CUTTER CONSORTIUM
Access to the Experts

Cutter Business Technology JOURNAL

Vol. 30, No. 7, 2017

Management, Innovation, Transformation

"We're in the very beginning of a revolution dubbed the 'Internet of Things,' which enables us to propose and develop solutions for interacting with everything connected to the global Internet. Today, it's the time for every*thing*, rather than every*one*, to get connected."

— Charalampos Patrikakis and José Barbosa, Guest Editors

The Industrial Internet:
Driving Digital Transformation

Opening Statement
by Charalampos Patrikakis and José Barbosa 3

The Why and Hows of IIoT Implementation:
The View from a Regulated Industry
by Łukasz Paciorkowski 6

Cyber Security Risks and Challenges for the Industrial Internet of Things
by Anjali Kaushik and Kanishk Gaur 13

Enterprise Personal Analytics:
Embracing the Potential, Avoiding the Pitfalls
by Trevor Clohessy and Thomas Acton 18

Opportunities and Challenges for IIoT in Oil and Gas
by Claude Baudoin 28

From "Fast-Bleeding" to Market-Leading:
A Telecom's Digital Transformation Journey
by Evangelos Vayias and Ioannis Konstantinidis 36

NOT FOR DISTRIBUTION
For authorized use,
contact Cutter Consortium
+1 781 648 8700 or
service@cutter.com

Cutter Business Technology JOURNAL

As business models for creating value continue to shift, new business strategies are constantly emerging and digital innovation has become an ongoing imperative. The monthly *Cutter Business Technology Journal* delivers a comprehensive treatment of these strategies to help your organization address and capitalize on the opportunities of this digital age.

Founded in 1987 as American Programmer by Ed Yourdon, and until recently known as *Cutter IT Journal*, *Cutter Business Technology Journal* is unlike academic journals: Each monthly issue, led by an expert Guest Editor, includes five to seven substantial articles, case studies, research findings, and/or experience-based opinion pieces that provide innovative ideas and solutions to the challenges business technology professionals face right now — and prepares them for those they might face tomorrow. *Cutter Business Technology Journal* doesn't water down or delay its content with lengthy peer reviews. Written by internationally known thought leaders, academics, and practitioners — you can be certain you're getting the uncensored perspectives of global experts.

You'll benefit from strategic insight on how the latest movements in digital innovation and transformation, IoT, big data analytics and cloud, to name a few, are changing the business landscape for both new and established organizations and how cutting-edge approaches in technology leadership, enterprise agility, software engineering, and business architecture can help your organization optimize its performance and |transition to these new business models.

As a subscriber, you'll also receive the *Cutter Business Technology Advisor* — a weekly bulletin featuring industry updates delivered straight to your inbox. Armed with expert insight, data, and advice, you'll be able to leverage the latest business management thinking to achieve your organization's goals.

No other journal brings together so many thought leaders or lets them speak so bluntly — bringing you frank, honest accounts of what works, what doesn't, and why. Subscribers have even referred to the Journal as a consultancy in print and likened each month's issue to the impassioned discussions they participate in at the end of a day at a conference!

Get the best in thought leadership and keep pace with the technologies and business models that will give you a competitive edge — subscribe to *Cutter Business Technology Journal* today!

Cutter Business Technology Journal®

Founding Editor: Ed Yourdon
Publisher: Karen Fine Coburn
Group Publisher: Christine Generali
Managing Editor: Karen Pasley
Production Editor: Linda Dias
Client Services: service@cutter.com

Cutter Business Technology Journal® is published 12 times a year by Cutter Information LLC, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA (Tel: +1 781 648 8700; Fax: +1 781 648 8707; Email: cbtjeditorial@cutter.com; Website: www.cutter.com; Twitter: @cuttertweets; Facebook: Cutter Consortium). ISSN: 2475-3718 (print); 2475-3742 (online).

©2017 by Cutter Information LLC. All rights reserved. Cutter Business Technology Journal® is a trademark of Cutter Information LLC. No material in this publication may be reproduced, eaten, or distributed without written permission from the publisher. Unauthorized reproduction in any form, including photocopying, downloading electronic copies, posting on the Internet, image scanning, and faxing is against the law. Reprints make an excellent training tool. For information about reprints and/or back issues of Cutter Consortium publications, call +1 781 648 8700 or email service@cutter.com.

Subscription rates are US $485 a year in North America, US $585 elsewhere, payable to Cutter Information LLC. Reprints, bulk purchases, past issues, and multiple subscription and site license rates are available on request.

☐ Start my print subscription to *Cutter Business Technology Journal* ($485/year; US $585 outside North America).

Name _____ Title _____

Company Address _____

City _____ State/Province _____ ZIP/Postal Code _____

Email (Be sure to include for weekly *Cutter Business Technology Advisor*) _____

Fax to +1 781 648 8707, call +1 781 648 8700, or send email to service@cutter.com.
Mail to Cutter Consortium, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA.

Request Online License Subscription Rates

For subscription rates for online licenses, email or call: **sales@cutter.com** or **+1 781 648 8700.**

CUTTER CONSORTIUM
Access to the Experts

Opening Statement

by Charalampos Patrikakis and José Barbosa, Guest Editors

> Such gliding wonders! such sights and sounds!
> Such join'd unended links, each hook'd to the next,
> Each answering all, each sharing the earth with all.
>
> — Walt Whitman, "Salut au Monde!"

Whitman's delight in the connected world is well supported by all the benefits that have arisen since the introduction of the Web, which has democratized access to information by allowing it to circulate more rapidly and globally. Use of the Internet has brought people closer, provided early and almost instant access to news, changed the way business communication is performed, and given birth to a plethora of new business domains. The potential of the Internet and the parallel growth of computational and data storage capabilities have led to a new situation: a huge amount of information is out there, ready to be harvested, scrutinized, analyzed, and exploited. And the means to do that are also available, providing a fertile ground for the development of new services and applications.

The result is a proliferation of smart things, empowered by Internet communication, proving the validity of the proverb "None of us is as smart as all of us." While your furnace at home may be smart enough to understand that it should switch off after you leave the house, it is the evidence of your absence — reported by your GPS-enabled smartphone — that can trigger the logic. Platforms that allow the creation of rules and logic (such as IF This Then That, or IFTTT) for the collaboration of Internet-connected devices let users connect hundreds of types of devices operating in full cooperation.

Today, it's the time for every*thing*, rather than every*one*, to get connected. We're in the very beginning of a revolution dubbed the "Internet of Things," which enables us to propose and develop solutions for interacting with everything connected to the global Internet. We're convinced that we have just started to grasp all the possible capabilities that could emerge from this revolution. In our everyday life, at home, at work, or on the road, we have started to see its benefits: thermostats that can heat our houses while we are driving home, automatic tracking of goods and improvement of transportation/delivery times, and connected cars that can automatically search for a parking place or warn us of an accident ahead.

On the other hand, there are many factors we still need to consider and many problems we still need to solve in order to continue this revolution. Issues related to security, protection of personal privacy, even ethics will arise. The more intelligent the connected machines are, the more the issues we must face will shift from a strictly technological focus to one involving societal and human concerns. Control over production of goods and services marks a critical borderline. With state-of-the-art research in machine intelligence (e.g., deep learning) yielding results that can be applied to machines that control production (even that of producing the components from which they are made), machines have already started to infiltrate human territory, transforming from products to creators.

The more intelligent the connected machines are, the more the issues we must face will shift from a strictly technological focus to one involving societal and human concerns.

In past moments of transition (e.g., the Industrial Revolution), changes in technology, society, and government have led to transformation in activities, processes, competencies, and models. This is happening again with digital transformation, which is usually linked with revolutionary changes to business. Yet although this transformation has a direct impact on industry (introducing all the benefits and promise of Industry 4.0 and the Industrial Internet of Things [IIoT]), in many countries its effects have already

started to appear at the societal level. A characteristic example is that of Japan, where we find the "Society 5.0" initiative, a government program aimed at preparing Japanese society for digitization.

There is no doubt that the IoT is causing a series of revolutionary changes in the way we interact with machines, but one could argue that all technological advances are followed by similar changes. This time there are some fundamental differences, however, which can be attributed to the way humans are affected. The personal sphere is being invaded through access to information that has long been deemed private: health data, location tracking, personal identification, and so on. The recording and reporting of personal data, which in many cases is made available (sometimes inadvertently) by devices such as mobile phones and wearables, can reveal personal status, preferences, or particularities. If we consider the rise of data analytics and machine intelligence, we see that there is incredible potential for understanding and reasoning over the processed data, well surpassing human capability and intuition. As a result, moral, ethical, and legal issues are among the first ones that must be addressed in this new era of digital transformation.

Upcoming Topics

Agile Leadership: Foundation for Organizational Agility
Don McIntyre

Insurtech: Reinventing the Insurance Industry
Steve Andriole

Big Data Trends: Predictive Analytics, Machine Learning, and the Cloud
Bhuvan Unhelkar

Change Management
Sheila Cox

Customer Experience
Jeanne Bliss

The transformation that the new interconnected world of humans and machines is going through contains an implicit roadmap, and the job of practitioners is to find it out. Apart from the technical questions firms must answer in order to correctly implement IoT technologies in an industrial environment, questions concerning the human aspects involved are of utmost importance. What organizational culture and skills are necessary to encourage innovation and make a digital industrial transformation successful, and what steps should be taken during the transition to a connected facility? What measures should be taken so that the IIoT will encompass the necessary mechanisms for confronting cyber-physical risks? After all, we cannot forget that the IIoT refers to an industrial environment, where any cyber security threat may have a direct impact on products and people's lives. This issue of *Cutter Business Technology Journal* features five articles discussing the opportunities and challenges in this dawning era of IIoT and digital transformation, as well as (some) solutions to its likely problems.

In This Issue

We begin the issue with an article by Łukasz Paciorkowski, who starts by asking two critical questions: first, why should we implement IIoT solutions, and second, how should we do so? The author convincingly demonstrates *why* companies should invest in the Industrial Internet by offering a real-world example taken from an ongoing project in the biopharma industry, one of the world's most restricted fields. In explaining *how* companies will need to go about implementing IIoT initiatives, Paciorkowski draws attention to some very crucial issues, including the clash between the operational technology (OT) and information technology (IT) worlds and the always pertinent aspect of security. He ends with a brief glimpse of what lies beyond the IIoT, presenting some additional concepts worth exploring.

In our second article, Anjali Kaushik and Kanishk Gaur discuss the most important reason for *not* adopting IIoT: security. Like Paciorkowski, Kaushik and Gaur warn readers of the possible damage that can result from a lack of adequate security, providing several real-world examples of the harm caused by past cyber attacks. Also very interesting are the common mistakes they present — many simple to correct —accompanied by mitigation strategies that could turn out to be lifesavers or at least raise reader awareness about the need to include

©2017 Cutter Information LLC

security at the top of the priorities list when designing for IIoT.

Next, Trevor Clohessy and Thomas Acton examine the way the data collected over the IIoT ecosystem of interconnected humans and machines can be collected, managed, and exploited. They focus particularly on a concept they call *enterprise personal analytics*, "through which industrial organizations enable their workers to use their personal data to manage their digital working lives from descriptive, diagnostic, predictive, and prescriptive points of view." The authors provide a digital transformation roadmap companies can use to adopt enterprise personal analytics, examining the emerging concept through different perspectives (company, worker, and modality) and related concerns (individual information systems architecture, knowledge and intellectual property, motivation and remuneration, information governance, and quality assurance). Clohessy and Acton conclude with some further guidance on putting their digital transformation roadmap into practice within a company.

In our next article, Cutter Senior Consultant Claude Baudoin discusses promising IIoT applications in the oil and gas (O&G) sector. After giving readers some O&G context, the author suggests some "obvious" IIoT opportunities in the industry, including worker safety, pipeline surveillance, and pump monitoring. While individual readers might not have any oil well pumps to monitor, several use cases Baudoin describes (predictive equipment maintenance, asset monitoring, worker safety, etc.) are opportunities that can be applied to plenty of other domains. After describing these IIoT implementations, he turns his attention to IIoT challenges. Among these are the clash between OT and IT, security, and connectivity issues. As in our first article, Baudoin concludes with a glimpse into what is to come.

We end the issue with an article by Evangelos Vayias and Ioannis Konstantinidis, who also offer a roadmap for digital transformation and tell us how OTE Group used it to transform itself "from a 'fast-bleeding,' bureaucratic telco into a modern, competitive, high-performance service company" through the application of IoT-related technologies. The authors start with a contemplation of the digital age, observing how it — like the technological transitions that preceded it — has resulted in "an increase in human expectations for the available technical tools and capabilities." Vayias and Konstantinidis describe how OTE Group has employed the user journey design approach to: create a target picture of these expectations, identify and develop the capabilities needed to satisfy them, set up projects to deliver them, and establish metrics for measuring the company's progress toward the desired (and continuously evolving) end state. They close by outlining the challenges to their digital transformation program and the steps the company is taking to address them.

As one might expect, the digitization of the world is not an easy task, and many challenges lie ahead. In fact, we're in the very early stages of the IIoT and have barely scratched the surface of its full potential. We trust that the five articles in this issue will provide insight into the things to come and help you deal with the risks and challenges. There are rewards hidden in the road toward the digital transformation of our world into one of interconnected things, "each answering all, each sharing the earth with all." We hope this issue will help you find them.

Charalampos Z. Patrikakis is Associate Professor in the Department of Electronics Engineering at Piraeus University of Applied Sciences (PUAS). He has participated in more than 32 national, European, and international programs, 16 of which he served as Technical Coordinator or Principal Researcher. Dr. Patrikakis has more than 100 publications, including book chapters, international journals, and conference proceedings, and he has made two contributions to national legislation. He is a member of the editorial committee of more than 50 international journals and conferences, has acted as Editor of special issues of international journals and conference proceedings, and has coedited three books. Dr. Patrikakis is a senior member of IEEE; a member of the Technical Chamber of Greece, the European Association for Theoretical Computer Science, and the ACM; and a counselor of the PUAS student branch of IEEE. He can be reached at bpatr@puas.gr.

José Barbosa has a PhD in automation and computer science from the University of Valenciennes and Hainaut-Cambrésis (France) and an MSc in industrial engineering from the Instituto Politécnico de Bragança (IPB). He is a researcher at IBP, where he currently participates in the EU FP7 ARUM project and formerly participated in the EU FP7 GRACE project. He is also an invited professor in IBP's Department of Electrical Engineering. Dr. Barbosa has more than 30 papers published in international journals and proceedings of international conferences. His main research topics focus on the development of self-organizing and evolvable manufacturing control architectures following the holonic and multi-agent system paradigms enriched with biologically inspired mechanisms. Dr. Barbosa is also a member of the IEEE Technical Committee on Industrial Agents. He can be reached at jbarbosa@ipb.pt.

The Why and Hows of IIoT Implementation:
The View from a Regulated Industry

by Łukasz Paciorkowski

Barriers to IoT Adoption

Almost every article about the Internet of Things (IoT) starts with predictions of how many connected devices there will be beyond 2020. Those statistics try to catch our attention and make sure we understand (and agree with the assumptions about) how big the impact of IoT will be on consumer electronics, various industries, and the global economy in general. Proponents rave about the connected toasters we will be able to operate remotely using any smartphone.

But the reality is that organizations are often not able to clearly answer the simplest questions regarding the business case for IoT implementation. After the initial excitement — often fueled by consulting and market research companies — comes the hesitation and doubt: is IoT really such a cool and useful concept? Figure 1 shows the three main barriers to IoT adoption.

Why Should We Implement IoT?

The first barrier to IoT adoption is the question "Why?" Why should producers release connected products in the first place? The famous "connected toaster" sounds great until you start to analyze implementation and maintenance costs versus potential benefits. Creating a comprehensive business case for IoT is not a straightforward thing. Not only are connected products a fairly new and unexplored concept without well-defined and proven revenue models, but there are additional factors such as technology-related fees and new ways of selling products. All of these factors impact time and effort estimations and financial projections.

How Do We Implement IoT?

The second barrier to IoT adoption is the question "How?" Traditional product companies rarely have

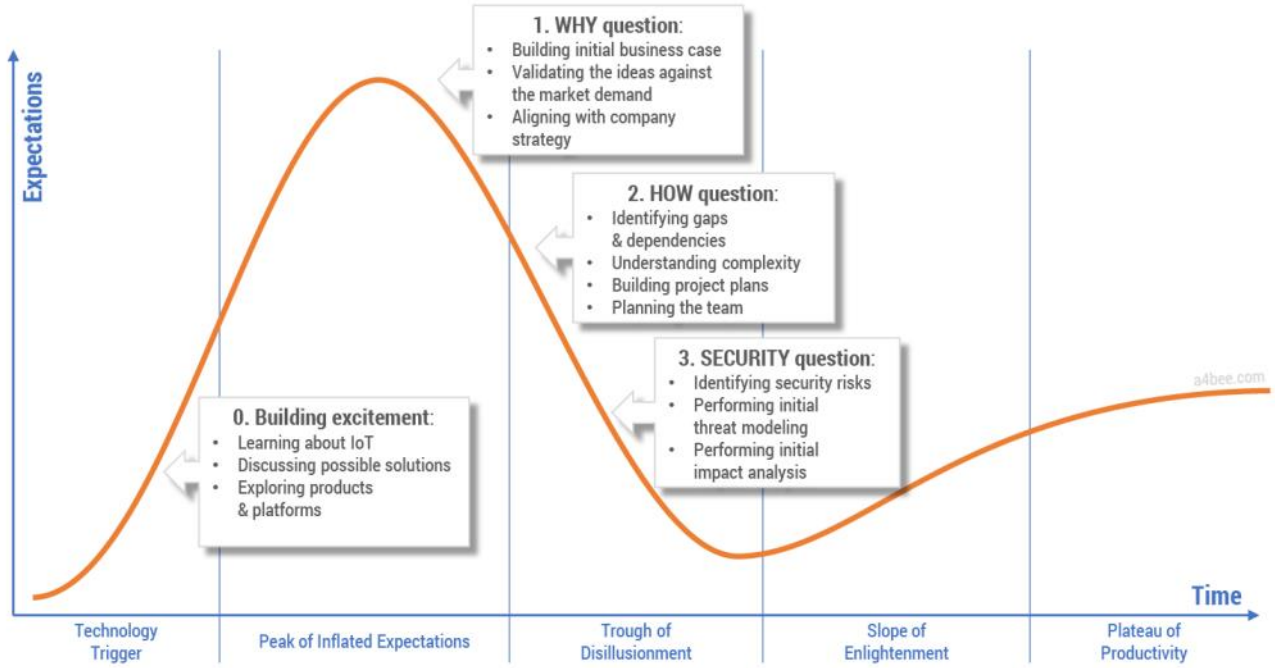


Figure 1 — Technology hype and the three barriers to IoT adoption.

©2017 Cutter Information LLC

the knowledge and capabilities to envision, design, implement, and maintain the complex IT systems that provide advanced communications and data processing capabilities. Many manufacturers face an almost existential question: are we still a product company or have we already become a software company? How do we bring new talents to the organization? How should we manage projects that are so different in nature from the ones we did in the past?

How Do We Ensure IoT Security?

The third barrier is security, the most often-used argument against implementing IoT. A justified fear of "being hacked" makes business stakeholders think twice before jumping on the connected products bandwagon. Recent publications showing just how unsecured connected products can be serve to discourage even the most enthusiastic innovators.[1] Consider the damage that could be done to an established product brand due to an IT hack. Is IoT worth it?

In this article, I will briefly discuss why companies should invest in the Industrial IoT (IIoT), offering a real-world example taken from an ongoing project in a global life science–biopharma organization. Then I will focus in greater detail on the second barrier: how to implement IIoT and address the challenges related to the implementation project. As we will see, the "how" does not relate solely to the technical aspects. In fact, technology is just one item on the long list of impediments connected to IIoT adoption. Organizational, cultural, and process-related challenges consume the greater portion of the time, money, and resources needed for IIoT-related efforts.

A Real-World Why: IIoT's Value Proposition for Biopharma

Let's begin by considering a potential business case that could justify investment in a connected products initiative. The example we will look at comes from biopharma, which is considered one of the world's most regulated and controlled industries.

In biopharma, a bioprocess is used to produce a wide range of drugs and vaccines leveraging living cells. The process itself consists of multiple steps — from upstream bioprocessing, where cells are grown and cultivated, to downstream processing, where the product (cells mass) is purified, concentrated, and polished.[2] The entire process is enabled by equipment that provides the environment for the bioprocessing. This equipment consists of many different Unit Operations (Unit Ops or devices) used to perform specific steps in the bioprocess. Unit Ops available on the market fall into one of the three categories: manual, semiautomatic, or automatic. As we might expect, IIoT initiatives aim to automate the end-to-end bioprocess, eliminating manual actions and assuring higher performance and quality of the entire production process.

Some of the advantages IIoT could provide for the biopharma industry include:

- **A higher level of automation.** As a bioprocess consists of multiple steps performed on multiple devices using a range of consumables, automated orchestration of data collection and data processing is a highly desired feature. In more detail, there are four main issues to be resolved:
    - **Integration.** Without automatic integration, activities within the bioprocess have to be performed by the human operator. Obviously, such a requirement increases the cost of labor and creates more opportunities for human error.
    - **Data acquisition.** Data acquisition and, specifically, a track-and-trace feature are critical from a regulatory and compliance standpoint. Each consumable used within the process needs to be properly evidenced and recorded. Automating this part of the process using sensors, wireless tags, and other techniques provides a great improvement opportunity.
    - **Data integrity.** With more data being collected and analyzed, data integrity is growing in importance. Ensuring that data was not tampered with, altered, or deleted is critical for security, safety, and compliance. Especially in drug- and food-related industries, implementation of regulations such as 21 CFR Part 11 or EudraLex is a must. IIoT with strong data encryption capabilities can satisfy "hard" system requirements, while the "soft" ones can be addressed through proper process and standard operating procedure (SOP) definitions.
    - **Reporting.** Batch reporting, which relies on documenting all data related to the manufacturing process (order and the details of every step) and underlying conditions (data from sensors like temperature or pH value), is critical in the biopharma industry. Without the proper collection

of the data, the final product cannot be released to the market, and the batch will be considered a waste (or loss, in business terms). End-to-end reporting is a perfect example of where IIoT capabilities can bring significant benefits, savings, and optimization.

- **New capabilities and services driven by data.** Data collection is nothing new in software automation. Nevertheless, historically, data in automation was used in a limited manner (e.g., directly supporting the manufacturing process). With the advent of advanced analytics, machine learning, and deep learning, new opportunities emerge. Process-related improvements discovered through data mining or predictive maintenance are examples of putting data to good use. Additionally, data integrators (vendors or service providers) can offer additional services based on insight-rich, cross-customer data lakes.

Technologies, definitions, wording, and even their ways of working and thinking are so different that it is almost impossible to imagine how OT and IT could cooperate.

- **Lower setup and operational costs.** In biopharma, as in some other industries, a new breed of startups are emerging: young firms with big budgets that want to set up their own bioprocess production. Without deep expertise or know-how, such organizations rely heavily on the external expertise and out-of-the-box functionality delivered with the automation platform. A high level of standardization and a comprehensive set of functions drive the design of modern, future-proof IIoT platforms. In addition, new and established market players are constantly searching for ways to lower the risk and cost related to compliance. Standardization of data formats (e.g., B2MML), protocols (e.g., OPC UA), and integration capabilities provides an optimization and cost-reduction opportunity for both startups and existing companies. Surprisingly, for a traditional, regulated, and closed industry like biopharma, usage of cloud is being discussed as well. It is seen as a way to shorten the release and time-to-market cycles, while at the same time lowering CAPEX investments.

These are some of the most obvious benefits the IIoT could offer the biopharma industry. Further analysis of business models, processes, and market segmentation provides many more arguments for IIoT implementation. Assuming we are already convinced that connected products are the way forward, let's now look at some challenges related to the IIoT implementation process.

How #1: Bridging the OT-IT Gap

For years, operational technology (OT) and information technology (IT) have lived in their own worlds. OT concentrated on operational excellence, safety, and reliability, whereas IT focused on rapid innovation, new technologies adoption, and continuous delivery. Indeed, those worlds grew so far apart that it takes quite a bit of time before OT and IT engineers can have a meaningful conversation. Technologies, definitions, wording, and even their ways of working and thinking are so different that it is almost impossible to imagine how the two could cooperate. And yet IIoT is bringing these two worlds together.

For manufacturing companies, connected devices, sensors, and automation are nothing new. Over the past 40 years, industrial software platforms have steadily grown, bringing reliable automation to the manufacturing sector to help car manufacturers, oil companies, utilities, and many more organizations optimize and automate their operations. Including sensors in every moving component is bread and butter for seasoned automation professionals. So what is different about the IIoT?

One of the most significant changes in current industrial automation trends is that, until recently, OT lived in its own closed ecosystem. Starting from specific software like DCS or SCADA, through costly hardware like PLCs and industrial sensors, up to dedicated network infrastructure, OT was connected but isolated. Cyber threats so common to the IT world were mitigated by cutting any external access to the industrial automation systems. Compliance and regulatory requirements along with international standards made OT a very stable environment. In many industries, upgrading an operating system with newly released patches is a totally novel concept. Once validated and qualified, a piece of equipment could work without a single update for years! Confronting this reality with, let's say, smartphone upgrade frequency shows just how different IT and OT lifecycle management is.

©2017 Cutter Information LLC

Yet as early as 2010 the industrial world was clearly shown that the separation of IT and OT was not exactly working. That's when the Stuxnet virus successfully penetrated isolated industrial computer systems and targeted Iran's nuclear power plants, causing irreversible damage.[3] This was one of the most sophisticated cyber attacks the world has ever witnessed.

Despite growing security concerns, business stakeholders across industries were put under greater pressure to deliver innovative solutions faster, while at the same time lowering operational costs. As a result, industrial automation practice has been forced to move from a connected but isolated environment to the globally connected ecosystem. With this new reality, manufacturers must embrace new opportunities but also prepare for new threats and challenges coming from the traditional IT world. This is where the aforementioned IT/OT convergence is taking place.

How #2: Rewiring the Organization's Collective Brain

Although a fair amount of OT innovation was introduced over the years, it was nowhere close to what was happening in the pure IT world. Today, however, the rate of innovation is rapidly increasing, even in the most regulated and conservative industries. This is caused partly by the advancements in technology and partly by geoeconomic and globalization trends. Quality comes with an ever-decreasing price tag. Emerging market players can successfully compete with well-established Western corporations. The competitive ecosystem is changing — with IIoT-based capabilities being at the center of this change. Doing "things" the same way is not enough to retain market share.

In our biopharma industry example, the traditional business model relies on selling a product: a standalone, often disconnected, and self-sufficient device. Software automation was a necessary addition and was treated as an integral part of the product. With IIoT platforms coming into the picture, new data-driven services influence how we look at the final product. Suddenly the software and data platforms are as important and valuable as the hardware product itself. A logical step for vendors is to stop talking about products and move toward services. This transformation is very similar to what happened in the IT hardware market after the concept of cloud was introduced and the "as a service" revolution took off. It can bring a lot of benefits, but if not managed properly, it can kill the organization.

Going from being a product to a service company is a truly transformational experience. This shift does not impact only one group or one department in the organization. It requires rethinking the entire organization, starting from the foundation of business and revenue models, through go-to-market strategies, and on up to organizational structure, processes, skills, and capabilities. This cannot happen without the support, understanding, and dedication of people on all levels in the organization: the board of directors and C-suite, middle management, and the operational staff. This is also the moment where the most pushback can be seen from the participants.

Changing the way of working is never easy, especially in such a conservative and traditional industry as biopharma. Continuous education, discussions, and leadership involvement are necessary to manage the transition to a new reality. Not everybody will agree, not everybody will get it, but eventually rewiring the organization's collective brain has to happen. Although regulated industries tend to be very stable, as the barriers to entry for new market players are high, even there exponential technologies[4] such as IoT are disrupting the status quo. It is always better to be the disruptor than to be disrupted.

How #3: Ending the Clash of the OT and IT Titans (Process, Security, Organizational Transformation)

Process Convergence

Good manufacturing practices (GMP) are well-established, globally recognized, and widely applied guidelines for food and drug production processes.[5] Good automated manufacturing practices (GAMP) guide the software automation domain in the pharmaceutical industry.[6] At the core of both GMP and GAMP is the quality assurance process. The behavior of the manufacturing system has to be unconditionally predictable and clearly defined. Each deviation from the standard process has to be recorded, approved, and managed by a dedicated procedure. Quality is embedded on every level: from the equipment design and production, up to the manufacturing line assembly, configuration, and operation, and ending at the device's decommissioning.

OT engineers and specialists live and breathe those regulations and practices every day. The waterfall

development/delivery method is thus a natural choice for them. The V-model for software development[7] — an extension of the waterfall process — encourages up-front design and long delivery cycles. This method of project delivery worked for years. Why change it?

On the other side, there is a "new" IT delivery model characterized by flexible planning, fast delivery iterations, and a fail-often/fail-fast mentality. Agile practitioners do not understand five-year-long release plans. What matters is the current sprint (or iteration). Young IT professionals are using the newest (but not always the most reliable) technologies available on the market. They ask:

- Why use 30-year-old technology if Facebook just released a new front-end library?
- What do you mean "It has to be Windows"? Don't they use Linux in the automation world?
- Microservices are the way forward. But how do we install Docker and a Kubernetes cluster on a single embedded PC? Does that makes sense?
- And finally, what is wrong with this quality assurance? Why do they check everything that we do and deliver? Do we really have to document *everything*?

And on it goes …

The differences in the IT and OT approaches to system design are so profound that it takes a lot of energy to bring those two worlds together. Yet IIoT requires this convergence (see Figure 2). There has to be alignment on the technology stack, data models, integration method, reliability targets, and security policies. Both the IT and OT worlds have their own points of view, experience, and best practices. Willingness to listen to the "other side" is a must. An IT engineer will not succeed in the automation world without support from an experienced OT colleague. Similarly, an automation engineer will have a hard time navigating in the new IT environment. They both have to work together and be open to learning from each other — and there is a lot to learn.

Safety, Security, and Speed of Delivery

Two very important differences between OT and IT concern reliability and security. Traditionally, if a system fails in the customer-centric IT world, the worst-case scenario is that a user will complain about the poor experience. If a system fails in the OT world, somebody might die. It is important for IT architects and engineers to understand this significant difference and ensure that the reliability requirements are properly reflected in the system design.

Security by design is a natural thing for IT. Modern IT platforms are designed to be exposed and to be resilient in the face of any type of cyber threat. In contrast, manufacturing systems need to be safe, not necessarily secured. It is hard to ensure the security of a platform that is updated once every few years. The standard approach to security in the OT world is system isolation: limiting access to the platform, cutting all connections, and controlling user interactions with the processes and SOPs. But IIoT requires connectivity on multiple levels. OT can learn a lot from IT when it

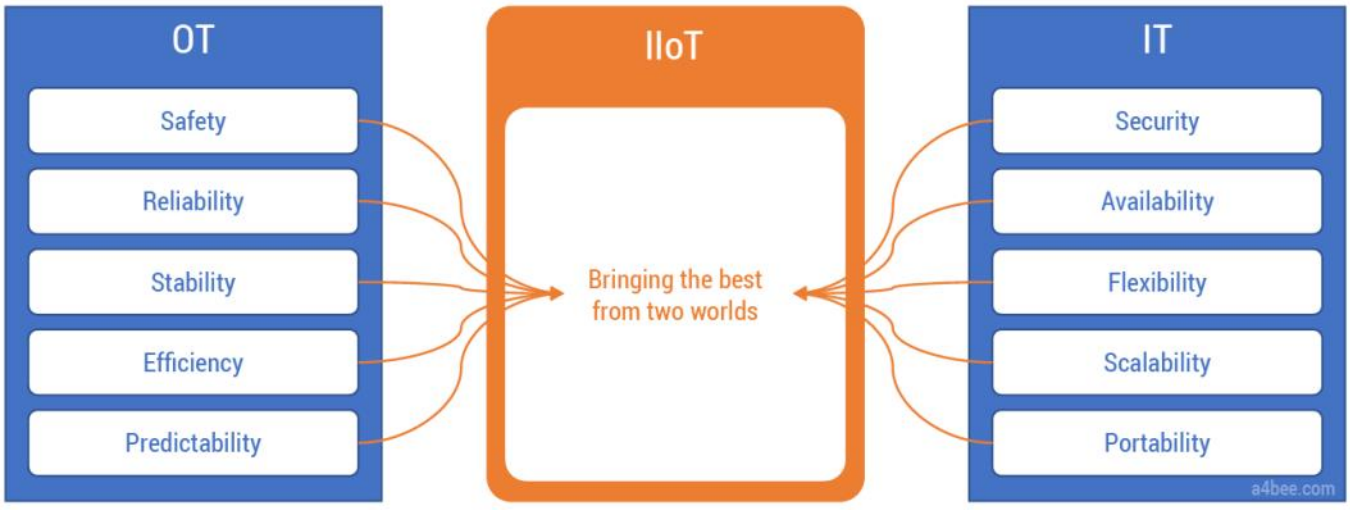


Figure 2 — OT and IT meet in the IIoT.

©2017 Cutter Information LLC

comes to introducing advanced threat modeling, implementing modern security controls, and practicing appropriate lifecycle management.

There are many more differences between OT and IT that are encompassed in their respective ways of looking at system design and implementation — namely, waterfall (V-model) versus Agile (iterative model). How can system implementers stay flexible while at the same time respecting GMP/GAMP principles? This is where a huge amount of effort is required.

One answer would be to move from one V-model to a model made up of multiple small Vs (see Figure 3). Instead of designing and planning an entire system in a single go, let's follow the Agile, iterative approach, while also respecting all of the quality assurance requirements. That way we end up with a delivery process in which the complete V-model is executed in each sprint. All quality artifacts (tests, risks assessments, etc.) are produced together with the code during the sprint execution. The quality department becomes an integral part of the Agile development team. This is not easy, and it requires a lot of discipline, but it is doable.

Impact on the Organization

With all the changes described above, it is natural that many other parts of the company will have to adjust as well. The organizational structure should transform in preparation for maintaining and delivering new types of services. The IT organization needs to prepare for new kinds of systems and platforms being introduced to the corporate ecosystem. Go-to-market and sales teams must educate themselves in new offerings, services, and business models. Finally, the entire organization has to continue innovating, since in the hyperconnected world of IIoT, things will change faster than they ever did before.

The organization's transformation will not happen immediately. Acquiring necessary skills (or developing them in-house) will take time. Based on the experience of the biopharma industry, it makes a lot of sense to use external consultants, experts, and coaches. This approach significantly shortens the learning curve for the organization and the people in it. Creating multiple lightweight proofs of concept that confirm (or don't confirm) vision and design assumptions will lower the risk for the overall IIoT program. Using an Agile delivery method will help the organization adjust its course and introduce improvements early in the development process. Cooperating across multiple departments is critical for success.

Beyond IIoT

IIoT is an enabler. It provides plumbing for data-driven capabilities and services. Connected products are an interesting concept, but the real value is in the data produced by the devices. That is why it is so important to have a clear vision and strategy on what data to collect and for what purpose(s). Some concepts worth exploring together with IIoT are:

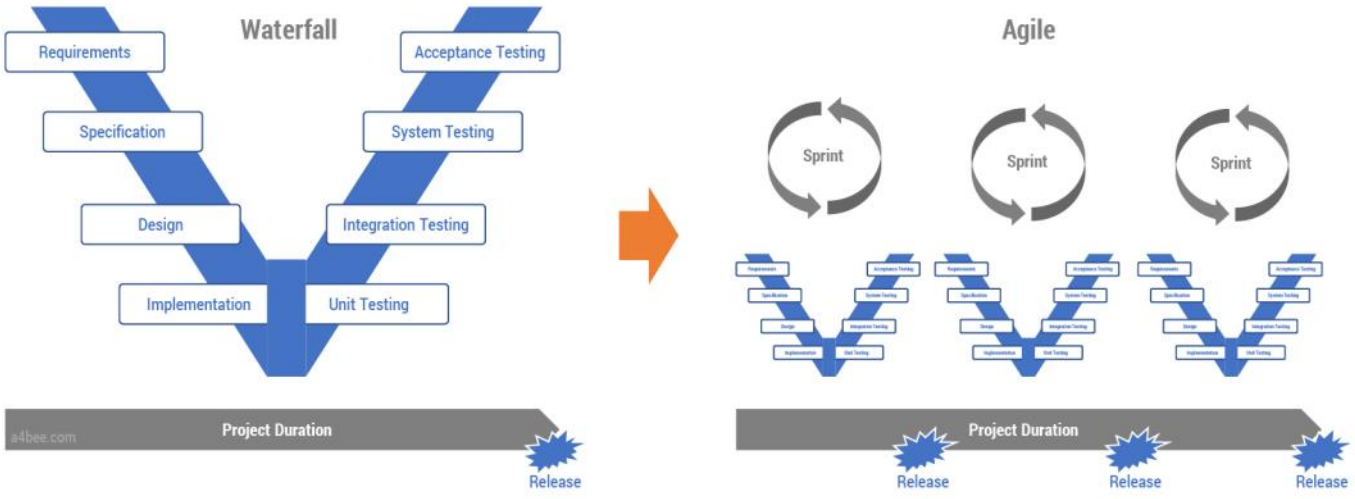


Figure 3 — From a waterfall/V-model to an Agile delivery method in a regulated environment.

- **Advanced analytics with predictive modeling.** Analytics and deep data mining can be used both for optimization purposes as well as for exploring and discovery. Applying techniques from the artificial intelligence (AI) domain on IIoT data sets seems to have great potential.

- **Blockchain.** When data generated by the devices represents a value that can be traded or exchanged, blockchain can be helpful. Blockchain is already used in the energy industry, where electricity trading is governed by distributed ledger. Blockchain can also be used for managing a digital trail attached to a physical object. In the biopharma industry, the products or consumables genealogy can be managed using distributed ledger.

- **Self-managing control platforms.** With sufficient sensor data, advanced real-time analytics, and AI, it is possible to create a self-managing, self-adjusting, and self-optimizing control system. Such a platform would be able to detect and correct deviations in the process, adjust parameters accordingly, and properly record the actions taken. In laboratories, self-managing control platforms could take care of performing experiments and refining process parameters continuously to find the optimal setup. With enough data from IIoT instead of physical experimentation, predictive process simulation could be used.

Researchers and system designers are constantly exploring these and many other ideas. The IIoT represents a big opportunity for all industries, even regulated ones. However, it also requires new system designs, new tools, new processes, and — above all — a willingness to change. In the coming years, we will see more and more connected products with amazing capabilities released to the market. Pressure to reduce costs will push manufacturers to search for additional savings related to optimization and automation. In the center of this change is the IIoT with its interconnected sensing-and-reacting systems and platforms. It is important not to miss this opportunity and to start exploring the IIoT as soon as possible. You can be sure that your competition is already doing so.

Endnotes

[1]Ronen, Eyal, et al. "IoT Goes Nuclear: Creating a ZigBee Chain Reaction" (https://eprint.iacr.org/2016/1047.pdf).

[2]"Bioprocess." Wikipedia (https://en.wikipedia.org/wiki/Bioprocess).

[3]"Stuxnet." Wikipedia (https://en.wikipedia.org/wiki/Stuxnet).

[4]Dorrier, Jason. "Staggering Promise of Exponential Technologies in a Succinct 5-Minute Video." SingularityHub, 10 June 2014 (https://singularityhub.com/2014/06/10/staggering-promise-of-exponential-technologies-in-a-succinct-5-minute-video/).

[5]"GMP Resources." ISPE (www.ispe.org/gmp-resources).

[6]"Good automated manufacturing practice." Wikipedia (https://en.wikipedia.org/wiki/Good_automated_manufacturing_practice).

[7]"V-Model (software development)." Wikipedia (https://en.wikipedia.org/wiki/V-Model_(software_development)).

Łukasz Paciorkowski is a Principal Architect and cofounder of Architects of Business (a4bee.com), an independent group of architects, designers, and IT specialists focusing on IIoT, cloud, security, and digitization in general. Previously, Mr. Paciorkowski worked for IBM as an Executive Architect and for Accenture as a Senior Principal. For the last 12 years, he has been helping customers around the world to envision, design, and implement complex systems and platforms. Mr. Paciorkowski is particularly interested in exponential technologies, hyperconnectivity, and how technology influences business, society, and people. He can be reached at lukasz.paciorkowski@a4bee.com.

©2017 Cutter Information LLC

BETTER SAFE THAN SORRY

Cyber Security Risks and Challenges for the Industrial Internet of Things

by Anjali Kaushik and Kanishk Gaur

In recent years there has been significant growth in the Industrial Internet of Things (IIoT), both in terms of the types of devices getting connected and the applications for which they are used. The number of Internet-connectable devices worldwide has increased from 8 billion in 2011 to 17.4 billion in 2016.[1] This connectivity is providing benefits such as better analytics to improve productivity and quality, predictive maintenance, and remote monitoring of industrial equipment. The growth of the IIoT is also bringing challenges, such as the need for a strategy to manage high data volumes and promote secure coding practices in IIoT devices.

As the Internet reaches beyond computers and mobile phones to other devices — especially in industrial systems — the threat of remote exploitation is also extending to new areas. Nearly half of US firms using an IoT network have been hit by a recent security breach, which can cost up to 13% of a smaller company's annual revenue.[2] IoT attacks expose companies to the loss of data and services and can render connected devices dangerous to customers, employees, and the public at large. The potential vulnerabilities for firms of all sizes will continue to grow as more devices become Internet dependent.

While some risks in the IIoT arise from its unprecedented scale (with such a large number of inadequately protected things connected to the Internet), other risks stem from the nature of these devices and how they are designed, deployed, and managed. These risks range from malware attacks, hacktivism, and espionage to physical damage or sabotage. When deployed in an industrial control system (ICS) or production process, the IIoT controls switches, valves, and motors, which in turn may control vital systems. Critical infrastructure sectors such as power, oil, natural gas, manufacturing, and transportation use IIoT devices as sensors and actuators for automation, remote monitoring, and control. The controllers themselves may be Internet accessible. As a result, cyber attacks in the industrial space can have severe consequences for operations and safety.

An awareness of IIoT risks and challenges and how to manage them is important to making safe and beneficial use of the Industrial Internet of Things. In this article, we discuss those risks and challenges. To make the IIoT viable, organizations will need a strategy to address them.

Possible Risks

The possible risks to IIoT devices include reduced performance, reduced quality, poor reliability, and nonavailability of the IIoT device owing to physical damage/destruction of the production system deploying it. Other risks may arise from a "botnet of things," data leaks, and increased concerns around privacy, interoperability, and data access privileges.

Physical Damage/Destruction and Operational Losses

If malicious attackers wish to take over IIoT devices remotely, they can do damage by calling, texting, or clicking from anywhere on the Internet. As the Stuxnet incident[3] shows us, the possibility of cyber-physical attack is real. IIoT devices are now used in power plants, water pumps, and oil rigs, and these devices appear to be far less secure than we might assume.

An insecure remote access control protocol can allow a cyber criminal to hijack a process control system and push parameters to unsafe levels. For instance, in 2000, in what is known as the Maroochy Shire incident,[4] a hacker remotely seized control of an Australian wastewater facility on 46 separate occasions and, over the course of two months, spilled 264,000 gallons of sewage into nearby streams and rivers.

In another incident in Germany in 2014, attackers used spear phishing and social engineering to gain access to the office network of a steel plant. This gave them access to the production network and further to the

devices controlling the production machines. The outages in the production machines prevented the plant from appropriately shutting down a blast furnace, leaving it in an undetermined state. This resulted in significant damage to the plant.[5] In such attacks, the malware is introduced through conventional IT systems and goes on to affect the operating system in the device. For the attacker, it requires specialized knowledge of not only corporate IT, but also industrial control systems and the production processes.

Given the vulnerabilities in today's corporate IT (which includes firewalls, routers, desktops, and mobile devices), significantly better security will be required, even in small and seemingly insignificant IIoT devices. This is even more the case as such devices may be interconnected, and thus an insignificant IIoT device may lead to an important control device.

In 2017, the WannaCry ransomware attack crippled the UK National Health Service and severely impacted operations in different organizations.[6] Likewise, car manufacturers Renault, Nissan, and Honda were forced to shut down their production facilities because systems were infected with WannaCry. Such malware attacks can disrupt the operations of IIoT devices and gain unauthorized access to production systems and corporate IT systems. There have been instances where IIoT devices have been compromised, allowing unauthorized users to perform surveillance and monitoring, gain access to or control production systems, and induce device or system failures.

IIoT devices may leak private user data, both from the cloud (where the data is stored) and between IIoT devices themselves. Most IIoT devices do not encrypt data that is being transferred; the clear-text data can be read in transit. This can cause a breach and is a potential risk to the safety and security of the systems.

"Botnet of Things"

Most IIoT devices are vulnerable to compromise and capable enough to be part of a distributed attack. If we do not deploy adequate security measures on these devices, multiple hacked connected "things" can be taken over and then used for coordinated distributed denial-of-service (DDoS) attacks. Many devices that unknowingly contribute to DDoS attacks are not behind any firewall or else have weak default firewall configurations which, again, are easily compromised. Individual IIoT devices that are compromised can be pulled into a new botnet anytime.

In 2016, the Mirai botnet[7] caused a massive DDoS attack that brought down parts of the Internet using a large number of hacked surveillance cameras and home routers. Devices infected by Mirai malware continuously scan the Internet for the IP address of IoT devices. Mirai then identifies vulnerable IoT devices (those using common factory default usernames and passwords), logs into them, and infects them. In another incident in 2016, routers from Deutsche Telekom crashed due to exploitation by a variant of Mirai, which resulted in Internet connectivity problems for the users of these devices.[8] Such DDoS attacks can cause immense damage.

Privacy, Interoperability, and Data Access Privileges

A security breach in an IIoT device can have implications for life and property. This risk is heightened if the devices are deployed in the healthcare industry. A malware or ransomware attack on thermostats or medical appliances in hospitals (body scanners, infusion pumps, etc.) can threaten human lives and safety. Privacy requirements and data access privileges must be carefully crafted in IIoT devices. In addition, standards are needed to facilitate interoperable installations and seamless integration involving many different vendors' devices.

Common IIoT Flaws and Vulnerabilities

Failure to Observe Fundamental Security Principles

Not all vulnerabilities stem from the technologies themselves — behavioral aspects also come into play. For instance, a lack of security awareness within the organization can inadvertently expose systems to cyber attacks, such as when employees bring portable media that is infected with malware. Some operations employees working on the IIoT simply believe their systems are an unlikely target, and therefore they are reluctant to change their behaviors and implement new security protocols.

Many IIoT breaches are caused by exploiting the rudimentary default passwords that connected device owners didn't bother to change, as in the Mirai attacks discussed above. In August 2017, Bharat Sanchar Nigam Limited (BSNL), an Indian national

©2017 Cutter Information LLC

telecommunications company, suffered a malware attack that targeted 60,000 modems with a default "admin-admin" username/password combination. BSNL's broadband customers had not changed the modems' default user name and password, thus enabling the breach.[9]

Most IIoT devices have a Web or mobile interface. If the interface is vulnerable, it may lead to a breach in the system. Sometimes, the data access privileges flout basic security principles such as "least privilege" and "need to know."

Finally, the majority of IIoT devices do not encrypt data that is being transferred. As mentioned above, this means the clear-text data can be read in transit. This can cause a breach and is a potential risk to the safety and security of the systems.

Outdated Software

The updating of software and plugging of vulnerabilities do not occur as promptly with IIoT devices as in corporate IT. As a result, devices may be running vulnerable and outdated software, which can be easily compromised. If used in process automation and industrial control systems, such software can compromise the quality and specifications of products, be a safety hazard, and cause damage.

In some cases, IIoT devices may be dispatched from the factory with embedded software that is either outdated from the start or becomes outdated over time. In other IIoT devices, the device may carry more current software, but vulnerabilities may be discovered in the future. This makes the IIoT device less secure unless there is an automated mechanism to update the software.

A number of IIoT devices allow for automated software updates. In such cases, the system may fail if the corresponding authentication mechanism is not robust. Weak authentication mechanisms can be misused by an attacker to compromise the IIoT device.

Increased Connectedness, Data Volumes

Until recently, enterprise information systems and production systems were not linked to IIoT devices. The new trend toward connectedness has brought the challenge of developing a unified, secure enterprise architecture. Also, a huge volume of data is expected to be generated as a result of the growth in interaction between devices and systems. The real value of the IIoT comes from the ability to extract, organize, and mine this data and take proactive action based on the insights gained. For example, the device data can be used to design safer and more efficient mechanisms, practice predictive maintenance in ICS, and so on. Organizations will need a strategy to manage the high data volumes and push secure coding practices in IIoT devices.

The new trend toward connectedness has brought the challenge of developing a unified, secure enterprise architecture.

Crafting a Mitigation Strategy

The IIoT risk is real. A strategy to manage this risk is a must, and the following components can help.

Proactive Awareness and Understanding of the Risks

The IIoT is not a standalone device. Organizations that adopt it must embrace a total system perspective that takes into account vulnerabilities in the devices, firewall security, network connections, cloud services, and the Internet itself. Along with that, organizations need to proactively assess how integrating the IIoT with ICS and corporate IT will affect their risk profile. They should also conduct security awareness trainings on behavioral issues[10] such as failure to change default passwords, improper use of portable devices, and similar security risks.

Pushing Secure Coding Practices for the IIoT

Organizations and industry vendors that are developing IIoT devices need to embed robust security and privacy practices into their design and development. Data access privileges should be based on established security principles such as "least privilege" and "need to know." Data in transit between IIoT devices or between an IIoT device and a corporate IT system must be encrypted. Organizations should avoid the tendency to introduce beta test versions of systems without conducting sufficient trials in an IIoT device.

Vendors need to design IIoT devices so that they can receive software updates over their entire lifespan. This will help user organizations in the rapid automated remediation of serious flaws. This is important, as new vulnerabilities may be discovered in IIoT devices over a period of time. The automatic updates should be supported with a robust authentication mechanism. For instance, IIoT devices can be designed with unique credentials, and users can be made to change the default password upon first use.

Furthermore, organizations should implement resilient system architectures that can inherently minimize the risk in case of a breach or failure of an IIoT device. This may be done through techniques such as segregation, backup, redundancy, proactive monitoring, and so forth.

For consumer IoT, the end user is also the system administrator. Organizations that deploy IIoT devices can define the role of IIoT device administrator depending on the ICS and production processes in which each device is deployed. For instance, devices deployed on the shop floor can be connected so that they give a warning signal to the supervisor or local maintenance technician in case of a security flaw. This can aid in better management of IIoT devices.

Cyber Insurance

A possible strategy to reduce (or mitigate) IIoT breaches is cyber insurance. Lower insurance premiums for more secure IIoT devices would be an incentive for organizations to take IIoT security seriously. Cyber risk issues that challenge insurability and market development include:

- **Lack of awareness of cyber insurance products.** The biggest challenge in obtaining the insurance is business leaders' lack of awareness of cyber being an insurable risk.
- **Low level of cyber insurance coverage.** The level of coverage provided by the insurer may not meet the organization's need. Insurers must also take the initiative and communicate to business leaders the value of cyber insurance in coping with cyber risk.
- **Problems in fixing liability.** When major disruptions occur due to an IIoT device, is it the fault of the manufacturer, the vendor, the person or organization that deployed the device, the cloud or back-end communications provider, or the user of the device? More work needs to be done to define possible scenarios and standardize the cyber insurance industry's methods for establishing liability for irresponsible cyber security actions.
- **Difficulty in pricing cyber insurance products.** Standardized definitions are needed across the cyber insurance industry. For instance, how are different risks — and the policies surrounding those risks — defined? This will require data and analysis of that data to fine-tune the pricing models. Another approach would be to set up a forum to facilitate the sharing of insights on cyber disaster scenarios, with a view to improving the ability to underwrite risks and understand their aggregation.
- **Uncertainty as to what is covered under a cyber insurance policy.**[11] What further complicates the development of cyber risk insurance offerings is the fact that traditional insurance products have not been designed to protect clients against cyber risks. In fact, underwriters of traditional business insurance lines have reacted to the emergence of this new class of risk by introducing cyber exclusions. The resulting mix of implicit and explicit coverage creates a complex situation in which the buyer is never able to ascertain the true level of coverage for any given cyber risk scenario.

With ransomware-based attacks increasing day by day and attack vectors getting more complex, it is not possible for the insurance market to develop a dedicated product line that addresses many of the key risks clients face. Hence true end-to-end cyber insurance coverage remains a far-off dream for today's business users. Instead, businesses can explore the possibility of purchasing cyber-specific coverage in the form of extensions to traditional policies or as standalone cyber policies.

More Advanced System R&D

To ensure that all known risks are reasonably managed, it is a good idea to study a few categories of IIoT devices in research and development. This research can specifically focus on design and development of trustworthy systems. Blockchain technology appears to have immense potential for increasing IIoT security as it can transfer data in a way that is transparent, safe, auditable, and resistant to outages. This can help IIoT devices to update software and manage bugs directly.[12]

©2017 Cutter Information LLC

Government Regulation

Electronic products that have the potential to hurt or kill people or cause serious business disruptions need to be brought under some form of government regulation and testing. IIoT device development, distribution, and maintenance processes need to be strengthened by ensuring that robust security and privacy practices are used in design and development. National governments can play an active role in harmonizing international best practices for the IIoT and deciding on security checks and compliance requirements. The distribution of IIoT devices that suffer from significant security and privacy issues must be prevented.

Discretion Is the Better Part of IIoT Valor

How much automation is too much? When extending Internet connectivity to the process automation industry and industrial control systems, we need to measure the risk and then decide which types of devices should (and should not) be connected and the applications for which they can be used. It may simply be too risky to connect all types of devices to the Internet. An organization's IIoT strategy should be supported by a formal risk management plan that addresses such issues. Meanwhile, governments can intervene by clearly defining the categories of IIoT devices that, in view of the health and safety risks, they deem too risky to be connected. Overall, IIoT devices have increased the vulnerability of all stakeholders, and we need to take responsible steps to reduce cyber attacks and make the IIoT viable.

Endnotes

[1]Schneier, Bruce. "Botnets of Things." *MIT Technology Review*, March/April 2017 (https://www.technologyreview.com/s/603500/10-breakthrough-technologies-2017-botnets-of-things/).

[2]"Survey: Nearly Half of US Firms Using Internet of Things Hit by Security Breaches." *IoT Business News*, 1 June 2017 (https://iotbusinessnews.com/2017/06/01/65662-survey-nearly-half-u-s-firms-using-internet-things-hit-security-breaches).

[3]Langner, Ralph. "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve." The Langner Group, November 2013 (www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf).

[4]Crawford, Michael. "Utility Hack Led to Security Overhaul." *Computerworld*, 16 February 2006 (www.computerworld.com/article/2561484/security0/utility-hack-led-to-security-overhaul.html).

[5]Kovacs, Eduard. "Cyberattack on German Steel Plant Caused Significant Damage: Report." *SecurityWeek*, 18 December 2014 (www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report).

[6]Palmer, Danny. "WannaCry: Why This Ransomware Just Won't Die." ZDNet, 22 June 2017 (www.zdnet.com/article/wannacry-why-its-ransomware-that-just-wont-die).

[7]"Mirai (malware)." Wikipedia (https://en.wikipedia.org/wiki/Mirai_(malware)).

[8]Krebs, Brian. "New Mirai Worm Knocks 900K Germans Offline." *Krebs on Security*, 30 November 2016 (https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline).

[9]"Affected Modems Were Not Updated, Says BSNL." *Deccan Chronicle*, 30 July 2017 (www.deccanchronicle.com/nation/current-affairs/300717/affected-modems-were-not-updated-says-bsnl.html).

[10]Berman, Francine, and Vinton G. Cerf. "Social and Ethical Behavior in the Internet of Things." *Communications of the ACM*, Vol. 60, No. 2, February 2017 (www.cs.rpi.edu/~bermaf/Berman+Cerf_IoT.pdf).

[11]"UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk." HM Government and Marsh Ltd., 2015 (www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf).

[12]"19 Industries the Blockchain Will Disrupt." Future Thinkers, 15 June 2017 (www.youtube.com/watch?v=G3psxs3gyf8).

Anjali Kaushik is Professor of Information Systems at the Management Development Institute, Gurgaon, India. She has almost 23 years of consolidated experience in the area of IT business consulting and research in both the corporate world and academia. Prior to joining academia, Dr. Kaushik headed the vertical research group in IDC (India) Limited. She is also a regular consultant to the government of India for various projects related to strategic planning, policy making, monitoring, and impact assessment on e-governance and cyber security. Dr. Kaushik has authored five books with major publishers and has more than 20 published research papers in various journals. She holds a PhD from Delhi University in the area of information systems planning. She can be reached at anjalikaushik@mdi.ac.in.

Kanishk Gaur is a Senior Manager with Deloitte Touche Tohmatsu LLP in the Cyber Risk Advisory Practice. He has more than 10 years of experience in information and cyber security consulting, advising both enterprise and government clients in the areas of risk management and business protection. Prior to joining Deloitte, Mr. Gaur spearheaded an advanced security service line for EY in North India, where he advised various banking, telecom, and technology clients on cyber threat management and incident response. He holds a postgraduate diploma in management from the Management Development Institute, Gurgaon, India, in the area of information systems. He can be reached at kagaur@deloitte.com.

THIS TIME IT'S PERSONAL

Enterprise Personal Analytics:
Embracing the Potential, Avoiding the Pitfalls

by Trevor Clohessy and Thomas Acton

Introduction

> We're in the age of auto-analytics, or the capturing and analysis of personal productivity data.
>
> — Thomas H. Davenport

Organizations have long used analytics to improve performance. Indeed, research shows that top-performing organizations use business analytics five times more than lower performers do.[1] In 2016 the business analytics industry was worth an estimated US $130 billion. It is predicted that industrial sectors such as discrete manufacturing, process manufacturing, telecommunications, and healthcare manufacturing will invest a combined total of $101.5 billion in business analytics by 2020.[2]

We believe that the emerging concept of enterprise personal analytics has the potential to become the new frontier of competitive differentiation.

One promising technological advancement in this regard will be the use of personal analytics. While traditional organizational intelligence metrics deliver a big picture of structures, processes, and roles, more detailed and personalized analytics enables employees to scrutinize their personal productivity in terms of their desired versus their actual way of working. Personal analytics empowers individuals to analyze and exploit their own data to achieve a range of objectives and benefits across their work (e.g., productivity, quality, performance) and personal lives (e.g., sleep, exercise, health). Personal data can relate to biometrics, personal finance, social media activities, health status, behaviors, emotional states, mobility, personal interest areas, and so on.

Organizational interest in personal analytics is also beginning to gain traction. In this article, we will focus on a concept that we call "enterprise personal analytics" (or EPA, for short), through which industrial organizations enable their workers to use their personal data to manage their digital working lives from descriptive, diagnostic, predictive, and prescriptive points of view.

Like many IT analysts, we believe that the emerging concept of enterprise personal analytics has the potential to become the new frontier of competitive differentiation. EPA may be of particular interest to industrial sectors such as manufacturing, utilities, energy, and aviation. For instance, EPA can enable skilled and unskilled industrial operators to analyze their own personal data to understand why they're making the choices they're making and then to combine their human expertise with the underlying objective data to create new operating procedures and processes.[3] Wearable technology is increasingly being used in the manufacturing industry for employee safety, employee monitoring, video applications, field service, and plant monitoring.[4] Organizations can also leverage the rich insights provided by nonverbal data — which can be captured by personal digital monitoring technologies for time management (e.g., Microsoft MyAnalytics), facial coding (e.g., Affectiva, Microsoft Emotion), brain imaging (e.g., NeuroSky, Emotiv), pupillometry (e.g., Tobii, Eye Square), and physiological monitoring (e.g. Empatica, Fitbit) — to improve efficiency and attention management, increase well-being, and reduce mistakes. Industrial organizations can use all of this EPA data and more to provide actionable insights that directly support their most important business decisions (automating a process versus losing employees' tacit knowledge, rewarding star players/teams, enhancing the physical and mental well-being of employees, etc.).

©2017 Cutter Information LLC

The EPA Digital Transformation Roadmap

The use of personal analytics in an enterprise setting is different from its use in other environments (e.g., private use). This has implications for which aspects of personal analytics should be considered in an enterprise context. We have identified five specific concerns pertaining to the use of personal analytics in an enterprise setting: individual information systems (IIS) architecture, knowledge and intellectual property (IP), motivation and remuneration, information governance, and quality assurance. As EPA involves a number of stakeholders, it is useful to study the concept from different perspectives. Our analysis has revealed three relevant perspectives: company, worker, and modality (i.e., the mode through which companies enable their workers to use personal analytics). Consequently, we have used a two-dimensional grid (concerns vs. perspectives) to define a roadmap that organizations can use to guide their EPA digital transformation efforts (see Table 1).

Concerns

IIS Architecture

IT consumerization, or the adoption of consumer devices and applications in the workforce, is pervasive. Employees bring computer tablets and smartphones into the workplace and harness social media applications and special-purpose apps for their work lives.[5]

According to Georgia State University Computer Science Professor Richard Baskerville, a typical IIS architecture consists of two specific work systems: the individual's work system as an employee, and the individual's work system as a person.[6] These systems are facilitated by individually and enterprise-provided cloud computing technologies, which produce and consume services.

Figure 1 depicts an employee's IIS architecture. Given the opaque nature of IIS, our knowledge of how the employee has designed and planned the architecture and how he controls it is limited. Why has he made the choices and investments reflected in Figure 1? How could the organization optimize his IIS architecture? Baskerville opines that organizations can no longer ignore IIS architectures for the following reasons. First, IIS "represent the most recent frontier for the design of computer-based [information systems]." Second, IIS are "complicated and unique systems that cross the boundaries" between personal life (e.g., social aspects) and work life (e.g., organizational aspects). Third, IIS do not merely store data; individuals are "actively collecting data and processing it into information for various purposes and feeding it outward."[7]

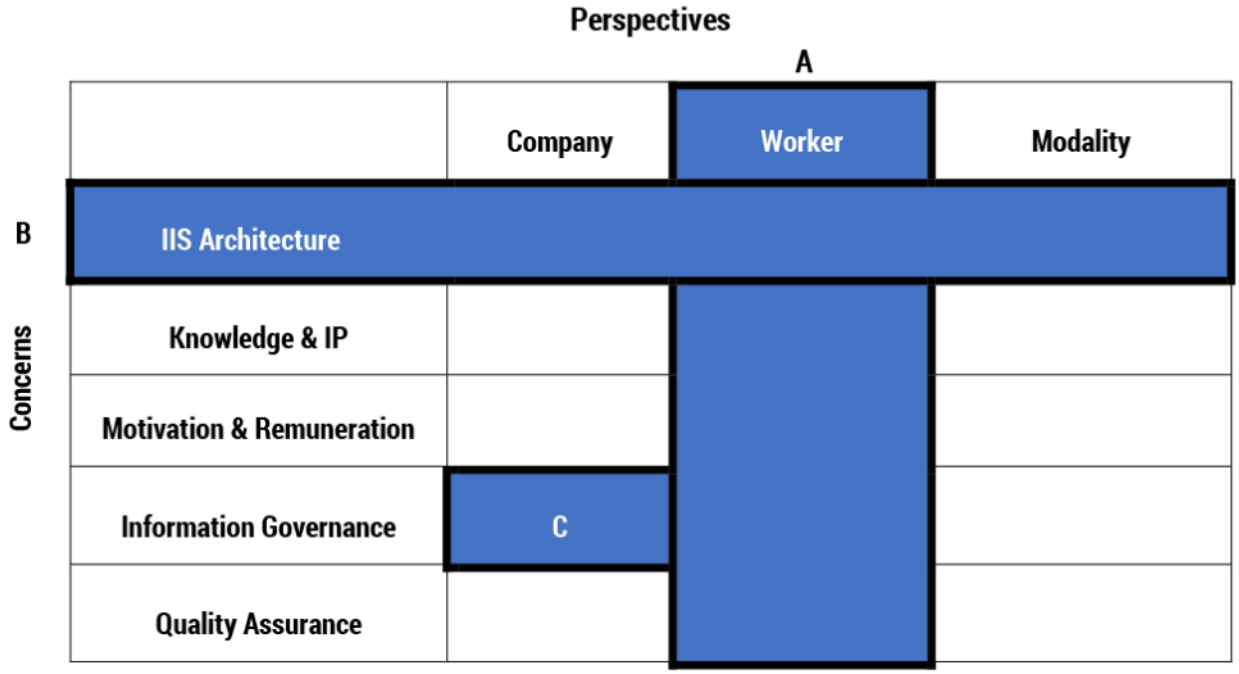


Table 1 — The EPA digital transformation roadmap: (A) a multi-concern, single-perspective view; (B) a single-concern, multi-perspective view, (C) a single-concern, single-perspective view.

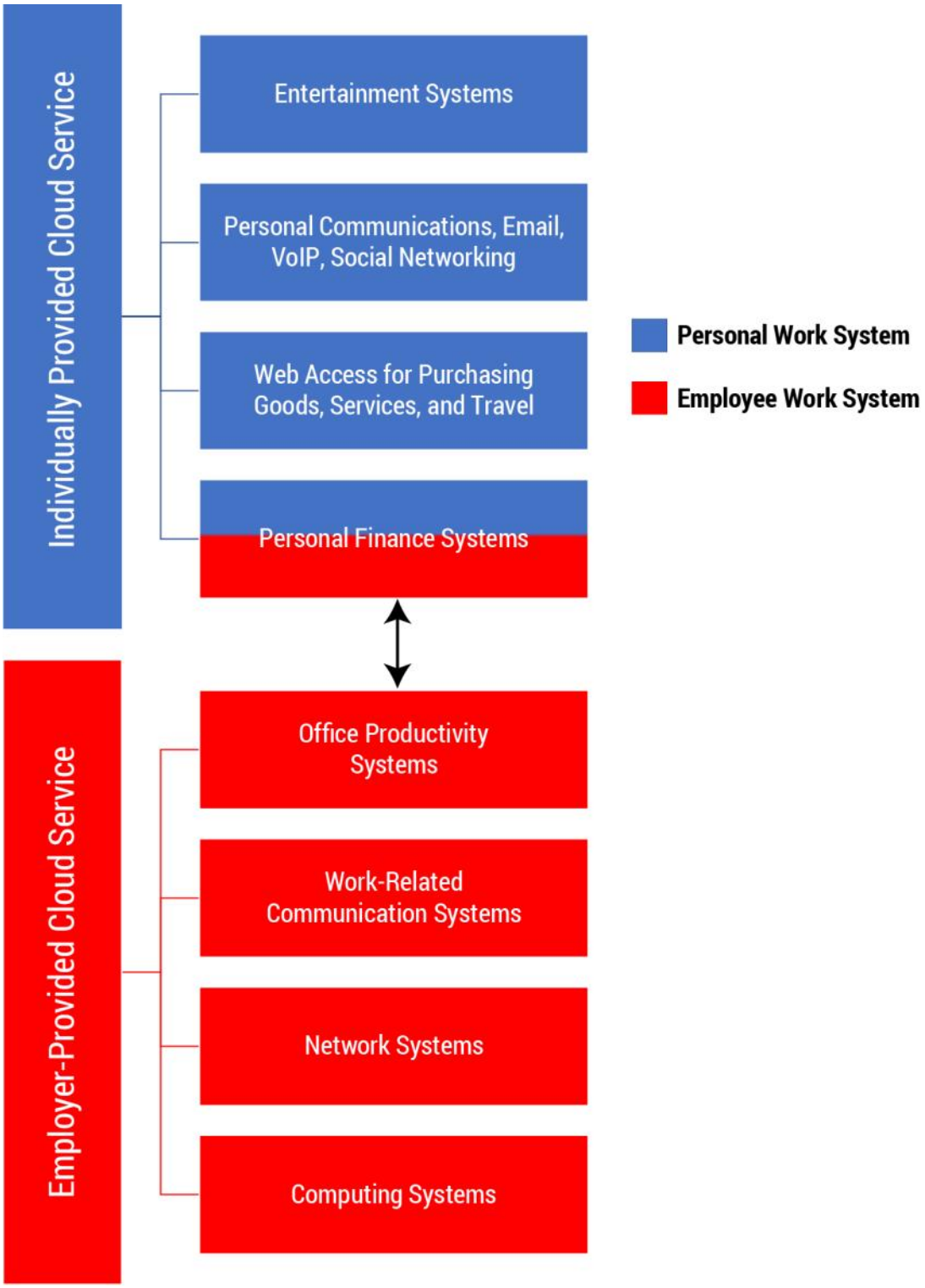


Figure 1 — An employee's IIS architecture. (Adapted from Baskerville.)

©2017 Cutter Information LLC

Knowledge and IP

With the aid of digital technology and the tracking and monitoring of the self, optimization becomes not only possible but also desirable. In an EPA context, where the individual worker's personal analytics data is viewed as an information asset, the manner in which knowledge and IP are managed becomes of paramount importance from a legal perspective. For instance, when an employee leaves a company, who owns the individual worker's EPA data — the company or the worker? If the latter, can the worker use her own personal analytics data to highlight her expertise and skills to prospective employers in a sort of digital résumé? Would this transfer of EPA data make companies more vulnerable to competitors employing collective intelligence techniques (e.g., using competitor data sources to predict their strategies)?

It may be that there are irreconcilable conflicts between a company's and an employee's interests with regard to EPA. Take, for instance, cases where organizations make employees sign noncompete agreements, which can hinder the employees' ability to take their personal data to another job in their current industry. For EPA initiatives to succeed, organizations must be sensitive to employees' concerns, which can be alleviated through education and transparency. One possible solution would be for organizations to create BYOD policies that encourage workers (e.g., by providing financial support) to purchase and bring their own monitoring devices to work. In such an arrangement, the workers would have full control of their own data. For example, Philips has developed the Rationalizer EmoBowl and EmoBracelets for stock traders. These products are designed to feed data solely to the individual workers (e.g., the primary consumers), with no executive involvement, so that they can alter negative working patterns and enhance productivity. Further EPA business cases are required to determine how companies can effectively implement a requisite level of knowledge production versus knowledge protection in an EPA context.

Motivation and Remuneration

EY Global Chief Analytics Officer Christopher Mazzei observes that "how an organization measures and rewards employee performance matters," underscoring "the importance of aligning incentives with desired behaviors" in the context of personal analytics use.[8]

Because meaningful individual analysis can only be achieved after an adequate volume of data has been collected, the choice of EPA data analysis medium is an important consideration. In a personal analytics context, "employees may look into their data with different goals, backgrounds, and expectations (e.g., internal context). However, the vast majority of people are not visualization or data analytics experts, so analytical tools will need to be accessible,"[9] note University of Victoria researcher Dandan Huang and her coauthors. It is recommended that organizations opt for technologies that come with minimal learning overhead. Ultimately, organizations must develop EPA strategies that inspire long-term use amongst workers.

Workers may be reluctant to share their personal data openly with peers, particularly when that data is used to compare their individual performance with others on their team.

That said, there is a gray area with respect to how continuous self-monitoring of one's personal analytics can impact workers. For instance, UK researchers concluded "it is conceivable that people may become over-reliant on automated systems that provide a false sense of security or ... could also suffer from negative consequences of excessive self-monitoring by finding it uncomfortable, intrusive, and unpleasant."[10] Workers may also be reluctant to share their personal data openly with peers, particularly when that data is used to compare their individual performance with others on their team. The lessons learned from the large-scale abandonment of personal health–tracking technologies, which is currently occurring amongst users of smart watches and fitness trackers, can provide valuable insights. One study found that "features that signal the device's ability to collect activity data are essential for adoption, whereas device portability and resilience are key for sustained use."[11]

Information Governance

Information governance is the set of multidisciplinary policies and controls aimed at managing information at an organizational level, supporting legal, regulatory,

and risk compliance requirements. Effective information governance policies secure confidential data and enable unneeded data to be disposed of in a systematic and legally compliant manner. The potential nexus of parties (e.g., partners, workers, customers, data pools, cloud and network providers) encompassed in an EPA initiative necessitates robust information governance mechanisms. Specifically, the European Union's General Data Protection Regulation (GDPR), which comes into force in 2018, applies to all companies worldwide that process the personal data of EU citizens. GDPR will introduce:

- A broader definition and scope in relation to personal data
- Stringent worker consent procedures
- Mandatory privacy impact assessments
- The appointment of a data protection officer
- Common data breach notifications
- Stringent data-handling principles (e.g., the right to be forgotten)
- Privacy by design requirements
- A tiered financial penalty structure

Industrial companies considering implementing EPA initiatives will have to operationalize information governance strategies that are fully in line with GDPR requirements.

The use of personal analytics has much to teach organizations about alignment, performance improvement (individual and team), and business ecosystems.

There may also be a need to develop regulatory frameworks that support the validation of EPA initiatives. Such frameworks could potentially persuade enterprises to collaborate within a community of organizations with a vested interest in providing open access to their collective personal analytics methodologies and data collection and analysis protocols. Similar approaches have already been effectively adopted in the healthcare industry, where manufacturers of wearable technology devices have established interconnected open source platforms where information can be exchanged in order to ensure the reliability of the devices while also alleviating security and privacy concerns.[12] Another example is the Connected and Open Research Ethics (CORE) initiative, which aims to bridge the gap between manufacturers, researchers using wearable technologies, and ethics boards tasked with protecting the research participants with respect to the processing of personal data.

Quality Assurance

Personal data is characterized by unpredictability and high volume, variety, and velocity, and the value of this data to an enterprise will be commensurate with the data quality and the power of the analytics done on it.[13] Many enterprises have reached a point where their ability to generate data exceeds their ability to consume it. Furthermore, they have merely developed the capability for analytics production in the absence of any analytical tools that can provide significant insights.

Data visualization tools (Tableau, Raw, DataHero, etc.) have been lauded as a means of addressing this disconnect. With regard to EPA, we encourage industrial organizations to develop new methods, tools, and principles for ensuring data quality, reliability, and certainty throughout the data transformation and analysis process. New tools are also required to support personal data analysis in order to make insights easy to comprehend and actionable at every point within an organization and at every skill level, from experts to analytical amateurs.

Organizations may find that there are many data sources that can be better and more easily analyzed through their enterprise BI analytics tools, as opposed to the less robust analytical capabilities and limited data sets on workers' individual mobile and wearable devices.[14] If that's the case, workers might be more willing to use EPA in their working lives in order to derive more meaningful results.

Perspectives

Company

Companies can have different motivations for using EPA. The use of personal analytics has much to teach organizations about alignment, performance improvement (individual and team), and business ecosystems.[15]

©2017 Cutter Information LLC

For example, a company may want to increase innovation in its current business processes. The use of personal analytics can enable employees to identify and suggest improvements that can result in cost savings, better customer service, and decreased employee frustration. These new improved processes and follow-on developments can become institutionalized across an organization. Furthermore, companies can derive value from employees who use their personal analytic devices (e.g., smart watches) to productively sync to organizational resources while working remotely.

In most businesses, "analytics have typically focused on operational or marketing issues and not on the human dimension of performance…. Even when companies do employ human resource analytics, their approaches are not sophisticated and have been applied only to individuals,"[16] writes Babson University Professor Thomas Davenport. Yet there is also scope for organizations to use EPA in a team context so that they can evaluate performance across different team compositions. Davenport discusses how companies, employing a technique called "plus/minus" analysis, can use personal analytics to assess not just individual performance, but the way specific teams perform with or without a particular worker.[17]

Before launching an EPA digital transformation initiative, however, there are a number of considerations a company must take into account. These include identifying the maturity and sophistication of the organization's analytical capabilities, determining the turnaround time for implementing such a strategy (e.g., quick wins vs. longer-term goals), implementing procedures for gaining strong organizational commitment toward the new EPA strategy, and, most significantly, considering the impact on individual worker morale and team dynamics.

Worker

The use of personal analytics can also benefit workers by increasing their understanding of how their work impacts the company's strategy and goals (e.g., business insight), facilitating meaningful working environments, enhancing career opportunities, and improving job satisfaction. These factors are critical for retaining and engaging all types of workers. For instance, analytics expert Jeanne Harris and her coauthors found that the use of modern digital technologies in the face of "changing characteristics of the generation of employees now entering the workforce, particularly their high levels of comfort with, and expectations about, social networking and consumer technologies ... was seen as a valuable tool in attracting and retaining these new hires."[18]

Companies require a better understanding of how to best operationalize EPA efforts within the organization at an individual worker level and assistance with the core analytics processes that would be required to support this. For example, Davenport[19] describes a scenario in which a company enables its sales employees to use the extensive data from its customer relationship management applications in order to assess and improve their performance. If, for instance, the most successful sales professionals tend to spend less than 10% of their time on lead generations, then average and low performers could adjust their daily work routines to do likewise.

The use of personal analytics can benefit workers by increasing their understanding of how their work impacts the company's strategy and goals, facilitating meaningful working environments, enhancing career opportunities, and improving job satisfaction.

Modality

Modality refers to the mode through which personal analytics is experienced by the worker or is deployed by the company. This is becoming an increasingly important perspective, as intelligent digital ecosystems are being supported by a fluidly and dynamically interconnected mix of:

- Individuals
- Information
- Services
- Devices, such as:
  - Traditional computing and communications (platform, desktop, mobile, tablet)
  - Wearables (health monitors, augmented and virtual reality displays)
  - The Internet of Things (consumer appliances, transportation, and environmental sensors)
  - Data storage (hard drives, cloud, USB)

As our digital environment evolves, a number of important questions emerge in the context of EPA modality. For example, how does the user experience fundamentally change, and what digital technologies, security architectures, and platforms are required to support this change? Most significantly, the ability for workers to use multiple modalities effectively (which will entail multi-tasking and context switching) is a salient requirement for the successful development of a company's personal analytics strategy. Therefore, when contemplating the best modalities for their EPA initiatives, organizations should consider the frequency of interruptions and how quickly users can recover from them.

Using the Digital Transformation Roadmap

Having examined the five core EPA concerns and the three perspectives, let's take a look back at the EPA digital transformation roadmap depicted earlier in Table 1. A novel feature of this "grid"-type roadmap pertains to the various pilot study designs that can be operationalized. The first design is a multi-concern, single-perspective view denoted by the letter A. The second design is a single-concern, multi-perspective view denoted by the letter B. The final design represents a single-concern, single-perspective view denoted by the letter C. Given the rather infant status of the EPA phenomenon, we encourage future organizational pilot studies to populate each of the cells within this grid framework. To assist the process, we have devised a number of questions that we believe merit further consideration (see Table 2).

		Perspectives		
Concerns		**Company**	**Worker**	**Modality**
	IIS Architecture	What reference architectures are suitable for creating productive and interoperable IIS architectures for workers?	How can the company effectively develop a flexible IIS architecture that continuously facilitates worker learning and improvement?	How can IIS architectures contribute to the teams' and company's overall goals?
	Knowledge & IP	What data governance agreements can be put in place to handle scenarios in which workers request access to their EPA data when they leave the company?	How can workers create and analyze knowledge in a meaningful way?	What digital tools should be in place for effective knowledge sharing between workers?
	Motivation & Remuneration	What practices should be established to effectively empower and satisfy workers?	How can personal analytics be made appropriate for use in enterprise contexts — including by people who have little experience with data, visualization, or statistical reasoning?	What are the effects of using multiple digital devices and ubiquitous connectivity on individuals' attitudes, behaviors, and performance?
	Information Governance	How can the company minimize privacy and IT security issues for individual workers' private lives?	Who assumes the responsibility for monitoring and controlling worker personal analytics data?	What digital device policies are appropriate for data retention, data sharing, and interteam data transfers?
	Quality Assurance	Who or what algorithms govern the analysis and presentation of personal analytics data?	What specific individual worker metrics can contribute to organizational KPIs in a meaningful way?	What digital tools can workers use to ensure the effective sourcing and subsequent analysis of their personal data?

Table 2 — EPA digital transformation roadmap example questions.

©2017 Cutter Information LLC

Furthermore, there is a significant need for EPA business use cases and EPA adoption frameworks. In our analysis, history suggests there are two dimensions that impact how a disruptive technological trend and its business use case evolve. The first is complexity, which is represented by the level of coordination required by all parties in an organizational ecosystem in order to produce value with the technology. The second dimension is novelty, which describes the level of effort a user requires to understand the problems that the new technological trend can solve. The more novel a concept is, the greater the learning curve.

We encourage industrial organizations to develop adoption frameworks that map possible EPA implementations against these two dimensions. Complexity and novelty can vary from low to high in terms of the stage of technology development. For instance, industrial organizations new to the EPA concept may want to introduce an EPA pilot program that is low in novelty and low in complexity (e.g., use of wearable fitness trackers to reduce the organization's insurance policy premiums).

In order to advance the emergence of EPA business use cases, we have also devised a visual mapping artifact that we have coined the "EPA digital transformation metro map" (see Figure 2). It depicts possible routes that companies must navigate through the five concerns across the three perspectives raised in this article:

- Pink = IIS architecture
- Blue = Knowledge and IP
- Yellow = Quality assurance
- Red = Information governance
- Green = Motivation and remuneration

For illustration purposes, we have completed the journey for the IIS architecture concern (i.e., the pink

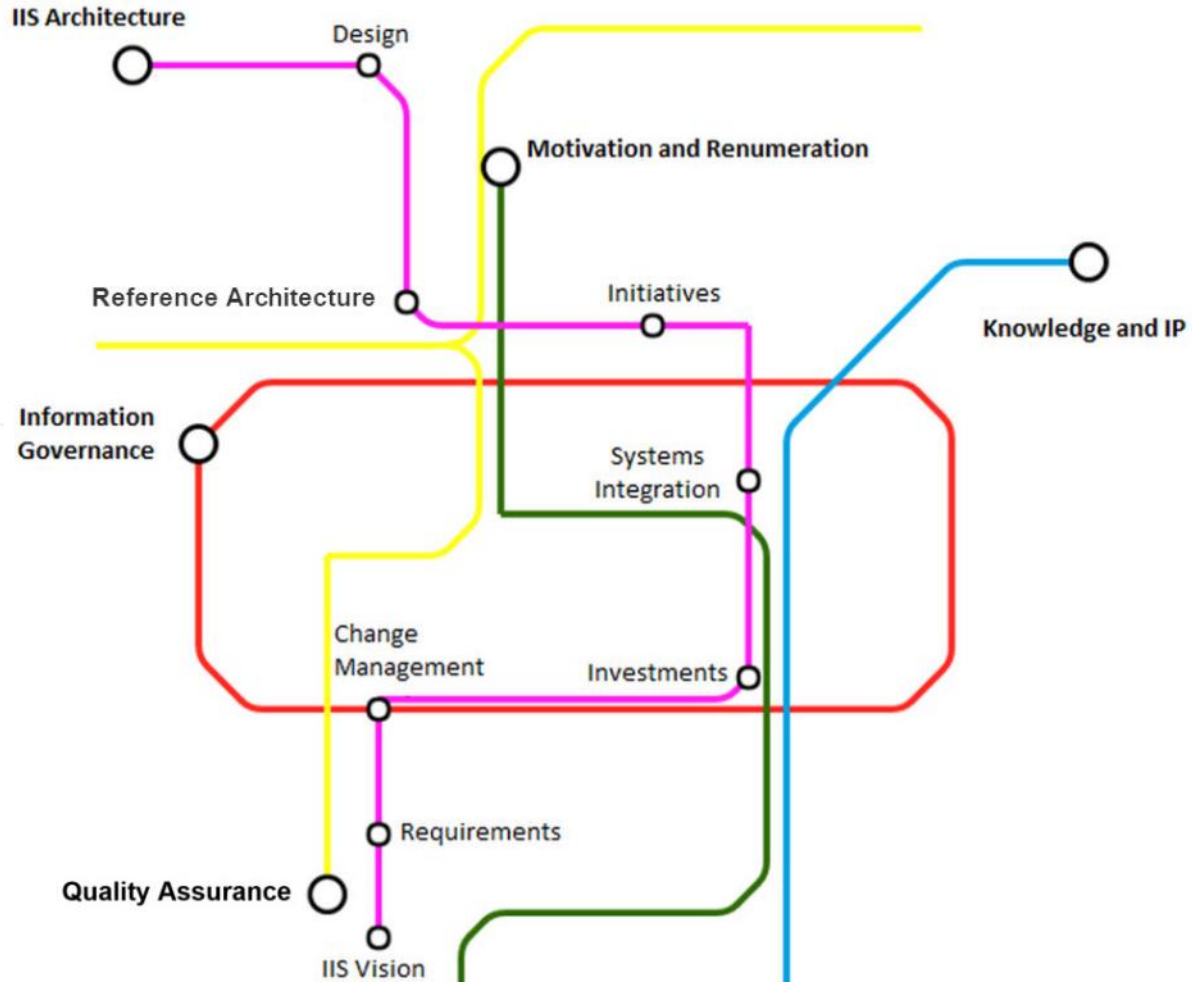


Figure 2 — EPA digital transformation metro map.

route). This specific journey comprises possible "route stops" that organizations must consider in terms of:

- Design (e.g., security, applications, and process architectures)
- Reference architecture (e.g., business continuity management, analytics sources)
- Initiatives (e.g., flexible architectures to ensure continuous learning)
- Systems integration (e.g., legacy systems)
- Investments (e.g., wearable technology vs. desktop monitoring)
- Change management (e.g., new employee onboarding)
- Requirements (e.g., individual vs. group)
- IIS vision (e.g., alignment with the main EPA strategy)

We must stress that we have only used these specific route stops for illustration purposes, and we encourage industrial organizations to carry out pilot EPA projects to identify the specific stops that are the best fit for them with respect to all the concerns outlined above.

While the application of EPA in an industrial setting remains a relatively niche practice, we believe its impact will fundamentally change the industrial landscape.

Conclusion

Global businesses are increasingly embracing the use of personal digital technology in the workplace. Wearable technologies, for example, are providing capabilities that are completely new to mainstream business practices (e.g., Tobii's EyeX, SMI eye-tracking glasses).[20] While the application of EPA in an industrial setting remains a relatively niche practice, we believe its impact will fundamentally change the industrial landscape. Ultimately, industrial sector organizations will be at the forefront of the EPA drive with, according to Davenport, "the bulk of data from emanating sensors within an 'the industrial Internet,' comprising a very large number of networked devices in plants, transportation networks, energy grids, and so forth."[21] We believe that if organizations behave appropriately and build a culture of trust, companies and workers (and customers) will become acclimatized to capturing and analyzing their personal data within an enterprise setting. Organizations need to proactively prepare themselves for this change, as EPA is coming soon to a company near you!

Endnotes

[1]LaValle, Steve, et al. "Big Data, Analytics and the Path from Insights to Value." *MIT Sloan Management Review*, Winter 2011 (http://sloanreview.mit.edu/article/big-data-analytics-and-the-path-from-insights-to-value/).

[2]"Big Data and Business Analytics Revenues Forecast to Reach $150.8 Billion This Year, Led by Banking and Manufacturing Investments." Press release, IDC, 14 March 2017 (www.idc.com/getdoc.jsp?containerId=prUS42371417).

[3]Bell, Steve, and Karen Whitley Bell. "Big Data and Lean Thinking: Balancing Purpose, Process, and People." *Cutter IT Journal*, Vol. 29, No. 6, 2016 (http://cutter.com/article/big-data-and-lean-thinking-balancing-purpose-process-and-people-492041).

[4]Leavitt, Steve. "Five Ways You'll See Wearable Technology in Manufacturing." Exact, 2017 (http://blog.exactonline.com/five-ways-youll-see-wearable-technology-manufacturing/).

[5]Harris, Jeanne, Blake Ives, and Iris Junglas. "IT Consumerization: When Gadgets Turn into Enterprise IT Tools." *MIS Quarterly Executive*, Vol. 11, No. 3, September 2012 (https://informationstrategyrsm.files.wordpress.com/2012/09/it-consumerization-when-gadgets-turn-into-enterprise-it-tools.pdf).

[6]Baskerville, Richard. "Individual Information Systems as a Research Arena." *European Journal of Information Systems*, Vol. 20, No. 3, May 2011 (https://link.springer.com/article/10.1057/ejis.2011.8).

[7]Baskerville (see 6).

[8]Mazzei, Christopher. "Human-Centered Analytics Improving Healthcare." EY (http://www.ey.com/gl/en/industries/health/ey-health-reimagined-human-centered-analytics-improving-healthcare).

[9]Huang, Dandan, et al. "Personal Visualization and Personal Visual Analytics." *IEEE Transactions on Visualization and Computer Graphics*, Vol. 21, No. 3, March 2015 (http://ieeexplore.ieee.org/document/6908006/).

[10]Piwek, Lukasz, et al. "The Rise of Consumer Health Wearables: Promises and Barriers." *PLOS Medicine*, Vol. 13, No. 2, 2 February 2016 (http://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1001953).

©2017 Cutter Information LLC

[11]Canhoto, Ana Isabel, and Sabrina Arp. "Exploring the Factors That Support Adoption and Sustained Use of Health and Fitness Wearables." *Journal of Marketing Management*, Vol. 33, No. 1-2, 26 October 2016 (http://www.tandfonline.com/doi/full/10.1080/0267257X.2016.1234505).

[12]Piwek et al. (see 10).

[13]LaValle et al. (see 1).

[14]Huang et al. (see 9).

[15]Davenport, Thomas H. "What Businesses Can Learn from Sports Analytics." *MIT Sloan Management Review*, Summer 2014 (http://sloanreview.mit.edu/article/what-businesses-can-learn-from-sports-analytics/).

[16]Davenport (see 15).

[17]Davenport (see 15).

[18]Harris et al. (see 5).

[19]Davenport (see 15).

[20]Gleasure, Rob, and Jeremy Hayes. "Breaking Waves: Wearables and the Future of Digitization." *Cutter IT Journal*, Vol. 28, No. 11/12, 2015 (http://cutter.com/article/breaking-waves-wearables-and-future-digitization-489161).

[21]Davenport, Thomas H. "Big Data: Personal Analytics Going Beyond Sports into Realms of Wealth & Life Satisfaction." *The Economic Times*, 14 May 2014 (http://economictimes.indiatimes.com/magazines/corporate-dossier/big-data-personal-analytics-going-beyond-sports-into-realms-of-wealth-life-satisfaction/articleshow/31942693.cms).

Trevor Clohessy is a postdoctoral digital transformation researcher and lecturer at the National University of Ireland, Galway, Ireland. His research interests are digital transformation, cloud technologies, organizational ambidexterity, blockchain, and business analytics. Dr. Clohessy holds a PhD degree that focused on the impact of cloud-based digital transformation on IT service providers. In conjunction with organizing both national and international academic and practitioner workshops and panels, he is an undergraduate awards computer science judge, an editorial advisory member of both the Irish Business Journal *and IGI's* Handbook of Research on Architectural Trends in Service-Driven Computing*, and a director with Youth Work Ireland. Dr. Clohessy has also founded an award-nominated technology ezine resource called NoiseyGen.XYZ and an undergraduate research e-journal called* Novo Verse*. He can be reached at trevor.clohessy@nuigalway.ie.*

Tom Acton is Head of the School of Business & Economics and a lecturer in business information systems and digital transformation at National University of Ireland, Galway, Ireland. His research interests are cloud computing, decision support systems, business analytics, and mobility. He holds a PhD degree focused on decision support for small-screen information systems. Dr. Acton has a number of journal publications, book chapters, and conference papers. Recently he served as Vice Dean for Teaching & Learning, Associate Head of Teaching & Learning for the School of Business & Economics, and Head of the Business Information Systems discipline. Dr. Acton has also served as Associate Editor of a number of journals, including European Journal of Information Systems *and* Journal of Theoretical and Applied E-Commerce Research*. He can be reached at thomas.acton@nuigalway.ie.*

HERE COMES PRO&GRESS

Opportunities and Challenges for IIoT in Oil and Gas

by Claude Baudoin

The oil and gas (O&G) industry, in particular its so-called upstream segment, which includes the exploration and production of hydrocarbons (see Figure 1), seems ripe for the application of Industrial Internet of Things (IIoT) approaches. Yet the data acquisition and control processes used in the industry are still often in a "pre-IoT stage" or not automated at all, for reasons I will discuss in this article. As much as we might conclude that IIoT deployments are an obvious and urgent need in O&G, we also need to remain aware of the specific challenges, including connectivity and security, that are perhaps even more daunting in this industry than in others.

Obvious Opportunities

When we consider the size of the O&G industry, which extracts almost US $2 trillion worth of oil from the earth each year (even at the current relatively low price of $45 a barrel[1]) and produces about twice that amount in refined products, it seems obvious that any process improvements that might reduce costs or help find more oil should be eagerly embraced.[2]

Many of the applications that have shown successful results in other industries directly translate to the needs of the O&G industry. For example, the program of the 2016 *IoT for Utilities* conference notes that utilities are utilizing IoT to:

- Prevent outages and failures
- Improve energy efficiency
- Improve operational efficiency
- Improve maintenance strategies and overall asset health
- Improve the user experience

Arguably, the O&G industry shares all these goals except the last one, given that most of it does not deliver its product directly to consumers. Even so, we can imagine a day when, as we stop at a gas station, our car will tell the pump what grade of fuel is needed, how much is left in the tank, and what additives should be mixed with the fuel to improve the engine's performance.

Looking at both the demand side (what the industry needs to improve its operations, increase safety, lower costs, or find more oil) and the supply side (what techniques have proved successful in other industries

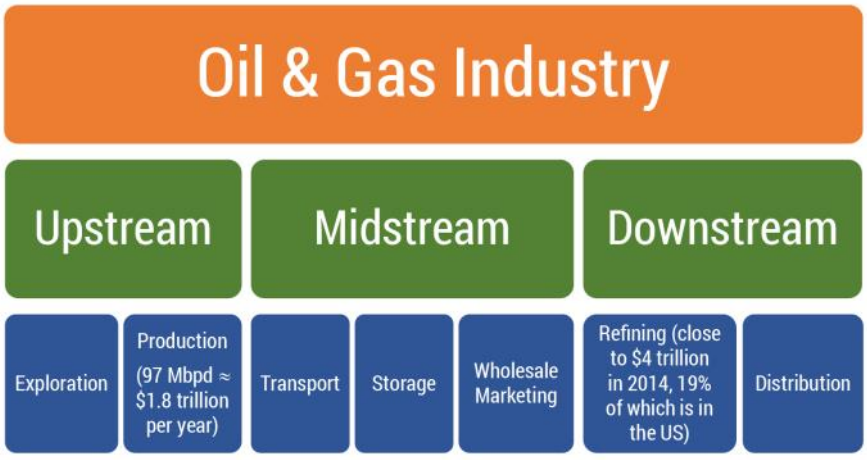


Figure 1 — Segmentation of the O&G industry.

©2017 Cutter Information LLC

and are supported by an ecosystem of technology and service suppliers), we can list at least the following potential applications of IoT:

- Conducting predictive maintenance based on condition monitoring
- Managing the performance of rotating equipment (engines, pumps, drills)
- Optimizing the replacement of expensive components (drill bits, batteries, etc.)
- Tracking expensive assets (logging tools, trucks, skids, etc.)
- Surveilling unmanned production platforms
- Ensuring early detection of leaks
- Monitoring pipelines (both for mechanical condition and physical security)
- Implementing machine-to-machine communication for greater automation and safety
- Tracking personnel to improve safety
- Decreasing human intervention (resulting in cost reductions, reduced safety risks, reduced operator errors, faster reaction to changes, and more)

In the next section, we will examine some of these scenarios in more detail.

Specific Use Cases

It is now possible to search on the Web for "IoT use cases in [industrial sector __]" and find links to hundreds of case studies and white papers. Of course, these should sometimes be taken with a grain of salt, as:

- It is easy to rename an existing data acquisition process "IoT" when in fact it does not meet the criteria required to merit this appellation. In particular, traditional closed-loop SCADA systems that do not include an analytics component or integration with enterprise systems or across locations should not be called examples of IIoT.
- Many of these case studies and white papers are published by suppliers, with all the biases this may imply.

In general, however, published case studies (especially when an end-user company is named) present some good evidence of an area in which the IIoT shows solid potential. Consider the following examples:

Worker Safety

Marathon Petroleum Corp., an Ohio-based refining and distribution company with approximately $65 billion in annual revenue, collaborated with Accenture to develop an IoT-based system to improve worker safety. The project is summarized in a case study poster from the Industrial Internet Consortium.[3] Using a "smart helmet" with a few embedded sensors, the system tracks the locations of employees, alerts them to excessive gas levels, and is able to report an alarm in the absence of movement for a certain amount of time, potentially indicating an "employee down" situation.

> *We can imagine a day when, as we stop at a gas station, our car will tell the pump what grade of fuel is needed, how much is left in the tank, and what additives should be mixed with the fuel to improve the engine's performance.*

Pipeline Surveillance

In the Niger Delta, where Shell Oil operates, the safety of oil pipelines is a key concern — in part because of oil theft. This is one of the situations, common in the oil industry, in which traditional solutions may be inoperative due to the lack of cellular or Wi-Fi connectivity. Shell implemented pipeline surveillance and wellhead monitoring using wireless endpoint devices from the Croatian company Končar Inem (to measure pressure, temperature, and flow) and a long-range, low-power connectivity capability called RPMA (random phase multiple access) supplied by San Diego–based Ingenu.[4]

Pump Monitoring

In wells that produce low amounts of oil, low flow rates can allow suspended solids to settle and damage the

equipment. Thus, pumps need to be cycled on and off in order to decrease the so-called lifting cost and to increase the equipment's expected life. This cycling is done through "pump-off controllers." Traditionally, inspection was done manually, with technicians literally driving from wellhead to wellhead. To minimize this time-consuming and costly activity, Midland, Texas–based equipment supplier Henry Pump and Austin-based IoT company Meshify put in place a system that uses measurements from flowmeters and tank-level monitoring sensors to monitor the equipment and optimize its operation in real time.[5]

Managing the Performance of Rotating Equipment

An oilfield is full of pumps, compressors, and motors, most of which work 24/7 and control significant parts of the exploration and production processes. Breakdowns are costly and even potentially dangerous. Doing preventive maintenance on a fixed schedule is not optimal — it may lead to replacing parts before they are worn out, or conversely, to excessive downtime that could have been avoided.

An oilfield is full of pumps, compressors, and motors, most of which work 24/7 and control significant parts of the exploration and production processes.

As in the manufacturing industry, the term "predictive maintenance" is increasingly being heard in O&G. Predictive maintenance requires monitoring various operating factors (number of rotations, vibration, temperature, flow, etc.) and using analytical techniques to improve the maintenance process. This results in both improved reliability and reduced cost — two goals that until now seemed contradictory.

More complete descriptions of this use case are contained in a short white paper and a presentation by Dave Feineman, Upstream Advisor at BP in Houston.[6]

Fluid Tank Monitoring

Oil typically comes out of the ground mixed with water and natural gas. The water, which is extracted through "separators" and stored in tanks in the oilfield, cannot be easily disposed of — it is briny and may contain various chemicals used in the production process. Instead, the oil companies pay contractors to remove the water and send it to remote treatment facilities. Traditionally, operators drive around with a tanker truck to empty the tanks on a periodic basis. They measure the amount removed and send a bill to the oil company.

There are several obvious problems with this process. A tank may fill up prematurely, requiring production to stop. Conversely, the truck operator may find only a quarter-full tank on some runs, which means that the overall operation is costlier than it should be. There can also be disputes over the amount of water the client is charged for.

Using sensors that monitor fluid levels and transmit the information through a long-range wireless network, it is possible to create dynamic daily truck routes that skip locations that do not require emptying and to make the calculation of the invoice automatic and more traceable. A company called Amalto has deployed a solution called Ondiflo to provide this exact capability.[7]

Gas Pipeline Tunnel Monitoring

A Singapore-based engineering firm needed to reduce the risks related to overheating in tunnels containing gas pipelines. San Diego–based Moxa Software provided a monitoring system that includes sensors, daisy-chained logic boards, and efficient and low-cost Ethernet wiring.[8]

And the List Goes On ...

From the few industry-specific case studies available just three years ago, we have seen such an interest in IoT in the O&G domain that dozens of examples can be readily found by your favorite search engine. Note, however, that the word "interest" is very different from the word "commitment."

©2017 Cutter Information LLC

Obstacles to Adoption

Clearly, many of the methods used in manufacturing to manage tools, rotating equipment, and so on, can translate directly to the equipment present on an oil rig or offshore platform. Similarly, some of the techniques used by water utilities to manage usage and detect leaks can apply to pipeline monitoring. So why is the industry still considered a laggard in IoT adoption?

Economics

The obvious issue since late 2014 has been that implementing IoT systems in O&G requires new investments, at a time when the industry is hurting badly from the decline in crude prices. The impact of the oil price (barely edging back up to $50 a barrel at the time of this writing, less than half of its 2013-2014 peaks) is actually twofold. First, there is obviously less money around to fund innovation, and second, the headcount cuts leave the remaining people so busy "keeping the lights on" that even if they had the money, they would be hard-pressed to find the time to work on new projects.

At the same time, the O&G industry's deep crisis is creating an opportunity and even an urgency to add the Industrial Internet to the range of "intelligent energy" solutions deployed by the industry, for two reasons:

1. The infrastructure has been aging without much replacement or modernization work since the crisis started, and a new wave of necessary investments is being predicted for when oil prices recover. Instead of replacing equipment and facilities with the same technology, there will be an opportunity to embed more sensors, actuators, control systems, and analytics in new equipment to make it more efficient and reduce its maintenance costs.

2. Some of the experienced personnel who were laid off in successive waves since 2015 will not be available for rehire in 2017 or beyond. Some have now retired, while others have found jobs in other industries and will not want to return even if the job opportunities reappear. The O&G industry will have to complement its remaining personnel with more junior recruits, whose lesser knowledge and experience will need to be supplemented by increased automation.

Fragmented Technology Approaches

Past approaches to automation have been fragmented. We in the O&G industry solved isolated problems with isolated systems. The closed loop of a SCADA system may have included a few sensors, a PLC, and perhaps a connected PC that allowed the display of certain charts, but there was no integration into a complete architecture, and therefore little integration and interoperability with the rest of the systems that control other aspects of a rig, platform, or oilfield. As a result, the "glue" between the systems is all too often a human who needs to interpret the information coming from one system and enter a parameter into another system — a handoff that is prone to delays and errors.

In addition, the various systems tend to speak different languages, even at the basic level of communication protocols. There are 11 standards-developing organizations that are part of the O&G Standards Leadership Council (SLC):

- Energistics
- MIMOSA (Machinery Information Management Open Systems Alliance)
- OGC (Open Geospatial Consortium)
- OMG (Object Management Group)
- OPC Foundation
- PCA (POSC Caesar Association)
- PIDX International (Petroleum Industry Data eXchange)
- PODS (Pipeline Open Data Standard)
- PPDM (Professional Petroleum Data Management)
- SEG (Society of Exploration Geophysicists)
- USPI-NL (Stichting Uitgebreid Samenwerkingsverband Procesindustrie-Nederland)

While the mission of this body is to provide visibility and coordination between its members, it has little power to influence their course of action.

Even when combined together, the isolated solutions that have been developed to solve specific, narrowly

defined problems do not amount to a strategy. We need a consistent approach and structure in order to be able to integrate an entire system that spans the range of capabilities from sensing and control to computer-aided decision making. The Industrial Internet Consortium has defined for this purpose an Industrial Internet Reference Architecture (IIRA), first published in July 2015.[9] The main characteristics of the IIRA are that it:

- Covers the end-to-end scope of IIoT systems
- Enumerates the key components of an IIoT system and the interfaces between them
- Establishes functional requirements for each component
- Lists the technologies that already exist and the additional ones that need to be developed
- Is based on core use cases, not just on intellectual speculations
- Is being exercised (and thus is receiving feedback from) the testbeds developed under the aegis of the IIC — including, in 2017, at least one integration testbed specific to O&G

The evolution from localized and relatively simple SCADA systems to the IIoT presents a serious organizational challenge.

Connectivity

A specific challenge for the O&G industry is connectivity. On land, rigs and production facilities are often located in remote areas where even that most basic fabric of our Internet age — cellular telephone coverage — is unavailable or spotty. On offshore platforms, remote connectivity usually requires satellite communications equipment, which is expensive and offers relatively low bandwidth and high latencies.

The situation is changing thanks to technological advances as well as the economics of deploying existing solutions to high-density areas. For example, fiber-optic cables can be run to certain locations from which traffic can be relayed through microwave links or WiMax, and cellular towers have been installed offshore in the Gulf of Mexico.

Some new technologies are particularly well suited to these difficult environments, in particular LoWPAN (Low-Power Wireless Personal Area Network). Sigfox and the LoRa Alliance are the two main organizations that provide such solutions, and they are actively wooing the O&G industry.[10]

The IT/OT Chasm

The evolution from localized and relatively simple SCADA systems to the IIoT presents a serious organizational challenge. The former used to be acquired and managed by the operations function — hence the abbreviation "OT" for "operational technology." On the other hand, the IT group was in charge of enterprise systems and common services such as enterprise connectivity, email, the help desk, and so forth. OT did not want IT to meddle in its affairs and was generally able, with the help of the SCADA system vendors, to manage the deployment and use of SCADA systems without IT help. As long as those systems were not connected to the enterprise network, IT couldn't care less.

This siloed model totally breaks down with the evolution from SCADA to IIoT. IIoT systems *are* IT systems — they still include special-purpose components, but they also include servers that run mainstream operating systems and databases, they connect to the rest of the enterprise, and, more menacingly, they use public networks to communicate back to the "mother ship" (literally or figuratively).

As a result, there is now a significant tension between IT and OT. OT may be overwhelmed by the management of systems that have become more complex than they were used to, but they still fear the meddling of IT ("Hello, we're from corporate IT, and we're here to help you"). IT very much wants to make sure that IIoT systems are secure and are not going to cause support headaches, but it also has little understanding of what those systems do.

The Society of Petroleum Engineers (SPE) Digital Energy Technical Section (DETS) published, just before the *Intelligent Energy 2016* conference, a fairly short paper that "discusses the need and presents means to align business strategy, process capabilities, technical disciplines, work processes, and organizational models to achieve value in convergence."[11] Perhaps because the authors realized that their audience was ill-prepared to seriously address this issue, the paper is mostly a

©2017 Cutter Information LLC

tutorial followed by a set of wishes for convergence, cast into the general framework of change management. This is clearly only a preliminary awareness step on the way to actual converged ownership and management of IIoT systems.

Security

It is hardly necessary to explain or justify the statement that security is a concern when we think of applying IoT technology in O&G. Clearly, the risks range from industrial spying to disrupting operations (resulting in economic damage) and triggering accidents (resulting in loss of life, damage to reputation, environmental accidents, and/or loss of ability to operate).

The owners of IIoT systems are generally extremely ill-educated about information and systems security. They do not have the first idea of what questions they need to ask of their suppliers and integrators, or what are appropriate defenses against hacking, phishing, denial-of-service attacks, and the like — all of which are made more likely in O&G by the broad geographical footprint of the industry. After all, how do you protect yourself from hackers when you operate in certain countries (which shall remain nameless here) that essentially operate government-sanctioned information espionage programs?

A concrete example of how security vulnerabilities can escalate into physical disasters is provided by the well-known explosion of the Baku-Tbilisi-Ceyhan (BTC) pipeline in 2008. According to the Wikipedia article on this accident:

> On 5 August 2008, a major explosion and fire in Refahiye (eastern Turkey Erzincan Province) closed the pipeline. The Kurdistan Workers Party (PKK) claimed responsibility. The pipeline was restarted on 25 August 2008. There is circumstantial evidence that it was a sophisticated cyberattack on line control and safety systems that led to increased pressure and explosion. The attack might have been related to Russo-Georgian War that started two days later.[12]

With 20 days of lost deliveries, the potential economic damage if the pipeline had been running at full capacity could have reached $2.5 billion.[13]

Although accounts differ somewhat, it seems that the BTC attack was two-pronged, electronic as well as physical. The attackers penetrated the monitoring and control system for the pipeline through the network of security cameras placed along the pipeline — *cameras that in effect were nodes in an IP network but were installed without changing their default factory passwords.* Having penetrated the network, they disabled the alarm system that would detect a physical malfunction and would allow operators to take quick action to remediate problems. Finally, although this is not mentioned in all sources, it has been reported that an explosives truck was detonated next to the pipeline, causing the explosion and fire, which were not immediately detected at the control center because of the effects of the cyber attack.

While this happened in 2008, well before we started seriously talking about the Internet of Things, the same form of attack is quite possible today in many systems. In fact, the attack against the electric distribution system in Ukraine in December 2015 has some of the same characteristics, apart from the physical attack. One of the forms of attack used in the Ukraine case was to insert malware into networking equipment as much as six months before the actual event, leaving it in a dormant state until it was called into action. And again, the entry point was systems whose passwords had been left unchanged from their well-known default value.

These attacks were facilitated by very basic vulnerabilities, and they could have easily been prevented or made considerably less likely by observing trivially simple steps, such as changing passwords. In fact, a rigorous threat assessment of the BTC pipeline system was only conducted after the fact.[14]

Data Residency

The issue of data residency only started to be considered as a separate challenge of distributed systems and information in the last few years. OMG started discussing it in early 2015 and published a comprehensive paper on this subject jointly with the Cloud Standards Customer Council (CSCC) in May 2017.[15]

The working group that wrote the paper defined data residency as:

> the set of issues and practices related to the location of data and metadata, the movement of (meta)data across geographies and jurisdictions, and the protection of that (meta)data against unintended access and other location-related risks.

The legal, regulatory, and financial risks related to the location of data are common to all international companies, but the issue is exacerbated by certain specific factors in O&G, which would have an impact even outside the realm of the IIoT. For example, a company that is contracted to collect and process geophysical measurements may wish to perform that process in a central facility staffed with international experts and equipped with large computer clusters or supercomputers. Remote monitoring of operations has also become a source of higher efficiency and safety, allowing fewer personnel to be posted in potentially risky areas. However, attempts to achieve such efficiencies run into the issue that the data that needs to be processed is considered a national asset — often called "sovereign data" by many countries. Examples include Russia and Venezuela, where subsurface data about oil reserves is considered a state secret. Therefore, the transmission of such data outside of the country may be prohibited or severely restricted.

It is a common refrain, but it bears repeating: do not deploy IIoT technology (or any technology for that matter) just because it is "cool," because your boss read about it in the airline magazine, or because your competitors are doing it.

What's Next?

The Industrial Internet presents huge opportunities for the O&G industry, especially considering the greater level of automation required to ramp up exploration, and maintain or increase production, whenever the current depression ends. This set of technologies also presents an unprecedented level of complexity, which requires a systematic and integrated approach rather than piecemeal solutions. Then there's the fact that IoT systems in general, including IIoT systems for oil and gas, present security challenges and a tempting target to attackers.

To realize the benefits and overcome the challenges, enterprises should use the following approaches in combination:

- **Strategy.** Understand that the adoption of the Industrial Internet is a strategy that needs to be driven from the top of the organization, with a clear vision of the desired business outcomes, not a collection of tactics pursued individually by engineers, operations managers, and the middle management of various product lines.
- **IT/OT collaboration.** If the CIO is unable to support oilfield operations needs with the required agility, or is seen as the person who rejects or delays everything because of slow and conservative processes, or even if the disconnect between operations and IT is simply due to ignorance or "territory ownership" concerns, this needs to be fixed. Creating a separate OT department that doesn't talk to IT is not the right solution.
- **Business cases.** It is a common refrain, but it bears repeating: do not deploy IIoT technology (or any technology for that matter) just because it is "cool," because your boss read about it in the airline magazine on his way back to Houston, or because your competitors are doing it. Build the use cases and transform them into business cases that are aligned with the overall strategy. For example, if cost reduction is a key desired outcome, show how much it is worth to delay maintenance on an electrical submersible pump by one day 20% of the time, thanks to a predictive maintenance algorithm that uses sensor data to monitor the equipment's condition.
- **Readiness assessment.** Are you ready? Assess your readiness and maturity to address the challenges posed by the introduction of IIoT by asking the following questions:
    - Do you have an adequate governance structure, with the business, operations, and IT people willing to sit down together and find a compromise between rigor and agility?
    - Are you good at planning and executing projects on time and on budget?
    - Do you have a good partnership model for working with suppliers, partners, and consortia?
    - Have you outsourced so much of your IT that you no longer have the internal skills to manage the new architecture, sourcing, and security challenges that your IIoT strategy will pose?

©2017 Cutter Information LLC

- **Security, security, security.** Do not assume that your IIoT infrastructure will not be attacked or that it is not vulnerable. Assume that it *will* be attacked, especially since you probably work in many countries, some of which harbor elements hostile to you. Look at all the ways in which every component of the system could be misused, then protect against it. In particular, look into the identity management and provisioning of devices, the mutual authentication and access control of both devices and servers, and the encryption of the data so that it cannot be used if intercepted. Finally, when a system is deployed, monitor it constantly to detect any anomalies.

These measures may not automatically confer invincibility and the total assurance of success, but they are a significant set of first steps toward realizing the potential of the Internet of Things in the O&G industry.

Endnotes

[1]A barrel of oil is 42 US gallons, or about 159 liters. Figure 1 and this discussion focus on liquid oil, as natural gas production represents a smaller amount of industry revenues (roughly $350 billion a year) at current volumes and prices.

[2]Slaughter, Andrew, Gregory Bean, and Anshu Mittal. "Connected Barrels: Transforming Oil and Gas Strategies with the Internet of Things." Deloitte University Press, 14 August 2015 (http://dupress.com/articles/internet-of-things-iot-in-oil-and-gas-industry/).

[3]"The Industrial Internet in Action — Marathon Petroleum Company." Industrial Internet Consortium (www.iiconsortium.org/images/case-study-posters/Accenture_Marathon-Petroleum_Poster.jpg).

[4]"Ingenu and Končar Partner with Shell to Deliver Digital Oilfield Connectivity to Nigeria Pipeline Facility." Press release, Ingenu, 30 March 2016 (www.ingenu.com/2016/03/ingenu-and-koncar-partner-with-shell-to-deliver-digital-oilfield-connectivity-to-nigeria-pipeline-facility/).

[5]"Henry Pump Case Study." Meshify, 2017 (https://meshify.com/customers/henry-pump-case-study/).

[6]Feineman, David. "Managing Performance of Rotating Equipment." Information Days on Standards for Process & Information Integration, 24 February 2014 (www.energistics.org/Assets/20140225feineman.pdf).

[7]"Amalto Introduces New Integration Solution — Ondiflo." Amalto, 23 February 2017 (www.amalto.com/news/amalto-introduces-new-integration-solution-ondiflo).

[8]"Remote Gas Pipeline Tunnel Temperature Monitoring System." Moxa, 22 December 2009 (www.moxa.com/applications/Remote_Gas_Pipeline_Tunnel_Temperature_Monitoring_System.htm).

[9]"Industrial Internet Reference Architecture V 1.8." Industrial Internet Consortium, July 2015 (www.iiconsortium.org/IIRA.htm).

[10]"SigFox vs. LoRa: A Comparison Between Technologies and Business Models." LinkLabs, 13 January 2016 (www.link-labs.com/blog/sigfox-vs-lora).

[11]Kamal, S.Z., et al. "IT and OT Convergence — Opportunities and Challenges." Society of Petroleum Engineers, 2016 (www.onepetro.org/conference-paper/SPE-181087-MS).

[12]"Baku-Tbilisi-Ceyhan Pipeline." Wikipedia (https://en.wikipedia.org/wiki/Baku%E2%80%93Tbilisi%E2%80%93Ceyhan_pipeline).

[13]"Baku-Tbilisi-Ceyhan Pipeline" (see 12).

[14]Steinhäusler, Friedrich, et al. "Applying Advanced Technology for Threat Assessment: A Case Study of the BTC Pipeline." *Journal of Energy Security*, August 2009 (www.ensec.org/index.php?view=category&id=98%3Aissuecontent0809).

[15]Baudoin, Claude (ed.). "Data Residency Challenges and Opportunities for Standardization." Object Management Group, 22 March 2017 (www.omg.org/cgi-bin/doc?mars/17-03-22.pdf).

Claude Baudoin is a Senior Consultant with Cutter Consortium's Business & Enterprise Architecture and Data Analytics & Digital Technologies practices. He has been owner and Principal Consultant of cébé IT and Knowledge Management, a boutique consulting practice, since 2009. Prior to that, Mr. Baudoin spent 35 years in IT and software management roles in industry, including 26 years at Schlumberger, the global oilfield services company, in France and the US. Since 2015, he has served as an energy domain advisor to the Object Management Group and the Industrial Internet Consortium and has sat on the Steering Committee of the Cloud Standards Customer Council.

Mr. Baudoin's undergraduate engineering degree is from École Polytechnique in Paris, and he holds an MS in computer science from Stanford University. He has published two books on software engineering, Méthodes de Programmation *and* Realizing the Object-Oriented Lifecycle, *and numerous papers and conference presentations, including a number of Cutter reports, advisors, and* Cutter IT Journal *articles. Mr. Baudoin holds two patents related to IT infrastructure and security. He can be reached at cbaudoin@cutter.com.*

PLOTTING A NEW COURSE

From "Fast-Bleeding" to Market-Leading:
A Telecom's Digital Transformation Journey

by Evangelos Vayias and Ioannis Konstantinidis

Transformation is a continuous process. During the last six years, OTE Group has been transformed from a "fast-bleeding," bureaucratic telco into a modern, competitive, high-performance service company and the leader in its core markets. This turnaround was achieved by implementing an encompassing transformation program across all business functions supported by a vision, strategy, plan, and cross-functional collaboration, while at the same time instilling a customer-oriented and performance-based culture.

The time has now come for the next step: digital transformation. At the dawn of the so-called Fourth Industrial Revolution, which is changing customers and enterprises at unprecedented speed, no sector or organization can hold out without daring to change at a similar pace.

In this article, we present the approach and steps taken to set a roadmap for the journey of the Hellenic Telecommunications Organization (OTE), the incumbent telecom operator in Greece, toward digital transformation. We discuss how we have structured a transformation program to fulfill this transition to the digital age, our achievements so far, the challenges we face, and upcoming plans.

Understanding the Digital Age

The starting point for establishing a roadmap for digital transformation is to understand the nature of the need urging us toward this transition. We are entering a new technological era in which massive advances in various technology fields are taking place simultaneously, in a way that one multiplies the other and the overall pace accelerates. This "exponential acceleration" of technology advances drastically shortens the lifecycle and timeframe — from the inception to the application and large-scale deployment of technological developments. To illustrate this, consider that from laying the foundations of computing in the 1940s to the massive adoption of personal computers, the timeframe was around 50 years; large-scale adoption of mobile telephony took place in approximately 20 years; while smartphones were invented just over 10 years ago and now can be found in over 40% of the world's population.[1] This lifecycle is expected to shorten further, as the adoption of each new technological concept benefits from the deployment of previous ones. For example, based on the proliferation of smartphones, social networks are now managing to reach hundreds of millions of users in fewer than five years.

Each transition from one technological era to the next is characterized by an increase in human expectations for the available technical tools and capabilities. Hence, in the first industrial era, machines were expected to facilitate laborious tasks. In the second industrial era, mass production and electricity were considered the norm. And in the information age, repetitive computation tasks were expected to be handled by computers, and long-distance communication became a commodity.

In the digital age, digital technologies are raising the bar of expectations once more by commoditizing capabilities such as:

- Being able to do everything with a personal mobile device
- Completing transactions from anywhere, in a simple way, saving time and effort
- Having products and services that are adaptable to personal needs
- Having instant access to any information worldwide and being able to share and interact not just one-to-one, but across online social communities organized by the users themselves

Such expectations define a paradigm shift, which is the essence of the digital age. As with any technological transition, people will identify whether a product, service, or corporation has made the shift to the new age based on its ability to demonstrate that it addresses these newly emerging expectations.

©2017 Cutter Information LLC

In our view, digital transformation is driven by the urgency of a company to be relevant in the digital age. At OTE, we have set the goal to be recognized as a leading digital age corporation and to be perceived as such in the minds of all our primary audiences: customers, employees, and partners. Therefore, the key to our digital transformation is to leverage digital technologies to upgrade their experience of interactions with the enterprise to a level that satisfies their expectations as citizens of the digital era.

This requires the adoption of a "digital way" of conducting enterprise operations and interacting with our audiences. The digital way is adapted and relevant to users' needs and context and enables things to happen in a simpler, faster, and more efficient fashion, thus saving them time and effort.

The crux of the transition to the digital age is focusing on people and structuring a transformation program that leverages digital capabilities to offer a simple and intuitive experience to the main audiences, simplifying and automating processes and ways of working and integrating systems and tools (see Figure 1).

Structuring a Digital Transformation Program

Our transition to the digital age is based on two pillars:

1. **Digital company.** We are becoming a Lean-Agile enterprise with simple, flexible structures and processes and creating a digital age workplace, which will facilitate collaboration and foster creativity and innovation.
2. **Digital customer.** We are invigorating our relationship with customers, raising their quality of experience by leveraging digital technologies and offering an ecosystem of digital products and solutions to address their expectations in the digital age.

> *The key to our digital transformation is to leverage digital technologies to upgrade our primary audiences' experience of interactions with the enterprise to a level that satisfies their expectations as citizens of the digital era.*

The first step in our approach has been to illustrate the big picture of the end state. What are the main elements that our enterprise and our relationship to our audiences should possess in the digital age? This target picture (see Figure 2) has been depicted:

- Conceptually, as a narrative stating the core elements and concepts that characterize the experience of our key audiences
- Technologically, illustrating the capabilities that we need to build to achieve it
- Tangibly, by defining quantitative targets and metrics that we will use to measure our progress and assess how close we are getting to the end state

The approach for designing our digital transformation program is based on user journeys — a series of user experiences that, when put together, visualize the target picture end to end, according to user demands.

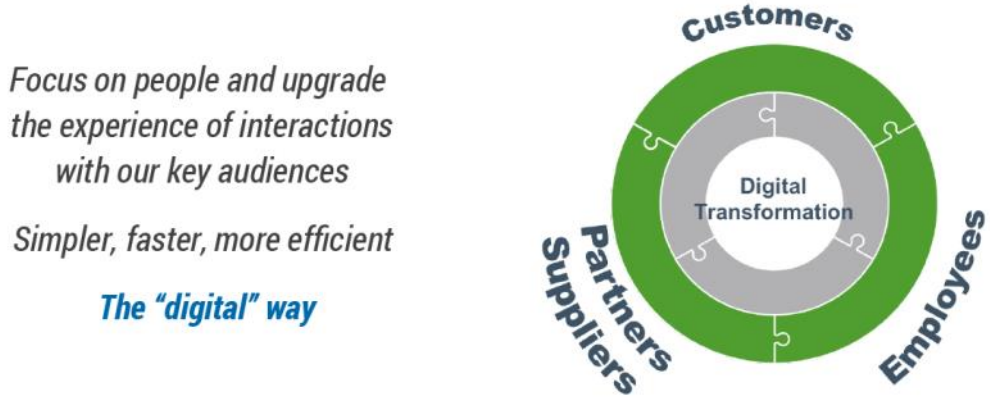


Figure 1 — What digital transformation is about.

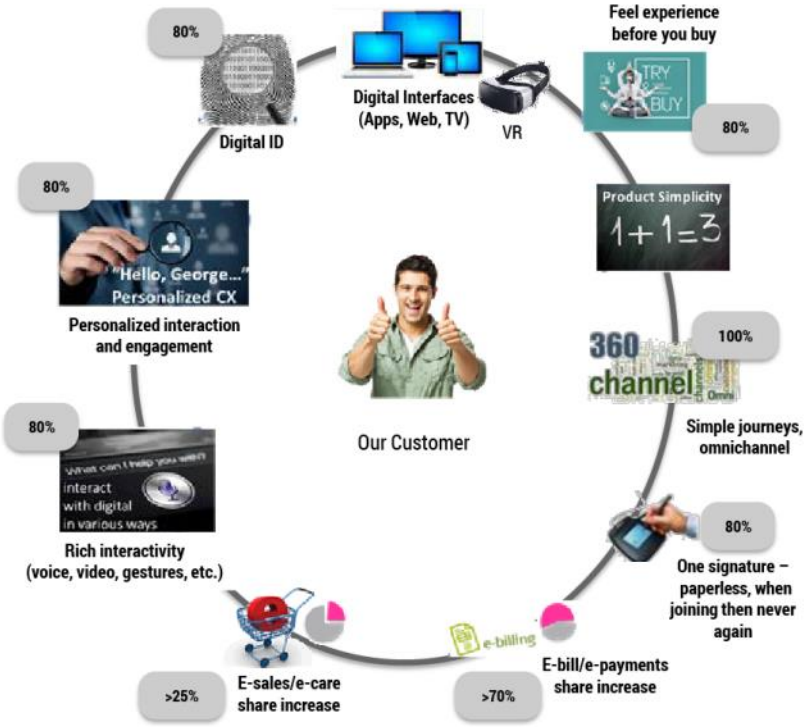
Customer Digital Experience 2021 – Target Picture

Transforming customer experience in a digital world is about …

- **Personalized interaction and contextual engagement,** proactively addressing what the customer needs
- **Possibilities and simplicity of products**
- **Simplicity and harmony of seamless customer journeys** across digital and physical channels

With one purpose:

✓ **To truly differentiate our branded customer experience**



Our Digital Company in 2021 – Target Picture

Transforming to a digital company for employees and partners is about …

- **Digital interfaces with single sign-on** for performing business operations
- Work and collaborate **from any device and anywhere**
- **Simplification, digitization of e2e workflow journeys** without "digital gaps"
- **Business transactions with partners made digital,** with e2e visibility and traceability

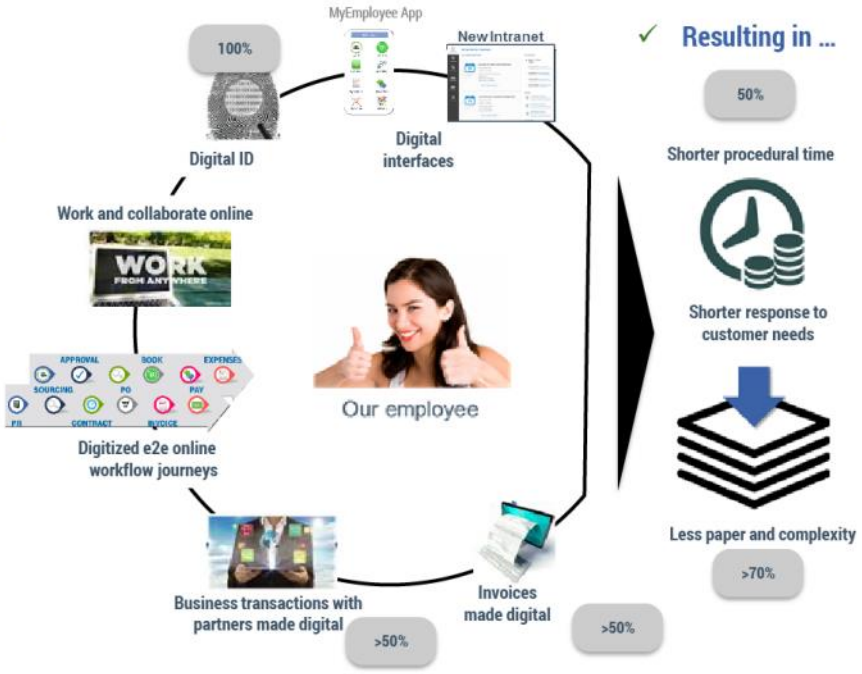


Figure 2 — Target picture for the digital customer and digital company depicted as: a conceptual narrative, a series of technical building blocks, and quantitative targets.

©2017 Cutter Information LLC

Customer, employee, and supplier/partner journeys have been our main design tool in the program.

We have structured a holistic digital transformation program to achieve this target experience, in two planes:

1. **Design plane,** where the user experience is illustrated as journeys across company touchpoints. This is a story from the user's perspective — relating the experience when he buys, pays, gets service from us, and so on — in two versions: "as-is" now and as he would want it "to-be." This gives us the expectations (wants) from the user viewpoint, which can serve to identify what digital capabilities are needed in order to satisfy them.

2. **Enabler plane,** which identifies the digital building blocks and capabilities required in order to enable the desired user experience.

We illustrate the structure of our program in Figure 3. In the design plane, there are some key "digital journey" workstreams that address customer, employee, and supplier/partner journeys with the aim of designing and building the target user experience; these are the projects that address the conceptual target picture. To support them, building blocks and technical capabilities are needed, which are created by projects in the "digital enabler" workstreams.

We do not expect the target picture of our digital transformation to stay static, but rather to constantly evolve as technological advances influence user expectations. Therefore, the project portfolio in the enabler plane will be continuously redefined, updated, and refreshed based on the evolution of the target picture, which will be addressed by the digital journey workstreams in the design plane. An advantage of the described program structure is its ability to accommodate such evolution.

How the User Journey Design Approach Works

Now let's consider an example of how the journey design approach is used for visualizing the target picture end to end according to user demands and for identifying required digital capabilities and building blocks.

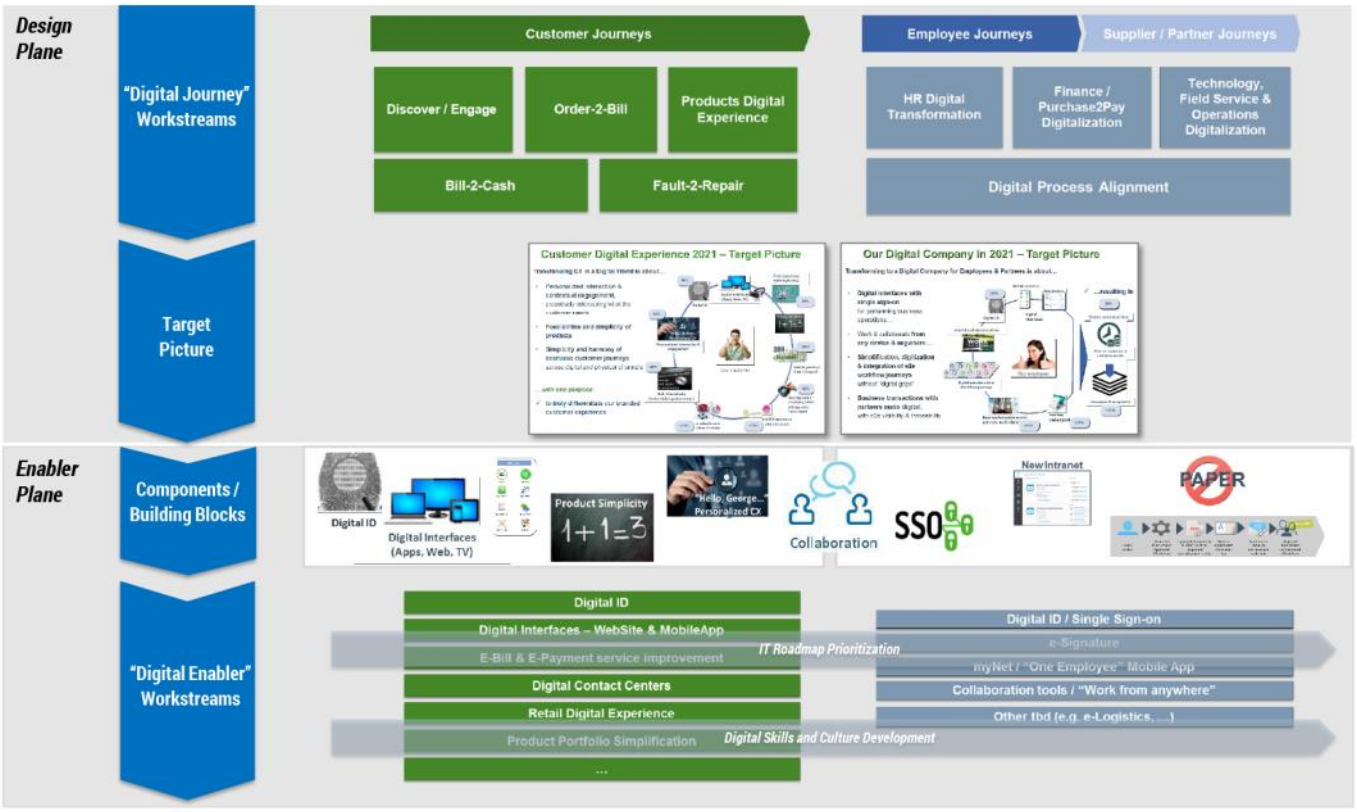


Figure 3 — Digital transformation program structure in design and enabler planes.

Suppose that Catherine, a lawyer who frequently works from home, wants to upgrade her household broadband connection. Catherine visits our website from her smartphone to browse upgrade options. Our site identifies her and, based on the geographical information of her household, suggests that ultrafast broadband is indeed available in her location. It then gives product propositions relevant to Catherine's behaviors in terms of communication service usage and entertainment options. She is interested but would like to talk to a salesperson before finalizing her decision, so the website offers her an appointment at a shop nearby with Mark, one of our sales agents.

Upon entering the shop, Catherine is identified by scanning a QR code on Mark's tablet using our customer service mobile app on her smartphone. This enables Mark to see on his tablet the product options that Catherine had browsed previously. After getting the desired clarifications, Catherine completes the order through the mobile app on her smartphone, which carries her unique customer digital ID.

From such a simple narrative, various required building blocks become apparent: a customer service mobile app and digital ID, a contextual platform offering Web propositions with behavior relevance, and a unified view and integration of the customer's interaction on information systems across sales channels (online shop, retail store, omnichannel).

This two-plane approach facilitates dealing with the moving target of digital transformation in an iterative and Agile way: as we go along, we redefine wants and redesign and complement the digital building blocks we need.

Now let's see how the approach works to address user journeys in the digital company pillar (see Figure 4). First, we identify the as-is situation from the users' viewpoint (employees, partners, or suppliers) in order to identify their main experience pain points.

For example, consider the end-to-end journey of purchasing from our partners and vendors, from the moment a purchase requisition arises to the delivery and payment. We call this the Purchase2Pay journey. These are the elements we identify from the users' viewpoint for the as-is state:

- We have a multitude of information systems and online tools, to the degree that, in most cases, completing a specific task entails the use of more than one system.
- We have to enter each of these systems individually, manually start each process step, and sometimes repeat much of the "story" — reentering information, running approval flows several times, and so on.

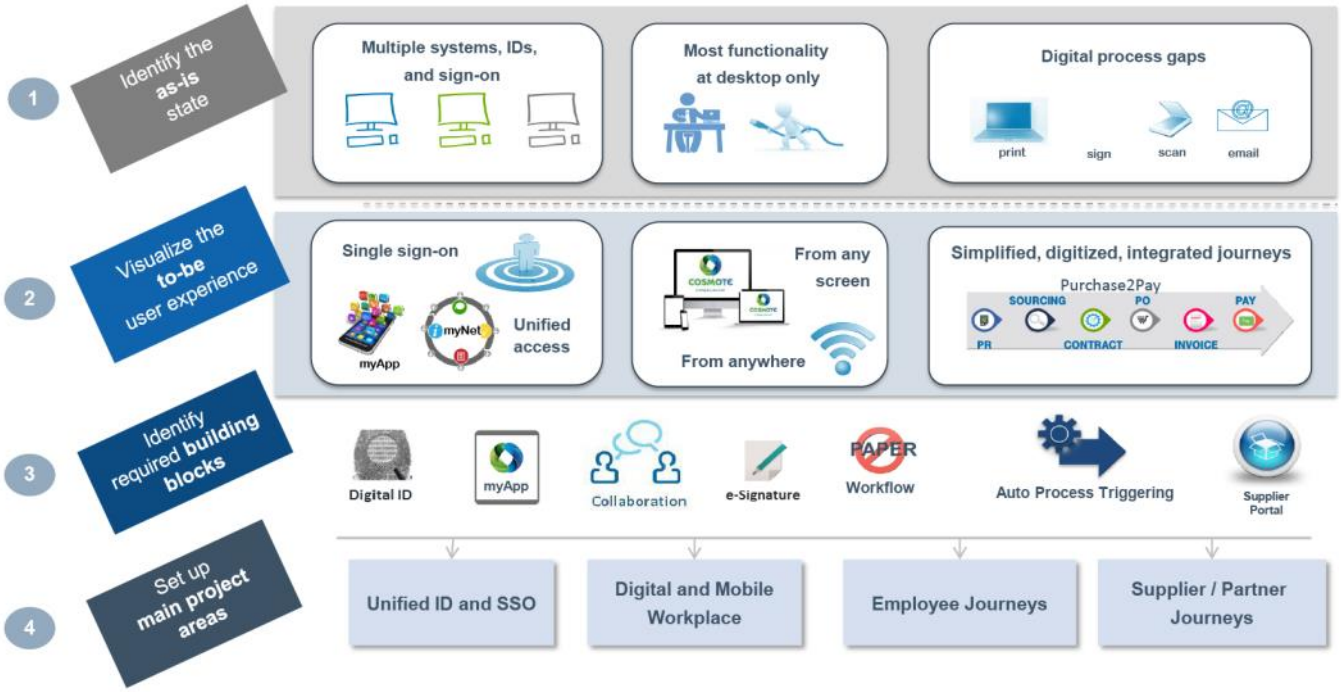


Figure 4 — Digitizing journeys in the company.

©2017 Cutter Information LLC

- Sometimes, there are "digital gaps" — breakouts from the digital process to print and sign a paper and then to scan it and send it by email.
- At the very least, it would be great to be able to do these tasks during nonproductive idle times, such as while waiting for a meeting, but this is not usually possible. Most of the functionality is available only at the desktop.

In short, this situation involves a lot of repetition and time and effort wasted on procedural, laborious, and nonproductive tasks.

We then identify what the user expectations ("wants") would be in the digitized to-be situation:

- The user could go through the workflow seamlessly, without having to identify which system is required for the next step.
- The user would be able to do this from any screen and anywhere with similar functionality.
- Process steps would be seamlessly linked across systems, without digital gaps, without story repetition, and with uniform experience.
- The task status would be available with a few clicks rather than dozens of phone calls and emails.

In order to realize this target experience, we then identify various building blocks and capabilities, such as:

- Single sign-on (SSO) through online and mobile workspace portals with a unified digital ID
- E-signature and paperless approvals
- An online portal for external partners and vendors
- The ability to link and auto-trigger subsequent process steps

In order to analyze this end-to-end journey, we have engaged all stakeholders into a cross-functional journey workstream called Purchase2pay Digitization. Stakeholders from relevant business units are collaborating in workshops with a design thinking approach to analyze use cases, determine the to-be target experience, and identify the required building blocks. Stakeholders from legal, risk and compliance, and security are also part of the team, as it is important to consider and incorporate such issues into the design right from the start.

To implement the building blocks identified by a journey workstream such as Purchase2Pay, projects are set up to deliver them. Some of the building blocks a journey workstream identifies may also be useful to another journey; for example, the e-signature and SSO capabilities identified by Purchase2Pay are useful for several other employee and partner journeys. The journey workstreams will then combine these building blocks to build the desired user experience.

We don't need to specify everything from the beginning. We can extend the journey portfolio with more detailed journeys at any time, according to any new demands.

In order to stay focused on the long-term goal, we work in Agile sprints. Rather than waiting for everything to be ready, we focus on building blocks that can be readily implemented, so we can get some quick wins and gain early feedback to adjust our course to the target picture. We then incorporate building blocks into the picture as they become available. For example, we have started with the vendor portal and e-signature to start fixing the experience, even if SSO and process step linking have not yet been delivered.

Benefits of the User Journey Approach

In our experience, the user journey design approach provides the following benefits:

- It helps to effectively and tangibly communicate the to-be vision to a variety of stakeholders, align them toward the target picture, and set the expectations properly.
- It offers the right level of analysis — not too rigorous or too detailed, but practical and simple.
- It enables an Agile design approach. We don't need to specify everything from the beginning. We can extend the journey portfolio with more detailed journeys at any time, according to any new demands. The identified building blocks can be incorporated into the target picture as they become available, in Agile sprints.

Based on the above example, we feel overall that design by end-to-end journeys is a valuable tool to address all digital transformation dimensions in a consistent way.

Current Status and Upcoming Plans

We consider our program to be a holistic 360-degree initiative. Our approach does not only address the digital experience of customers. We believe that in order to be a leading organization in the digital age, the paradigm shift must also become intrinsic to every operational aspect of the enterprise. The only way to achieve this is to adopt a similar paradigm for all business functions, outward and inward. That is why we have adopted the same approach and corresponding initiatives aimed at providing the digital experience throughout our interactions with all our external (customer, partner) and internal (employee) audiences. This is evident in the current roadmap of our digital enabler projects shown in Figure 5.

Already we have scored some key quick wins toward becoming a digital company for employees and partners:

- We have launched the main Web portals for both our employees and our vendors.
- The vast majority of internal approval workflows are now paperless and can be accessed by smartphone.
- An e-learning and micro-learning platform is available to all employees.
- Field technicians use a tablet to access their work plan and all relevant information.
- We have introduced an e-signature pilot for certain supplier contracts.

There are also several concrete initiatives on the digital company roadmap ahead of us:

- SSO will be deployed for more systems. We are working on how to provide a unified way to access both IT systems and physical spaces with the same user experience by using a mobile app with a unique employee ID.
- This mobile app (One Employee App) is also planned as the unified digital channel for employees to access useful information and complete tasks on the go.
- We will aim to link and seamlessly trigger process steps, thereby alleviating digital gaps and providing a uniform experience of online workflows.

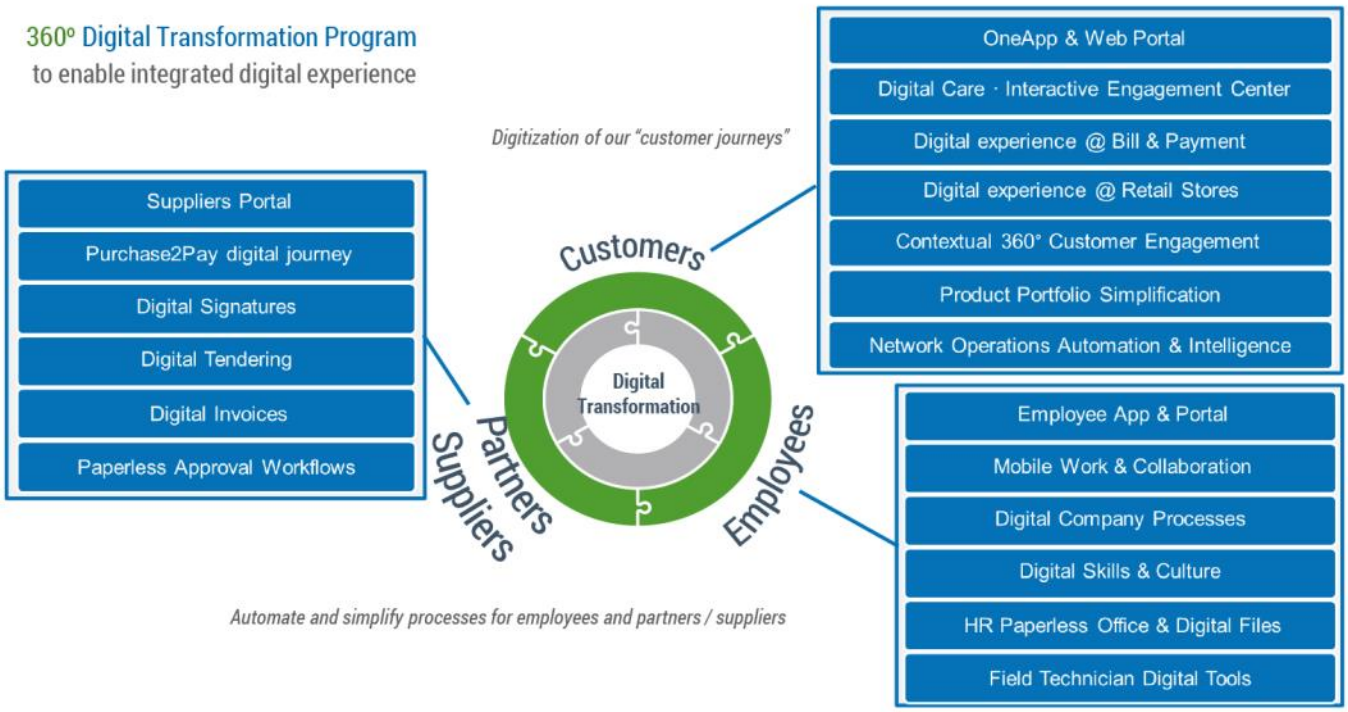


Figure 5 — Digital transformation 360-degree approach.

©2017 Cutter Information LLC

- We will work to expand e-signatures to all company internal and external documents.

With regard to the digital customer experience:

- We have launched a customer service mobile app (myCosmote) that uniquely identifies each customer, providing a unified view of all his services and products for fixed and mobile communication and entertainment. Common tasks such as viewing service usage, bills, and payment can be done through the app.
- We have upgraded our customer Web portal in terms of look and feel and ease of browsing and ordering products. The portal has been linked with the unique customer ID on the myCosmote app, enabling the customer to identify himself using the app by scanning an onscreen QR code on the portal.
- We have introduced new, automated functionalities to enhance customer experience in service fulfillment and assurance, such as e-signature for service contracts, timely information on expected time to resolve a fault, and video-based technical support (e.g., "Point your smartphone camera to your router, and we will draw on your smartphone screen what to do" — U Fix It).

We will continue to evolve our customer mobile app to an integrated digital service channel through which the customer will have a unified picture of his relationship with us and the ability to access and manage all of our apps and digital services.

We have introduced new, automated functionalities to enhance customer experience in service fulfillment and assurance, such as e-signature for service contracts, timely information on expected time to resolve a fault, and video-based technical support.

We will complete the unified 360-degree view of the customer across all sales and service channels (physical and digital) and personalize the propositions to him through a contextual marketing platform. The goal is to communicate with the customer at the right time through the appropriate channel based on his contact history and overall profile (see Figure 6).

Figure 6 — Current status and upcoming roadmap.

Challenges

The key challenges we face in this journey come from two main directions.

Aligning the Workforce to the Vision

The first one has to do with people — the natural human resistance to change. Especially in a large organization, the maturity and level of understanding for such a novel and vast undertaking vary greatly. Culture and mindset shift initiatives are needed to bring all internal stakeholders forward at the same pace. This is why we make sure we clearly communicate the vision of the digital age to our people, explaining what it means to them and to the company.

> *If we are not fast enough, what we design now may become obsolete before we get the chance to deploy it.*

Digital skills are also an issue. For this purpose, we run special programs to take advantage of our organization's "fresh" minds, our young people with growth potential. They are digital natives, and we want to infuse their outlook to the entire organization. The goal is to make everyone understand that in the digital age, we will all be constantly learning.

An Exponentially Evolving Target

The second is the fact that the digital landscape evolves exponentially. Technology lifecycles are constantly becoming shorter. If we are not fast enough, what we design now may become obsolete before we get the chance to deploy it.

To address this "evolving target" challenge, we need to work in an Agile way. We have to start by planning the big picture, set the overall direction, and start producing results to get us a step closer to the goal.

As discussed above, this is how we have started. Moreover, we expect our digital transformation to unfold as a series of sprints. We will roll out any viable implementation as fast as possible in order to achieve quick wins and get early feedback, and then adjust the course to the destination and plan the next wave of rollouts accordingly.

Conclusion

Digital transformation is a big bet and a massive undertaking for enterprises. It requires a different approach from classical technology upgrade projects, since the point here is not the technology, but the human experience from it. Making employees key stakeholders of the program and communicating clearly that digital transformation is about becoming a modern enterprise in every aspect and creating a simpler experience are essential for drawing engagement and ensuring the success of the program.

The expected benefits from this program fall into two categories. There will be material benefits such as savings in paper, printing, and postal costs, as well as a reduction in certain commissions paid to third parties, as a result of shifting various transactions (orders, invoices, payments, etc.) to online channels and becoming paperless.

The most important benefits, however, are of a qualitative nature and relate to our goal of becoming a leading digital age corporation. In this respect, we look to this program to:

- Address the expectations of our customers in the digital age: faster and better response to their needs, simple and instant access to the services they want, with minimum time and effort required from their side
- Streamline and simplify our internal operations by freeing company resources from bureaucratic and mundane tasks and facilitating productivity, creativity, innovation, and responsiveness to customer needs

Achieving these goals carries great value potential for the company by enabling it to stay at the forefront of developments in the digital era and laying the foundations for its sustainable growth.

©2017 Cutter Information LLC

Endnote

[1]Sui, Linda. "44% of World Population Will Own Smartphones in 2017." Strategy Analytics, 21 December 2016 (https://www.strategyanalytics.com/strategy-analytics/blogs/smartphones/2016/12/21/44-of-world-population-will-own-smartphones-in-2017#.WbLAzLKGO70).

Evangelos Vayias joined OTE Group in 2007 as Head of Operations and Engineering of OTEGlobe, the group's international wholesale network infrastructure arm. Since 2012, Dr. Vayias has been Senior Manager of OTE Group's strategic and transformation projects for operational optimization and business development. Currently, he is driving projects for OTE Group's digital transformation. Dr. Vayias has been involved in digital technologies for more than 20 years, having implemented important IT and telecommunications projects and solutions. He has also led a number of R&D and innovation projects funded by European Union and Greek national research funds. Dr. Vayias has lectured at the Universities of Piraeus and Aegean, Athens Information Technology (AIT), and the Hellenic American Educational Institute (Athens College) and has published over 40 articles in scientific journals and conference proceedings. He holds a degree in electrical and computer engineering as well as a PhD from the National Technical University of Athens and is a Senior Member of the IEEE. He can be reached at evagias@ote.gr.

Ioannis Konstantinidis has been OTE Group Chief Strategy, Transformation and Wholesale Officer since November 2015, having served as Chief Strategic Planning and Transformation Officer since June 2011. From 2000 until 2011, Mr. Konstantinidis held various senior managerial positions at OTEGlobe, an affiliated company of the OTE Group, the latest of which was the position of COO, responsible for the commercial and technological issues of the company. Today, besides his tasks at OTE, he is the Chairman of the Board of Directors of OTEGlobe, as well as Chairman of the Board of Directors of OTE Rural North and South. Prior to the OTE Group, Mr. Konstantinidis worked for Global One Hellas SA, where he was head of the technical department. He holds a degree in electrical engineering from the National Technical University of Athens, with a specialization in telecommunications. He can be reached at ikonstantinidis@ote.gr.

CUTTER CONSORTIUM
Access to the Experts

Cutter Business Technology JOURNAL

Management, Innovation, Transformation

Get global perspectives on critical business technology issues — anytime, any place — with a *Cutter Business Technology Journal* Online Subscription!

Cutter Business Technology Journal is the go-to resource for innovative ideas and solutions to today's — and tomorrow's — IT challenges. ***Cutter Business Technology Journal*** is *the* forum for debate for academics, practitioners, and thought leaders on the critical issues facing today's business technology professionals.

And now, accessing this insight can be even simpler — *exactly when you need it most* — with an online subscription!

Become a *Cutter Business Technology Journal* Online Subscriber and receive:

- Unlimited, fully searchable access to all ***Cutter Business Technology Journal*** issues, including a 12-year issue archive
- Free PDF downloads of all issues
- Weekly industry updates via the ***Cutter Business Technology Advisor***
- Strategic insight on digital innovation and transformation, technology leadership, IoT, big data analytics, security, mobility, FinTech, machine learning, cloud, enterprise and business architecture, enterprise agility, and more!

— *Cutter Business Technology Journal* Online Subscription Information —

To find out how you can start your single-user or enterprise-wide online subscription to ***Cutter Business Technology Journal*** via www.cutter.com — which includes access to a 12-year issue archive — and determine the best option for you and/or your team, please contact Tomlin Coggeshall at tcoggeshall@cutter.com or +1 207 631 0802.

Digital Transformation & Innovation Bootcamp

Karim Lakhani
Professor, Harvard Business School
Fellow, Cutter Consortium

Next Bootcamp: October 25-27

Babson Executive Conference Center Wellesley, MA USA

The Digital Transformation & Innovation Bootcamp program fee is US $15,000 for a team of 3-5, plus an additional fee per person for accomodations and materials.

For more information or to register your team, contact your Cutter Consortium Account Executive at +1781 648 8700 or sales@cutter.com.

Is Your Business Model Still Relevant? Will It Be Next Year?

The competitive landscape is nothing like we've seen before. An organization in a completely different industry may be poised to swallow up your market — and you might not even see it coming.

> Did Nokia — a cell phone company — see Apple — a niche personal computer company — sneaking in to pull the market out from under it?

There's much to learn from Nokia's and others' experiences about what to do, what not to do, how to plan for, and how to manage a shift toward creating and capturing new value. At Cutter Consortium's *Digital Transformation & Innovation Bootcamp* you'll dive deep into what you need to do to succeed.

> Designed for just a handful of teams from noncompeting firms, the *Bootcamp* provides a rigorous process for you to revolutionize your digital transformation journey.

The Agenda

Case Studies & Lectures. Harvard Business School Professor and Cutter Fellow Karim Lakhani will lead you through several case studies and lectures. Prior to each case discussion, you'll work through its issues from the variety of perspectives you enjoy when collaborating with colleagues from outside your industry.

Hands-on Working Sessions. Based on the framework you'll learn, you'll begin working on a transformation project that will power your organization. During multiple Transformation Sprints, your team of 3-5 colleagues from your own organization will develop new ideas and new business models to help your business thrive. You'll be ready to prototype the resulting new/revised project or strategy when you get back home.

Project Assessment. You'll get feedback on your transformation project from the other teams. The fresh perspective of executives from other sectors/non-competing companies will uncover insights about your situation that you'd otherwise likely miss.

Register Your Team Now

In just 2 days, Professor Lakhani will guide you through an examination of how digital innovation is transforming our business landscape. You'll learn:

- What's truly unique about the new digital strategies that are changing our environment?
- What digital strategies have established organizations employed?
- What strategies might be right for your organization?

With only one organization per industry permitted, spaces are filling quickly!

For more information, or to reserve your team's spot for our October 25-27 *Digital Transformation & Innovation Bootcamp,* call us now at +1 781 648 8700 or email sales@cutter.com.

CUTTER CONSORTIUM
Access to the Experts

Cutter Business Technology JOURNAL

About Cutter Consortium

Cutter Consortium is a unique, global business technology advisory firm dedicated to helping organizations leverage emerging technologies and the latest business management thinking to achieve competitive advantage and mission success. Through its research, training, executive education, and consulting, Cutter enables digital transformation.

Cutter helps clients address the spectrum of challenges technology change brings — from disruption of business models and the sustainable innovation, change management, and leadership a new order demands, to the creation, implementation, and optimization of software and systems that power newly holistic enterprise and business unit strategies.

Cutter pushes the thinking in the field by fostering debate and collaboration among its global community of thought leaders. Coupled with its famously objective "no ties to vendors" policy, Cutter's *Access to the Experts* approach delivers cutting-edge, objective information and innovative solutions to its clients worldwide.

For more information, visit www.cutter.com or call us at +1 781 648 8700.

CUTTER CONSORTIUM
Access to the Experts