BEYOND SMART SYSTEMS – CREATING A SOCIETY OF THE FUTURE (5.0) RESOLVING DISRUPTIVE CHANGES AND SOCIAL CHALLENGES

Erwin Schoitsch

AIT Austrian Institute of Technology GmbH (Vienna)
erwin.schoitsch@ait.ac.at

Keywords

Smart Systems, Autonomous Systems, Industry4.0, Systems of Systems, Cyber-physical systems, Internet of Things (IoT), Artificial Intelligence, Society 5.0, Ethical Aligned Design, Sharing Society, Sharing Economy.

Abstract

Smart Systems are today's drivers of innovation, in all industrial and social areas highly automated or autonomous intelligent systems are taking over tasks and services – and maybe, one day, control of our lives. The keynote will address technologies of the fourth industrial revolution in a holistic manner (e.g. IoT, Big Data, Artificial Intelligence, Connectivity, robots) enabling disruptive developments (evolutionary or revolutionary), but also discussing ways they could enable towards a creative, innovative and sustainable sharing society. It will focus on a few areas not covered by other topics of this year's IDIMT, particularly on highly automated systems in transport, smart farming, smart cities and homes, infrastructure, economic systems, and for "inclusion" of elderly or handicapped persons to facilitate longer independent living ("ageing well"). A short critical survey of the Japanese concept of "Society 5.0" will be provided. First approaches of international organizations, e.g. ICT standards organizations, some governments, the European parliament and the UN, are explained on how society and the technical community may meet the rising awareness and ethical concerns, human factors and the like, besides safety, security and resilience and their interplay.

1. Introduction and Overview – Smart Systems Everywhere

Smart things everywhere – an estimate of IDC (International Data Corporation), a worldwide active global provider of market intelligence and advisory services, expects by 2025 that every average person will interact each day many thousand times with a smart device. And smart devices are not just single devices – that would be the conventional way of some equipment used for a particular purpose in an isolated manner with only local intelligence based on some sensors or actors, no, they are connected with systems and systems-of-systems in your environment and to a certain extent even worldwide. The pretended purpose of this high degree of connectivity is to serve customers (peoples) needs for their benefit – but the impact is much higher. Challenges are not only on the technical and usability level, they are on the level of increased risks, threats and vulnerabilities of the systems concerning safety, security and privacy. Last but not least are we afraid of the "transparent citizen", the total surveillance ("Big Brother") like shown in a much simpler and less professional manner in the famous book "1984" by George Orwell; less professional because of lack of the technology that is easily available now.

This will impact considerably our lives and lifestyle, and, as a consequence, we will have to face the new challenges, opportunities and risks. The technological basis is laid by IoT (human – smart devices interaction and communication) and IIoT (IoT in industrial context, machine-to-machine communication) as infrastructure (connectivity), and CPS (Cyber-physical Systems) as "things" or "devices". However, "smart things everywhere" is not just IoT or IIoT, or mobile phones – it means intelligence, cognitive systems and technology, machine learning and artificial intelligence, security, big data and cloud connectivity, involving many domains of everyday life and digital transformation of our world. IDC expects, that AI will be a new standard element in virtually all enterprise and consumer apps and services, including home, health-care, industry and transport as well, and that AI capabilities being used today are only one-third of what will be available over the next five years.

Cognitive technologies for smart systems include particularly:

- Cognitive decision and self-organizing systems,
- Swarm intelligence
- Cognitive technologies to create applicable information from big data generated by massively deployed smart things,
- Embedded, distributed and resource-aware machine learning of IoT and IIoT devices and systems

With respect to safety, cybersecurity, privacy, and data sovereignty, these cognitive technologies are a severe concern for specialists, politicians and citizens, and raise severe ethical and societal concerns.

Smart Systems are digitalized – and part of the so-called "Digital Transformation". This covers all aspects of economy, industry and living, examples are (without prioritization):

- Smart Production/Manufacturing,
- Smart Health,
- Smart Mobility,
- Smart Farming,
- Smart Energy,
- Smart Critical Infrastructures
- Smart Cities/Homes/Buildings,
- Smart Construction (of buildings by smart machines and robots)
- Smart Living for Ageing Well,
- Smart Wearables (for health, comfort, security, particular services),
- Smart Water or Waste Management, etc.

2. Smart Systems Everywhere – Research and Standardization Efforts

In all technological and industrial advanced regions of our world, research and innovation in this field are considered essential and a lot of money is invested by governments and industry (and, not to forget, military). On European level, organizations like AIOTI [AIOTI], the Alliance for Internet

of Things Innovation, which takes care of the IoT aspects in 13 Working Groups, or the industrial associations ARTEMIS [ARTEMIS] (Advanced Research and Technology on Embedded Intelligent Systems), EPoSS [EPoSS] (European Technology Platform for Smart systems Integration) and AENEAS (Association for European Nano-Electronics Activities), which are the private partners in the ECSEL Joint Undertaking, a European PPP within Horizon 2020 (Public-Private Partnership) with an industry-oriented Research Program, and other PPPs, take care of further development of research, standardization and promotion of these topics, together with the European Commission and national funding authorities. China is already keeping up with Europe, US and Japan, e.g. with its AI initiative and strategy.

The digital transformation of European business and society is a major goal of the EC. EC Growth, the DG (Directorate General) for Internal Market, Industry, Entrepreneurship and SMEs, considers digital transformation as a key element for European growth, because Europe can build on its strength in traditional sectors and can take up the potential and challenges of advanced digital technologies. Technologies considered in this context are IoT, big data, advanced manufacturing, robotics, 3D printing, blockchain technologies and artificial intelligence (see European Commission, 2018).

The initiative "Digitizing European Industry" targets to meet Europe's needs to join forces under a common strategy that takes digitalization of the EU's economy forward in order to unlock the full potential of the 4th industrial revolution. The pillars of this initiative are:

Figure 1: Pillars of the European Initiative "Digitizing European Industry"

Source: https://ec.europa.eu/digital-single-market/en/pillars-digitising-european-industry-initiative

In the booklet "My agenda for Europe" of Ursula von der Leyen, the new President of the European Commission, is one chapter dedicated to "A Europe fit for the digital age". It focuses on AI, IoT, 5G, and ethical and human implications of these technologies, empowering people through education and skills, and on protecting ourselves with respect to the risks of these technologies.

DG CONNECT, DG for Communications Networks, Content and Technology, has a strong focus on "Digitalization of European Industry", with the pillars IoT (physical meets digital), Big Data (value from knowledge) and AI and Autonomous Systems (which is somehow a revival of AI in a new context and now considered as the "next digital revolution"). The links between technologies are shown in [European Commission, 2017b].

Additionally, DG Growth delivers an annual report on standardization, e.g. the "Rolling Plan on ICT Standardization", which includes most of the relevant areas in this paper's context and is a key pillar in Digitalization, and have started a Joint Initiative on Standardization (JIS) http://ec.europa.eu/growth/single-market/europeanstandards/notification-system_en, although they do primarily consider the European SDOs (Standardization Organizations, ESOs) CEN, CENELEC and ETSI.

On international level, the large standardization organizations ISO and IEC have joined forces in many respects. One the one hand, in the Joint Technical Committee 1 (ISO/IEC JTC1, Information Technology), starting several new or extending existing Subcommittees, e.g. JTC1 SC41 (Internet of things and related technologies, which covers also wearables and sensor networks), JTC1 SC42 (Artificial intelligence, which covers also Trustworthiness in AI, Bias in AI, Risk Management of AI, Big Data and Algorithms), JTC1 SC 38 (Cloud computing and distributed platforms), JTC1 SC 27 (Information security, cybersecurity and privacy protection), WG 11 (Smart Cities) or AG 6 (Autonomous and Data Rich Vehicles) and AG 11 (Digital Twin). On the other hand, they have installed coordination groups on several topics, e.g. Smart Manufacturing, Ethical considerations, or Focus Groups like CEN/ETSI/CENELEC on AI, or ITU/WHO (International Telecommunication Union/World Health Organization) on "AI for Health". In some sectors, like ISO TC 22, Road vehicles, many standards are arising on automotive safety, cybersecurity engineering, extended Vehicle standards (connectivity, V2I, V2V), and a Roadmap towards "Automated Driving" is developed in coordination with various related ISO subcommittees and SAE (Society of Automotive Engineers, US) by an Ad-hoc Group AG1 (ADAG – Automated Driving Ad-hoc Group). In IEC TC 65 (Industrial-process measurement, control and automation), a new focus is on "Smart Manufacturing", including Joint Working Groups with ISO TC 184 (Automation and Integration).

An overview over the rich landscape of standards and standardization organizations (SDOs) in an ordered manner (domains and generic/horizontal standards) is provided by Figure 2:

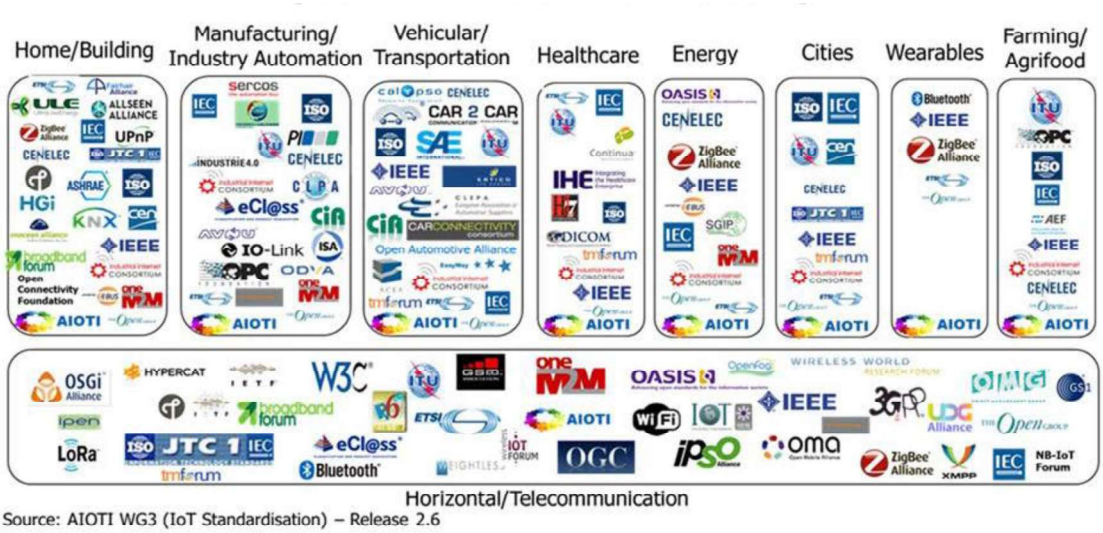

Figure 2: AIOTI Standardization landscape, ordered overview (Source: ETSI 2016a)

3. Autonomous Systems, CPS and IoT as Drivers for Digitalization

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, (cyber-)security, maintainability, but additionally resilience, robustness, sustainability, etc.) in a holistic manner becomes an important issue, despite emergent behaviors and critical interdependencies.

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. Movies from YouTube are often informative or funny, but on the other hand anybody can upload nonsense, lies and conspiracy theories, which already without the seemingly plausibility of a movie were dangerous in the past (see Wikipedia https://en.wikipedia.org/wiki/Conspiracy_theory). There are studies [Primack, 2017], 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, and countermeasures are often impossible – "the net never forgets" (which is a basic property in Blockchain!), as Facebook has proven, although it was illegal according to European Privacy Laws not to delete completely contents everywhere if the generator wants to have deleted it. And anyway, you cannot delete illegal or fake contents that has been downloaded already by users.

Autonomous systems have a property that is new to ICT systems – they have to decide on basis of data provided to them based on algorithms (particularly neural networks, big data, and AI methods), where predictability of dependability properties (safety, security, resilience) is not possible today or difficult to prove. The dependability of results of such decisions is a major obstacle to implementation of fully autonomous systems without human control – and liability issues are difficult to handle in a fair manner. This raises severe ethical questions as well, additionally to all technical questions, – how to decide in a no-win situation? A few principles and recommendations will be discussed later under "Ethical considerations".

A critical part of the AI game is "Machine Learning". ISO/IEC JTC1 SC42 ("Artificial Intelligence") has started a New Standardization Work Item (NP AWI 23053) "Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)". This is a first approach to provide some structure to such systems; the resulting Specification or Standard should be the starting point for further work towards safety and security considerations of such systems, and include later on ethical considerations as well (WG 3 on "Trustworthiness of AI").

Here again we have to take into account that existing standards and certification procedures do not fit. We have to "re-think" standardization and certification, and recent research projects in ECSEL JU (see acknowledgements) like the "lighthouse" projects Productive 4.0 (Industry4.E) and AutoDrive (Mobility.E) have set the goal to promote work in that direction. Related projects like SECREDAS, AMASS, AQUAS, and now iDev40 or even AfarCloud in the Smart farming sector, will be invited to participate in the "lighthouse initiatives" to provide synergies in a larger context to promote digitalization/digital transformation in these sectors.

Originally, communication and connectivity included 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).

AIOTI [3], the Alliance for Internet of Things Innovation, 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. 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 its own vending machines! One rather new attack-type are ransomware attacks encrypting the users disk and blackmailing the owner.

Another key issue are interoperability of protocols, data and semantic interoperability, and security – therefore the AIOTI Standardization WG issued several reports and is very active because of the importance of standardization for huge IoT systems with many interfaces and "things". Standardization as such is done via ETSI [ETSI] as supporting standardization organization (SDO). 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. (see Figure 2).

4. Evolutions in Industry, Automated Driving - and Society

Europe has focused very much on the "Industry 4.0" aspect (somehow driven by Germany's "Industrie 4.0") in driving the Digitalization, and mainly from the economic/manufacturing/ competition point of view. The "generation aspect" can be observed in all contexts of evolutions (revolution is just a term describing when the evolution leads to a dramatic fast change of the situation with disruptive consequences for people, society and economy).

The stages of evolution from Industry 1.0 to Industry 4.0 over time are characterized by the means and processes typical for a longer period of time (see Figure 3):

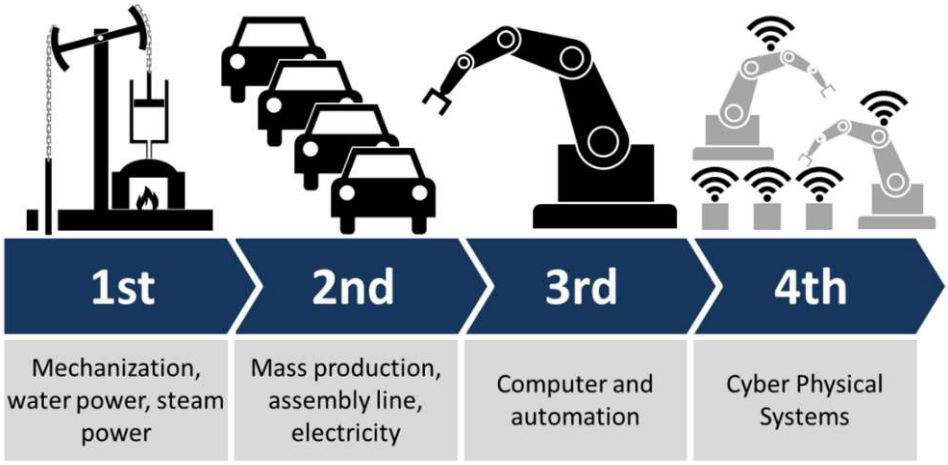

Figure 3: Industrial evolution over time: 18th-19th century (1), 19th-20th century (2), 1970+ (3), today (4)

Source: Christoph Roser at AllAboutLean.com, Creative Commons Attribution-Share Alike 4.0 International license

The change from one stage to the next higher stage was often accompanied by severe consequences for people and society – jobs were lost or changed dramatically, social instabilities, threats to people and environment followed, and in many cases the situation became disastrous for masses of citizens as "losers" of the changes. Only when social systems were introduced in time, the effects could be buffered to avoid catastrophic situations for the society.

Highly automated systems in a stable society under socially compliant conditions have a good chance to lead to benefits for all in the end – but politics has to be careful to avoid too much inequality of distribution of benefits from the opportunities achieved by automation. The threats of digitalization are not only in economic change – it may endanger our democracy, citizens independence and freedom we have fought for more than 200 years now!

Automated Driving is a particular result of the technology-driven evolution in our society: The goal of "Zero Accidents", as announced by the EC when introducing the automated driving programs, is only one side of the coin: besides clear benefits for health and environment, there may be a disruptive change in transport, affecting not only taxi drivers, but also public transport, vehicle sales, the whole vehicle market, etc. We have still some time to adapt – and large OEMs are already planning ahead towards a future where managing fleets of autonomous vehicles used on demand only may become a major business case. One key issue, that the autonomous vehicles should mainly be used for the "last mile" or remote country side, to reach the next more efficient and environmentally sustainable public transport means, e.g. high- speed trains, was not very often mentioned in the "green transport scenarios" or research projects.

From Horse Power to Driverless Vehicles: The Road to Automated Driving, Vienna Convention, 1968, Article 8:

- Every moving vehicle or combination of vehicles shall have a driver.
- Every driver shall at all times be able to control his vehicle or to guide his animals.

Remark: Horses find their home "autonomous" – nothing new, take-over from driver automatically!

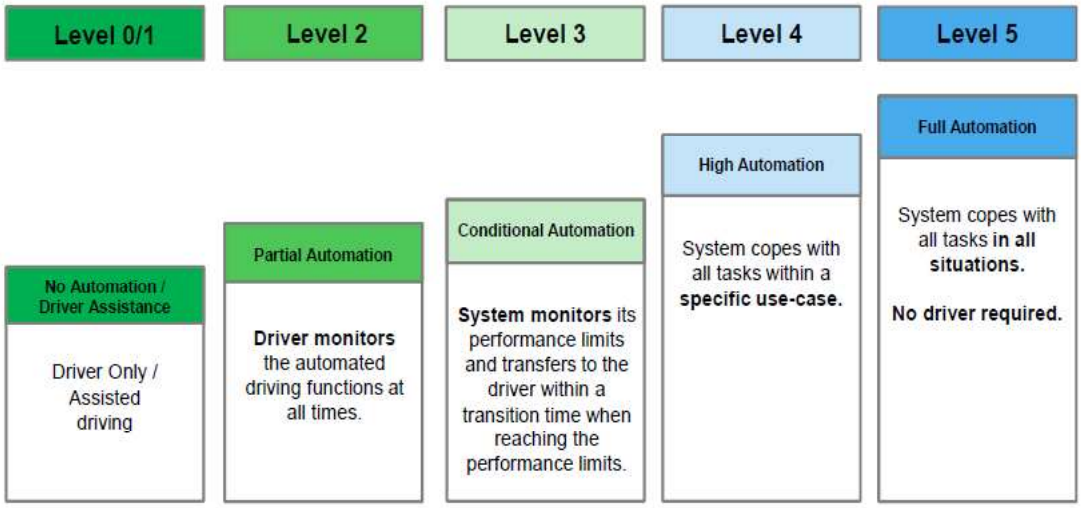

Figure 4: Source: SAE (Society of Automotive Engineers, USA) – Levels of Automation for Automated Driving

The best automation levels reached in practice are 2 -3 at the moment. Test vehicles claiming higher levels at least under certain conditions are at the moment not allowed to drive autonomously without a responsible, trained driver (see GOOGLE car accident and TESLA crash) as a fall-back solution. Especially critical is considered the "mixed mode" situation – non-automated and autonomous vehicles interfering, and additionally in urban environments VRUs sharing the road (cycles, pedestrians, …). Therefore, several organisations tried to establish rules on "Intelligent transport systems and automated driving" (e.g. UNECE ITS/AD).

But what about human society? – The Japanese Strategy Society 5.0

5. Society 5.0 – Aiming for a New Human-Centred Society

There are far reaching concepts implemented around us with the "Smart Systems Everywhere". On the other hand, all technologically and economically highly developed countries face chronic social challenges, which add up to the challenges and risks impacted by all the "4.0" revolutions to people and society.

The Japanese strategy "Society 5.0" envisions a so-called "Super-Smart Society". It should create a sustainable, inclusive socio-economic system, powered by the achievements of the fourth industrial revolution and the digital technologies. It leads far beyond Industry 4.0, it aims at benefitting the whole society by utilizing the integration of cyberspace and physical space [UNESCO 2019]. It is fully supported by government and industry to revitalize Japan, an extremely aging society with shrinking work force [Japan Business Federation, 2016, 2017] [Japanese Government, 2017, 2018].

Evolution of Human Society over time:

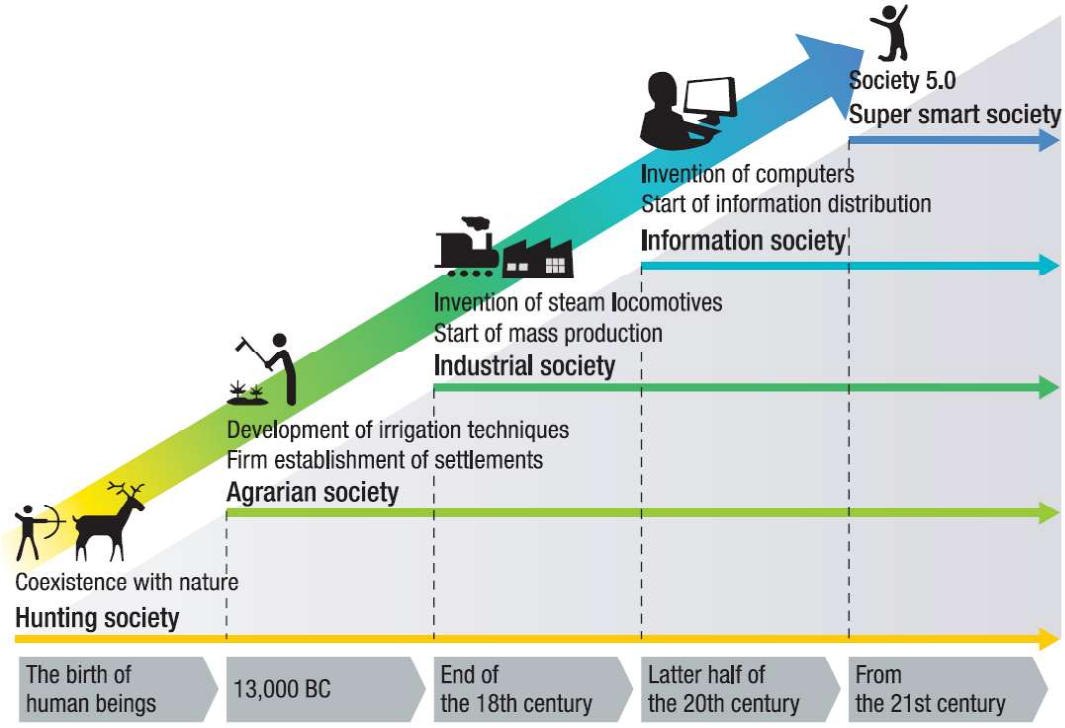

Figure 1: Evolution of Human Society towards Society 5.0 (Source: Mayumi Fukuyama (2018))

The documents on their vision say (citation from [Japanese Government, 2017])

"We aim at creating a society where we can resolve various social challenges by incorporating the innovations of the fourth industrial revolution (e.g. IoT, big data, artificial intelligence (AI), robot, and the sharing economy) into every industry and social life. By doing so the society of the future will be one in which new values and services are created continuously, making people's lives more conformable and sustainable.

This is Society 5.0, a super-smart society. Japan will take the lead to realize this ahead of the rest of the world."

The concept of "Society 5.0" was drafted in the 5th Science and Technology Basic Plan by the Council for Science, Technology and Innovation 2016.

Key issues of this plan are sustainability and social benefit for all citizen ("inclusion") by utilizing the advanced opportunities of Digital Transformation and Smart Technologies. Social reform (innovation) will achieve a forward-looking society that breaks the existing stagnation in societal and economic stagnation, forming a society of mutual respect, transcending the generations, and a active and enjoyable life for every person. This concept should also face challenges on a global scale, like depletion of natural resources, global warming, growing economic disparity, and even terrorism, by sharing knowledge and information, and cooperation.

From a moral and ethical point of view, this sounds extremely well. The question that arises if it fits to other kinds of societies and regions in the world, having different social and economic preconditions, and different long-standing cultures and mind sets. From experience in history we know, that the fantastic technologies and opportunities can be misused by some people, criminals or governments against citizens. Therefore, in Europe, which is by far not so homogeneous in culture and mutual influences of neighbours as Japan, and America, institutions of different type have tried to set up ethical guidelines in the field of automated systems, cognitive decision taking (AI), and governance of data and connectivity.

6. Ethics Guidelines

6.1. Ethics Commission for Automated Driving (German Federal Ministry of Transport and Digital Infrastructure)

Automotive is a real mass market, and the trend towards highly automated and autonomous driving is ongoing in research and development. On the one hand, it is rather simple compared to complex AI issues and cognitive decision in achieving transparency in self-learning systems in detail (which is not possible at the moment), but even high-level principles are interesting.

The German document (available in English) [German Federal Ministry, 2017], includes a punctuation of 20 ethical rules for automated and connected vehicular traffic (shortened):

- The primary purpose of partly and fully automated transport systems is to improve safety for all road users. Another purpose is to increase mobility opportunities and to make further benefits possible. Technological development obeys the principle of personal autonomy, which means that individuals enjoy freedom of action for which they themselves are responsible.
- The protection of individuals takes precedence over all other utilitarian considerations. The objective is to reduce the level of harm until it is completely prevented. The licensing of automated systems is not justifiable unless it promises to produce at least a diminution in harm compared with human driving, in other words a positive balance of risks.
- The public sector is responsible for guaranteeing the safety of the automated and connected systems introduced and licensed in the public street environment. Driving systems thus need official licensing and monitoring. The guiding principle is the avoidance of accidents, although technologically unavoidable residual risks do not militate against the introduction of automated driving if the balance of risks is fundamentally positive.
- The personal responsibility of individuals for taking decisions is an expression of a society centered on individual human beings, with their entitlement to personal development and their need for protection. The purpose of all governmental and political regulatory decisions is thus to promote the free development and the protection of individuals. In a free society, the way in which technology is statutorily fleshed out is such that a balance is struck

between maximum personal freedom of choice in a general regime of development and the freedom of others and their safety.

- Automated and connected technology should prevent accidents wherever this is practically possible. This includes dilemma situations, in other words a situation in which an automated vehicle has to "decide" which of two evils. In this context, the entire spectrum of technological options should be used and continuously evolved. The significant enhancement of road safety is the objective of development and regulation, starting with the design and programming of the vehicles such that they drive in a defensive and anticipatory manner, posing as little risk as possible to vulnerable road users.
- The introduction of more highly automated driving systems, especially with the option of automated collision prevention, may be socially and ethically mandated if it can unlock existing potential for damage limitation. Conversely, a statutorily imposed obligation to use fully automated transport systems or the causation of practical inescapabilty is ethically questionable.
- In hazardous situations that prove to be unavoidable, despite all technological precautions being taken, the protection of human life enjoys top priority in a balancing of legally protected interests. Thus, within the constraints of what is technologically feasible, the systems must be programmed to accept damage to animals or property in a conflict if this means that personal injury can be prevented.
- Genuine dilemmatic decisions, such as a decision between one human life and another, depend on the actual specific situation, incorporating "unpredictable" behavior by parties affected. They can thus not be clearly standardized, nor can they be programmed such that they are ethically unquestionable. It is true that a human driver would be acting unlawfully if he killed a person in an emergency to save the lives of one or more other persons, but he would not necessarily be acting culpably. It would be desirable for an independent public-sector agency (for instance a Federal Bureau for the Investigation of Accidents Involving Automated Transport Systems or a Federal Office for Safety in Automated and Connected Transport) to systematically process the lessons learned.
- In the event of unavoidable accident situations, any distinction based on personal features (age, gender, physical or mental constitution) is strictly prohibited. It is also prohibited to offset victims against one another. General programming to reduce the number of personal injuries may be justifiable. Those parties involved in the generation of mobility risks must not sacrifice non-involved parties.
- In the case of automated and connected driving systems, the accountability that was previously the sole preserve of the individual shifts from the motorist to the manufacturers and operators of the technological systems and to the bodies responsible for taking infrastructure, policy and legal decisions.
- Liability for damage caused by activated automated driving systems is governed by the same principles as in other product liability.
- The public is entitled to be informed about new technologies and their deployment in a sufficiently differentiated manner.
- The complete connectivity and central control of all motor vehicles within the context of a digital transport infrastructure is ethically questionable if, and to the extent that, it is unable to safely rule out the total surveillance of road users and manipulation of vehicle control.

- Automated driving is justifiable only to the extent to which conceivable attacks, e.g. manipulation of the IT system or innate system weaknesses, do not result in such harm as to lastingly shatter people's confidence in road transport.
- Permitted business models that avail themselves of the data that are generated by automated and connected driving and that are significant or insignificant to vehicle control come up against their limitations in the autonomy and data sovereignty of road users. It is the vehicle keepers and vehicle users who decide whether their vehicle data that are generated are to be forwarded and used.
- No abrupt handover of control to the driver ("emergency"): To enable efficient, reliable and secure human-machine communication and prevent overload, the systems must adapt more to human communicative behaviour rather than requiring humans to enhance their adaptive capabilities.
- It must be possible to clearly distinguish whether a driverless system is being used or whether a driver retains accountability with the option of overruling the system. The distribution of responsibilities (and thus of accountability), for instance with regard to the time and access arrangements, should be documented and stored. This applies especially to the human-to-technology handover procedures.
- In emergency situations, the vehicle must autonomously, i.e. without human assistance, enter into a "safe condition". Harmonization, especially of the definition of a safe condition or of the handover routines, is desirable (standardization).
- Learning systems that are self-learning in vehicle operation and their connection to central scenario databases may be ethically allowed if, and to the extent that, they generate safety gains. Self-learning systems must not be deployed unless they meet the safety requirements regarding functions relevant to vehicle control and do not undermine the rules established here. It would appear advisable to hand over relevant scenarios to a central scenario catalogue at a neutral body in order to develop appropriate universal standards, including any acceptance tests.
- The proper use of automated systems should form part of people's general digital education. The proper handling of automated driving systems should be taught in an appropriate manner during driving tuition and tested.

6.2. Trustworthy AI (Highly Automated systems in General)

Here is only a short overview on a few AI-related documents on "Trustworthy AI" and Ethical Guidelines for "Smart Systems' Decision Taking" provided:

- The IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems (AI/AS) (April 2016)
    - Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems (EAD V1 released)
    - Identification and recommendation of ideas for Standards Projects focused on prioritizing ethical considerations in AI/AS.
    - IEEE ECAIS "Ethics Certification for Autonomous and Intelligent Systems" (Industry Connections Activity Initiation Sept. 2018!).
- IEC/SMB Ad Hoc Group on autonomous systems and ethics (AHG 79) (ISO/TC299, June 20, 2018!!), scope commitment:

- SMB (Standardization Management Board) agreed to setup AHG 79, Autonomous Systems – Ethics, with the task of assessing the role of IEC and standards in addressing ethics, trust and values particularly in autonomous systems, and making recommendations. The review should consider the work of JTC 1/SC 42 (Artificial Intelligence), ACART (Advisory Committee on Applications of Robot Technology), ACOS (Advisory Committee on Safety), TC 59 (Performance of household and similar electrical appliances), TC 100 (Audio, video and multimedia systems and equipment), SyC AAL (Systems Committee on Active Assisted Living), SyC Smart Cities, IEEE, ISO and others.
- "When Computers Decide" – European Recommendations on Machine Learned Automated Decision Making (Informatics Europe & EUACM 2018) includes Technical, Ethical, Legal, Economic, Societal and Educational recommendations)
- EC: "Ethics Guidelines for Trustworthy AI" (Final report April 2019, HLEG AI) https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
- ISO/IEC JTC1 SC42 (Artificial Intelligence): TECHNICAL MANAGEMENT BOARD RESOLUTION 53/2018: Approval of the inclusion of certain aspects of 'societal concerns' in the ISO/IEC JTC1/SC 42 programme of work.

7. Conclusions

The technologically oriented funding organizations and the EC have a very positive approach and high expectations concerning the benefits of digitisation of economy, industry and society. They highlight the fascinating opportunities for a better life for all, better and sustainable usage of resources, reduced environmental footprint, and of course economic competitiveness for European industry. The Japanese approach to "Society 5.0" even goes far beyond Industry 4.0, and the visionary declarations are of high ethical and moral value. Applications like military, espionage etc. are explicitly excluded in Research here. However, we should be aware that many of the achievements could be used against us as well (and some research projects consider this fact already) – drones help with precision farming, and building inspection and maintenance, but also as war drones. Robots can help in health (exoskeletons), ageing well, rescue and maintenance actions, etc. by saving peoples life or keeping people to live longer independently, but also serve as a robot army. Knowledge and information can build a better society, but also be used against you by criminals or organizations. This requires careful European and international legislation and control to avoid the worst outcomes of these new technologies, and requires high public awareness. Politics sometimes tend to use safety and security threats as argument for more surveillance and control of people, endangering freedom and democracy. A first approach is taken by several authorities and international or governmental organisations to provide guidelines and recommendations for an ethical approach to highly autonomous systems.

8. Acknowledgements

Part of the work received funding from the EC under grant agreement n° 645149 (CP-SETIS), from the EU ARTEMIS/ECSEL Joint Undertaking under grant agreement n° 692474 (AMASS), and from both, the EC ECSEL JU and the partners' national funding authorities (in Austria FFG (Austrian Research Promotion Agency) on behalf of BMVIT, The Federal Ministry of Transport, Innovation and Technology) - (Grant agreements n° 692455-2 (ENABLE-S3), n° 737475-2 (AQUAS), n° 737459-2 (Productive4.0) and n° 737469-2 (AutoDrive) and SECREDAS (783119), iDev40 (783163) and AfarCloud (783221)).

9. References

URL-Links were valid July 23, 2019.

AIOTI – Alliance for Internet of Things Innovation, http://www.aioti.org/resources/

ARTEMIS Strategic Research Agenda 2016, ARTEMIS Industrial Association, Eindhoven, NL.

Delsing, J. (Ed.), et. al. (2017). "IoT Automation – ARROWHEAD Framework", CRC Press, Taylor & Francis, 2017, ISBN 978-1-4987-5675-4

ECSEL Austria, bmvit, ITS Austria, austriatech, A3PS, Austrian industry, research and academia: Austrian Research, Development & Innovation Roadmap for Automated Vehicles, 2016.

EPoSS Strategic Research Agenda of the European Technology Platform on Smart Systems Integration, 2017. http://www.smart-systems-integration.org/public/documents/publications/EPoSS_SRA2017.pdf/view

ETSI TR 103 375, (2016a). SmartM2M: IoT Standards landscape and future evolutions.

ETSI TR 103 376, (2016b). SmartM2M - IoT LSP use cases and standards gaps (2016).

European Commission, (2017a). White Paper on the Future of Europe, Brussels, European Commission (https://ec.europa.eu/commission/sites/beta-political/files/white_paper_on_the_future_of_europe_en.pdf)

European Commission, (2017b). "Digitising European Industry – Digital Industrial Platforms", Final Version, Aug. 2017, https://ec.europa.eu/futurium/en/system/files/ged/dei_wg2_final_report.pdf

European Commission, (2018). "Digitising European Industry – Two years after the launch of the initiative", Brochure March 2018, ISBN 978-92-79-80325-3, doi:10.2759/024187 https://ec.europa.eu/digital-single-market/en/news/digitising-european-industry-2-years-brochure

European Commission, (2019). Ethics Guidelines for Trustworthy AI, EC, High Level Expert Group on AI, April 2019, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

German Federal Ministry of Transport and digital Infrastructure, (2017). Ethics Commission on Automated and Connected Driving – Report June 2017 (Extract)

https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission-automated-and-connected-driving.pdf?__blob=publicationFile

Greenberg, A. (2017). „How an Entire Nation became Russia's Test Lab for Cyberwar", WIRED, Security, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine?mbid=nl_62017_p1&CNDID=49159081

Heindl, P. & Damm, W. (Eds.), (2016). SafeTRANS Working Group "Highly automated Systems: Test, Safety, and Development Processes", Recommendations on Actions and Research Challenges, 2016, http://www.safetrans-de.org/en/Latest-reports/index.php#latest-reports

i-SCOOP, (2016). From Industry 4.0 to Society 5.0: the big societal transformation plan of Japan, https://www.i-scoop.eu/industry-4-0-society-5-0/

Japan Business Federation (Keidanren), (2016). Toward realization of the new economy and society - Reform of the economy and society by the deepening of "Society 5.0", http://www.keidanren.or.jp/en/policy/2016/029_outline.pdf

Japan Business Federation (Keidanren), (2017). Revitalizing Japan by Realizing Society 5.0, http://www.keidanren.or.jp/en/policy/2017/010_overview.pdf

Japanese Government, Cabinet Office (2018), Achieving Society 5.0, https://www8.cao.go.jp/cstp/english/society5_0/index.html

Japanese Government, (2017). Realizing Society 5.0. https://www.japan.go.jp/abenomics/_userdata/abenomics/pdf/society_5.0.pdf

Mayumi Fukuyama, (2018). Society 5.0: Aiming for a New Human-Centered Society, Japan Spotlight, July/August 2018, p. 47-50.

Mobility4EU, (2016). Action Plan for Future Mobility in Europe (Horizon 2020 Coordination and Support Action 2016-2018), http://www.mobility4eu.eu/

Özgür Önday, (2019). Japans Society 5.0 – Going beyond Industry 4.0, https://www.researchgate.net/publication/330500307_Japan%27s_Society_50_Going_Beyond_Industry_40

Primack, B. A. & Shensa, A. et. al., (2017). "Social Media Use and Perceived Social Isolation Among Young Adults in the U.S", American Journal of Preventive Medicine, 2017, 4, Elsevier publ.

Prime Minister's Office of Japan, (2019). Society 5.0,

Concept, https://www.youtube.com/watch?v=SYrv6kOsU1o

Highlights, https://www.youtube.com/watch?v=S9JMuwvzz8g

Human Ability, https://www.youtube.com/watch?v=odjuqbLJRMY

Schoitsch, E. & Niehaus, J. (2017a). Strategic Agenda on Standardization for Cyber-Physical Systems, CP-SETIS (EC Horizon 2020 project n° 645149), publ. by ARTEMIS-IA, Eindhoven, 2017, ISBN 978-90-817213-3-2.

Schoitsch, E. (2017b). „Smart Systems Everywhere – how much Smartness is tolerable?", IDIMT 2017, Proceedings, p. 361-373, Trauner Verlag, Reihe Informatik 46, 2017.

Schoitsch, E. (2018). "Smart Systems Everywhere – Intelligence, Autonomy, Technology and Society", IDIMT 2018, Proceedings, p. 153-165, Trauner Verlag, Reihe Informatik 47, 2018.

UNECE Regulation April 17, 2014, Amendment to Article 8, §5 and to Article 39, §1, to the Vienna Convention 1968 and the Global Technical Regulations for wheeled Vehicles, Geneva June 25, 1998. https://www.unece.org/fileadmin/DAM/trans/doc/ 2014/wp1/ECE-TRANS-WP1-145e.pdf

UNESCO (2019). Japan pushing ahead with Society 5.0 to overcome chronic social challenges, https://en.unesco.org/news/japan-pushing-ahead-society-50-overcome-chronic-social-challenges

Von der Leyen, U. (2019). A Union that strives for more – My agenda for Europe. https://www.europarl.europa.eu/resources/library/media/20190716RES57231/20190716RES57231.pdf

Verizon RISK – 2017 Data Breach Digest Scenario