„Smart Systems Everywhere – how much Smartness is tolerable?"

Erwin Schoitsch

AIT Austrian Institute of Technology GmbH (Vienna)

(erwin.schoitsch@ait.ac.at)

Keywords:

Smart Systems, Internet of Things (IoT), Autonomous Systems, Embedded Intelligence, Cyber-physical Systems, Safety, Security, Systems-of-Systems, societal impact, liability, ethical aspects, legal aspects

Abstract:

Smart Systems are today's drivers of innovation, in all industrial and social areas highly automated, intelligent systems are taking over tasks, services – and maybe one day, control of our lives. The keynote will address critical incidents in several areas – medical devices, industrial plants, autonomous vehicles, smart infrastructures, privacy, (big) data, malicious security breaches and attacks, demonstrating the limitations of too excessive use of not very trustable, uncertified systems, developed rather for functionality and neglecting too much safety, security and resilience and their interplay. An overview on methods and standardization efforts towards achievement of trustworthy systems and systems of systems is provided, societal impacts and market disruptions respectively new market opportunities are addressed, not to forget sustainability as property. Large European projects and smaller Support Actions are introduced which proposed recommendations, roadmaps and guidance, and results, how to meet the challenges – from the technical as well the economic and societal view point.

1. Introduction – Smart Systems on the Rise

Smart Anything Everywhere – that's the new hype on IoT, Internet of Things, combined with Intelligence, Autonomy and Connectivity. IoT is the infrastructure, Cyber-physical systems (CPS) are the basis of components and "Things" – may they be visible or "invisible", integrated into every day devices. The extremely high connectivity of "smart things" composed of CPS, from intelligent sensors and actuators up to more complex compnents and systems, leads to this world of "Internet of Things", and in the last consequence, to "Smart Anything Everywhere". Comfort, health, services of all kinds (including emergency services, rescue work and surveillance/monitoring etc.), safety, security and privacy of people depend increasingly on these. Smart Health, Smart Farming, Smart Mobility, Smart Energy, Smart Production/Manufacturing, Smart Cities/Homes/Buildings, Smart Wearables, Smart Living for Ageing Well, Smart Water Management, or Smart Critical Infrastructures in general, these are the major areas as e.g. taken up by AIOTI, the Alliance for Internet of Things Innovation. There are even developments towards unusual "smart" applications like "Smart Gastronomy",

utilizing 3D printing for creating unusual forms of food, or "Smart Construction", i.e. creating buildings by smart robots and machines in very short time out of modules, which can create unusual designs not possible with standard machinery and people. The latter was reported in a separate session and working group at the euRobotics European Robotics Forum 2017 in Edinburgh.

Highly automated or autonomous smart interacting systems are becoming the main driver for innovations and efficient services. The impact on society and economy as a whole is tremendous and will change our way of living and economy considerably - thus dependability (safety, reliability, availability, security, maintainability, but additionally resilience, robustness, sustainability, etc.) in a holistic manner becomes an important issue, despite emergent behaviors and critical interdependencies. Besides technical risks, there are considerable risks to people's privacy, independence and freedom. "Big Data" is no longer a protection making total control of a society difficult, it is now an enabler; "Big Brother" of 1984 is a weak story compared what is or can happen today! Social media have proven, that they are not only supporting people in emergency cases, connecting people, support learning and increase knowledge, but also cause the opposite: enable new crimes, make mobbing undefeatable, distribute wide spread rumors, "fake news", undermine substantially the belief in objectivity and science, and influence even elections and referendums in a manner never foreseen before. There are studies [1], which detected, that young adults with high level of social media use feel more social isolation than those with lower social media use. The "Pisa tests" demonstrate that many abilities are lost because of the new media and new technologies, methods and tools. This has of course also happened in the past, but the influence on social behavior and the control of society was not so perfect as it will become now.

2. Internet of Things – Hype or Enabler?

Originally, communication and connectivity including always humans as one partner. With the ascent of machines talking to each other without human interaction, the age of "M2M" (Machine-to-Machine Communication) has begun, with first working groups and standards arising e.g. at ETSI, the European Telecommunications Standards Institute, one of the official ESO's (European Standardization Organisations, the others are CEN and CENELEC). With the success of the internet this led to the vision that all "Things", in all domains and applications, billions in the end, might be connected and communicating, facilitated by the extreme progress in micro- and nano-electronics and low power electronics. This vision led to the assumption that the new age of IoT (Internet bof Things) has started. Even evolving technologies and applications, which worked already quite well in a rather conventional communication environment claimed no longer to be "embedded systems" or "cyber-physical systems" but IoT (Internet of Things in general, or IIoT (Industrial Internet of things, if in the industrial domain) – this included highly automated driving, robotic applications and so forth. This is considered typically characteristic for a "hype" – but the development around the evolving ecosystem of IoT led the EC to support the IoT European Research Cluster IERC in the preparation of the Alliance for Internet of Things Innovation AIoTI. The work started in 2014 followed by a high-level meeting on 4th February 2015 in Brussels. In the first years being an informal organization under the umbrella of DG Connect, which created a separate unit for IoT research, and as platform hosted by the EU platform Cordis, it became in the meantime an association under

Belgium Law with 200+ members, among them other platforms and industrial associations like ARTEMIS-IA (Nov. 11, 2016). AIoTI has now 13 working groups as depicted in Figure 1, covering horizontal themes as well as "smart" domains. The working groups developed documents, which are available on their website [3].

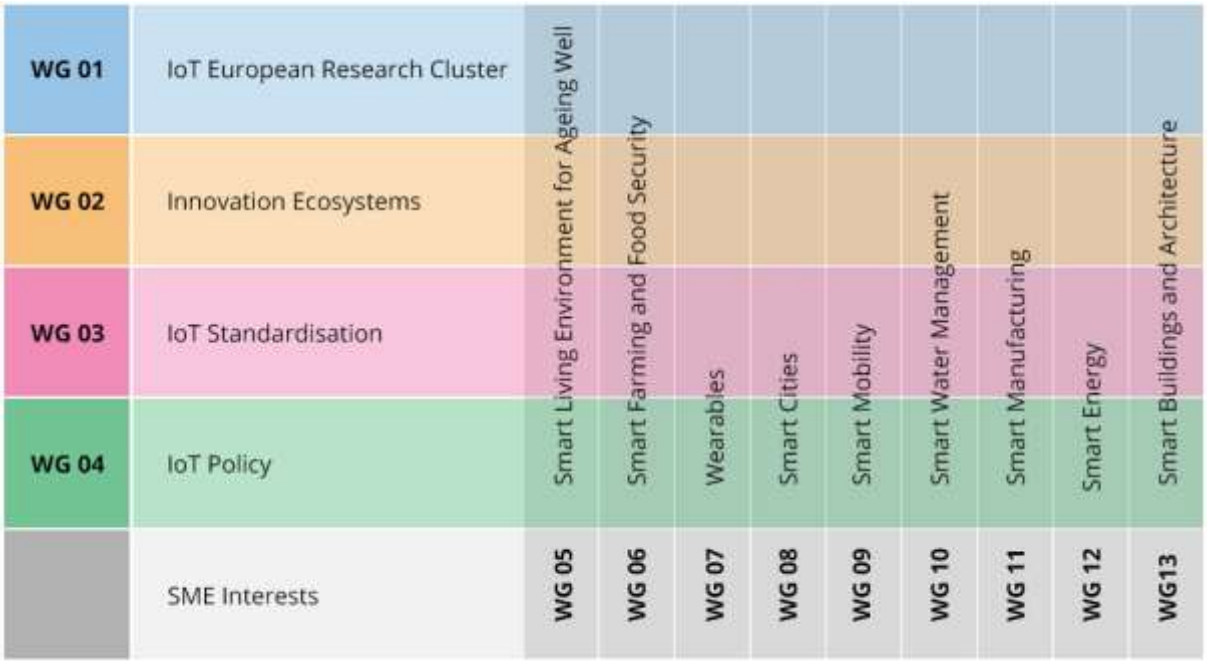

Figure 1: AIoTI – Internet of Things Alliance – Topic- and Domain Working Groups for the „Smart Universe"

This development clearly shows that it is more than a hype. AIoTI really aims at making Europe the leading region in the world to create and master sustainable innovative European IoT ecosystems in the global context to address the challenges of IoT technology and applications deployment including standardization, interoperability and policy issues, in order to accelerate sustainable economic development and growth in the new emerging European and global digital markets. The initial documents of the working groups became basis of Calls of the EC Research Programs, e.g. the so-called "Large Scale Pilots", the first ones in the domains of "Smart Farming" and "Smart Mobility".

One of the key findings of the recommendations was, that privacy, security and trust challenges are everywhere in the IoT – privacy and trust have to be built-in by design. There are already several known attacks on IoT-systems, e.g. a University was attacked by it's own vending machines! They built a Botnet of 5000 machines of the Campus (IoT system, including even smart bulbs) which sent permanent request messages to seafood website which slowed down considerably all network and Internet services. The reason was a naive approach to security not separating the network parts from each other [4]. Another case was a hotel in Styria in the Alps where a Ransomware blocked access to all rooms. The owner paid 1200$ (because he could not reprogram locally in time. Fortunately, safety requirements always allow to leave a room without key as fire escape measure so fortunately people were not locked in, only locked out (the original news report that people could not leave was therefore wrong). Other ransom ware attacks were on ticketing machines in the San Francisco Public Transport area.

Another key issue is interoperability: protocols, data and semantic interoperability – therefore the AIoTI Standardization WG issued three reports and is very active because of the

importance of standardization for huge IoT systems with many interfaces and "things", an extremely inhomogeneous environment. These were on

- High Level Architecture
- IoT Standardization Landscape
- Semantic Interoperability

A view on the "Standardization Landscape" shows the heterogeneity of the landscape: horizontal, rather generic standards and domain specific standards, from many international and industrial standardization organizations. ETSI, AIoTI and associated groups like ARTEMIS Standardization WG, but also IEC and ISO (ISO/IEC JWG 41, Internet of Things and related standards) try to cooperate and coordinate efforts to achieve a joint view and make the "landscape" more usable (hopefully).

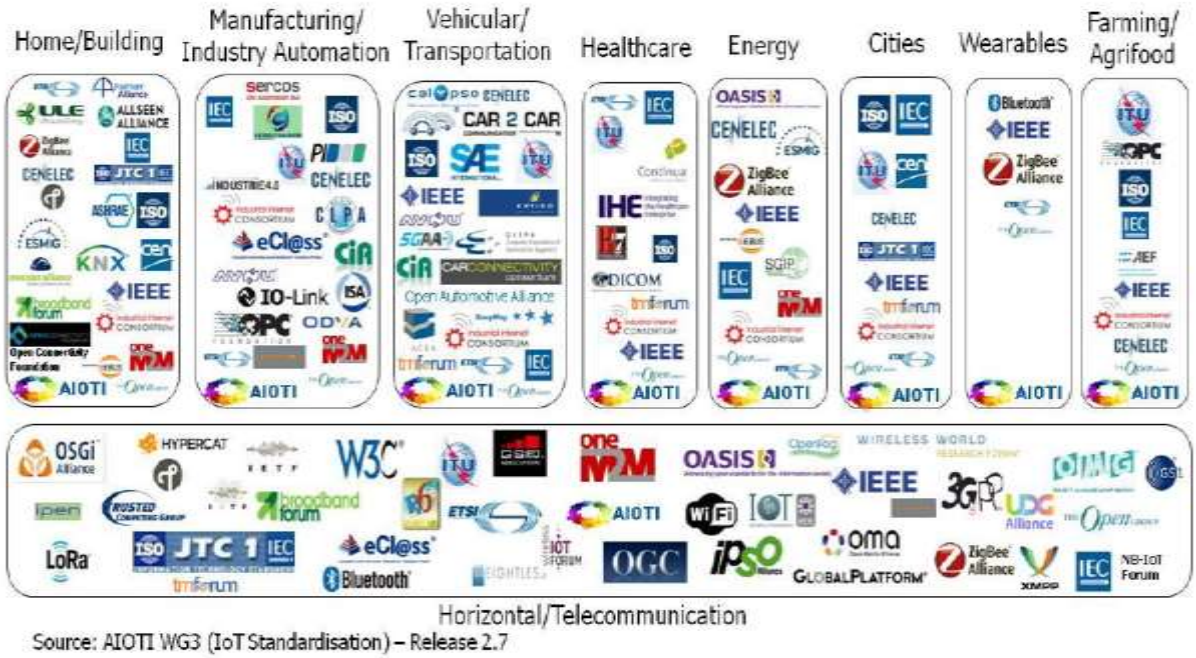

Figure 2: IoT Standardization Organizations (SDOs) and Alliances, vertical and horizontal domains

IoT has to be seen on European level as one important component to driving the "Digital Transformation", as depicted in Figure 3. The others are "Big Data" (Analytics, Cloud, High Performance Computing) and "Intelligence and Autonomous systems" (which is somehow a revival of AI – Artificial Intelligence, with decision taking, situational awareness etc.).

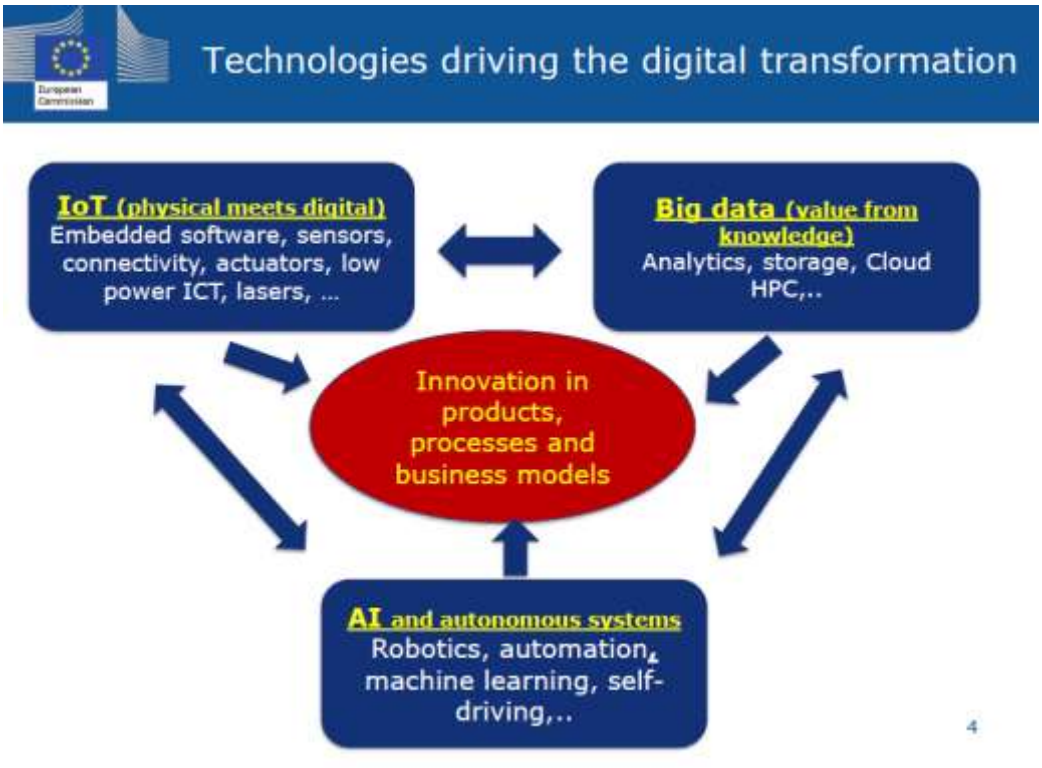

Figure 3: Technologies driving the digital transformation (source: DG CONNECT, W. Steinhögl).

3. Autonomous Systems – beyond Automated Driving!

Automotive is a real mass market, and the trend towards highly automated and autonomous driving is not only because of the (funded) efforts of the EC ("Zero accident scenario") but also in the interest of the big OEMs to change the market and open up new opportunities. In any case, it will disrupt current businesses. In the announcement of the WardsAuto Outlook Conference June 6th, 2017, in Birmingham, it says:

With automakers embracing and investing in mobility services, including hailing and sharing ventures, **will vehicle ownership become a thing of the past?** Examples are co-operations with partners in new businesses, investments in new mobility services, particularly in urban environments. They include ride-hailing, ride-sharing (also known as carpooling), car-sharing, new businesses in fleet management and service of "car-on-demand" (driverless taxi) and, in the case of Ford, even bike-sharing endeavors:

- General Motors and Maven.
- Ford and Chariot.
- Volkswagen and Gett.
- Daimler and Car2Go.
- Toyota and Getaround.

Another example may be that for fully autonomous cars, insurance and liability will become the OEM/manufacturer's responsibility and no longer be with the driver, the driver's licence will become a vehicle licence. Challenges like these are e.g. discussed at the conference "Connected Car Insurance Europe 2017" (April 19-20, London), so it is taken for earnest by business.

Will it hurt automakers' core business of selling vehicles to those who choose to own them? And do people really want to share or hail instead of own? That's the question of large

societal impact and may change our mode of transport considerably, even the role of public transport (particularly intermodal transport, e.g. long distance high speed trains, locally autonomous cars, including local traffic in rural areas, but longer distances by train).

Even national projects are now active, not only on European level. These national efforts are not restricted to large countries like Germany and France - for example, the Austrian Federal Ministry for Transport, Innovation, and Technology (BMVIT) has launched a call to set up and run a public test region for automated vehicles, the 'Austrian Light-vehicle Proving Ground' (ALP.Lab) starting in 2017.

But "autonomous vehicles" covers not only automotive. It covers

- robotics (industrial, health, ageing well applications),
- heavy machines (as demonstrated at euRobotics Conferences in civil applications like fire extinguishing, mining, snake robots),
- cleaning services in all dimensions (large and small),
- inspection (dangerous or difficult to access areas)
- transport and logistics,
- waste disposal (a smart city application!),
- decommissioning of difficult to handle or poisonous components,
- underwater robots off-shore in dangerous environments,
- construction engineering (composing buildings!),
- rescue (tunnels, mines, especially snake robots), and last but not least,
- precision farming.

There are many challenges to consider:

- Safety and security, privacy, dependability in general (see articles under 'Generic Challenges')
- Sensors and actuators
- Software development, life cycle issues
- System integration
- Connected vehicles, V2X connectivity
- Cooperative driving and transport systems, systems-of-systems aspects
- New mobility (multi-modality enabled by highly automated/autonomous vehicles)
- Simulation and control
- Verification and validation
- Standardisation
- Situation understanding, cognition, decision making
- Path planning, (precision) maps, localisation and navigation
- Environmental awareness, self-learning,
- Human interaction and (public) acceptance, and
- Societal, ethical and legal aspects.

Connected cooperative autonomous vehicles are adaptive systems-of-systems. In this context, we have to consider several levels of system autonomy:

- the vehicle (robot) as such (level 1, local autonomy, self-dependence),
- the fleet/swarm/ad-hoc group of connected vehicles (level 2, increased amount and chances for information and adaptation of control), and

- the regional/global level 3 (throughput, environmental friendly operation, saving of resources), which needs to be considered for traffic or logistics optimisation or multi-modal transport, for instance.

There is a big difference between development and use in specialised fields of application, where trained operators and/or structured environments are involved (like construction, manufacturing, on-site operations, railways/metros, aircraft and space) and where the general public and public spaces set the requirements (road transport, smart cities/buildings/homes and care). 'Mixed traffic' of autonomous and traditional vehicles is the most demanding scenario, and in urban environments the 'vulnerable road users' (people, bicycles etc.) will still remain as partners. Therefore, the Roadmaps for automated driving foresee five levels of 'take over' from the driver, the highest one being urban traffic. Similar levels are defined for other transport systems like railways and aircraft.

4. Smart Precision farming

Precision farming seems to be of particular interest. European regions with challenges of failing water supplies and climate change as well as environmental challenges (soil cultivation, fertilization, irrigation, plant growth and quality inspection, minimum pesticide disposal). Therefor in particular Southern Europe regions like Spain invest a lot and claim savings of water resources of up to 80% without loss in harvest!

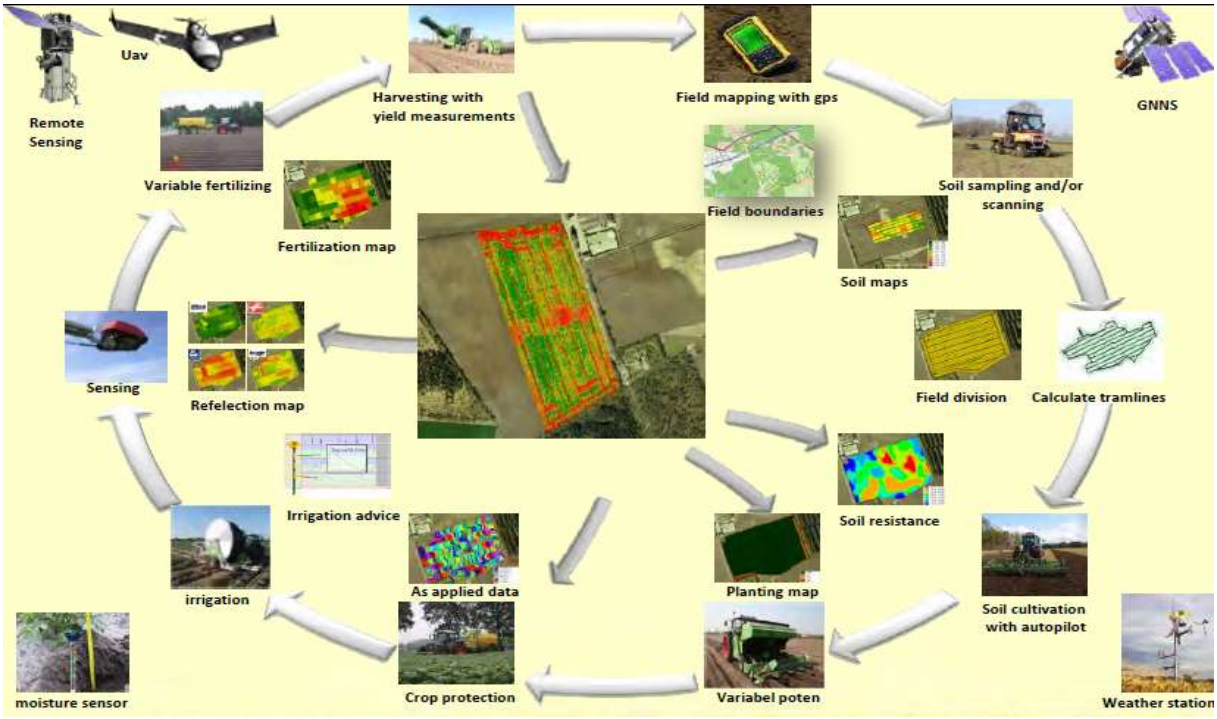

Figure 4: Smart Farming – Impressive Example from van den Borne, Ardappelen (Potatoe Farmer, The Netherlands)

A most impressive example (Figure 4) is from the Netherlands, where even a large number of distributed, not connected fields is managed in an optimal manner by use of many high tech means. Permanently monitoring soil and crop and individually doing variable fertilizing, irrigation and so on, taking into account weather data of the near future, drones, satellite data and highly automated machines for all sort of activities from soil cultivation to harvesting. Even the quality of harvested crop is registered and data sent to the customers, and on the

other hand everything is registered and stored that come as information and goods from suppliers.
In an EC document are stated what the Commission expects from smart farming and precision farming technologies [6]:

- Make farming more transparent to consumers (food security and quality)
- Optimization (precise application of fertilizers, pesticides, irrigation water – positive environmental impact, reduce application of chemicals and antibioticals)
- Reduce environmental footprint (Report of the STOA – Scientific and Technological Options Assessment committee of the European Parliament) – measurable and verifiable by digitisation of agriculture.
- Optimization of the outcome: achieve "more with less"
- Making farming more sustainable
- Collaborative approaches are possible with smart farming: regional and local data required can be provided by farmers' co-operations for all members in a region. Heavy machinery can be shared in such co-operations and supported by NGOs in third world countries – this should help to overcome sever criticism of NGOs (Greenpeace etc.) and the European Environmental Bureau that the technical skills and heavy machine overhead required are a barrier (concentrate smart farming in high-tech countries) and an environmental price tag at the same time.

5. Conclusions

Most of the ideas presented here try to highlight the fascinating opportunities for a better life for all, better and sustainable usage of resources, reduced environmental footprint and so on. Research as described here and funded by the EC and national authorities do explicitly exclude certain applications like military, espionage etc. But we should be aware and take carefully into account that many of the achievements could be used against us as well – drones help with precision farming and building inspection and maintenance, but also as war drones. Robots can help in health (exoskeletons), ageing well etc. by keeping people longer involved and live independently, but also as in science fiction movies shown serve as a robot army. This requires careful international legislation to avoid the worst outcomes of these new technologies, and high public awareness. Politics tend to use safety and security threats as argument for more surveillance and control of people, endangering freedom and democracy.

6. References

[1] Brian A. Primack, Ariel Shensa, et. al., "Social Media Use and Perceived Social Isolation Among Young Adults in the U.S", American Journal of Preventive Medicine, 2017, 4, Elsevier publ.
[2] Jerker Delsing (Ed.), et. al. "IoT Automation – ARROWHEAD Framework", CRC Press, Taylor & Francis, 2017, ISBN 978-1-4987-5675-4
[3] AIoTI – Alliance for Internet of Things Innovation, http://www.aioti.org/resources/
[4] Verizon RISK – 2017 Data Breach Digest Scenario
[5] Van den Borne, Aardappelen, impressive example for Smart Precision Farming, http://www.making-sense.nl/nl/270/making-sense
[6] Sarantis Michalopoulos, EURACTIV.com, Commission: Technology will make farming more transparent to consumers, https://www.euractiv.com/section/agriculture-food/news/commission-technology-will-make-farming-more-transparent-to-consumers/