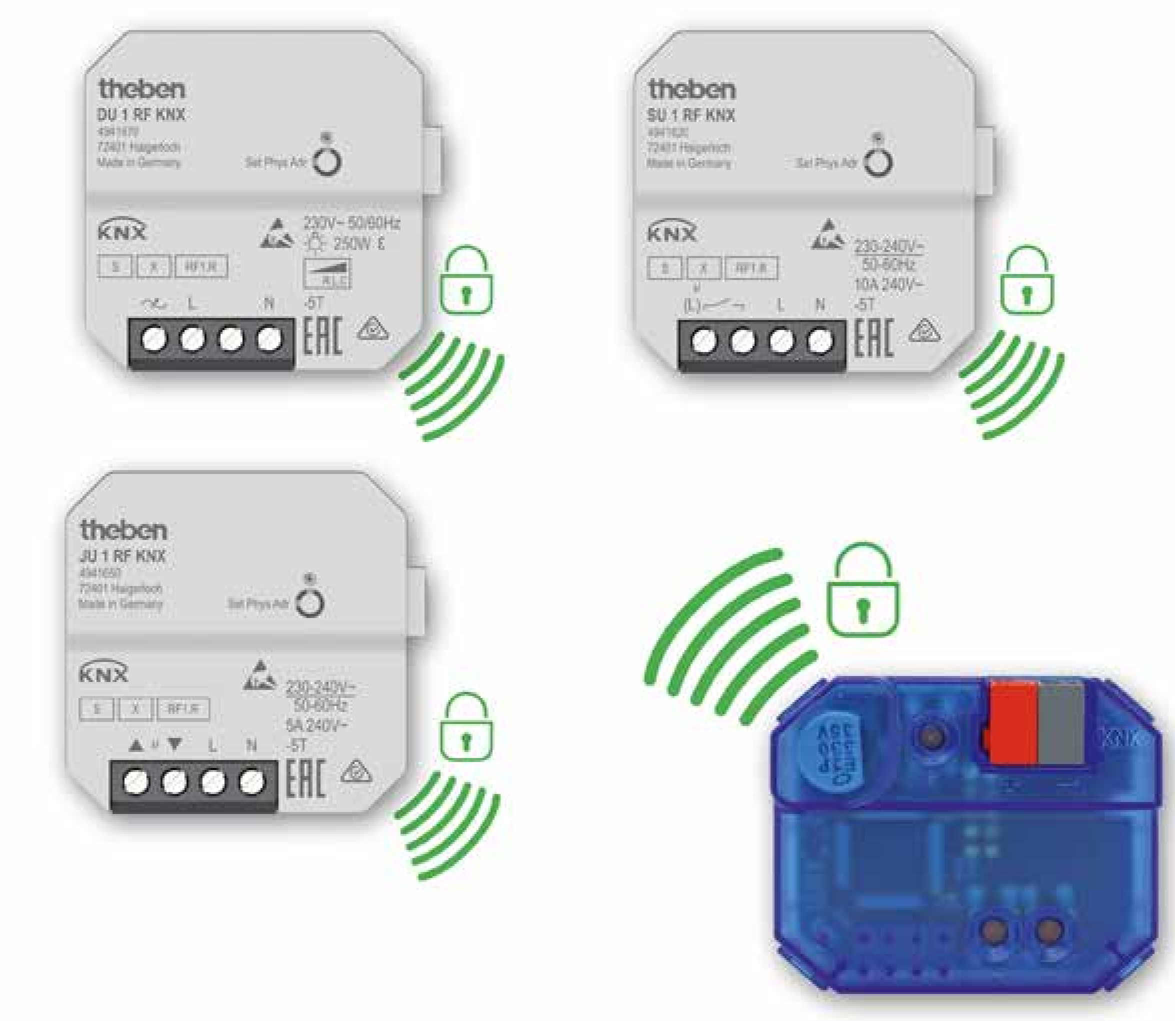
KNX WIRELESS ACTUATOR

Protected against manipulation thanks to KNX Data Secure: Theben KNX wireless actuators for flush-mounting

Theben AG is expanding its range of KNX RF products with new KNX RF flush-mounted actuators and media couplers. Encryption through KNX Data Secure ensures communication is optimally protected against tapping and manipulation.

Wireless protocols can be tapped into relatively easily in current KNX systems. KNX RF flush-mounted actuators and the media coupler support secure communication according to the KNX Data Secure standard and therefore effectively prevent interpretation of the transmitted data. This guarantees maximum data security for the customer and effective protection against tapping and manipulation.

The portfolio comprises a universal dimmer (DU 1 RF KNX), a blind actuator (JU 1 RF KNX), a switch actuator (SU 1 RF KNX) and a heating actuator (HU 1 RF KNX). All actuators have 2 external inputs for connecting buttons, a signal contact or a temperature sensor.



Maximum data security, effective protection against tapping and manipulation:
The KNX RF flush-mounted actuators and the media coupler support secure communication according to the KNX Data Secure standard.

ACCESSIBILITY OF RECESSED SCREWS

Standard insulated screwdrivers offer good protection, however users find them difficult to use when faced with recessed screws. This often leads to dangerous workarounds, such as cutting open or shortening the screwdriver insulation. This is precisely where the SLIM screwdrivers made by CIMCO-Werkzeugfabrik provide the right solution: With their narrow blade insulation, they make the user's life much easier when faced with recessed screws.

The classic SLIM screwdriver programme has been extended by new sizes: five slot-head screwdrivers, two Phillips and two Pozidriv screwdrivers, as well as four special screwdrivers with a combination profile, and in addition to that, five TORX® and two screwdrivers with square heads. These are available both individually and also in three attractive and practical sets.

The handle, which is made in a three-component injection molding process for the SLIM version, is important for working without tiring, as its tried and trusted ergonomic triangular handle shape perfectly supports the 120° rotation angle of the human hand.

Its curved, longitudinal contour optimises the pressure applied by your hand, allowing the entire handle to be grasped. Due to the special composition of the three components, the SLIM screwdriver is resistant against petrols, thinners, and other chemical solvents. In addition to that, the plastics are UV-resistant and also highly suitable in extreme cold (down to -40 °C).

All blades are manufactured according to the current DIN-ISO and VDE standards. Of course the tooling manufacturer from Germany's Bergisches Land produces every screwdriver in accordance with IEC 60900:2004 and they are individually tested up to a test voltage of 10,000 volts. In addition to that, these professional screwdrivers are tested in accordance with the German Equipment Safety Act (GS).

You can obtain comprehensive information directly from your specialist electrical wholesaler, or request the latest product information free of charge from CIMCO-Werkzeugfabrik in Remscheid.

You can of course also find all the information on the Internet:

FTCAP FILM CAPACITORS

Thanks to its recent acquisition of FTCAP (Germany), Mersen is now able to offer electrolytic or film capacitors which can be mounted on a specific bus bar, ensuring very low inductance value and high temperature capability. One example is the CX and CS series of low-inductance film capacitors for high-current applications which can be combined with compatible busbars and heat sinks.

Film and foil capacitors of the Coax Cap series are designed for extremely low inductance, a very high current carrying capacity, and good self-healing properties. Mersen offers the time-proven high-current capacitors not only as the CX type for extreme performance requirements, but also in the cost-optimized CS version.

Image 1: Mersen Capacitors CX and CS series

TWO TYPES OF HIGH-CURRENT CAPACITORS

The film capacitors of the CX and CS series from FTCAP are available in five different heights from 40 mm to 100 mm and a broad selection of capacitances from 20 µF to 830 µF with voltage ratings from 600 V to 1900 V. The classic applications include DC filters. In general, these high-current capacitors, due to their low inductance coefficient, are a good choice for applications with high ripple frequencies or pulse discharges. A good choice for less extreme performance requirements is the CS version, which due to the less stringent performance requirements also offers the advantage of a lower price. Compared to the CX type these film capacitors have a lower current carrying capacity and higher inductance.

DIFFERENT HEIGHTS FOR FLEXIBLE USE

The windings of the Coax Cap capacitors are made of low-loss polypropylene film. Two solid brass terminals, each with a diameter of 16 mm, ensure a high current carrying capacity. They are available either with M8 threaded bolts or M6 internal threads, in addition to special versions on request.

For special applications, in which for example several capacitors of this type need to be connected to each other by means of a low-inductance busbar, Mersen can also implement connectors of different heights for the respective application. This simplifies assembly and prevents unnecessary contact resistances, which would result from the use of standard washers. The surface milled bottom guarantees excellent thermal contact to the mounting surface – for optimal cooling of the capacitors, which in turn results in a longer life cycle.

More info on
ep.mersen.com

ABOUT MERSEN

Global expert in electrical power and advanced materials, Mersen designs innovative solutions to address its clients' specific needs to enable them to optimize their manufacturing performance in sectors such as energy, transportation, electronics, chemicals, pharmaceuticals and process industries.

The Electrical Power segment comprises two businesses that serve the electrical power markets: Electrical Protection and Control and Solutions for Power Management mainly for power electronics. Mersen works with the customer to integrate the products for electrical power into the customer's application, to make it safer and more reliable.

Electrical Protection & Control

- Overcurrent Protection
  - IEC Fuses & Fusegear
  - UL/CSA Fuses & Fusegear
- Overvoltage Protection
  - Lightning & Surge Protection
- Control
  - Low Voltage Switches
  - Fuse Switch Disconnectors
  - Metering

Solutions for Power Management

- High-speed Fuses
- DC protection for electrical vehicles and battery applications
- Cooling for power electronics
- Bus bars for power electronics
- Power Capacitors

Power Transfer for Rail Vehicles

- Earth Return Current Units
- Current Collectors
- Fuse Boxes
- Connection Boxes
- On-board Switches

THE GROUP IS LISTED ON EURONEXT PARIS COMPARTMENT B

LEDVANCE

LIGHT MANAGEMENT SYSTEMS

LIGHT MANAGEMENT SYSTEMS

WE PRESENT: VIVARES LIGHT CONTROL - SO SIMPLE & FLEXIBLE

The prerequisite for a strong performance is good management. This applies to business life as well as to lighting. The best example: LEDVANCE VIVARES. Because with our new, wireless lighting management system, intelligently networked lighting control is easier, more convenient and more flexible than ever.

With the help of VIVARES, the advantages and possibilities of modern LED lighting can be exploited to the full.
For example, the lighting can be adapted to the most varied requirements in the simplest possible way. By integrating daylight and motion sensors, energy savings are increased even further. And cloud-based monitoring ensures, among other things, even greater reliability and safety.

A major advantage for lighting professionals: installation, operation and maintenance of VIVARES are extremely simple, convenient and user-friendly.

GOOD REASONS FOR VIVARES

SETUP & HANDLING

- Easy installation
- Quick initialization through commissioning with QR code
- Compared to other systems (e.g. DALI): no "flashing" required for identification
- Easy handling with mobile application
- Simple reconfiguration of the components

USER-FRIENDLINESS

- Simple and intuitive system programming
- Optional remote access for time-saving adjustments after installation
- Location-independent energy and status monitoring in real time
- Efficient maintenance online or on site

CONNECTIVITY & TECHNOLOGY

- Based on the leading standard ZigBee 3.0
- Easy integration of third-party devices
- Offline operation possible
- Highest possible security by separating the lighting communication from WLAN networks
- Placement of luminaires without control cable
- Scalable for larger projects

Conclusion: In addition to easy handling, LEDVANCE VIVARES is characterised above all by sustainability and cost saving. The system is ideally suited for existing properties and flexible office space solutions.

VIVARES - MODERN LIGHTING MANAGEMENT WITH SYSTEM

Whether sustainable lighting, dynamic Human Centric Lighting or increasingly individual requirements - light today must be able to do so much more than just "on" and "off". LEDVANCE VIVARES enables you to open up completely new possibilities for your customers.

- Future-proof and flexible thanks to the open communication standard ZigBee 3.0 and an easily scalable system.
- Simple and convenient through user-friendly installation/control and cloud-based monitoring.
- Sustainable and cost-saving through optimized use of lighting - e.g. with integrated sensors.

HOW VIVARES WORKS

The key component of LEDVANCE VIVARES is the VIVARES ZB Control, a controller with gateway functionality that enables IoT services. The Vivares portal enables configuration, commissioning and maintenance of the system and its components.

Via ZigBee 3.0, the VIVARES ZB Control communicates wirelessly with up to 200 ZigBee-enabled devices. These include the VIVARES components such as sensor, pushbutton coupler, ZigBee-DALI converter and luminaires (VIVARES Ready). At the same time, it can be optionally connected to a cloud application. In this way, a large number of location-independent monitoring and maintenance functions are possible.

Here's a tip: Many of our luminaires are already LEDVANCE VIVARES and ZigBee ready

GOOD REASONS FOR OSRAM DALI PRO 2 IOT DISTRIBUTED BY LEDVANCE

IMPROVED ENERGY EFFICIENCY

Through exact tracking of energy consumption, energy and electricity cost savings can be significantly increased once again (also relevant in terms of energy management according to EN ISO 50001).

OPTIMIZED MAINTENANCE CYCLES

Thanks to remote monitoring, you always know which lighting components will need to be serviced or replaced in the near future. This effectively reduces travel times, effort and costs for maintenance.

MORE PLANNING RELIABILITY

The tracking of operating data also makes it possible to plan any modernization work that may be necessary with much greater precision. For example, you are also able to offer extended warranty services.

OSRAM DALI PRO 2 IOT - READY FOR THE INTERNET OF THINGS

DALI has proven to be the standard for automated control of lighting equipment. With OSRAM DALI Pro 2 IoT you are now ready to take the next step: Modern, energy-efficient lighting management connects to the Internet of Things (IoT).

OSRAM DALI Pro 2 IoT distributed by LEDVANCE not only enables a further, systematic reduction in energy consumption: The IoT-capable system also enables you to make targeted use of the potential of tracking and monitoring in lighting (see "Good reasons for OSRAM DALI PRO 2 IoT").

The user-friendly use is particularly convincing: Commissioning, for example, is self-explanatory and browser-based - without special software, independent of location and with any smart device.

THE MOST IMPORTANT FEATURES AT A GLANCE:

- Fully DALI-2 certified
- Browser-based commissioning via WiFi with PC, tablet or smartphone - without additional software
- IoT-capable: Thanks to DALI 2 LED drivers, tracking and monitoring functions can be fully exploited
- Most modern security concept with encrypted data transmission

WE ARE GROWING

KONINKLIJKE OOSTERBERG

CHORUS ELECTRIC ECHIPAMENTE SI SOLUTII

With the start of 2020, IMELCO was able to welcome two more members to the group, Royal Oosterberg from the Netherlands and CHORUS from Romania.

Having started out in 1893 as a piano tuner, Oosterberg had the right instincts when the business weakened in the 1950s and switched to electronic wholesale. Later on, Oosterberg diversified and, in addition to the classic retail for electrical products, also took over the wholesale for installation products and divided the company into these two areas. Today, with 20 branches throughout the Netherlands, 300 employees and a revenue of 200 M€, Oosterberg is the third player in the dutch market and was rewarded with the Predicate "Koninklijk" in 2018, the 125th anniversary of the company and is now "Royal Oosterberg". However, Oosterberg continues to see itself as a family business that places its customers at the centre of its activities. The mission statement is to stay close to the customer despite the size of the company, to always offer the best and friendliest service and this around the clock.

Flip Oosterberg,
Company owner

Moreover, Oosterberg has started to offer not only installation material, but also the appropriate logistic solution, thus providing a further building block for future growth. Of course, this also includes contributing to environmental protection. Thus, Oosterberg is member of several sustainability initiatives such as "Greenworks".
In the currently highly competitive environment, Oosterberg seeks as a family-owned wholesaler to effectively react to rapid market changes. With IMELCO they have found a partner to connect them with other wholesalers worldwide without taking away their independence.

CHORUS was founded in 2001 by today's Director General Catalin Cisleanu in Bucharest, today it features 22 branches in major cities of Romania. The annual turnover was expectedly 35M€ in 2019.

Catalin Cisleanu, Chorus
Company owner

Always close to their customers, Chorus is providing holistic solutions in the field of electrical installations as for example technical consulting in selecting the electrical equipment and designing services in the electrical field at any installed capacity and at any voltage level. Through their philosophy to always offer the customer the best service, they do not only sell electrical products but also offer full service for electrical installations, including application software, manufacturing, installation and maintenance, automation and efficient solutions for the optimization of the electrical energy consumption, as the saved energy is the cheapest energy.

In their membership within IMELCO they see the opportunity not only to benefit from a global network of similarly structured wholesalers, but also to take advantage of IMELCO's diverse marketing activities.

Both companies combine the qualities that make IMELCO, the world's largest association of owner-managed, independent electrical wholesalers, so successful: With one ear to the market and another to the customer, they are able to react flexibly to seismic changes. But can they also cope with earthquakes like the Corona pandemic?

One thing is clear in any case: the importance of cohesion and integration a large network becomes particularly vital in a crisis.

PROVISIONAL SCHEDULE OF MEETINGS AND CONVENTIONS 2020 - 2021

Due to the outbreak of the Covid-19 pandemic, our lives - be it in private or business - have changed significantly. Many of us are working from home office. We are now experiencing a complete shutdown in almost all European countries and overseas.

Nevertheless, IMELCO intends to move on and to provide our members and partner suppliers with a platform to present their latest innovations and solutions, in this issue and in a special edition of the "Global Circuit".

We will be publishing this special online issue shortly - filled with items that would have been part of exhibitions and trade fairs now postponed or cancelled like the light + building fair.

Also, we want to give an outlook to our next activities and the provisional schedules – as far as we are able to foresee events at the moment:

- IMELCO meeting followed by the General Convention of EUEW in Barcelona has been postponed to next year and will be held from 03.05. – 06.05.2021. We will keep our strong cohesion with the EUEW to continue benefiting from the numerous synergies resulting from the combination of the two events.
- The meeting in Moscow is cancelled as well. Instead, we would like to investigate with our members and partner suppliers, which alternative events could be put in place. Most probably these will have virtual format to give us the opportunity to be flexible in terms of number of participants and dates. We would like to include
  - Speed-dating sessions
  - A digital day, as follow-up of the DIGILAB'19 in Amsterdam, NL

As the next year is not yet to be foreseen, for the time being we will keep in place our plans for the celebration of IMELCO's 30th anniversary:

- IMELCO Convention in Dubrovnik from 29.09.2021 to 02.10.2021

From our members, we have received information on their schedules being strongly affected by Covid-19 as well. A large majority of members took the decision to postpone their activities to next year or even later. Members' meetings as well as customer events had to be cancelled.

However, e.g. GRUDILEC managed to hold virtual meetings through video conferences for their monthly members' meeting in March and April. MITEGRO set up a digital trade fair (read more on page 6).

The next regular issue of our newsletter will be dedicated to the subject of "carbon neutrality / zero emission".
If you wish to be represented in it, send your contributions to marketing@imelco-solutions.com before 10.07.2020.

IMELCO®
International Marketing Electrical Corp.

#winnersoftomorrow

ahlsell
www.**ahlsell.com**

ANEW
ASSOCIATED NATIONAL ELECTRICAL WHOLESALERS
www.**anew.co.uk**

AUNA distribución
www.**aunadistribucion.com**

CHORUS
ELECTRIC × ECHIPAMENTE SI SOLUTII
www.**chorus.ro**

elex ITALIA
www.**elexitalia.it**

GEMCELL ELECTRICAL GROUP
Connecting Independents across Australia
www.**gemcell.com.au**

Gibed
Group of Independent Belgian Electrical Distributors
www.**gibed.be**

GRUDILEC
Distribución Material Eléctrico
www.**grudilec.com**

imagro
www.**imagrogroep.nl**

IMARK CANADA
www.**imarkcanada.com**

IMARK GROUP
Member Owned, Member Governed
www.**imarkgroup.com**

INTER ELEKTRO
www.**iesa.pl**

MENTAVILL
www.**mentavill.hu**

MITEGRO
www.**mitegro.de**

RAEC
RUSSIAN ASSOCIATION ELECTROTECHNICAL COMPANIES
www.**raec.su**

KONINKLIJKE OOSTERBERG
www.**www.oosterberg.nl**

GROUPE SOCODA
www.**socoda.fr**

2020 © IMELCO s.p.r.l. - 1151 Chaussée de Waterloo - 1180 Bruxelles - Belgique | **All trademarks, logos, service marks, collective marks, design rights, personality rights or similar rights that are mentioned, used or cited by GLOBAL CIRCUITS are the property of their respective owners**, provided by third parties and published under their sole responsibility. The reproduction, in whole or in part, in any form, is prohibited without prior authorization from the publisher/author **Design & production:** Jérôme VADON for IMELCO - jerome.vadon.fr / jerome@vadon.fr | **Front & back cover:** based on "5G network digital hologram and internet of things on city" @Yingyaipumi - Picture licenced by Freepik (License premium / ID: I-SK06J8WA007T) **- 2ND page (Edito) :** based on "Hacker using laptop with abstract skull shape binary code" @Nonnie192 - Picture licenced by Freepik (License premium / I-SK06J8WA007T)