TABC Paper

The Internet of Things Gets Smarter: Towards Industry 4.0

Background - The Building Blocks:

Industry 4.0 represents an evolution of technology, process and policy which has occurred over the last 25 years. In the late 1990s, researchers at Xerox Parc lab were working on concepts of ubiquitous computing, which came to represent a model of a highly interconnected and networked future: interconnection of people, objects and services in computer aware environments. In the early 2000s, Asian policy makers were using the phrase liberally in the Asia-Pacific Economic Cooperation (APEC) and demonstrations of the "house of the future" were being built globally.

Over time, technology and applications have developed to make this more of a reality. Machine to Machine (M2M) solutions have pushed the limits of non-human mediated communications to new capabilities, and the infrastructure of the Internet of Things (IoT) has progressed with significantly more ability to interact. However, policy and technical limitations persist which may limit further necessary innovation.

As the interconnection and interactivity has increased so has complexity. Where a main focus of interest in the early days of ubiquitous computing was radio-frequency identification (RFID) sensors, today the breadth of objects that can be connected and the information which can be provided or captured in real time has exploded. This variety and variability of information has also resulted in the emergence of concepts related to Big Data. Big Data represents not only a significant advance in the ability to capture and process data but also a significant progress in the ability to find correlations across these new and varied data sources as well as more sophisticated analytics to apply to them. Finally, Cloud Computing has evolved to provide numerous services which can be delivered with improved efficiency, economy, scope and scale, and which are completed by the increasingly rich and granular data and the related correlations and analytics.

Business has taken note of these advances: they have been or are being applied across the spectrum of commercial activity. In the consumer/individual space ever more sensors are embedded or attached to devices including in things we wear, medical devices that may be implanted or the "smart" environments we may live and work in – appliances, cars, homes, grids and cities. In the business-to-business (B2B) space, the explosion of sensors and data has led to the Industrial Internet, which refers to the integration of big data analytics, IoT Machine-to-Machine services and cloud computing to enhance operational efficiency[1]. This includes the interconnection of business objects that support healthcare delivery, service operations, supply chains, logistics, city planning, sustainable development and consumption - to name a few of the most important applications. Applying intelligence, applications and sectoral overlays build upon these uses to create the web of things, intelligent systems and Industry 4.0.

[1] Industrial Internet Consortium. What is the Industrial Internet? http://www.iiconsortium.org/about-industrial-internet.htm

Industry 4.0: Developments on the Ground

Industry 4.0/Industrial Internet is a high priority on the political agenda globally and in Europe as the next innovation in the digital transformation of manufacturing. This transformation, however, is more comprehensive and holistic than the advances in production, supply management and process tasking that were reflected in concepts like "just in time" manufacturing. In the U.S., Industrial Internet research and work is being led by the Smart Manufacturing Leadership Coalition as well as other numerous initiatives supported by the federal government[2]. U.S. industry is also looking to meet the new challenges of the digitalisation of industries. For example, in the spring of 2014, U.S. companies founded the Industrial Internet Consortium (IIC) to bring together all the relevant players across technologies to develop best-case practices, use cases, influence standards etc. IIC counts more than 120 members.

Among EU member states, Germany has shown a strong dynamic for several years in setting up an industrial platform called "Industrie 4.0" that bundles competencies and interests of companies active in ICT, automation, IT Services and in machine and plant construction. Industry 4.0 is a pioneering project that was originally conceived in the framework of the German Federal Government's High-Tech Strategy, focusing on the use of information and communication technology in manufacturing lifecycles. Also called the "4th Industrial Revolution," it aims to increase the industrial value creation through the use of cyber-physical systems in production processes[3]. Driven by the associations ZVEI, VDMA and BITKOM, the platform Industrie 4.0 aims to develop and apply technologies from IoT, Internet of Services (IoS) and Web of Things (WoT)[4] into the future manufacturing and production facilities which will be demonstrated by specific use-cases in different industry segments.

Currently, there is no coordination across Europe of developments around Industry 4.0/Industrial Internet and emerging technologies. In the UK, for example, the policy focus has been on the wide potential of Internet of Things (IoT) with a recent report by the Government Chief Scientist[5] on the internet of things' ability to transform the way we live and deliver significant benefits to the economy. The UK communications regulator Ofcom has consulted on various policy issues e.g. spectrum, standards, data security/privacy and what role Ofcom should play in enabling the success of the IoT industry. On the industry side, HyperCat is a consortium and standard driving secure and interoperable IoT for industry, based out of the UK.

---

[2] Kurfuss, Thomas (December 2014). Industry 4.0: Manufacturing in the United States. *Bridges, vol 42*. http://ostaustria.org/bridges-magazine/item/8310-industry-4-0

[3] Innovations in this field will enable machines and products to independently communicate with each other and exchange commands in real-time, which will lead to a digitalization and flexibilisation of (mass) production lifecycles. The flow of real-time communication between persons, objects, machines and systems creates the basis for cross-sectorial value creation as well as an efficient cost and resources management.

[4] Where the primary concern of Internet of Things (IoT) has been on how to connect objects together at the network layer, the Web of Things (WoT) regroups research and industrial initiatives looking into building an application layer for physical objects to foster their reusability and integration into innovative 3rd party applications. The WoT brings in all resources and interactions involving devices, data, and people on the Web. Correspondingly, it brings into focus a wide variety of challenges and opportunities and paves the way to a variety of exciting applications for individuals and industries. The Web of Systems (WoS) is the combination of Internet of Things with smart networked devices and domain know how

[5] Government Office for Science and The Rt Hon Oliver Letwin MP (18 November 2014). Vision set for UK to become a world leader in the internet of things [Press Release]. https://www.gov.uk/government/news/vision-set-for-UK-to-become-a-world-leader-in-the-internet-of-things

In Italy, the National Regulatory Authority AGCOM has consulted on various aspects related to Machine-to-Machine services and has consequently established a stakeholder forum to monitor on a permanent basis the developments of the IoT market, with the aim of evaluating the need of regulatory interventions in various fields (e.g. investments in infrastructures, connectivity, standards, verticals) to boost, or possibly remove barriers to, the services development. In addition Italian Privacy Authority has launched a public consultation in order to collect information on privacy issues related to Internet of Things. The Italian Privacy Authority aims at assessing the phenomenon as a whole in order to evaluate the definition of measures to ensure users transparency in the use of their personal data and to protect them against possible abuses. These are just a few examples of the several initiatives taking place at the member state-level.[6]

On the EU level, the importance of Industry 4.0/Industrial Internet has also been acknowledged. In the recent Communication on "A Digital Single Market Strategy for Europe", the European Commission recognised the central role of Internet of Things, Big Data tools and Cloud Services for economic growth and competitiveness, innovation, and digitisation across all economic sectors.

Furthermore, in its conclusions of May 21, 2015, the Competitiveness Council emphasised specifically 'the need to promote a simple and predictable regulatory framework that boosts innovation in the digitalisation of industry and the removal of all unjustified or disproportionate regulatory or non-regulatory obstacles to exploiting the full potential of a digital transformation of industry and cross-border e-commerce'. The Council is looking at the digitization of the Industry, focussing on the issue of standardization, interoperability, the commercial use of data, etc. and declared its support of the Commission's intention to work together with the industry to identify and promote European standards on the international level[7].

The Policy Challenges:

With these new advancements happening, as with many fast moving technologies, challenges exist for policy makers: Do existing policies apply? Are they sufficient? Are new frameworks needed? What is the appropriate approach to facilitate the innovation, adoption and implementation of the technology to allow society to benefit from its potential, while addressing the risks which may occur related to some of its applications?

Europe's overall progress in adapting to this new form of industrialization is hampered by the lack of a common approach across technologies to support industry's further digitalization. Based on initial considerations mentioned in a communication of the European Commission in January 2014[8], Europe needs a vision and an integrated cross-sectorial approach to regain industrial leadership based on a fully digitized industry. The lack of an integrated strategy in the IoT

[6] European Commission, DG Connect, Components and Systems (30 June 2015). Background Paper for the Round-Table of Leaders of European Initatives on "Digitising European Industry". Brussels, Belgium

[7] Council of the European Union (21 May 2015). Digital Single Market policy: draft conclusion on the digital transformation of European industry. http://data.consilium.europa.eu/doc/document/ST-8993-2015-INIT/en/pdf

[8] European Commission, Directorate-General (DG) for Internal Market, Industry, Entrepreneurship and SMEs (22 January 2014). For a European Industrial Renaissance [Communication]. http://ec.europa.eu/growth/industry/policy/renaissance/index_en.htm

technology solution space is puzzling.

More efforts are needed to build integrated industrial systems. Today, policy makers and industry continue to work together around European Commission initiatives that function still too much as fragmented silos when addressing new technological and regulatory fields like RFID, the Internet of Things, and Cloud Computing. R&D PPPs (Public Private Partnerships) for Robotics, FoF (Factories of the Future), SPIRE (Sustainable Process Industry through Resource and Energy Efficiency), FI (Future Internet), as well as the recently launched PPPs around Big Data Value (BDV), 5G and the JTI ECSEL (Electronic Components & Systems for European Leadership) function independently. There is also "Advanced Manufacturing" – which can be mentioned for completeness - as one of the KETs the Key Enabling Technology initiative of DG ENTR, and the European Institute of Innovation and Technology (EIT) Knowledge and Innovation Communities (KIC) on value added manufacturing in the pipeline. All of these technologies and related initiatives are components of the future digital environment and require cross-sectorial coordination across policy makers and industries.

Government will be relevant not only as policy-maker and regulator but also as enabler and adopter. From ensuring compatible regulatory regimes on security and privacy to transparent and predictable market access regimes, public sector services must be leading adopters of emerging technologies.

Failure to recognize the interconnected and interdependent nature of these technologies and related business models may result in policy and regulatory frameworks that needlessly impede innovation through unnecessary burdens or unintended consequences. At a minimum, close coordination, collaboration and cooperation is required across all government policy makers and actors (both users and providers). This coordination, cooperation and collaboration needs to also extend across stakeholders to include businesses which develop the technology, its applications and related business models, as well as those that need to implement or use these technologies, including businesses and consumers/citizens/individuals.

Policy Considerations:

Infrastructure and M2M

Industrial Internet / M2M / Industry 4.0 require constantly available as well as high-performance communication infrastructures, with reliable and stable speeds providing advanced Quality of Service, short latency and short provisioning times. This can only be realized if quality differentiation in traffic delivery services is allowed. For instance in the United States, net neutrality regulations do not apply to services that offer connectivity bundled with e-readers, heart monitors, or energy consumption. Another example of services excluded from the net neutrality regulations are limited-purpose devices such as automobile telematics. Therefore, the US and Europe should ensure a well-balanced net neutrality regime that can secure the technical requisites associated to such innovative services needed in the current digitization of traditional industries.

Strong incentives for continued investment in the EU and U.S. in secure and high-speed communication infrastructure is necessary to meet the demands of a digital economy and the exponential demands coming up in the Industrial Internet context in particular. There are significant differences in deployment and access to such infrastructure in different regions on both

continents, with some areas well served and some not. These gaps must be closed to drive global competitiveness. By investing in new network infrastructures a strong ICT sector will follow, boosting efficiency, innovation, growth and employment across all sectors of the economy.

A common vision for the sector that would promote an equally flexible and investment-friendly regulatory environment on both sides of the Atlantic is crucial. In the case of the EU, the Digital Single Market (DSM) strategy recognizes the need for simpler and more proportionate regulation in those areas where infrastructure competition has emerged at regional or national scale. More emphasis is needed on policies that promote dynamic outcomes such as investment and innovation by all parties. Current regulatory frameworks were not created thinking of M2M/IoT services. Therefore policy makers should have a flexible approach to smoothly adapt current rules to innovative M2M/IoT services.

One element that will be critical for the development of the Industrial Internet will be related to the ability for the commercial provision of seamless cross border services and the facilitation of the movement of data. For instance, compatible legal frameworks will allow efficiency of interconnected, cross border value chains.

Governments and regulators should ensure a policy framework based on a light-touch, pro-competitive regulatory approach that incentivizes investment and enables the development of new business models for all players. Governments and industry members also need to continue to work to strengthen the protection of customer data. Regulation should also avoid technology restrictions given convergence trends (including telecoms-media) while relying on sustainable competition. Excessive or technology biased regulation can stifle innovation, raise costs, limit investment and harm consumer welfare.

Allocation of sufficient spectrum in an internationally harmonized manner will also be critical. Internationally harmonized spectrum is essential to enable wireless M2M/IoT technology for global deployment, ensuring interoperability and driving down costs to increase economies of scale. Nevertheless, a balance should be reached between unlicensed and licensed spectrum avoiding any market distortions between both. This will enable spectrum sharing between M2M/IoT applications, driving spectrum efficiencies, helping promote innovation and competition. Some M2M/IoT services usually have very long life cycles based on 2G/3G technologies. There will be an increasing need for international spectrum coordination to adequately protect these services from any disruptions worldwide.

With the expected explosion of M2M/IoT devices, sufficient identifying resources must be available (such as IP addresses and resource identifiers) to ensure there is structural capacity to accommodate newly connected devices. Today, local telephone numbers (E.164) are the most widely deployed numbering resource used to connect to mobile networks. Some traditional consumer protection requirements commonly associated with E.164 numbers are not needed or appropriate in the IoT context, for instance number portability, possibility to call emergency services and Calling Line Identification (CLI) rules. However, there is concern that M2M/IoT technology will subsume their availability. International mobile subscriber identity (IMSI) numbers (E.212) offer a solution to increasing numbering resources. Government regulators should ensure that IMSI's or other suitable resource identifiers are permissible and interoperable with local mobile networks to enable traditional mobile and M2M/IoT growth. Policies providing an IPv6-friendly environment will also open an effectively limitless range of "things" to be globally addressed thus further enabling new IoT and M2M applications."

M2M/IoT tax burdens should be minimized as these services are usually characterized by very low Average Revenues Per User (ARPUs) and could harm seriously their current low profitability. Additionally, if any taxation or fee is required, it should be balanced across the M2M/IoT value chain.

Privacy

A policy issue of great concern to individuals is the need to appropriately protect their personal data and provide assurances of privacy. This issue is predicated on the nature of the information being collected and used. We note that in many B2B/Industrial applications no personal data is involved and those applications do not raise privacy implications.

The concept of Industry 4.0 or the Industrial Internet consists of a number of known and applied standards and technologies - it should be supported by reliable and coherent policy, and (only) where necessary supported by a regulatory approach. Existing policy and regulatory approaches on data protection are already applicable to IoT, although concepts of how to apply those rules should be considered in light of the need to expand use of these technologies throughout economic sectors. As in all regulatory constructs, they should be applied in a consistent manner to enhance legal certainty. Furthermore, general data protection regulations should apply consistently across all IoT providers - mobile operators, device manufacturers, online platforms- in a service and technology-neutral way.

As regulators review the application of existing rules and data protection frameworks, they should examine them through the filter of the potential impact on the IoT. The IoT is characterised by data originating and combined from a variety of sensor based sources, from ubiquitous devices – a growing number without user interfaces – and free flow of data across devices and systems for individual and/or organizational applications. As such, data protection legislation should consider the context of data use and reasonable expectations of users, and not take overly-prescriptive approaches to purpose limitation, notice, consent, profiling and cross border transfer. Policy makers need to consider the context and develop frameworks that can enable those flows which pose no risk to privacy while assuring appropriate mitigation of risk on those that may implicate privacy or other individual interests. Industry should continue to work within cross sectorial associations as well as in partnership with policy makers to consider what changes may be required to practices of security and privacy in relation to evolving uses of these technologies. There are already initiatives underway such as the Alliance for Internet of Things Innovation ('AIOTI'), which has been set up by the European Commission and has made a number of policy recommendations on how industry can address potential privacy challenges associated with IoT.

Security

Security is critical across all uses of the Industrial Internet, the development of Industry 4.0 and IoT technologies. Protection of proprietary information – like a manufacturer's supply-chain dashboard – is essential to ensure only authorized employees have access and prevent unauthorized individuals (inside or outside of the company) from copying or changing data. Policymakers, system owners, and system managers must consider the dynamic structure of systems that are distributed across multiple locations spanning the globe while transferring information between devices identified at times only by private IP addresses. In contrast to service

providers managing information transfers between public IP addresses, managers of private IP networks must choreograph information flows within these systems using various data pipes from multiple suppliers across the entire geography of the private network.

Due to the intensive data exchange Industrial Internet/Industry 4.0 requires, it must be established on communication infrastructures that are robust and resilient in the face of cyber security threats. Therefore, most Industry 4.0 services and applications will run on corporate *intra*-nets, i.e. over dedicated intelligent networks, which ensure a secure environment (not the public internet).

The benefits of and reliance on IoT enhanced supply chains will only persist if the security needs of this new infrastructure are met. Global standards, good business practices and government policy and regulatory environments all play a role in assuring this infrastructure. From a policy perspective, there is no need for a specific security approach, but the general aim should be to foster partnership through information sharing, incident response, awareness raising and global best practices.

Standards

Modern standards are at the heart of this new industrial revolution. Market-based, industry-driven standards that are globally consistent permit the creation of interconnected, cross border value chains and allow them to function efficiently and without disruption. Such common standards should be agreed among as many partners in Europe and the U.S. as possible. National industrial policy must also support global engagement and consensus in order to prevent silos that will defeat the adoption of Industry 4.0. It is absolutely crucial that from the beginning all involved and affected stakeholders are developing or reviewing standards jointly. While the needs of each industry have to be taken into account as the context of application for policy, high level interoperability can create both value and leverage across sectors It is important to encourage cross sector interoperability, so as to facilitate cross sector pollination and collaboration as well as reuse of IoT outputs.

In the manufacturing industry, for example, the real-time capability in wireless standards such as WLAN and Bluetooth need to be taken into account when elaborating horizontal (non-application specific) ICT standards related to Industry 4.0 or the Industrial Internet ("advanced manufacturing, wireless digital factory"). Neglecting such industry- and application-specific requirements could lead to needless limitations in the evolution towards the future of manufacturing.

Policy makers should encourage standards development by supporting the standardization bodies where the relevant stakeholders are already active, in line with the well-established market-driven and voluntary-based standardisation model. Having a number of standardization bodies involved in developing IoT relevant standards enables standards development where the technical focus fits best and where the non-technical elements, such as IPR policies, facilitate the smooth uptake and implementation of the standard.

Skills

Industry 4.0/Industrial Internet creates a new demand for convergence based skills combining classical engineering with electronics and software. This means new interdisciplinary teams and new individual skill profiles are needed which impact both education for new entrants to the

workforce as well as up-skilling the existing workforce. A need for recognised certification programmes also emerges. Furthermore, there will be a corresponding need to address skills of regulators to understand and address the needs of Industry 4.0/Industrial Internet products and services as they merge existing product categories.

Entrepreneurs will have to prepare their employees with high responsibility for the revolutionary changes the digitalization of production processes and enterprises will bring to the workforce. Policymakers should work with industry to accompany this development in assisting the industry at the creation of appropriate education and training programmes to ensure the labour force's skillsets are kept up to date, in the context of IoT in particular also looking at the digital skills needs of non-ICT specialists.

Conclusion - Policy Recommendations:

As policy makers tackle these evolving technological trends in the policy sphere, considerations should be made to the following:

- To ensure advances like the Industry 4.0/Industrial Internet- powered by Machine to Machine (M2M) and IoT/WoT/WoS and Communications technology - deliver on expected benefits, governments should promote an enabling public policy environment that does not prevent innovative solutions before their merits can be tested in the marketplace.

- The new European and US rules on Open Internet/Net Neutrality should be implemented in a manner where operators are allowed to secure differentiated quality of services on their networks and to conduct traffic management requirements accordingly, with the objective to support a variety of applications and services for Industrial Internet.

- Continued investment in the EU and U.S. in secure and high-speed performance communication infrastructure is necessary to meet the demands of a digital economy. Governments and regulators should ensure a policy framework based on a light-touch regulatory approach that incentivizes investment in high-speed and ultra-fast communication networks and enables the development of new business models. They should also ensure that sufficient harmonized spectrum resources are made available.

- Laws, policy frameworks and practices should provide for robust and context-appropriate data protection that guarantees the privacy of the citizen without hampering innovation. For example, companies should be aware that when they are collecting personal data from data subjects in the EU, the data protection law of the data subject will apply. Both privacy and security concerns need to be appropriately taken into account in order to provide the needed trust environment with the involvement of all players.

- Sufficient identifying resources must be available (such as IP addresses and resource identifiers) to ensure structural capacity to accommodate newly connected devices.

- M2M/IoT tax burdens should be minimized.

- Maintain support for the market-based and industry-driven standardization model enabling standards to be developed in the standards developing organizations (SDOs) most relevant to the specific issues being dealt with in each standard.

- Policymakers should work with industry to assist in the creation of appropriate education, training and certification programmes to ensure that labour force's skillsets are kept up to date and to educate regulators to appropriately address Industry 4.0/Industrial Internet's developments, products and services and other related emerging technologies.