Software and the Next Generation Internet

Executive summary

This paper is an analysis by NESSI[1] of how research in software technologies can best meet the needs of the Next Generation Internet (NGI) initiative, which is about to re-engineer today's Internet so that it "enables human potential, mobility and creativity of the largest possible scale."[2]

Software is a key element of this development, and places huge demands on the processes for software design, implementation, integration, operation and assurance of the intended outcomes. NGI will raise the bar in terms of system complexity, automation and intelligent adaptation. To deliver on the potential of NGI requires research and innovation to address challenges in:

- management of complexity in highly distributed, heterogeneous infrastructure and applications by using AI, and supported by standards designed for automated compliance checking;
- counteracting significant threats to trust from the erosion of authenticity and truthfulness and the potential abuse of personal data in online services;
- maintaining dependable service in the face of increasing threats from cyber-attacks, including managing risks and containing intrusions, and addressing threats from new technologies; and
- re-engineering software engineering processes for design, implementation and operation of systems composed dynamically from self-adapting components, assuring outcomes that comply with regulations and ethical requirements.

To meet these challenges will require innovative application and integration of digital enablers: ubiquitous connectivity, hyper-scalability, human centricity and artificial intelligence.

Software is a key digital technology for the Next Generation Internet

Software is one of the corner stones of digital technologies along with hardware, networking and data. Consequently, software is also a key digital technology for NGI and must meet its fundamental needs.

NESSI has previously analysed[3] the importance and impact that software has for the digitalization of Europe and how advances in software will meet the fundamental digital needs, which are perceived to be:

- Automation of processes and entire systems;
- Implementation of adaptive and cognitive services;
- Speed and agility in providing new functionalities; and
- Integration of systems into even more complex systems of systems.

Developing these advanced technologies will require research in the eight areas shown in *Figure 1*.

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

[2] Next Generation Internet 2025, European Union, 2018

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

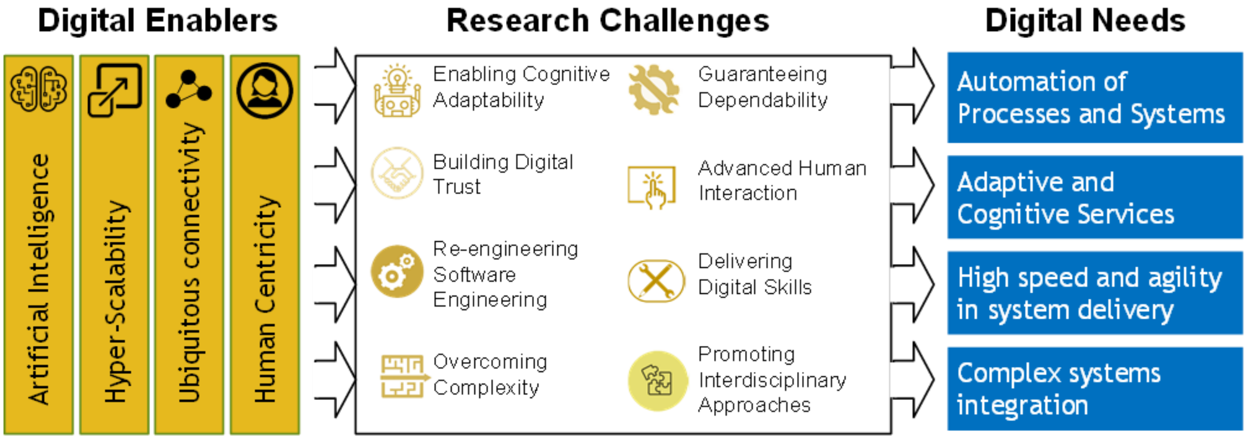
Digital Enablers
Artificial Intelligence
Hyper-Scalability
Ubiquitous connectivity
Human Centricity
Research Challenges
Enabling Cognitive Adaptability
Guaranteeing Dependability
Building Digital Trust
Advanced Human Interaction
Re-engineering Software Engineering
Delivering Digital Skills
Overcoming Complexity
Promoting Interdisciplinary Approaches
Digital Needs
Automation of Processes and Systems
Adaptive and Cognitive Services
High speed and agility in system delivery
Complex systems integration

Figure 1 Research challenges for the use of digital enablers to address digital needs

The Next Generation Internet initiative aims to shape a future human-centric Internet "as an interoperable platform ecosystem that embodies the values that Europe holds dear: openness, inclusivity, transparency, privacy, cooperation, and protection of data."[4] In order to achieve this visionary goal, digital technologies have to support the fundamental needs of the NGI, including:

- Enabling creativity and leveraging human potential, which will rely on advanced multi-modal and highly personalised digital interactions, and will require interdisciplinary approaches, and cognitive adaptability of software systems;
- Ensuring adaptability, resilience and reliability through the use of adaptive, intelligent services combined with the means to manage complex software systems;
- Building digital trust to underpin transparency and ease of use in the NGI, including building skills needed to participate in the new digital world, and ensuring NGI services behave fairly and meet other legal and ethical requirements; and
- Engineering software systems to manage complexity and interoperability challenges, maintain security and quality of service, while avoiding walled garden responses that destroy openness.

The research challenges associated with the future evolution of software and software creation and use are to address the needs of digitalisation in such a way that these requirements are met. Only through such advances in software related technologies can the goals of the NGI be achieved, as indicated in *Figure 2*.

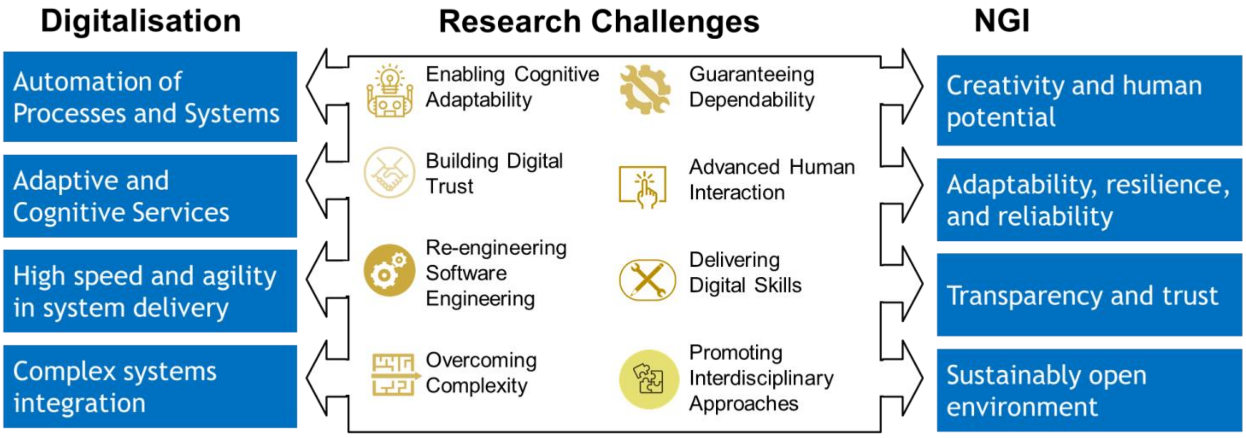
Digitalisation
Automation of Processes and Systems
Adaptive and Cognitive Services
High speed and agility in system delivery
Complex systems integration
Research Challenges
Enabling Cognitive Adaptability
Guaranteeing Dependability
Building Digital Trust
Advanced Human Interaction
Re-engineering Software Engineering
Delivering Digital Skills
Overcoming Complexity
Promoting Interdisciplinary Approaches
NGI
Creativity and human potential
Adaptability, resilience, and reliability
Transparency and trust
Sustainably open environment

Figure 2 Software research areas for the Next Generation Internet

[4] https://ec.europa.eu/digital-single-market/en/next-generation-internet-initiative

How software research will meet the needs of the NGI

The NGI faces several challenges to deliver the expected benefits in boosting creativity and exploiting responsiveness from an agile, open, resilient, reliable and trusted infrastructure. In most areas, these will push against the current limits of software and the processes for producing software. In many cases, the challenges ultimately stem from the great complexity of the NGI, and the need to manage complexity and risks through automated (i.e. software controlled) means including the use of AI.

Challenges exist in all the areas identified by NESSI related to software lifecycle and applications[3]. The most important in relation to the NGI arise from its increased complexity; the need to (re-)build trust in the Internet and online services; guaranteeing dependability, especially in critical application sectors; supporting advanced human-machine interactions; and for software engineers in creating software that can address all these issues including the need to meet regulatory, ethical and other non-technical requirements.

Managing complexity

The trend of centralising data and processing at huge data centres accessed via cloud services cannot deliver the Next Generation Internet. Applications need low latency and large numbers of IoT devices, and this is driving an increased interest in edge and fog computing. The NGI will be decentralised and ubiquitous, characterized by hyper-connectivity capabilities (5G and beyond) and an increasing interoperability of systems (on average, 40% of the value that IoT applications can generate is achieved through the interoperability of IoT systems[5]). One benefit of centralised cloud services is simplified resource and service management. The new trend will lead to greater heterogeneity and complex resource management and optimisation problems including the optimisation of energy consumption across data centres. Computing and intelligence will be distributed between cloud, fog, edge and terminal devices with different performance and security properties arising from the device characteristics and their connectivity and proximity to users.

New methods will be needed to manage resources and services in this new and more complex environment and to allow efficient interworking of systems and their integration into complex systems of systems such as smart cities and smart mobility. These will need to handle dynamically changing requirements as users connect, move around and disconnect, and applications respond by migrating workloads and data between cloud data centres and the edge in Fog computing environments. Software frameworks may facilitate the design, development and operation of interoperable systems of systems. Furthermore, it seems inevitable that artificial intelligence will be one of the enablers for maintaining near optimal resource utilisation and quality of service. This presents new requirements for comprehensive monitoring to ensure AI algorithms can be trained and used effectively. Developing and deploying applications and middleware that use the different levels of computing devices is a challenge for software developers, who will have to consider non-functional characteristics, such as performance indicators, QoS levels, etc.

Where necessary and appropriate, standards and regulations must be developed to allow automated compliance checking to ensure interoperability in dynamic, heterogeneous compositions. These must include standardised APIs for accessing IoT devices at and from the edge, and standards for cyber security, privacy and other regulatory compliance.

Building digital trust

Trust in Internet services is already under threat on two fronts. The first threat is the increased concern about the liberties taken with citizens' personal data. Citizens need to regain control of their valuable and possibly sensitive data. Security mechanisms are already able to enforce access restrictions, but data owners currently

[5] The Internet of Things: mapping the value beyond the hype, McKinsey, 2015

lack a means to understand the implications of their decisions and manage access based on its consequences. This can lead to excessive risk aversion and stifle data sharing.

The second major concern relates to the use of the Internet as a channel for misinformation and propaganda, leading in many cases to harmful social phenomena such as polarisation, intolerance or extremism. One important aspect is the use of personal data to profile users and find ways to influence them via advertising (which may be legitimate) or propaganda (which is not). The impact of NGI will be very limited if risk averse users refuse to share data through fear it may be misused, or turn away from advanced NGI applications because they feel manipulated by its services. Applications with a high impact on society or citizens such as online elections or some health care applications may not be viable unless this challenge can be addressed.

We need ways to determine data authenticity and truthfulness as well as trusted digital interactions even in dynamically composed service environments. The foundation will come from online identities and authentication services for software and devices as well as humans, and access control mechanisms that can be made understandable to users and allow control over the full lifecycle for sensitive and/or personal data resources from creation to destruction. Trusted digital interactions may be enabled by smart contracts, i.e. software that runs on a blockchain and verifies and enforces a set of rules under which the parties of that contract agreed to interact and to perform transactions. Fact checking services may build on such security measures but must be compatible with freedom of expression and pluralism avoiding any form of censorship and any harmful consequences for users or for the Internet's technical functioning through effects such as fragmentation. More generally, authenticity must be demonstrable not just for the data itself, but also for the consequences of using data in AI-controlled decision-making algorithms. Technologies alone will not be enough – they must be used in a citizen-centric fashion, giving humans control over their NGI interactions.

Guaranteeing dependability

Cyber-attacks are predicted to continue growing in frequency and scale. The Internet is already a critical infrastructure, and the benefits of the NGI will allow greater use in critical sectors such as energy, health care and transportation. NGI infrastructure and services must be far less vulnerable than current generation networks. However, software is the main root cause for the vulnerability of those systems. It is estimated that 111 billion lines of new software is written every year with billions of vulnerabilities included[6]. Current statistics[7] confirm this dramatic increase in the number of software vulnerabilities.

To stop this trend, joined up approaches will be needed for collaborative operational security management. Many security standards exist covering software implementation and information system operation. These standards need to be combined to ensure overall security of NGI, and this requires development of an integrated approach. Multiple stakeholders and actors (e.g., developers, managers, operators and users) will need to be included in a holistic yet standardised security management process. Humans and automated (including AI) processes involved in managing the NGI will need to cooperate across organisational and jurisdictional boundaries. Software developers must be part of this joined up approach, and better tools are needed to support 'security by design', as well as reliable production of software code that does not provide ways for attackers to compromise or bypass operational security measures. As the security threats are frequently and continuously changing, providing developers with the ability to continuously evolve their services is decisive to ensure and increase their trustworthiness. Experience shows that it is not possible to achieve 100% security, so more emphasis must be placed on managing risks to ensure that most users are protected most of the time. Intrusion tolerance will be important so the inevitable (but hopefully infrequent) breaches can be contained and serious harm prevented. Security measures must also cope with new or

[6] https://cybersecurityventures.com/application-security-report-2017/
[7] https://www.enisa.europa.eu/publications/info-notes/is-software-more-vulnerable-today

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

Beyond traditional security mechanisms, non-conventional and more diversified approaches, possibly through a trans-disciplinary approach also encompassing Life Sciences, need to be investigated, to reduce the risk of a given exploit rapidly propagating to large numbers of devices, as it has been the case with exploits such as MIRAI[8] or Krack[9].

Re-engineering software engineering

Most modern technologies, including internet and AI, rely on software. Also the business value is moving away from HW to SW and service layers. This has a profound impact on the need for better methods and tools for software and information systems engineering. 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 software intensive systems. This unification of operational IT (OT) and business IT is not supported by adequate software tools today. Therefore, software research is an essential enabler for almost any kind of innovation and well as European competence on all kinds of products. Ways to do better software faster, use cleverer algorithms, provide better user experiences, create more robust software etc. are all dependent on software research. Traditional software engineering methods such as UML modelling cannot handle situations where interconnected services are not known in advance, and cannot easily model consequences that may have a legal or ethical dimension. Some aspects previously considered the responsibility of programmers such as the composition of resources and services will also need to be handled autonomously at run-time.

We need new engineering approaches that can be applied throughout the lifecycle of software services and data, respond to agile changes, handle ethical and legal aspects, and support purposeful sharing to deliver the promise of NGI. Developing code is not the only concern, as testing and maintenance frequently consume a larger share of lifecycle costs. Service composition and adaptation to meet performance and security requirements will be automated. The challenge with distributed highly adaptive and cognitive systems (including AI at the edge) is to ensure that they work reliably. Therefore, new methods, tools, and processes are needed to verify, validate and monitor highly distributed, intelligent and adaptive software in the NGI.

Of course, to achieve the high-level NGI goals, software engineering methodologies and tools must provide a basis for trust between NGI stakeholders: software developers, service operators, business customers and consumers, and also regulators and certification agents. The certification of products and services will also be an important issue, and in some sectors such as medical technology will play an essential role in regulation to ensure security and safety. As certification procedures are expensive, software design and development methods are needed that can safely limit their cost in dynamically changing systems, e.g. by focusing on critical sub-systems or operational contexts. In some areas, new procedures will be required, e.g. today there are no standards (similar to ISO 26262) which can be used to certify software based on machine learning/AI.

Finally, the approaches developed must be able to handle requirements from new technologies, e.g. programming requirements and constraints for the use of quantum computing devices.

Supporting advanced human interaction

Advancements in sensor technology, natural language processing, or computer vision, combined with the smart connectivity and real-time capabilities provided by the NGI will enable new multimodal ways of

[8] https://en.wikipedia.org/wiki/Mirai_(malware)

[9] https://en.wikipedia.org/wiki/KRACK

interacting with the digital world. Software is the indispensable substrate to build and shape these interactive systems and services and augment human experience, senses, and intelligence as never before. Software will underpin both the abstraction layers needed to map complex problems to understandable user choices, and the shaping and control of advanced user interfaces.

The importance of software in this context is obvious and known from the past. For example, the discipline of mobile software engineering was and is crucial for the success of mobile apps by addressing key challenges in mobile computing such as the software development across multiple and rapidly changing mobile platforms (e.g. 12 major releases of the Android operating system has been released since 2008) or energy-aware programming (energy-inefficient behaviour is one of the top reasons why users uninstall an app)[10]. Today, it is becoming best practice that interaction designers (IxD) join multi-disciplinary software development teams and design thinking methods complement agile software development[11], both enhancing the interaction capabilities and the human-centricity of applications.

In the future, an increased variety of smart devices and smart materials will offer interaction techniques ranging from voice and gesture to holograms and haptic. Their combination will provide novel interaction spaces supporting humans in their digital life and inspiring human imagination and creativity. Software will continue to play a fundamental role in making this happen. Human-centred software engineering processes need to be further advanced to allow incorporating input from multiple disciplines such as psychology, social science, or gaming. Formal languages will be required to describe complex interaction concepts and frameworks are needed to support the fusion of multimodal techniques. Specific challenges to be solved by software include for example cross-platform developments required because of the diversity of devices and materials as well as context-sensitive programming that must reconcile diverse requirements such as usability, user experience and acceptance, trust, security, and privacy.

Promoting interdisciplinary approaches

Next Generation Internet software and services will operate in a realm where non-functional concerns are not limited to performance and security. In the NGI, services will need to address ethical concerns such as fairness, as well as related regulatory requirements such as the protection of fundamental human rights.

Organisations such as ACM have published codes of ethics[12]. Also, 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[13]. 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 in particular so that the resulting systems are compliant with ethics standards. This will be extremely challenging in dynamically changing NGI 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 a separate NESSI paper on Artificial Intelligence[14].

[10] Future of Mobile Software for Smartphones and Drones: Energy and Performance, Abhijeet Banerjee and Abhik Roychoudhury, 2017 IEEE/ACM 4th International Conference on Mobile Software Engineering and Systems

[11] https://www.interaction-design.org/literature/topics/design-thinking

[12] ACM Code of Ethics and Professional Conduct, https://ethics.acm.org/, 2018

[13] Draft Ethics Guidelines for Trustworthy AI, https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai, 2018

[14] Software and Artificial Intelligence, NESSI, 2019.

Recommendations

Meeting the above challenges will require support for software innovation in multiple areas. Investment in software-related research is needed in Horizon Europe to support:

- Intelligent architectures, tools and middleware capable of managing complexity in heterogeneous environments with extensive distribution of software and data from the cloud to the edge, able to integrate human actors and decision-making using appropriate abstractions.
- Re-engineering software engineering to allow development of software able to meet requirements that change over time and can only be known at run-time in dynamic compositions managed by intelligent middleware and AI, and spanning the full lifecycle including operation as well as design and implementation.
- New security by design tools and security mechanisms to cope with the constraints of a wide range of devices and platforms, reduce the risk of a security weakness being able to propagate to many devices, and address new threats arising from technologies such as AI and quantum computing.
- Trust enablers including methods for identification, authentication and accreditation of devices, software and data resources as well as human users; citizen centric and understandable methods for controlling access to personal data, and services to check the quality of information, including data from sensors that may produce poor or unreliable measurements; and fact checkers to verify data from users and counteract propaganda while respecting human rights including free speech.

The first two recommendations are key requirements, without which other innovations are likely to be less effective. They require dedicated support as persistent research objectives with recurrent calls. The first is strongly linked to the requirements of NGI as a human centric evolution of today's Internet. The second is a key requirement for NGI as a dynamic, agile environment, but is also relevant to other initiatives (such as partnerships in AI and security). Together, they will underpin important economic and societal gains from NGI-related research, e.g. reducing the cost of certification for software-intensive systems, or delivering fair and ethical outcomes from automation and AI.

In some areas the challenge comes not only from gaps in capability but also from lack of operational capacity or best practice. These should be addressed in Horizon Europe, but are also relevant to Digital Europe:

- Tools and procedures to manage cyber security risks, involving software developers and operators over the full software lifecycle, and collaboration across national and organisational boundaries.
- Better ways to train and incorporate humans who may have expertise in different disciplines into socio-technical NGI applications and systems, including but not limited to involvement in managing accountability, security, quality of information, and purposeful sharing of data in complex systems.
- Development of new standards designed for automated compliance and/or low-cost certification, which may include non-functional metrics and monitoring approaches that cover social, ethical and legal as well as technical requirements such as transparency.

NGI aims to enable human potential, mobility and creativity, and will support achievement of the UN sustainable development goals[15], including for example building sustainable cities, ensuring good health and well-being, or fostering innovation for an inclusive and sustainable industrialisation. In this context, software technologies have to be advanced to support security by design, privacy by design, and also energy efficiency by design, digital inclusiveness by design, and system resilience by design. These developments will change the way humans interact with NGI infrastructure and applications, with intelligent adaptation handling some of the tasks we find most difficult in today's Internet, but also posing new challenges for accessibility by all citizens. It will therefore be necessary to develop an understanding of the skills needed for experts and ordinary citizens to engage in such systems, and of how these skills can be imparted to all classes of users.

[15] https://sustainabledevelopment.un.org