efca
Representing
FIDIC in Europe

FUTURE TRENDS
IN THE CONSULTING ENGINEERING INDUSTRY

June 2020

FUTURE TRENDS
IN THE CONSULTING ENGINEERING INDUSTRY

Preface

The future is inevitable. The only constant is change and the rate of that change is increasing uncontrollably, or so we thought. A tsunami of challenges brought about by COVID 19 unleashed a seismic shift in what we consider to be our norms. This pandemic has transcended political, ideological, religious, cultural and corporate boundaries. It has forced our industry to work in ways many considered impossible only a few short months before.

Our competition is no longer the multinational multi-disciplinary practice with thousands of employees. Instead, we are challenged by new nimble exponential organisations that utilises the latest technologies to create a fusion of minds in global collaboration. 2020 has clearly demonstrated this to us.

EFCA owe a sincere depth of gratitude to our very own futurist Maurizio Boi for compiling another wonderful publication, along with our committed team of Nikola Matić, Maximilian Grauvogl, Christophe Castaing and Jan Van der Putten.

Now more than ever we must challenge the AEC Industry to break through our traditional boundaries of knowledge and become thinkers, to solve the problems of humanity with the passion and creativity of an artist. We must have the courage to transform ourselves, to abandon preconceived frameworks, to embrace new models and welcome new experiences; allowing us to truly evolve as an industry and society.

In this Third Annual EFCA Future Trends Booklet, we invite you examine the optimum blend of technologies and techniques to adopt with different clients in different markets, to suit the scale of your company. Our goal is to expose the European AEC Community to the possibilities and opportunities that this inevitability will create and the consequence of ignoring it. Along with the world, industry as we know it is changing. It may not be the future we were expecting. It may not be the future we have prepared for. However, we must change with it.

Kevin Rudden
EFCA President
Maurizio Boi
Chair Future Trends Task Force
Nikola Matić
Vice-Chair Future Trends Task Force

Maurizio Boi - Christophe Castaing- Maximilian Grauvogl
Nikola Matić - Kevin Rudden - Jan Van der Putten
Future Trends Task Force Members

Kevin Rudden - EFCA President

Table of Contents

PREMISE

In the 2018 booklet, we examined the new "**disruptive**" technologies and **revolutionary** processes which helped us discover the potential exponential models of evolution in our business sector.

The 2019 edition focused on **innovative**, **anticipatory strategies** in new management models and how to make decisions by **analysing data** and **information** using these **powerful new tools** together with **cognitive collaboration**.

The 2020 booklet looks into the **right mix of practical aspects and applications** inthese innovations within our specific field.

We will be looking at the **right combinations** of **technologies** and **techniques** to adopt with various clients in different markets, taking into account the size of the company.

Already in possession of the necessary instruments, we are ready to make our choices on the road to becoming a "4.0 Industry".

EFCA wishes you all a pleasant journey along this road to the future.

A NEW APPROACH TO CUSTOMER SATISFACTION: THE LAW OF CUSTOMER

Amazon has invented new business models in selling products by creating new markets and breaking away from existing traditional systems.

To achieve these results, Amazon has adopted a new approach in customer relations.

Simplifying the process as much as possible, it began a detailed **analysis of qualms before making a purchase and determined the final factor** in submitting the order or not.

In order to encourage the customer to buy products online, it has gradually assuaged each of these fears, obtaining full satisfaction and the results everyone is familiar with.

Let's try to implement the same approach in our world.

Customer fears in the construction world (AEC)

1) Find the right interlocutor for the overall process

2) Have/find the right budget and stick to it

3) Be supported in the definition, description and respect of the work's final objectives and expected results

4) Be supported in the definition, description and respect of lead times

5) Have adequate insurance guarantees and countermeasures in the event that any of the 4 previous points do not turn out as expected

A hypothesis in problem solving:

1) From the customer's point of view, the right interlocutor means someone who has:

• Proven experience in managing complex construction processes in all phases, from design to final realisation;

• Reputation through reviews from other customers;

• Proven credibility in financial institutions;

• Control of the supplier network organised across transparent and open platforms using smart working, videoconferencing and virtual reality;

• A Willingness to sign target contracts.

In regards to handling points 2), 3) and 4), we recommend the project management model in line with the IPD approach, already widely covered in the two previous booklets.

5) We suggest using an insurance model distributed amongst all players in the chain, to be activated in two phases:

• immediate intervention of the player who created the problem or other equivalent to replace them;

• immediate acknowledgement of the certified damage.

Obviously, management of the problem is considerably more complex and should be specialised according to the customers, works and market of reference.

Each situation should be addressed according to specific needs, yet always in line with the suggested approach.
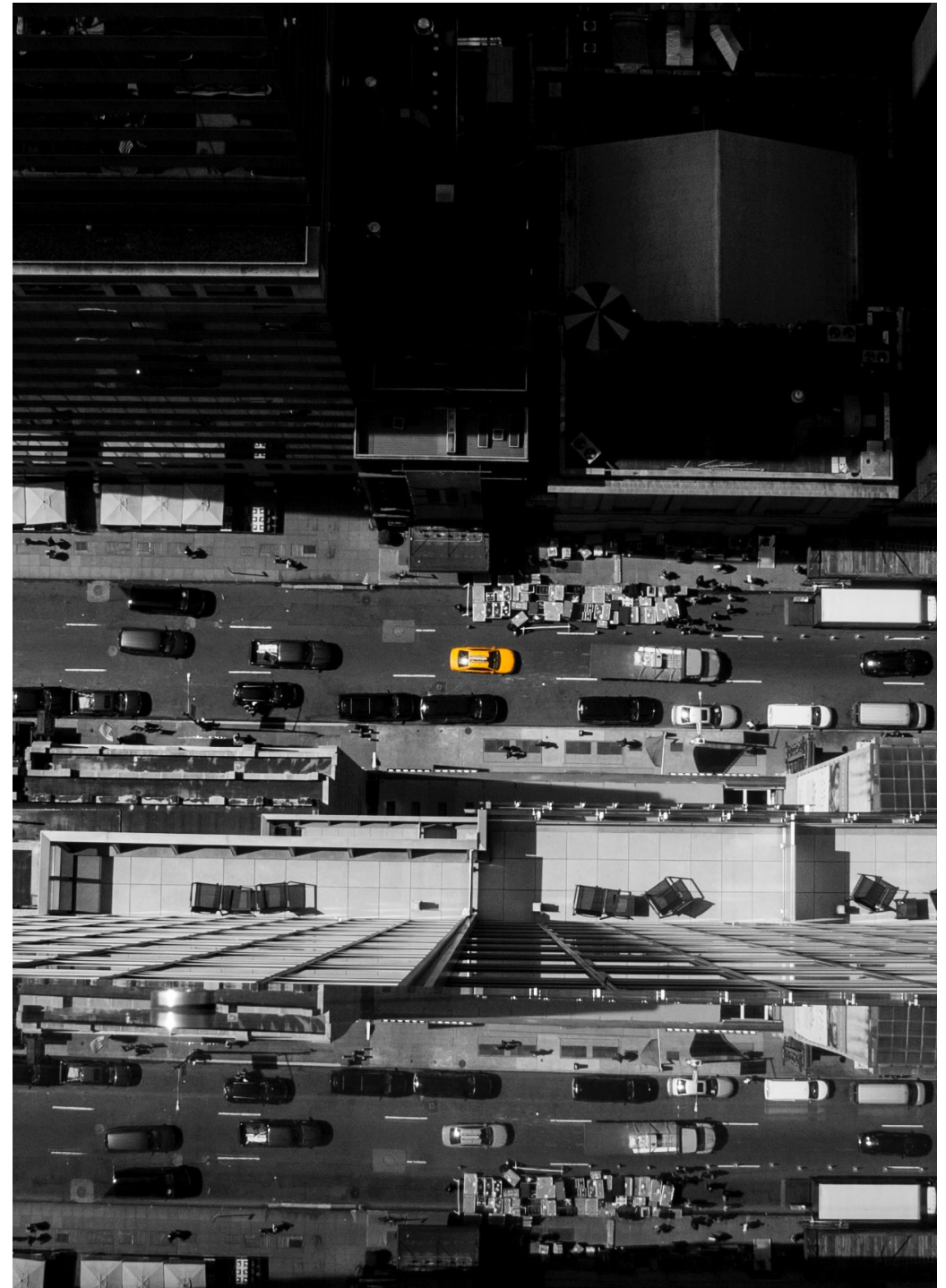
Measuring company performance
OKRs: an agile management tool

John Doerr, who introduced Google to OKRs, has created the following formula: **"I will...........................as measured by.............................."**

Doerr's formula explains the structure of OKRs very well:
I will (objective) as measured by (Key Results)

In other words, an Objective becomes a goal if you can measure its achievement.

The OKRs (Objective and Key Results) have two components:

- The Objective describes in qualitative terms what you want to achieve. The description should be short, simple and easy to remember but also engaging, motivating and challenging.

- Key Results are a set of metrics that track the distance from the goal. For each Objective, there should be two to five Key Results. Not more, otherwise no one will remember them

There are different versions of OKRs: each company or team adapted and tailored the methodology to its culture and its core business.

However, there are some basic common concepts:

- OKRs are a management tool, not an employee evaluation methodology (employees should not expect any reward or negative consequence when they set ambitious objectives);

- OKRs get companies used to being agile and to responding to rapid change—they are set, tracked and re-evaluated using short cycles instead of static, annual, top-down planning, whilst the cycles adopted may vary (half-yearly, quarterly, monthly, weekly) depending on if the focus is strategic, tactic or an open-ended rational goal.

- OKRs are open and available to all company levels (everyone can see everyone else's OKRs) — the purpose being to create alignment in the organisation.

- OKRs use a simultaneously top-down and bottom-up approach instead of a traditional, time consuming waterfall model knowing company's strategic OKRs, different teams realise how they can contribute to the overall strategy, set their own suitable OKRs and be strongly engaged in contributing to the final goals.

- OKRs target ambitious goals — if a Key Result is reached at a level of one hundred percent, it means that the OKR was too easy, since OKRs that are difficult to achieve make the team rethink the way they operate and to reach peak performance.

Companies adopting OKRs are more ready to change, improve collaborations, better recognise priorities, create focus and alignment, promote disciplined effort and initiatives, increase innovation and reduce time wastage.

The adoption of OKRs further enables them to use and manage smart working, since teams receive a clear path and are free to choose the best way to achieve goals.

They become more responsible, determined, inspired and challenging. Clear Key Results shared and known to all, create reciprocal obligations, solve interdependencies and unify competing initiatives.

OKRs are different from other goal-setting techniques due to the aim of setting very ambitious objectives.

Even if the stated objectives are not completely achieved, OKRs can help teams and individuals get out of their comfort zones, prioritise work and learn from both their successes and failures.

Stretch Goals go beyond the threshold of what seems possible (shoot towards the moon rather than the roof), could be seen as "setting a team up for failure".

However, more often than not, stretch goals can tend to attract the best people and create the most exciting work environments.

When aiming high, even missed goals tend to result in substantial advancements.

Many companies with experience in OKRs consider accomplishing 70% of the Key Results an extraordinary achievement, 60-50% not a bad outcome, whilst a measurement of 40-30% means that effort was applied but not in the right way.

On the other hand, if someone fully attains their objectives, this proves that the OKRs are not ambitious enough and they need to think bigger.

When setting your Key Results, the question to ask is whether you are measuring efforts or results.

A common pitfall in setting Key Results is looking at tasks rather than deliverables or milestones. Key Results should not be activity-based but value-based.

The typical structure of a value-based Key Result is:

Increase/reduce "ABC-metric" from X to Y

where X is the baseline (the starting point) and Y is the target (what you want to achieve)..

Even if Silicon Valley digital companies were the first to adopt the OKR method, nothing precludes its application to other companies with different core business, such as engineering organisations.

Engineers are accustomed to working on projects and focusing on delivering them on time, on the scope and on the budget (the Project Management Triangle).

This might be necessary but it is not enough—the project must also successfully reach the valuable objectives of those to have motivated it. Therefore, the engineer should have the objective to create value both for themselves and for their client.

Whilst they know what is valuable for themselves, they need to put in all possible efforts to realise what is valuable for the client.

OKRs can help on this way.

If you focus on value, you can find the following link between OKRs and Project Management:

- **Objective:** what we want to achieve;
- **Key Results:** how we are going to measure our progress;
- **Project:** what we are going to do to reach OKRs.

At the heart of any Project is one or more Objectives, the achievement of which can be measured by specific Key Results.

Thus, instead of only tracking the Project delivery, we should measure the indicators that motivated it and how the deliverables align with these indicators.
Without a Project, we cannot achieve the OKRs but if Key Results are not improving, we must be ready to revise everything.
OKRs and Agile Project Management can help engineer organisations to achieve valuable results both:

- **For the company**: aligning a project team's OKRs with the strategic OKRs of corporate management;

- **For the client**: focusing the project team's OKRs on the client's expected outcomes.

Cybersecurity in the AEC industry

Construction companies have primary focus on dealing with buildings, infrastructure and other tangible resources, very often offline using pen and paper checklists. It is therefore understandable that digital assets do not always receive the same attention as they have in other industries.

However, progressive AEC companies have started to adopt modern technology such as with BIM, Drones, Augmented Reality, Internet of Things and Data Management Platforms. While using all of those devices, it is of the highest importance to recognize associated risks.

With the majority of cyber-incidents going unreported, and no industry-wide practice of reporting or sharing details on such incidents, it is difficult for construction organizations to learn from each other's mistakes and collectively improve cybersecurity across the sector.

It appears that impact from a cyber-attack extends far beyond the digital domain. Any company—including those from the AEC sector—experiencing a cyber-breach can suffer devastating reputational damage and financial losses.

Businesses such as those in the construction industry, that may not be considered amongst typical targets, are increasingly falling victim to attacks, as many lack the necessary controls to mitigate cyber risk.

Construction firms represent low-hanging fruit for cybercriminals, with common vulnerabilities witnessed throughout the industry.

Discovering Future Trends and fresh ideas, this conservative approach is set to change.

New demands and needs for Digital Transformation and the development of cyberspace — especially the use of available Internet of Things and Industry 4.0 products—will be followed by cyber-attacks.

Therefore, both private and public organizations in the construction industry need to define strategies, processes and data management capable to mitigate cyber violence.

In doing so, one of the challenges will be how to simultaneously comply with the requirements of the General Data Protection Regulation (GDPR) and the need for confidentiality and traceability.

"The Internet of Things (IoT) devoid of comprehensive security management is tantamount to the Internet of Threats.
Apply open collaborative innovation, systems thinking & zero-trust security models to design IoT ecosystems that generate and capture value in value chains of the Internet of Things."

(Stéphane Nappo, Global Chief Information Security Officer at OVH)

The reliance that businesses place on their digital platforms is ever increasing.

The common view that "as long as everything works, there are no problems" no longer functions.

In addition to the regular management frameworks and organization chart, a modern AEC organization must include a robust Cybersecurity mitigation plan.

Cyber-attacks can be classified in the following categories:

- **Financial** – Financial motivation on organized criminal groups

- **Espionage** – investigations motived by state-affiliated agencies or to gain industrial insights

- **FIG** – Fun, Ideology, Grudge motives or even threats from activist groups

From one perspective, any of the listed categories shall not be underestimated or neglected. Crucially, cyber risk should not be seen as an issue solely for the IT Department or provider.

Whilst IT infrastructure is an important factor in managing cyber risk, it is just one piece of a much larger puzzle. Collaboration must be established between all Departments and in managing risk strategy identification.

What can business leaders do to strengthen their resilience to cyber-threats?

Firstly, they must recognise that risks in the digital space are present at all times, and represent a real threat to the success of the business.

The traditional "**measure and manage**" approach to risk management appears insufficient, as opposed to the "**sense and respond**" approach that must be considered in the digital ecosystem.

Cyber-Resilience is built on, and can be monitored against, five categories:

- **C-Suite Cyber Model** – cyber-awareness and culture within the organization coming from top management

- **Vendor Cybersecurity** – management of contractors, third-party procurement and all IoT devices including Drones and Artificial Intelligence

- **IT management** – handling information technology applications in general operations and administration

- **IT security** – both human and technological aspects of Cybersecurity breaches

- **Data governance** – the security and integrity of an organisation's data and information assets

"Passwords are like underwear: don't let people see it, change it very often, and you shouldn't share it with strangers."
(Chris Pirillo, CEO of Locker Gnome)

Attacks are increasing in terms of diversity, frequency and ferocity, necessitating a challenge to the accepted practice that cyber risk can be mitigated within the IT function. To build effective digital resilience, leaders must adopt a C-Suite response, embracing both robust technology and approaches to organisational culture.

As a performance measurement, most organisations these days are using Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs).

A dedicated team will have to develop a set of suitable KRIs and KPIs to apply within an organisation in order to construct a cyber-risk dashboard for the C-Suite to review their performance.

Evidence suggests that building resilience stems from top-level strategies and governance to provide an organisation-wide approach of embedding cyber-risk within a strategic hazard overview.

Continuous monitoring and improvement are vital for early threat detection and prevention. They also enable the identification of underlying causes of risk exposure and refinement of the selection of suitable leading KRIs.

Organisations must adopt a proactive view to retaining key business knowledge of cyber operations, reviewing and responding to new developments both internally and externally, whilst always aiming towards continuous improvement.

The National Institute of Science and Technology (NIST) has developed logical flow for Cybersecurity framework (figure below)
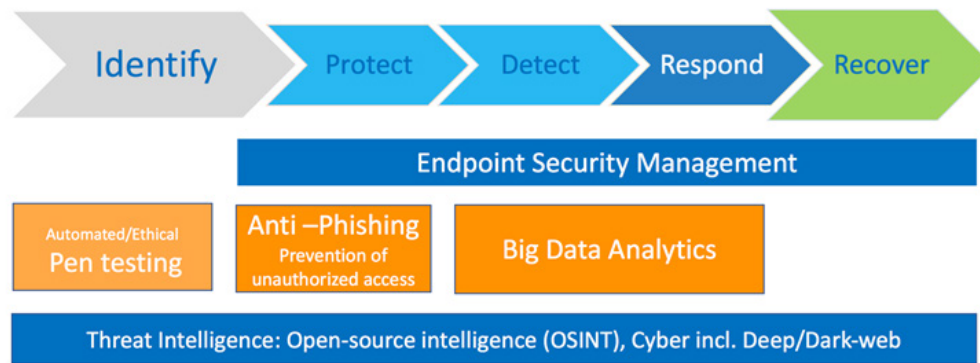
Cybersecurity framework

1. Identify

- Identify what is most critical to the running of your organisation from the information in your possession to key activities and processes.

- Risk assess all IT assets - software, hardware and data.

- Classify assets according to their role in the running of your organization and their level of exposure to cyberattacks.

2. Protect

- Prioritise actions concerning the assets identified as most in need of protection.

- Start with basic protections, of physical, technical and administrative nature.

  - Physical - including storage locations, physical barriers, screen-locking and personnel access authorisation;
  - Technical: including encryption, network segmentation, security patching, passwords, access privileges and endpoint protection tools;
  - Administrative: including policies, procedures, standards and staff training.

- Establish more sophisticated and targeted protection for you most sensitive or at-risk assets.

3. Detect

- Establish a means of continually testing that your protective controls are functioning and that procedures are being followed by staff and partners.

- Recognise when protective controls have failed or have been bypassed as an early warning of a potential attack.

- Have effective means for determining when a cyberattack is underway.

4. Respond

- Theorise various types of breach and plan precisely how to respond to different scenarios.

- Ensure that you have the capacity to continue to defend against other attacks whilst responding to a specific type of security breach.

- Periodically test and renew your response plans.

5. Recover

- Regularly back up critical data and have the ability to establish a clean computing environment.

- Develop a "Plan B" early on, focused on how to minimise the impact of a breach and recover quickly.

"If the facts don't fit the theory, change the facts"
(Albert Einstein, German Theoretical-Physicist)

The digital assembly line
"It is an extraordinary instrument to manage smart working during the coronavirus period"

Maurizio Boi - Italy -

After these years of research, we have come to the conclusion that:
"**in the digital age, collaboration is inevitable**"

By collaborating, people pool **skills**, **information**, **talent** and **resources** with the aim of achieving a **shared goal**.

Collaboration is not something that is improvised but rather it is the result of a **well**-**structured project**, **requiring focus on the results**, to be distinguished from simply work done with others.

Furthermore, **collaboration doesn't have to be just between people**, hence why we've wagered on the **blockchain** that has the potential to transform the construction sector by creating the **right ecosystem** in which **machines** and **people can interact and collaborate**.

- **Why the blockchain?**

Because the blockchain has the ability to create conditions of:

- trust and transparency amongst the numerous participants of the system;
- security in regards to the correctness and unchangeability of information.

OPERATIVE EXAMPLE OF EXPONENTIAL ENGINEERING

The business model is that of an exponential organisation that uses an **agile core** team of 15 employees and a **network** of 1,300 technicians, with a potential equivalent to that of a traditional company with 600 employees.
To create an **innovative** and **efficient ecosystem** for the implementation of engineering works, two platforms are used:

- **Collengworld** – the community in which professionals and organisations interact;
- **SCORE** – the collaborative platform in which projects are carried out.

15

How to make the collaboration smart:

- By optimising research and information costs, for example to form a temporary group during a tender process, using match algorithms

- By reducing the costs necessary to reach, draft and manage contractual agreements using Smart Contract

- By managing the reliability of the parties involved using an effective reputation measurement system

Smart collaborative Engineering is based on the blockchain and permits collaboration in the development of engineering service assignments from the tender to the final drafting of the project and construction.

The stages of the process are as follows:

1. The company wanting to take part in a tender uploads the tender data to the platform, defining the qualification requirements they are lacking in order to meet the requirements for participation in the tender;

2. Algorithms are applied to identify the ideal potential partners in the network who are able to provide the requirements lacking for participation in the tender;

3. The companies agree to the contractual conditions via Smart Contract;

4. The Smart Contract automatically performs the contractual conditions through to payment for the services performed;

5. The digital assembly line, being the physical or virtual place, is created to facilitate collaboration during the execution of the project.

The most innovative part of the platform is the Smart Contract, being software with an active role in the process via automatically executing the contractual conditions, rather than playing a passive role like a standard contract that has no automatic features.

The main participants in the Smart Contract are:

- The producer   (the entity who manages the service);

- The performers (the subjects who perform the services);

- The verifiers (professionals identified in the network who verify the work of the performers).

The Smart Contract includes the following processes:

a) Definition of the project's planning objectives, including:

- Activities to be performed and specifications to be observed, times to be respected, agreed-upon fees and penalties;
- Performance, such as regarding environmental sustainability;
- Deliverables, including reports, estimates, designs, etcetera;

b) Development of the service followed by the activities to begin, during which all crucial steps are confirmed in writing via the blockchain;

c) Quality control, during which the auditors check the quality of the documents;

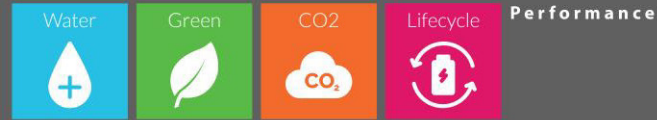d) Final delivery and payment of dues, upon all checks having a positive outcome, as per the established terms;

At this point, the data entered into the Blockchain ledger can no longer be changed.
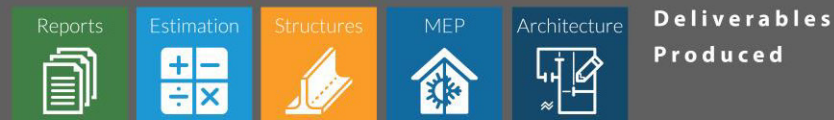
SMART CONTRACT DASHBOARD

Planning Phase

Planning
- Deadline
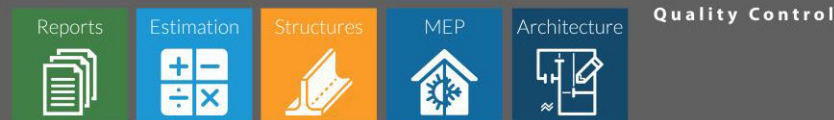- Team
- Budget
- Penalties

Performance
- Water
- Green
- CO2
- Lifecycle

Deliverables
- Reports
- Estimation
- Structures
- MEP
- Architecture

Design Phase

Deliverables Produced
- Reports
- Estimation
- Structures
- MEP
- Architecture

Quality Control

Quality Control
- Reports
- Estimation
- Structures
- MEP
- Architecture

Final Delivery

Performance
- Water
- Green
- CO2
- Lifecycle

Deliverables
- Reports
- Estimation
- Structures
- MEP
- Architecture

Payment

a. Defining project goals

b. Service developement

c. Quality control

d. Final delivery and fee payment
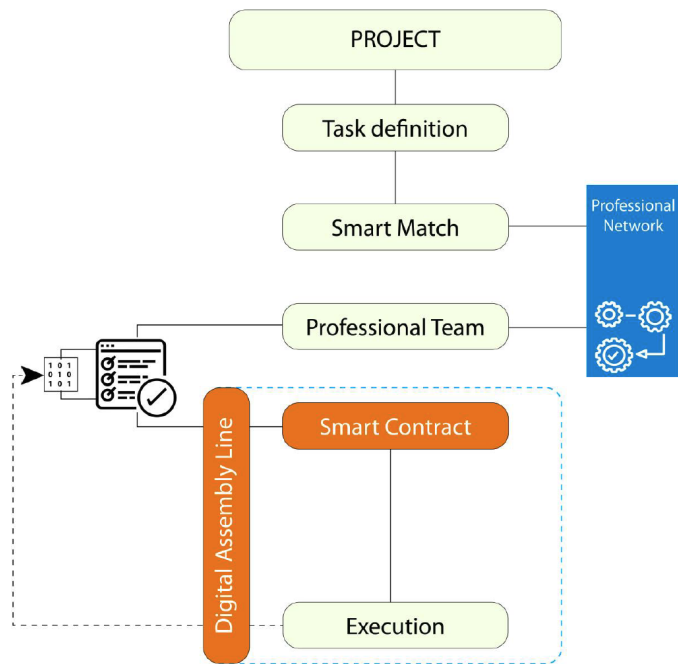
Of course, the system has the flexibility to permit agreed-upon contractual addenda to be inserted.

For example, the following are written in the blockchain:

- The established fees and contractual conditions

- The uploading of the performed tasks

- The uploading of verification reports

- The delivery of the documents to the client

- The demonstration of fee payment

In the Smart Contract dashboard, icons and symbols facilitate the overview, understanding and management of the project's objectives.

A practical application of the previous concepts is the realisation of the Big Room.

The Big Room is the real or virtual location in which collaborative engineering projects are elaborated.

The platform is designed to create a virtual assembly line for joint processes by facilitating smart working and coordination between the stakeholders.

The innovative aspects include:

- The Exponential Project Manager leading the digital assembly line via the digital dashboard, having all project monitoring and progress data available in real-time;

- The active planning of the project, with each team receiving the daily tasks to be carried out directly on their computer in accordance with previously-coordinated and agreed-upon schedules;

- The information network coordinated by a dedicated team;

- The latest technologies available such as the BIM and Virtual Reality can be used as visualisation and simulation tools

The pilot of the project is the Exponential Project Manager who can take action in real time in the supply of resources, as and when necessary, by simply calling on additional technicians and resources that are always available on the network.

DIGITAL ASSEMBLY LINE

BIG ROOM

Exponential PM

Digital Dashboard

Active planning

TASK 1   TASK 2   TASK 3   TASK 4

Virtual Reality
Simulation
and
Visualisation

Organisation

PROFESSIONAL
NETWORK

Information
Flow

team

Product   Process

BIM Model

Integrated Information
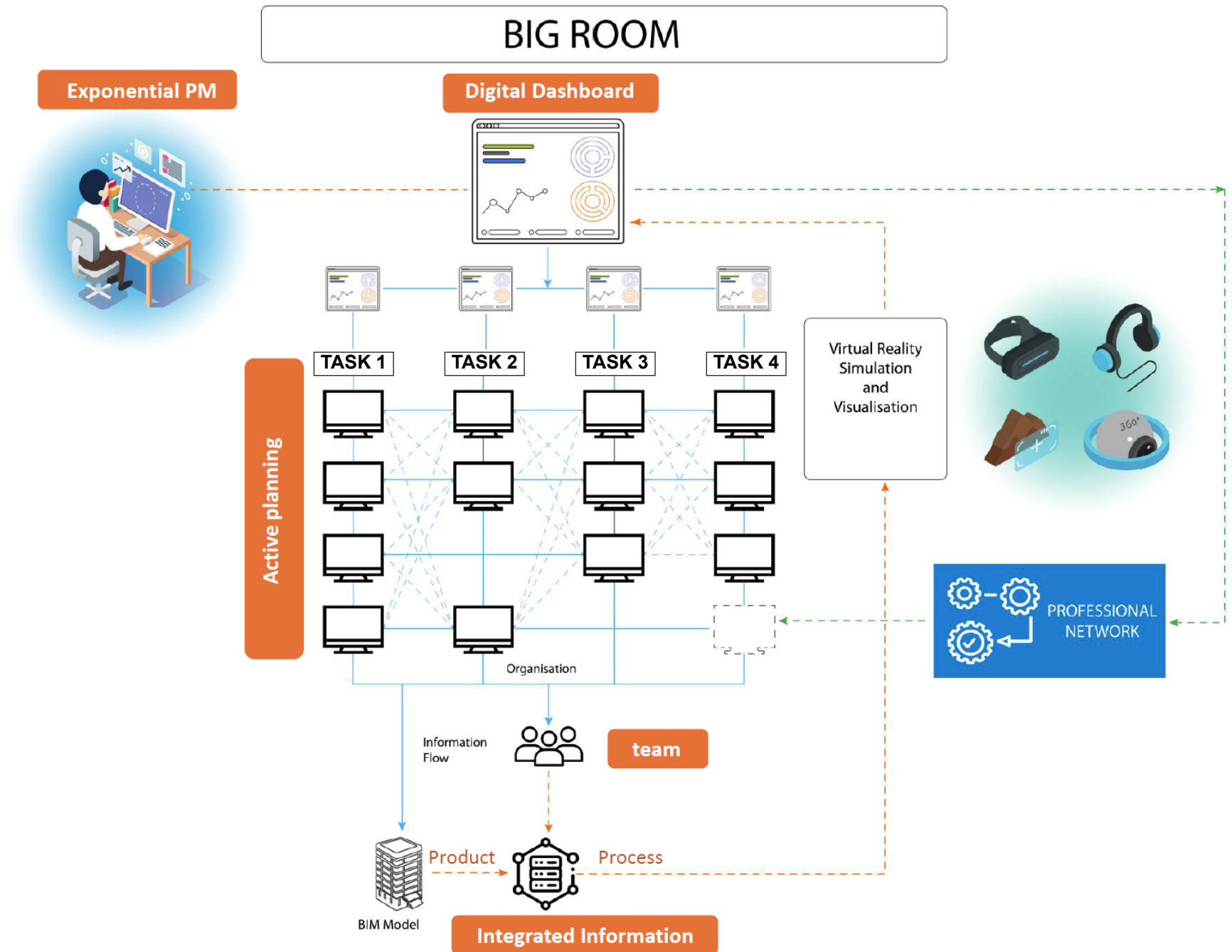
Conclusion: The right mix to becoming a 4.0 industry

In order to identify our path of improvement, we start with an analysis of:

- The framework of reference,

- available technologies;

- suitable management models;

- amount of information and data to be managed;

The framework of reference

This concerns the type of customer, the pertinent market and the characteristics of our engineering company.

Type of customer

- Local Client;

- International Client.

The pertinent market

- Traditional market;

- Innovative market.

The company's characteristics

- Consultant engineering company;

- General contractor engineering company.

Available technologies

Information Technology	Autonomous Agents
Building Information Modeling (BIM)	3D Printing
Cloud Computing	Internet of Things
Community	Ledger of Things
Algorithms	Virtual Reality
Dashboards	Augmented Reality
Blockchain Technology	Robotics
Network	
Smart Contracts	
Platform	

Management models

- Traditional Management
- Agile Management
- Wikinomics
- Integrated Project Delivery (IPD)

Information and data to be managed

- A small amount of data
- Many data
- Big Data

The right mix

The following graphs are taken into consideration to identify the technologies and management models to be adopted, in accordance with the area of reference and an analysis of the data to be handled.

In the following graphs we will analyse some situations related to different areas:

- With a small amount of data to be managed
- With big data

TAB 1 - FEW DATA TO MANAGE

	TECHNOLOGIES									
	Monitor	BIM	Cloud	COLLENG	Algorithms	Chart	Link	Share	Document	Logo
LOCAL CLIENT	●		●							
INTERNATIONAL CLIENT	●	●	●							
TRADITIONAL MARKET	●		●							
INNOVATIVE MARKET	●	●	●	●	●	●	●	●		●
CONSULTANT ENGINEERING COMPANY	●		●			●				●
GENERAL CONTRACTOR ENGINEERING COMPANY	●	●	●	●	●	●				●

IoT 3D VR IPD

TAB 2 - BIG DATA TO MANAGE

TECHNOLOGIES

	Desktop	BIM	Cloud	COLLENG	Algorithms	Analytics	Link	Share	Document	Logo
LOCAL CLIENT	●	●	●		●	●				●
INTERNATIONAL CLIENT	●	●	●		●	●	●	●	●	●
TRADITIONAL MARKET	●	●	●		●	●				●
INNOVATIVE MARKET	●	●	●	●	●	●	●	●	●	●
CONSULTANT ENGINEERING COMPANY	●	●	●		●	●	●			●
GENERAL CONTRACTOR ENGINEERING COMPANY	●	●	●	●	●	●	●	●	●	●

MANAGEMENT

3D · IoT · VR · IPD

We use the balance of decisions to make our choices and create the right mix, being the proper combination in the particular context.

The possible combinations are practically infinite and everyone can build their own personal 4.0 style which, taking into account the context and the choices made, will render us unique.

Public Blockchain
More transparency and trust

Private Blockchain
Adequate transparency and trust

VERY EXPENSIVE

CHEAPER

Cybersecurity
More data safety and security

Automation
More automation and AI Systems

LOTS OF PROTOCOLS

FAST AND AGILE

Collaboration
Human-based

Cognitive Collaboration
Hybrid between IA and Human

MORE HUMAN CONTROL

HIGHER PERFORMANCE

"*Many studies have shown that in order to solve complex problems, the best solutions are obtained precisely through the interaction between AI and people*"

(Francesca Rossi, Il Confine Del Futuro. Possiamo fidarci dell'intelligenza artificiale. Feltrinelli editore)

The results of a study showing errors in the diagnosis of breast cancer were published in the United States, with the following outcomes:

- without the help of AI systems, the best doctors were wrong 3.5 times out of 100 on average;

- without the support of doctors, the best AI systems were wrong 7.5 times out of 100 on average;

- the same doctors, but helped by AI systems, were wrong 0.5 times out of 100 on average.

This example demonstrates that people and AI systems make different and complementary contributions to problem-solving, with cognitive collaboration being more efficient.

The future is unforeseeable, as the spread of Coronavirus and its impact on our business demonstrates.

Our evaluations reported in this first cycle of booklets focusing on the possible means of collaboration across platforms and networks (Smart Working and cognitive collaboration) were offered as voluntary choices for our companies, without having ever imagined that they could become almost obligatory in order to continue working in such tragic times.

The important thing is be prepared from a technological and organisational point of view to implement these significant changes.

We hope our work has been helpful in facilitating your current and future business strategies.

With this booklet, the task force believes that the first cycle of three booklets on future trends has concluded.

We started in 2018 with identification of trends and we concluded in 2020 with possible operational applications in our sector. EFCA intends to continue this process with a new cycle of ideas and invites members to submit new proposals.

BIBLIOGRAPHY

Arthur D. Little Viewpoint: "From risk to resilience: Digital defence" - 2019

Boi Maurizio and Boi Patrizia, Engineering [n] - Engineering the Future or the Future of Engineering?, Te.x 2017.

Boi Maurizio and Boi Patrizia, Ingegneria elevato [n], Ingegneria del Futuro o Futuro dell'Ingegneria?, Dei Merangoli Editore 2017.

Collins K.: "Inside the digital heist that terrorized the world—and only made $100k." – 2017

Dwoskin Elizabeth and Karla Adam: "More than 150 countries affected by massive cyberattack" – Washington Post - May2017.

Ismail S., Exponential Organizations: Why new organizations are ten times better, faster, and cheaper than yours (and what to do about it), Diversion Books 2014.

Kelly K., The Inevitable: Understanding the 12 Technological Forces That Will Shape Our Future, Penguin 2016.

Libert M. Beck, J. Wind, The Network Imperative: How to Survive and Grow in the Age of Digital Business Models, Harvard Business Review Press 2016.

Martini P., Blockchain Fast and Simple - What It Is, How It Works, Why It Matters: Understand the Basics, Join the Revolution, independently published 2016.

Maasik A., Step by step guide to OKRs, Weekdone 2017.

McAfee A. and Brynjolfsson E., Machine, Platform, Crowd: Harnessing Our Digital Future, W W Norton & Co Inc, 2017.

McCord P., Powerful: Building a culture of freedom and responsibility, Silicon Guild 2018.

Mougayar W., Buterin V., The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, John Wiley & Sons 2016.

Nielsen M., Reinventing Discovery: The New Era of Networked Science, Princeton University Press 2012.

O'Reilly T., WTF?:what's the future and why It's up to us, Cornerstone Digital, 2017.

Parker T., Smart Contracts: The ultimate guide to Blockchain Smart Contracts – Learn how to use Smart Contracts for cryptocurrency exchange!, CreateSpace Independent Publishing Platform 2016.

Ramsey S., Blockchain: Quick start guide to understanding Blockchain, the biggest revolution in financial technology and beyond since the internet, CreateSpace Independent Publishing Platform 2016.

Raskino M., Waller G., Digital to the core: Remastering leadership for your industry, your enterprise, and yourself, Routledge 2016.

Ries E., The Startup Way: How Modern Companies Use Entrepreneurial Management to Transform Culture and Drive Long-Term Growth, Currency 2017.
Rifkin J., The zero marginal cost society: The internet of things, the collaborative commons, and the eclipse of capitalism, St. Martin's Press 2014.

Rogers D. l., The digital transformation playbook: Rethink your business for the digital age, Columbia University Press 2016.

Rossi F., Il Confine Del Futuro. Possiamo fidarci dell'intelligenza artificiale?, Feltrinelli editore, 2019

Schwab K., The Fourth Industrial Revolution, Crown Publishing Group 2017.

Susskind R., D. Susskind, The Future of the Professions: How Technology Will Transform the Work of Human Experts, OUP 2015.

Tapscott D., Tapscott A., Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world, Penguin 2016.

The National Institute of Science and Technology (NIST), U.S. Department for Commerce: "What is the Internet of Things (IoT) and how can we secure it?" – 2018

Thiel P., Masters B., Zero to one: Notes on startups, or how to build the future, Crown Publishing Group 2014.

Trusted Cyber Security Solution, Pascha Soufi Siavoch: "Cyber Security Trends: Aktuelle Entwicklungen, Herausforderungen Lösungen" - 2019

Williams D., Tapscott D., Wikinomics, Atlantic Books Ltd 2011.

Williams A. D., Tapscott D., Macrowikinomics: New solutions for a connected planet, Atlantic Books Ltd. 2011.

Zurich insurance plc Cybersecurity and the construction industry Staying ahead of emerging threats - 2019

Chapter Photos: www.unsplash.com

efca

Representing
FIDIC in Europe