Software and Smart Networks and Services

The COVID-19 situation unfolded as this paper was being drafted. It has drastically modified the lives of billions of people around the world and forced individuals, enterprises and administrations to rely more than ever on digital services to help fight the disease and keep the economy running. Performance and availability of networks and digital infrastructures, access to digital services by most of the population, and innovation on usages are key factors in maintaining key processes and allowing remote cooperation and interactions at an unprecedented scale. This reinforces all the challenges presented in this paper and emphasizes the importance of developing and maintaining European leadership and sovereignty in key digital technologies.

Executive summary

This paper is an analysis by NESSI[1] about the role of software and services technologies for future Smart Networks and Services (SNS), which is one of the proposed Partnerships in Horizon Europe[2].

Software and service-based software design principles are already fundamental technologies for 5G systems: key concepts of 5G such as network slicing are based on cloud and Software Defined Networking (SDN) technologies, and the design of the 5G core network follow a service-oriented approach. Building on 5G, the SNS proposal aims to develop a 'scalable, robust, secured, distributed, high-performance, energy-efficient and environment-neutral ubiquitous digital infrastructure'. This future digital infrastructure is considered essential for enabling the digital transformation of society and promoting businesses innovation in areas such as Industry 4.0/5.0, Smart Energy, Smart Cities, Smart Healthcare, etc. Future digital services will heavily rely on Artificial Intelligence and Machine Learning as enabling technologies. Thus, SNS will face the software-related challenges described in the NESSI position papers 'Software and the Next Generation Internet'[3] and 'Software and Artificial Intelligence'[4]. These challenges stem from the need for:

- new, more powerful orchestration models, architectures and abstractions for highly distributed, heterogeneous and multi-stakeholder infrastructures and resources;
- new business models for monetizing SNS and for controlling environmental and social impacts, making SNS applications sustainable and justifying investment in infrastructure;
- management of complexity in the presence of dynamically changing and uncertain future requirements arising from and addressed by using self-adaptation powered by artificial intelligence;
- building trust in applications and services with high levels of security and dependability, preventing manipulation of humans by SNS technologies, and protecting critical services and sensitive data;
- new methodologies for software and information systems engineering, maintaining productivity while addressing increased complexity and (in some cases) criticality, and balancing the need for agility with the need for consolidation and optimisation in the use of resources; and
- Incorporating new methods combining software engineering and data science approaches to ensure quality, performance and cost-efficiency for software incorporating AI algorithms.

We recommend research topics on software and services be included in the Horizon Europe work programme to address these challenges, without which the success of Smart Networks and Services may be in doubt.

[1] NESSI (Networked European Software and Services Initiative), the European Technology Platform (ETP) dedicated to software, data and services; http://www.nessi.eu/

[2] https://ec.europa.eu/info/horizon-europe-next-research-and-innovation-framework-programme/european-partnerships-horizon-europe_en

[3] http://www.nessi.eu/Files/Private/NESSI%20-%20Software%20and%20NGI%20-%20%20issue%201.pdf

[4] http://www.nessi.eu/Files/Private/NESSI%20-%20Software%20and%20AI%20-%20issue%201.pdf

Future of smart networks and services

The Digital Single Market (DSM) is one in which the free movement of persons, services and capital is ensured and where the individuals and businesses can seamlessly access and engage in online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence. Creating the conditions for the DSM is a top priority for the EU, and it depends on the emergence of advanced networks and services in Europe. These networks must be:

- ubiquitous, scalable, distributed, heterogeneous and offering guaranteed performance levels (both throughput and latency) for users in any location;
- open and interoperable, allowing application developers and operators to implement a wide range of digital services;
- easily accessed by users regardless of varied physical abilities, cultural background or other factors;
- secure, trustworthy, and able to meet European regulations on network information security, privacy and data protection;
- fair to and trusted by citizens as consumers and data subjects, and businesses engaged in the DSM;
- energy efficient and environmentally benign.

To deliver these characteristics, networks and services will need to be smart, self-organising, self-managing and self-healing. They will need to automatically manage applications and resources, detecting and addressing deviations in performance, security, efficiency or regulatory compliance. These requirements apply to both the network and the services deployed in it. Smart networks and services technology will therefore need to address the full lifecycle of devices, services and applications. To do this, and to ensure that requirements are continuously met, they will need to use state of the art technologies including AI, as well as develop new advanced technologies.

Note that being 'secure and trustworthy' is necessary but not sufficient to ensure smart networks and services will be 'fair and trusted'. This depends on a combination of technical, policy and other measures, especially related to the use of automated decision-making algorithms including AI5.

As already pointed out by NESSI[6,3], advanced software and software engineering technologies must be developed and researched to meet the needs of the digitalisation and the Next Generation Internet:

- software enables the automation of workflows and systems and provides speed and agility in delivering systems;
- software is essential for building adaptive and cognitive services to stimulate creativity and to leverage the human potential as well as to ensure the adaptability and reliability of entire systems;
- the integration of digital systems in complex systems of systems will not be possible without software-based solutions and mechanisms; and
- transparency, digital trust, sustainability, and openness will rely on the software design and the algorithms applied in building systems.

Smart networks and services address the same needs of the digital market and the NGI, and software will be a fundamental key technology also for smart networks as indicated in Figure 1, below. Indeed, software will

[5] See for example 'Shaping Europe's Digital Future', February 2020; https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

[6] Next Generation Software Technologies Empowering the Digital Transformation of Europe, NESSI position paper 2018; http://www.nessi.eu/Files/Private/NESSI%20-%20Software%20Empowering%20the%20Digital%20Transformation%20of%20Europe%20-%20final%20version%2009-2018%20v1.pdf

play an increasingly important role in smart network and service infrastructures, continuing the trend observed in the recent move to cloud computing, but with some new and distinctive challenges.

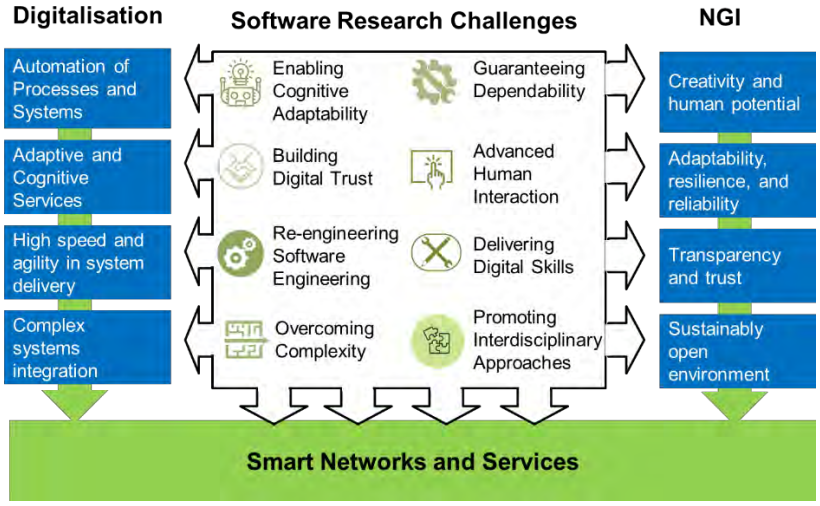

Figure 1 Fundamental digital needs addressed by both SNS and Software

The softwarization of network and service infrastructures

In the past, networks have been built by deploying proprietary control software running on and tightly integrated with proprietary hardware. Operation of such networks was costly, and introducing new functionalities and innovations was tedious. This has changed with the softwarization of networks. Network Function Virtualization (NFV) and Software Defined Networking (SDN) have separated hardware and software, made it possible to use off-the-shelf hardware, and to implement network functions purely in software running in the cloud and decoupled from the hardware. Thus today's networks are programmable, allowing for highly automated and efficient network operation and agility in delivering new services. Modern architectural patterns such as microservices have demonstrated how the entanglement between network and modern software architectures and practises can lead to huge benefits in terms of scalability and flexibility. At the same time, automation of software development processes using DevOps methodologies allows developers to exploit this flexibility and continuously improve application and services to meet the expectations of users.

5G has been following this softwarization trend:

- 5G has adopted a service-based architecture (SBA) for its core functions providing the flexibility and scalability mentioned above;
- standardized APIs (e.g. Network Exposure Function – NEF) have been introduced to provide applications with access to network resources and data in a controlled manner and thus to enable them to provide optimized performance and user experience;
- NFV and SDN allow the flexible deployment and orchestration of 5G functionality across distributed cloud infrastructures, including core and edge clouds; and
- network slicing is a key concept of 5G, built on NFV, SDN, and the flexible SBA of the 5G core. It allows the dynamic creation of multiple virtual end-to-end networks across the same physical infrastructure. These virtual networks can be tailored to use cases by assigning only the network resources and functions that are needed to fulfil the SLA requirements of an application.

However, in the future, this software-based automation becomes more complex on systems with multiple or shared ownership of computing resources, and more frequent with the increasing interest in federated

systems and services. Different ownership complicates the automation as assumptions that could be made on private networks may not hold. Additionally, increased automation especially in a multi-stakeholder environment makes it harder to predict outcomes and ensure networks and services will meet the needs of the DSM. Smart networks and services require a deepening and strengthening of DevOps to manage the use of intelligent automation at all architectural layers and stakeholders from the infrastructure to the business applications. Also, the challenges related to the increasing use of Artificial Intelligence and Machine Learning components in smart networks will need to be mastered. Challenges arise in the governance of self-adapting AI-based software, in explaining decisions taken by AI, in ensuring that appropriate data is used for the training phase of ML models, and in addressing legal and ethical issues[3].

Future services enabled by smart networks

5G not only enhances mobile broadband communications for consumers, but also aims to support industrial communications, to open up new areas of potential data monetization using cognitive analytics and/or real-time sensing, and deliver societal benefits in areas like healthcare and public safety.

Network capabilities such as highly reliable connections with low latency or the ability to connect a much larger number of devices are key to these innovations. Network slicing, APIs and the distributed cloud infrastructure, being integral part of 5G, make these capabilities accessible to users and developers, and enable a broad range of applications in various industrial sectors. The ongoing roll out and large-scale availability of 5G will finally make it possible to unleash its full innovation potential and to create new application and service ideas. However, it will also very likely unveil deficiencies and issues - in the network in providing optimal support to applications, and in the applications in making best use of the network. It will be up to SNS to take the lessons from these large-scale commercial deployments of 5G and to address the new requirements of emerging applications. What the requirements of future services enabled by SNS might be, and the role software plays in meeting these requirements, is illustrated by the following examples: spatial computing, industrial automation, and smart mobility.

Spatial Computing is the emerging interaction mechanism for digital content in a converged cyber physical world [7,8]. Spatial Computing seamlessly embeds digital information into the physical world. Thanks to mixed reality glasses, gesture recognition and haptic feedback, we can interact with digital assets as if they were part of the real world. Spatial Computing thereby empowers us to use natural real-world interaction mechanisms with digital content. Just like the real word, Spatial Computing offers a rich environment for multi-user interaction, and the delivery of information that is relevant to the task at hand.

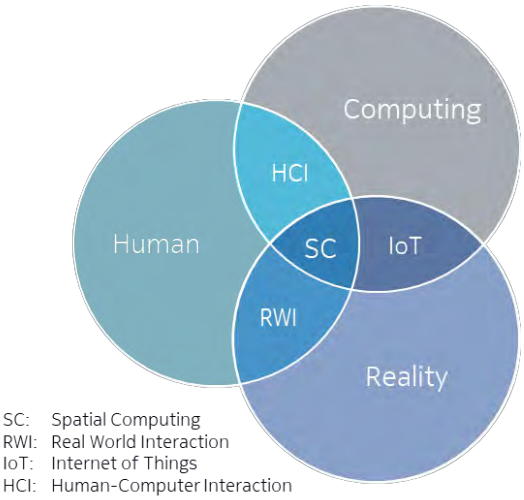

Figure 2 Spatial Computing: a new interaction paradigm

The Spatial Computing system that will emerge over the next decades will be a complex constellation of software and content components operated by a multitude of ecosystem participants. It creates substantial challenges for future smart

[7] An Introduction to The Spatial Web, Gabriel Rene, October 2019; https://medium.com/swlh/an-introduction-to-the-spatial-web-bb8127f9ac45

[8] Enter the next dimension of Spatial Computing, Ori Inbar, AWE 2019, May 2019; https://www.awexr.com/blog/75-enter-the-next-dimension-of-spatial-computing, https://www.youtube.com/watch?v=nPWxmu-Bvj4.

networks and services, with demanding networking performance requirements, complex service platforms, and hard privacy and security guarantees. Many of these will need to be addressed by software engineering and deployment practices; compliance to privacy, confidentiality, sovereignty and security requirements; standardization of data interfaces and information descriptors; automation of system integration and distributed software processes; and interaction design tuned to human cognitive processes.

Promising higher productivity and flexibility for novel and customized products in a sustainable way, industrial digital automation is an important and demanding application segment for smart networks and services. The vision is one of autonomous operation of the entire production chain in a dynamic market environment, integrating production systems, product lifecycle management and supply chains. Digital automation depends on collecting and analysing massive amounts of sensor data from real-time digital twins that are connected across all stakeholders in the industrial eco-system into a super twin. Challenges for digital automation include the integration and orchestration of complex real-time and AI-enabled systems across multiple stakeholders, while ensuring the safety, security and reliability of the connected production system.

Autonomous driving, Connectivity, Electrification, and Shared mobility (ACES) will shape the future automotive market, resulting in safer, environment-friendly, more efficient and cost-effective, and more customized mobility services. Those services might include navigation services with real-time updates for road and weather conditions, and AR-powered navigation, personalized infotainment, smart parking, remote diagnostics and predictive maintenance, over-the-air software updates, or pay-per-use and personalized insurance. Obviously, these services will benefit from the advanced capabilities and services provided by a future smart network and cloud computing infrastructure. However, they will also rely on the way that software and service engineering use these capabilities to build smart mobility services which provide appropriate performance and user experience. Thus, the automotive technology stack of smart mobility services shown in Figure 3 comprises the devices (i.e. the vehicles and roadside sensors), the connectivity layer connecting those devices, the distributed cloud layer for processing the huge amount of data generated by vehicles and roadside sensors, and a broad range of diverse mobility services[9]. Software-related challenges arise from integrating advanced SNS features into extremely complex in-vehicle software, aggregating and processing data in real-time across a distributed cloud environment, and developing application platforms capable of real-time analytics and strong integration with the hardware generating the data and which allow interactions between the many players involved in smart mobile ecosystems.

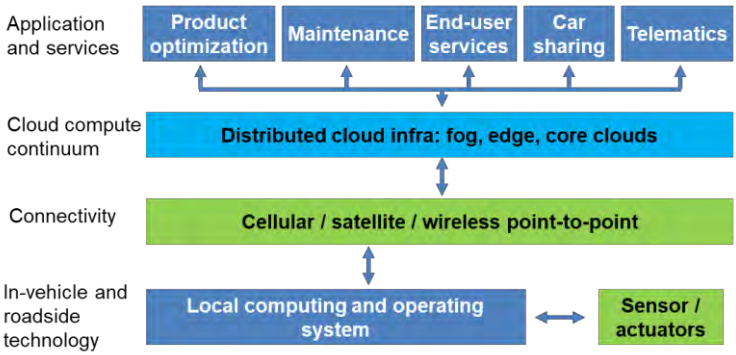

Figure 3 The automotive technology stack

Ecosystems enabled by SNS

Future smart networks will catalyse new business ecosystems, formed by SNS stakeholders such as network operators, infrastructure and equipment suppliers, device manufacturers, (vertical-specific) service and application providers, system integrators, as well as end users[10,11]. Advanced capabilities offered by smart

[9] Development in the mobility technology ecosystem—how can 5G help? McKinsey & Company, June 2019
[10] https://5g-ppp.eu/wp-content/uploads/2017/01/5GPPP-brochure-MWC17.pdf
[11] https://www.pwc.nl/nl/assets/documents/the-great-potential-of-5G-ecosystems.pdf

networks will enable these actors to co-develop new solutions and to discover new and potentially disruptive business models for capturing the value generated by these solutions, including B2C, B2B, but also B2B2X. They will increasingly share and mutually use data resources and AI/ML-based software components so that the line between producers and consumers will become even more blurred. Thus, SNS will also foster prosumer ecosystems at an industrial scale, involving communities of developers and prosumers working alongside with machine intelligence.

The success of these SNS ecosystems will depend to a great extent on the capabilities and value added services of the smart network infrastructure, and on the wide spread of devices connected to smart networks, together with the availability of applications and services running on top of smart networks, implementing use cases in vertical industries and in settings such as smart cities, automotive, and healthcare. Software technologies play a fundamental role in network infrastructures, devices and applications as enabler and differentiator: software is fundamental for building the capabilities and solutions that allow ecosystems to thrive and to create value, and superior software quality of a solution will provide differentiating customer experience. The importance of software will grow with the value of technology, and will shift from hardware and connectivity to software and applications. Figure 4 shows the growing share in the IoT value chain revenue that applications will have[12].

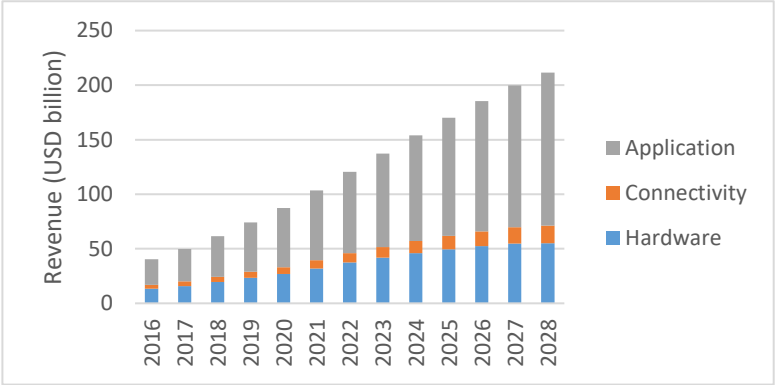

Figure 4 IoT revenue by technology (Source: Analysis Mason)

Accordingly, software-based capabilities of smart networks can be expected to play a significant role for the commercial success of SNS ecosystems, by addressing the digital needs for automation, for adaptive and customized services, and for agility in delivering complex but reliable and trusted systems.

Extreme automation in network operation and orchestration

Artificial Intelligence and Machine Learning will help to achieve extreme automation, which will be required not only to manage the increasing complexity of smart networks and to save operational cost, but also to increase speed and agility in providing digital services to the market

Flexible service-based architectures

Service-based (e.g. microservices based) architectures combined with DevOps offer greater agility for introducing new and enhanced functions required to stay competitive or to develop competitive advantages.

Network slicing and its evolution in SNS

Network slicing is a key concept allowing for flexible and resource-efficient service customization and provisioning to the many diverse verticals.

Compute continuum across cloud-based SNS

The compute continuum of smart networks will provide seamless access to the resources of the underlying distributed cloud infrastructures (including edge, fog and HPC resources), providing scalability to future multi-tenant and customized SaaS solutions.

[12] IoT forecast: connections, revenue and technology trends 2019-2028, Analysis Mason, January 2020

Standardized IoT infrastructure abstraction layer

Similar to and complementing the compute continuum, a software layer on top of an IoT SNS infrastructure can provide a global multi-vendor distributed platform that facilitates the management and utilisation of the capabilities of the infrastructure, including all the IoT devices connected to it.

Software engineering of infrastructure-aware applications

Design, development, operation and quality of new digital solutions and service offerings is dependent on the interplay of two parallel software engineering processes: software engineering enabling virtualization, management and operation of the emerging distributed computing and networks infrastructure, and software engineering enabling new end-to-end digital solutions and services as application software over the top of the emerging infrastructure. The quality and performance of digital innovations is dependent on seamless interplay of these two overlapping software engineering processes.

Software Research Challenges for Smart Networks and Services

Orchestration architectures going beyond virtualisation

To automatically manage resources in SNS we will need novel virtualization techniques and programming abstractions to allow devices, services and data to be composed and used, ideally without knowing the details about how they are implemented. An abstract network service representation enables on-demand processing anywhere, dealing with complexity of the physically distributed network underneath. To cope with the scale of accessible resources, abstractions should address flocks of cooperating resources as well as individual services and interactions. This is a form of reverse virtualization, in which physical entities are physically/logically grouped together under a single virtual interface for better reliability, increased quality of information, and better elasticity. They will need to handle IoT sensors and actuators and their (possibly dynamically changing) relationships with - and effects on - real-world entities, including humans (to enable for example smart mobility services or the multimodal interactions in spatial computing). Emerging technologies will also need to be supported, including AI components providing embedded intelligence, specialised processors (e.g. neuromorphic chips or tensor processing units), and quantum computing devices.

These innovations in resource abstraction and orchestration models will require a new and more general-purpose SNS architecture. The need for low cost, automated governance will still favour virtualisation as the main ingredient, especially when handling dynamically changing requirements as users connect, move around and disconnect, and as applications respond by migrating workloads. However, some aspects cannot be virtualised, e.g. physical, real-world elements of IoT devices, or quantum information processing models. The SNS architecture must go beyond virtualisation, using a range of abstractions to achieve the same benefits for agile, automated composition and management of resources. Where necessary and appropriate, standards and regulations must be developed to allow these new orchestration architectures. For example, standardised APIs will be needed for accessing IoT devices at and from the edge, and for QoS levels, cyber security, privacy and other regulatory compliance. New models and tools will also be needed for software engineering, for business engagement, for trust, security and dependability, and for user interactions.

Software for sustainable business models

Building an SNS infrastructure will require huge investments by network operators. In order to afford these investments and to obtain sufficient return on it, operators will not only increase automation of network operations to save opex, but also try to tap additional revenue streams based on new business models and service offerings that provide value to a broad range of diverse verticals by addressing their specific needs. The section ‘Ecosystems enabled by SNS’ (above) lists advanced software-based capabilities that will play a

key role in developing and providing those services and business models. The list includes service-based architectures, the evolution of network slicing, the compute continuum across the distributed cloud infrastructure of SNS and its extension to include IoT devices, and the software and service engineering methods required to develop SNS-optimized applications. The challenge will be to develop these capabilities in a coherent way so that they best support SNS ecosystems and their business models.

In order to make these business models sustainable, SNS will need to address societal priorities, such as the need for energy efficiency and minimisation of environmental impact. SNS can provide powerful tools to monitor natural and human activities and support decisions that reduce the consumption of resources and energy from non-renewable sources. However, digital systems produce their own environmental footprint which must itself be managed and minimised. For SNS this will require continuous evaluation and optimisation of the use of hardware resources and of the way software is developed to make best use of this hardware. In many domains, migration to cloud infrastructures and the use of agile DevOps methods has led service designers and developers to focus more on time-to-market and continuous functional improvements. Self-adaptation and AI/ML, including the desire to collect increasing volumes of data to facilitate the use of AI, may contribute to greater focus on those aspects and less on sustainability. The challenge will be to address the demand of service developers and end users while maintaining the craftsmanship necessary to provide optimized and energy-efficient infrastructures, and software foundations and tools, in a design-to-cost and design-to-energy-efficiency manner.

Sustainable business models and the solutions they are based on must also follow legal and ethical guidelines. For example, frictionless optimisation across cloud, edge and fog platforms will be important to meet application requirements for latency and performance, and to meet operator requirements for efficient utilisation of resources. However, these will need to be balanced against the need for data to remain under the control of its owner, even while it is dispersed in computing and storage devices from the data centre to the edge, in support of performance and efficiency goals. Ethical aspects are a focus when it comes to self-adapting intelligent systems using AI decision-making algorithms in network operations and service enablement. Organisations such as ACM have published codes of ethics[13], and the European High-Level Expert Group on Artificial Intelligence has drafted AI ethics guidelines and indicated already some technical methods how to achieve trustworthy AI[14]. Those methods refer to the classical stages of the software development lifecycle, and cover architectures, design, test, and the auditability of software and AI systems. These guidelines also call for research that is needed to advance engineering of software systems and the engineering of AI-based systems so that the resulting systems are compliant with ethical standards. This will be extremely challenging in dynamically changing environments, and in some situations the solution may depend on AI-based systems being transparent and explainable. These issues, and the need for multidisciplinary approaches to address them, are also covered at length in the NESSI position paper 'Software and Artificial Intelligence' [4].

Managing complexity

Smart networks will be a highly distributed and decentralised system of systems comprising countless heterogeneous physical and virtual entities and supporting a broad range of services and applications with divergent requirements. The countless entities need to be managed throughout their lifecycle and to have their parameters configured and adapted to a dynamically changing environment. The services have to be of high quality and provided in flexible ways to meet users' demanding expectations, whilst consuming network

[13] ACM Code of Ethics and Professional Conduct, https://ethics.acm.org/, 2018
[14] Draft Ethics Guidelines for Trustworthy AI, https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai, 2018

resources as efficiently as possible to minimize cost. Managing the resulting system complexity will become increasingly challenging and will require new operational concepts based on sophisticated self-adaptation models and relying heavily on AI algorithms.

Developing, debugging and testing such complex cognitive systems will be challenging. The conflicting requirements of extreme flexibility, dynamic adaptation and optimized resource utilization are hard to reconcile in a distributed system of autonomous AI-based subsystems, and the resulting overall system behaviour might be unexpected.

To avoid unexpected and even hazardous effects, what is needed is predictable governance for self-adapting AI-based software systems. This implies that AI/ML algorithms have to be made aware of changes in the surrounding system that impact the learned model, and would require re-training. It also involves explainable AI, for transparency of how an AI-based system works and responsibility for the resulting output. Access to high-quality training data needs to be assured, so that no undetected biases find their way into AI systems.

Security and dependability

Cyber-attacks are predicted to continue growing in frequency and scale. The Internet is already a critical infrastructure and will become more critical as smart services are increasingly used in sectors such as energy, health care and transportation. Smart networks and services must become far less vulnerable than today's networks, where software is the main cause of vulnerability. It is estimated that 111 billion lines of new software is written every year with billions of vulnerabilities[15,16], and most critical applications require penetration tests to discover and remove vulnerabilities.

In future, some software as well as system configuration data will be generated dynamically by self-adapting applications and resources, and AI algorithms will be created whose behaviour depends on the data they encounter. Penetration tests for key software and services will still be important but cannot provide high levels of security when services which are initially protected may be exposed by future changes, or when software is created dynamically at run-time. At the same time, the supply chain for SNS is becoming more complex and diverse[17], with new and existing players (integrators, service providers and software vendors) being more involved in the configuration and management of key parts of the network.

A holistic approach to security is needed, spanning the lifecycle of smart networks and services, using secure software engineering and operational security procedures together to manage risks. Developers will need better tools for 'security by design' and for creation of code that cannot easily be exploited by attackers, while run-time stakeholders (SNS operators and all types of users) will need collaborative methods and tools to manage risks in the face of dynamically evolving requirements and threats. It is not possible to achieve 100% security, so more emphasis must be placed on managing risks to protect vulnerable stakeholders and resources and achieving resilience. Intrusion tolerance will be important so that the inevitable but hopefully infrequent breaches can be contained, and serious harm prevented. This may require unconventional approaches inspired by biological defence systems, whereby a new security exploit is met by self-adaptation to immunise resources and prevent attacks spreading to large numbers of devices, as it has been the case with exploits such as MIRAI[18] and Krack[19]. Security measures must also cope with new and potential new

[15] https://cybersecurityventures.com/application-security-report-2017/
[16] https://www.enisa.europa.eu/publications/info-notes/is-software-more-vulnerable-today
[17] See https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049: EU coordinated risk assessment of the cybersecurity of 5G networks.
[18] https://en.wikipedia.org/wiki/Mirai_(malware)
[19] https://en.wikipedia.org/wiki/KRACK

developments in areas such as AI and quantum computing, whether they are used by attackers or used to protect SNS resources and users.

Building digital trust

Trust in Internet services is already under threat on two fronts. The first is the increased concern about the liberties taken with citizens' personal data. Citizens need control of their valuable and possibly sensitive data. Security mechanisms are already able to enforce access restrictions, but data owners currently lack the means to understand the implications of their decisions and manage access based on the consequences. This can lead to excessive risk aversion and stifle data sharing. The second concern is the potential use of the Internet for misinformation and propaganda, which may lead to harmful societal consequences such as polarisation, intolerance or extremism. This is linked to the use of personal data to profile users. SNS may allow the creation of private channels to influence specific groups via advertising (which may be legitimate) or propaganda (which is not). The impact of SNS will be limited if risk-averse users refuse to share data fearing it may be misused, or reject advanced applications because they feel manipulated. Without trust, services such as health care or applications such as online elections may not be viable.

Ways to verify data authenticity and truthfulness will be needed, along with trusted digital interactions, especially in dynamically-composed service environments. Trusted identities and authentication services for software and devices as well as humans are essential, along with access control mechanisms that users can understand, to manage their data and protect themselves from manipulation. Smart contracts and distributed ledgers, trusted hardware, and homomorphic encryption may provide links in the chain of trust, but the key is to use security measures to support a holistic network of trust between stakeholders. Fact-checking services based on AI may play a role, as may services that govern the AI to ensure that novel technologies and applications remain compatible with societal needs such as the right of individuals to freedom of expression. Authenticity must be demonstrable, not just for data but also for the consequences of using data in AI-enabled decision-making algorithms. Technologies alone will not be enough – they must be deployed in a citizen-centric fashion, giving humans control over their interactions.

To achieve high levels of trust, software engineering methodologies and tools must provide the trust anchors needed by stakeholders: software developers, service operators, business customers and consumers, regulators and certification agents. Some work is ongoing to address trust in data sharing[20,21], which could be embedded into a trustworthy software methodology. Certification of products and services will be important, and will play an essential role in regulation to ensure security and safety in sectors such as medical IoT. As certification procedures are expensive, software engineering methods will be needed to implement them for dynamically changing systems in a cost-effective way, e.g. by focusing on critical sub-systems or operational contexts. In some areas, new procedures and standards (similar to ISO 26262) will be needed, e.g. to certify software based on machine learning/AI, for which there are no established methods today.

Engineering software intensive systems

The scope of software engineering must be expanded to encompass the full range of possible deployments from embedded devices to the cloud, and the full lifecycle of the software including automated operation of self-adapting software intensive systems. This unification of operational and business aspects is not supported by adequate software tools today. Software engineering methods such as UML modelling cannot handle situations where interconnected services are not known in advance, and cannot easily model

[20] The International Data Spaces Association has a technical specification for trust on data, with implementations and services under development; see https://www.internationaldataspaces.org/

[21] GAIA-X is addressing trust and data sovereignty; see https://www.bmwi.de/Redaktion/EN/Artikel/Digital-World/data-infrastructure.html

consequences that may have a legal or ethical dimension. Some aspects previously considered the domain of programmers such as the composition of resources and services will also need to be handled autonomously at run-time. Therefore we need new engineering approaches which can be applied over the lifecycle of software services and data (including design, implementation and testing); respond to agile changes in self-adapting systems; handle ethical and legal aspects; and support purposeful sharing.

The coherent use of DevOps tools and methodologies has greatly increased productivity by introducing a high degree of automation in the production of software, and this is one of the key enablers in the rise of cloud computing. DevOps can unlock the potential of smart networks and services in a similar way, but the emphasis on agility and rapid development of products works against the requirements for greater security and trustworthiness, greater efficiency in the use of ever more diverse resources, and societal goals for fairness and compliance with regulations that protect both fundamental human rights and the cost-effective operation of market forces. DevOps applied in cloud computing transformed software development from 'creating the service' to 'controlling the cost of the service'. As the infrastructure starts to incorporate edge devices interacting with the physical world, the emphasis may evolve into one that seeks to control the world. This poses new challenges: how to model the world (e.g. using simulation models and techniques like 'digital twins'), how to test software and services interacting with the world, and how to consolidate and optimise so SNS will be economically and environmentally sustainable. Possibly the most challenging aspect of all is the need for new software engineering methods to engage with and meet the needs of multiple stakeholders. Today, it is becoming best practice that interaction designers (IxD) join multi-disciplinary software development teams, and that design thinking methods complement agile software development[22], both enhancing the interaction capabilities and the human-centricity of applications. In future, co-creation models for new software intensive technologies (now in their infancy) must be broadened and deepened to address the needs of whole SNS ecosystems, possibly informed by other applications of co-creation principles such as patient engagement in the development of health care[23].

The use of AI presents both challenges and opportunities for software engineers. As previously noted, operating software on a large-scale, distributed, heterogeneous and smart infrastructure requires new approaches such as AI. Can AI also be used to support the evolution of DevOps methods for software design and development? How will those methods enable the design and development of smart components that use AI, and ensure that those components meet ethical, legal, social and economic requirements as they evolve in the presence of new input data? The approaches developed must be able to handle requirements and constraints not only in the use of AI, but also of other novel technologies such as specialised (including quantum) processing devices, and novel modes of human-computer interaction.

[22] https://www.interaction-design.org/literature/topics/design-thinking
[23] Patient and Public Participation Policy, NHS England, 2017; see https://www.england.nhs.uk/wp-content/uploads/2017/04/ppp-policy.pdf

Recommendations for Horizon Europe and SNS

To meet the above challenges will require support for software innovation in multiple areas.

- Development of new, more powerful orchestration models, architectures and abstractions for highly distributed, heterogeneous and multi-stakeholder infrastructures and resources.
- Enabling new business models for monetizing SNS and for controlling environmental and social impacts, making SNS applications sustainable and justifying investment in infrastructure.
- Management of complexity in the presence of dynamically changing and uncertain future requirements arising from and addressed by using self-adaptation powered by artificial intelligence.
- Building trust in applications and services with high levels of security and dependability, preventing manipulation of humans by SNS technologies as well as protecting critical services and sensitive data.
- New methodologies for software and information systems engineering, maintaining productivity while addressing increased complexity and (in some cases) criticality, and balancing the need for agility with the need for consolidation and optimisation in the use of resources.
- Incorporating new methods combining software engineering and data science approaches to ensure quality, performance and cost-efficiency for software incorporating AI algorithms.