We continue our discussion with Ovidiu Vermesan, this time covering the impact that COVID 19, security and sensing has had on the development of the Internet of Things (IoT).

How and when shall we expect the IoT to morph into IoTS?

OVIDIU VERMESAN: Internet of Things Senses (IoTS) is part of the IoT concept involving new sensing technologies that can reproduce, over the Internet, the senses of sight, hearing, taste, smell, and touch, enabled by AI, augmented reality and virtual reality (AR/VR), intelligent connectivity, and automation. The IoTS developments are essential for the IoT considering that AI algorithms can implement the cognitive decision-making capabilities of the devices for the intelligent IoT devices (e.g. robotic things) at the edge and experienced by humans with assistance of AR/VR.

The Tactile IoT/IIoT is expected to be the first implementation of IoTS around 2030. Tactile IoT/IIoT represents a transformation in the Internet collaborative paradigm, adding sensing/actuating capabilities that can be transported over network communications modalities. People and machines/devices no longer need to be physically close to the systems they operate or interact with as they can be managed remotely.

Tactile IoT/IIoT connects ultra-low latency with extremely high availability, reliability, and security, and enables humans and machines/devices to interact with their environment, in real-time, using haptic interaction with visual feedback, while on the move and within a specific spatial communication range.

The next generation of connected, autonomous vehicles will make use of the principles of IoTS as the vehicles need to have real-time perception systems to sense the environments and require real-time connectivity and a significant quantity of data collecting and processing. Through IoT applications and services, these vehicles share information about the road, the actual path, traffic, pedestrians, surroundings, local map/landscape, infrastructure, and how to navigate around any obstacles. This information can be shared between IoT connected vehicles and uploaded wirelessly to the edge or/and cloud system to be analyzed, improving the automation and automated/autonomous driving functions and levels of each vehicle.

Are we becoming more secured or more vulnerable along with the digitalization?

OVIDIU VERMESAN: IoT devices generate large amounts of data used in decision-making processes for digitizing industry (e.g. predictive maintenance, environmental monitoring, autonomous systems coordination, etc.). The data generated at the edge by IoT and IIoT devices are used in different industrial applications and could be vulnerable to cyberattacks and manipulation. Nevertheless, the degree of vulnerability when data is generated at the edge is much lower than the alternative, namely the centralized configuration. If designed and implemented with end-to-end security, safety and privacy-by-design, the edge technology should increase the trustworthiness for IoT/IIoT applications.

IoT/IIoT technologies are the critical enablers of digital transformation and catalysts in the move towards autonomous models for collaboration among machines and remote work to secure employee environment safety, flexibility, and continuity. In this context, it is critical for the IoT/IIoT to guarantee reduced vulnerabilities from cyber threats, which are advancing due to the proliferation of IoT-based digital systems.

How is IoT/IIoT evolving and adapting in these COVID challenging times?

OVIDIU VERMESAN: In the process of digitization of industries, IoT/IIoT are seen as enablers and catalysts of this transformation towards automated and digitized processes.

The need for a more automated process accelerates the development of new IoT connected products and services to achieve a competitive advantage in the market. As COVID-19 has led to an increasing customer need for more transparency and visibility of operations, IoT/IIoT applications will play a crucial role in the future. The IoT/IIoT brings ingredients such as data collection, AI processing at the edge, real-time monitoring, control, and autonomy, that are key for the digital transformation of all industrial sectors.

The use of IoT/IIoT technology will only accelerate as COVID-19 moves the technology from a long-term business strategy at many firms to an immediate business necessity in the healthcare, business, and industrial sectors. Using IoT for COVID-19 safety is a priority for many industrial firms.

IoT technology is deployed by several companies to keep track of their pest populations. IoT powered sensors in vineyards upload data on multiple parameters, like soil humidity, air humidity, sunshine, and intensity of sun, temperature, and rainfall, to the cloud. Predictive maintenance is frequently applied to building management and industrial manufacturing, where IoT finds its application for optimizing processes and operations.

Smart sensors in devices can help bring better waste management, intelligent street lighting, and better parking. IoT technologies have redefined our immediate surroundings.

IoT-based digital systems can support employees to collaborate remotely and enable operations to be executed on remote manufacturing sites. Remote monitoring of production setup and machinery using IoT solutions supports continuous manufacturing processes even in cases of pandemic crises.
Another example, the built environment is expected to undergo essential changes as AEC firms are requested by their clients to reconsider designs to deal with people assembly, making wellness and other infection control measures.

On the other hand, Covid-19 has driven the proliferation in cyberattacks and shifts in hackers' strategies, requiring organizations using IoT technologies to take more precautions and redefining the IoT security techniques and strategies.

IoT and edge computing generate real business value with benefits in improving operational efficiency and creating new connected products and services. During the current pandemic, the IoT adopters realized that the IoT was a crucial factor in maintaining business continuity throughout the period and this prompted them to accelerate the pace of adoption to create sustainable, long-term, competitive advantage.