PLATFORMS 4CPS

Societal and Legal Issues

Workshop Report

Brussels, 14th of May

Table of Contents

Figures

The Platforms4CPS project is co-funded by the European Community's Horizon 2020 Programme under grant agreement no 731599.

Executive Summary

This document presents an overview of the Platforms4CPS Workshop on Societal and Legal Issues Regarding CPS Deployment. The introduction of future CPS with increased interconnectivity, autonomy and Artificial Intelligence raises a number of concerns for society that need to be addressed. In many cases the technology is available but external barriers such as safety, privacy, security, contract law (e.g. SLAs), liability and public trust in the new technology are preventing successful deployment within applications. Based on desk research, questionnaires, discussions with key stakeholders from large industry, SME's, academia, government, certification bodies, policy makers the following "hot topics" were identified:

- **Connectivity** considering privacy, confidentiality and cybersecurity for CPS/IoT
- **Legal Issues** considering risk and liability due to safety concerns in areas such as autonomous cars, ships, aircraft, trains, energy, health and Service Level Agreements for new services, e.g. mobility providers and medical monitoring
- **Ethical issues of AI** considering transparency and the need ethical training for engineers
- **Social impact of Automation/Robotics** considering the threat to jobs as well as proposed approaches to address this such as a "robot tax" and Universal Basic Income

The aim of the Constituency Building workshop held on 14th May 2018 in Brussels was to raise awareness amongst stakeholders and to discuss these topics in greater detail. The event attracted around 20 experts to discuss the hot topics in the area and to identify needs for regulation, training and EC support going into Horizon Europe.

1 Introduction

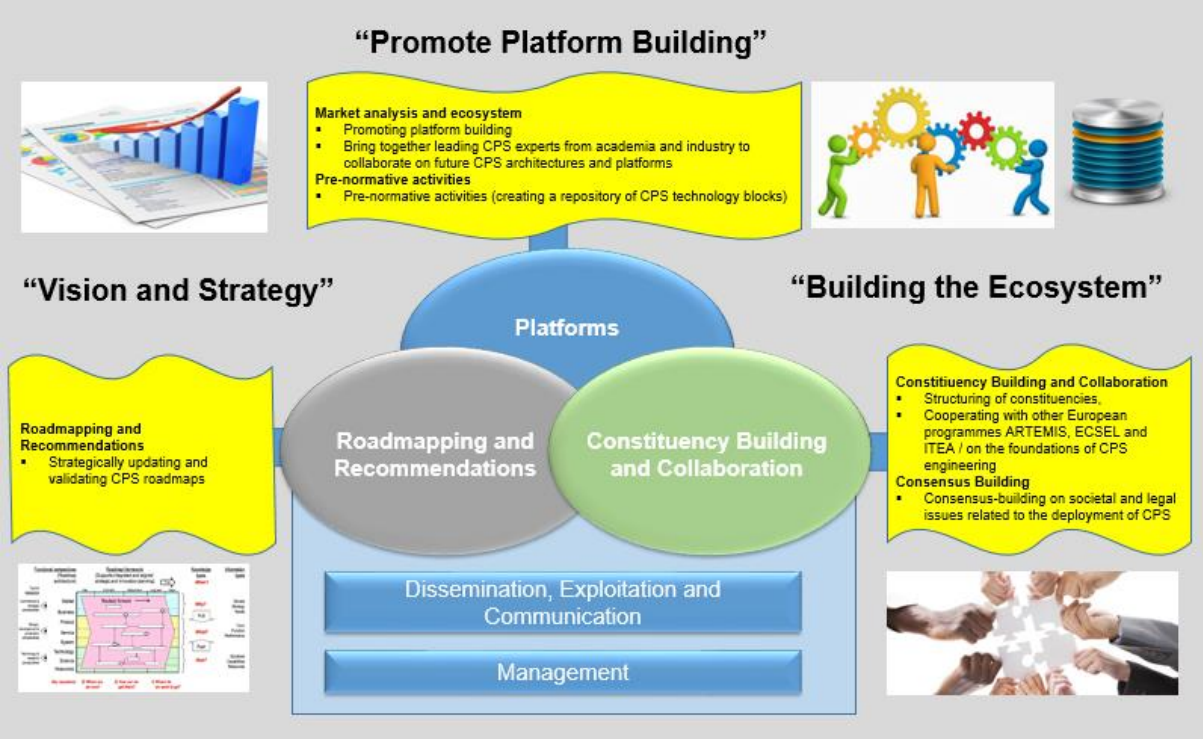

Figure 1. Overview of the Platforms4CPS Objectives

Cyber-Physical System (CPS) are established from networked embedded systems that are connected with the outside world through sensors and actuators and have the capability to collaborate, adapt, and evolve. An increasing number of interacting systems with strong connectivity are being utilised in both society and in industry with application in many areas such as multi-modal transport, eHealth, smart factories, smart grids and smart cities. The deployment of Cyber-Physical Systems (CPS) is expected to increase substantially over the next decades, holding great potential for novel applications and innovative product development, however, there are a number of barriers and societal concerns about their introduction considering safety, security, privacy and impact on employment.

The Platforms4CPS project (See **Figure 1**) aims to 'create the vision, strategy, technology building blocks and supporting ecosystem for future CPS applications' with three key objectives to:

- Create a vision and strategy for future European CPS by analysing the ecosystem and market perspective, and strategically updating and validating existing CPS roadmaps across multiple domains
- Promote platform building, bringing together industry and academic experts and create a repository of CPS technology building blocks
- Build an ecosystem by creating a constituency and through cooperating with ECSEL, ITEA, and ARTEMIS projects on the foundations of CPS engineering, and **consensus building on societal and legal issues related to the deployment of CPS**.

It is the latter area of consensus building on societal and legal issues related to the deployment of CPS that the workshop addressed. In addition to identifying and describing the relevant drivers, needs, underlying technology fields and related research priorities to fuel the development of trustworthy CPS, it is also important to address the barriers that prevent successful implementation.

2 Societal and Legal Issues Workshop

2.1 Workshop Aims

Figure 2 Societal and Legal Issues Workshop

The introduction of future CPS with increased interconnectivity, autonomy and Artificial Intelligence raises a number of concerns for society that need to be addressed. In many cases the technology is available but external barriers such as safety, privacy, security, contract law (e.g. SLAs), liability and public trust in the new technology are preventing successful deployment within applications. Based on desk research, questionnaires, discussions with key stakeholders from large industry, SME's, academia, government, certification bodies and policy makers a number of "hot topics" have been considered:

- Connectivity considering **privacy, confidentiality and cybersecurity** for CPS/IoT
- **Legal Issues** considering risk and liability due to safety concerns in areas such as autonomous cars, ships, aircraft, trains, energy, health and Service Level Agreements for new services, e.g. mobility providers and medical monitoring
- **Ethical issues** of AI considering transparency and the need ethical training for engineers
- **Social impact** of Automation/Robotics considering the threat to jobs as well as proposed approaches to address this such as a "robot tax" and Universal Basic Income

The objective of the workshop was to

- **Raise awareness** amongst stakeholders
- Discuss the results of the analysis of the "**hot topics**"
- **Provide recommendations** with respect to needs for regulation, training and EC support going into Horizon Europe

2.2 Workshop Agenda

	Platforms4CPS – Societal and Legal Issues Regarding CPS Deployment
12:30	**Registration**
01:00	**Welcome and Introduction (Haydn Thompson; THHINK)**
01:05	**Overview of Platforms4CPS Societal and Legal Work (Haydn Thompson; THHINK)**
01:30	**Warming-up to Cybersecurity Hygiene (Afonso Ferreira; CNRS-IRIT)**
01:50	**Privacy, Confidentiality, Security (Group Work)**
14:30	**Legal Issues – Risk, Safety, Liability, Service Level Agreements (Group Work)**
15:10	**Coffee Break**
15:40	**AI Ethical Issues (Group Work)**
16:20	**Impact of Automation on Jobs – Robot Tax and Universal Basic Income (Group Work)**
17:00	**Visions for CPS in FP9 (Sandro D'Elia; European Commission)**
17:30	**Wrap Up, Close of Workshop**
19:30	**Networking Dinner at: L'Entree des Artistes http://www.lentreedesartistes.be/de/**

2.3 Overview of Platforms4CPS Societal and Legal Issues (Haydn Thompson, THHINK)

To set the scene an overview was given of the Platfroms4CPS work on societal and legal issues. It was highlighted that there were similar trends in transportation (automotive, rail, aerospace and maritime) for autonomous systems as well as optimised traffic flow/operations relying on new techniques such as big data analytics and AI. There is also a trend towards increased monitoring of systems. This is leading to safety concerns, ethical concerns in both the decision making for autonomous systems and also for optimisation, and privacy concerns from monitoring of vehicles (and humans). As an example there are 5 levels of autonomous cars from 0-4. Current cars have functionality up to level 2 which includes ADAS features such as automatic braking and lane keeping. For the next step Level 3, the car is autonomous, but the driver must still be able to take over control of the vehicle, however, at level 4 the driver is not expected to take over control and there may not be a steering wheel. These steps will require changes to regulation. Notably the amount of technology required goes up as more autonomy is built in. Although there are many benefits: lives saved, fuel savings and reduced traffic congestion, there are also concerns. Challenges are consumer acceptance and trust, the current high cost of the technology, liability concerns and a lack of harmonisation of regulations across Europe. Security is also a key concern as hacking of cars has been demonstrated. As systems will need to be monitored privacy is also an issue.

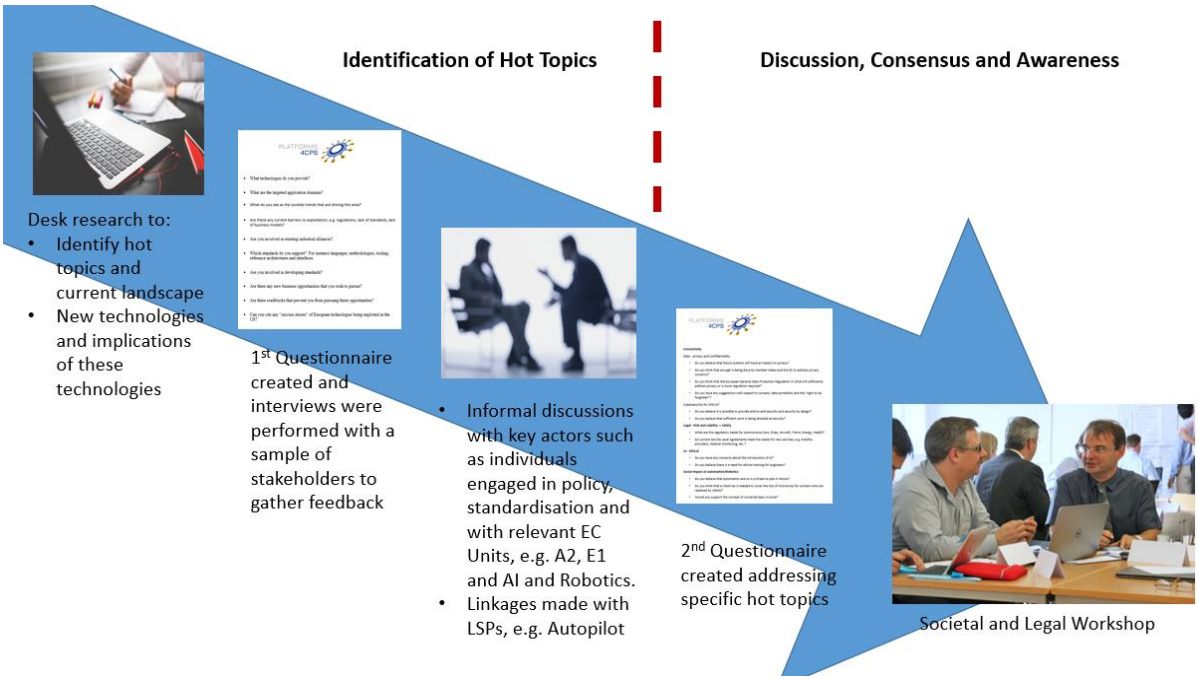

Figure 3. Approach to Identification and Consensus Building on Societal and Legal Issues

The aim of the work on societal and legal issues is to build consensus, raise awareness and foster a dialogue with society on the societal and legal issues that arise from future CPS. The approach that has been taken is shown in **Figure 3**. Initially effort was directed at identifying "Hot Topics and Concerns". This was in order to narrow the scope of the work to address areas which were identified by key protagonists as being important. Desk research was performed to identify new technologies and potential implications of these technologies particularly with respect to societal and legal issues. Based on this initial research a questionnaire was created and interviews were performed with a sample of stakeholders to gather feedback. Informal discussions were held with key actors such as individuals engaged in policy, standardisation and with relevant EC Units, e.g. A2, E1 and AI and Robotics, that are addressing applications of CPS. Linkages were also made with relevant Large-Scale Pilots, e.g. Autopilot, that is addressing autonomous vehicles. Based on this a list of Hot Topics was created which led to a second more targeted questionnaire which was circulated to experts working in a number of CPS and IoT domains including aerospace, space, automotive, rail, maritime, health, etc. The results from this were analysed and combined into a proposed consensus view. The aim of the workshop was to raise awareness, discuss and further elaborate on the hot topics identified.

Each of the identified hot topics were briefly introduced. With respect to privacy the General Data Protection Regulation will be introduced May 25, 2018 (the week after the workshop). Companies that collect data on citizens across all 28 EU member states will need to comply with strict new rules. This dictates that it will not be allowed by law to collect data on: basic identity information such as name, address and ID numbers, web data such as location, IP address, cookie data and RFID tags, health and genetic data, biometric data, racial or ethnic data, sexual orientation and political opinions. Thus, there is a need to consider the impact of future systems on privacy, the GDPR regulation, consent and "right to be forgotten".

Considering security there have been some high-profile ransomware and malware attacks particularly affecting manufacturing and engineering as well as causing major disruption in the NHS in the UK. Notably the threat is not from lone hackers but from state sponsored hacking. Hot topics associated with this are end-to-end security and security by design. There are also concerns about

the lack of effort being put into security by industry, and at research level, as well as the general lack of awareness of security risks.

In the area of autonomous systems as we move to more autonomy there will be a need for regulation for Autonomous Cars, Ships, Aircraft, Trains, Energy and Health. Accidents are inevitable and an approach to liability is needed as well as some thought on Service Level Agreements for new services, e.g. mobility providers, medical monitoring, etc.

In the area of Artificial Intelligence examples were given of how AI is not very accurate (identification of age and emotions) and also potentially dangerous in giving information that individuals want to conceal. The ethical issues of speaking with AI to make an appointment were also demonstrated. At an extreme level Kalashnikov have developed an automatic cannon that uses AI to identify human enemies and then automatically shoot them. It was noted that ethical concerns have been expressed by Elon Musk, Stephen Hawking and Bill Gates. Facebook have also had some high profile bad publicity with Cambridge Analytica. There is thus a need to consider the impact of AI on future society and the need for ethical training for engineers.

The social impact of automation is raising concerns with respect to threats to jobs. The predictions are that increased automation and AI will be a threat to white-collar jobs. An example was given on the impact of automated trading on the London Stock Exchange. There are various predictions PwC - automation will take 40 per cent of US jobs by 2030 Bank of England - 15 million jobs in the UK may go (half the current working population) and McKinsey in 2015, quoted by the WEF, found that 45% of the activities that workers do today could be automated if companies want to do so. Although there are many benefits, e.g. in automotive improvements in safety, improved traffic flow, reduced emissions, and mobility services, there will also be significant job losses. The threat to jobs thus needs to be considered along with approaches that are being proposed to deal with this, such as a Robot Tax and Universal Basic Income.

Finally, it was highlighted that by 2035 it is predicted that 2/3rds of the jobs that will exist have not even been thought of yet. If 40-70% of jobs are automated, there will be a lack of jobs and an increase in the gig economy with the associated issues of not being able to support people when they do not have a job. Considering todays' children, key questions are what skills are needed in the future and what education should we provide to support this?

2.4 Warming Up to Cybersecurity Hygiene (Afonso Ferreira, CNRS-IRIT)

It was highlighted that cyber-attacks are costing large companies €100M every year. The WannaCry and Petya-NotPetya virus attacks had caused massive problems across the world raising awareness of the need for cyber-security. These had started with government software being stolen. The progress of the spread had been rapid. Even though Microsoft was aware of the problem an update to protection produced in response to the threat was not installed by users in time. There have also been some notable hardware bugs with Spectre and Meltdown. More recently there have been widely publicised unscrupulous use of data such as data from Facebook by Cambridge Analytica.

The increased use of technology, in particular wireless connectivity, for card transactions and for access are also a concern. The ease of stealing access codes by intercepting wireless messages was demonstrated with a video of a car being stolen [http://www.bbc.com/news/av/uk-42132804/relay-crime-theft-caught-on-camera]. It was noted that increasingly the state is watching social media and this can lead to arrest if activities are posted that are considered to be against laws, cultural norms or inflame local sensitivities.

It was highlighted that people do not follow good security and today there are many passwords needed for devices. There is a need for strong passwords on all devices, a diversity of passwords, protection of password information and also increasingly protection of cards, etc., via enclosure

within a Faraday cage. Most importantly data should be backed up regularly to avoid loss. Some key messages were made:

- Cybersecurity is an investment, not a cost
- It is best is to secure IT by design
- Back up your data
- Think before you post
- Act as if you are already infiltrated
- Understand and contain cyber risks
- Secure IoT now or cry later

It was noted that there is a tension between many actors involved in security. Sovereignty is a key concern for governments, but too much security is a concern for law enforcement. There are also conflicting calls for fundamental rights for privacy from society as well as more access from marketing companies who want to access data for commercial purposes. For safety-critical applications such as CPS in automotive and health there are concerns about safety as well as software liability.

2.5 Session on Privacy, Confidentiality and Security

The breakout session on privacy, confidentiality and security considered the following questions:

- What are your key concerns of future systems with respect to privacy?
- European General Data Protection Regulation – too much, too little?
- What can member states and the EC do to address privacy concerns?
- How to raise awareness of security – research, industry and general public?
- How to persuade people to pay more for security?

It was highlighted that GDPR will change everything, however it was not clear how it would be possible to track and police privacy or prove that the processes in place to protect data where “reasonable”. Something akin to ISO 9000 may appear in the future. It was noted that companies are liable for subcontracted services, e.g. a cloud provider, and companies need to assign a DPO who is responsible for data protection. Data breaches now also need to be reported within 72 hours. With respect to data GDPR covers Europe but we should be more careful of what we store outside the EU and know when data is stored outside the EU. There are some concerns with respect to GDPR. Potentially the cost of implementation is a barrier to European companies and it may act as a barrier to innovation. Support was thus advocated for SMEs and non-profit companies and potentially this could be subsidised via a tax. Other foreign companies may have an advantage if they do not need to comply with GDPR.

It was noted that Blockchain is potentially easier to police, but it is not covered by GDPR. This raises difficulties when considering the right to be forgotten. Here Zero Knowledge proof approaches may be a useful concept to avoid sharing of knowledge.

A challenge is that the younger generation are quite often happy to post information without realising the full consequences. Here an ID system for under 16’s may be useful. It was highlighted that there is a need for education on security and this could be done in schools, perhaps via a game, to help children and parents understand implications. It would also be helpful to label websites and IoT with a CE mark. Regulation could then be used to encourage people to use compliant systems. It would also be useful to have a way of obtaining a list of permissions given. Consent is important, and people should have the choice to not share data as well as the right to be forgotten. It was noted that there is an interlinkage between privacy, trust and security.

There are a number of challenges. A key challenge is how to secure the supply chain for ICT to avoid back doors. There is also a need to design systems such that they are resilient knowing that there will be breaches. There are also key liability issues with respect to security and privacy. It was noted that in cyber-security the real issues are protecting financial data and IP addresses.

Although everybody is talking about security there is a lack of awareness of risk and there needs to be guidelines. There will be much more liability for manufacturers if security is breached and this may lead to the need for manufacturers to take out insurance for breaches in privacy and security. A key area that needs to be addressed is service liability.

It was noted that some things could be done to better enforce security. Systems should be better developed to enforce passwords. For instance, devices should not work out of the box without a password change to a suitably strong password. Safety and security go together with certification and the public needs to be better educated that a cheap solution is not normally the best solution and so they need to pay more for security.

With more connectivity there are more challenges. If connected thermostats or smart meters were attacked en masse it may be possible to bring down infrastructure and this may be a target for foreign states.

Help should be provided via providing password generator tools and a toolbox for storing passwords. Although biometric data is being promoted as the future, there is a major difficulty in that once biometrics data is stored electronically, if it is stolen then it is difficult to prove it is not you. Effectively the use of biometric data introduces one password for everything which goes against the fundamentals of using many different passwords.

2.6 Session on Legal Issues, Risk, Liability and Safety

The session on legal issues, risk, liability and safety addressed the following questions:

- What are the regulatory needs for Autonomous Cars, Ships, Aircraft, Trains, Energy, Health and how do we promote trust?
- Liability – who is liable and how to address?
- Do current Service Level Agreements meet the needs for new services, e.g. mobility providers, medical monitoring, etc., considering increasing number of SLAs and ad-hoc interactions?

It was highlighted that an independent body for certification, such as that used in aerospace, would be useful for other sectors such as automotive. In general regulation exists at a national level but there is a need for harmonisation across countries such as for the train industry. In the energy sector there had also been recent problems across Europe due to differing power frequencies which had led to clocks being incorrect. The area of health is strongly regulated but there is a need for harmonisation of reimbursement across member states. It was noted that the area of well-being is not regulated, and this may be required in the future. Although there is regulation in place for product liability there is a need for regulation for IT service reliability. Notably Garmin as a product falls under product liability laws whereas Google as a service has no liability. As they both provide the same functionality this does not seem fair. As we move towards autonomous cars there is a need for service level agreements with network providers. In general, large organisations will take care of infrastructure deployment/operation and it is likely that smart infrastructure will be rolled out on private highways first. A problem is that autonomous transportation will reduce overall death rates, but each individual accident will be high profile and people are likely to sue. It is also predicted in the future that people will use more public transport such as trains and buses. Trust will build up slowly and the insurance industry for injuries and deaths will be affected greatly. A key challenge will be

where to place liability for unforeseen events. As systems will rely more on connectivity security will also be a big issue.

2.7 Session on AI Ethical Issues

The session on AI ethical issues addressed the following 3 questions:

- What are the chief ethical concerns with respect to the use of AI? (Might want to think of examples)
- How can we verify the behaviour of AI?
- What action is needed at a European level in order to address these concerns?

It was noted that many hypothetical situations are put forward, e.g. to choose between running over an old lady or a child, but the reality is that this approach is fundamentally wrong as these are decisions that humans would not make in practice. It was noted that ethically if we have the autonomous technology to reduce the overall numbers of deaths on the roads then it is not ethical to delay introduction of autonomous cars as we are currently killing 100's of people and ruining many lives. It was noted that in many cases schools are already teaching ethics to some degree. There is a need to understand what an algorithm does, but it is also important to know the situations when it does not work. It was noted that if humans drink and drive they are punished so there are consequences. With AI there is no conscience about doing something wrong, for example in the case of the automated Kalashnikov gun that targets and shoots people. There is thus a need to train AI systems to act in a human way.

2.8 Session on Social Impact of Automation/Robotics

The session on social impact of automation and robotics considered the following questions:

- Do you believe that automation and AI is a threat to workers in future?
- Is a robot tax to cover the loss of income tax for workers who are replaced by robots workable? (How would you do it?)
- Would you support the concept of Universal basic income?

There was general consensus that new technology will result in people losing their jobs who may well end up in lower status jobs. An example is that bookshops are disappearing and people who know about books are now ending up in jobs where they just deliver them after they have been bought off the web. A problem is that new jobs will not be generated as fast as jobs are lost and the technology will ruin people's livelihoods. There is an option not to do this, but change is already underway. It was noted that in the past there was a very fundamental shift when technology came along from 80% of people working on the land to now only 2% with very efficient farming. The use of AI affects senior jobs in particular as it targets decision making. This will unbalance society with the workforce being divided into very senior levels and people at the working-class level leading to greater differences in distribution of wealth. The middle class will thus be most affected. However, there are many jobs that exist today that did not exist 10 years ago. There will be a need for retraining in all sectors. There is a need to identify where humans can best contribute and what they are good at. Machines are good for repetitive cognitive jobs, but humans have experience. It was noted that not everybody will have a PhD or formal education. Some people like human interaction, however call centres, etc. are an area that is being automated. A challenge will be to smooth the transition from one job to another when there may be big shocks and changes. It may be unwise in future to have one specialism as people may need to move between areas.

Robot tax, although a good idea, would be difficult to implement in practice. How could IT services be taxed when there is no border or nationality? There is also a difficulty in identifying what is a robot. Robots make products cheaper and so if a tax is applied then the products will be more expensive. An automation tax could be used to contribute to society, however, a problem is that taxing profits is a tax on innovation. A more fundamental question is whether working is a thing of the past? If the state owns manufacturing, then it would be possible to implement a robot tax. It was noted that salaries increase at a slow pace and there would be a need for a much higher robot tax. One idea was that in the future companies will need to be forced to contribute to a sustainable society rather than making money only. Society would then need to find other activities to fulfil their lives. This may include activities such as voluntary work and caring for people, however, not everyone would want to do this.

Another question is what skills are needed for the future? There will always be new jobs, but a concern is that these new jobs will be "working poor jobs". This is driving inequality with more poor people with low income which destabilises society. It is also clear that trained people will want fulfilling jobs. This may lead to issues with status.

It was noted that the UBI experiment in Finland had stopped as it was found to be unworkable. In essence, the approach simplifies existing benefits systems so in many ways UBI already exists. It is unclear, however, how everybody can contribute to society, such as the unemployed and retired people. There is a fundamental question of how we value jobs. Young people are increasingly volunteering and this may help their social standing. There is also an increasing number of people who do not want to work a full 5-day week.

3 Visions for CPS in FP9 (Sandro D'Elia, European Commission)

Sandro D'Elia highlighted that almost any complex machine these days has a computer inside. The expectation is that for Horizon Europe there will be more funding with a focus on innovation and a strong emphasis on AI. A communication had been produced but what will actually be done in this area is still being defined. There is also an emphasis on missions which target "moonshot" activities. An Edge 2030 vision is being promoted addressing the key trends for evolution of computers that interact with the physical world. This needs to include a range of technologies such as heterogeneous, Tensor, quantum processors, ASICs, etc., as well as AI powered by Big Data, and Cybersecurity. Looking longer term there is interest in synthetic biology, bio-processors and DNA computing. Key challenges are trust in AI and autonomous systems. There is also a perceived threat that robots will steal jobs. It was noted that it has now become too difficult and expensive to develop dependable high-quality software. Also, since there is no access to the internals of processors (e.g. Qualcomm and Intel) it is not possible to guarantee security. Energy consumption of computing is a concern as it is not sustainable. Notably blockchain uses far more energy per transaction, i.e. 5000 times more than it takes to process a VISA credit card.

There are a number of constraints coming from the high cost of data transmission within limited radio spectrums which limits the amount of data that can be transmitted in a given area. It was noted that guarantees on safety, latency and predictability are not possible for autonomous cars if there is a reliance on a cloud connection. Privacy and security also pushes people towards processing data at the edge rather than transmitting or storing data in the cloud. Notably edge computing is more amenable for privacy/security and is also GDPR compliant.

Open Source Software is now used in all data centres and Neural Network technology is mostly open source. Even Microsoft is providing open source software. However, for AI the real value is in the data. Here China is using Open Source but not contributing to it. There is a need for Open Innovation, Open Science and for being Open to the World. In the area of AI there is an initiative to support an "AI-on-demand platform" with a desire to connect and strengthen AI activities across Europe.

Support will also be provided for AI developments in key sectors. An ethical and legal framework is being put into place to support AI. Already GDPR is coming in, but this will be followed by AI ethical guidelines and product liability guidelines in 2019. There will also be a need to support skills in response to the socio-economic changes that are likely. A declaration of cooperation on AI has been signed by 25 European Countries which will produce a coordinated plan for AI by the end of 2018.

For CPS the Commission has defined 3 main pillars. The first pillar addresses trust and acceptance. Here there is a move towards localised intelligence at the "edge" in order to react promptly in time critical applications. In order to generate trust there is a need for a factor of 10 reduction in bugs in software, better usability, resistance to cyber-attacks, and an approach to explainable AI technologies. A vision is to have software that just needs updating once a year. Pillar 2 addresses productivity. The aim is to increase the productivity of companies in dependable software automation systems, robots, AI, and also in using AI to deal with complexity management. Here there is a desire to make digital technology accessible for non-geniuses. Pillar 3 addresses energy. The goal here is to provide 2-3 orders of magnitude improvement in energy consumption. This is required for exascale computing and also batteryless computing for IoT devices. It is also planned to explore unconventional computing techniques such as neuromorphic, approximate, bio-inspired and DNA-based. Here it is expected that there will be a significant contribution to sustainability goals. In addition to the main pillars there is a need to address the hardware internals for European industry. This is needed to avoid security issues from backdoors in the hardware and also to allow real-time for safety-critical applications so that WCET can be guaranteed. A goal is to have processors that have deterministic behaviour. There is a key desire for full European sovereignty for defence and security applications which will require more electronic design activities in Europe.

It was highlighted that the next framework program will define missions and under this projects will be funded that contribute to the missions. An example of a mission related to CPS is "an integrated transport system reducing car congestion by 50% in 10 European cities by 2030". Several other proposed missions also address CPS topics.

4 Conclusions and Recommendations

The work on societal and legal issues has identified a number of hot topics:

- Privacy and Confidentiality
- Security
- Legal Issues – Risk, Safety, Liability
- Service Level Agreements
- AI Ethical
- Impact of Automation on Jobs

These were discussed in the workshop by experts in the domain leading to consensus and recommendations for potential ways forward. These will be encapsulated in key recommendations addressing regulation, training and EC support going into Horizon Europe in deliverable D4.4.