WAVESTONE

IoT
FROM FASHIONABLE TREND TO LARGE-SCALE TRANSFORMATION

Since the advent of the Internet of Things, IoT has become an everyday reality for businesses and initiatives in this field are becoming increasingly widespread in all sectors of activity.

While many types of application exist today, such as behavioral assurance depending on the client's lifestyle, as well as connected vehicles and even airplanes, and smart cities, implementation of an IoT-based project rarely takes place. What are the obstacles encountered and the pitfalls to be avoided to enable players to go beyond the idea-emergence and proof of concept (PoC) stage?

HIGHLY DIVERGENT LEVELS OF MATURITY IN CORPORATE LIFE

With regard to how the Internet of Things is used by major companies for industrial ends, the field of application is very wide: enhanced reliability or optimization of production tools, product/services diversification, back-office efficiency and employee well-being. This is underpinned by numerous projects concerning transport and energy-production infrastructure surveillance and predictive maintenance and logistics chain optimization ("connected bottles") as well as building management and plant automation (known as "industry 4.0", or the fourth industrial revolution).

All of these projects illustrate various levels of corporate maturity. Some industrial majors with massive quantities of connected products already on the market have structured their organization, and implemented a solid group governance model around a set of connected solutions. Their major challenge now is to successfully integrate these dedicated entities in the rest of the industrial production process, which is, by nature, less agile due to longer lifecycles.

AUTHOR

LAURENT FELIX
laurent.felix@wavestone.fr

Aside from these pioneering majors, many companies are still at the idea-emergence or the use-case stage and have launched tests by way of models or PoCs. Almost all of these players are now faced with the challenge of being able to reach this milestone so that they can transform their ideas into real commercial opportunities. On the business side, there is a lot pressure from the growing demand to implement these new services. However, issues at the technical level, as well as those concerning sourcing, the ability to convince management, and even the organization are thorns in the side of program managers, technical directors and Chief Digital Officers (CDO), as well as the more recent Chief IoT Officers, and tend to obstruct the deployment of initiatives.

ESTABLISH AN OPEN DIALOGUE BETWEEN BUSINESS LINES AND IS DEPARTMENTS

The development of the Internet of Things in companies is driven by the numerous business opportunities it generates in all of the organization's entities. Business value is most often generated by the data captured by objects and their effective exploitation by application blocks, namely the Data Management systems of the company's IT System. The diversity of needs, types of objects and data to be collected could prompt the IS Departments in charge of solution maintenance to optimize standardization and rationalization in order to define a technological framework and, as such, enhance interoperability, maintenance and security. A dialogue is being established to find a better balance between the technological framework (which can curb initiatives) and business innovation. It is still too early to impose too many limitations on technical solutions: IS Departments cannot impose a platform or type of network on business lines. Forcing business lines to adapt would be counter-productive, mainly due to the immaturity of the market.

Vis-à-vis business lines, IS Departments must act in a consulting capacity; a role that is governed by the company's decision-making bodies which foster a continuous and open dialogue. This has seen the emergence of the "IoT business consultant" who plays a key role within the IS Department alongside the business lines, IS and network architects and the data scientists, who ultimately ensure the value of projects.

CONVINCE MANAGEMENT TO UNDERTAKE TRANSFORMATIONS

IoT projects are by nature infrastructure projects that sometimes require substantial investments and are quite risky due of the fledgling ecosystem. Not surprisingly, these factors could cause some uncertainty in management. Moreover, enthusiasm and motivation for IoT projects is often fostered by operational teams working on the ground who still have considerable difficulty in convincing their superiors. So, what's the answer?

Proof of Value (PoV) testing is carried out between the model and pilot stages. The purpose of PoV is to install and test solutions in a production environment to gauge its real contribution. PoVs are concrete projects deployed on a small scale and most often supported by a cloud visualization solution and/or data analysis. By revealing the real business contribution, the PoV is a very effective means of leverage to convince management.

PoV results should nevertheless be integrated in a comprehensive financial model covering the entire financial equation of the business line. Return on Investment is not always obvious: for example, for an average-sized plant, using IoT to optimize a production line can require a substantial investment amounting to several hundreds of thousands of euros. In addition, these investments must be justified which is not always easy, particularly for plants turning at relatively low saturation, and high yield rates.

Moreover, it is important that all IoT- related risks be highlighted in the investment plan. Security, for example, must be adapted across the entire value chain, from the objects themselves, through to the connectivity solutions and ultimately the data exploitation platform. There is also a risk of supplier default in a fledgling market where consolidation is intensifying every day. In addition, two specific legal risks should be taken into consideration: firstly, the loss of ownership rights of data produced by companies to their suppliers, and secondly, the use of employee personal data in certain situations (connected bracelets to measure physical activity, smart buildings and employee well-being applications). Although no legal framework has, as yet, been set up for IoT, an arsenal exists comprising personal data, electronic communications, network loyalty, etc. which, in principle, covers risks. Other measures, such as user trust, which is a key success factor, and the Privacy by Design approach, could be adopted to limit project risk by using personal data.

SKILFUL SELECTION OF SOLUTIONS NEEDED TO MAKE GOOD SOURCING CHOICES

In a nutshell, the technical IoT chain may be summed up as a collection of objects or sensors, connectivity, and data collection, cleaning and processing systems, as well as analysis and visualization systems and applications.

Applying the principle not to duplicate solutions within the company that are vertical and which are not interoperable for reasons of maintenance and security is therefore relatively simple. It is important to bear in mind the fact that, at a later stage, interoperability could enable the development of other innovative services.

As such, it would almost be tempting to opt for the strategic choice of adopting a central IoT platform for the entire company. Although theoretically interesting, this choice is not realistic in the short or medium term due to the immaturity of the platform market (as reflected by the frequency of partnership and acquisition announcements); a situation which could last another 18 to 24 months. In addition, the platform ecosystem as we know it has several particularities that should be taken into account. For example, every platform has its own specific characteristics, notably in the way it adapts its functioning to the type of data to be collected, as well as frequency measurements or resilience, etc. This is what is called a pattern. Capturing the geographic data of mobile data in real time (such as vehicle-fleet trip optimization) cannot be achieved using the same type of platform as that adapted for taking gas and electricity meter readings.

The choice of platform therefore calls for an analysis of short and medium-term needs: if the scope of needs is quite limited and corresponds to a significant volume of objects, an appropriate choice would be a platform with a suitable preferential pattern. If, on the other hand, there are a lot of different needs for an

average amount of objects, an open platform providing access to operating interfaces of other platforms should be considered. In this case, caution is warranted since needs and development costs of interfaces, such as SDK (Software Development Kits) and API (Application Programming Interface) can turn out to be very high.

Connectivity solutions have become extremely diversified, notably in terms of cover and debit, and some new operators have yet to demonstrate their staying power. As such, this entails anticipating the ways sensors will be used and to align their needs with the telecoms solutions already in place in the company. Contracts with new players should always be drawn up for a relatively short period of time (24 months) and contain a reversibility clause allowing for a return to a traditional operator.

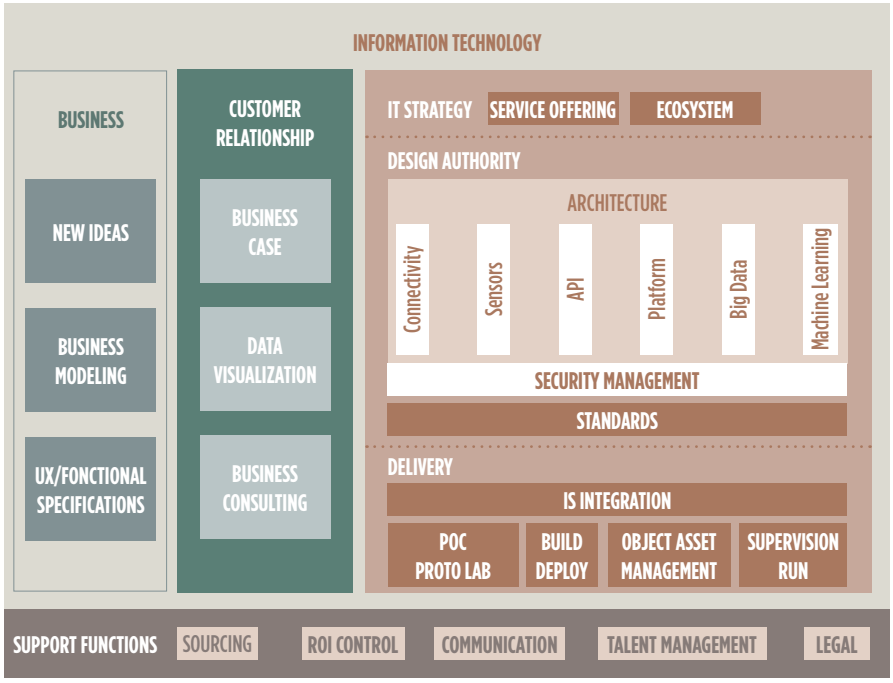
With regard to long range and low debit networks (such as LPWAN and 3GPP) and given the fact that there is still no recognized market standard, it is worth studying the choice of sensors with multi-solution chipsets. At present, these are not that much more expensive than mono-technology chipsets and offer greater flexibility in terms of suppliers.

The IoT ecosystem is still extremely prolific, which makes it difficult for all players (major industrial groups, integrators, Cloud operators and start-ups, alike) to make the right choice. The volatility of the market and what has become pretty much of an obligation not to make a long-term choice are prompting players to opt for, at least, partial Cloud solutions.

It is also interesting to note the approach of certain major players, and operators in particular, with regard to the vertical integration from the supply of sensors through to delivery of cleansed data. These offers, which are now modular in terms of scope and interface, can be a good solution for first deployment.

ORGANIZATION REQUIRED TO ADDRESS HIGHLY DIVERSE IOT CHALLENGES

Major companies currently employ 3 levels of general IoT governance. At the first level, the Group leaves IoT project incentive/management in the hands of its subsidiaries and runs a community involving "think-tank" workshops. At the second level, the Group creates services and IoT expertise centers to serve as accelerators for its subsidiaries which maintain budget and thus project-initiative control. At the third level, governance is ensured completely by the Group which carries out IoT projects for its subsidiaries. At present, the second level seems to generate the best results, while the third is lacking in on-the-ground knowledge at Group level, and the first often fails dues to the lack of expertise at subsidiary level.



The chart opposite shows the functions that must be implemented to ensure the correct deployment and exploitation of IoT solutions in large companies. Among these singular functions, note the need for highly experienced IS architects to ensure the integration of these solutions across the entire IT System of the company. The Information Systems Security Manager (ISSM) also requires support from a Security Bundle Manager whose role is to ensure the overall security of the chain.

The management of complex objects (i.e. those requiring regular software updates) is a major issue often encountered in large-scale deployment. Updating security (or more broadly data), particularly for fleets of mobile objects, is a very arduous task. Having a temporary asset management transition function would be an additional advantage when it comes to defining and implementing appropriate management processes.

In addition, it should be noted that in technology departments such as the ISD, expertise in sensor technologies and particularly those involving electronics and electro-technologies is generally limited. Henceforth, the ability to leverage the skills of specialized engineers will strengthen the ability of players to challenge suppliers and also carry out more agile testing. It is the job of the talent manager to recruit and train these key players.

In addition, given the current absence of a specific regulatory framework for, and the lack of maturity in the IoT market, the IoT organization should integrate the role of a lawyer specialized in data to ensure the integrity of data produced by the company and its employees.

Companies would be advised to launch IoT projects now if they wish to remain competitive; a reality the business lines have understood only too well. The pitfalls to be avoided and the associated risks are manifold, but the keys to success exist. It is now up to companies to prove themselves to their departments and to find the sourcing and governance solutions appropriate for their activity.

WAVESTONE

www.wavestone-advisors.com

Wavestone is a consulting rm, created from the merger of Solucom and Kurt Salmon's European Business (excluding retails and consumer goods outside of France). The rm is counted amongst the lead players in European independent consulting.

Wavestone's mission is to enlighten and guide their clients in their most critical decisions, drawing on functional, sectoral and technological expertise.