2022 | Volume 6

electronics update

Image credit: Raeng on Unsplash

Industrial Electronics | IIoT | Automation | Data Security

Trends and Lessions from 2021 Machine Vision Market

Every year for close to 40 years, machine vision users and systems integrators have been leveraging better imaging, optics, illumination, and software. And 2021 is no exception. Even though machine vision is a relatively mature technology, decreasing component, software, and engineering costs, combined with increasing ease of use and application expansion, continue to drive healthy revenue growth for component and system suppliers serving the machine vision market. Compared to 2020, the robot and machine vision markets made substantial gains in the second quarter of 2021 according to a recent Association for Advancing Automation (A3) report. While robot orders in Q2 2021 were up more than 67% compared to Q2 2020, the North American machine vision market grew by 26% to $764 million. More than half of the robot orders came from non-automotive industries, including metals (up 99% over Q2 2020), semiconductor and electronics/photonics (up 62%), plastics and rubber (up 51%), food and consumer goods (up 51%), and life sciences/pharmaceutical/biomed (up 21%).

In addition to the large increase in robot orders, A3's report showed record increases for the machine vision and motion control and motor markets over Q2 2020, and from January through June 2021, the North American machine vision market grew 18% to $1.5 billion, which is the best start to a year on record.

Machine Vision Adoption Gains Momentum

The COVID-19 pandemic seemed to accelerate adoption of machine vision technology in 2021. As businesses rushed to bolster digital infrastructure to support remote workers, manufacturers accelerated adoption of automation and machine vision to keep operations running as efficiently as possible and to keep up with increasing demand. Increased online purchase volumes propelled a steep rise in logistics-related applications. These included imaging systems used in retail distribution centers and automated warehouse storage and retrieval systems, as well as at manufacturers of PPE-related items such as face masks, face shields, protective garments, and respirators.

“Due to labor shortages, we're seeing a significant increase in companies that want to automate, with the ultimate goal of something as close to a lights-out manufacturing process as possible,” says Mark Kolvites, senior technical sales manager at Metaphase Technologies Inc. “Due to supply chain issues, companies want to be less reliant on off-shore suppliers, and in order to meet demand, they need to automate the inspections and visual portions of the product fabrication.”Companies aren't looking to replace people. It's just that they can't find enough of them as they increase production capacity due to greater demand. Automation technologies such as machine vision have helped manufacturers meet demand and continue to grow. Edgewater Automation control design engineer Dan Rutkowski confirms this, noting that in the past year, the designer/builder of custom automation equipment has done a lot more jobs incorporating machine vision. “There‘s definitely no shortage of work for us,” Rutkowski explains. “Compared to 2020, we've more than doubled our business, as a lot more of our customers, struggling to find people and meet increased demand, see the value of investing in automation and machine vision.”

Vision Application Base Expands

Accompanying the recent double-digit growth in the North American machine vision market, one of the most significant and overarching trends this year is the ever-expanding application base in just about every sector. These days, industrial automation and machine vision technologies don't just replace people performing error-prone manual assembly and inspections. Rather, they enable new products that are more complex and have tighter tolerances, and therefore require automated inspection.

Image credit: Possessed Photography on unsplash

Automation and machine vision technologies also improve operational efficiency and productivity, reduce production costs, and expand worker capabilities. Austin Storm, controls engineer at Edgewater Automation, agrees, noting, “Many applications are beyond the capabilities of people, and the vision systems we're working on are becoming more and more complex, sometimes trying to find defects on parts that can't even be seen with the naked eye.” Applications involving complex parts and defects that are too small for people to see aren't the only things driving expansion of the application base. Also important are new types of inspection that can be readily accomplished with nonvisible industrial machine vision applications.

As is typical, the number of viable SWIR, hyperspectral, and multispectral applications has increased as the cost of the technology has decreased and as camera resolutions and ease of use have improved. Consequently, this year there's been a significant increase in such applications as they move from research experiments into real-world industrial applications, such as detecting opaque container fill levels and epoxy presence/absence using SWIR imaging.

“Over the past several years, we've all witnessed a steady increase in such applications,” says Kolvites, “but there's been a steep increase in interest this year for not only UV-fluorescence but also IR, SWIR, hyperspectral SWIR, and hyperspectral VNIR in industrial machine vision applications.” While ongoing advances in every area of machine vision technology continue, a few trends are of particular interest this year due to their value in real-world applications. These involve high-speed, high-resolution cameras, optical components and advanced illumination, and deep learning and other advanced software.

High-Resolution Cameras, Optics, LEDs, and More

Manufacturers continue to develop image sensors with higher resolution and faster frame rates. In turn, camera manufacturers leverage the latest sensor developments and improvements in camera design, helping machine vision system developers and integrators create faster, more flexible, and more capable imaging systems.

With higher camera resolutions comes the need for higher-quality, larger-format optics, which are readily available, with options including embedded liquid lenses for auto-focusing systems. Optics for nonvisible wavelengths enable new ways to detect things with specialized imaging using wavelengths that range from the UV through the IR bands. LED illumination products, critical to all machine vision applications, now come in a wide variety of wavelengths and form factors. They feature increased flexibility, with tunable angles and additional wavelengths, more consistent spectral response, and even programmable sources with embedded controls. The practical value here is that machine vision developers and systems integrators now have more choices to enable more complex applications. “An important enabler is the emergence of up to 100 G interfaces as well as the recently updated CoaXPress 2.0 interface and even PCI interfaces,” says David Dechow, principal vision systems architect for Integro Technologies. “The great variety of mature technologies that deliver a high level of reliability, flexibility, and ease of use, and with broader technology compatibility mostly driven by rapidly developing standards in the industry, benefits of all of us who work with machine vision technology.”

Deep Learning and Easier Integration

Deep learning offers the advantages of traditional rules-based machine vision systems, with the judgment that human inspectors bring, but in a semi-automated fashion that requires continuous optimization. The technology is helping machine vision expand into new industrial applications. For machine vision users and integrators, deep learning is very well indicated for applications where subjective decisions need to be made, similar to human inspection, particularly where the identification of features is difficult due to the complexity or variability of the image. “We have a lot more activity this year with deep learning applications, and although still in the experimental or feasibility stages, we are confident these will come to fruition in the near future,” explains Sam Lopez, senior vice president of sales and marketing at Matrox Imaging. “We had all these existing customers who had shelved a lot of vision projects that they weren’t able to solve with the traditional approaches. But now they have pulled those projects off the shelf, dusted them off, and started looking at them again from a deep learning perspective.”

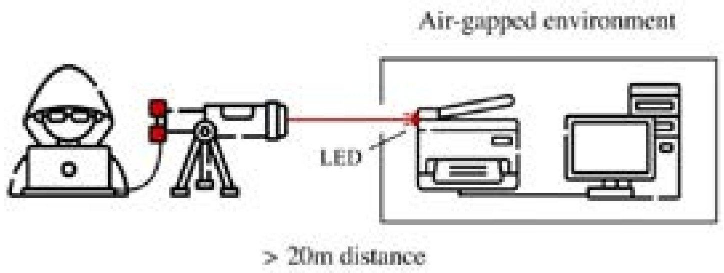
There are several graphical user interface–based software options for neural network training. Matrox Imaging, for example, offers deep learning software and hardware. The company’s software offerings—Matrox Imaging Library (MIL) X and Matrox Design Assistant X—include vision tools for classifying or segmenting images for inspection using deep learning. Both software packages deliver optimized convolutional neural networks (CNNs) or models for the task. Key to deep learning is the training of a neural network model. MIL CoPilot’s interactive environment provides the platform for training models for use in machine vision applications. MIL CoPilot delivers all the functionality needed for this task, so you can create and label the training image dataset, augment the image dataset if necessary, and train, analyze, and test the neural network model. Another example, the In-Sight D900 from Cognex, is a smart camera powered by In-Sight ViDi software designed specifically to run deep learning applications. In-Sight ViDi applications are deployed on the In-Sight D900 smart camera without the need for an industrial PC, making deep learning technology accessible to non-programmers. It uses the familiar and easy-to-use In-Sight spreadsheet platform which simplifies application development and factory integration.

More Tools in the Toolbox

Continued development of new and improved machine vision components and easy-to-use software is driving this year’s increased machine vision adoption and application expansion. To meet increasingly complex manufacturing challenges, vendors are continually developing new components that vision system developers can deploy to address an increasing variety of application challenges more quickly and easily. From high-speed and high-resolution cameras to LED illumination, optics, smart cameras, and embedded cameras to advanced imaging components such as spectral and nonvisible imaging, vision system developers have never had more tools in the toolbox.

IT security: computer attacks with laser light

Computer systems that are physically isolated from the outside world can also be exposed to attack. This is demonstrated by IT security experts at the Karlsruhe Institute of Technology (KIT) in the LaserShark project: With a directed laser, data can be transmitted to light-emitting diodes already installed in devices. In this way, attackers can secretly communicate with physically isolated systems over several meters. LaserShark shows that security-critical IT systems not only have to be well protected in terms of information and communication technology, but also optically. Hackers attack computers with lasers - this could be a scene in a James Bond film, but it is also possible in reality. At the beginning of December 2021, scientists from KIT, TU Braunschweig and TU Berlin presented their research project LaserShark, which investigates hidden communication via optical channels, at the 37th Annual Computer Security Applications Conference (ACSAC). Computers or networks in security-critical areas, such as those found in energy suppliers, in medical technology or in traffic control systems, are often physically isolated to prevent external access. With this so-called air gapping, the systems have neither wired nor wireless connections to the outside world. Previous approaches to this protection via electromagnetic, Breaking acoustic or optical channels only works over short spatial distances or at low data transmission rates; often they only allow data to be extracted.



Hidden optical channel uses LEDs in standard office equipment

The method demonstrated by the research group Intelligent System Security at the KASTEL - Institute for Information Security and Reliability of the KIT together with researchers from the TU Braunschweig and the TU Berlin, on the other hand, can initiate dangerous attacks: With a directed laser beam, outsiders can smuggle data into and out of systems protected by air gapping channel them out without the need for additional hardware on site. „This hidden optical communication uses light-emitting diodes as they are already built into devices, for example to display status messages on printers or telephones,“ explains junior professor Christian Wressnegger, head of the Intelligent System Security research group at KASTEL. „These LEDs are actually not intended for receiving light.

Data transfer works in both directions

By directing laser light onto built-in LEDs and recording their reaction, they have for the first time set up a hidden optical communication channel that extends over distances of up to 25 meters, works bidirectionally - in both directions - and has high data transmission rates of 18.2 kilobits each Second inwards and 100 kilobits per second outwards. This possibility of attack affects commercially available office equipment such as those used in companies, universities and authorities. „Our LaserShark project shows how important it is to protect security-critical IT systems not only in terms of information and communication technology, but also optically,“ says Wressnegger.
In order to advance research on the topic and to further develop protection against hidden optical communication, the researchers provide the program code used in their experiments, the raw data from their measurements and the scripts on the LaserShark project page:

https://intellisec.de/research/lasershark

Keeping Distributed Systems Secure

Image credit: Carnegie Mellon University

With more and more devices able to connect to the Internet or to one another, it's becoming increasingly important to ensure that those connections are secure.

When a group of devices—be it computers, sensors, or otherwise—connects and communicates directly with one another, it's known as a "distributed system."

Imagine, for example, a group of sensors monitoring the doorways in a particular building. They could communicate with each other to tell you which doors are open and when, which could be used to better secure the building as a whole. This is an example of a "wireless sensor network," a particular kind of distributed system. Another would be a group of devices connected to the Internet of Things (IoT) in your home.

With these direct lines of communication, however, there is an increased danger of one sensor or device becoming compromised and taking down the entire system.

Two members of Carnegie Mellon's Electrical and Computer Engineering Department are working to improve the ways those systems communicate with one another and keep them safe: Ph.D. student Mansi Sood and Professor Osman Yağan.

The pair recently won the Best Paper Award at the Institute of Electrical and Electronics Engineers International Conference on Communications in June of 2021. This conference occurs yearly and seeks to drive innovation in the field of telecommunications. Their paper titled, "Tight Bounds for the Probability of Connectivity in Random K-out Graphs" won in the "Communication Theory Symposium" category due to its focus on foundational research into the topic.

"This paper is part of our group's ongoing research on designing secure, connected, and resilient ad-hoc networks for diverse applications including wireless sensor networks and distributed private averaging," Sood explained.

She accomplished this using a mathematical model known as a "random K-out graph." Each node of that graph represents a device setting up connections with other nodes in a random, "undirected" pattern.

But why do we need mathematical models like the random K-out graph to represent these networks?

"In many distributed systems, connectivity is a fundamental driver of system performance," Sood says. But, establishing the links between nodes can be costly, and as you set up more, you approach a trade-off between connectivity and cost.

As a result, research like Sood's is incredibly important to understand how these networks can be designed such that they are provably guaranteed to hold up during an attack. With applications including the IoT and aggregating user data for distributed learning, that privacy and security becomes paramount.

The interdisciplinary aspect of this research also gives Sood the chance to use tools from probability, graph theory, statistical mechanics, and data science all together. She also enjoys doing work with real-world applications and is ready to explore more ways to do this in the future.

"We wish to further explore and design distributed network topologies that are scalable, reliably connected, and resilient and establish analytical guarantees for their performance," she says.

As more and more of our daily lives move online, we can thank researchers like her for keeping those systems safe and secure.

A Beginner's Guide to Internet of Things (IoT) 2022

We are able to turn on the lights in our homes from a desk in an office miles away. The built-in cameras and sensors embedded in our refrigerator let us easily keep tabs on what is present on the shelves, and when an item is close to expiration. When we get home, the thermostat has already adjusted the temperature so that it's lukewarm or brisk, depending on our preference.

These are not examples from a futuristic science fiction story. These are only a few of the millions of frameworks part of the Internet of Things (IoT) being deployed today. IoT has redefined the way we interact, communicate, and go about our daily work. From homes to maintenance to cities, the IoT ecosystem of devices is making our world smarter and more efficient.

In this guide, we will walk you through everything you need to know about the increasingly connected world of IoT. This guide discusses in-depth:

- What Is the Internet of Things?
- Examples of IoT
- The Internet of Things Ecosystem: How Does it Work?
- Sensor Technology & IoT
- Benefits of Sensor-Based IoT
- IoT & Data Security & Privacy
- Key Takeaways & The Future of IoT

What Is the Internet of Things?

Broadly speaking, the Internet of Things (IoT) encompasses all physical objects - aka "things" - that connect to the internet and to other devices. The definition of IoT is evolving, as the term is increasingly being used to describe objects that interact and "speak" to one another, so we can have the opportunity to be more efficient in how we do things. More specifically, IoT devices are characterized by the ability to gather data on their surroundings, share this data with other electronic devices, and ultimately, help us, the end-user gain information, solve an issue, or complete a task.

To visualize the concept, think of a time you've gone to the restroom in a hotel, and the light has turned on by itself. Ever wonder how that happened? There is probably a motion detection sensor there that detects movement, which automates and connects to the light to turn it on. This is only one of the simplest forms of an IoT solution, as the technology is now being used to create larger ecosystems such as smart homes and smart cities. If you read your emails through a voice-controlled virtual assistant, measure your steps and heartbeat with a smartwatch, or control your security system through your mobile phone, you're benefiting from IoT solutions on a daily basis.

Examples of IoT

Depending on their usage, we divide IoT devices into four main categories: consumer, organizational, industrial, and infrastructure applications. The consumer IoT refers to the dozens of personal devices, including smartphones, wearable technology, fashion products, and an increasing range of household appliances, that are linked to the internet, continuously gathering and distributing information.

In organizational settings, IoT is mostly widespread in the medical and facilities management field. Specifically, IoT devices are being used for remote monitoring and for creating emergency notification systems for people, buildings, and assets. The COVID-19 pandemic has also urged the use of IoT for smart cleaning and smart occupancy so that workplaces of all types can return to the office with the help of technology.

Industrial IoT (IIoT) brings devices, clouds, analytics, and people together to advance the execution and productivity of industrial processes. More specifically industrial IoT (IIoT) enables solutions such as equipment monitoring, predictive maintenance, condition monitoring, error detection, and much more.

Lastly, we have infrastructure IoT appliances that enable monitoring and controlling operations of sustainable urban and rural infrastructures like bridges, railway tracks, and on and offshore wind farms. These technologies help the construction industry by cost-saving, time optimization, better quality workday, paperless workflow, and an increase in productivity.

The Internet of Things Ecosystem: How Does IoT Work?

IoT operates over a boundless network, and thus it requires various components to form a cohesive system. We divide these components into three main categories.

First, you need a device that gathers input from the real world. This is usually done through sensors that work to gather real-time data from their surrounding environment. They're also often called "detectors" as their main purpose is to detect the slightest changes in their surroundings. For example, Smart ACs or thermostats work through a motion detector that is able to sense room temperature and humidity and adjust accordingly. More often than not, these sensors/detectors can also be bundled together as part of a device that does more than just sense things - phones are made up of several sensors such as GPS, camera, compass, fingerprint detection, to help us perform a handful of tasks. For the sensor to interconnect with other devices, and ultimately perform an action, it needs a medium of transport, which is connectivity. Connectivity is responsible for transferring data into the online world. Some of the most popular IoT wireless protocols and standards include Bluetooth, Wi-Fi, DDS, cellular BLE, Z-wave, etc. The choice of the network depends on several factors such as the desired speed of data, transfer, range, power consumption, and overall efficiency of the network. After data has been collected and has traveled to the cloud through a communication medium, it needs to be processed. This is the second component of the IoT ecosystem, where all of the "smart stuff", i.e. context and analytics, takes place. The basic role of analytical tools is to investigate a situation and form a decision based upon the insight. This can be as simple as analyzing when a room's temperature falls within the desired range, or as complex as, for example, a car that's close to a crash.

The very last element of the IoT system is the end-user device or user interface. This is the visible device or application a user uses to access, control, and set their preferences. A user-friendly and attractive design is a major consideration in today's IoT world. Companies are continuously working on the integration of convenient tools, such as touch interfaces, or the use of colors, font, voice, to put themselves on solid footing for a great customer experience.

Sensor Technology & IoT

In order for objects to be connected to each other and IoT to come to life, there must be a device that gathers the information that will be transmitted (the input). As we've mentioned, for many applications, this is done through sensors.

Just what sensors are collecting depends on the individual device and its task. But broadly speaking, sensors are tools that detect and respond to environmental changes, which may come from a variety of sources such as light, temperature, pressure, and motion. Because of the wide range of inputs IoT sensors are able to gather, they're being used extensively in various fields, and have become crucial to the operation of many of today's businesses. One of the most pivotal benefits of these sensors is their ability to warn you of potential issues, which allows businesses to perform predictive maintenance and avoid costly damages.

To exemplify the value of IoT sensors, let's take our wireless sensors at Disruptive Technologies as case studies. We offer small ingenious sensors for humidity, temperature, water detection, touch, and remote monitoring of your buildings & assets.

The **temperature sensor** can measure the surrounding temperature in any space or surface and wirelessly transmits the result to a Cloud Connector via SecureDataShot technology. A global chain restaurant in the UK used a partner solution to remotely monitor the temperature in each of their 100 freezers all across the UK, in real-time, 24/7. As a result, the restaurant saved more than £1.25 million in food inventory.

Image credit: Disruptive Technologies

The t**ouch sensor** is able to detect whenever the sensor is being touched, notifying the user about the event through a cloud server. Dorint Hotels installed touch sensors around their serving areas and washrooms to allow their customers to call servers to place orders or reach staff about hygiene concerns via the touch of a button. Dorint Hotels also saved 8700 KwH per year, by using our temperature monitoring to save data and energy, as it allowed them to adjust the Air Conditioning run time in their server rooms.

The **water sensor** is able to detect high water levels or water leaks, and immediately signal that water is coming in contact with the front of the sensor. These devices have been used in utility rooms, grocery stores, and restaurants, to alert management in case of any leaks from fridges, boilers, water heaters, or water softeners.

The **humidity sensor** senses and measures the moisture and air temperature of the surrounding environment where they are deployed, e.g., air, soil, or confined spaces. They can be used to ensure proper storage conditions for temperature-sensitive products, to enhance temperature monitoring functionalities in buildings and offices, for comfort optimization, for predicting leakages, and more.

Benefits of Sensor-Based IoT

IoT Benefits for
Hospitals & Restaurants:
For starters, IoT improves patient comfort. Through solutions such as smart thermostats, smart beds, and customizable lighting controls, patients can have a more enjoyable experience, reduce stress, and go through faster recovery. Next, IoT enables remote health monitoring and emergency notification systems through the use of wearable technology - these include electronic wristbands, advanced hearing aids, wearable heart monitors, and so forth. Such devices allow physicians to monitor their patients with greater precision and ultimately be able to come up with better-informed treatments. Another extremely important benefit of sensor-based IoT devices in hospitals relates to the safety of the patients and staff. Temperature sensors and cold storage ensure food, blood, and medications are stored safely, water sensors prevent potential leaks and hazards, occupancy sensors monitor waiting areas to control capacity, disinfection systems keep areas sanitary, and much more. For example, UK's National Health Service (NHS) has improved patient safety and reduced costs through sensors that automate daily hospital tasks such as medicine temperature checks, fire door monitoring, comfortable temperatures for patients, and much more.

Another sector IoT has also greatly impacted is the **food industry, specifically restaurants & restaurant chains.** The most prominent benefit relates to food safety and monitoring systems. With IoT temperature sensors, restaurants can remotely monitor their refrigeration 24/7 to make sure temperature changes don't go unnoticed, lowering the risk of spoiled food and food waste. IoT apps can also remotely monitor equipment and troubleshoot potential problems to avoid their failure and the cost of repair. These apps even send restaurant managers recurring reminders to schedule maintenance.

And that's only the tip of the iceberg when it comes to the solutions of remote monitoring for buildings & workplaces. For more interesting benefits, you can head over to our 10-minute read on 9 Benefits of IoT-Enabled Remote Monitoring For Buildings & Workplaces.

IoT Benefits For Offices:
Due to the pandemic, more than 50% of workers are afraid to return to the office. That's why real estate and facilities management companies are opting for IoT sensor technology and smart infrastructure, to help reduce some of these Covid-related concerns and risks. Say, for example, by placing a proximity sensor in bathroom stalls, the sanitary staff can get insights on how often workers use the restroom. Then, the staff can clean whenever there is a need, based on actual bathroom occupancy instead of a manual cleaning routine. This validates cleaning schedules, optimizes the office's resources, and increases the employee's overall health & well-being. Proximity sensors can also ensure safe social distancing, through reminder alerts to keep workers at appropriate distances from one another, whenever the occupancy of a room starts to increase.

IoT Benefits for Industrial Settings:
The Industrial Internet of Things (IIOT) uses smart sensors to enhance manufacturing and industrial processes.
One of the most praised benefits of IIoT devices is that they enable predictive maintenance. Predictive maintenance means businesses can schedule their maintenance activities based upon accurate predictions about an asset's lifetime. These benefits result in improved asset utilization, visibility of the asset's condition, and allows optimal planning of maintenance activities. A second important benefit of predictive maintenance is in facilities management and smart substations. Sensors can monitor vibrations, temperature, humidity, and other factors that could lead to deficient operating conditions, and alert management so they can take action to fix or prevent damages.

IoT and Data Security & Privacy

With all these devices consistently gathering everything we do, IoT is susceptible to a lot of privacy & security problems.

The main issues today are cybercrime and the risks of data theft. Cybercriminals are constantly evolving and looking for methods to hack passwords, emails, and impersonate staff to malware. And as the pandemic has forced people and businesses to go fully remote, there has been an increased focus on the issue.
IoT's security history doesn't do much to prevent these issues, either, as many IoT devices fail to consider the basic protocols of security, such as data encryption, blocking tags, authentication, and so on. They operate over a long period of time without supervision or updates and work with cheap, low-cost systems that are prone to cybersecurity risks. With all this being said, there are responsible manufacturers who go the extra mile to fully secure the embedded software or firmware built into their products.
Now, we know you're worried and wondering: what can I do to own my data and privacy?

The most important step is research - learn about your IoT solution supplier. How well do they comply with federal protocols and regulations? What are their privacy standards? Do they implement any encryption tools? And as dreadful we know it may be, it's important that you also read the terms of conditions for services, devices, and apps every single time to understand what you are agreeing to. Then, to reinforce your protection once you've purchased or installed a product, disable features that allow multiple devices to share data with third parties, constantly delete data history, install updates promptly, use two-factor authentication when applicable, and always create complicated, secure passwords.

The Future of IoT

And that's a wrap on our IoT guide! As the number of devices connected expands, our homes and workspaces will become increasingly overrun with smart products – presuming we are prepared to accept some of the privacy and security trade-offs. Some people will be happy about the upcoming world of advanced things. Others will miss the good old days when a table was indeed just a table.

Image credit: Disruptive Technologies

Endrich's new E-IoT Platform for IoT Developers

There is a special way to demonstrate the exceptional product and technology knowledge base built up during the 45 years of Endrich's history in design-in distribution, which is to share this with customers in a form of a free-to-use hardware and software eco-system. The company has state of the art product portfolio, good mix of quality suppliers, hundreds of won designs at customers and still our major role, what Endrich is known about is component distribution. In order to adapt to the very fast changing market, offer something extra to the customers – and that is knowledge. We participate on trade shows and technical conferences, we publish dozens of technical articles and running our traditional Endrich News, but there were no practical, touchable, physically manifested evidence of our competence in product design. That is what changes now by releasing our own design of an IoT computer and a complete hardware and software ecosystem around it.

As Endrich was always well known about its perfect sensor line, we have a leading manufacturer of communication modems behind, and one of the first RISC-V based MCU in our portfolio has won the innovation prize of Embedded World 2020, everything is given to create an own single board computer with the capability of sensing, controlling and communicating over narrow band GSM networks – which are the major requirements of a fully featured IoT device. However Endrich did not did not stop here, dozens of external peripherals, such as wired and wireless sensor extension boards, display boards have been created. The IoT ecosystem cannot exist without software services. Although our SBC can communicate through several protocols (MQTT, UDP etc.) to well-known database providers such as Microsoft's Azure, we thought simplicity is a major factor, therefore we also created our own Endrich Software Ecosystem, the Endrich Cloud DB system and the Data Visualization Gateway. These services thus can be offered free to use for our customers. As Endrich is about to enhance serving its customers, and our primer goal is to support components sales, we release all the knowledge about this hardware development in a book "Connecting conventional devices to make them SMART – The E-IoT Concept", where the complete hardware and software concept is detailed written. Not only the used components are introduced, but also the way to interface different sensors to an MCU, to realize power domains, to use GSM communication - and to build a single board computer at the end - are detailed through dozens of chapters.
The E-IoT ecosystem is intended to be used as a demo system for boosting component sales at first, but we are targeting a second - and on long term even more important – stage: to use this ecosystem as an evaluation platform of customer driven product development. With the E-IoT SBC in the middle as a basic platform, we can develop customer required unique functions on an extension board and using the Endrich Cloud System and the Visualization gateway all functions of a finished product can be realized, developed and tested . All the software can be written, all the hardware functions can be built, and only the last stage remains then, which is the industrialization: miniaturization and approval process. The SBC can also be used as a finished product already now, with the help of it, one can connect conventional devices to the Internet, making them SMART devices, which are able to report their operational and environmental parameters to a cloud database. In this way special services such as online status reporting or predictive maintenance can be supported.

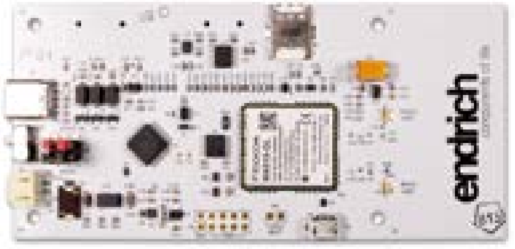


Image credit: Endrich

SBCs provide the key to Industry 4.0

The popular image of the industrial shopfloor is of conveyors passing components and subsystems down a fixed production line. Since the days of Henry Ford, it has been the metaphor for high productivity in manufacturing. However, it is one that is notoriously inflexible. The static nature of the fixed production line makes it hard to customise products and to reschedule operations to produce different products as demand changes. Industry 4.0 breaks down the production line, providing the opportunity to make manufacturing a far more flexible, cost-effective and sustainable operation than has ever been possible before.

There are several key components to Industry 4.0. One is to replace the single fixed production line with cells that can be dynamically reconfigured down to the level of individual orders. It may use automated guided vehicles (AGVs), robots, conveyor segments and automated manipulators to move components and subsystems around the factory to where they are next needed. To facilitate this smarter approach, each product is tagged. Staff, machine tools and robots use that information associated with the tag to determine what needs to happen next on the product's journey through the facility. Even the cells themselves, which could consist of several machine tools and robots, may be virtual in that they can be dynamically assigned to other cells based on demand.
Secondly, machine tools interact with each other using the ubiquitous connectivity associated with an Industry 4.0 plant. The systems employ a combination of wired and wireless networking technologies to exchange information in real time with each other and with distant cloud servers. Those remote servers can use their powerful computation capabilities and Artificial Intelligence (AI) to schedule the shopfloor systems in smarter ways.

Finally, sensors track the status of everything on the shopfloor. RFID readers pick up information from each product using its associated tag. Vision and chemical sensors check the progress and quality of the product at each step so that repairs can be made before it is too late as well as to guide maintenance. If the surface finish of a product is found to be moving out of specification, for example, it indicates a potential problem with the upstream machine tools or the raw materials. By recognising these situations quickly, the Industry 4.0 factory avoids waste and the costs it incurs. The result is a manufacturing environment where products can be customised down to the per-unit level based on customer demand and one that can quickly switch schedules if a key source material is in short supply or if the customer-ordering systems indicate a change in ordering behaviour.

A new generation of single-board computers are now available that support industrial use; developed for and increasing adopted to smarten manufacturing facilities and support the move to Industry 4.0. Although Industry 4.0 introduces novel ways to restructure the factory, manufacturers do not have to replace everything, and SBCs can be adopted to drive new benefits in a range of ways.

Couple SBC-based computing with industrial networking

Manufacturers can leverage existing investments in the machine tools and production automation they already have to deliver significant benefits. Many of the machine tools already in use can be adapted for the Industry 4.0 environment as long as they are augmented with additional levels of communication and intelligence which can be done economically, and effectively with SBCs. Indeed, there may be no need to replace the programmable logic controllers (PLCs) that provide the instructions needed to carry out the operations that each machine tool provides. Many fieldbus protocols have been adapted to work over industrial Ethernet to ensure commands can be relayed to and from a nearby compute module. One possibility for integrating this functionality into both existing and new machine-tool panels lies in the Kunbus range of DIN-rail compatible Revolution Pi modules, an open-source industrial PC based on Raspberry Pi. These combine the compute power of an Arm Cortex-A processor with Ethernet connectivity plus expansion for sensor feedback through a range of I/O modules and fieldbus interfaces.

Image processing and machine learning for quality control

Industrial Shields, a leading European manufacturer of industrial automation devices, uses the Raspberry Pi platform to provide another option for implementing smarter, more flexible PLCs. One application for this generation of higher-performance PLC lies in the coordination of movements of subsystems and materials around the factory. A USB connection can provide the interface to a barcode reader or RFID scanner that picks up the tag on an incoming pallet or product carrier. A display connected using HDMI can be used to provide confirmation to an operator assigned to check its operation. When the package is confirmed, the Raspberry Pi-based PLC uses industrial networking and I/O connections to activate motors to move the package through a series of conveyors to its destination. Alternatively, it may communicate a route to an AGV that picks up the product and delivers it. When the first cell has processed the product, the PLC can then act to guide it to its next destination or pass control to a motion-control PLC that is closer.

A key advantage of using hardware such as the Raspberry Pi is its future upgrade path. Many of the existing industrial-control solutions are based on the third-generation module but products are now being built around the latest iteration of the hardware: the Computer Module 4. The increased processing power of the module, which is based on a quad-core Arm Cortex-A72 processor attached to up to 8GB of high-speed DRAM and 32GB of eMMC non-volatile storage.

The level of performance available in the Computer Module 4 can support intensive machine-learning and vision-processing applications. In addition, as the Computer Module 4 runs Linux, the many tools and development environments on that platform (such as Tensorflow, PyTorch and OpenCV) provide easy access to highly sophisticated techniques for analysing components and subsystems to check they meet quality standards. Subtle changes in colour or surface composition that AI can identify means alerts can be sent to upstream supervisory systems to take corrective action.

The supervisory systems can also harness the processing power of Intel's ecosystem. Intel's NUC family includes models that scale up in cost-effective performance to processors such as the i7-8665U, a quad-core device that can run at several gigahertz. The NUC boards and systems are highly suited for use as supervisory systems. Multi-channel video connections provide the ability to run several displays at once. NUC-based computers can therefore provide a high degree of local intelligence, reacting to alerts generated by PLCs and other SBCs on the shopfloor and sharing graphical updates with shopfloor staff so they can see if problems are building up that require their attention.

Equipment monitoring and information analysis

At the other end of the scale, flexible processes need responsive, easily programmable low-level control. This can be delivered, for example, by the Arduino platform, a combination of microcontroller-based hardware and an optimised software-development environment that supports rapid prototyping and algorithm evaluation. The Arduino Pro Portenta provides a low-cost but powerful option by using a dual-core pairing of the Arm Cortex-M7F and M4F processor cores, both of which support integer and floating-point arithmetic. This makes the Arduino Pro Portenta suitable for the execution of mathematical models and closed-loop control algorithms.

For greater performance in a compact package, the DFRobot LattePanda couples an Arduino-compatible microcontroller with an Intel quad-core 1.8GHz processor able to run Windows 10. Using this combination, the SBC can perform tasks such as AI-assisted equipment monitoring as well as image processing and computer numerical control (CNC), making it highly suited to building customised machine tools.

BeagleBone AI provides a further option for adding support for machine learning, smart sensor and image processing in real time. By using a variety of sensor modalities, it can provide access to non-destructive testing in real time coupled with equipment monitoring. The onboard dual-core Arm Cortex-A15 running at 1.5 GHz works with a pair of TI C66 digital signal processors and four Embedded Vision Engines with support for TI's deep-learning software.

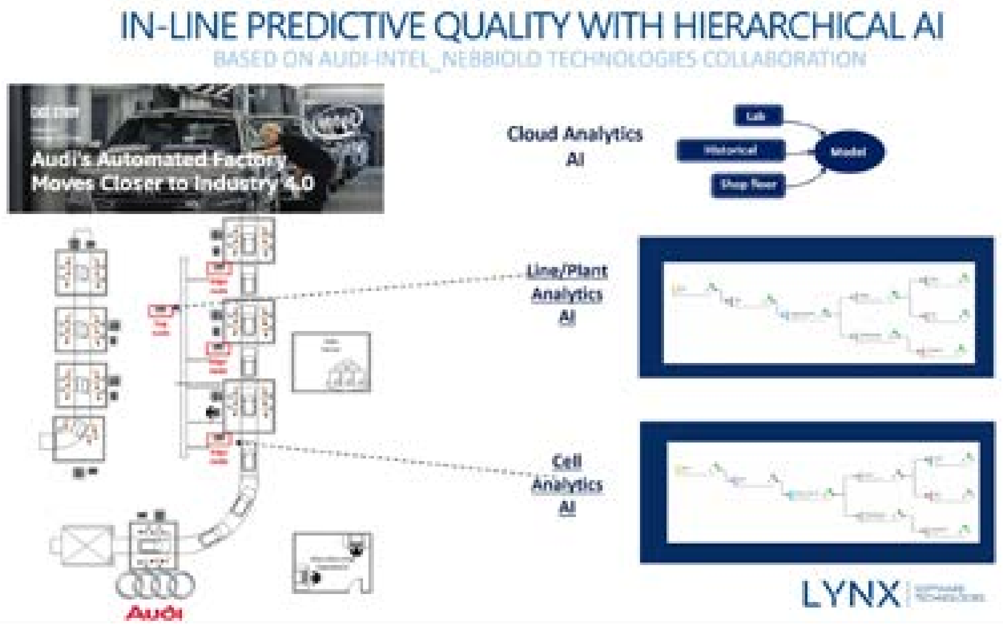
AI and MV combine to improve Quality and reduce Costs in Automotive Manufacturing

Artificial intelligence (AI) is proving a game changer in ensuring the quality of automotive components, which are complex, price sensitive, high volume and frequently safety-critical. By pairing it with Machine Vision (MV) it has become possible to inspect every part coming off the line – something that was neither economic nor practical using human operators. This enables a camera feed to be reviewed in real-time and have faulty widgets identified and tagged either physically or virtually. In this article, I will look at two pioneering installations, and point to the lessons that they offer in terms of realising these benefits in the context of a safe and secure connected IT environment.

100% inspection of welds by Audi

One of the pioneers was the Audi A3 line at its Neckarsulm plant (**Figure 1**). This site has 2,500 autonomous robots on its production line. Each robot is equipped with a tool of some kind, from glue guns to screwdrivers, and performs a specific task required to assemble an Audi automobile. Audi assembles up to approximately 1,000 vehicles every day at the Neckarsulm factory, and there are 5,000 welds in each car. To ensure the quality of its welds, Audi performs manual quality-control inspections. It is impossible to manually inspect 1,000 cars every day, however, so Audi uses the industry's standard sampling method, pulling one car off the line each day and using ultrasound probes to test the welding spots and record the quality of every spot. Sampling is costly, labor-intensive and error prone. So the objective was to inspect 5,000 welds per car inline, and infer the results of each weld within microseconds.

A machine-learning algorithm was created and trained for accuracy by comparing the predictions it generated to actual inspection data that Audi provided. The machine learning model used data generated by the welding controllers, which showed electric voltage and current curves during the welding operation. The data also included other parameters such as configuration of the welds, the types of metal, and the health of the electrodes. These models were then deployed at two levels, firstly at the line itself and also the cell level. The result was that the systems were able to predict poor welds before they were performed. This has substantially raised the bar in terms of quality.


IN-LINE PREDICTIVE QUALITY WITH HIERARCHICAL AI
BASED ON AUDI-INTEL_NEBBIOLO TECHNOLOGIES COLLABORATION
Audi's Automated Factory Moves Closer to Industry 4.0
Cloud Analytics AI
Lab
Historical
Shop floor
Model
Line/Plant Analytics AI
Cell Analytics AI
Audi
LYNX

Digital transformation at Bosch

Another major name in the automotive industry, Bosch, is trialling a similar approach. In partnership with Lynx Software Technologies, Bosch VHIT, the vacuum & oil pumps manufacturing subsidiary of Bosch, is testing a new proof of concept camera-based quality program for use with real-time decision making in industrial settings. The move is part of Bosch VHIT's digital transformation of its processes and product development. The program captures data from cameras on manufacturing plant floors and logistics warehouses and harnesses machine learning algorithms to identify quality issues and feed information into the MES system, in order to generate an optimal decision in real time.

When securely connected to the cloud, the system benefits from continued access to advanced artificial intelligence algorithms and data analytics packages. Since these systems are critical to the manufacturing process, they need to be protected against hacking and the malfunction of another program running on the same hardware. By partnering with Lynx, Bosch VHIT was able to close the digital feedback loop that is reliant on capturing quality images and analyzing the data to provide a safe real-time action. The LYNX MOSA.ic for Industrial product enables the program to run multiple functions on a single SoC without compromising performance, security or safety. "As we continue advancing cutting-edge technology applications for factory automation, we are excited to partner with Lynx to accelerate a new, secure IIoT-based quality system for the market," said Riccardo Sesini, Digital Transformation Manager, Bosch VHIT. "In increasingly connected manufacturing environments, manufacturers require safe, versatile, and resource-conserving solutions. Lynx has a long history of robust, safety-critical, high-availability systems and was the obvious choice to help us realize this latest program in a safe and scalable way."

Securing the new infrastructure

Central to the success of both installations is the collection and processing of data relating to a mission critical process at the edge (i.e.: on the production line) rather than in the cloud, so that adjustments to the process can be made in real time. For these new manufacturing quality systems, the LYNX MOSA.ic for Industrial framework is focused on ensuring security and mitigating any period of equipment downtime that could impact business output. It provides a software platform that can run the inference engine and control functionality on the same platform, ensuring that these applications are appropriately isolated and allocated the right hardware permissions (and nothing more) to perform their tasks. A camera might highlight an issue; then a soft PLC can then connect to the line and make appropriate process improvements. We call this infrastructure the mission-critical edge. The Lynx framework consolidates mixed criticality workloads running on the same multicore processor - the resources and performance provided by the hardware platform, and the capability of the software components. At the same time, it completely isolates critical applications from non-critical workloads, in order to provide high levels of immunity to the former from cyber-attacks. Additionally, this greatly reduces the architectural complexity, cost, and number of points of failure - a critical factor in ensuring business resiliency. Many manufacturers are exploring better ways to proactively and continually improve quality. Whilst these approaches may generate some false positives, this is much better than failing parts making their way to end customers. As the algorithms improve, the incidence level of those occurrences will reduce. The combination of AI and MV is significantly more effective than batch testing, which is used to manually and retrospectively trace faults back to the manufacturing environment and workers to understand root causes and make changes to processes. However it is important to appreciate that this approach relies on the availability of robust edge solutions for the connected camera-based quality system that enable real-time responses to be delivered to events while ensuring critical applications run reliably and safely alongside other functions operating on the server / gateway hardware.

Effective Remote Thermal Management of Electrical Systems

To operate reliably and safely in remote locations, industrial automation systems and other electrical installations need their thermal status to be fully and constantly monitored.An abnormal increase in temperature is frequently an early indication of a fault condition and needs to be addressed before the system is damaged or worse still, combusts.

Increases can take the form of individual 'hot spots' where parts of a panel or individual components are operating close to or above a safe temperature and rises in the ambient temperature. The first can be due to a fault condition, such as a short circuit, or by a component such as a transformer running at peak load for lengthy periods. The second can be caused by the operating environment (prolonged exposure to intense sunlight), or a failure of cooling components such as fans. Both are a threat.

Maintenance by IoT

The goal of maintenance over the Internet of Things (IoT) is always to ensure "zero down time" and eliminate unforeseen device failures that can lead to serious accidents or unplanned facility stops.

To achieve this, the temperature of every panel in a plant as well as the surrounding ambient temperature needs to be monitored continuously using appropriate sensor solutions. Real-time remote monitoring in this way ensures that the need for site visits is kept to an absolute minimum. Sometimes the fault can be rectified remotely, perhaps by reducing power demand from the system to allow key components to cool. Other times an engineer site visit is needed, for example to replace a faulty component or to repair a short circuit.

Monitoring of the temperature of the whole cabinet in which the system is housed is essential but by itself clearly insufficient: a component can be running dangerously hot and be in danger of meltdown or combustion without affecting the overall temperature of the system. On the other hand, attaching an individual temperature sensor to each electrical component is completely impractical – a wiring loom for example can develop hotspots almost anywhere. New wide-angle thermal image sensors that can detect hotspots in large areas of a system such as a whole panel, provide a great starting point for the truly effective remote thermal management of electrical systems. Complemented by ambient temperature sensors and air velocity sensors to verify the correct operation of cooling fans, they can provide a complete IoT based thermal monitoring and remote maintenance solution.

Wide-angle thermal sensors

New infrared thermal sensors with a wide viewing angle in a compact body highlight hotspots anywhere in their field of view, filling the gap between taking an 'average' value of the temperature of the whole system and taking a reading of the temperature at one or two selected points (**Figure 1**). Omron D6T MEMS thermal (IR) sensors measure the surface temperature of objects without touching them using a thermopile element that absorbs radiated energy from the target object. Incorporating a state-of-the-art MEMS thermopile, custom designed sensor ASIC and signal processing microprocessor and algorithm into tiny package, the D6T is believed to offer the highest signal-to-noise ratio (SNR) in the industry.

Image credit: Omron

This ensures clear, reliable measurements that can readily be interpreted by the system. A key advantage of the integrated signal processing microprocessor is the fully linear output. By pre-processing the signal on the module, the D6T converts the sensor signal to a digital temperature output giving a straightforward interface to a microcontroller, simplifying the system integrator's task. Alternative devices do not provide a temperature output, so the designer needs to implement a signal processing algorithm to convert the output to temperature.

The space saving design of the D6T, at only 14 x 8 x 8.93 mm for the largest 32 x 32 element version, makes it exceptionally well suited for installation in a panel or system. Its field of view of 90.0° by 90.0° encompasses an area of 200cm x 200cm from 1 meter distance, providing contactless measurement of temperatures of 0-200ºC in ambient temperatures of -10-70ºC. For smaller systems requiring a more restricted field of view, a suitable alternative is the 1x8 D6T-8L-09H or the 4x4 D6T-44L-06H, offering 54.5° x 5.5° and 44.2° by 45.7° respectively. At 1 meter distance; the field of view of these devices is 10cm x 103cm and 81cm x 84cm respectively. There is also the single element Omron D6T-1A-02 which has a viewing angle of just 26.5° x 26.5° translating to an area of 47x47cm at a distance of 1 meter, giving a highly directional characteristic.

Ambient temperature

Whilst these sensors will identify specific hot spots, there remains a need to monitor the ambient temperature of the system as a whole. A high ambient temperature can be the reason why parts of the system are threatening to overheat and can by itself cause it to malfunction. Compact multi-purpose environmental sensors make it very easy for the designer to deliver a wide range of measurement functions including temperature, humidity, air quality, light, barometric pressure, noise and acceleration from just one small sensor. Sensors like the Omron 2JCIE provide the capability to monitor all of these and provides data via popular wireless and wired data interfaces like Bluetooth and USB. Despite its compact size, 2JCIE features its own embedded memory for data logging to keep track of the surroundings.

Monitoring of cooling systems

Increases in ambient temperature can, of course, be caused by degradation or even failure of the cooling systems such as fans. These need to be maintained, like every other component and monitored continuously in real time to ensure that their performance has not dropped below the required level due to wear or to a buildup of dirt in the airway.

Suitable sensors are available to help with this task. Omron's D6F-PH digital pressure sensors for air flow and clogged filter detection in heat recovery units do this by detecting the differential pressure upstream and downstream of the fan or filter, detecting the degradation in performance as it becomes clogged with dirt and providing an alert when cleaning or replacement is required. The Omron D-6FV can improve efficiency by monitoring the exact air rate at which air is extracted by the fans.

Conclusion

Maintenance engineers should be able to carefully monitor the thermal status of a panel in real time without needing to open the panel door. A combination of the three types of sensors described in this article fully achieves this goal. Wide angle IR sensors identify hot spots wherever they occur on a panel; ambient temperature sensors monitor the overall temperature of the cabinet while air flow sensors verify that the cooling fans are operating correctly. The real-time output of these sensor solutions can then be analysed with algorithms, deskilling the maintenance process and allowing personnel to identify a fault and react in real time. By tracking temperature changes over time, predictions can be made allowing maintenance to be scheduled to maximise engineer productivity and minimise downtime.

High Availability with Secure Remote Control Connections

IT security is by no means a new topic. For a long time now, administrators of IT networks have tried to ensure a high level of security in their networks. But until now, little consideration has been given to OT networks, i.e., automation networks, or indeed the remote control connections used here. This needs to change, and the sooner the better. Against this backdrop, it is not surprising that many of those responsible are unsure in terms of the measures necessary to protect connections to the water management structures and yet still meet the rapidly changing functional requirements of operational management. The implementation of IT security must not make operational management more difficult; rather, it must be considered an integral part of any future concept – keyword: Water 4.0. To this end, the German DWA and DVGW water associations are working intensively on the issues of IT security and digitalization. Specially established working groups are highlighting the various issues and support is being provided, for example through the industry-specific standard "B3S Water/Wastewater" and the DWA specialist publication "Digital Transformation in German Wastewater Management". Anybody wondering why this is necessary only has to read the latest press releases about successful attacks on companies to find the answer. The cyber attacks they describe and their consequences run counter to the requirements on the availability of water management facilities to maintain the security of supply for citizens. Discussions with IT Security can therefore be seen as being a new part of plant maintenance. The latest attacks underscore that the size of a company is not what makes attackers interested in a company. The majority of water management companies in Germany belong to the category of small to medium-sized enterprises (SMEs), and they are responsible for the water supply and wastewater treatment in their respective area.

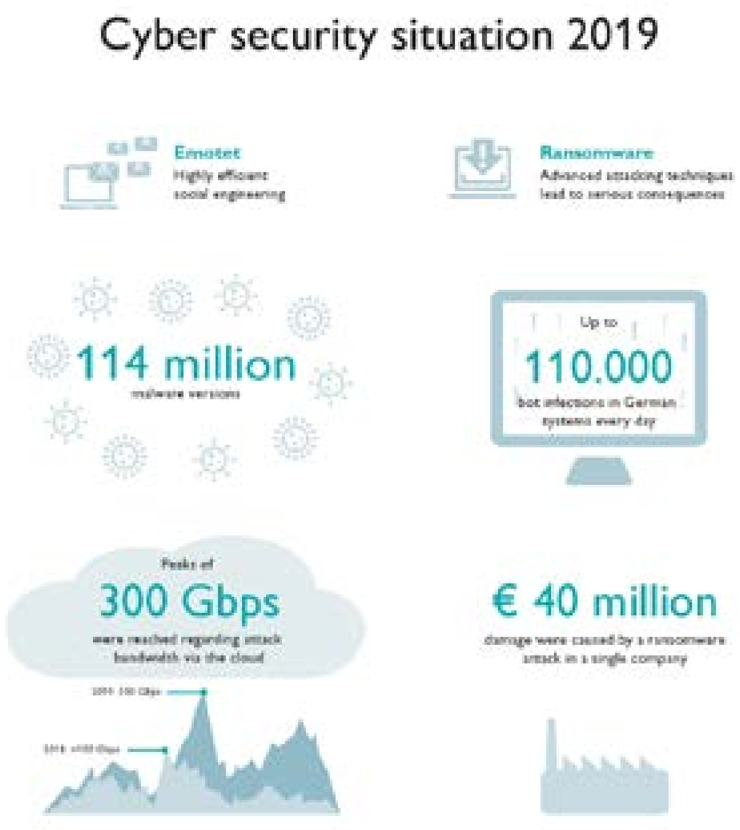


Image credit: Phoenix Contact

Technological requirements

This article will consider the OT networks for automation and, in particular, the state-of-the-art and secure networking of buildings – also known as remote control technology. Here, the focus is on the technological test of the connection in terms of IT security. Additional aspects, such as personnel and organizational measures, can be only be considered as part of a risk analysis focusing on the respective plant. So, which general technological requirements need to be met when connecting a remote station? Criteria such as an uninterruptible power supply and surge protection are clearly a part of any concept for realizing high availability, but are not the subject of this article. The following basic requirements have to be met:

- Power supply
- Surge protection
- Securing the remote control technology against unauthorized access
- Protecting the data connection between plants
- Encryption
- Anomaly detection

Moreover, the operator should take into account the fact that different conditions and technologies require different protection concepts. These considerations are taken into account below for the connection types listed:

- Coupling remote structures via cellular communication
- Networking remote structures via license-free wireless solutions
- Integrating remote structures via dedicated remote control lines.

Coupling via cellular communication

A large number of decentral stations have been coupled to the supervisory control room via cellular communication over the last few years. During transmission, the data can be protected by using a VPN tunnel (Virtual Private Network). In the future, the starting point of this tunnel should come directly from the remote control station (automation device), and not from an additional upstream device. This is already a normative requirement in the power industry. Moreover, the data must be encrypted during transmission to prevent eavesdropping and manipulation. Ultimately, private APN network cards (Access Point Name) should be used that allow a virtual network to be set up with its own IP address within the network of the cellular communication provider. Access control within the structure provides protection against unauthorized access and is therefore a key part of data security. Furthermore, users should have to authenticate themselves to the remote control system as part of an assignment of rights. Individual network sections must be separated from each other and open interfaces must be disabled. A firewall at the central Internet connection in the central plant protects the data connection. Network segmentation and the separation of IT and OT networks is also recommended here. A virus scanner updated daily identifies malware, while anomalies in the network can be detected via appropriate monitoring – for example IRMA. This will report if a device within the network is subject to unusual data traffic, for example.

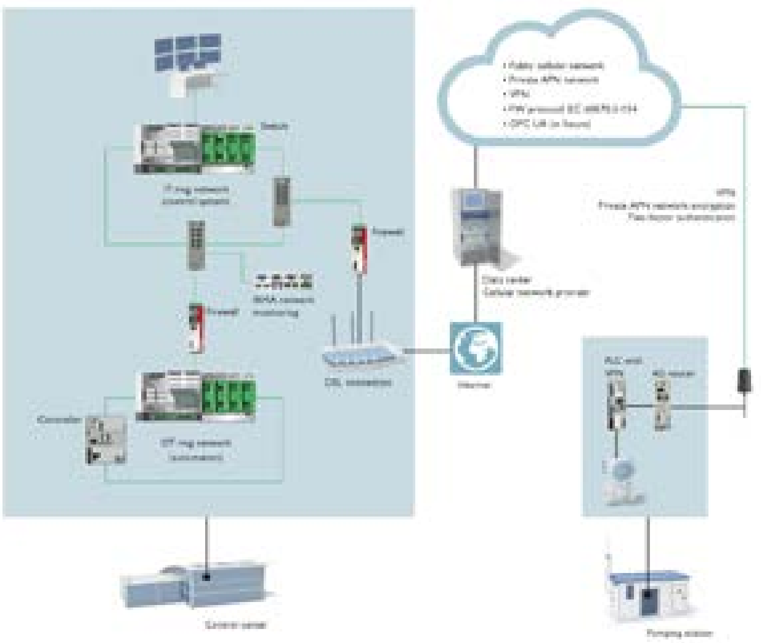


Image credit: Phoenix Contact

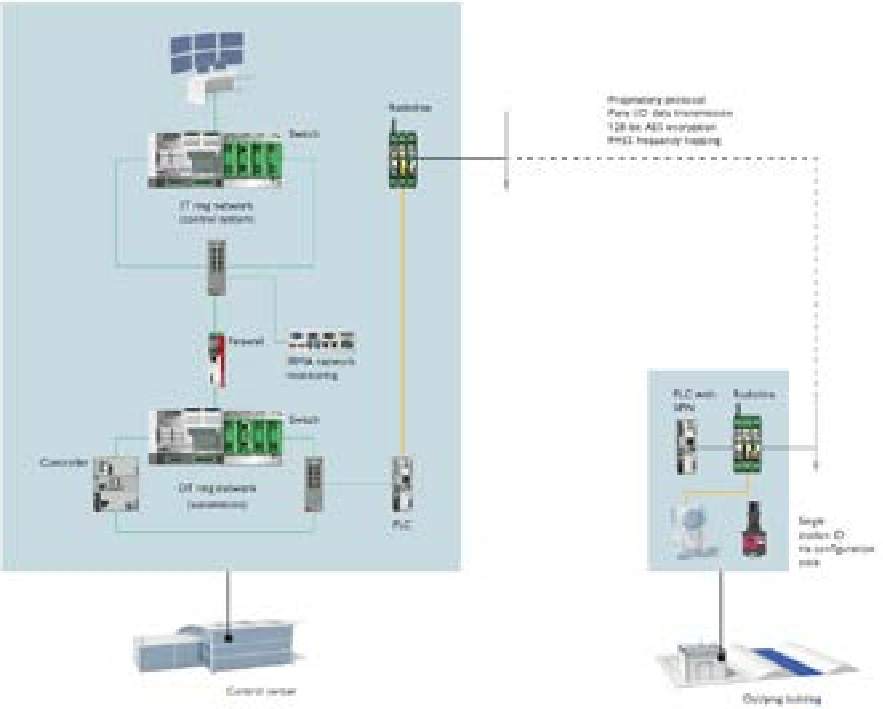
Networking via a proprietary wireless technology

Networking via a proprietary wireless technology – such as the Radioline system from Phoenix Contact – is another option for connecting external stations that combines the advantages of wireless communication with those of a company-owned network. The data should also be encrypted during transmission to prevent eavesdropping and manipulation. Moreover, proprietary protocols with bit-wise data transmission are not open-source, which also makes unauthorized access more difficult. To secure data in the decentral structure, the structure should have access control. Moreover, a unique station ID prevents a device from being replaced or an additional station from being added to the network if the hardware stick is not located on site. In the central plant, the data connection is also protected via network segmenting and the separation of IT and OT networks. Communication in the control engineering system is via a head station in the OT environment. Moreover, it is also advisable to install a network monitoring system in the system network that detects anomalies, such as data transmission between two devices that have so far never communicated with each other.

Integration via dedicated remote control lines

In the drinking water supply industry, remote structures are often connected to the supervisory control room via dedicated remote control cables. This is often assumed, incorrectly, to be an island solution that does not have to be secured against unauthorized access. It does in fact need to be secured, but what technical measures need to be taken to secure the connection? During data transmission, the VPN tunnel is also a suitable approach that should be set up directly from remote control system (PLC) to remote control system (PLC).

Image credit: Phoenix Contact



Data encryption is also a must to prevent eavesdropping and manipulation. This is because there is always the possibility that the dedicated cables can be tapped – whether in the remote structure or along the route on the roadside distributors. Such tapping can be used to install malware within the central control engineering system, even with a supposedly secure communication concept.

As already stated, the data connection in the structure can be protected via access control and user authentication in the remote control system with individual rights allocation. Segmenting network sections and disabling open interfaces are also useful protective measures. In the central plant, a firewall should be installed at the remote control line inputs to protect the data connection. Network segmenting, separating IT and OT networks, and anomaly detection via network monitoring are again useful in this case. And finally, a remote control head or a firewall is recommended as the peer for the incoming VPN tunnel.

Support from the specialists

What, then, are the most important points that the operator should consider when planning the remote control technology? Wherever possible, an open communication standard should be used. Future requirements will only be able to be satisfied by state-of-the-art solutions that are easy to extend. IT security must play a central role in all activities. For visualization, web-based systems are the best approach.When setting up the remote control technology, networks should be segmented systematically. A VPN tunnel is to be established from the remote control system controller. Moreover, the firewall has to be configured correctly, the delivery passwords have to be changed, and graded user rights issued. Once the remote control technology is in operation, regular system updates, regular data backups, and virus scanners that are updated daily are of importance. Employees must be trained and continuously involved in the security process. Moreover, a risk analysis must be performed regularly to safeguard the security concept effectively against the latest threats. The security specialists at the Services Center of Excellence at Phoenix Contact will be happy to provide support in developing the respective measures. In these times of limited opportunities for in-person contact, they are also available in an online Q&A session.

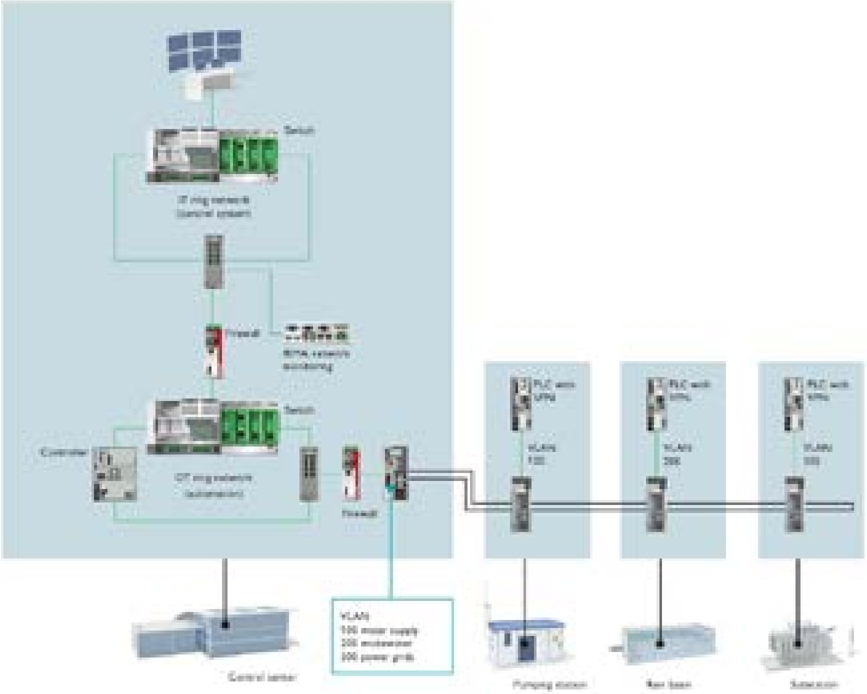


Image credit: Phoenix Contact

5G Technologies: Improving the Rail and Transport Expericnce

Mandated lower CO2 emissions, demands for cleaner air, and increasing urban population densities are key drivers in the phasing out of fossil fuel usage (particularly diesel) and the push for further electrification of railway and traction applications.

These trends present unique opportunities for technological solutions from traction providers that could effectively future-proof an expensive asset with a likely lifespan of thirty years or more. These opportunities are largely enabled by 5G and its key features, including enhanced mobile broadband (eMBB), ultra-reliable low-latency communication (URLLC), and massive machine type communications (mMTC). Each of these features plays a role in the traction vehicle of the future.

Electrification and Smart Grids

Traction applications place significant demands on electrical grids. These demands for electrical power tend to spike at specific times of the day, typically in response to rush hour traffic. This power demand can be accurately estimated for each locomotive connected to the grid using a vehicle-to-everything (V2X) connection. The V2X connection can accurately instruct the grid to provide sufficient power for the locomotive, ensuring a balance between power supply and demand. Artificial intelligence can use this information to help electricity providers to accurately estimate demand, deploy adequate power energy storage solutions, and have sufficient charge to meet the grid demands at peak times.

5G and Industry 4.0, Sensors and Machine Learning

Temperature, pressure and motion sensors monitor the state of the motors and wheels, ensuring safe and reliable operation. Condition-based monitoring is a recent development and requires high-precision vibration sensors connected to suitable analog front-end circuitry, as well as analog-to-digital converters (ADCs) that generate large amounts of data. Monitoring this valuable data on the wheels and motors plays a vital role in scheduling train component maintenance. MEMS sensors, together with analog front-ends and precision converters from Analog Devices, can be used to build the necessary sensors for condition-based monitoring.

Due to the size and nature of the data gathered from the sensor, it is not suitable for processing at the sensor node, as it requires too much computing power and memory. It must be sent to the cloud, where all the data from each connected train can be fed to a machine learning algorithm. This data is then compared against the data of a "digital twin," which is a term used for a virtual model that serves as a real-time digital counterpart of an object, process or system.

The rail system's digital twin will alert the maintenance company of the likely time and nature of a fault in the locomotive or carriage. This predictive fault-finding is considerably less costly (from both financial and reputation perspectives) to the traction system operator than unexpected shutdowns for maintenance and repairs. Data can be connected to the grid using the new narrowband IoT (NB-IoT) standard enabled by cellular modules from technology providers such as Sierra Wireless, u-blox and Fibocomm, and it can be processed in the cloud using cloud-based machine learning solutions from companies such as Microsoft Azure, AWS, Google Cloud Platform and Bosch.

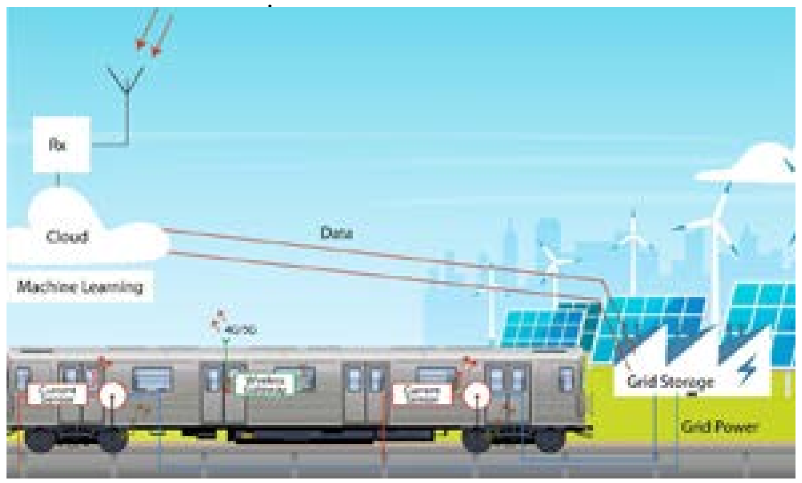


Fig. 1: Wheel, sensor, conditioning, gateway and antenna to cloud |Image credit: Richardson RFPD

Vehicle-to-Everything (V2X) Communications

It is difficult to overstate the importance of safety in traction applications. Vehicle speed management and maintaining safe distances between vehicles are just two examples of critically important measures that ensure passenger safety and mobility. Vehicle-to-everything (V2X) communication enables a train travelling at very high speed to do so with the full knowledge of the location and speeds of the trains ahead of it. This can greatly improve passenger safety—and safely permits greater train volumes and reliable schedule updates. The ultra-reliable low-latency communication (URLLC) of 5G (<10 ms) in comparison to 4G systems (>50 ms) enables this, and devices such as the Sierra Wireless EM9191 5G router module is a good example of a compatible unit for the 5G standard. Passengers wanting live timetables can also check the location, predicted arrival time and nearest station for the next train to their desired destination, avoiding frustration and unnecessary delays.

Connectivity Applications for Transport

One of the main attractions of rail travel for passengers is the ability to use internet-connected devices for work and email while on the move. Other passengers want to enjoy on-demand entertainment from providers like Netflix or Disney. These streaming services create a bottleneck for 4G to Wi-Fi routers, and railway operators generally block them.

The enhanced mobile broadband (eMBB) of the 5G new radio (NR), with downlink speeds of approximately 700 MB/s, would generally permit most passengers of a train carriage to enjoy high-quality streaming with little or no noticeable buffering. Millimeter wave improves on this with data rates as high as 5 GB/s.

Antenna Selection

The right antenna is key to the achievement of good radio performance. Rail applications are long-lived and require a robust antenna that covers a wide frequency range. The antenna will need to support GNSS and 5G NR bands. An antenna with suitable gain will ensure maximal coverage and simplify the architecture and/or power requirements of the power amplifier stage. The antenna will need to be securely mounted to the roof of the carriage or locomotive and be suitable for outdoor use. Richardson RFPD can help identify antennas that support the 5G band n78 and GNSS bands as well as meet all other RF requirements. For example, frequency range can be traded for gain and efficiency, depending on the application.
In addition to antenna performance considerations, the antenna may need to be qualified for the demands of rail applications and to meet the standard for electronic equipment used on rolling stock, EN 50155.
Good antenna selection maximizes first pass success and minimizes costly iterations.

Security and Safety

Passenger safety is a key factor in encouraging the repeated use of public transport. From avoiding overcrowding to enabling security cameras, 5G will play an important role.The increased bandwidth and lower latency of 5G will allow railway operators and security services to have real-time video monitoring of any potential threats, and a passenger can alert authorities more quickly to such threats, facilitating faster responses. This improves the reputation and adoption of public transport and contributes to smarter and more liveable cities.

Conclusion

The transformative nature of 5G—with its vastly increased data rates, lower latencies and abilities to handle a greater number of users and nodes—means it will have profound implications for traction applications. 5G has the additional benefit of being a worldwide standard, which simplifies development and certification. It also simplifies deployment, along with already-available embedded SIM cards (eSIMs). Additionally, the growing trend of free firmware over-the-air (FOTA) allows users to easily keep software up-to-date with the latest functionality and security features.

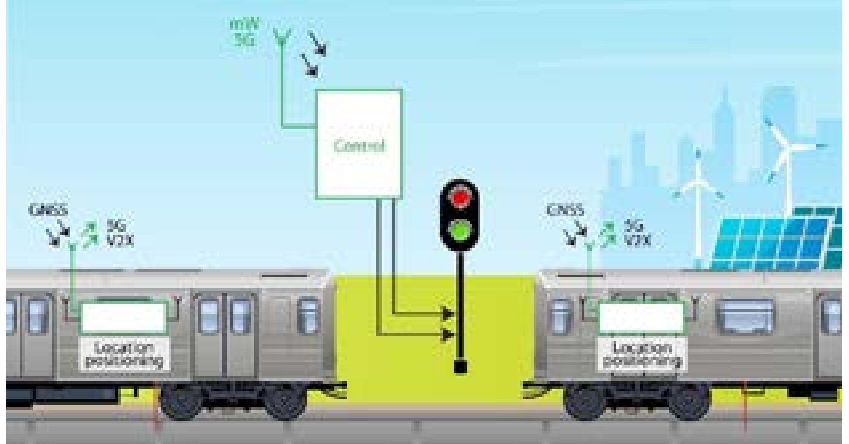


Fig. 1: Separate locomotives to infrastructure (V2X diagram)
Image credit: Richardson RFPD

The challenge of powering Industrial IoT Applications

The hype around IoT devices nowadays is not surprising. IoT engineering kits and the appropriate technologies for designing IoT prototypes are widely available and affordable for creative technology enthusiasts. Consequently, there are no limits for enabling ideas and possible business models based on these technologies.
Also in the industrial environment, there has been an rapidly increasing demand for professional IoT applications. Common characteristics include the ability to distribute intelligence by connecting various sensors and actuators with decentralized control. The ability to make them smart is that these sensors and actuators can collect and communicate data and are designed to be managed with intelligence. The market for industrial IoT applications will continue to expand as more applications evolve, including (home) healthcare, infrastructure, utilities, home automation and smart homes, vehicle, mobility and more. These professional IoT trends will undoubtedly involve miniaturization, mobility, robustness, efficiency (degrees of effectiveness) and the networking of electronic devices.

In contrast to hobby IoT applications, such safety-relevant industrial IoT applications are subject to strict regulations, both, for the engineer and for the components being used. This poses a great challenge for developers of industrial IoT applications. The use of certified, reliable and long-term available electronic components is critical, as they are often used in safety and function-critical applications. The professional support of component suppliers is playing a very important role.

Requirements for powering professional IoT applications

Critical modules within professional IoT devices are without a doubt the power converters and the power supply. Miniaturization, low power consumption, size and a high efficiency are playing an increasingly important role for those products. Semiconductors are probably the components which offer the highest level of innovation. As a second key technology I'd mention the power transformation and isolation devices used in the products. Additionally, since these mostly battery-powered IoT systems spend most of their time in standby mode and only a small part is in active mode, the built-in DC/DC converters must cover a wide load range with high efficiency.

Size and efficiency matter- what else?

In order to design, certify and market such professional IoT devices, not only these technological product features matter. If these professional IoT devices want to be certified and sold, they have to be fully compliant with increasingly stringent regulations through globally harmonized standards and guidelines, which bring a big challenge to today's IoT electrical engineer. If IoT functionalities are required for critical applications such as in medical technology, the electronic components must be designed in such a way that they can be used accordingly, meeting industry specific regulations. As an example, let us take a medical approved, wireless, battery-powered control panel with Internet access to the patient file. Wirelessly connected to this control panel is another device, which may can come into contact with the patient (e.g. a blood pressure monitoring device). One of the key safety concerns with respect to medical devices is that the patient is often electrically connected to the device. As a consequence, the power supply and the DC/DC converter of this IoT application must meet safety critical regulation such as BF compliance and 2XMOPP standards within IEC/EN 60601-1 3rd Edition.

Image credit: Traco Power

Another good example are industrial IoT applications for “smart” homes and buildings. High efficiency & low no-load power consumption (ErP compliant), small size, high reliability and an affordable price are key elements to all these home/building IoT automation applications, and the ever-increasing compliance & standards including IEC/EN 60335-1.

Careful planning is required, with the entire supply chain

We know the use of new technologies in security-sensitive and functionally critical applications requires increased reliability, quality, service life and certifications and - last but not least - seamless traceability of electronic key components.

Manufacturers are more and more in the need to use tools that have been established and perfected in the automotive industry for years, such as failure mode analysis, Corrective actions, 8D Reports, DFMEA, PFMEA, Total Quality Management and continuous improvement).

Today Total Quality has to find its way into the earliest phase of almost every development. To achieve this, a developer today has to do more than just provide a functioning solution. Where a mobile telephone used to be a useful accompanying instrument, today we are increasingly dispensing with redundancy from other means. Cash, camera, address book, subscribers are all integrated into the smartphone. Smartphones are therefore critical life companions today. The product designer today bears much more responsibility for the quality of his development than he did 10 years ago. We all know that this trend not only continues but will continue to develop rapidly. Moreover, suppliers should regard the digital transformation in the individual components’ supply channels as a highly significant development. By establishing, analyzing and processing relevant data, a fast, reliable and economic availability of the components can contribute to increased productivity at the customer‘s facility.

Conclusion

This means that in IoT applications in critical applications, for example in medical technology, building automation or mobility, not only need to be efficient, miniaturized with a ultra-low standby power consumption, they also need to be available for decades, tracable and fully compliant with the relevant standards and regulations.