IU

INFORMATION UNLIMITED

INDUSTRIAL SECURITY

Security in Manufacturing Alarm Management with zenon 15 Years of COPA-DATA Italy

THE COPA-DATA MAGAZINE | ISSUE #27 2015

IU
INFORMATION UNLIMITED

THE COPA-DATA MAGAZINE

ISSUE #27. APRIL 2015

PRESIDENT AND PUBLISHER:
Thomas Punzenberger
Ing. Punzenberger COPA-DATA GmbH
Karolingerstrasse 7b, 5020 Salzburg, Austria
Commercial Register Number: FN56922i
t +43 (0)662 43 10 02-0
f +43 (0)662 43 10 02-33
www.copadata.com

EDITOR-IN-CHIEF: Julia Angerer
EDITORIAL TEAM:
Gernot Bugram, Eva-Maria Oberauer-Dum, Steve Poynter, Nicola Richter, Esther Rutter, Phillip Werr, Bertold Wöss
ART DIRECTOR: Manuela Bacher
DESIGN SUPPORT: Lisa Mitterbuchner
COPY-EDITING: Kristen Kopp

AUTHORS/CONTRIBUTORS: Emilian Axinia, Christian Bauer, Mark Clemens, Maarten van Dam, Christoph Dorigatti, Bernhard Ebert, Lisette Lillo Fagerstedt, Gian Luca Fulgoni, Thomas Glander, Andrea Grall, Sandra Handke, Robert Harrison, Stefan Hufnagl, Young Su Kim, Bernhard Korten, Giuseppe Menin, Hermann Oswald, Louis Paglaiccetti, Anita Perchermeier, Johannes Petrowisch, Thomas Punzenberger, Marco Ramilli, Klaus Rebecchi, Jürgen Resch, Stefan Reuther, Noemi Torcasio, Phillip Werr

PRINT OFFICE:
Offset 5020 Druckerei & Verlag Ges.m.b.H., Bayernstrasse 27, 5072 Siezenheim, Austria,
LETTERSHOP & DISTRIBUTION:
Mailinghaus GmbH Dialog Marketing Agentur, Neualmerstrasse 37, 5400 Hallein, Austria
PRINT RUN: 12,820 copies
FREQUENCY: twice a year

linkedin.com/company/copa-data-headquarters
gplus.to/COPADATA
facebook.com/COPADATAHeadquarters
twitter.com/copadata
xing.com/companies/copa-dataheadquarters
youtube.com/copadatavideos

MIX
Paper from responsible sources
FSC® C106019

CONTENT

CONTACT/
FREE SUBSCRIPTION:

IU@COPADATA.COM
WWW.COPADATA.COM/IU

EDITORIAL

Dear readers,

At the moment, I hear the key words "Industry 4.0" or "Internet of Things" at virtually every meeting. I am happy about that, because these concepts suit us very much. We have been involved with the issues of communication and connectivity in different forms for a long time. Be it with more than 300 connections to controller systems, our gateways to the CIM level and higher-level systems, or our interfaces to SAP or Microsoft Dynamics – zenon is your hub for data acquisition and distribution.

But what about security?

The most secure option is, of course, to remove all drives, to block USB ports and not connect production computers to the network. However, you then have no option but to write down data from the screen – not really what is envisaged with a concept such as Industry 4.0. Anyone who wants to open up a system in order to really benefit from it must look at the issue of security.

The good news is that we, at COPA-DATA, have looked at security since we made zenon network-capable. You can find, for example, user administration and encrypted communication, as well as encrypted storage of data and tamper-proof zenon program files. Many years of cooperation with universities and companies that specialize in security have opened many doors to us, from which you can now also benefit. Of course, even with such refined security mechanisms, you must also be aware that each opening also means a little bit of risk.

We provide you with many tools, so that you can make your Industry 4.0 concepts and projects as secure as possible. Enjoy finding out more in this special security issue of *IU*.

THOMAS PUNZENBERGER, CEO


• Patch Management ✓
• Read IEC 62443 standard
• Install security updates → how?
• Secure USB ports: call Sarah
• What is Social Engineering?
• Encrypt network communication ✓
• Integrate Active Directory:
meet Walter from IT

SPOTLIGHT

OPEN HOUSE?

WHY PEOPLE INVOLVED IN AUTOMATION HAVE TO TAKE SECURITY SERIOUSLY.

PHOTOGRAPHY: BERNHARD MÜLLER, PHOTO DESIGNER FOKUS VISUELLE KOMMUNIKATION

PHOTO LOCATION: KÄRNTNERFRUCHT KFG GMBH, KLAGENFURT, AUSTRIA

Viruses, Trojans, hackers – for a long time, they primarily affected IT systems and private users. At the level of production processes, it was the "analog" security problems that got the attention. Machines might have been networked with one another, but anyone who wanted to spy or sabotage had to at least come in person. A well-sealed and monitored production hall offered more protection against spies and thieves than any firewall. This is now changing fundamentally.

THE PRODUCTION LEVEL is being opened to the outside to a greater extent and at a faster pace than ever before. On the one hand, preparation for the Smart Factory of Industry 4.0 requires direct communication with different areas of the company, and even beyond company limits. On the other, managers want reports, key figures and even access to SCADA level via mobile devices, in real-time if possible. A massive challenge for those involved in automation: areas that were previously isolated from outside needed to be opened up. That sounds like an ever increasing risk. And it is, if communication channels are barely secured or only secured with standard measures. Things happen in production halls that are of great interest to others.

WHY THE FUSS?

Notwithstanding Stuxnet, all major, known attacks have targeted the IT structure or databases of companies. It's easy to dismiss it as a non-issue for SCADA and HMI. But it is an issue. However, attacks on production structures are less well known, sometimes not even discovered. The German BSI (the German Federal Office for Information Security) states the following in its 2014 security report: "Many of these systems were not designed with possible attacks in mind." And this has effects.

The magazine c't, in the March 2015 issue, quotes information from the hacker group "SCADA Strangelove". The group found over one million web interfaces for solar-power plants and wind-power plants online. The passwords of the interfaces are generally easy to crack; the group even managed to overwrite the firmware of one device. In addition, there are programs that are still open to attack methods though weaknesses have been known for ten years. It is no wonder: closing reported loopholes takes an average of 18 months in industrial production. An invitation for attacks? Access to a web interface does not mean that a plant has been compromised. But it is the first important step towards it. But why would someone make the effort?

FROM SCRIPT KIDDIES TO STATE-FUNDED HACKS

There are many motives for getting access to a system. It starts with playful random attacks and ranges through to laboriously-conceived attacks carried out by professionals or even state institutions. The so-called "script kiddies" usually don't have the know-how to attack protected targets effectively. They use known loopholes and automated methods. It is nice for them when they stumble across unprotected web interfaces. They rarely know what they are actually doing. And this is precisely what makes their access to plants via the web dangerous.

Hackers are equipped with more knowledge and criminal energy; their objective is blackmail. Access to a plant simply means cash for them. It could be expensive for the company involved, but they nevertheless find out that they can be attacked and can close the loophole. Hacker groups however focus much more on targeting databases, customer data or internal data of companies.

A significant number of the attacks related to automation take place very quietly and inconspicuously. It is not about quick cash, proving oneself, or fame. It is about monitoring the competition, industrial espionage, gaining advantages for tenders and sometimes even inconspicuous sabotage. Companies who want to improve their standing in the market may be behind this, but increasingly it is also state institutions which want to get advantages for "local" companies. The German Federal Office for Information Security, which aims to protect companies and public institutions from cyber-attacks, has determined in the case of Germany: "The improved technical detection of the German Federal Office for Information Security gave stronger and clear indications of cyber-attacks from intelligence organizations which were attacking industry, research and public administration."[1] This is not just major companies, it also affects SMEs. As suppliers and institutions with expertise, they become targets or even the entry point for attacks on other companies. It does not matter how big or important a company is, but rather how important it is for the attacker. And you can be sure that it is not just Germany that is affected by it.

The Top Ten list of the biggest threats for ICS (Industrial Control Systems) in 2012 included "human error and sabotage" and "allowing access to malicious code via a data medium". In first place was "unauthorized use as a result of remote maintenance access". Different tests by trade journals carried out in 2013 and 2014 also found that there were still many open or badly-protected remote access points in the Internet. Tools that allow maintenance personnel to save themselves long journeys are also an open gate for criminal intruders if the protection is weak.

The following are seen as the main threats for industrial plants:

- Break-in via remote maintenance access
- Infection of controller components with malware via captured office networks
- Allowing malware in via data media or external hardware
- Social engineering
- Human error and internal sabotage

However, you can protect yourself! To an extent.

LOOPHOLES AND BARN DOORS

Technical systems, in particular software, are never completely free of errors. It is a matter of discovering loopholes and using them or closing them – depending on your perspective. Well-maintained IT systems are characterized by having known loopholes closed, being monitored for attacks and malfunctions, and being continually optimized. Networks in automation are normally designed to work as fail-safe and with high availability. The most important rule is that production must not be affected. However, from the perspective of system security, barn doors are opened. Operating systems and programs that are not in line with current security standards are easy prey. And communication that is unencrypted, as is the case with most machine protocols, can easily be uncovered. For a long time, this was not a particularly large problem.

IT is focusing on security: the system must be secure against unwanted access. Automation takes precedence over reliability: the equipment must run without interruption. As long as automation processes cannot be reached from outside, reliability was rightly the main focus. Why should the equipment be affected by a software update that is not important for production? As a result of the opening to the outside world for remote access and even networking with suppliers or customers, these networks are now in a tricky position: they must primarily run without interruptions. But an intrusion into these networks can massively endanger the robustness against a failure of entire production plants. It is thus a matter of ensuring security and reliability to the same degree. Automation experts must acquire or purchase expertise for network security. The task is a major one, but it can be achieved. Firstly, IT in companies has already gained expertise. Secondly, there are special service providers. The IEC 62443 standard is an important first step for greater security in the production network.

IEC 62443 – STANDARDIZED SECURITY

Security needs standards, precisely when sensitive data is to be made externally accessible, and even shared with other suppliers or customers. The IEC 62443 range of standards for "IT Security for Industrial Control Systems – Network and System Protection", which was published between 2008 and 2010, is an important step towards this. It has now been accepted by the European standardization organization CENELEC as a European standard. The range of standards describes the requirements for IT security of industrial automation systems. For each basic requirement, there are system requirements and possibly additional requirements.

For example, the basic requirement "checking usage" is accompanied by twelve system requirements. One of these requires the implementation of authorization. This means that control units can only be used with authorization. This requirement is further enhanced with the granting of authorization according to roles. This means that operating authorization is issued according to the roles of respective users.

The requirements of IEC 62443 can also be used as instructions for targeted, practical measures for the effective safeguarding of the company's internal production. For security workers in charge of production processes, this is certainly mandatory reading – but it is for the manufacturers of HMI/SCADA software too.

TECHNICAL SYSTEMS, IN PARTICULAR SOFTWARE, ARE NEVER COMPLETELY FREE OF ERRORS. IT IS A MATTER OF DISCOVERING LOOPHOLES AND USING THEM OR CLOSING THEM – DEPENDING ON YOUR PERSPECTIVE.

TO DOS

Anyone who opens their production, or parts of it, to access from other systems should first think about how all areas can be protected as much as possible. In order to maximize digital security, all components must be involved. You should most of all keep a cautious eye on the weakest links in your security chain. These could undermine your security measures and cause your stronghold to fail.

You will find weak points inside and out. Externally, a badly-protected partner company could be the gateway. Internally, programs that are not up to date, protocols that have known security loopholes and interfaces or devices in the company network are the most frequent candidates. However, it could also be employees who use weak passwords or who are negligent with their passwords which allow access to your network. Phishing emails or calls from people purporting to be IT employees in order to get access data are also common. You should therefore combine all security measures with thorough training for all employees. The top weak points that you should have in mind are:

1. Insufficient patch management and use of outdated software. Also, devices that are connected to the network and cannot be protected from attacks or can only be protected with great difficulty. This can concern time recording just as it could be the telephone system or even the alarm system.
2. Cyber-attacks using spam emails with malicious code attached or social engineering. These aim to mislead users into executing a malicious program.
3. Attacks via comprised web pages or manipulated web banners that install malicious programs when you visit a web page.
4. Attacks on service providers that lead to customer data being extracted.
5. Carelessness when using mobile devices or apps, as well as divulging personal information.

Demand security as a basic condition for yourself and your digital contacts: anyone who wants access to your network must meet basic security standards, regardless of whether it is people, companies, hardware or software.

Incidentally, focusing on security protects not just you and your company. As a mechanical engineering or plant engineering company, Security by Design can primarily be a valued quality feature for your customers. Ensure that all components that you supply correspond to the latest security standards – each machine, each PLC, each piece of software, each communication protocol and all access possibilities. Companies that place great value on security also make their customers more secure.

For COPA-DATA, security is just as important as reliability. The new IEC 62443 standard is thus already one of our requirements for security. Of course, we also have our programs tested externally for vulnerability and quickly implement recommendations from security experts.

SECURITY STARTS NOW

Seize the moment. Start checking and adapting your security concepts. To do this, you should above all consider the following:

- Plan for additional, qualified staff.
- Regularly analyze your protection needs, rectify known problems and analyze again.
- Provide an appropriate budget.
- Carry out audits for infrastructure in relation to IT security.
- Only open to the outside what really needs to be opened.
- Do not link systems with contact to the outside world with other systems.
- Also implement protection from internal threats.
- Test prevention and reaction plans.
- Carry out regular training sessions to recognize new threat potential.
- Promote an active security culture.

You can find further ideas, news and perspectives on the topic of industrial security in this edition of *IU*:

In the article entitled "An Innovative Smart Factory. Unassailably!" starting on page 12, Stefan Hufnagl poses fundamental questions in relation to security in smart factories. He wants to know how well your production facilities are protected and shows you everything you need to consider before you open yourself to external access or cloud solutions.

We find out from Jürgen Resch and Mark Clemens, in their article entitled "Exposed energy customers?" starting on page 16, that the issue affects everyone, from major energy distributors through to private households. We will find out that smart meters will soon replace the old electricity meters throughout Europe. However, the solutions are not consistent – with consequences for customers and grids.

We already spoke with the Italian cyber security expert, Marco Ramilli, in the last issue of *IU*. We received many questions in response to this interview. Marco Ramilli answers some of these questions in this *IU* starting on page 18. The main focus: attacks at process level. We learn that you must look carefully, because "if your company is connected to the Internet, you'll have a 95 % probability of being the subject of opportunistic attacks."

Work well. Work securely.
Understand to whom you open your house.

RECOMMENDED READING

[1] *https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html*
[in German only]

IEC 62443 standard
http://www.vde.com/de/technik/fs/seiten/informationenzu62443.aspx
[in German only]

c't magazine. March 2015 issue:
Hacker mit Blick auf die Morgenröte.
p. 16-18. [in German only]

Heise Zeitschriften Verlag. iX Kompakt Security 2014. [in German only]

An Innovative Smart Factory. Unassailably!

HOW WELL IS YOUR PRODUCTION PROTECTED?

PHOTOGRAPHY: BERNHARD MÜLLER
PHOTO DESIGNER, FOKUS VISUELLE KOMMUNIKATION

PHOTO LOCATIONS:

KÄRNTNERFRUCHT KFG GMBH, KLAGENFURT, AUSTRIA

COPA-DATA HEADQUARTERS, SALZBURG, AUSTRIA

DISCUSSIONS ABOUT THE security of data have been with us for years. They always – you could say reliably – produce astonishment at how weak points in IT applications are ruthlessly used for attacks and what consequences this can have for people affected. It is only the proverbial tip of the iceberg that attracts the attention of the media and thus the public. Information about the actual consequences of an IT security incident remains often closed to media consumers. No wonder that the spheres of large amounts of data and information networks create a sense of being inherently diffuse and incomprehensible. The often very cryptic portrayal of circumstances and techniques surrounding the issue of data security ensures a certain fundamental skepticism. Key terms such as "Big Data" or "Ubiquitous Computing" thus inevitably induce a particular, almost conspiracy-tainted aftertaste.

However, anyone who wants to use the comprehensive possibilities of modern platforms such as the Internet of Things, cloud computing and distributed cyber-physical systems for innovative development of their products and services will also increasingly have to look at the scenarios and consequences of the system possibly being compromised by an unwanted protagonist.

IMMUNITY IN THE WORLD OF AUTOMATION?

A consistent pattern has become apparent over the years: the distinction between IT and automation technology. This usually entails a specific handling of the issue of security, both in the corporate departments responsible for it, as well as by the providers of ICS (industrial control systems). While comprehensive and permanently-adaptive safeguarding against security risks is an integral component of system operation for IT, in many places automation staff are still looking for a suitable security concept. The fact is that the area of attack has enlarged considerably. The opening of production systems for interaction via the Internet and in the context of the intelligent networks of Industry 4.0 is responsible for this, as is the continued merging of previously separate domains as part of vertical and horizontal integration. Thus security needs naturally increase and become increasingly significant in relation to pure process security and productive availability.

Where previously an attack on a machine in relative technical isolation required having a person insert a USB stick into it manually, attacks on data security now can take place through many scenarios.

THE CHANGING THREAT SCENARIO

As the BSI (German Federal Office for Information Security) established in its latest list of threats for ICS[1], "infection with malware via the Internet and Intranet" is one of the most relevant entry points for potential attacks. This means that the attack is carried out step by step, first by compromising a standard commercial IT component, such as an email client, web server, browser or operating system. As a result of security loopholes in these programs, which are not known to software manufacturers and users, or for which no adequate security package has been released ("zero day exploits"), the attacker is able to put unknown malware into place. Subsequently this then helps an attacker get deeper into the system. There is often a data connection between the office network and the ICS network, for example, by means of commonly used databases, ERP, file servers or email systems. There is no longer a complete separation of the network areas ("air gapping").

Here, it may be possible that certain security information and access data is obtained which may, under certain circumstances, allow access to other internal systems. Another direction of attack can be the manipulation of network components such as routers or firewalls in order to change security settings or re-route data traffic. Components in an automation environment are often directly incorporated into an Ethernet-based network. It is self-evident that this close technological coupling can favor the penetration of sensitive areas. At field level, we may encounter further weak points. Many automation components still communicate by means of unencrypted plain-text protocols. Here, data traffic can be read without great difficulty. The interpretation and manipulation of these communication processes is thus possible with relative ease.

Further gateways for attacks from the Internet are offered by remote maintenance access or the direct connection of control components with the Internet. Here, security risks arise in particular if secure user authentication and the protection of transfer methods (encryption) is not sufficient. It is usually difficult to recognize unwanted access to a system. Also, if the areas of the local system or network that can be accessed via external access are not sufficiently "fenced off", there is again a channel available for deeper access.

An interesting new entry to the observations of the German Federal Office for Information Security is the compromising of smartphones in the production environment. This concerns recording communication

for the monitoring of production data and, in the worst case scenario, the manipulation of it. The prevalence of such attacks appears to still be relatively low at the moment. However, this can change due to the simple technical localization of such communication incidences, as well as the frequency with which such communication occurs. The compromising of components in the Extranet and cloud-based solutions also now appear on the list of relevant threats. Here, it must be ensured from the start that the strictest security requirements are met. These latter scenarios particularly point to the necessity of valid security concepts based on robust security for tomorrow's production.

PROTECTED ISLANDS

One of the most fundamental recommendations for a security-orientated design of industrial equipment is dividing the ICS networks and surrounding network areas in clearly delimited segments – security zones – and having the data connection between these areas precisely qualified and monitored. Unnecessary and – in the event of doubt – also insecure communication channels should thus be avoided, which makes conspicuous data traffic easier to detect. However, in practice, such a strict segmentation of the network areas is often difficult.

Equipment that has grown in size historically, on the basis of automation components from different manufacturers and product generations, often does not meet the requirements for these security islands from the start. In addition, there are the frequently necessary adaptations and expansions to the operation of the equipment and, as mentioned before, the intended data convergence of equipment, monitoring and planning systems for the purpose of dynamic optimization. The systems that allow connection between the different areas and, for example, allow the user in the industrial environment – increasingly regardless of location – to interact with the equipment are playing a special role in the process.

SECURITY AS A HOLISTIC CHALLENGE

The current challenges in the security field for industrial applications and equipment can be effectively tackled with the planned implementation of security strategies and associated methods. A precise analysis of possible security risks and the detection of security incidents goes hand in hand with the formation of corresponding emergency plans. Security weak points, both technical and organizational, must be rectified or at least actively controlled. The international security standards ISO 27000 ("Information Security Management Systems") and IEC 62443 ("IT Security for Industrial Control Systems – Network and System Protection") outline the required structures and provide recommendations.

National and international institutes are contributing, with the publication of their observations and analyses, to the heightening of awareness of the security challenges to industrial applications. From this, it is evident that the systems being particularly tested are the ones that can portray operation at local level and also in distributed scenarios and that allow dynamic interaction beyond the conventional limits on this basis.

It is necessary to accept this challenge and to select suitable technologies, and for IT and automation to work in collaboration to keep everything under control. This is how the production potential in Smart Factories is uncovered – unassailably!

STEFAN HUFNAGL,
JUNIOR PRODUCT MANAGER

[1] *https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/hardware/BSI-CS_005.pdf;jsessionid=E1C418A160FD8D4954230F30FD86A31F.2_cid341?__blob=publicationFile*
[in German only]


HMI
SCADA
PLC
?
?
?

EXPOSED ENERGY CUSTOMERS?

Security in Smart Metering

The topic of security in the smart grid is very diverse and affects many different areas. However, one aspect is discussed in particular at the moment – the possible breach of privacy through smart meters. Is this pure scaretactics or will the exposed energy customer soon become a reality?

Smart meters are minicomputers that act as intelligent meters. They will soon be in many distribution cabinets and will communicate with energy supply companies via PLC, LAN, GPRS, GSM or PSTN[1]. The most important reason for the widespread introduction in Europe is that smart meters can be used to query consumption data remotely. At the press of a button, energy suppliers can establish the energy consumption and issue an accurate bill. By 2020, 80% of households in Europe will be equipped with a smart meter.

WHAT DOES ENERGY CONSUMPTION SAY ABOUT US?

Depending on the level of detail in the data queried, together with meter data from other media, it is possible to draw conclusions about consumer behavior. If only the medium of electrical energy is considered, it is hard to make a distinction between whether the washing machine or the dryer is in operation. However, if you take water consumption into account it becomes obvious because the dryer does not need water. This analysis is very easy for a single-person household. With households of more people analysis is more difficult, but not impossible.

As part of a research project[2], an attempt was made to determine the television program being watched by means of the smart meter. In doing so, the data that is available to the electricity supply companies was used. The result: because a television uses a different amount of electricity depending on the screen brightness, it is possible to deduce, if the consumption profile of a movie is known, which movie is currently being watched.

The data needed for analyses like these is genuinely available. However, whether it will be actually used and whether anyone is interested in the enormous effort of carrying out a load profile analysis remains open to debate. Nevertheless, every consumer should be aware of these possibilities. And for regulatory authorities, there is a need, in terms of the right to privacy, to implement the appropriate legislation.

SMART METERS AS AN EFFECTIVE CONTROL INSTRUMENT

Smart meters also have potential to become a significant aid for the optimized application of renewable energy sources. The sudden increase in the proportion of decentralized energy generators and the foreseeable increase in energy demand, for example due to electric cars, will make it necessary to be able to control private generators and consumers. If this is not done, upgrading the medium-voltage and low-voltage grid will be the only – very costly – alternative.

However, those who benefit most of all from smart meters are those who do not need to upgrade their grid, do not need staff to read the meters and can cut off the power supply at the click of a mouse in the event of a problem. The consumer may gain a financial benefit that amounts to a single-digit or double-digit figure – each year and without deduction of the rental fee.

A smart meter can also receive commands to shut down the supply, but the regulations on this are very different in the individual member states in Europe. In a recommendation for the minimum scope of services of a smart meter, the European Commission listed remote shutdown as one of ten functions. However, member states are not obliged to adhere to this.

In Sweden, smart meters have been introduced almost everywhere, mostly without remote shutdown. By contrast, in Italy the remote shutdown function is currently used on average three million times a year against fraudsters and

debtors. In Austria, 95 % of households will have a digital meter by 2019. Customers will be able to deactivate the 15-minute scanning and the daily counter status on request at installation, but the remote shutdown option will remain. Consumers also have the option to reject smart meters by opting out.

Shutting down individual devices to stabilize the network will certainly be acceptable. The possibility of issuing shutdown commands in response to late payment will require scrutiny and public debate. A shutdown command that does not even come from the electricity supply company but is instead a cyber attack that can "switch off" whole countries is the worst case scenario.

JUST FICTION?

In his novel "Blackout", Mark Elsberg explores how switching off grids has an effect on Europe. In it, smart meters with a remote shutdown function played a role. Are we actually protected from this scenario becoming reality? By the meter manufacturers? Or the authorities? Or does everybody have to protect themselves?

In Germany, the Federal Office for Information Security has comprehensively looked at the protection profile of a smart meter gateway[3]. In Austria, E-Wirtschaft commissioned the European Network for Cyber Security (ENCS) to create a requirements catalog for the security of smart meters[4]. The catalog has been accepted throughout the industry. However, both the way that testing is actually carried out and how it will be ensured that devices comply with the requirements remains unclear. It is also not clear whether meters that have already been installed meet the requirements.

At the "Black Hat Europe" conference in Amsterdam in 2014, security researchers showed that there is no guarantee that the manufacturers themselves check the interoperability and security of their products. They managed to get smart meters under their control in a test environment.

However, there are also other areas of energy supply, such as equipment for generation, transfer and distribution of energy, that are security-critical infrastructure and are in need of protection. Until recently, the overriding premise for this infrastructure was that availability takes precedence over security. However, as a result of the increasing networking of control units and the use of standard technologies, more and more threat scenarios emerge as a result of external attacks.

Internal vulnerabilities also need to be considered: in 2013 – presumably when a gas provider in southern Germany put a control system into operation – a legitimate broadcast to all devices in the gas grid accidentally reached the control system of the Austrian Power Grid as well. An infinite loop was created which prevented regular communication for some time.

A standard for smart meters that takes cyber security and the privacy of smart meters into account seems far off. To prevent exposed consumers and create secure grids, we need the corresponding statutory requirements and monitoring for anomalies at protocol level in the network, the isolation of networks, and modern testing.

JÜRGEN RESCH,
INDUSTRY MANAGER ENERGY
& INFRASTRUCTURE

MARK CLEMENS,
SENIOR CONSULTANT

[1] Abbreviations:

- PLC (Powerline Communication / transfer of data via the power grid)
- LAN (Local Area Network / local network)
- GPRS (General Packet Radio Service / mobile phone network)
- GSM (Global System for Mobile Communications / mobile phone network)
- PSTN (Public Switched Telephone Network / land-line telephone network)

[2] http://1lab.de/pub/smartmeter_sep11_v06.pdf [in German only]

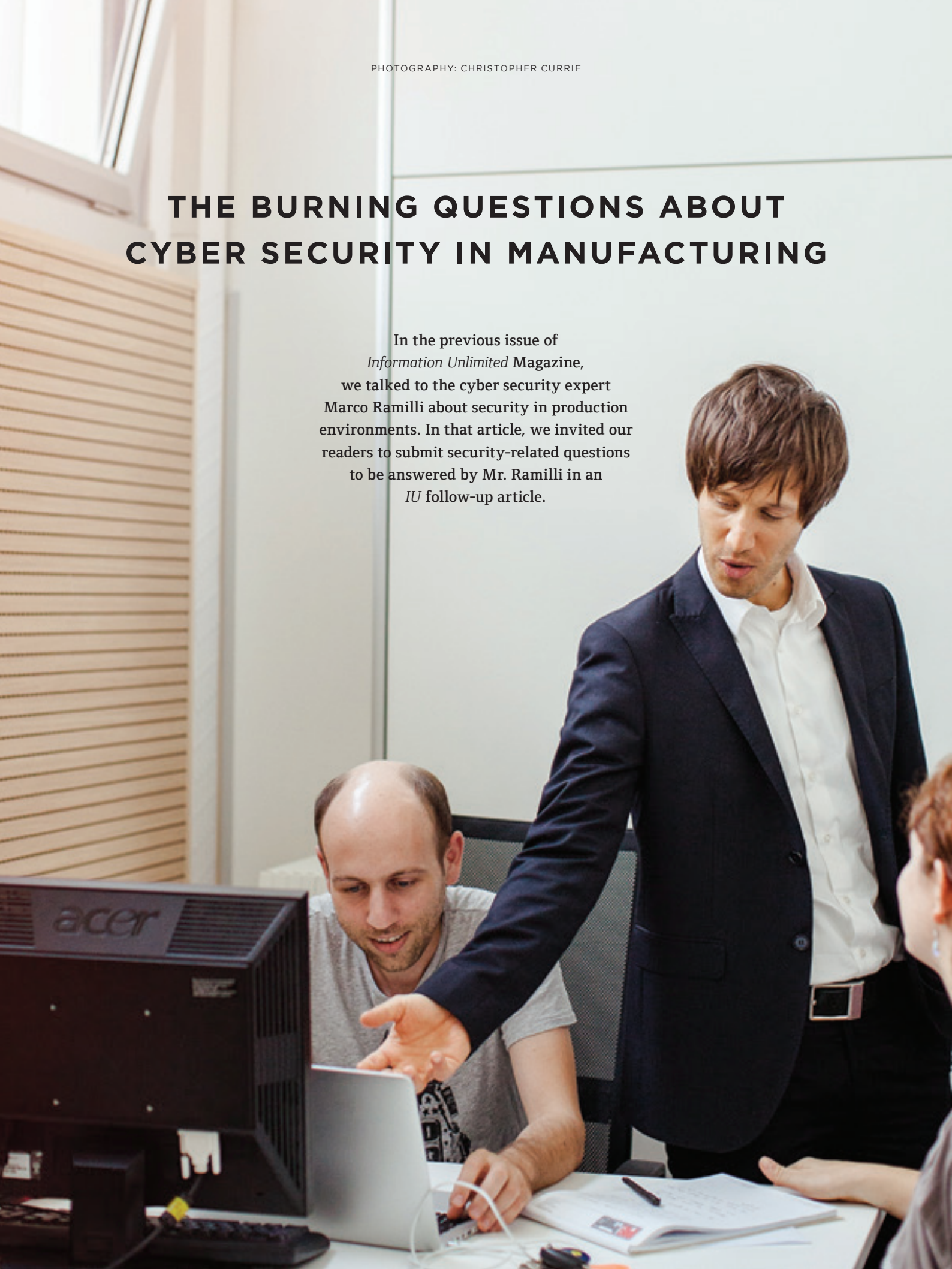
[3] https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Security/security_module_node.html [in German only]

[4] http://oesterreichsenergie.at/daten-fakten/informationssicherheit-in-der-energieversorgung/sicherheitsanforderungen-fuer-smart-meter.html [in German only]

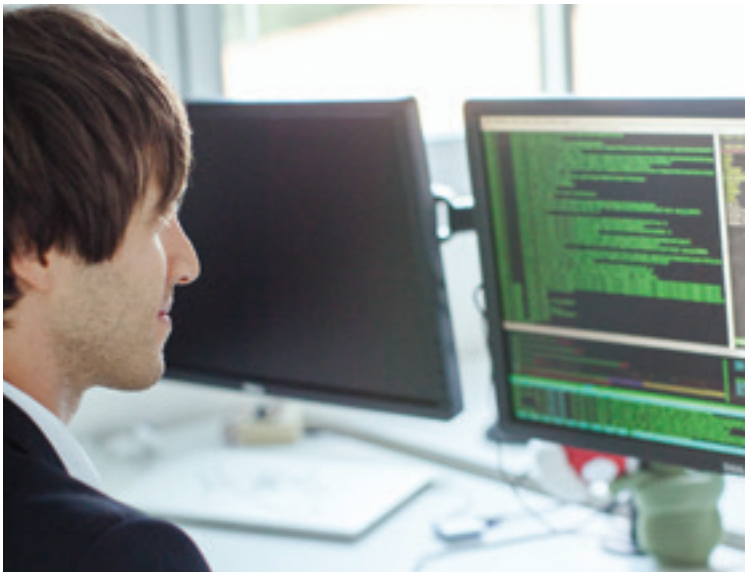
PHOTOGRAPHY: CHRISTOPHER CURRIE

THE BURNING QUESTIONS ABOUT CYBER SECURITY IN MANUFACTURING

In the previous issue of *Information Unlimited* Magazine, we talked to the cyber security expert Marco Ramilli about security in production environments. In that article, we invited our readers to submit security-related questions to be answered by Mr. Ramilli in an *IU* follow-up article.



THERE ARE CERTAINLY many questions and anxieties about security in industrial automation and many people working in production environments are just starting to deal with cyber security. In this Q&A, you can discover the main concerns of our customers and partners and Marco Ramilli's recommendations.



In your estimation, how real is the danger of malicious attacks? How great is the risk of being the target of such an attack?

MARCO RAMILLI: Network and service companies such as Cisco, HP, and IBM periodically release specific reports on the cyber threats observed during the past year. Every year, those reports detail an increasing number of threats – and victims. We deal with companies of all sizes which experience daily opportunistic attacks and, typically, two attacks per month that could be considered as targeted. Most of our customers do not even know about some of the attacks affecting their company. Attackers silently steal information.

If your company is connected to the Internet you'll have a 95% probability of being the subject of opportunistic attacks. If your company owns intellectual properties and/or deals with user data and/or is multinational you'll have a higher probability of being affected by a targeted attack. The likelihood of a targeted attack really depends on the business, company size, intellectual properties, and so on, but it's going to be a high percentage.

What would a hacker attack on my production plant look like? What would the hacker do?

MARCO RAMILLI: Attackers perform a set of actions named attack vectors in order to reach their target. Attack vectors differ from attacker to attacker, from businesses to business, and from environment to environment. It's hard to define a meaningful action set that every attacker follows but, logically speaking, every attacker needs:

- an "analysis phase" which includes (but is not limited to) information gathering, intelligence analysis and information orchestration.
- a "planning phase" which includes (but is not limited to) defining breaking points, defining exploitable sections and weaknesses, defining breaking and hooking actions.
- a "getting privileges" and "persistence" phase where the attacker plans how to get the right privileges and maintain persistence.
- an "attacking phase" in which the attacker undertakes the planned attack.

Blocking a cyber-attack is always hard since they are multifaceted and might affect many company operations (hardware, software, social, etc.). Automatic solutions such as antivirus, next generation firewall, intrusion prevention systems, proxies, and sandboxing are very important and highly recommended but, by definition, they can't block targeted attacks (targeted attacks are designed to evade specific countermeasures) so employing professionals to protect the "cyber perimeter" of the company is going to become the default choice for many companies.

What kind of people are behind attacks on a production plant? What is their motivation? Are they criminally motivated or do they simply enjoy the challenge of getting into a system?

MARCO RAMILLI: Before answering this question, I would like to underline that a cyber-attack is not considered a "crime" (cybercrime) in many states around the world. In many countries, even those where it is considered a crime, there is no practical enforcement so the cyber attackers are free to attack.

Now, depending on the company size, the people behind attacks might be involved in:

- Cyber warfare (conducted by nations, military institutions, secret services). More likely if the attacked company is a key national company, such as a utilities provider, top national employer, public company, etc.

- Cyber espionage (conducted by competitors and private agencies). More likely if the attacked company owns intellectual properties and/or is a leader in a specific business market.
- Cyber hacktivists (Anonymous, Syrian Electronic Army, LulzSec, AntiSec, SABU, etc.). More likely if the company has particular political involvements or relationships.
- Cybercrime (most of the opportunistic attacks) affects every company and/or private individuals connected to the Internet.

These four possibilities represent the most commonly accepted logical subdivision of threats.

Could I be opening "doors" to a system without knowing it?

MARCO RAMILLI: Every company should interact with its security specialists before introducing any new "object" to the company's network. The introduction of a single weak link could potentially expose the entire company system to attack.

For example, we saw one company that had up-to-date intrusion detection systems, next generation firewalls, advanced proxies, up-to-date url filtering devices, daily automated backups, disaster recovery plans over three different countries, regularly updated antivirus software with automatic patching system, advanced malware protection and data leak prevention but its automated production machines were driven by an unprotected Windows PC. That PC took a new version of CryptoWall malware belonging to the ransomware family which propagated itself through sharing folders to almost 38% of the entire network, encrypting Gigabytes of data.

The need for security managers and/or a consultancy agency on cyber security is becoming really important in every industry. If the industry's main activity is not cyber security, it should consider hiring external experts (such as Cyber Security Operation Centers or Managed Security Service Providers) to protect the company assets on an ongoing basis.

Do you think that Industry 4.0 and the Internet of Things are a danger for production plants?

MARCO RAMILLI: Production plants are often complex systems composed of mechanical, electrical, and software components such as programming logic and human interaction devices and interactional components. The Internet of Things (IoT) and Industry 4.0 bring even more complexity to production plants in order to empower communications, sensors distribution, controls and even automation. Nowadays, attackers have specific malicious actions (the aforementioned attack vectors) to attack each of these components; the more components in the attacked system, the more likely an attack will be successful. In my view, production plants are as vulnerable as any other complex system, but differ in the way they protect themselves. Cyber security is a relatively new challenge for production environments, whereas it is a well-known issue for many other complex IT environments. I would definitely suggest every production plant develops a strong cyber security defense.

Are there any advantages to "the cloud" in terms of security?

MARCO RAMILLI: Well, this is a complex question. We should consider "cloud security" as a totally different topic in which trust plays an important role. But let me put it this way: nowadays attackers usually target a user's PC as the first stage of a more complex attack vector. After taking control of the user's PC, attackers begin to move laterally to servers, backup, production plants and so on – thanks to user credentials or user rights. Usually those attacks are performed through malware propagation or "watering hole" attacks which carry backdoor payloads. So under these circumstances moving to the cloud (which has many advantages in terms of service, maintainability and cost) does not improve (but nor does it make worse) the security of the system.

How do I know whether my production plant has been a victim of a cyber-attack?

MARCO RAMILLI: Cyber-attacks on production plants have two main scopes:

1. Stealing information
2. Tampering with the entire system

The second type is mainly created to destroy a victim, such as to manipulate a drug's formula, to deny the service of public electricity, to deny the communication between airports and planes or to manipulate the backbone routing infrastructure (leaving nations without Internet). If your production plant is affected by a type 2 attack you'll notice it because your quality office (or your customer) will warn you. On the other hand, if your production environment is affected by a type 1 attack you will not notice. The first type of attack is totally invisible. Deep and continuous analysis is needed to fight (discover, block and mitigate) both types of attacks.

ABOUT MARCO RAMILLI

Marco Ramilli received his PhD in Computer Security following study at the University of California at Davis (USA) and the University of Bologna (Italy). He worked on computer security, in particular on malware evasion techniques and voting machine reverse engineering at UC Davis and, later, at USA Federal Government (National Institute of Standards and Technology (NIST), Security Division). He then worked in cyber security intelligence at Palantir Technologies and is now one of the founders of YOROI, a very promising start-up which protects industrial data from cyber-attack. According to Mr. Ramilli, SCADA and ICS security plays a key role in today's attacks on industrial data. To find out more about Mr. Ramilli and his activities in the field of cyber security, visit **www.marcoramilli.com.**

ABOUT YOROI

YOROI gets its name from the ancient name of the Samurai's armor. Today, YOROI protects its customers as the YOROI protected the ancient Samurai. The goal is to use our experience and education to "map a company": understanding the business processes, assessing the business risks and thinking as an attacker would do in order to apply security measures to protect the company. For each customer we have an active map (see Figure 1) which is able to geo-localize the threat callbacks, to interact with Active Directory in order to localize an attack, to analyze malware and threats, and to monitor email metadata in order to discover covert channel information leakage or attack. The "map" is active 24/7 and is even available on monitors in the company's IT offices. Our system strategically checks the company's vulnerabilities, dynamically checks the malware propagation status, and guarantees fast and deep analysis for our customers. We offer a 24/7 cyber security service, where our security samurais analyze the customer network flows using our technology in order to find intrusions and threats, such as vulnerabilities, email flows, data moving between entities, and so on, which might be exploited by attackers. We promptly act to block that specific flow, according to the customer's process policy, and proactively work to secure the customer's private, SCADA and public networks. For further information visit **www.yoroi.ninja**.

PRODUCTS & SERVICES

PHOTOGRAPHY: BERNHARD MÜLLER,
PHOTO DESIGNER, FOKUS VISUELLE KOMMUNIKATION

PHOTO LOCATION: KÄRNTNERFRUCHT KFG GMBH,
KLAGENFURT, AUSTRIA

EVERYTHING UNDER CONTROL – WITH THE RIGHT ALARM ADMINISTRATION

TEXT:

BERNHARD EBERT,
INTERNATIONAL SALES MANAGER

BERNHARD KORTEN,
INTERNATIONAL SALES MANAGER

THE ERGONOMIC MANAGEMENT and handling of alarms is significant for plant safety, but also for reducing the strain on the person operating the equipment, as well as boosting productivity and product quality. The focus is on avoiding unplanned downtime and increasing equipment availability.

The alarm concept is continuously gaining in significance in human process communication in particular. The operator should be optimally supported by their system when receiving alarms and messages, to ensure appropriate reactions to any situation. The idea here is to always have an overview and have the most important facts available at a glance.

WHY IS ALARM MANAGEMENT IMPORTANT?

Well-conceived alarm management in the process control system is a decisive factor in increasing plant safety. The focus is on the number of active alarms and their prioritization. Too many alarms frequently result in important information such as messages, warnings, alarms or problems not being given enough attention or not getting any attention at all. The desensitizing of the operator can have far-reaching consequences: alarms are frequently acknowledged "blindly" or ignored; alarm signals are often put out of operation. Furthermore, insufficient prioritization of alarms leads to increased strain on the user, resulting in unnesessarily delayed reaction times for vital corrective action or alarms which are even overlooked. This can have far-reaching financial consequences and endanger people and the environment.

ERGONOMIC ALARM ADMINISTRATION IN ZENON

Alarms can be configured and presented in many ways in zenon. For example, they can be allocated to alarm groups, alarm classes and alarm areas. Alarms can be defined as requiring acknowledgement or deletion. This ensures that the alarm has been noted in a traceable manner. All actions are logged in detail. The acknowledgement of an alarm in Runtime can be combined with acknowledgement from the PLC by setting an acknowledgement bit.

The alarm management integrated into zenon as standard supports companies, in particular equipment operators, with important decision-making processes in the event of problems. Transparency, a clear overview and data consistency are an important part of this.

As a configurable tool with complete function modules, such as the alarm message list for example, the alarm administration in zenon meets all requirements for an ergonomic alarm message system. This function module is fully integrated into the zenon philosophy and parameters can be set easily, without a single line of code having to be programmed. Active alarms can be notified by means of SMS, email, app or on-screen alarms in the corresponding process screen. In a redundant network, alarm message data

is automatically synced between the Server and Standby Server, as well as the client. This way, alarm functions are guaranteed and up to date; no data is lost even in the event of the failure of a computer.

The alarm message list in zenon has been continually optimized over a period of more than 20 years and incorporates the experiences of our customers gained from everyday use. In figures for programmers: over 60,000 lines of code. That corresponds to a development time of around 2,000 man days (incl. specification, requirements specification, test and documentation), if a developer programs an average of 30 lines of code per day. These figures show that alarm administration in zenon is significantly more complex and refined than the apparently simple-looking alarm message list looks at first glance.

CONSISTENCY AND AVAILABILITY OF THE ALARM INFORMATION

From the HMI to the MES/ERP level, alarm data is provided according to need. Alarm messages from individual machines (HMI), alarm messages throughout complete production plants (SCADA) through to alarm management throughout a site – with an option to use the "zenon cloud solution" – and dashboarding throughout a site can be implemented with zenon by means of simple configuration. zenon has a direct Microsoft Azure Cloud connection. The ergonomic alarm administration of zenon can process both online alarms and historical alarms. Statistical evaluations of alarm data and unplanned downtime make it possible to localize and reveal weak points in the system. One of these key figures is availability in relation to equipment downtime. In addition, the statistical evaluation of alarm data provides a meaningful overview of problems. The user can thus quickly find out which errors occur most frequently and which cause the longest downtime. This enables targeted measures to be implemented which minimize equipment downtime.

Displaying alarms on mobile devices is another strength of zenon. It is left to the user to decide whether this happens by means of an app on a mobile device, such as a smartphone or tablet, a browser or even by means of smart glasses. zenon is always up to date, supporting the latest technology on the market and offering the highest security available. This allows for valuable information to be effectively distributed beyond the native zenon clients or web clients.

zenon's ergonomic approach, its alarm management and consistency from the sensor through to the MES/ERP increases not just the availability of equipment and thus the reliability of the entire plant, it most of all provides a significant contribution to the profitability of a manufacturing company.

Figure 1: Example of an F&B alarm report in zenon. The bar chart on the left side provides information regarding the alarm duration per machine; the pie chart on the right shows the number of alarms per machine.

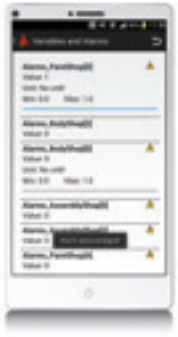


Figure 2: The Everywhere App by zenon gives users an overview of the faults in production, anytime and anywhere, and alarms can easily be acknowledged directly via the App while out and about.

FAST FACTS

ALARM ADMINISTRATION IN ZENON

- Out-of-the-box
- Grouping, classification and prioritization of alarms
- Simple setting of alarm message list parameters
- Comprehensive filter possibilities
- High performance
- Immediate redundancy capability
- Graphical display with a clear overview
- Dashboarding throughout a site
- Unlimited availability: from the HMI to the MES/ERP on all end devices
- Reliable messaging system

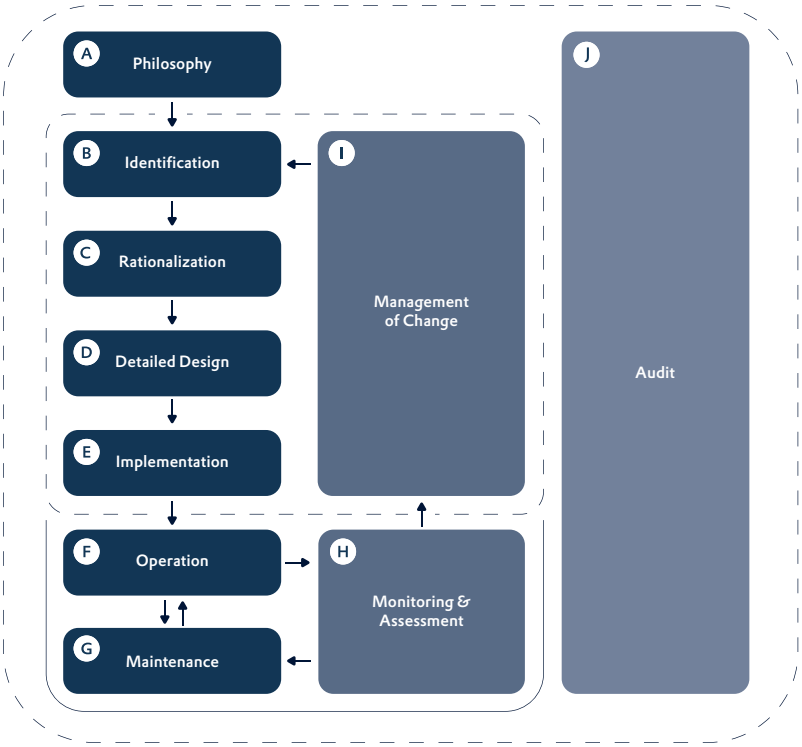
SAVE TIME AND MONEY WITH
AN ERGONOMIC SYSTEM IN PLACE AND USEFUL
STANDARDS TO GUIDE YOU

Alarm Management with zenon

COPA-DATA HAS MORE than 80,000 zenon HMI/SCADA installations worldwide. The one zenon feature which is used in nearly every installation is the alarm concept. As a native part of the zenon Runtime, the core zenon alarm functionality is available for all users and all licenses. This article will explain how companies can improve productivity, efficiency, and safety by utilizing zenon HMI/SCADA solutions in combination with international alarm management standards such as ISA 18.2 or IEC 62682.

The task of implementing and maintaining an effective alarm management system compliant to the International Society of Automation (ISA) ISA 18.2-2009 or the International Electrotechnical Commission (IEC) IEC 62682 is by no means a simple one. A successful implementation requires input from plant management, engineering, facilities, information technology and operators. To start a successful alarm management project, we show you which aspects one should consider according to ISA 18.2 / IEC 62682.

Figure 1: Alarm Management Lifecycle according to ISA 18.2 and IEC 62682.



Alarming has been a crucial and important topic for manufacturers since the days of giant control rooms with massive annunciator panels. In the early days of Human Machine Interfaces (HMI), the annunciator panel offered a limited amount of space to give plant operators only the most crucial information to maintain safety and productive operations. Since the inception of PC-based HMI systems, the amount of alarms which can be configured and shown on HMI screens with relative ease has escalated at Moore's Law proportions. This influx of storage and processing capabilities eventually led to one of the biggest problems facing a typical plant operator: the overwhelming amount of information presented by the modern alarm system.

Let's have a closer look at how engineers can cope with this and some other challenges:

ALARM MANAGEMENT CHALLENGE 1: TOO MANY ALARMS

The test of a good alarm management system does not occur when the plant is running smoothly, but instead when there are disruptions in the process. According to the IEC, an average rate of 288 alarms per day or twelve alarms per hour or two alarms per ten minutes is maximum which is manageable. The ISA classifies an alarm flood as more than ten alarms, per ten minute period, per operator. The target alarm volume, over a 30-day monitoring period should be in the range of one alarm, per ten-minute period, per operator.

ZENON'S ALARM MANAGEMENT SOLUTION 1: DELAY TIME, THRESHOLD, AND DYNAMIC ALARM LIMITS

zenon offers features and functionalities to reduce unnecessary alarms. For example, in zenon each variable when activated as an alarm has both a delay time and dead band property. Here we offer a short technical description of each method:

DELAY TIME EXAMPLE:

A pressure transmitter is monitored by zenon and is set to alarm when the value reaches or exceeds 350 psi. If the normal operating condition and ideal pressure is 349 psi, the operator may encounter many chattering alarms which takes focus away from more serious alarms. In this case, one is able to define a delay time of 15 seconds. This means that alarm conditions will only be triggered if the pressure transmitter has a value > 350 psi lasting for at least 15 seconds. If the 15 second period has lapsed and the value is still > 350 psi, then zenon will generate the alarm with the timestamp when the limit violation originally occurred. If any time before the 15 seconds the value drops below 350 psi, the alarm will not be generated.

ALARM THRESHOLD EXAMPLE:

A threshold value can be defined that will be used for clearing a limit violation so unwanted reactions for chattering analog values can be avoided. If an alarm threshold of 5 for the pressure transmitter is set on the limit, which still alarms at > 350 psi, then the alarm will occur as normal at 350 psi or greater. However, now the alarm condition will only clear if the threshold value of 5 has been reached. In our example, this means the alarm will be only cleared if the value returns to < 345 psi.

DYNAMIC ALARM LIMITS:

zenon also allows for Runtime-based alarm set point tuning through a functionality called dynamic alarm limit. This can be implemented for any numeric variable, regardless of the PLC. The alarm set point tag can come from the PLC or can even be an internal zenon variable. In Runtime, if we find that the pressure transmitter alarm limit of > 350 psi is too low, the operator or supervisor with appropriate user rights can push the limit up to 355 psi, without changing the engineered configuration or project. Of course, this change will be logged in the zenon Chronological Event List.

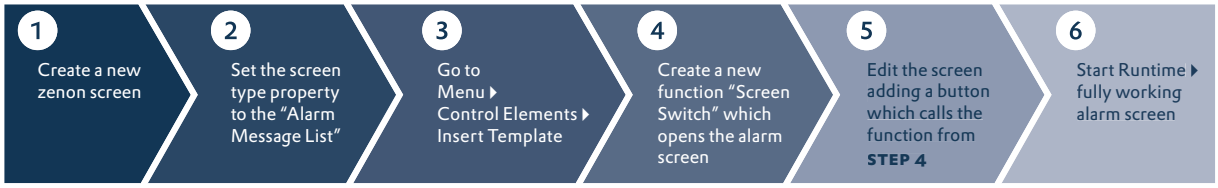


Figure 2: Alarm visualization steps with zenon.

ALARM MANAGEMENT CHALLENGE 2: MANAGING A DIVERSE INFRASTRUCTURE

Only in very few cases, are plants and facilities built from the ground up with a single turnkey solution that provides both the controls as well as HMI/SCADA. In well-developed markets, many manufacturers have a diverse infrastructure of different PLCs, HMIs, and a general mixture of new and old technology. Each PLC program or HMI system follows its own unique conventions which only adds to the problem.

A good alarm management system must be based on a solid, efficient, and a reliable communication foundation to bring these components together. In a production facility where alarms are provided to operators who must make critical decisions with serious operational or safety implications, the quality of data must be called into question. The fact is that many existing HMI/SCADA systems still rely on additional software components (e.g. a middleware OPC Server) or PLC head stations which adds additional complexity and extra components which may fail.

ZENON'S ALARM MANAGEMENT SOLUTION 2: A SOFTWARE SOLUTION FOR ANY HARDWARE

With more than 300 native drivers and communication protocols – actively developed and maintained by COPA-DATA – zenon has the unequaled ability to be installed in a production facility that has a mixture of old PLCs, new PLCs, proprietary PLCs, and PLCs supporting standardized communication protocols (Modbus, BACnet, OPC UA, etc.). Since zenon uses its direct communication drivers, the alarms are always derived from a variable that is being mapped to the logic controller. The zenon variable list provides an overview of all variables at all times, and in Runtime there are 64 dedicated status bits to ensure the communication status and the quality of data.

The functionalities of the core zenon alarming system require no extra configuration, settings, databases, or a dedicated server. When a new zenon project is created, alarming is activated by default, and all the engineer needs to do is define the alarm states and implement the alarm screens.

ALARM MANAGEMENT CHALLENGE 3: MULTIPLE POINTS OF CONFIGURATION

Many alarm systems in use today require an additional alarm server or require tags to be configured multiple times, adding to inefficiencies in engineering and hindering the process of creating a proper alarm management system.

ZENON'S ALARM MANAGEMENT SOLUTION 3: TAGS DEFINED ONE TIME, OBJECT-ORIENTED ENGINEERING

With zenon, variables are only defined once. For example, if a pressure transmitter is being read from an Allen Bradley ControlLogix PLC, this is just one variable in zenon. This one pressure transmitter variable can be displayed on HMI screens, recorded in the Historian, plotted in the Extended Trend diagram, or used to generate an alarm. Therefore, if the alarm condition must be modified for the pressure transmitter it must only be done once, in a single location.

To take object-oriented engineering a step further, zenon supports the creation of custom and structured datatypes. All zenon variables are based upon a driver (e.g. Siemens S7), a driver object type (e.g. Ext. Datablock), and a datatype (e.g. Real). There are multiple benefits in creating and using custom datatypes in zenon. For example, it is possible to create a custom datatype for the pressure transmitter. This can be set as a Real datatype and will inherit the properties of the default Real type in zenon. The new pressure transmitter can then be customized even further by adding the measuring units of psi, showing three decimal places, and defining a series of four limits on the datatype.

Sample Datatype Configuration for Pressure Transmitter

Limit Nr.	Alarm Text	Value	Alarm Class	Color/Flashing
1	HCL Tank LOW-LOW ALARM	≤ 55.25 psi	Critical Class	Purple Flashing
2	HCL Tank LOW ALARM	≤ 56.5 psi	Warning Class	Light Purple
3	HCL Tank HIGH ALARM	≤ 60 psi	Warning Class	Yellow
4	HCL Tank HIGH-HIGH ALARM	≥ 65.75 psi	Critical Class	Red Flashing

Figure 3: Custom datatype example in zenon.

As you can see in *Figure 3* the creation of this custom datatype for the pressure transmitter will take an engineer approximately five minutes to configure and check. The savings and benefits come in at the next step, since the engineer must display 150 pressure transmitters in the SCADA system, each with the above configuration and limits configured. This process in zenon will only take the engineer one minute since he is able to create an array of 150 elements for the pressure transmitters which will automatically inherit the properties set on the pressure transmitter datatype set in *Figure 3*. Of course, individual instances can still be customized and "unlinked" with the datatype.

Not only is this a huge time saver, it also guarantees that every individual pressure transmitter is configured accurately. If, after two weeks of operation, the operations manager wants the Low-Low limit for the pressure transmitter changed to only alarm at < 56 psi, the engineer only needs to make this change at the pressure transmitter datatype, and all 150 pressure transmitters will be updated automatically with the new Low-Low limit of < 56 psi. After the configuration is changed, the zenon Editor downloads the updated files to the Runtime server via zenon Remote Transport over the network, then the engineer remotely reloads the project with a mouse click. The changes are live and deployed throughout the zenon network to all connected servers, clients, and web clients in just a few moments, all happening without any downtime, operational inconvenience, or concern.

ALARM MANAGEMENT CHALLENGE 4: QUALITY OF VALUES AND STRING PROCESSING

It's a matter of fact that the communication quality to the PLC very much influences the alarm generation in the SCADA system. If the communication is bad, interrupted, or even lost, the system generates a flood of alarms which might lead to false conclusions. Therefore, the quality of values is essential. Another common challenge is the monitoring of string values via alarming features.

ZENON'S ALARM MANAGEMENT SOLUTION 4: REACTION MATRIX

The most powerful tool for a global alarm definition, status supervision and string monitoring in zenon is the Reaction Matrix, known by zenon users by its abbreviated name ReMa. The Reaction Matrix differs from variable and datatype limits in a few ways, but most notably in its linking. Where limits are defined directly on the variable or datatype, the Reaction Matrix makes it possible to define a global alarm condition and reuse it for multiple variables. For example, in an automation system using zenon, there could be 300 valves and all valve statuses are read in as an integer for the defined states. Since all valves have a common value reading for their states, the Reaction Matrix is perfectly suited. The engineer must create only one reaction matrix with this configuration and it is then simply linked to all instances of the valve.

In addition to the global aspect of the Reaction Matrix, zenon also offers the ability to use a Numerical Reaction Matrix, a Binary Reaction Matrix, or a String Reaction Matrix. The Numeric Reaction Matrix gives the user the option to define the alarm set points in terms of less than, greater than, or equal to a specific numeric value. It also has a unique feature to "treat any value change as a limit violation". The Binary Reaction Matrix gives the engineer the ability to define alarm conditions based on the state of individual bits of a word. The String Reaction Matrix can be linked with any string variables being read from the PLC to generate an alarm. Value monitoring can be achieved with static values or even with wildcards.

STATE-BASED ALARMING:
In zenon Runtime a variable always consists of the following three things: (1) the variable value, (2) the variable timestamp, and (3) the variable status. The variable status is maintained for every zenon variable and is composed of 64 individual status bits to always give a clear indication of the real-time or recorded variable status, whether it was a good status, communication fault status, alarm suppressed status, etc.

The main benefit of the Reaction Matrix is that not only can it analyze the value of a variable, it can also generate alarms or event conditions based upon a specific status bit. Or sometimes even more important: it can suppress alarms if the status information does not fit. For example, if there is a communication problem no alarm will be triggered. This makes it quite easy to avoid thousands of alarms during a communication problem with the PLC.

ALARM MANAGEMENT CHALLENGE 5: KEEPING AN OVERVIEW AND FINDING SPECIFIC ALARMS

This challenge is very much interconnected with the challenge of how to cope with too many alarms presented earlier in this article. If the amount of information presented by your alarm management seems already overwhelming, you will be surprised how lost you would feel in an alarm flood without proper filtering mechanisms. For a truly effective and manageable alarm system, finding and displaying the most critical alarms is a key success factor.

ZENON'S ALARM MANAGEMENT SOLUTION 5: ADVANCED FILTERING MECHANISMS

zenon offers flexible and user-definable solutions to enhance operations such as alarm classes and alarm groups for the purpose of classification and prioritization. Alarm groups and classes in zenon are also defined globally and set independently of the variable limits or Reaction Matrix states. Therefore, it is possible to have a pressure transmitter with a High Alarm with a class of Warning and the same pressure transmitter with a High-High Alarm with a class of Critical.

In Runtime mode, individual colors of the alarms can be defined within the alarm groups or classes to give operators a clear indication from the Alarm Message List about the most important alarms to handle. Of course, filtering in the groups and classes is an integrated part of the zenon filtering concept.

When alarm classes are used in combination with zenon alarm areas, then the ultimate statistics and overview are provided to the operator. Alarm areas are abstracted so they can be used for a variety of purposes, but they provide detailed information about active, unacknowledged, and acknowledged alarms within a logic area. *Figure 4* shows a simple example how alarm groups, classes, and areas can be used together to provide a complete overview of the alarm status of an entire production facility.

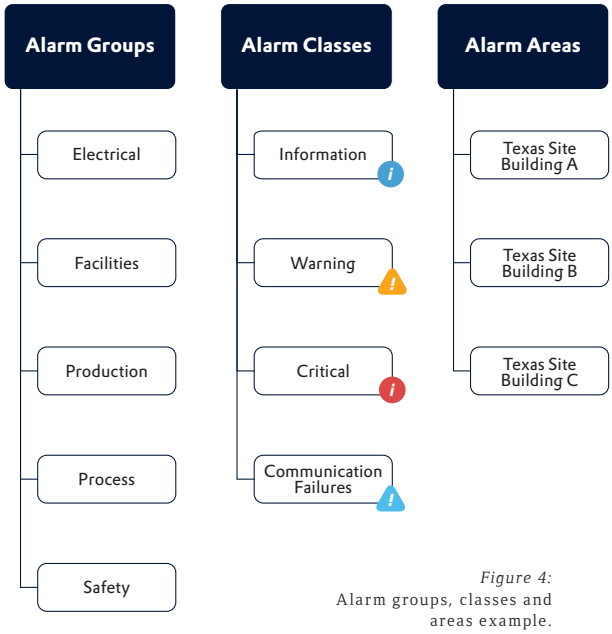


Figure 4:
Alarm groups, classes and areas example.

There is one additional attribute to the unique alarm concept in zenon, and this is the Equipment Model. The Equipment Model in zenon represents an ISA 88 and 95 model that allows for the linking of objects to a physical piece of equipment. In general, it is a structured, hierarchical tree view of equipment within a plant or facility (see *Figure 5*). The zenon variable which generated an alarm can be linked to one or multiple equipment groups. When this is utilized, it provides not only a connection of a variable to a piece of equipment for the operator, but will also provide a hierarchical alarm filtering mode. If we look at an example from a beverage bottling facility, the equipment model may be structured as follows:

In Runtime, if the operator filters on Line 3, all alarms that occur from any piece of equipment within Line 3 will be returned. If the operator filters alarms in the Runtime for just Line 3 filler, only the alarms generated from the Line 3 filler will be returned. As a result, the operator who is looking to troubleshoot or diagnose a problem can quickly and effectively narrow the results of hundreds of alarms to just the alarms relevant for their investigation.

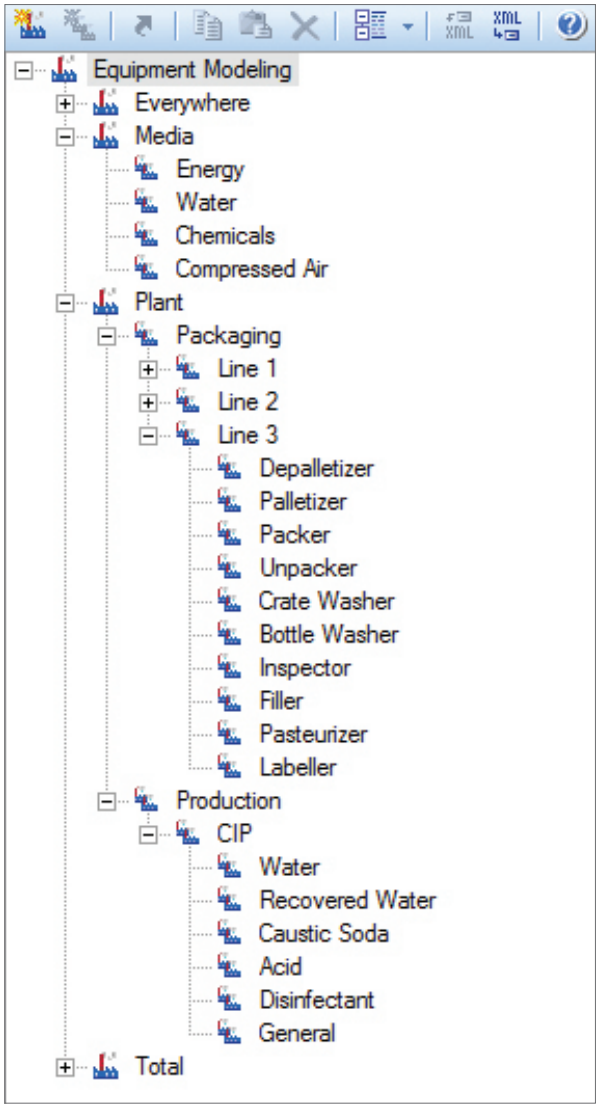


Figure 5: Equipment model example in zenon.

CONCLUSION

Alarm management standards such as ISA 18.2-2009 and IEC 62682 are practical guidelines developed by industry professionals to implement and maintain an effective alarm management system. These standards are, however, just one piece of a larger equation.

Contact COPA-DATA to learn how zenon HMI/SCADA can help you convert these standards into reliable, dynamic, and effective alarm management solutions.

LOUIS PAGLAICCETTI,
TECHNICAL CONSULTANT

zenon 7.20

Ergonomics for the Smart Factory

The new version of zenon, version 7.20, is fully consistent with the Smart Factory. Many new features and improvements lead us another step closer to the Smart Factory which is characterized by:

- Cloud solutions that enable work and benchmarking throughout different sites
- Highly significant analyses using Big Data applications
- The availability of information, at all times and everywhere

The right ergonomic software is required in order for a production operation to become a Smart Factory. This primarily means modern usability, simple and rapid engineering and a great user experience. The performance must correspond to current technologies and allow fluid work. Not least, security is an ever-more important issue – security against spying and external attack. zenon 7.20 meets all these requirements for Smart Factory software.

ZENON CLOUD SOLUTION

The factories of large production companies are often distributed over several sites in different countries. However, measures to reduce consumption, to manage energy, OEE and performance improvement often take place in isolation from one another, with much optimization potential remaining unexploited. With zenon 7.20, you can move the data that is necessary for production optimization into the cloud and use it for company-wide benchmarking. The integration of zenon into the Microsoft Azure cloud platform makes it possible to provide all data from the individual production sites of a company into a single system in real time. This is how distributed production sites can be networked and integrated with one another. Local and company-wide energy management, OEE or quality management becomes possible. Dashboards provide global information in real-time, and historical analyses are prepared with a clear overview. zenon thus becomes a tool for company-wide optimization.

ZENON AS A BIG DATA APPLICATION

With zenon, data from production can be processed very effectively. A large amount of data is often required in order to obtain meaningful statistics and analyses. zenon 7.20 makes it even easier to extract significant trends from such quantities of data. To do this, even more performance optimizations were carried out in the new version. These affect, for example, zenon Historian, which can now query very large amounts of data.

AVAILABILITY OF INFORMATION – ALWAYS AND EVERYWHERE

The mobile solutions have also been refined for zenon 7.20. Graphical amendments to the Everywhere App ensure that work with smartphones and tablets is even more user-friendly. The Everywhere App has also grown with 7.20: the Notifier app for Android simplifies the acknowledgment of alarms on smartphones.

The enhancement of the SAP interface in zenon also ensures optimized data availability. The calling up of production data can also be instigated immediately from SAP, and not just from zenon as before. In doing so, users benefit from synchronized data handling and optimized event chains, in which data from zenon is called up by SAP in a targeted manner and only when required.

HTML 5 is a major topic in the area of mobility and data availability. Now, a screen can be created as usual in zenon Editor and rendered using HTML5. The screen is compiled in the Editor and stored on the Internet Information Server as an HTML client project. The client – or the local end device, such as a tablet or smartphone – uses a browser to access the Internet Information Server and renders the HTML 5 page. Dashboards, for example, can thus be easily displayed using a browser.

The benefits of the HTML 5 solution in zenon:

- Clients with lower performance can also be used.
- The screen only needs to be drawn once in the zenon Editor and can be compiled directly as an HTML 5 project. This means that only one engineering tool is needed.

SMART ENGINEERING: ERGONOMICS AND USABILITY

Ergonomics and optimal usability are present throughout the new version. For example:

- *Upgrade to DirectX version 11.1:*
  The use of DirectX 11.1 means that modern, powerful graphics technology is being used. In zenon Editor, graphics are now also displayed with DirectX.
  The principle is "what you see is what you get".
  Through this step forward in graphics technology in visualization, zenon enhances its status in the market as a pioneer.
- *New "Command Sequencer" module for the energy industry*
  In the command sequences of zenon Energy Edition, command actions can be configured step by step and executed in an automated manner. Simple compilation by means of drag & drop guarantees ergonomic application.
- *Enhancements and improvements in the Recipegroup Manger*
  The Recipegroup Manager (RGM) has been optimized in several areas. A highlight, for example, is the new recipe value table. For large recipes in particular, zenon 7.20 offers considerable performance improvements.
- *zenon Logic 8.7*
  With the latest release, the IEC 61131 programming environment of the zenon Product Family was enhanced with version 8.7.

ENERGY DATA MANAGEMENT

Energy data management is also a central topic in zenon 7.20. Three of the many highlights:

- The integration of zenon Analyzer with zenon has been enhanced.
- The new Metering Point Administration creates an overview of meters and measured values.
- The newly-available "zenon Energy Data Management System" solution package has been tailor-made for automated energy management applications.

SECURITY

To protect against spying and external attacks, companies and software manufacturers must constantly work on protecting their applications and IT infrastructure. With zenon, security has been at the forefront of design for a long time. With the focus on the Smart Factory and Industry 4.0 in zenon 7.20, security and cyber-security is given even greater significance by COPA-DATA.

ANDREA GRALL,
PRODUCT MARKETER

Do you want more details on zenon 7.20? Go to:

http://kaywa.me/X9pOr

Big Data in the Production Environment?

Big Data has been one of the hyped topics in the IT field for some time. But what's the situation in automation infrastructures? Is the handling of large amounts of data also becoming more significant in the industrial production environment?

In the recommendations for implementing Industry 4.0[1], Big Data is named as one of the future technology requirements. But where are we now? Handling data amounts in petabyte dimensions is currently the exception in production. However, today there are already application scenarios that lead us towards very large amounts of data.

Figure 1:
Analyze large amounts of data directly in zenon Runtime.

TYPICAL STATUS QUO

When archiving production data, choices are made selectively in relation to which data is saved. Some data is automatically deleted again after certain time periods. With applications such as energy management, for example, a multitude of data points are often archived, but generally with a very rough granularity, which in turn keeps the amount of data low. In HMI applications, machine-orientated data is often saved at the panel directly and, at least in part, exported to central archives or databases.

POSSIBLE SCENARIOS

With Big Data in manufacturing, all relevant data in relation to the complete life cycle of a machine or plant can be saved. Based on this data, completely new possibilities for analysis arise. The operators of machines and equipment (manufacturing companies) can work with the data from their entire production estate. The machine and equipment manufacturers have data from a number of the same machines available for their evaluations.

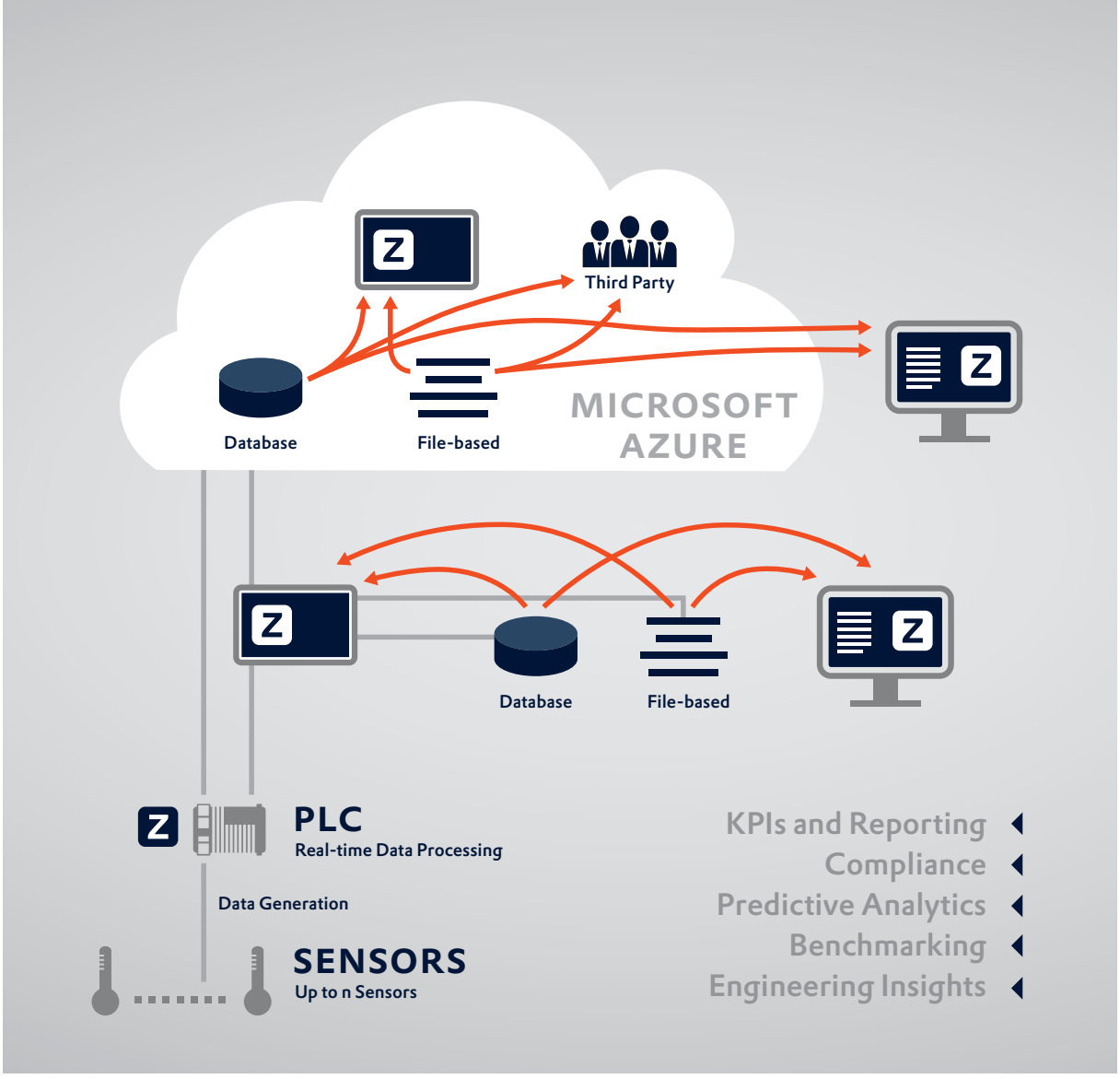


Figure 2: zenon offers flexible possibilities for data storage and analysis.

THE BENEFIT OF BIG DATA

Manufacturing companies can uncover unexploited potential in equipment efficiency and effectiveness as well as quality management with Big Data analyses, which in turn increases the Overall Equipment Effectiveness (OEE). Another advantage is that it allows predictive maintenance. Optimized maintenance management has a positive effect on production costs and overall equipment effectiveness.

Machine and equipment manufacturers can also gain additional valuable findings in relation to improvements in construction using Big Data analyses which can, for example, consequently increase the manufacturing capacity and energy efficiency at the same time.

BIG DATA WITH ZENON

zenon already offers possibilities for handling very large amounts of data. Data security, the rapid evaluation of data and ergonomic handling are the main focus. Users can freely choose whether they operate zenon purely on-premises or scale it with enhancements to the cloud. With version 7.20, zenon can be seamlessly integrated with the Microsoft Azure cloud platform.

In addition, we are working in both Product Management and Research & Development to make zenon even better at handling ever-larger amounts of data.

PHILLIP WERR,
MARKETING MANAGER

[1] http://www.plattform-i40.de/finalreport2013

FAQs

zenon in the Cloud

zenon supports manufacturing companies on the road to the Smart Factory. A significant contribution to this is provided by the newly-integrated IoT solutions, which use the most up-to-date Microsoft technology. With the connection to Microsoft Azure, for example, companies can thus create a cost-effective and at the same time highly scalable infrastructure for analyses of data throughout sites. You can find out how it works, what you need to be aware of in the process, and what costs are involved in the following FAQs.

What requirements must be met in order to use the zenon Cloud Solution?
To be able to use the zenon Cloud Solution, you need a Microsoft Azure subscription, zenon from version 7.20 and the appropriate license.

What options are there to connect zenon to the cloud?
There are two scenarios:

1. You move historical data to the cloud.
2. You combine the Azure driver and the Azure Process Gateway and send actual values in real-time to the cloud and have this displayed by using a dashboard, for example.

What data is written to the cloud by zenon?
When moving archive data into the cloud, zenon creates a table in an Azure SQL database for each archive. This is then named with the zenon project name and the archive ID. The following data is saved by zenon in this table: variable ID, aggregation type, time stamp, variable value, variable status. This information is written cyclically to the SQL table in accordance with the save cycle and storage duration that has been set locally.

If the Azure Process Gateway is used in zenon, the above-mentioned information – with the exception of the aggregation type – is compressed into a message and sent to the Microsoft Service Bus. There, the messages are cached until the driver reads this data. Sending takes place either after a change to a value or after the set cycle time (integrity period). The FIFO principle (first in, first out) is used for reading.

How is my data protected on the way to the cloud?
zenon transfers the data to the Azure cloud by means of HTTPS using SSL (TLS) encryption, thus ensuring consistency of data. The one-way connection is created using port 443 and is a purely outgoing connection. This therefore also prevents attacks from outside. If there is a firewall, this should also be configured so that it only allows outgoing connections via port 443 using HTTPS in the IP range of the Azure datacenters.

Where is my data saved physically and can I influence the save location?
The data is physically saved in Microsoft datacenters around the world. It is possible to stipulate which one when creating the respective service (SQL server, Service Bus, etc.). In Europe, for example, there are two Microsoft datacenters, one in Ireland (Dublin) and one in the Netherlands (Amsterdam).

How fail-safe is Microsoft Azure Cloud?
Microsoft guarantees an availability of 99.9% for the Service Bus and 99.95% for cloud VMs and cloud services as worker role instances. Microsoft even guarantees an availability of 99.99% for SQL databases.

How much does SQL evacuation to the cloud cost?
With Microsoft Azure, you only pay for the services you have used. These are billed by the minute. To move data to the cloud, you need a cloud service in Azure that works as a worker role instance and an SQL database. You can find all information about prices, including a price calculator, on the Microsoft Azure website.

How does the real-time transfer of values via the Service Bus work?
Transfer is implemented by means of name-based addressing. The Azure Process Gateway transfers the variable values from the source computer to the Microsoft Service Bus. To do this, you must enter the connection string to the Microsoft Service Bus and stipulate a freely-definable name for the queue to be created in the Service Bus and the name of the target computer to which the values are ultimately to be transferred.

You also need an Azure driver on the target computer, which reads off the values from the Microsoft Service Bus. To do this, you need only enter the connection string to the service bus in the driver settings and the corresponding queue from which the values are to be read. As soon as the Azure Process Gateway starts, the selected queue is created in the Service Bus. In this way, only the correct target computer can read the variable values.

How long are the messages in the queue saved in the Service Bus?
You can set the duration of the messages by means of a property in the queue. This means that if the messages are not immediately read by the Azure driver or the worker role instances, they are saved according to the setting in the queue. The default value is one day.

What happens if the Internet connection is interrupted during a set archive evacuation?
This is not a problem at all. If the Internet connection is interrupted, the archive files are cached locally in the Runtime folder until the connection is reestablished. Then all archive files to be evacuated are written to the SQL database in the cloud.

Can I reuse archive data that is stored in the cloud in zenon?
Yes, the archive data that has been evacuated can, of course, be reused from the cloud. The reading of data from the cloud SQL database works in exactly the same way as a local SQL database. This data can therefore be displayed in reports or trends.

What next? What do I do if I still have questions or want to see more functions?
The zenon Cloud Solution has been implemented in zenon version 7.20 for the first time. Further performance enhancements and new functions are expected in future software versions. You can find more information in zenon documentation, in the COPA-DATA knowledge base and in our forum at www.copadata.com/support. Your local COPA-DATA sales contact would also be happy to help you.

CHRISTIAN BAUER,
TECHNICAL CONSULTANT

INDUSTRIES & SOLUTIONS

FOOD & BEVERAGE

ENERGY & INFRASTRUCTURE

AUTOMOTIVE

PHARMACEUTICAL

Figure 1: User-centered and flexible line management with zenon.

MULTIPLYING SUCCESS IN FOOD & BEVERAGE

The Ease of Rolling Out a Line Management System using zenon

TEXT: EMILIAN AXINIA,
INDUSTRY MANAGER FOOD & BEVERAGE

INTERNATIONAL CORPORATIONS are often not only characterized by their size, but by their complexity. Spread over multiple culturally and economically diverse countries, with production plants which have grown heterogeneously over time, food & beverage groups often face unequal levels of performance and unequal degrees of automation. To achieve global harmonization, corporate standards are rolled out step by step. Such standards will target all plant sectors, processes and resources, starting with obligatory quality prerequisites and progressing to the optimization of production costs and efficiency improvements. Defining milestones and KPIs for these developments helps corporate management to monitor and drive the progress of standardization and continuous improvement.

The ongoing transformation of such international organizations is usually strongly connected to the automation and IT infrastructure. When cohesive concepts have to be successfully implemented across many different food & beverage production plants, a key success factor will be the chosen technology and how profitably it is used.

Here, we look at a line management system from the perspective of a corporate rollout. A filling or packaging line is usually subject to very high performance expectations and is, therefore, a good example of how the technology embedded in the zenon Product Family pays off. Nevertheless, zenon's product philosophy and universality also enables a similar approach within other plant sectors as part of a corporate rollout.

PILOT PHASE: RICH IN EXPERIENCE

What to roll out? This question is the starting point for any rollout project team. Corporate standards, previous local experiences, internal competencies in automation and IT, and critical analyses of industrial standards will bring clarity here. User requirements specifications set out functional wishes in an organized way. But simply distributing such a document throughout the organization will not deliver the benefits of a corporate rollout. More likely, existing differences would be further deepened. Instead, the aim should be to establish real technological concepts which deliver tangible benefits. This is why a pilot phase is essential.

What is the secret of a successful pilot phase? For a professional project team it is more than playing with a nice local project example. The team should consider how exactly the rollout will work in plants with different automation landscapes and what hidden costs and risks need to be mitigated. Let's see how this works when using zenon.

"Every zenon system integrator, especially those active within the COPA-DATA Partner Community, represents a great choice as a professional engineering partner for corporate rollout projects in the food & beverage industry."

In terms of the functionalities of line management using zenon, the system delivers complete and reliable information flows for data acquisition, archiving, processing and analytics. The end user – whether an operator, line supervisor or manager – is supported by a wide range of tools to contribute decisively to the plant performance: process supervision, alarm and event management, parameter trend curves, key performance indicators displayed in dashboards, reports at line or machine level, changeover control integrated within production planning, and more – see *Figure 1*. zenon provides real-time information to support responsive decision-making and historical analysis for a deeper understanding of improvement potential.

What does this mean for the corporate organization? We at COPA-DATA find that software technology brings more ergonomics for production teams and essential help to continuously improve process quality, production and consumption effectiveness.

A pilot project has to answer many questions about integration and cost. The base of a line management system is its connection to any relevant production equipment or measuring systems – a strength of zenon. Old or new machines can be integrated independently of automation technology or supplier – so process parameters, status and context information, production and consumption counters are brought easily into the system. The next steps of archiving, displaying, trending or analyzing from different perspectives are supported by configurable out-of-the-box components in the zenon development environment. In comparison to other approaches where software code must be programmed, this results in an extremely fast system integration with plenty of possibilities, based on reliable software and sophisticated technologies.

It often surprises newcomers to zenon just how accessible the system integration is to a wide range of people; not just for advanced programmers. One direct effect of this is that the costs of a pilot project will remain reasonable. The freedom to choose who will integrate – existing or new project partners, internal personnel or members of the corporate project team – encourages creativity and transforms the pilot phase into a very rich experience. The modular development of the application, the system openness and the convenient horizontal and vertical expandability all work to help zenon answer the challenge of the food & beverage industry's particular dynamism.

If very particular or innovative functionalities have to be implemented, zenon is open and supports software programming in IEC 61131-3 PLC, VBA or modern VSTA languages.

There are many other innovative technologies and concepts enabled by the zenon Product Family capable of raising the technical enthusiasm of the project team and the value of the entire line management system: process simulation, interface usability, mobile solutions, Multi-Touch interface, Worldview, 3D-process visualization, automated project documentation, and the list goes on ...

ROLLOUT: ADAPTABLE, COST-EFFECTIVE AND COMPLIANT

The benefits zenon delivers during a corporate rollout go beyond delivering ergonomics to every member of each international production team in a standardized way. From an engineering point of view, it is desirable to use as much as possible from the pilot to decrease implementation costs and integration time of every local project. zenon projects can be integrated with any existing PLC or third-party software thanks to its hardware and platform independence. This ensures that the new line management system can be easily adapted, avoiding unexpected or expensive replacement costs.

zenon enables universal utilization within existing or new infrastructure thanks to over 300 native communication protocols and interfaces for vertical integration. Technologies such as XML import/export, object orientation with global, central or local configuration, template-based interfaces and numerous other mechanisms guarantee high efficiency in the zenon development environment. zenon's network technology supports the full reuse of a server project so a line management system can be extended with a client-server, web-server or mobile apps architecture over the corporate intranet or Internet.

zenon also spectacularly increases the speed of implementation through its wizard-based "Automatic Engineering". Applications can be generated first by using standardized components defined during the pilot phase, such as machine tags, calculation libraries, graphical symbols, screen templates, terminology within language translation tables, measuring units conversions, color codes, reporting templates and the like. Furthermore, user options deliver flexibility in local implementations. For instance, by determining the type of packaging machines, the PLC interface, the functionalities, etc.

Weihenstephan Standards and OMAC PackML are two industrial standards supported by zenon, which help efficient integration and the reuse of entire information flows in line management applications.

All these highly sophisticated technologies bring ergonomics in engineering to the ever-growing family of system integrators who deploy zenon. What does this mean for the rollout project team? You are no longer dependent on one company which owns all the "engineering secrets". Risk stemming from the availability and cost of particular system integrators can be avoided. You gain the freedom to choose from local, regional or global partners at any time.

A line management system today has more than a local relevance for any food & beverage production company. zenon enables local systems to be extended at a corporate level.

Acquired production data can be made centrally available via the IT infrastructure, including the company network, database systems, virtualization and even via the zenon Cloud solution. Highly available stored data opens the way for comprehensive reporting across entire international operations, based on zenon Analyzer. And zenon Everywhere Server supplies data for mobile apps in real-time without any geographic limitation while delivering state-of-the-art communication security.

In order to underwrite corporate change management, the multi-user engineering technology of zenon offers a central SQL-based storage for all engineering resources.

Figure 2: Dynamic Production Reporting with zenon.

With zenon, the rollout of a line management system addresses both local peculiarities and corporate conformity. Production teams and central specialists are equally well-served with information; making their optimization efforts easier. Real-time operation or historical analytics are accessible not only plant-wide, but throughout all corporate operations.

FURTHER IMPROVEMENT – A CONTINUOUS PROCESS

The food & beverage industry is a field where line management has to change and adapt regularly. Continuous improvement processes bring new ideas. These could include new ways of data analytics, correlations of data or innovations for the user interface. Newly installed machines or energy counters, the involvement of additional people, or demands for an ERP-to-HMI flow, will typically require adaption to the line management system. Therefore, even a successfully deployed system will likely be subject to extensions or modifications over time.

The expandability of a zenon line management system makes such changes possible, freeing the creativity of production managers. Plus, zenon's ease of engineering provides flexibility over who will implement any changes: your internal automation specialists, your favorite local system integrator or your favorite regional engineering partner?

zenon's licensing system follows the same "freedom of choice" principle for updates and extensions. The initial investment is protected by backward compatibility in the development and runtime system for heterogeneous project networking.

The consequences of keeping engineering costs low despite high flexibility are evident and are a prerequisite for a reduced total cost of ownership (TCO).

THE FREEDOM TO DRIVE GREAT PERFORMANCE

In conclusion, the zenon Product Family represents a development framework for line management systems and many other applications combining maximum openness and flexibility with high-performance automation and IT technologies embedded within reliable ready-made components.

COPA-DATA strives to eliminate unnecessary creativity constraints and dependencies, making every zenon system integrator, especially those active within the COPA-DATA Partner Community, a great choice as a professional engineering partner for corporate rollout projects in the food & beverage industry.

Innovative software technology and engineering is enabling international groups to gain freedom and optimization in all the steps of their strategic projects and with all their related costs.

TECHNOLOGIES SUPPORTING YOUR ROLLOUT PROJECT

- Entire zenon Product Family
- zenon development environment with efficient engineering
- Hardware independence through more than 300 communication protocols
- Native multi-language support
- Flexible and secure network, client-server and redundancy
- Automatic engineering
- Vertical integration, e.g. with Process Gateway
- Microsoft Dynamics interfaces
- Integration of Microsoft Azure Cloud
- Dynamic Production Reporting
- Message Control
- Everywhere Server for mobile apps

http://kaywa.me/I0JJx

Line Management with zenon
Watch our video!

The Automated Substation

[PART 3]

ERGONOMIC OPERATION

After focusing on ergonomic engineering *(IU No. 25, April 2014)* **and ergonomic implementation** *(IU No. 26, November 2014)* **we are now addressing the topic of ergonomic operation in this third and last part of our Energy topic series on automated substations.**

TEXT: JÜRGEN RESCH,
INDUSTRY MANAGER ENERGY & INFRASTRUCTURE

OPERATION of a substation is then ergonomic, if everything works like clockwork and the substation can stay unmanned. Yet sometimes it may be necessary for the plant to be staffed. It is important in such cases, to give even untrained employees a tool with which they can intuitively work.

INTERLOCKING AND USER RIGHTS

First of all, a possible operating error should be prevented by the system itself. For this, a switch gear protection is used to catch the user's attention. Here interlocking and topology check support command input. The system detects, independently or via preconfigured rules, that a certain (switch) handling can have a negative impact on the equipment.

To be sure that only authorized employees can edit commands, the user administration verifies if the user has the necessary access rights. The zenon-based user administration, which is also combinable with Windows Active Directory, is also used in the pharmaceutical and food industries due to its security benefit.

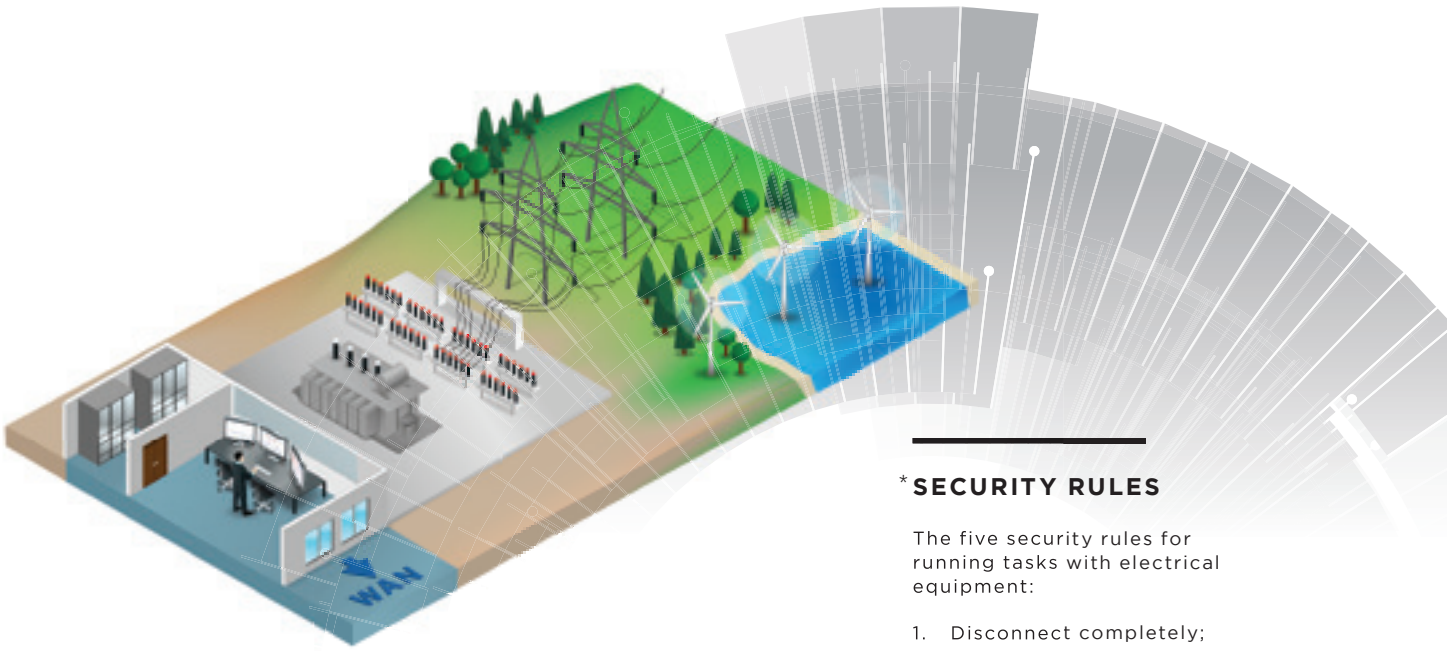
WATCHDOG TIMER

Critical events often involve many switch operations to be carried out directly one after another. The user can not however wait for every disconnector to reach its final end position, but must proceed directly to the next action. So that intermediate positions are not overseen, zenon can bring the user's attention to it via alarm or a blinking symbol. The so-called watchdog timer is an integral part of zenon's command input.

SWITCH LOCK / COMMAND

In order to fulfill the second of the five security rules "Secure to avoid reconnection", the switch lock is an integral part of the command input module. Per locking code, a switch is put into a mode in which it is no longer possible to control the switch. Only after taking various steps, including entering a lockout code, can the switch be used again, and that across the zenon network. The locking and unlocking of the switch is logged in the chronological event list.

zenon's command input is capable of much more than the standard commands of ON and OFF: Switches and variables of entire branches can be switched to revision (no alarm), decoupled from the process (no data transfer) or switched to a replacement value (no data transfer and new value for the system).



MANUAL DATA HANDLING

Switches that are only available in the screen but not (yet) transmitted, can be brought into the according position with so-called manual correction.

BREAKER TRIP DETECTION

Immediate information regarding an independently triggered circuit breaker is then important if, for example, the protection relays aren't yet reported. zenon can notify the user in the form of alarms or special display of symbols. Furthermore it is possible to suppress the switch operation detection, for example through the connection with a place/remote control switch.

LOGGING VIA CEL, AML AND ARCHIVE

For automatic and timely accounting about equipment operation, the Chronological Event List (CEL) delivers information. The CEL displays all configured messages as well as messages on the system itself. The required information for analyses and reports are put together via filters. The list is stored in the system in a binary format, so that it cannot be manipulated later. Furthermore, the operator can comment on the list entries for more efficient traceability.

Other than the Alarm Message List (AML) in which numerous and filtered alarms and their statuses are displayed, zenon also recognizes so-called alarm areas. This can lead the on-site employees from the aggregated alarm overview to the detail view of the actual problem. A further component which makes up an ergonomic process control system.

Besides the events which are displayed in the Chronological Event List or in the Alarm Message List, the data can also be logged in a measured-value archive. Therefore all data from the process is made available for analyses and reports. The measuring curves can be precisely assessed in the trend display and compared with binary signal states or other measuring curves. Typically counter values are evaluated in reports, displayed in tabular or graphical form, stored, printed or forwarded via data transfer.

Fault records from protective relays can be read manually or even automatically and stored in the system or passed on to the superior instance (control center). Such automatism is made possible thanks to the appropriate fully-implemented IEC 61850, IEC 60870, DNP3 or FTP protocols.

*SECURITY RULES

The five security rules for running tasks with electrical equipment:

1. Disconnect completely;
2. Secure to avoid reconnection;
3. Verify that the installation is dead;
4. Carry out grounding and short-circuiting;
5. Provide protection against adjacent live parts.

FAST FACTS

- Automated unmanned substation; but still user friendly
- Topology check
- Command input – interlocking
- User administration
- Command input – watchdog timing
- Command input: revision, decoupled, alternative value
- Manual correction, switch locking
- Breaker tripping detection
- Chronological Event List
- Alarm management – user guidance
- Archiving, trend analysis
- Reports
- Reading, saving and forwarding fault records

You can find further information about exciting energy topics and zenon energy solutions at www.copadata.com/energy.

ZENON AS AN EARLY WARNING SYSTEM IN AUTOMOTIVE PRODUCTION

Reduce Production Losses in a Targeted Manner

Today, automotive production is characterized by large, global production and logistics networks. Production downtime comes at a high financial cost. It is therefore all the more important to react quickly to interruptions and deviations from the plan and be able to introduce efficient reaction mechanisms and countermeasures.

A PRODUCTION FACILITY FREE OF PROBLEMS – that's the dream of every automotive manufacturer: no interruptions to production, short and plannable lead times, no waste from defective products. This would guarantee reliability and a stress-free working environment. At the same time, the quantities produced could be planned and controlled with absolute accuracy. This absolute freedom from interruption does not exist of course, but there are means and methods to achieve shorter lead times and to limit downtime to a minimum. With zenon, automotive manufacturers can implement rapid-reaction fault management and implement dashboards that always show all current key performance indicators (KPIs) in a clear overview.

AN EARLY WARNING SYSTEM WITH ZENON

If automotive manufacturers implement their fault management with zenon, they are not only able to detect problems in a production line at an early stage, they can also communicate them to neighboring equipment or equipment areas along the entire production chain. Therefore, all other manufacturing employees can be informed of a possible production standstill and the likely duration of the problem – even before it occurs. An example: in the event of the equipment coming to a standstill, zenon shows a 15-minute stoppage of the equipment in question on the zenon client, on the basis of having determined the average duration of similar stoppages. Depending on how full the buffer is, this problem may affect other equipment, both upstream and downstream. zenon can now calculate the duration of the interruption that may occur on neighboring equipment, based on the information available. The production managers involved can instantly see the mean values of the interruption time displayed on their zenon clients.

The affected decision-maker has, as a result of this information, sufficient time to consider suitable measures in case the interruption occurs. This might be a group meeting, a break, equipment cleaning, TPM, autonomous maintenance, replacement of spare parts, etc. in order to use the expected downtime effectively.

INFORMATION – AT ANY TIME AND EVERYWHERE

In production, and in fault management too, it is important that a consistent flow of information is guaranteed. Regardless of where the people in charge are, they must receive all relevant information in real time. COPA-DATA ensures the necessary platform independence here and thus enables timely reaction: with the Everywhere App by zenon, managers can have all the information that is relevant to them, such as equipment status and production figures,

displayed on end devices such as smartphones, tablet PCs or smart glasses. Logging in to the zenon Everywhere server with their user name and password is all that's required to access user-specific data. When incorporating this mobile solution into existing infrastructure, all common security functions are supported.

KPI-BASED OPERATION

However, it is not just rapid-reaction fault management that is the basis for short lead times, but also the constant monitoring of decisive KPIs such as the degree of usage, overall equipment effectiveness (OEE), the rate of defective units and employee productivity. These figures provide production managers with information about the efficiency of production at any time. With zenon, automotive manufacturers can prepare these figures and thus form a "single point of information", which contributes significantly to an increase in effectiveness.

INDIVIDUAL FIGURES FOR DIFFERENT TARGET GROUPS

In production, there is a massive amount of data generated, every hour of every day – with a different degree of relevance for the target groups such as production manager, maintenance worker, service technician, etc. For the production manager, the quantities produced or the defective waste goods that were produced are most relevant, because they can and must have a direct influence on these results. In contrast, senior management is interested in plant-wide, key financial figures that reflect both current productivity as well as competitiveness.

However, each key figure considered in isolation does not form a well-founded basis for a decision. These figures must be put in an overall context so that production managers can make the correct deductions and implement the correct measures. The OEE comprises, for example, three key figures: availability, quality and output. This means that there are three things that can be adjusted that can change overall equipment effectiveness significantly. zenon displays complex interrelationships of this kind in a real-time synchronized management cockpit – accessible at any time and in any place by the appropriate target group.

HERMANN OSWALD,
KEY ACCOUNT MANAGER
AUTOMOTIVE

zenon as an early warning system – your added value

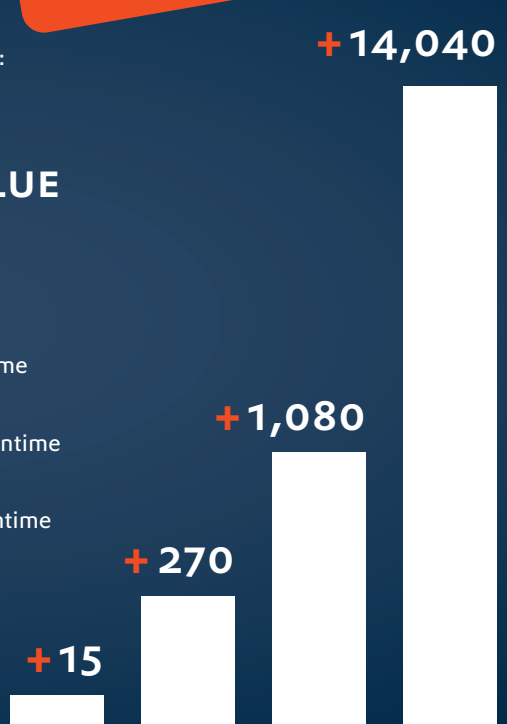
EXAMPLE / ASSUMPTION:

Production line in automotive production;
6-3 model (three-shift operation)
Cycle time = 1 min; amount of downtime (≥15 min):
1 period of downtime (≥15 min) in each shift

OPPORTUNITY: ADDED VALUE IN QUANTITIES (UNITS)

1) +15 units with one period of downtime (≥15 min) per shift *
2) +270 units per week with one period of downtime (≥15 min) per shift *
3) +1,080 units per month with one period of downtime (≥15 min) per shift *
4) +14,040 units per year with one period of downtime (≥15 min) per shift *

* as a result of taking action early (e.g. TPM) or effective use of the downtime.



"Death rates fall by 15 % after handheld devices replaced paper charts at hospitals in Coventry and Portsmouth, England."

Paper on Glass

THE MOMENT THE PENNY DROPPED

A news article recently caught my eye: *iPods save 750 lives during hospital trials.* **It detailed a recent study focusing on two hospitals in the UK collectively testing the use of Apple iPod Touch devices on the wards to record each patient's vital statistics. Very positive results were recorded: in one year 750 fewer patients died following the introduction of the new system.**

MOST OF US, at one time or another, have had the unfortunate experience of being in the hospital – either as a patient or visiting. Do you remember the chart hanging on the end of the bed? It's the chart that we all look at, feigning some latent medical knowledge and, for the most part, understanding nothing.

Well, it appears we were not alone in finding it difficult to interpret the chart. One nurse reports that "The old paper charts were very, very difficult to decipher. The crosses and arrows were written on the chart by the previous nurse and you couldn't distinguish where the cross was."

"With the new iPod system everything is color-coded, in more detail and accurate which means you can read it and you are more obviously able to see whether your patient is the same, better, or worse."

The nurses' procedure on the ward round is to ask the patient certain questions, measure certain clinical values and record the data on an iPod Touch device The vitals of each patient such as blood pressure, heart rate, oxygen levels, temperature, general well-being, and pain levels, are available live, with a history of readings displayed over time.

If we view the whole process in terms of the patient experience, very little has changed. The paper records of regular patient checks have been replaced by electronic records on tablets. The rules and procedures a nurse or

doctor follows are exactly the same: patients have the same operations, with the same aftercare. The only change to the nurse is a small mobile device in place of a paper chart. Yet more useful and accurate data is gathered through the use of appropriate software, recording is never missed and care can now be targeted on those who need it and at the right time. It is fast, convenient and easy to use.

The bottom line is that 750 fewer people died in one year. The study was small, covering only two hospitals in a small corner of England. However, using exactly the same medical procedures and very little investment they have gained major benefits (especially if you are one of the 750!). If replacing hospital paper charts with medical software on mobile devices can achieve so much and change the lives of so many, where else can one replace paper charts with electronic records to such a positive effect? Take a look at the similarities we find using zenon in paper-based pharmaceutical batch production.

Process industries, particularly regulated life sciences, talk a lot about CQAs (Critical Quality Attributes). CQAs are process variables that enable us to monitor crucial stages of manufacturing. CQAs have strict control limits since any violation directly impacts product quality, possibly rendering it toxic and hazardous to a patient's health. In normal practice, a CQA has several warning stages indicating when the process is pushing the limits of acceptable performance, leading eventually to violation levels stating that an "out of tolerance" has occurred.

CQAs can be any measurable value in the process, for example temperature, pH or O2 levels, blending time, or tablet press speed. It is clear that a wide variation in any of these values would produce a product which is out of tolerance for a variety of reasons e.g. drug strength or potency, tablet coating imperfections or tablet hardness.

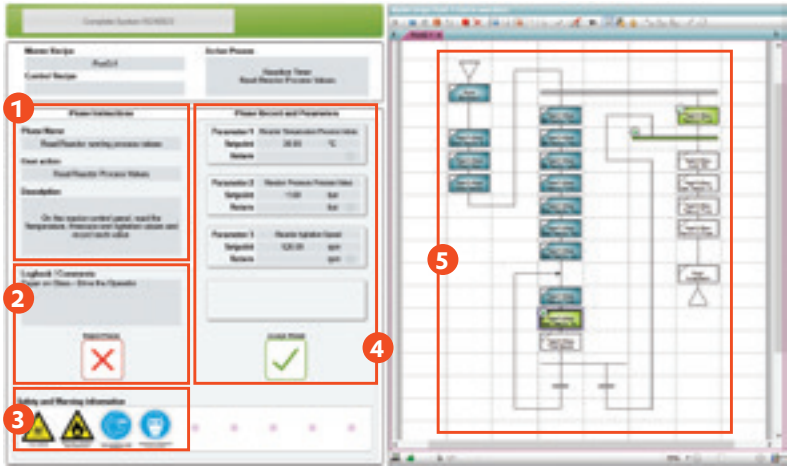
Swapping the paper-based operator instructions and paper-based batch records for a zenon-powered mobile tablet enables operators to record vital CQAs directly into a safe electronic system, then lets zenon's functionality expose opportunities never granted to manual production before. This is 'Paper on Glass'.

Paper on Glass uses zenon's Batch Control module to provide clear instructions for each task the operator needs to perform, e.g. a phase/step name, a user action, and a detailed description. Batch Control also prompts the operator to record information at certain times during specific points in the process, with an electronic logbook to add comments. The user interface enables inputs by the operator and the Historian archives the data. zenon pushes the final archived data to the Report Viewer or zenon Analyzer to provide batch reports, analysis data, material information, equipment information, a full audit trail and alarms. It can be operated stand-alone or as a client-server system.

When I recently introduced Paper on Glass to a veteran zenon user, I didn't expect the very passionate negative response:

"Not connecting zenon to the process? This is not useful. zenon's strength is about bringing automation and systems together."

Figure 1: zenon Paper on Glass application screen.



1. Name and description of the user action to execute
2. Comment must be entered before phase is rejected
3. Safety information and protection advice
4. User requested data must be complete before phase is accepted
5. Batch Control module commands production sequence

And then the penny dropped! Pharmaceuticals producers can't always make changes to equipment or, rather, certain quality and compliance obstacles are extremely difficult to overcome when making changes to validated equipment. COPA-DATA offers an additional solution, filling the gaps in current processes, and placing the latest technology on legacy systems.

This is the point when the veteran zenon user understood that the concept Paper on Glass is precisely about bringing processes together with automation: Keep the same processes, interface to the operator ergonomically, don't change the equipment, and don't change the procedures. Put the electronic recording into the operator's hands, secure the data and gain consistently accurate and detailed results.

The concept of Paper on Glass came from processes which are completely driven using paper Standard Operating Procedures (SOPs) and paper batch records. The operator is central to managing production execution and the recording of critical data. This user-centric environment holds a very important key to production success: how to deal with abnormality in a very complex critical process. The operator can react to any event, and avert events from critical failure. Loss of revenue in this costly production environment is mitigated with this user-centric approach.

Any zenon project can be expanded using the scalable modular functionality at zenon's core. Paper on Glass is no exception. Step by step the operator can link Paper on Glass to automated equipment and embrace the shades of gray between 'Manual' and 'Automated' environments, viewing both as one system, and integrate dated legacy processes with new technology. No gaps, no white spaces in the process, bridging quality across all production operations, controlling as one continuous process.

Having the tablet guide the operator through a production sequence, replacing paper instructions and the paper recording of critical data is only the start of this story. The benefits of zenon go further. It is reported that "Right First Time" when using paper in pharmaceutical production is less than 50% – with two thirds of rejects and reworks being caused by simple human errors such as missing the recording of a CQA, entering an incorrect value, or losing a paper record. We are talking about simple errors which, in the course of events, will happen time and time again.

Exactly as with the hospital study, by simply changing the mode of operator interface so many benefits are realized without changing the production process or the validation qualification state of these processes:

POINT OF ENTRY VERIFICATION

When a user writes a value on paper, it could be many weeks before the value is read again. Paper on Glass monitors the process in real-time and the value is checked against warnings and limits – instantly informing about any process violations. We can force the operator to acknowledge and verify the truth of this value, or we can force a different person (e.g. Quality Assurance) to verify the value. Automatically react to process exceptions and use Message Control to involve the right people at the right time before a critical event escalates.

Figure 2:
Point of entry verification screen which pops-up when a warning or violation has been entered. The operator either has to acknowledge that the value is correct or enter a modified value. A comment must be given. Having the verified value and a comment reduces the number of investigations as complete data is recorded.

REDUCED OPERATOR TRAINING

Paper SOPs only give information regarding user actions, there is no description or physical sequence. Paper on Glass gives very clear instructions, detailed descriptions, and safety information at each stage of production. With less for the operator to remember, less can go wrong.

BATCH-TO-BATCH CONSISTENCY

The Batch Control module executes recipes in a strict automatic sequence. In this manner, no stage can be missed, diverted or delayed. Each stage has a time-stamped confirmation of its execution.

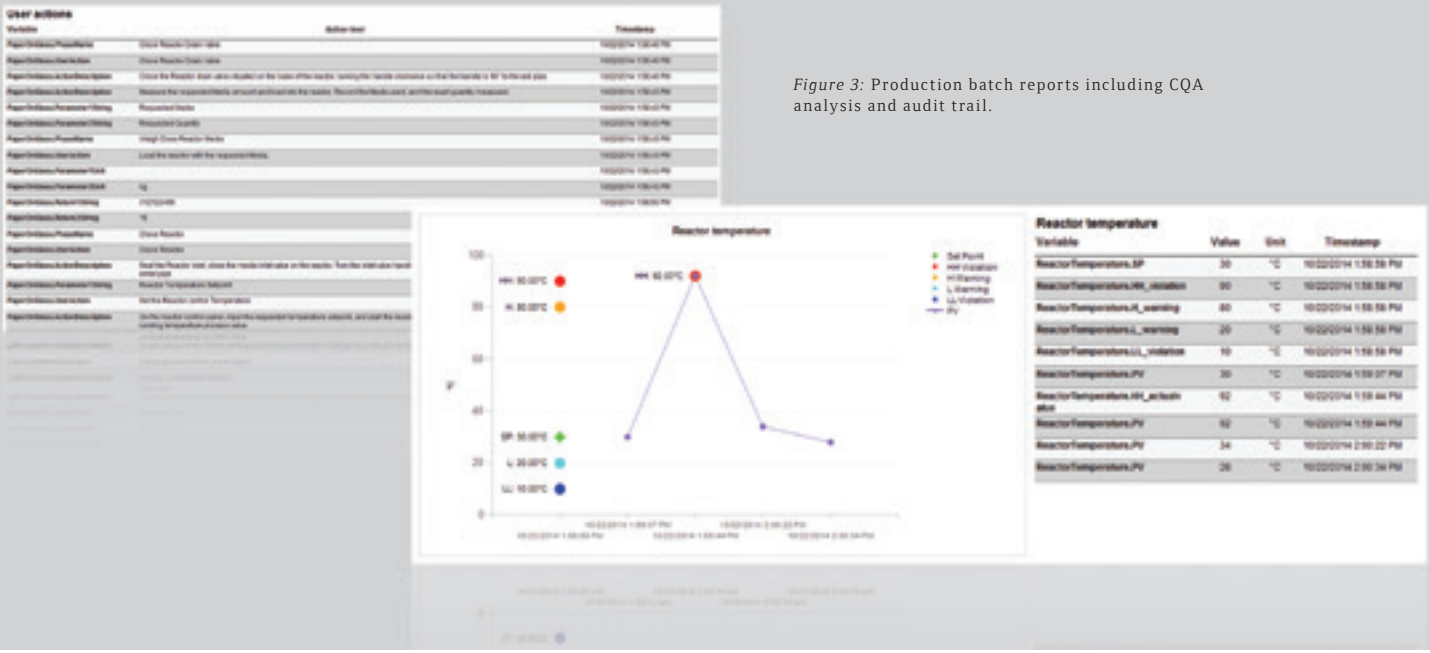


Figure 3: Production batch reports including CQA analysis and audit trail.

AUTOMATIC COLLATION OF DATA

Entered values go directly into the central zenon Historian. At no stage can requested information be overlooked, and so the company has complete, time-stamped and clear batch documentation. With central storage of process data, the tablet can be lost, dropped, smashed, or stolen, and the data is still safe. A batch has typically around one thousand manual entries. With paper activities, documentation needs to be manually collated and entered into electronic systems for analysis and reporting. Paper on Glass reduces post-batch tasks and the head count in this critical process.

POST-BATCH ANALYSIS: BATCH REPORTS ARE AVAILABLE INSTANTLY

The instant the batch finished, complete batch information is available and archives are accessed by the Report Viewer or zenon Analyzer to produce analysis and final compliance documentation. Reports give clear and precise information on CQAs, materials, equipment, operator actions and comments. Paper-based environments need an additional 10 - 30 days post-batch. Paper on Glass significantly reduces post-batch analysis time, and reduces the effort involved in producing compliance documentation.

COST AVOIDANCE

Paper is costly. It needs to be printed, tracked, and stored in environmentally secure areas over the long-term, with storage durations of eleven years being common. Paper on Glass requires no paper to drive production, thus no large scale storage of paper is needed. Given that the pharmaceutical branch uses a lot of paper, this is a huge cost advantage.

Paper on Glass offers the latest technology to complement manual processes, embracing legacy processes with new equipment. It is a simple and elegant cost-reducing solution that improves operational performance.

zenon's Paper on Glass is a complete batch solution in the palm of your hand.

ROBERT HARRISON,
INDUSTRY MANAGER PHARMACEUTICAL

REFERENCES

Lisa Dowd.
'iPods Save 750 Lives During Hospital Trials'. September 24th 2014.
http://news.sky.com/story/1340999/ipods-save-750-lives-during-hospital-trials

Andrew Gregory.
'Nurses save nearly 800 lives a year by using iPads, iPods and mobile phones instead of paper charts'. September 24th 2014.
http://www.mirror.co.uk/news/uk-news/nurses-save-nearly-800-lives-4315486

zenon is the Power Behind a Major Upgrade Project

COPA-DATA ENERGIZES POWERLINK QUEENSLAND'S HMI SYSTEMS

TEXT: BERNHARD KORTEN,
INTERNATIONAL SALES MANAGER

Queensland's high-voltage electricity transmission network provider chose zenon to carry out a major upgrade to its HMI. COPA-DATA's commitment to 'parameterization instead of programming' enabled a cost-effective and highly-functional solution without the need for an expensive recommissioning effort.

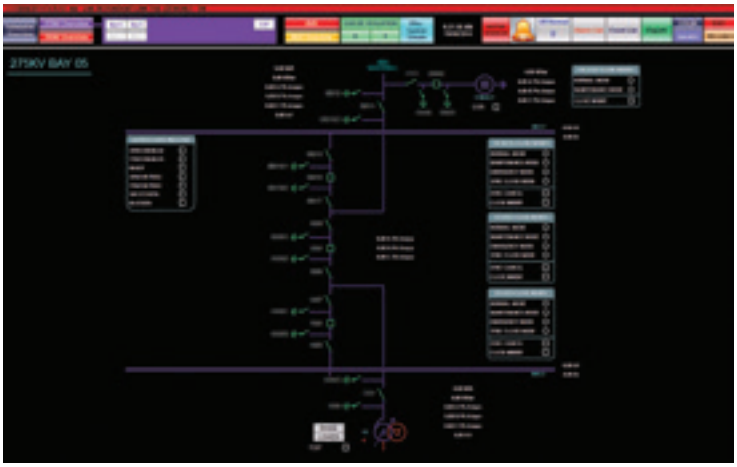


Figure 1: IEC 61850 Substation – Detailed Bay Screen
While immediately recognizable (by Powerlink) as an IEC 61850 design, it is similar in look and feel to the legacy systems.

POWERLINK QUEENSLAND operates, develops and maintains Queensland's high-voltage electricity transmission network. The transmission network extends along almost half of Australia's eastern seaboard; it stretches 1,700 km south from north of Cairns to the New South Wales border. It includes more than 15,000 high-voltage transmission circuits, 132 substations and employs over 1,000 people.

In 2011, it was evident that Powerlink's existing Foxboro/Invensys HMI platform needed replacing. The existing hardware had become obsolete and there was no simple solution for maintaining or expanding this platform. An alternative solution was required and, because a new SPARC platform was ruled out, an automated conversion process to a new HMI platform was needed.

At the same time, Powerlink needed a new HMI solution for its in-house IEC 61850 station bus system, which included protection, bay control, network, gateway, and HMI design, configuration and testing.

SELECTING ZENON AS THE CENTRAL HMI PLATFORM

Powerlink began evaluating HMI software in 2011 and selected COPA-DATA's zenon software as its preferred HMI solution. zenon was selected due to the:

- ease of engineering
- built-in IEC 61850 and DNP3 process drivers
- XML import/export of all design objects
- VSTA and VBA programming interfaces
- zenon Logic IEC 61131-3 capabilities

Powerlink also found COPA-DATA's close relationship with Microsoft an attractive reason to select zenon as its preferred HMI solution.

Powerlink Queensland's goal was to find a single HMI solution which would meet all of their requirements – both in terms of a replacement to their Foxboro/Invensys system and as an HMI for their IEC 61850 station bus system.

A NEW IEC 61850 HMI SOLUTION

Powerlink's internal design standards team develops and maintains the secondary systems design standards. This enables Powerlink to take advantage of external design resources as required while ensuring a consistent design state-wide and maintaining internal design expertise. The new system needed to meet the team's requirements in terms of performance, control features and functions, alarms, events, security, user administration, remote access, internal logic and graphical display functionality while being cost-effective as well.

zenon's design capabilities have enabled a similar look and feel to the existing HMI solutions. With over 100 installations of the previous generation HMI, this was vital for Powerlink Queensland to ensure consistency and ease of use.

zenon has subsequently been used to visualize Powerlink's GOOSE isolation implementation, its station bus network and to monitor the status of buffered reports on all server IEDs.

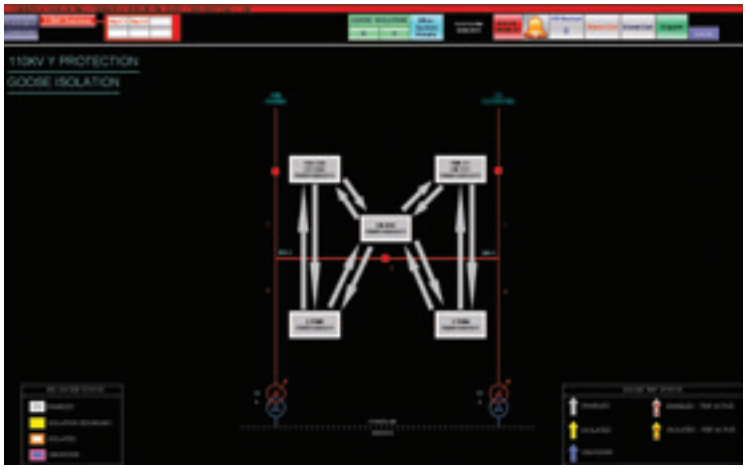


Figure 2: GOOSE Isolation - Remote Web Client
Remote access via Web Client without difference to the local substation interface.

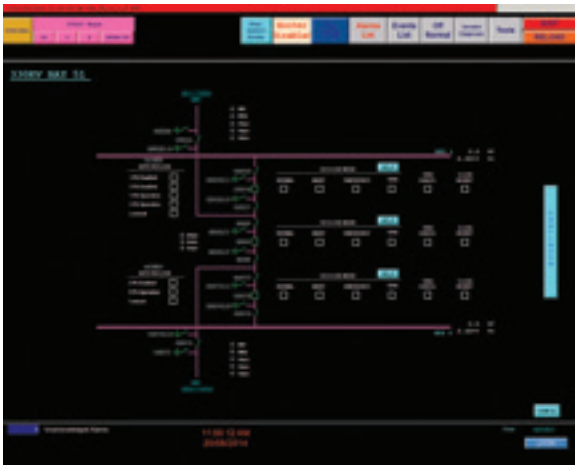


Figure 3: Legacy system converted to zenon 7.0
With little to no compromise, the converted legacy systems look and feel identical to the original system.

RAPID COMPLETION OF THE DNP3 LEGACY PROJECT

zenon also provided Powerlink with a fully-tested and automated way of converting from an existing, yet no longer supported HMI into a completely new platform without the need for a time-consuming and expensive recommissioning effort.

zenon is simple and quick to engineer, and offers many options to automate design inputs. With basic automation, Powerlink has been able to reduce design time and the associated costs.

These time-saving results were achieved through a number of key zenon features:

- zenon's parameterization enabled the simple reuse of standard objects and functions with minimal engineering,
- the zenon Logic IEC 61131-3 interface to the zenon Runtime allowed for the simple emulation of functions that were specific to the legacy HMI, and the creation of new functions,
- VSTA allowed for the creation of simple import wizards that automated the import of files and project-specific settings using a proven, consistent process that required minimal user input,
- zenon's XML import/export for data points, screens, functions and alarm groups, facilitated simple process automation within rapid development timeframes and with high levels of consistency.

Powerlink Queensland will be happy to enjoy further savings. Project and file management is simple and flexible, depending on the requirements. Local management of the Runtime files with or without the zenon Editor enables them to work on their current processes. Remote project and file management options provide them with scope to streamline their processes as their confidence with the product and surrounding infrastructure grows. They will no longer need to send two people driving for six hours to a remote site to make minor changes or fix defects as these can now be performed remotely. This would potentially provide cost savings, allow resources to be used elsewhere and have obvious safety benefits.

A SINGLE, EFFECTIVE SOLUTION

In addition to the individual requirements of each project, both applications had to support:

- running the Runtime on a virtual machine,
- local access (within the substation) to the Runtime visualization with a Thin Client (WYSE terminal) via substation LAN,
- remote access to the Runtime visualization over WAN,
- automatic daily exports of events in a text format,
- automatic activation of external audible alarm when a new alarm is generated,
- project comparison utilities to identify the exact changes between projects so a complete scope of work for testing/retesting can be established,
- project change logging capability to provide complete audit trail of project development,
- diagnostic tool to investigate communication errors.

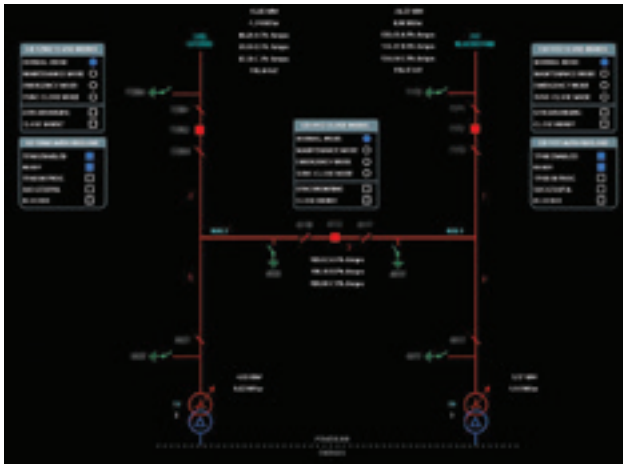


Figure 4: 110 kV IEC 61580 substation, Powerlink's first in-house developed, designed, tested, and commissioned IEC 61850 station bus solution.

Finding a single HMI solution which could meet these common requirements and both sets of project requirements will be a huge advantage for Powerlink Queensland. Choosing zenon allowed them to settle on a single product for both their new IEC 61850 systems and legacy DNP3 systems. This has reduced the incline of Powerlink's learning curve, enabled rapid project delivery and saved money. With the legacy systems, their choice to use zenon has avoided the need for recommissioning, redesign and outages.

A GREAT PARTNERSHIP

Over the course of the project, Powerlink identified some areas where some of zenon's existing drivers were not able to fulfill in full the application requirements. In response, the COPA-DATA support team provided a driver update for the zenon IEC 61850 driver and an enhanced DNP3 driver within a short period of time. This close collaboration and the support provided to date by COPA-DATA has been well received by the Powerlink team.

COPA-DATA TECHNOLOGY IN USE

- zenon Energy Edition
- zenon Logic
- Web Server
- Web Client
- Drivers: IEC 61850, DNP3, SNMP
- Gateway: OPC UA Server, DNP3 Outstation, IEC 61870 Slave, Modbus Slave, SNMP Server/Agent

ONE HMI FOR ALL APPLICATIONS

- Simple, flexible engineering which reduces costs of development and enables rapid project delivery
- Concise visualization for screens including: high-level substation line diagram, voltage-level line diagram, switching plant and bay-specific visualization, device health summary overview and secondary system connectivity.
- Supports multiple instances of DNP3 including combinations of Serial and IP
- Automated conversion from the Foxboro database format to the zenon database format
- Automated conversion of SAMMI screens to equivalent zenon screens, functions and frames
- Reuse of standard symbols from the legacy HMI
- Supplemented by standard symbols in zenon (circuit breakers, isolators, earth switches, etc.)
- Provides essential control functions and operator feedback
- Alarm, event and off-normal displays, including link to external audio alarm.

AROUND THE WORLD

COPA-DATA Italy 15 Successful Years

"INNOVATION AND EXPERTISE ARE KEY FACTORS FOR SUCCESS."

In his interview with *Information Unlimited* Magazine, Klaus Rebecchi, Managing Director of COPA-DATA Italy, talks about the achievements over the last 15 years and his future plans.

PHOTOGRAPHY: LUIGI CAPUTO

How did things start out for you at COPA-DATA Italy?
KLAUS REBECCHI: It all began in the summer of 1997. At the end of the 1990s, COPA-DATA Headquarters wanted to take steps towards internationalization with the goal of opening new branches. I met with the Punzenberger brothers at the Salzburg office, and we all agreed on zenon's potential in the Italian market, so we took initial steps for the launch of the software in Italy. The very first sales and marketing operations were run from a small office near Bolzano. In 2000, we opened our first proper subsidiary. From then on, we began to develop the significant potential of the Italian market.

Can you tell us a little bit about your team? How is COPA-DATA Italy structured?
KLAUS REBECCHI: In 2000, we started out with just three of us. I took care of sales and my two colleagues worked on license order management and technical support service, respectively. Business did very well, so in 2004, we expanded our facility by hiring two area managers for north and north-west Italy. Together we began introducing zenon to the Italian market. I am very pleased to say that both area managers are still working with us. Over the years, we built up our technical department, which now consists of four employees. Clearly, all of them are zenon experts, but each of them also has specialized experience. From 2008 onwards, we were able to increase our market share despite a challenging macroeconomic environment, and we could hire new employees for the Marketing and Administration departments. Just a couple of years ago, we moved into our new 400 m^2 offices in order to lay down the foundation for future growth. We recently welcomed two new area managers aboard to join our team. Now there are twelve of us. Each of us has his/her own area of responsibility and is able to add his/her own professional qualification. However, we are united in our objective: continue to sell one of the best HMI/SCADA systems in the world in the Italian market.

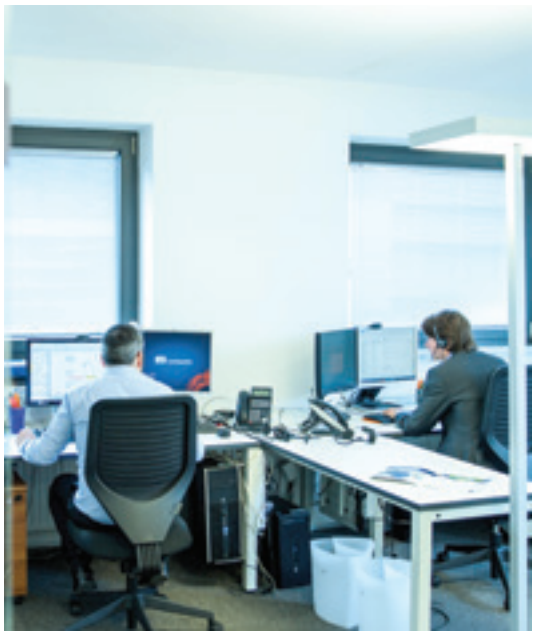
What is COPA-DATA Italy's secret to success?
KLAUS REBECCHI: Most of the credit goes to the product and its high level of innovation, of course. While primarily used as HMI/SCADA software, zenon also acts as a dynamic production reporting system and is very ergonomic and flexible. The zenon Product Family not only meets the most diverse demands. Moreover, our product is valued because our customers are optimally supported for secure and speedy development, no matter how complex.

Another factor is our market position. Our objectives are clear, as are the industries we want to work with. Over the years, we have established ourselves in the Italian energy & infrastructure sector. We have won important customers in the food & beverage industry while we have also made first acquisitions in the pharmaceutical industry, and are very pleased with our development in the steelmaking industry as well.

Our know-how, experience and the references we have been able to build up over these 15 years also contribute to our success. Customer satisfaction is our number one priority. Keeping close contact before, during and after project design and implementation, as well as a reliable and expert Customer Service Department complete the support cycle.

What are some of the challenges Italian businesses are facing today?
KLAUS REBECCHI: I believe that the challenges are pretty much the same for everyone: produce more, in less time and with better quality. At COPA-DATA Italy, we are seeking to assist our customers in overcoming these challenges. Our solutions are easy to use and reduce operator training time. zenon is simple to set up, which greatly reduces application development time. In addition, there are clearly many functions that help save resources. For example, it is becoming ever more important to keep control over energy and raw material consumption. Therefore, an Energy Data Management System such as ours is becoming essential for reducing costs.

Our customers are faced with a further challenge: For years, they have been storing huge amounts of data on different media, and they will continue to do so in the future. We have all come to understand that this data should not just be filed away and only pulled out in case something goes wrong or for compliance. This data is a highly valuable asset that needs to be interpreted. The question now is: How can we transform this enormous quantity of data into clear and simple information, which we can use to help uncover the hidden potential in our plants? Not only do we offer a complete Business Intelligence solution as well as one for Big Data management, we also give access to the data our customers need anytime and anywhere. If they desire, they can also store the data in the Cloud.



What is the added value offered by COPA-DATA to its customers?

KLAUS REBECCHI: First of all, we offer our know-how and experience. We assist our customers every day through our technical service support and consultancy. The expertise brought in via the COPA-DATA Partner Community can also offer further value. In Italy, we have successfully created a network of professional partners, all with many years of experience in creating industrial automation projects for every industry, all of whom are very familiar with the zenon technology. Thanks to these partners and continuous teamwork, we are capable of offering our customers complete, turnkey solutions.

What are COPA-DATA Italy's plans for the next five years?

KLAUS REBECCHI: Clearly, our main objective is to continue to grow, to obtain new important customers in all sectors of industrial automation and to grow our market share. To achieve this, we intend to continue developing and updating our competencies. We also strive to keep our role as pioneers in communicating and bringing innovative and highly technological solutions to the Italian market.

We want to work on current issues such as Smart Factory, Industry 4.0, the Internet of Things, Big Data, the Cloud and Cyber Security just to name a few, while keeping our outlook projected towards the future, seeking to understand today what will be needed in three to five years and beyond.

Last but not least, we aim to strengthen our business relationships with our partners so we can continue to offer our customers the best solutions, both in terms of products and services.

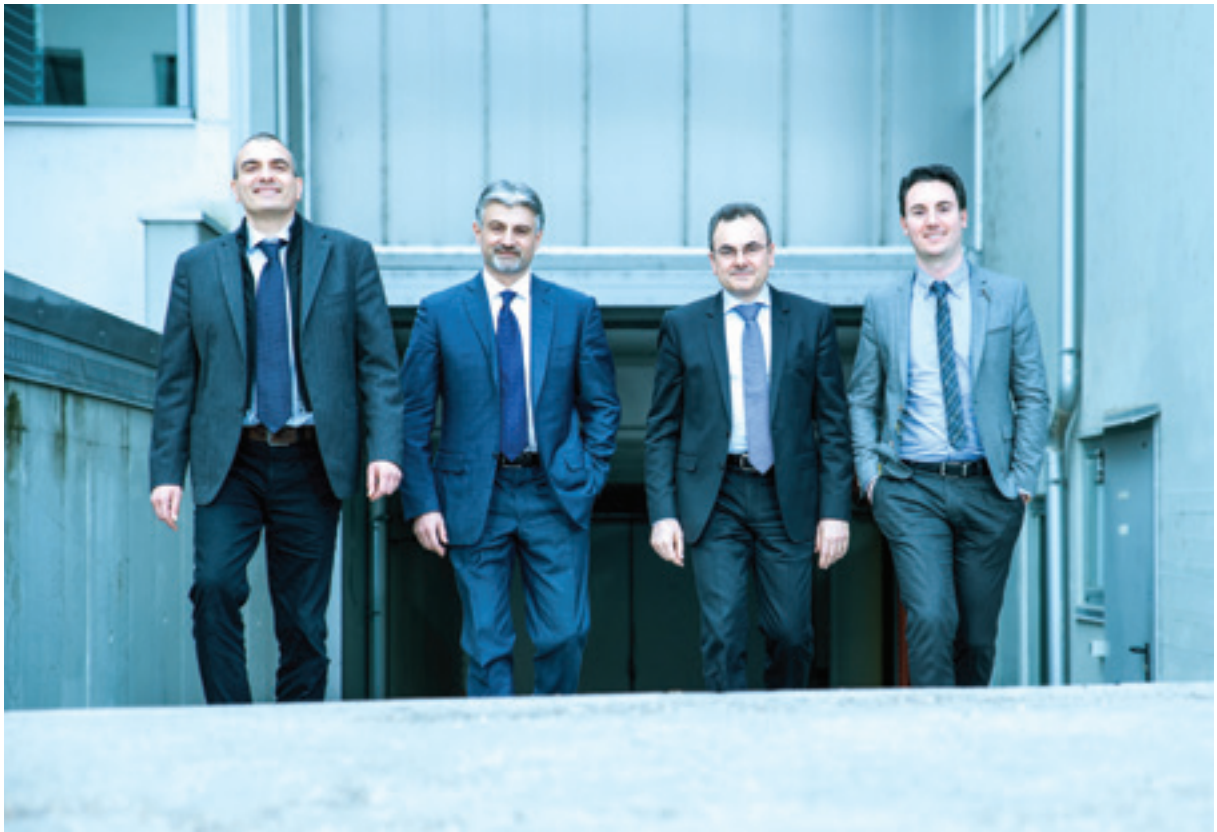
CONTACT

Ing. Punzenberger Copa-Data Srl

Via Pillhof 107
39057 Frangarto, Bolzano
Italy

t +39 (0471) 674134
f +39 (0471) 674133

www.copadata.it
sales@copadata.it



WHO IS WHO

The topic of security obviously includes personal privacy. And we take this very seriously, especially when it comes to the people we work with. So we won't be revealing any secrets here, no slip-ups and you also won't be finding out where you can best find our professionals after work. But you will get to know some of our employees from a very different perspective. Because we like to let them have their own say. That way, they can best decide what we should know about their lives, preferences, their professional responsibilities and their opinions. Let`s be surprised!

Maarten van Dam

INTERNATIONAL SALES MANAGER

COPA-DATA HEADQUARTERS

AT COPA-DATA SINCE: 2014
RESPONSIBILITIES:
I'm part of the International Sales Team and am responsible for supporting our subsidiaries and distributors in France, Scandinavia, Turkey and the Benelux countries. Besides my office job, I also travel a lot to these companies in order to advise and support them in their work with zenon.
I GET MY INSPIRATION ...
from my family and my friends, when snowboarding, tinkering with my vintage Vespa and traveling.
IF I COULD DO AS I WANTED, ...
I would travel to Thailand and the USA, and then open a repair shop for old timers where I'd tinker and take part in rallies.

You can reach me at:
maarten.vandam@copadata.com

Gian Luca Fulgoni

AREA MANAGER

COPA-DATA ITALY

AT COPA-DATA SINCE: 2005
RESPONSIBILITIES:
I am responsible for sales in north-western Italy and in some regions of southern Italy. In the last ten years, I have had the opportunity to participate in developing the Italian sales market. With our efforts and dedication we were able to develop new important markets like Energy and Railway. Today, my duties at COPA-DATA involve consolidating our presence to the more important end users, system integrators and OEMs. I am also focused on new targets, such as the pharmaceutical industry and energy data management systems, thanks to the evolution of the brand with the presence of new powerful solutions by COPA-DATA.
I GET MY INSPIRATION ...
from my family – my wife, my two sons and Yaki, our dog. They give me support in my life. The people that make up COPA-DATA are also a means of inspiration as I consider them a kind of business family.
IF I COULD DO AS I WANTED, ...
I would travel around the world to look after children and animals.

You can reach me at:
gianluca.fulgoni@copadata.it

Thomas Glander

SALES MANAGER

COPA-DATA GERMANY
Cologne office

AT COPA-DATA SINCE: 2014
RESPONSIBILITIES:
I'm responsible for selling zenon in north-western Germany. This position involves pursuing new customers with a focus on large and key accounts, and developing and fortifying existing customer relations. My tasks also include going to customer appointments as well as providing sales support at trade fairs and looking after our partners.
I GET MY INSPIRATION ...
from being able to position an innovative product in often technically demanding and interesting customer situations, and gaining insights into industry areas I have always dreamed about.
IF I COULD DO AS I WANTED, ...
I would like to study again and spend more time abroad.

You can reach me at:
thomas.glander@copadata.de

Anita Perchermeier

SCREEN & INTERACTION DESIGNER

COPA-DATA HEADQUARTERS

AT COPA-DATA SINCE: 2014
RESPONSIBILITIES:
I'm principally involved in working on individual customer solutions. This includes visualizations of zenon projects, with a focus on optimal usability. I also contribute when it comes to new developments around zenon itself, such as creating graphics/icons and usability concepts.
I GET MY INSPIRATION ...
from music! I love going to concerts and exchanging information with other musicians or music enthusiasts. There are days when I can sit for hours in front of the stereo, with a laptop and a pile of music magazines, discovering new bands and their music.
IF I COULD DO AS I WANTED, ...
I wouldn't change much. Shouldn't we always live our own dreams? But one day, a trip around the world in the footsteps of the great musicians – from Beethoven to Kurt Cobain – would be a dream come true.

You can reach me at:
anita.perchermeier@copadata.com

Giuseppe Menin

INDUSTRY MANAGER

COPA-DATA ITALY

AT COPA-DATA SINCE: 2004
RESPONSIBILITIES:
My position covers two roles: Industry Manager and Area Manager. I pursue our business development for the key industries in the Italian market: Energy, Infrastructure & Transportation, Food & Beverage and Pharmaceutical. I monitor local industry trends and evaluate key account requests. I share this information with my colleagues from headquarters, feeding new ideas to bring into the zenon Product Family. I'm a member of ISPE Italy. Furthermore, together with my colleague Diego Fila, I handle sales activities in north-eastern Italy.
I GET MY INSPIRATION ...
from the motto: "Passion removes most difficulties from any activity." I'm also encouraged by the giants in history that rendered Italy the most beautiful country in the world.
IF I COULD DO AS I WANTED, ...
I would jump in a DeLorean, like Marty McFly in the movie "Back to the Future", travel over time and see what kind of Europe we will hand down to our offspring.

You can reach me at:
giuseppe.menin@copadata.it

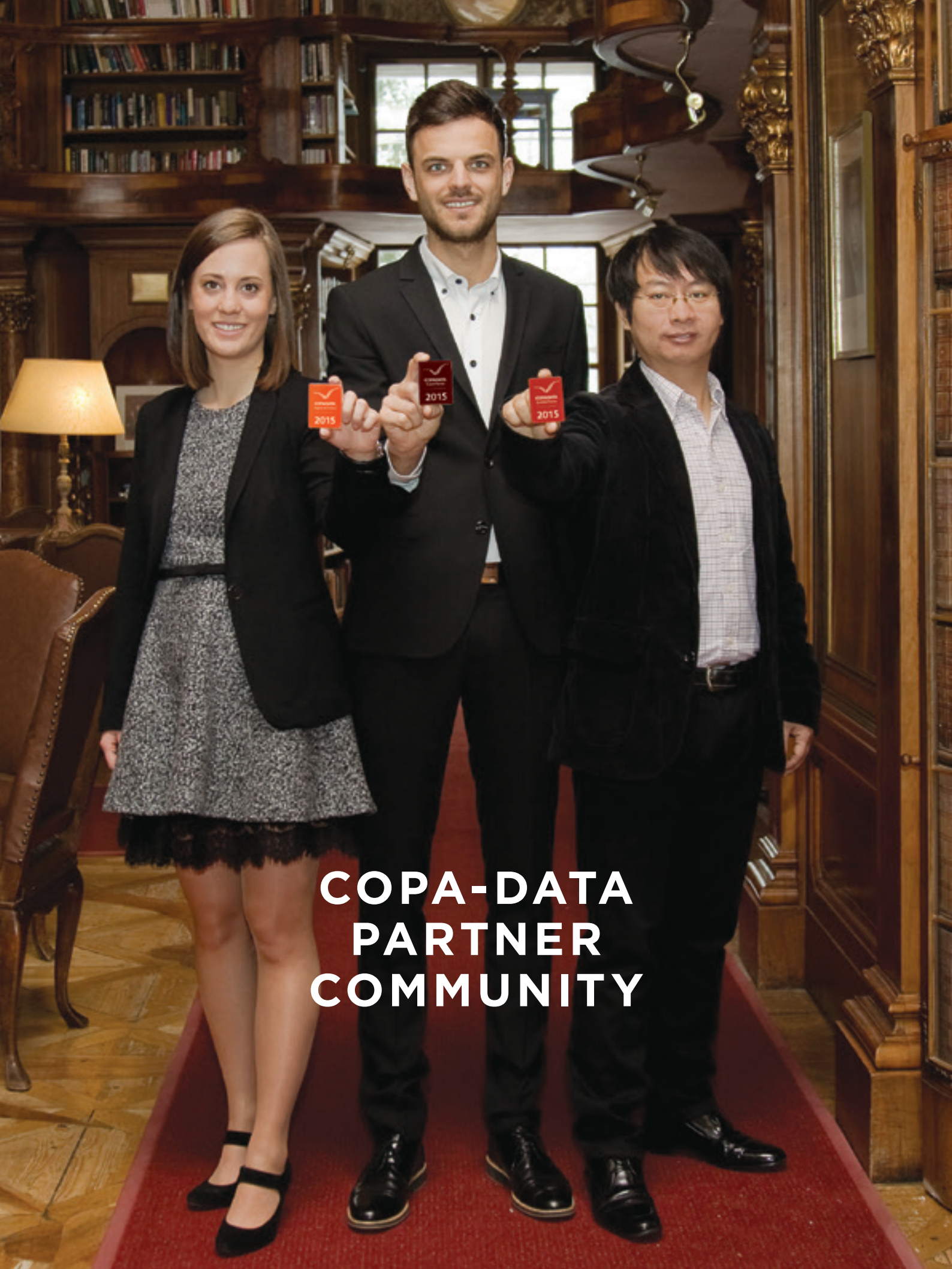
Stefan Reuther

HEAD OF BUSINESS INTELLIGENCE

COPA-DATA GERMANY

AT COPA-DATA SINCE: 2002
RESPONSIBILITIES:
It's my job to develop a new business segment in the Business Intelligence area. Data should become knowledge – that's why I'm working on establishing company-wide applications based on zenon. In addition, I perform classic business development activities paired with the acquisition of strategic partners and end customers. In parallel, I promote the implementation of zenon as an Energy Data Management System according to ISO 50001.
I GET MY INSPIRATION ...
from sports and from people who take risks in order to follow their own dreams and stand by what they do. The realization that has shaped me is that a goal can be reached with many small, continuous steps as long as the path is in the right direction.
IF I COULD DO AS I WANTED, ...
I wouldn't know where to start. I have so many goals and plans, they wouldn't even have enough space in an *IU*.

You can reach me at:
stefan.reuther@copadata.de



COPA-DATA PARTNER COMMUNITY

In previous *IU* issues we have explored the overall concept and ideas behind the COPA-DATA Partner Community and focused on international growth and events. This time, the emphasis is on the Asian Partner Landscape and its great development driven by COPA-DATA Korea.

Insights into the Thriving Partner Community in Asia

함께 성장합니다

Prior to the establishment of COPA-DATA Korea in 2011, zenon projects in Asia were managed from Europe. With the new office and the experienced team in Korea, COPA-DATA has been able to enter new market fields and start establishing business relationships with local system integrators. In order to meet demands from customers for innovative and reliable automation applications and to consider the local characteristics of the different Asian markets, experienced partners are essential for ensuring the highest quality in everything from product know-how through to implementation and project go-lives.

COPA-DATA Korea is growing at a tremendous pace and its first partner signed up in March 2012. As its growth continues, the COPA-DATA Korea team will place an even stronger focus on their partners. In order to get a better insight into the thriving Partner Community in Asia, we have asked our Korean colleagues to provide a few details. Read through our interview with some of the key people at COPA-DATA Korea: Kim Young Su (Technical Sales General Manager), Christoph Dorigatti (Area Manager Asia) and Sandra Handke (Marketing Coordinator Korea).

From COPA-DATA Korea you are covering large parts of the Asian market. What do you see as the main industry trends in Asia, particularly in your core market of Korea?

CHRISTOPH DORIGATTI: In Korea we have a strong focus on Energy applications. In this area there are a lot of new requirements due to new market trends such as Smart Grid and Renewables. We can also see these trends influencing other markets in Asia such as China and Japan. At COPA-DATA we have a long history in the area of Energy applications and this knowledge is helping us to deliver reliable solutions for these specific kinds of requirements.

As you already mentioned, you are focusing strongly on your partners and we saw a growth of your partner base during 2014. We are curious to know, how is the COPA-DATA Partner Community perceived in Korea and the other Asian countries you are focusing on?

SANDRA HANDKE: The feedback we receive from our partners in our daily working life is really positive. They enjoy working with us and our solutions. One area that they especially appreciate is the customer focus of our employees. Furthermore, they highly value personal interaction and the detailed information about coming product releases provided via the Partner Newsletter and the exclusive Partner Login Area on the COPA-DATA website.

"Coming to Salzburg and to COPA-DATA Headquarters was a great experience. Not only did we get to meet the people behind zenon and gain some direct insight and information, but we also experienced a great city and welcoming atmosphere throughout all of our stay".

HONG SEOK-BONG, NEXPO

What are your business strategies to continue your growth over the coming years?

CHRISTOPH DORIGATTI: From the start of our operations in Korea, the target was to build up COPA-DATA's first local footprint in Asia and to grow the brand awareness of our company and solutions in this market.
A good installation base already existed, which had been built up by European machine builders and system integrators. Today, we are concentrating our activities on COPA-DATA's core industries and, in the last few years, we have delivered various applications in the fields of substation automation, wind farms and gas terminals. The semiconductor industry is another important area in which we are increasingly successful. Together with our strong local partners, we have delivered projects for some of the top global players in this field, such as Samsung Electronics and LG Innotek.

We are also leveraging our strong collaboration with Microsoft to develop new solutions in the direction of Energy Management and Manufacturing Cloud Applications with the goal of not only serving our existing business areas but also to develop ideas about how we can enter new fields.

Our focus is on developing a good and profitable collaboration with our partners where we can assure their competence level as well as make sure they get all the attention and support they need and deserve.

One of your partners, NEXPO, recently visited COPA-DATA's headquarters in Salzburg. What was the focus of the trip and how did the NEXPO team feel about it?

KIM YOUNG SU: NEXPO was one of our first partners, signing up in 2013. It was also our first system integrator using the zenon Energy Edition on different energy projects. With this trip we really wanted to provide both further technical insight into the zenon Energy Edition and to give them the possibility to meet up with key people at COPA-DATA Headquarters. The ways we work are very different in Korea and Austria, however, we all have the same target – to make our existing zenon customers the most profitable customers there are and to find new customers that want to join us on our road to success. NEXPO greatly enjoyed the trip to the beautiful city of Salzburg, and we exchanged many good ideas and insights during the week.

So what's next with NEXPO?

SANDRA HANDKE: The work with our partners is always ongoing and we are constantly looking at new opportunities, both in terms of what we can do together with our partners and what COPA-DATA can do specifically for them. Besides our collaboration in different Energy automation projects, we are currently focusing on marketing activities together with NEXPO to promote our product and service portfolio. Furthermore, due to its great achievements thus far, its partner status will be upgraded soon – so we will be happy to announce our first Korean Qualified Partner at our forthcoming Asian Partner Academy.

You just mentioned the Asian Partner Academy – this event will be hosted in June 2015 and will be the first-ever COPA-DATA Partner Academy in Asia. Can you tell us a bit more about it?

SANDRA HANDKE: Yes, of course. We are really looking forward to this event! With the main focus on the new zenon version 7.20 we can already guarantee some exciting news and we will, of course, also include the new Energy-related functionalities. On the second day of the event, we are planning an IEC 61850 hands-on workshop. During the event we will show the importance of our growth in the Asian market, especially within the context of the global COPA-DATA strategy.

The reasons for holding a local partner event are many and diverse but, in the end, it is all about improving the service to our customers through a stronger collaboration with our partners.

We look forward to having deep conversations with our partners and potential partners, getting feedback and more ideas about their expectations and discussing future cooperation and ongoing projects. This is a great opportunity to meet up in a relaxed and friendly atmosphere to exchange knowledge and ideas.

Thomas Punzenberger (COPA-DATA CEO) discusses the next steps for a successful partner collaboration with Park Jun-Ho (NEXPO), Hong Seok-Bong (NEXPO) and Kim Young Su (COPA-DATA Korea) during their visit to Salzburg.

Thank you COPA-DATA Korea for sharing your insights with us.

THIS INTERVIEW WAS CONDUCTED BY LISETTE LILLO FAGERSTEDT, PARTNER PROGRAM MANAGER, AND JOHANNES PETROWISCH, PARTNER ACCOUNT MANAGER.

ASIAN × Partner Academy ×

COPA-DATA Asian Partner Academy

June 16-17, 2015
Seoul, South Korea

http://kaywa.me/HHi76

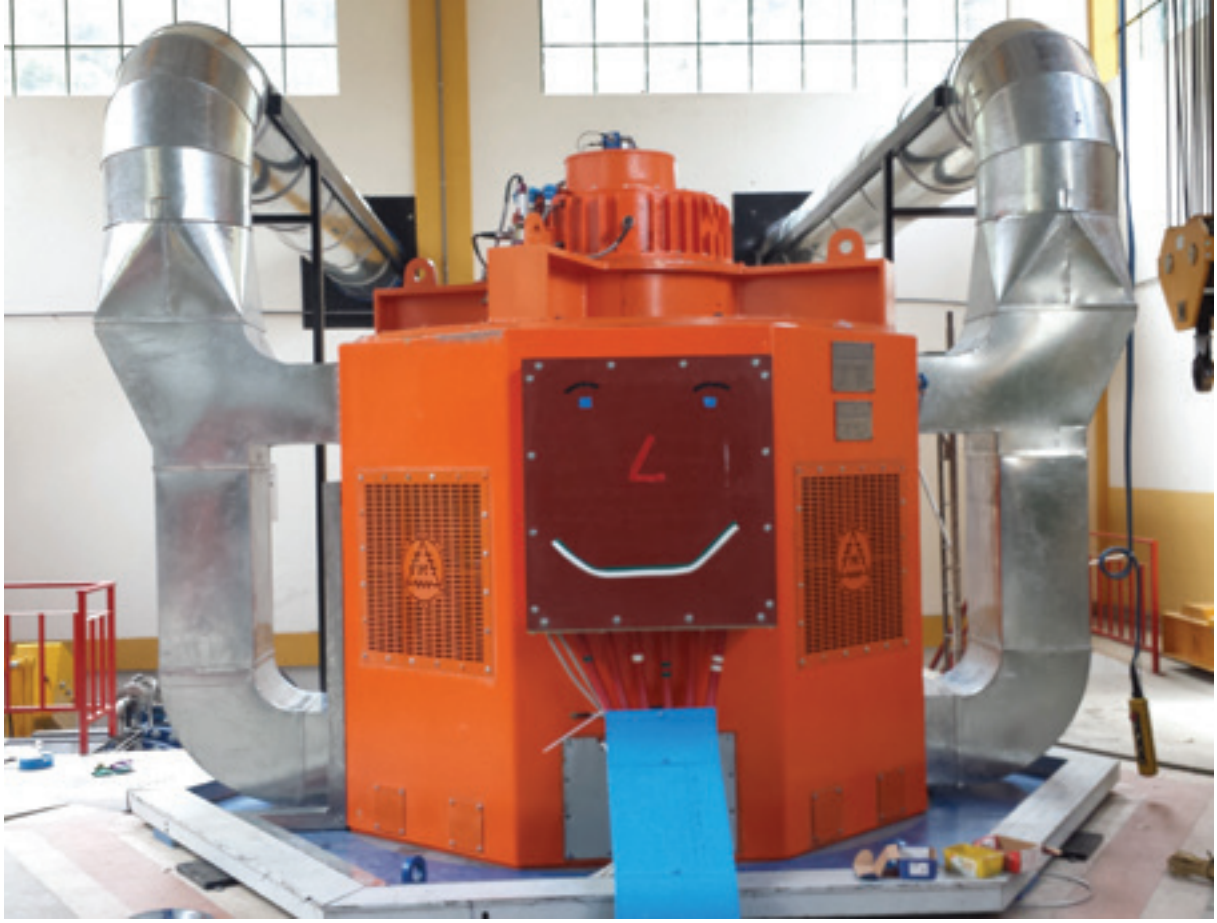
NORTHERN EUROPEAN × Partner Academy ×

COPA-DATA Northern European Partner Academy

Another upcoming event is the Northern European Partner Academy dedicated to the partners of COPA-DATA UK and COPA-DATA Scandinavia.

June 9-10, 2015
Manchester, UK

http://kaywa.me/V9ciq



Supporting Latin America on a United Energy Mission

EACH DAY, WE COMMIT OURSELVES to the company we work for. Together with our colleagues, we dedicate our expertise, passion and time to developing great projects. More often than not, this happens in the private economic sector. If we engage in projects in the public sector, we can help to improve many people's lives. For example, by developing and maintaining local infrastructures with water and electricity supply, hospitals, road networks, railways and educational institutions.

Developing a basic infrastructure requires time but above all expert knowledge, appropriate machinery, sites and technology, and, of course, sufficient funding. Wouldn't it be amazing to have the same assets available for humanitarian projects in less-privileged countries around the world?

A couple of months ago, I was fortunate to be able to interview Mr. Stefano Bellabona from Impel Systems S.r.l., an Italian member of the COPA-DATA Partner Community. In collaboration with other professionals, Mr. Bellabona donated his time, expertise, efforts and materials to build a hydroelectric station in the Cordillera Blanca mountain range in Peru. The goal was to help improve the conditions of the local population who live in this mountain region at more than 3,500 m above sea level.

The project was initiated by the international volunteer movement, Operazione Mato Grosso, which unites many supporters and key staff members to create perfect synergies. Also on board was our zenon software. On the following pages, I would like to report on the wonderful professional as well as personal experiences of the volunteers who brought this project to life with their donations.

OPERAZIONE MATO GROSSO

Operazione Mato Grosso (OMG), the international volunteer movement, was founded over 40 years ago, aiming to support people in the poorest regions of Latin America. The movement originated at the initiative of a group of young Italians. Under the guidance of a Salesian priest, Father Ugo de Censi, they organized an aid expedition to assist a missionary father in Brazil's Mato Grosso region (hence the name). Based on this experience, the movement has initiated more than 90 missions across Peru, Bolivia, Ecuador and Brazil. Currently, more than 500 Italian volunteers are working without any compensation, so all proceeds from the initiative can go to those in need.

INITIATIVE LOCATION AND AID RECIPIENTS

Operazione Mato Grosso traditionally concentrates its activities on the Peruvian Andean Sierra. The greatest need for support is in the Ancash region, situated about 500 km from Lima at an altitude of between 3,000 and 4,500 m. Its estimated population of 35,000 is almost entirely dependent on food deliveries. Here the inhabitants live in small villages of clay huts with thatched roofs. Only a small part of these settlements have running water, sewage systems or electricity at their disposal. Their diet is mostly made up of rice, beans, potatoes and barley, with the occasional egg and, even more rarely, meat and milk. The levels of malnutrition are at 50%. Each year, Operazione Mato Grosso distributes 2,000 tons of food supplies to these people, which come from collections made in Italy by volunteers.

OBJECTIVE: REDUCE FOOD DEPENDENCE

In order to reduce these people's dependence on food aid, OMG supports the independent development of local infrastructures. Above all, the younger generation should get an opportunity to improve their living conditions, enabling them to raise and support a family without having to leave their homeland. Initiatives include the development of agriculture, reforestation and livestock husbandry as well as the construction of flour mills to process the cultivated grain and/or dairies for cheese production.

THE NEW HUALLIN HYDROELECTRIC POWER PLANT, CONTROLLED BY ZENON, MAKES AN IMPORTANT CONTRIBUTION TO AN AUTONOMOUS DEVELOPMENT OF THIS REGION AND TO THE SELF-SUFFICIENCY IN FOOD PRODUCTION FOR THE PEOPLE LIVING THERE.

Establishing training programs and workshops is particularly important, as this enables the local population to learn, produce and sell craft wares, allowing them an income and in turn a dignified life. To achieve this, schools have been put in place to teach carpentry, wood carving, stonework, glass and ceramics workmanship as well as professional mechanical skills.

Furthermore, hospitals, facilities for the disabled, orphanages and residential housing for seniors have been built.

ELECTRIC POWER, THE DRIVER OF DEVELOPMENT

All of these activities have been promoted and supported through the work and donations of Italian volunteers, but also thanks to the availability of electricity. In fact, Operazione Mato Grosso has already independently built several small hydroelectric power plants, each generating about 700 kW. Apart from operating the hospital, schools and craft workshops, electricity is indispensable for animal husbandry and agriculture processing. The national power grid has not yet been connected to the areas involved in

the initiative. However, a local distribution grid managed by the movement is in place, with the Parish handling the connection and distribution of power lines. With the energy produced by the two small power stations, activities that have already been implemented can continue, yet there is not enough power to ensure the development of new projects. This poses an obstacle in the way of reaching OMG's primary goal – self-sufficiency in food production and independent local development.

HUALLIN HYDROELECTRIC STATION

This is why Father Ugo De Censi asked the volunteers and benefactors to help him build a new hydroelectric station. In 2010, construction work began.
The final design, which included the technical specifications of the plant's different components, was prepared by a team of volunteer engineers and technicians who not only worked free of charge but also brought in external funding.

In 2014, in cooperation with other benefactors, they delivered a hydroelectric station capable of producing 3,000 kW, which can be turned into 6,000 kW using a second water bypass. Combined with the power produced by the other two stations, this will be enough to introduce new development initiatives and activities by Operazione Mato Grosso.

All this was made possible by many committed people, including Italian engineers and industry experts, Peruvian technicians, and other volunteers from OMG. Some benefactors donated the full amount of materials required, or provided them at a reduced price. Among these was also COPA-DATA – supplying the control system based on zenon.

SUPERVISION BASED ON ZENON

The supervision is managed by two redundant zenon Supervisor systems, ensuring the plant is always under control, also in case of a disruption or even breakdown in one of the two systems.

Using satellite connections, the technicians in Italy are able to access all of the automation and control systems. In case of a malfunction or breakdown, they can offer assistance to local volunteers to solve problems within timeframes which suit operational requirements.

Apart from zenon's standard functions, the Message Control module is also used to send critical alarms to the station's operators via email, ensuring the site is constantly monitored.

The multi-language function ensures easy access to the application for both Italian volunteers and Peruvian staff.

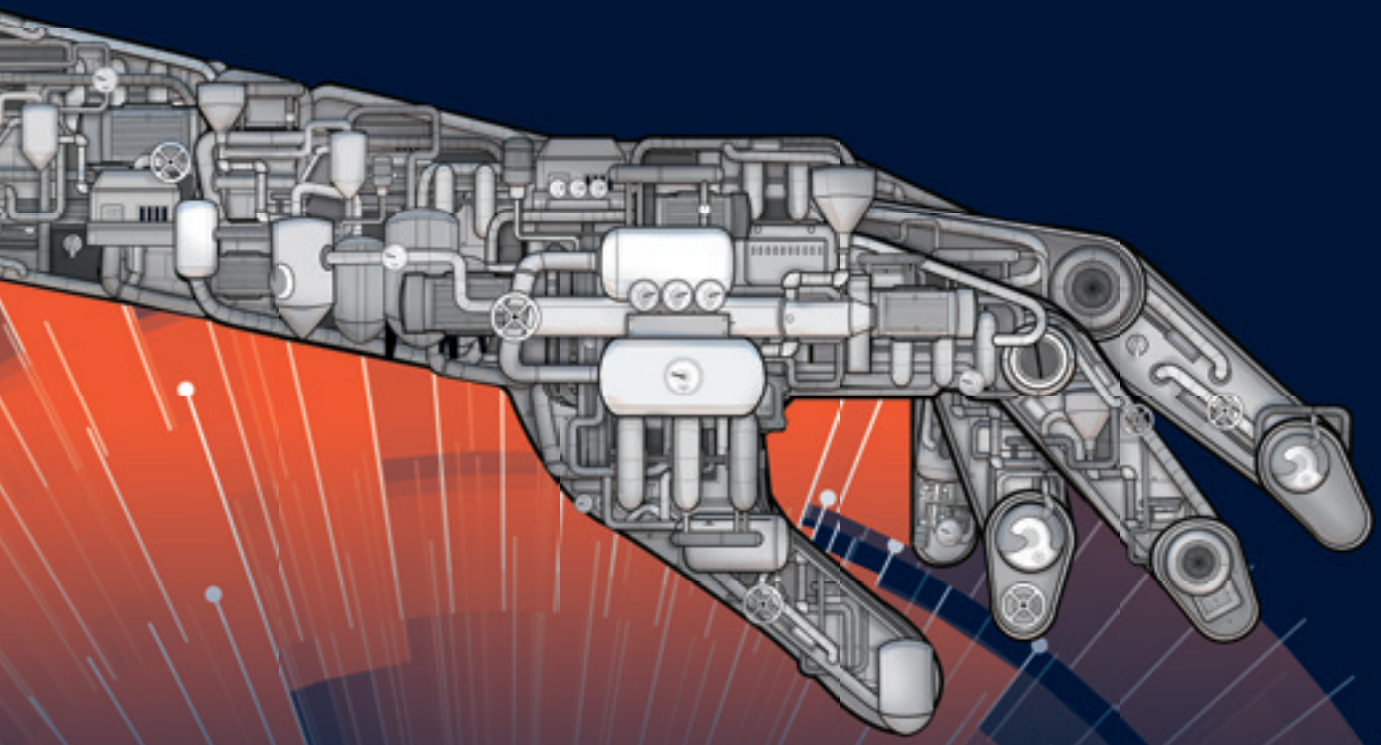
THANKS

A special thank you goes out to Mr. Stefano Bellabona, for providing us with his insights for this project. We would also like to express our great admiration for the Operazione Mato Grosso, which has been supporting Latin America's poorest for over 40 years. Thanks so much for giving us the opportunity to use zenon as part of such a remarkable initiative to improve living conditions for this region's people.

NOEMI TORCASIO,
MARKETING MANAGER
COPA-DATA ITALY

http://kaywa.me/ztg4V

Better visualization: At your fingertips.



Chris shrugged. He of course sympathized with his colleague who desperately needed to display those additional points of measurement. But there was nothing he could do except put it on the list for the next scheduled visualization update. Which wasn't anytime soon.

When Chris began to investigate among his peers in other companies he found that several of them found it totally normal to change details in their visualization themselves. One of them even sent him the link to the software company. ‚zenon', he read, and then he clicked.

Over the following months, Chris was in his element. Testing, evaluating, negotiating. And then just implementing zenon. It was surprisingly easy to switch. Now his integrator still delivered the main project, but maintaining it stayed in the hands of Chris and his team.

Creating a new button, additional functions, different colors – no problem. Chris could now manage many changes with only a couple of clicks. To top it off, he even could feed in changes on the fly. No more downtime or overtime during weekends. So that's how ergonomics worked. And what a relief it was.

The Future is Ergonomics. Ergonomics is zenon.

COPADATA
do it your way

www.the-future-is-ergonomics.com