

FIVE TECHNOLOGY TRENDS AUGMENTING THE CONNECTED SOCIETY

Rapid advancements in the use of machines to augment human intelligence are creating a new reality in which we increasingly interact with robots and intelligent agents in our daily lives, both privately and professionally. The list of examples is long, but a few of the most common applications today are found in education, health care, maintenance and gaming.

My vision of the future network is an intelligent platform that enables this new reality by supporting the digitalization of industries and society. This network platform consists of three main areas: 5G access, automation through agility, and a distributed cloud. A set of intelligent network applications and features is key to hiding complexity from the network's users, regardless of whether they are humans or machines.

The ability to transfer human skills in real time to other humans and machines located all around the world has the potential to enable massive efficiency gains. Autonomous operation by machines with self-learning capabilities offers the additional advantage of continuous performance and quality enhancements. High levels of cooperation and trust between humans and machines are essential. Building and maintaining trust will require decision transparency, high availability, data integrity and clear communication of intentions.

The network platform I envision will deliver truly intuitive interaction between humans and machines. In my view, there are five key technology trends that will play critical roles in achieving the vision:

- #1 The realization of zero touch
- #2 The emergence of the Internet of Skills
- #3 Highly adaptable, cyber-physical systems
- #4 Trust technologies for security assurance
- #5 Ubiquitous, high-capacity radio

BY ERIK EKUDDEN, CTO

#1 THE REALIZATION OF ZERO-TOUCH

THE ZERO-TOUCH networks of the future will be characterized by the fact that they require no human intervention other than high-level declarative and implementation-independent intents. On the road to zero touch both humans and machines will learn from their interactions. This will build trust and enable the machines to adjust to human intention.

Compute and intelligence will exist in the device, in the cloud and in various places in the network. The network will automatically compute the imperative actions to fulfill given intents through a closed loop operation. Today's complex networks are designed for operation by humans and

the complexity is expected to increase. As machine learning and artificial intelligence continue to develop, efficiently integrating learning and reasoning, the competence level of machine intelligence will grow.

AUGMENTATION OF HUMAN INTELLIGENCE

The realization of zero touch is an iterative process in which machines and humans collaborate reciprocally. Machines build intelligence through continuous learning and humans are assisted by machines in their decision-making processes. In this collaboration, the machines gather knowledge from humans and the environment in order to build models of the reality. Structured knowledge is

created from unstructured data with the support of semantic web technologies, such as ontologies. The models are created and evolved with new knowledge to make informed predictions and enhance automated decision making.

To maximize human trust and improve decision quality, there is a need for transparency in the machine-driven decision-making process. It is possible to gain insights into a machine's decision process by analyzing its internal model and determining how that model supported particular decisions. This serves as a basis for generating explanations that humans can understand. Humans can also evaluate decisions and provide feedback to the machine to further improve the learning

process. The interaction between humans and machines occurs using natural language processing as well as syntactical and semantic analysis.

ROBOTS AND AGENTS COLLABORATE WITH HUMANS

In a collaborative scenario, a robot will be able to anticipate human intentions and respond proactively. For example, an assembly-line robot would automatically adapt its pace to the skills of its human coworkers. Such interactions require the introduction of explainable artificial intelligence to cultivate human trust in robots. Robots will work alongside humans to aid and to learn. Robots can also interact

with other digitalized components or digital twins to receive direct feedback. However, further advancements in robot design and manufacturing will be needed to improve their dexterity.

A software agent in a zero-touch network acts in the same way as a human operator. The agent should be able to learn the role in real time, as well as the pattern and the proper actions for a given task. In particular, it should be able to handle a wide range of random variations in the task, including contaminated data from the real world that originates from incidents and mistakes. These agents will learn through a combination of reinforcement learning (where the agent

continually receives feedback from the environment) and supervised/unsupervised learning (such as classification, regression and clustering) from multiple data streams. An agent can be pre-trained in a safe environment, as within a digital twin, and transferred to a live system. Domain knowledge is a key success factor when applying agents to complex tasks.

Techniques such as neural networks offer significant advantages in learning patterns, but the current approach is too rigid. Differential plasticity is another technique that looks promising. ☺

03

IR12

#2 THE EMERGENCE OF THE INTERNET OF SKILLS

THE INTERNET OF SKILLS allows humans to interact in real time over great distances – both with each other and with machines – and have similar sensory experiences to those that they experience locally. Current application examples include remote interactive teaching and remote repair services. A fully immersive Internet of Skills will become reality through a combination of machine interaction methods and extended communication capabilities. Internet of Skills-based systems are characterized by the interplay of various devices with sensing, processing and actuation capabilities near the user.

Current systems lack the audio, visual, haptic and telecommunication capabilities necessary to provide a fully realistic experience. To enable the Internet of Skills, the interplay between humans and robots, and between humans and virtual content, is of particular importance. Both industry and consumers are showing great interest and openness in using these new capabilities.

HUMAN SKILLS DELIVERED WITHOUT BOUNDARIES

An authentic visual experience requires real-time 3D video capturing, processing

and rendering. These capabilities make it possible to create a 3D representation of the captured world and provide the experience of being immersed in a remote or virtual environment. While today's user devices don't yet provide the necessary resolution, field of view, depth perception, wearability and positioning capabilities, the quality and performance of these technology components is steadily improving.

Spatial microphones will be used to separate individual sound sources in the space domain. This implies that there will be an increased amount of data needed to capture the audio spatial aspects. Spatial audio rendering performance is very much tied to efficient head-related filter models. New formats for exchanging spatial audio streams have been specified and compression techniques are being developed.

Haptic components allow users to feel shapes, textures, motion and forces in 3D. Devices will also track the motions and forces applied by the user during interaction. With current technologies the user needs to wear or hold a physical device, but future ultrasound based haptic devices will offer a contact-free solution. Standardization efforts for haptic communication will allow for a quicker adoption of haptic capabilities.

INSTANT INTERACTION AND COMMUNICATION

Communication between humans and machines will become more natural, to the point that it is comparable to interpersonal interaction. Natural user interfaces such as voice and gesture will be commonplace. The use of vision-based sensors will allow for an intuitive type of interaction. To better understand human-machine interaction there is a need to evolve the understanding of kinesiology, ergonomics, cognitive science and sociology, and to incorporate them into algorithms and industrial design. This would make it easier to convey a machine's intent before it initiates actions, for example.

Large volumes of 3D visual information impose high network capacity demands, making ultra-low latency and high bandwidth communication technologies essential. Enabling the best user experience requires the use of network edge computers to process the large volumes of 3D visual, audio and haptic information. This setup saves device battery lifetime and reduces heat dissipation, as well as reducing network load.

#3 HIGHLY ADAPTABLE CYBER-PHYSICAL SYSTEMS

A CYBER-PHYSICAL system is a composite of several systems of varying natures that will soon be present in all industry sectors. It is a self-organizing expert system created by the combination of model of models, dynamic interaction between models and deterministic communication. A cyber-physical system presents a concise and comprehensible system overview that humans can understand and act upon.

The main purpose of a cyber-physical system is to control a physical process and use feedback to adapt to new conditions in real time. It builds upon the integration of computing, networking and physical processes. An example of a cyber-physical system is a smart factory where mechanical systems, robots, raw materials, and products communicate and interact. This interaction enables machine intelligence to perform monitoring and control of operations at all plant levels.

SYNERGISTIC INTEGRATION OF COMPUTATION, NETWORKING AND PHYSICAL PROCESSES

The main challenge is the orchestration of the networked computational resources for many interworking physical systems with different levels of complexity. Cyber-physical systems are transforming the way people interact with engineered systems, just as the internet has transformed the way people interact with information. Humans will assume responsibility

on a wider operating scale, supervising the operation of the mostly automated and self-organizing process.

A cyber-physical system contains different heterogeneous elements such as mechanical, electrical, electromechanical, control software, communication network and human-machine interfaces. It is a challenge to understand the interaction of the physical, cyber and human worlds. System models will define the evolution of each system state in time. An overarching model will be needed to integrate all the respective system models while contemplating all possible dynamic interactions. This implies a control program that delivers a deterministic behavior to each subsystem. Current design tools need to be upgraded to consider the interactions between the various systems, their interfaces and abstractions.

MODEL OF MODELS CREATES THE CYBER-PHYSICAL SYSTEM

Within the cyber-physical system all system dynamics need to be considered through a model that interacts with all the sub-models. Many factors impact the dynamics of the interactions between the systems, including latency, bandwidth and reliability. For a wireless network, factors such as the device location, the propagation conditions and the traffic load change over time. This means that networks need to be modeled in order to be integrated in the model of models.

The time it takes to perform a task may be critical to enable a correctly functioning

system. Physical processes are compositions of many things occurring in parallel. A model of time that is consistent with the realities of time measurement and time synchronization needs to be standardized across all models.

EXAMPLE: INDUSTRY 4.0

The factory of the future implements the concept of Industry 4.0, which includes the transformation from mass production to mass customization. This vision will be realized through large-scale industrial automation together with the digitalization of manufacturing processes.

Humans assume the role of supervising the operation of the automated and self-organizing production process. In this context it will be possible to recognize all the system models that need to interact:

- Physical and robotic systems such as conveyors, robotic arms and automated guided vehicles
- Control systems such as robot controllers and programmable logic controllers for production
- Software systems to manage all the operations
- Big data and analytics-based software systems
- Electrical systems to power machines and robots
- Communication networks
- Sensors and devices.

The master model consists of and interacts with all the listed processes above, resulting in the realization of the final product. 🌐

#4 TRUST TECHNOLOGIES FOR SECURITY ASSURANCE

TRUST TECHNOLOGIES will provide mechanisms to protect networks and offer security assurance to both humans and machines. Artificial intelligence and machine learning are needed to manage the complexity and variety of security threats and the dynamics of networks. Rapidly emerging confidential computing – together with possible future multi-party computation – will facilitate secure cloud processing of private and confidential data. Performance and security demands are driving the development of algorithms and protocols for identities.

The use of cloud technologies continues to grow. Billions of new devices with different capabilities and characteristics will all be connected to the cloud. Many of them are physically accessible and thus exposed and vulnerable to attack or to being misused as instruments of attack. Digital identities are needed to prove ownership of data and to ensure that services only connect to other trustworthy services. Flexible and dynamic auditing and compliance verification are required to handle new threats. Furthermore, there is a need for automated protection that adapts to operating modes and performs analytics on the system in operation.

PROTECTION DRIVEN BY ARTIFICIAL INTELLIGENCE

Artificial intelligence, machine learning and automation are becoming important tools for security. Machine learning addresses areas such as threat detection and user

behavior analytics. Artificial intelligence assists security analysts by collecting and sifting through threat information to find relevant information and computing responses. However, there is a need to address the current lack of open benchmarks to determine the maturity of the technology and permit comparison of products.

While the current trend is to centralize data and computation, security applications for the Internet of Things and future networks will require more distributed and hierarchical approaches to support both fast local decisions and slower global decisions that influence local policies.

CONFIDENTIAL COMPUTING TO BUILD TRUST

Confidential computing uses the features of enclaves – trusted execution environments and root of trust technologies. Code and data is kept confidential and integrity protection is enforced by hardware mechanisms, which enable strong guarantees that data and processing are kept confidential in the cloud environment and prevent unauthorized exposure of data when doing analytics. Confidential computing is becoming commercial in cloud systems. Research is underway to overcome the remaining challenges, including improving the efficiency of the trusted computing base, reducing context switch overheads when porting applications and preventing side channel information leakage.

Multi-party computation enables parties to jointly compute functions over

their combined data inputs while keeping those inputs private. In addition to protecting the confidentiality of the input data, multi-party protocols must guarantee that malicious parties are not able to affect the output of honest parties. Although multi-party computation is already used in special cases, its limited functionality and high computation complexity currently stand in the way of wide adoption. Time will tell if it becomes as promising as confidential computing.

PRIVACY REQUIRES SECURE IDENTITIES

Digital identities are crucial to maintaining ownership of data and for authenticating and authorizing users. Solutions that address identities and credentials for machines are equally important. The widespread use of web and cloud technologies has made the need for efficient identity solutions even more urgent. In addition, better algorithms and new protocols for the transport layer security provide improved security, lower latency and reduced overhead. Efficiency is particularly important when orchestrating and using identities for many dynamic cloud systems, such as those realized via microservices, for example.

When quantum computers with enough computational power are available, all existing identity systems that use public-key cryptography will lose their security. Developing new secure algorithms for this post-quantum cryptography era is an active research area. ☺

#5 UBIQUITOUS, HIGH-CAPACITY RADIO

THE WIRELESS access network is becoming a general connectivity platform that enables the sharing of data anywhere and anytime for anyone and anything. There is good reason to believe that rapidly increasing data volumes will continue in the foreseeable future. Ultra-reliable connectivity requires ultra-low latency, which will be needed to support demanding use cases. The focus will be on enabling high data rates for everyone, rather than support for extremely high data rates that are only achievable under specific conditions or for specific users.

A few technologies will need to be enhanced in order to create a ubiquitous, high-capacity radio network. The common denominator for these technologies is their capability to enable and utilize high frequencies and wide bandwidth operations. Coverage is addressed through beamforming and flexibility in device interworking. The challenge is to support data volumes and demanding-traffic use cases, without a corresponding increase in cost and energy consumption.

DEVICES ACT AS NETWORK NODES

To enhance device coverage, performance and reliability, simultaneous multi-site connectivity across different access

technologies and access nodes is required. Wireless technology will be used for the connectivity between the network nodes, as a complement to fiber-based networks. Device cooperation will be used to create virtual large antenna arrays on the device side by combining the antennas of multiple devices. The borderline between devices and network nodes will be more diffuse.

Massive heterogeneous networks will have a much more mesh-like connectivity. Advanced machine learning and artificial intelligence will be key to the management of this network, enabling it to evolve and adapt to new requirements and changes in the operating environment.

NO SURPRISE – EXPONENTIAL INCREASED DATA RATES

Meeting future bit rate demands will require the use of frequency bands above 100 GHz. Operation in such spectrum will enable terabit data rates, although only for short-range connectivity. It will be an implementation challenge to generate substantial output power and handle heat dissipation, considering the small dimensions of THz components and antennas. Spectrum sharing will be further enabled by beamforming, which is made possible by the high frequency.

Integrated positioning will be enabled by high-frequency and wide-bandwidth operation in combination with very dense

deployments of network nodes. High-accuracy positioning is important for enhanced network performance and is an enabler for new types of end-user services. The positioning of mobile devices, both indoor and outdoor, will be an integrated part of the wireless access networks. Accuracy will be well below one meter.

A NEW TRADE-OFF BETWEEN ANALOG AND DIGITAL RADIO FREQUENCY HARDWARE

For the past 20 years there has been a continuous trend toward moving functionality from the analog to the digital radio frequency domain. However, the trend is reversed for very wide band transmission at very high frequencies, in combination with a very large number of antennas. This means that a new implementation balance and interplay between the analog and digital radio frequency domains will emerge. Increasingly sophisticated processing is already moving over to the analog domain. This will soon also include utilizing correlations between different analog signals received on different antennas, for example. The compression requirements on the analog-to-digital conversion is reduced. The split between analog and digital radio frequency hardware implementation will change over time as technology and requirements evolve. ☺