Smart Systems Everywhere – Intelligence, Autonomy, Technology and Society

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 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 integrated into every day devices. Comfort, health, services of all kinds, safety, security and privacy of people depend increasingly on these. The challenges have been e.g. taken up by AIOTI, the Alliance for Internet of Things Innovation, or ARTEMIS, EPoSS and AENEAS, the three industrial associations in the ECSEL Joint Undertaking, with an industry-oriented European Research Program, and many national programs, e.g. by BMVIT (Austrian Ministry of Transport, Innovation and Technology). Highly automated or autonomous smart interacting systems are becoming the main drivers for innovations and efficient services. The impact on society and economy is tremendous and will change our way of living and economy in a disruptive manner, and we will face not only benefits but also new hazards and risks. Dependability (safety, reliability, availability, security, maintainability, resilience, etc.) in a holistic sense becomes an important issue. Artificial Intelligence, Machine Learning, Big Data and open, adaptive systems in a rather unpredictable environment are key challenges for systems of systems.

The paper will try to provide an overview not primarily on technological but also on some economic, societal and ethical aspects of highly automated and autonomous system in a changing world, hopefully better than the "Brave New World" of Aldous Huxley or "1984".

1. Introduction – Smart Systems as Key Elements of Digital Transformation

Smart Anything Everywhere – that is the new hype on IoT, Internet of Things, combined with Intelligence, Autonomy and Connectivity. Smart Systems are digitalized – and part of the progressing trend towards a digitalized world, 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,
- Smart Water Management, or even so curious ideas like
- Smart Food Production (e.g. by 3D-Printing!)
- Etc.

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 components and systems, leads to this world of "Internet of Things", and in the last consequence, to "Smart Anything Everywhere". On European level, organizations like AIOTI [3], the Alliance for Internet of Things Innovation, which takes care of the IoT aspects in 13 Working Groups, or the industrial associations ARTEMIS [10] (Advanced Research and Technology on Embedded Intelligent Systems), EPoSS [9] (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 and tri-partite Funding Programme, take care of further development of research, standardization and promotion of these topics, together with the European Commission and national funding authorities (therefore "tri-partite").

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, Enterpreneurship 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 [16], European Commission, "Digitising European Industry – Two years after the launch of the initiative"). 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, comprising

- Awareness, Education and Understanding about the European Standardization System i.e. increasing the use of standards and participation in the process at all levels
- Coordination, Cooperation, Transparency, Inclusiveness, i.e. ensuring adequate, high-quality, user-friendly and timely European standards
- Competitiveness and International dimension, i.e. standards supporting European competitiveness in the global markets.

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 Figure 1 (Source: [17] European Commission, "Digitising European Industry – Digital Industrial Platforms", Final Version, Aug. 2017).

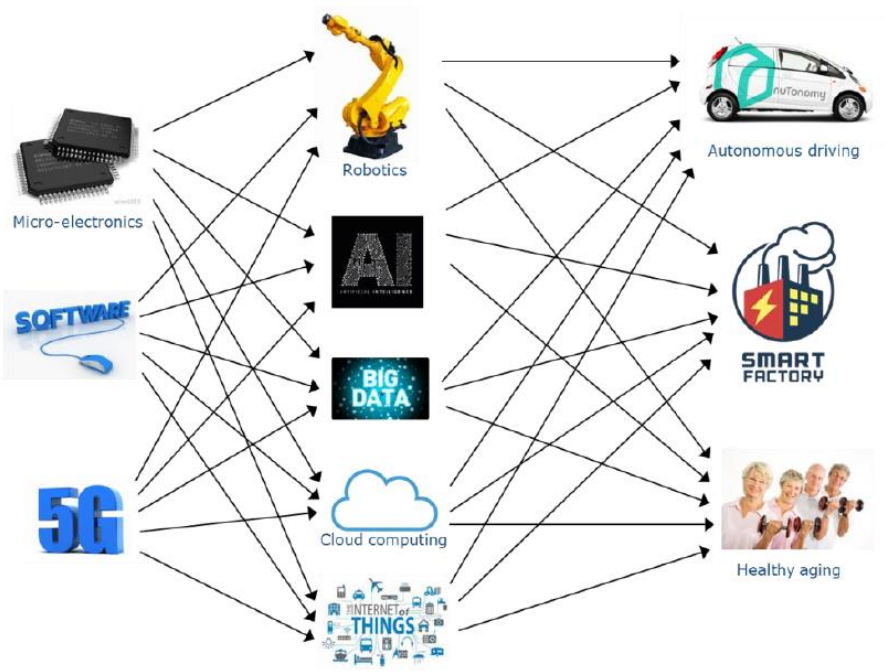

Figure 1: Links between technologies (source: European Commission, "Digitising European Industry – Digital Industrial Platforms", Final Version, Aug. 2017

In many European countries, many related initiatives have been started (see Figure 2)

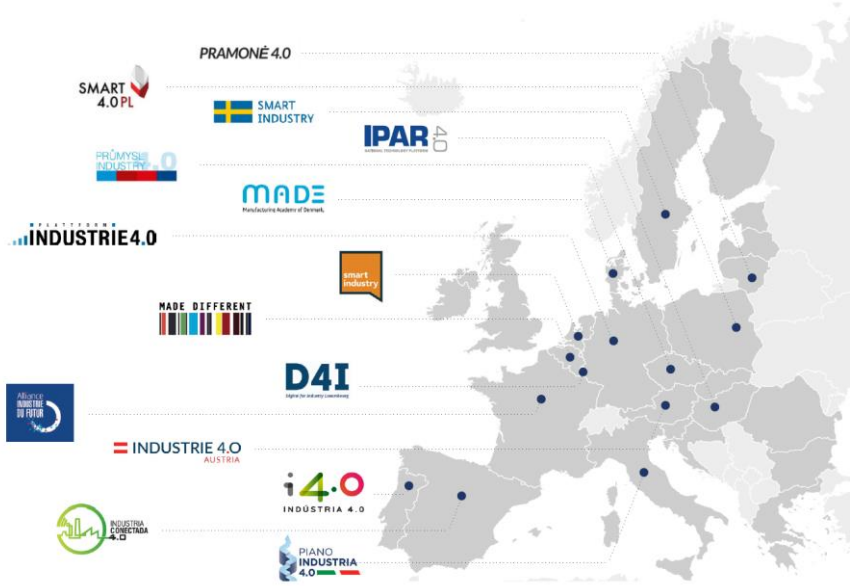

Figure 2: National initiatives for Digitizing European Industry in EU (Source: [16] EC, "Digitising European Industry – Two years after the launch of the initiative", Brochure March 2018)

2. Highly Automated/Autonomous Systems – Challenge for our Future

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”, which is not per se “knowledge”, but nevertheless 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 to 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. 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 [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, and countermeasures are often impossible – “the net never forgets”, 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.

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? Several models have been discussed, some ideas are:

- Model the average human behavior (whatever this means)
- Define priorities whom to protect (e.g. the people in the autonomous vehicle, or the VRUs (vulnerable road users) like cyclists or pedestrians)
- To put liability on the designer of the rules or software (the “programmer”)

Each of these proposed solutions has drawbacks. A few principles and recommendations will be discussed later under “Ethical considerations”. Anyway, there are challenges beyond the purely technical questions – they have severe societal and legal impact, and a joint international approach would be appreciated to serve people with products and solutions that can be well accepted all over the world.

A critical part of the AI game is “Machine Learning”. ISO/IEC JTC1 SC42 (“Artificial Intelligence”) has recently 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. The framework provides in the first draft some process model for ML which particularly looks at the “training” perspective of such systems. I want to emphasize that these are initial considerations and not a final document, but at least for the discussion at this conference it seems to be a worthwhile input. It is important to notice that the semiconductor industry has already taken up some ideas, the most important one being the idea that a well training neural network as AI component should be validated and then put into silicon – a module representing some behavior like a “basic instinct” in nature (“reflex”) (see Figure 3).

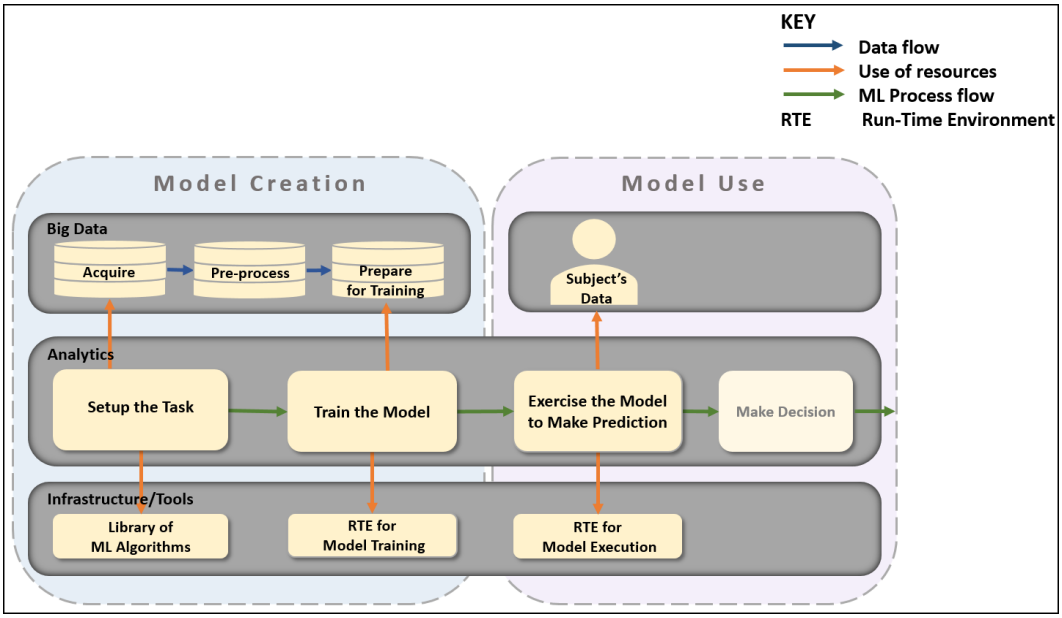

Figure 3: Typical Process for a ML Subsystem (from [21] ISO/IEC JTC 42, Artificial Intelligence, AWI 25053)

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 Industry4.E Productive 4.0 and Mobility.E AutoDrive have set the goal to promote work in that direction. Related projects like SECREDAS, AMASS, AQUAS, SemI40, IoSENSE 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 a rather joint effort in the end. There are arising risks and challenges for the public, particularly in the area of cybersecurity, safety and privacy, impacting also liability, legal issues and insurance issues as well.

3. Internet of Things – Driver for Digital Transformation

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. 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 its 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 several reports and is very active because of the importance of standardization for huge IoT systems with many interfaces and "things":

- High Level Architecture (IoT Reference Architecture mapping to existing IoT Reference Architectures, e.g. RAMI4.0 for Industry 4.0, as addressed in the ECSEL projects SemI40, Productive4.0, see Acknowledgements)
- IoT Standardization Landscape (maintenance of the IoT standardization landscape, gap analysis and recommendations, cooperation with SDOs (Standardization Organizations) and Alliances, see AIOTI [3], ETSI [12], [13], CP-SETIS [11])
- Semantic Interoperability (key issue, led to many co-operations with other standardization organizations and industrial or international working groups)
- IoT Privacy (IoT Platform, standard framework and references for "IoT Trust" and "IoT Privacy by Design")
- IoT Security (Security architecture for trusted IoT devices, baseline requirements for security and privacy, standard framework and "IoT Trust" based on Security by Design).

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 4).

Figure 4: The IoT StandardizationLandscape (Organizations (SDOs) and Alliances) (source: AIOTI, ETSI [14, [15])

ETSI, AIOTI and associated groups like ARTEMIS Standardization WG, but also IEC and ISO (ISO/IEC JTC1 SC41, Internet of Things and related standards) try to cooperate and coordinate efforts to achieve a joint view and make the "landscape" more usable (hopefully).

IoT has to be seen on European level as one important component to driving the "Digital Transformation", as depicted in Figure 1.

4. Autonomous Systems – Challenges and Ethical Questions

3.1 Automotive – Automated Road Traffic

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.

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. This is e.g. discussed at the annual conference "Connected Car Insurance Europe" (April, London), so it is taken for earnest by business.

A major issue is public (user) acceptance. AutoDrive (see acknowledgements) is the first research project including this question in its work programme, together with standardization/certification issues and disruptive business issues.

One business issue for OEMs will be that car ownership may no longer be the primary reason to use cars, it is becoming more a mobility service, one out of several options. Studies have shown that this may be a question of generation change; for the young generation in cities car owner ship is no longer such a prevailing prestigious issue as in the past, the number of driver license applicants and car ownership are reducing.

That's of large societal impact and may change our behavior in transport considerably, even the role of public transport. Particularly **intermodal transport** could benefit, because the choice is more open for the user of a service than for an owner of a vehicle. For example, one would no longer go from Vienna to Hamburg by car, but use locally autonomous cars to get to the main railway station, take for longer distances the high-speed train, and use again locally an autonomous car). In rural areas, local transport will connect to the next main line (railway, bus) easier by autonomous vehicles on demand than by regular public bus services, which very often have only a small degree of utilization. Since the prevailing autonomous road vehicle mode would be short-distance, electric cars would have a much better chance, and so overall transportation would be much more efficient and environmentally sustainable!

A European Coordination and Support Action Mobility4EU, Action Plan for the Future Mobility in Europe (2016-2018) ([14]), states on major trends and emerging societal factors:

- Enabling an inclusive society, personalization and accessability
- Safety & Security in Transport, Novel business models and innovation in Transport
- Environmental Protection benefits, Benefits for increased Urbanization and Smart Cities
- Digital society and IoT as benefit for sustainable growth: New products and services
- Changes in the legislative framework

'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 and most demanding one being urban traffic.

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, (Roadmap see [8]) 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.

3.2 Autonomous Systems in general

But “autonomous vehicles” covers not only automotive, although this is the largest market besides “Industry 4.0”. It covers

- Robotics (industrial, health, ageing well applications),
- Heavy machines (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, 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
- Sensors and actuators
- Software development, life cycle issues
- System integration
- Connected vehicles, V2X connectivity
- Cooperative driving and transport systems,
- 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.

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, industrial trucks) and others where the general public and public spaces set the requirements (road transport, smart cities/buildings/homes and care).

3.3. (End-) User/Public Acceptance and Ethical issues

User and Public Acceptance are very important in case of automated driving, since for many years a mix of vehicles of different levels of automation will co-exist. This, and aspects like insurance, liability and legal framework, are particularly addressed in the ECSEL projects AutoDrive and Productive4.0 (see Acknowledgements).

There are numerous risks already identified with end user behavior towards fully autonomous or highly automated systems:

- People may try to tease e.g. robots by deliberately crossing and standing their path so they have to stop or are forced to unusual paths to circumvent programmed potential critical situations

- An UK study warns that by just stepping before an autonomous car its stop is enforced automatically, and robbery/threat to life and limb easily facilitated, whereas a human driver might even overrun the dangerous persons and such avoid personal risks for himself.
- How should a "perfect" autonomous car behave in case of reckless driver behavior around him? How should it give warning signs or allowance signs to others (he can't "wave hands"?)
- Ransomware introduced in an autonomous car during a ride or becoming active during a ride at high speed may threaten the passengers and driver to kill them, such blackmailing him to pay a considerable sum!
- Highly automated distributed energy systems (electric grids) may be attacked as part of cyberwar – examples are the Russian Cyberattacks on the Ukrainian electric power grid (December 2016, revival just recently, see WIRED [5]). Even smart meters in Germany have no possibility for strong asymmetric encryption because of lack of resources! (Oral communication at Security Conference).
- Similar risks are evident in medical devices and hospital systems ([7])

Ethical concerns have already been taken for earnest by international and European authorities and organizations for automated driving as well as robotics and autonomous machinery.

As a famous example and first idea on how to manage the influence of robots on our daily life and protect humans were **Isaac Asimov's** "**Three Laws** of **Robotics**":

- A robot may not injure a human being or, through inaction, allow a human being to come to harm
- A robot must obey the orders given it by human beings except where such orders would conflict with the First Law
- A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws

The laws seem to reasonable and complete, but soon it was shown (even by Asimov himself) that realistic situations may result in unresolvable conflicts for a robot just adhering to this law. Soon, Asimov himself introduced a "Zeroth Law" (zero being of a higher level to obey than Law 1) for a broader context (e.g. one human endangering mankind, a situation similarly to the "tyrants murder" ethics (is it allowed to kill a dictator who endangers millions of lives?)).

- Law zero: A robot may not harm humanity, or through inaction allow humanity to come to harm.

It seems that the question "Is it possible to create practical laws of robotics which can guarantee a safe, conflict free and peaceful co-existence between robots and humans?" has no positive answer valid in all foreseeable situations. Even in Asimov's stories, robots had to decide which type of risk of harm is acceptable (e.g. autonomous robotic surgeon). Other authors assumed, that robots may have as logical result a mental collapse after detecting that an activity which seemed to follow Law 1 had a disastrous result, e.g. in "The Robots of Dawn" the whole plot of the story revolves around a robot which apparently was destroyed by such a mental collapse (like a "short circuit" in his computer brain).

These robotic laws were written in 1942, when robots were androids and just relatively simple "slaves" for humans, not taking into account the much more complex robots imaginable today. And what about a robot developed for an army? And who or how is defined as "human being" (from history we know that sometimes a certain group of people is not considered as equally human and killed, e.g. genocide?). This, we have to look at the humans behind the AI and robots as well.

Nevertheless, the issue was taken up by IEEE, the European Parliament, the German Ethical Commission for Automated and Connected Driving, UNO and some standardization organizations. Some general autonomous machines (robots) ethics recommendations are:

- 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.
- Petition to the UN to rule against „Drone Wars", „Robots at War" (Irak War: A far remote US UAV controller received a „Bravery Medal")
- European Parliament took first actions to study „Robots Ethics":
    - Resolution on automation ethics calling for robot "kill switches" (Jan 12, 2017)
    - Delvaux tabled a resolution at the European Parliament that stressed the need for an EU agency that is dedicated to dealing with A.I.
- 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.
- ISO/IEC JTC1/SC41 (IoT and related technologies), June 2018, Swiss proposal for establishment of a Subgroup on "Societal and human factors in IoT based services".

For Automated Driving, the relevant organizations set up already some recommendations and rules how this should be implemented in societal context, setting requirements on automated driving vehicles:

- UN, UNECE WP29 Report from Intelligent Transport Systems and Automated Driving (ITS/AD), setting rules in extension of the existing "Vienna Convention" for
    - **Type Approval** for **automated and connected vehicles**, testing of automated systems, real world and simulated
    - How to approve serial produced automated vehicle for usage on public streets
    - The original Vienna Convention defined in §5, that "Every driver shall at all times be able to **control his vehicle** or to guide his animals", which of course is no longer true**.** The functional safety standard ISO 26262 has "controllability" as one of the perimeters to derive the ASIL safety integrity level, which is no longer meaningful for automated vehicles. Thus, the amendments state:

      "When these vehicles are fitted with systems, parts and equipment that are ***in conformity with the conditions of construction, fitting and utilization*** according to technical provisions of international legal instruments referred to **…** they shall be ***deemed to be in conformity with Annex 5"*** *[15]*.

- DE, Ethics commission Automated and Connected Driving (Report June 2017, Federal Ministry of Transport and Digital Infrastructure):
    - 20 high level guidelines: "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.**"
- US National Highway Traffic Safety Administration, Federal Automated Vehicles Policy, September 2016
    - The **fall back minimal risk condition** portion of the framework is also specific to each HAV system. Defining, testing, and validating a fall back minimal risk condition ensures that **the vehicle can be put in a minimal risk condition in cases of HAV system failure** or a failure in a human driver's response when transitioning from automated to manual control.

SAFETRANS (Germany, WG "Highly Automated Systems: Test, Safety, and Development Processes"), has published a **Roadmap Highly Automated Systems** with recommendations on Actions and Research Challenges, in German, but the Management Summary is available in English.

4. 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. Research as described here and funded by the EC and national authorities do explicitly exclude certain applications like military, espionage etc. However, we should be aware and 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 or control our live in an undue manner. This requires careful European and international legislation and control of the automation impact on our lives 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.

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° 692466 (SemI40), n° 692480 (IoSENSE), n° 692455-2 (ENABLE-S3), n° 737475-2 (AQUAS), n° 737459-2 (Productive4.0) and n° 737469-2 (AutoDrive) and recently started projects SECREDAS (783119), iDev40 (783163) and AfarCloud (783221)).

5. 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] Andy Greenberg, „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

[6] European Commission (2017): 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)

[7] Peter Heindl, Werner Damm (Eds.), 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

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

[9] 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

[10] ARTEMIS Strategic Research Agenda 2016, ARTEMIS Industrial Association, Eindhoven, NL.

[11] E. Schoitsch, J. Niehaus, 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.

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

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

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

[15] 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

[16] European Commisssion, "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

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

[18] Erwin Schoitsch, „Smart Systems Everywhere – how much Smartness is tolerable?", IDIMT 2017, Proceedings, p. 361-373, Trauner Verlag, Reihe Informatik 46, 2017.