SECURE, RELIABLE AND EFFICIENT ENERGY SUPPLY IN PRODUCTION PROCESSES USING CLOUD-BASED TECHNOLOGIES

Paper No. PCIC Europe EUR19_33

Dr. Ralf Blumenthal
Siemens AG
Nuremberg, Germany
ralf.blumenthal@siemens.com

Felix Cadelcu
Siemens AG
Nuremberg, Germany
felix.cadelcu@siemens.com

Dr. Christian Blug
Siemens AG
Erlangen, Germany
christian.blug@siemens.com

Abstract – In recent times, a variety of cloud-based offerings have entered the market with the aim to support process and chemical industries to being supplied and using energy as securely, reliably and efficiently as possible. In this paper, we discuss the opportunities and risks that come along with cloud-based technologies in these environments, especially in the context of secondary assets (IEDs). We take the perspective that the benefits of data-driven and platform-based approaches are, and will more so over time, outweigh well-known risks even in security- and safety-sensitive areas of process and chemical industries. Among others, these are cyber and data security threats, corrupted sensor data, efforts in setting up and managing communication and data infrastructure, sensitive data sharing concepts, and more. On the other hand, stand the benefits of ubiquitous process transparency, among others, along with data-based levers for cost savings and performance increase which are hardly accessible by traditional means. Examples illustrated in this paper cover cloud-based approaches to secure asset and patch management, energy efficiency services, and power quality analytics.

Index Terms — cloud-based, IoT, analytics, power quality, energy efficiency, asset management

I. THE FUTURE IS CLOUD-BASED

The use of cloud has become ubiquitous in many parts of everyday life in recent years. This, however, stands in contrast to large parts of the industrial space, especially in safety- and security-sensitive areas, where cloud-based applications certainly exist, but have not yet entered the majority of operative systems. The main reasons for this lag between B2C and B2B environments are most often linked to hesitations regarding data privacy, risk of cyber-attacks, and reliability issues in cooperation with 3rd party service operators for infrastructure and platforms.

We argue in this paper that cloud-based applications and services are likely to take the same ubiquitous role in B2B as we currently experience in B2C, even in safety- and security-sensitive industrial areas such as the energy supply and use in process and chemical industries. We include in this perspective also areas where one currently might have significant trouble to see cloud-based realizations for various technical and regulatory reasons, such as in electric grid control and power systems. In the authors' opinion, the benefits of cloud, which we will outline below, are too compelling to enable additional value add and secure competitivity as to exclusively remain in B2C or non-sensitive areas of industry. Our view is based on long-standing professional experience in the field of energy supply, distribution and use. The interested reader will hardly find versatile literature-based evidence of our arguments that go beyond the broadly known and accessible general technical descriptions of cloud-based and cloud-related technologies. As the intention of the article is to bring forward a practical essay on why and (to a certain extent) how cloud will come out as the winning movement, we have intentionally chosen to present our personal view on the matter as basis for further discussions and exchange in the community, and to limit citations to a minimum.

The benefits of cloud are manifold and naturally linked to the definition of what a cloud is in the first place. According to the commonly accepted definition by the National Institute of Standards and Technology, an application qualifies as cloud-based if it fulfills five pillars: Computing capabilities are provisioned on demand (self-service); the application needs to be accessible from anywhere at any time by any device; computational resources are pooled for as many tenants as necessary; the latter scale up and down instantaneously according to current demand (elasticity); and lastly, full transparency on use of the application is granted to the user at all times. In our view, this yields five main benefits of cloud that we will outline in the following.

A. Cloud for efficient generation of insights

With full elasticity of computational resources at hand, cloud-based applications can be used cost-efficiently to run algorithms on vast amounts of operational data. The majority of science, research and development activities that base their simulations and findings on huge data sets is nowadays performed on computational clusters deployed as cloud, because it is otherwise extremely expensive to build up the computational resources for only one or selected applications. The computational power of large cloud-based infrastructure providers opens the space of having access to such resources even to individuals and small enterprises that would never have been able to do so on their own. In consequence, technological developments happen faster, new and more algorithms are created, and more data sets can be, and are, examined. This directly leads to the ability of taking in more data, of adding more sensors to measuring data points that might not be qualified relevant in the first place, but which may yield unforeseen benefit due to additional analysis capabilities. Cloud enables this cycle of continuous data-based value add.

B. Cloud for scaling of non-core competencies

Closely linked to A., but rather from the perspective of an individual enterprise, is that the availability of fully scalable computational resources on the market lowers the need for significant capital and operational expenditures into competencies that might not be qualified as the enterprise's core business. With the aforementioned speed at which the cloud market is developing, the required resources to stay competitive in this space can be significant.

C. Cloud for fast spread and development of insights

With cloud, process knowledge and domain knowhow can be transferred across space and time while maintaining complete anonymity on the process itself. That is, algorithms running (or trained, in the case of artificial intelligence engines) on the operational data set of location A can be transferred to the operational data set of location B without sharing data or process details between both locations. In this manner, knowledge can be spread faster to the greater benefit of all parties involved.

In the authors' view, this benefit is a powerful advantage of cloud, but in the same time seems to be the reason for much hesitation, or even fear, to opt for cloud-based applications. Enterprises certainly wish to keep a competitive edge regarding the knowledge of the processes they are running. In the same time, it can be powerful to leverage the knowledge of anonymous outside expertise to innovate faster and therefore to remain competitive, if the transfer of knowledge goes without sharing actual data or specific insights.

D. Cloud for fast and location independent reactivity

Cloud-based technology has made it common practice to have information at hand, and it is therefore straightforward to anticipate this expectation to enter all fields of work, also in safety- and security-sensitive domains. This may be more pronounced for the younger generation of workforce, but determines the flavor that enterprises need to respect to attract new talents.

In addition, the ease at which information is accessible and useable on cloud makes many time-consuming efforts which exist nowadays superfluous. Enterprises are well advised to use cloud-based technologies to increase internal process efficiencies and reduce overhead costs.

E. Cloud for easy and intuitive way of working

The expectations and common practice towards accessibility of information also extend to how this information is presented to the user. Reading extensive material such as user manuals to becoming able to master a certain application appears increasingly old-fashioned. So-called user experience design becomes a decisive competitive factor, not only in B2C but more and more also in very traditional domain-specific and critical B2B applications such as grid control software. Applications becoming more user friendly and intuitive is not per se a feature prone to cloud, but cloud-based developments with all-time accessibility and transparency of use have definitely contributed significantly to this shift of mindset. Taking advantage of this development in developments of applications and services, enterprises cannot only reduce the costs for employee trainings, but – to a certain extent – rely on less trained staff in times of shortfall of (traditional) extensively trained workforce and develop this workforce in shorter time scales and with less investment.

II. ON THE BENEFITIAL USE OF CLOUD IN ENERGY USE AND SUPPLY

In the present section, we will explicate the aforementioned benefits of cloud for the example of three cloud-based approaches to essential areas in the supply and use of energy in industrial environments, also in process and chemical industries. These are power quality (supply and demand side), asset management (demand side) and energy efficiency (demand and supply side).

A. Power quality

Reliability of electricity supply is the essential requirement to successfully operate a plant and keep the core processes running. Outages of electrical equipment lead to much higher costs due to loss of important process in comparison to the repair costs. Therefore, fault prevention and fast fault clarification is important to avoid outages and to re-energize the electrical supply as fast as possible. Especially the identification of critical system states and the fault disturbance clarification is a very complex task and requires a deep knowledge of steady state and transient effects and a lot of experience.

Furthermore, especially for the fault prevention a continuous monitoring of the most relevant parameters is mandatory. Based on the outcome of such measurements, simulation tools help to understand the behavior and to elaborate mitigation measures.

Only a few experts have the required domain know-how and the plant operator normally contact them in case of troubles. The analysis of the events is very time consuming: Relevant data have to be collected and

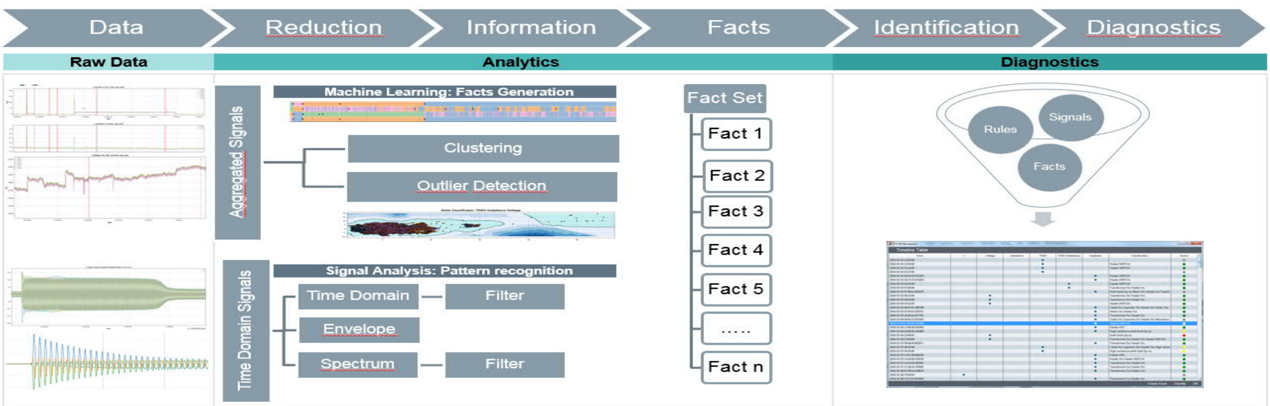

Fig. 1: Event classification with AI approaches

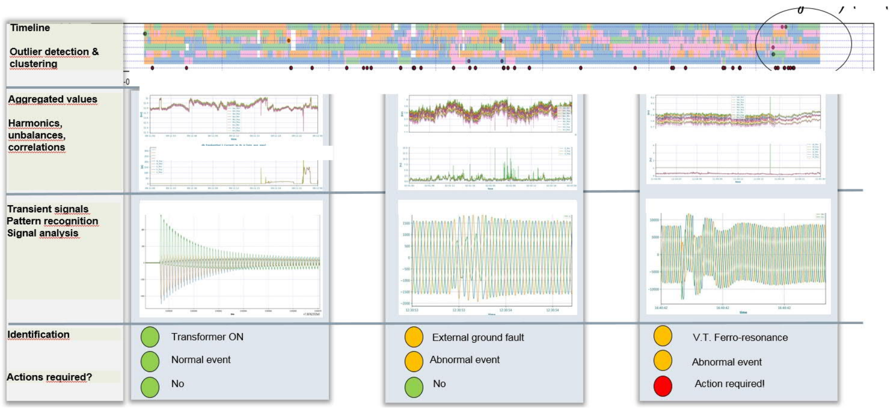

Fig. 2: Example of a disturbance detection

consolidated to get a solid starting point for the further analysis and to derive the relevant information.

Long-term practice on that field of disturbance analysis led to the following observations:

- A lot of events had a typical characteristic, which could be derived from actual and historical recordings of the electrical signals
- Evolving disturbances can be observed as anomalies of the relevant signals
- This requires a permanent monitoring at high resolutions instead of short-time spot measurements

Industry 4.0 and the digitalization is now able to provide the continuous data stream to do that task. Sensor data can be provided via TCP/IP via Ethernet or even wireless via LTE communication. At the same time the performance of the recorders increases with respect to resolution, memory and trigger capabilities.

This enables us today to establish a new service Power Quality Analytics, which combines data transfer, automated analysis and access on power quality experts to one managed service.

New challenges are rising with the new opportunities: Especially the huge data size because of the high degree of digitalization makes it hard for an expert to consolidate them and to extract the relevant information. The data is recorded at different locations and has to be transferred to a central place where inconsistencies should be eliminated first before the analysis can be started. Furthermore, different players have to access the information simultaneously. Cloud is the natural place to provide these options with sufficient storage space and highest availability.

The next challenge is the efficient generation of information on the basis of the data sets which can only be handled with powerful data analytics algorithms based on AI approaches. Normally they require sufficient computation power and should upscale with the problem size. Cloud solutions will replace on premise solutions in the near future due to the better scaling at lower specific costs.

The application of AI requires a sufficiently large training set to produce reliable results. Especially for fault prevention it is beneficial to explore different data sources from different plants, different customers and even different countries. One client is not able to provide a sufficient data set only by its own. The cloud is the natural link between those different information sources and enables all clients to benefit from each other.

The major goal of such an approach is definitely not the uncontrolled gathering of data but the gain of information and to derive knowledge from that information which can be provided to each player.

Power quality analytics as a managed service requires flexible and fast communication channels because the dialogue with the client based on the analytics results is essential to take counter or mitigation measures as soon as possible to prevent disturbances. Therefore, the support of mobile devices, an adequate GUI on mobile appliances is important for a successful service. Cloud already provides the necessary infrastructure and communication channels (push services, flexible remote access) and is therefore our first choice for the implementation of such kind of managed services. Last but not least the knowledge has to be distributed via different communication channels.

All the above described aspects were the reason to design Power Quality Analytics as a cloud-based service. Power Quality analytics combines the best of the two worlds – power analytics algorithms and expertise of an experienced expert – to permanently evaluate the state of a grid considering following criteria:

- Is a normal operation action responsible for an anomaly?
- Or is it an indication of an evolving fault?
- Is this critical and how fast do we have to take counter measures?

The core of the service is a server farm. Those servers host AI applications to sort out normal states and events and to provide relevant for further investigation. In this step technical domain know-how is required to derive the physical classification from the statistical nature of the outlier (Fig. 1):

- The wave form of transient events will be directly interpreted by comparison with already classified recordings (training set).
- Anomalies will be detected with outlier detection methods by Machine Learning combined with a classification process which describes the outlier signal in a well-defined and consistent way
- Classification results will be combined with rule sets to derive those physical events which are best matching the typical classification characteristic.

The approach strongly relates to the strategy of an expert who has to identify events: He has to visually recognize signals, he has to correlate signal features with historical recordings, and he is deriving his final decision on the basis of well-proven rules.

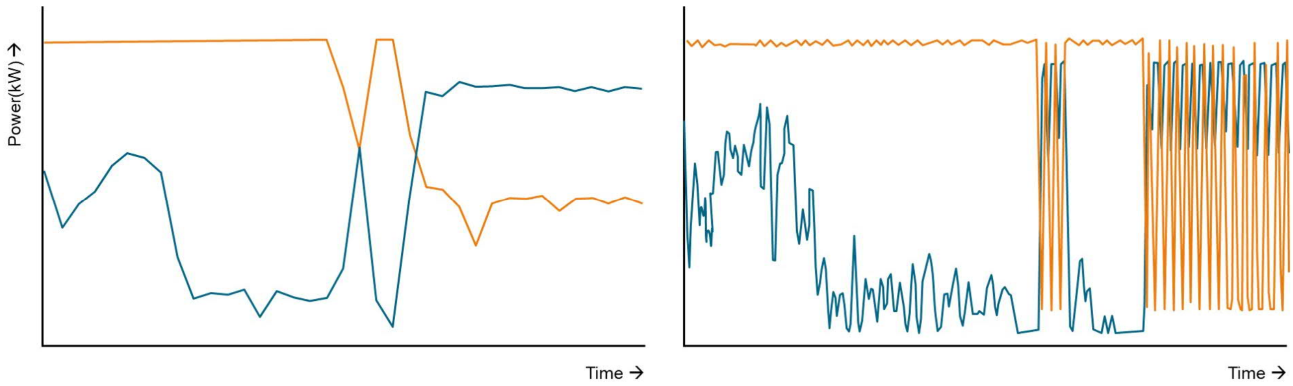

Fig. 3: Effect of time resolution for acquisition of energy consumption data for the example of two water pumps: 15-minute average (left) vs. 5-second sampling (right)

The combination of three different approaches which include also the domain know-how of the expert guarantees a fast decision process and a high quality if the classification result which can be directly communicated to the client.

A typical process is shown in Fig. 2: machine learning algorithms identify typical operation scenarios and abnormal events and visualize them with the timeline. Each dot refers to an event which has to be classified first, before one could device, whether further measures must be considered. The first event describes an overcurrent event which has been identified as transformer energizing. This is a normal operation event which needs no further actions. The second event shows the signature of an upstream earth fault at the transmission grid. That event could lead to disturbances at the downstream grid, nevertheless no further measures can be taken because the source of disturbance is upstream. The third event finally shows an outlier which indicates a serious problem: The pattern recognition and the fact classification indicate the occurrence of a ferro resonance which could lead to a damage of the v.t. and finally of the switchgear with high outage costs. Mitigation measures have to be taken immediately.

B. Asset management

For assets in the critical infrastructure the European Programme for Critical Infrastructure Protection (EPCIP) provides guidance for risk management. The program fulfills the requirements set forth by European Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2]. Following the US Homeland Security Critical Infrastructure Information Act, the Chemical Sector is considered to be a Critical Infrastructure Sector [1]. Major electrical substations in Germany are considered critical infrastructure according the German federal law for critical infrastructures [7] and must be protected against cyber threats.

To support the integrity and cyber-security of the infrastructure and sensors for power consumption and power quality, adequate measures must be taken. An Asset Management system for equipment of energy management / energy automation systems is an integral part of an Information Security Management System (6). The norm ISO 27001 [6] annex A.8.1.1 demands, that assets for information processing have to be reliably identified and managed over their lifecycle and the respective inventory is to be kept up to date.

Reliable identification criteria for secondary assets are e.g. device model, vendor and the serial number, making a device uniquely identifiable at least in a major substation environment, if not worldwide. Each intelligent electronic device in an installed base needs a firmware or software component to be able to work. Protection devices bear a communication module and a main CPU module, both containing a separate firmware. Routers and manageable network switches have their own firmware and PCs have an operating system plus additional software installed. For cyber security or functional safety reasons, or to cope with afore named regulatory requirements, companies might be obliged to keep these firmware and software components up-to-date.

The cloud-based approach supports the convenient data storage and connectivity of the monitored assets (see Fig. 4). Adding new production plants or system does not require adapting the parameters of the asset management system, it will scale smoothly even in rapidly growing environments.

Further, cyber-security patch information, as needed for identifying vulnerabilities and keeping assets up-to-date can be seamlessly deployed by cloud-to-cloud coupling mechan6 [3] presuming, the repository for the patch information is also maintained in a cloud-based infrastructure.

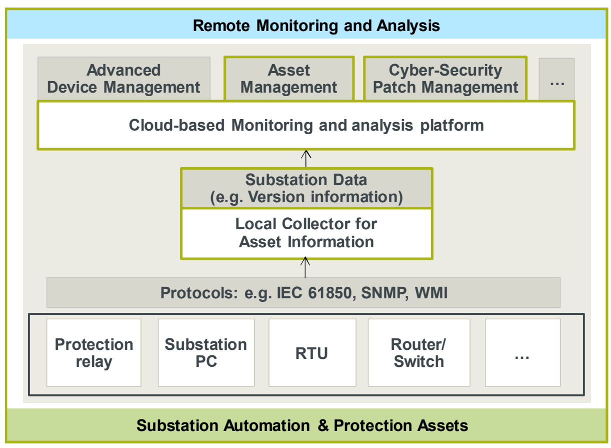

Fig. 4: Asset Management for Secondary Equipment

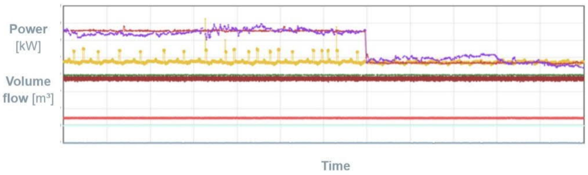

Fig. 5: Active power load of one transformer (yellow line) and four centrifuges (nearly constant lines), along with volume flow through the centrifuges (purple lines) over time

C. Energy efficiency

Global climate change, scarce energy resources and the increase in power demands and energy costs are making it urgently necessary to act in the area of use efficiency of energy consumption. There are significant energy saving potentials in all consumption sectors that become apparent when gaining visibility on energy consumption on asset level at high temporal resolution. Here, high temporal resolution refers to data sampling rates that are commensurate to the time scales of the monitored process, so that the dynamics of the process can be adequately resolved, see Fig. 3.

Such bottom-up approaches are not common in the space of energy efficiency, where the dominating approach is to take a top-down perspective in visualizing overall energy consumption and power flows, dashboarding distributions of energy consumption and defining key performance indicators (KPIs) with the aim to monitor the evolution of overall energy performance over time.

From a data point of view for the example of a typical process plant, top-down approaches involve 20-100 monitoring points at temporal resolutions of up to 1 per 1 to 15 minutes. With each electrical power meter delivering approximately 25 different measures (from reactive, active and apparent power to current and voltage in all phases, frequency and power factors), we look at data processing requirements of the order of 10^0 to 10^2 MB of data per day and site. Bottom-up approaches, where the aim is to resolve the dynamics of assets in charge of at least 80% of the energy consumption of the plant, involve 50-300 monitoring points per process plant, with sampling rates of 1 per 1 to 5 seconds. With above assumptions, the data processing requirement are of the order of 10^3 to 10^5 MB (equivalent to tens to hundreds of GB) of data per day and site. The present calculation is done based on electrical power meters, so metering equipment for water, gas, fuel or other energy flows, in addition to taking into account process variables of different types need to be added.

In such bottom-up approaches, the resulting amounts of data need to be processed and analyzed to derive meaningful information to be able to improve efficiency, all as cost-efficiently as possible, and applicable to multiple sites, process lines and types of equipment in parallel. The efforts required to do so typically exceed the duties of energy managers in charge for the site's energy management and efficiency, both in time and scope. Statistical and big data analysis tools and artificial intelligence engines become key to extracting the information necessary to derive and execute efficiency measures such as change in control and setpoint parameters, retrofits and modernization, change or addition of equipment.

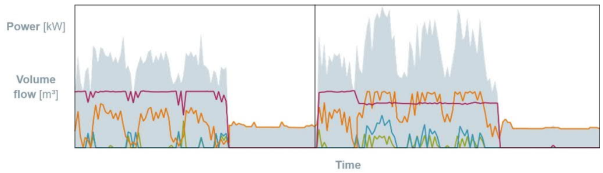

Fig. 6: Load curves of five network air compressors (colored curves), and specific consumption of air volume flow per energy consumed (gray shaded area)

The information derived from algorithm-based bottom-up approaches to energy efficiency need to be brought to the user as intuitively and as quickly as possible. For example, any unusual change in energy consumption, indicative of unusual process behavior, needs to be communicated to the person in charge of the process. sPlant management needs to be able to get a direct overview of plant consumption at any time and from anywhere, in order to know about current operational status but also to ensure proper follow up of energy efficiency measures (which is an integral part of globally accepted regulations for energy efficiency, e.g. ISO50001). Central functions for process excellence need the information generated from energy consumption data across different plants to derive and implement best practice process guidelines, and to ensure that overall enterprise goals to energy efficiency and carbon footprint reduction are met.

Cloud-based solutions are the approach of choice to meet the requirements and topics raised above with respect to bottom-up energy efficiency approaches. In this area of application, the benefits of cloud outlined in the introduction as to efficient generation of insights from huge amounts of data, scalability of resources to handle the ever-increasing amount of data over time, fast reactivity to observed incidents and user-friendly handling of information from anywhere at any time and by any device, are key.

As an example, to illustrate the above points, let's consider the continuous monitoring of a transformer that feeds into 4 centrifuges, in addition to the volume flow of fluid being processed in the centrifuges as depicted in Fig. 5. High-frequency sampling shows the transformer to exhibit frequent short-term peaks in active power at high volume flows, whereas this is not the case if the volume flow decreases. The overall power levels of the transformer and centrifuges is nearly constant over time and independent of the flow rate. After detection of the event, the operator is directly notified according to a pre-defined scheme of notification. She either knows or can come up with ways to solve the problem, or in some cases, the solution is already suggested by algorithms trained on historical events. In any case, the root cause analysis of the peaks led to decreasing power losses in the transformer, but especially in increasing the lifetime of the transformer and reducing required maintenance tasks. Energy efficiency monitoring seamlessly touches upon topics of asset and maintenance efficiency – a typical effect in horizontal digital approaches.

Finally, we would like to illustrate the implication of the benefit of cloud to the fast development and spread of insights using a practical example of air compressors, see Fig. 6. In this example, five air compressors are generating a certain air flow required for a process at a certain pressure level. High-frequency monitoring of the compressors in addition to the air flow volume, pressure and temperature, reveals the best configuration at which the five compressors should operate with respect to one another in order to deliver the required air flow at the least energy consumption possible. Once this optimum range of operating levels across different operating conditions is identified and communicated, the operator can adapt the control settings, leading – in this case – to a decrease in energy consumption by 24%.

The algorithms trained on certain types of air compressors – but this holds true for any type of asset monitored – can help define, detect and achieve industry-wide best levels of efficiency under real operating conditions, without sharing specific data or enterprise-specific ways of operating beyond process site boundaries. By use of cloud, anonymous knowledge can be generated and spread fast and effectively to the benefit of all.

III. CLOUD CLEARLY COMES AT A RISK, BUT IS NONETHELESS INEVITABLE

Despite the obvious benefits of cloud-based technology, cloud as such certainly bears risks, especially with regards to cyber and data security threats. In closing, we will therefore briefly touch on these topics, for which, nowadays, proven remedies exist to make the risk calculable and mitigatable.

A. Data protection

Applying data protection rules, like the new European DSGVO law, is vital in an environment, where also user related consumption data is collected. The GSDVO (General Data Protection Regulation [4]) handles especially user rights such as the right for correction of user data or the right of restrictive usage of user data.

Since users have also the right of deletion of their personal data, a worst-case scenario in such an environment would be, that too many users might demand the deletion of their consumption data, thus making the collected amount of data probably insufficient for a significant gain of knowledge for the generation of behavioral patterns of typical energy consumption. The GSDVO rules apply regardless of the underlying technology, cloud-based or on-premise, thus not influencing our cloud-based approach directly.

In an industrial context, like Power Quality or Energy Efficiency applications, analyzing consumption data might not affect user directly, thus companies might tend to handle corporate data protection rules less strictly. Nonetheless, protection of consumption data is vital since algorithms and data are "golden nuggets" for companies, which use such algorithms commercially.

B. Cyber Security Measures

Distributed Denial of Service (DDoS) attacks on cloud-based infrastructure are a widespread phenomenon. In these attack scenarios, multiple compromised hardware clients try to connect at once with a heavy number of attempts to the cloud-based server infrastructure.

As an adequate countermeasure, a load-balancing facility can be implemented. Load-balancers spread the workload across multiple entry-points and thus across multiple servers. The attack surface is being reduced and the failure of single servers is compensated by the others. Secured this way, the cloud-based instance for data collection and the database servers can withstand heavy DDoS attacks.

A method to secure login procedures for cloud-based infrastructure can be obtained, by using multi-factor authentication principles, e.g. applying the generally accepted evidences for authentication "something you have" (e.g. Smart Card), "something you know" (e.g. user password), "something you are" (e.g. finger print). A commonly-used subset of these three evidences is the combination of "something you have" and "something you know". Sending a one-time-password (OTP) via SMS to the mobile phone or using a token-generator mobile application serves the "something you have" evidence factor.

Personal login credentials like username and password fulfill "something you know". Of course, an additional step of security can be obtained by applying password rules, like obliging users to change their passwords cyclically. Deploying such rules is a convenient task in cloud-based infrastructures.

C. Summary

Cloud-based technologies are powerful and yield clear benefits, also in safety and security-sensitive areas of industry. Denying cloud will ultimately lead to losing out on the competitive edge and accepting mediocre "business-as-usual". It is the authors' opinion that cloud-based technologies will at some point dominate all areas of industry. Strategies on how to cope with such technological changes in safety- and security-sensitive areas, and how to deal with new players entering traditional markets, will thus be a decisive factor in securing business.

It is of course acknowledged that cloud cannot work if the trust to providers of cloud-based applications and services is missing. Issues with data and access security, transmission security (i.e., encryption and more), and especially data integrity (i.e., to be sure that the data that was stored is the data one is working with) need to be taken seriously. Hesitation towards cloud in safety- and security sensitive areas of industry is therefore understandable, but nonetheless does not solve the challenge.

It is a promising development that the risks associated to cloud have become calculable, and proven remedies exist. Compared to the beginning of the cloud-computing era, commercially used cloud-infrastructure offerings can be found in the portfolio of every major IT and industrial IoT provider. In addition, regulatory and legal guidance can be applied, such that the responsibility for commercial risks is and will become even more clearly regulated.

The future is cloud, let's work on how to embrace it.

IV. REFERENCES

[1] M. Stevens, Gina. (2003). Homeland Security Act of 2002: Critical Infrastructure Information Act

[2] Critical Infrastructure Protection X, 10th IFIP WG 11.10 International Conference, ICCIP 2016, Arlington, VA, USA, March 14-16, 2016, Revised Selected Papers

[3] https://www.tsn.hhu.de/fileadmin/redaktion/Oeffentliche_Medien/Fakultaeten/Mathematisch-Naturwissenschaftliche_Fakultaet/Informatik/Soziale_Netzwerke/pubs/Kalman.Graffi_2013_IEEE.ICC.13_Symbiotic.Coupling.of.P2P.and.Cloud.Systems.The.Wikipedia.Case.

pdf
[4] https://5-info.eu/
[6] https://www.6.online/iso-27001/annex-a-8-asset-management/
[7] https://www.gesetze-im-internet.de/bsi-7v/BJNR095800016.html

V. VITA

Ralf Blumenthal is driving the Energy Efficiency Analytics business for Siemens Digital Grid on a global scale. He previously worked as a Digital Senior Consultant for business innovation and digitalization at the Siemens in-house consulting unit. Ralf holds a PhD in thermoacoustics from TU Munich and IIT Madras, and a diploma in aerospace engineering from University of Stuttgart and Ecole Polytechnique.
ralf.blumenthal@siemens.com

Felix Cadelcu graduated in 2004 from the University o f Applied Sciences in Nuremberg with a diploma degree (Dipl.-Inf.) in Computer Science. From 2004 he was working in the Digital Grid Business Unit at Siemens AG in Nuremberg, with some intermittent stays in the Digital Factory Division. Since 2016 he has been dedicated as lifecycle manager for asset management solutions for secondary equipment. There he was defining the requirements for interaction of cloud-based asset management solutions with cyber-security patch management workflows.
felix.cadelcu@siemens.com

Christian Blug is a member of the consulting department Siemens DG PTI. He holds a PhD in electrical engineering from Universität des Saarlandes and joined Siemens 2000 as network planning consultant. Since 2007 he was awarded as senior key expert on protection. Since 2015 he works as department head for power quality and earthing studies. He has also several patents on protection and grid optimization.
christian.blug@siemens.com