# TUNNEL SENSORS 4.0 – NETWORKED TUNNEL SENSORS FIT FOR THE FUTURE

[1]René Jung
[1]JES Elektrotechnik GmbH, A

## ABSTRACT

The objective of this essay is to discuss how to introduce the concepts of Industry 4.0 like the Internet of Things (IoT) in transport infrastructure environments like tunnels.

Future generations of sensors will connect to an IP network like the Internet or a road operator's private corporate network. All other devices within the same IP network can remotely access the sensors. This bears a few risks regarding cybersecurity but none of them is nowadays uncommon especially that most sensors operate in corporate networks and such cannot be accessed from public networks. Direct access to sensors within corporate networks offers benefits and enables applications not possible in traditional topologies.

For example, communication amongst IoT-enabled sensors in the same network can cater for a higher reliability. Sensors could check their measured values for plausibility by comparing their measurements with other sensors that should indicate similar values. EDGE computing can create virtual sensors out of different measurements or redundant sensors.

Condition monitoring is the basis of modern maintenance strategies saving maintenance cost by performing maintenance only when indicated, and at the same time improves availability. Its implementation requires live condition data from sensors. Remote maintenance saves further cost, no matter if performed by tunnel operator's own maintenance staff or even by experts of the manufacturer.

Technologies of Industry 4.0 are proven and ready but sensor manufacturers, system integrators and tunnel operators need to work together to ensure that IoT-enabled sensors can easily integrate in tunnel control systems and tunnel operators' corporate IP networks. This may require some standardisation and/or guidance regarding protocols and models for data exchange.

*Keywords: Sensors, Industry 4.0, IoT, interfaces, protocols, remote access, condition monitoring, remote maintenance, configuration, software updates*

## 1. INTRODUCTION

IP networks in traffic infrastructure have quickly developed in the last years. Some road operators' corporate networks today are available throughout tunnels. Current tunnel sensors have not kept pace and many still use analogue outputs for measured values and relays for status information though they internally process information in a digital form. Besides, modern sensors have much more useful information available which today is "lost" in the interface to the tunnel control system.

Many sensors offer analogue outputs and relays as well as traditional 2- or 4-wire interfaces like RS-232 or RS-485 with field bus protocols like MODBUS RTU or Profibus DP. These sensors cannot seamlessly connect to a modern IP network infrastructure. Instead, a PLC part of the tunnel control system picks up their signals.

Many operators or integrators still prefer to use the analogue and relay outputs because these outputs are standardised and "can be measured" by maintenance staff.

Digital sensor interfaces lack standardisation. Even if protocols like MODBUS RTU are standardised sensors have proprietary interfaces with different addresses, commands and status information. Connecting such sensors to the tunnel control system a system integrator has to generate an own piece of code for every different sensor, a so-called plugin. Keeping the plugin simple it picks up only the data required to control systems of the tunnel like the ventilation or the lights. Data specific to the sensor needed for condition monitoring is "lost". Further, sensors connected through a device specific plug-ins cannot be replaced by other sensors (with the same functionality) without touching the software of the tunnel control system.

Besides, the topology of the cabling of traditional field buses like RS-485 is incompatible with tunnel installations. In tunnels, cables from sensors usually lead to an operating room or niche where a PLC picks up their signals. Such a star topology is not supported by field buses, which instead require a daisy-chain topology, i.e. a cable that leads to one sensor, from there to the next and so on.

Transferring technologies of "Industry 4.0" to the tunnel solves most of the mentioned issues. One thing is sure: the "Tunnel 4.0's networked tunnel sensors fit for the future" connect seamlessly to tunnel operators' (existing) corporate IP networks. But which applications unlock the most value both for sensor manufacturers and tunnel operators?

## 2. INDUSTRY 4.0 APPLICATIONS IN TUNNELS

Implementing Industry 4.0 is a process that could take years, and more applications will develop as technologies mature further. It is imperative that manufacturers in all countries start now with a set of concrete applications. This will build the organisational and technical muscle to tackle more ambitious projects in the future, such as the complete integration of data throughout the product life cycle. (McKinsey, 2016)

**Figure 1** shows the compass of Industry 4.0 levers and value drives created by McKinsey that helps to identify the technologies that deliver the biggest return on investment for a company, given its unique circumstances.

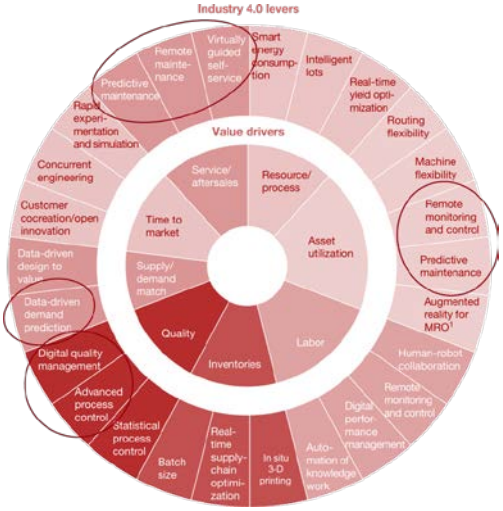


**Figure 1:** Digital compass to find tools (McKinsey Digital, 2016)

Tunnel operators would like to optimise their asset utilisation while manufacturers want to gain business in digital services and aftersales. Remote monitoring and control is the key to predictive maintenance, remote maintenance, but also to data-driven demand prediction when it comes to on-time supply with expendable parts.

Digital quality management and advanced process control include topics like the documentation of commissioning and maintenance, reliability statistics or automated test scenarios.

Anyway, before tunnel operators can unleash the potentials of the new technologies they have to transform the setup of their Industry 3.0 infrastructure through which they operate a tunnel today.

## 3. TRANSFORMING THE AUTOMATION PYRAMID

Since the beginnings of industry, the automation of manufacturing and production processes has been constantly evolving. This evolution was made possible by the integration of classic technologies like mechanics and electricity with other more modern ones such as electronics, computer science, communications, etc. playing a greater part day by day. (SMC International Training, 2020)

The concept of the "Automation Pyramid" allows classifying technologies and systems in automation and represents the different levels of an industrial production system.

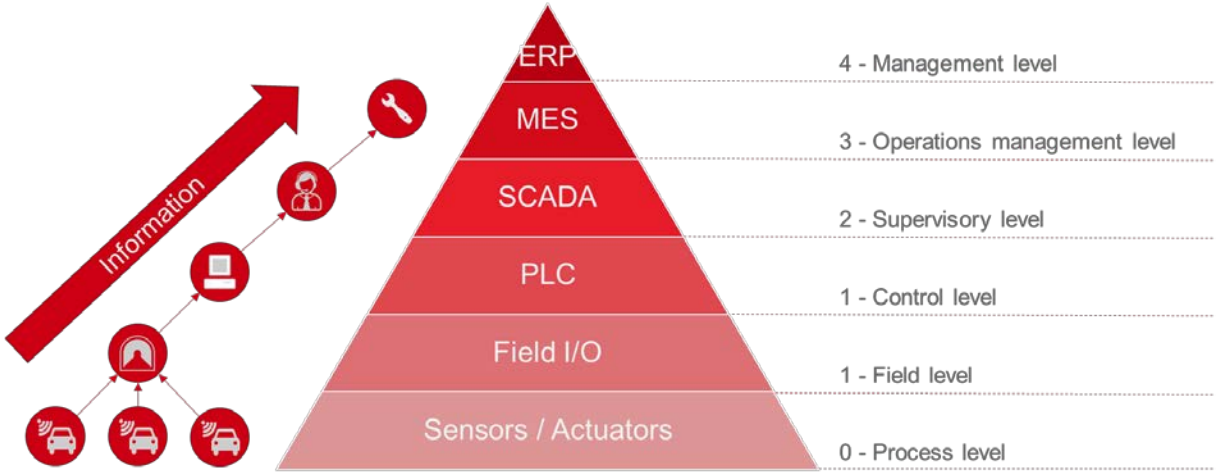


**Figure 2:** Automation Pyramid

The process level or level 0 forms the bottom of the pyramid. It represents the sensors and actuators in the tunnel, which serve as interfaces to the tunnel environment and the tunnel users, i.e. the "production process".

Field I/O devices pick up the signals from the sensors or control the actuators. These devices are usually components of the PLC used in the tunnel (but do not contain any control logic). The PLC handles the process logic and such serves as the tunnel control system. Field and Control level together are referred as level 1.

The Supervisory level (level 2) utilises SCADA, a control system architecture comprising computers, networked data communications and graphical user interfaces (GUI) for process supervisory management of one or several locations. Level 2 represents a tunnel control centre.

The next level (level 3) is the Operations Management level which normally employs a Manufacturing Execution System (MES). Considering that a "flawless tunnel operation" should be "manufactured" this level deals with optimising the availability of the tunnel by providing systems to control, track and document maintenance like a ticketing system where a tunnel operator files a complaint to the maintenance staff about a defect sensor.

Overall, the Automation pyramid depicts a classical hierarchical structure (of Industry 3.0) that does not allow exploiting the benefits of new technologies that drive the Industry 4.0. The Internet of Things, cyber-physical systems, and big data, promote the development of new solutions that do not adhere to the hierarchy outlined above. On the contrary, they demand a

more flexible, free perspective, without fixed integrations nor closed systems. In this new world without frontiers nor frameworks, systems are smart and highly interconnected. Data does not only flow in one direction, aggregated from the bottom up. (Giacomin, 2017)

While Industry 3.0 was focusing on the automation of single machines and process, Industry 4.0 focuses on the end-to-end digitisation of all physical assets and integration into digital ecosystems with value chain partners. (PWC, 2016)

End-to-end digitisation of the assets in the tunnel environment requires that all sensors connect to a tunnel operator's corporate IP network, i.e. are IoT-enabled, either instead or additionally to their connection to a PLC. It also means that other devices within the same network have access to these sensors.

**Figure 3** shows such a scenario. All systems and levels shown in **Figure 2** and described above are still there but the strict hierarchy is gone, data can flow from every node in either direction.

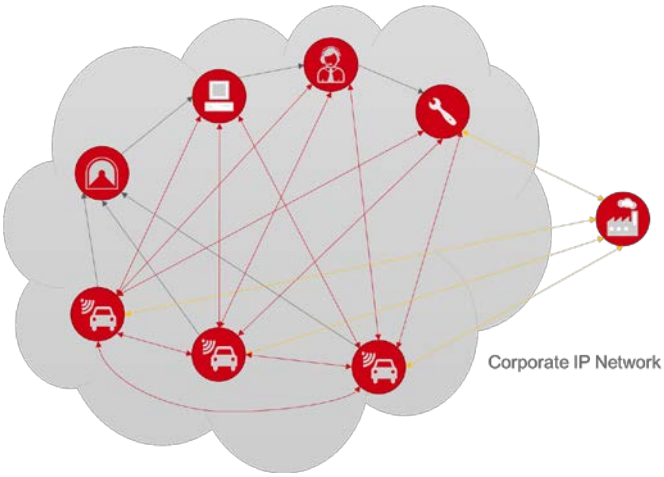


**Figure 3:** End-to-end digitisation

It is obvious that end-to-end digitisation will take years, so many new sensors will still have traditional analogue and digital interfaces to use them both in classic and new scenarios.

**Figure 3** also shows the possibility of integrating a value chain partner like a sensor manufacturer into the digital ecosystem of the tunnel operator. Such an integration of a third party often raises concerns about cybersecurity and data ownership. On the other hand letting a sensor manufacturer access "his" sensors for troubleshooting, performance analysis, condition monitoring, updating firmware, etc. improves reliability and availability. Instead of "locking out" the sensor manufacturer, adequate security and organisational measures should be developed and implemented.

## 4. NETWORK COMMUNICATION

Every sensor connected to an IP network can be accessed by other devices within this network like other sensors, a PLC, a SCADA system or a PC. This remote access via TCP/IP is the basis for all necessary and useful applications. Of course, a human needs a different interface than a SCADA system.

For a human, a modern sensor should offer a web interface, such that no longer special software from the sensor manufacturer is required to configure or troubleshoot a sensor. Functionality of such a web interface should include:

- Visualisation of measured values, warnings and errors, condition
- Sensor configuration (sensor settings, outputs, alerts, warnings)
- Network configuration (IP address, ports, security, protocols)

- Informational attributes (name, location, responsible organisational unit, etc.)
- User administration

Today sensors come with a set of supported application protocols to exchange data with other network devices. There are TCP/IP variants of established field buses like MODBUS/TCP and Profinet or other new Ethernet based field bus protocols like EtherCAT or EtherNet/IP. Again, all of these protocols are proprietary and communication between devices of different manufacturers requires interfaces and gateways. Even if communicating devices use the same protocol, the format of the data is again proprietary. In data processing this would be no leap forward compared to a traditional field bus. A system integrator would still need to implement sensor-specific plug-ins, an issue has been addressed by the OPC Unified Architecture (OPC UA).

OPC UA is a service-oriented architecture for the secure and reliable exchange of data in the industrial automation space and in other industries. It is platform independent and ensures the seamless flow of information among devices from multiple vendors. (OPC Foundation, 2020)

OPC UA has been designed for scalability and supports a wide range of application domains, ranging from field level (e.g. devices for measurement or identification, PLCs), to enterprise management support. To achieve these design goals, the OPC UA standard provides a multi-layered architecture as shown in **Figure 4**. (OPC Foundation, 2020)

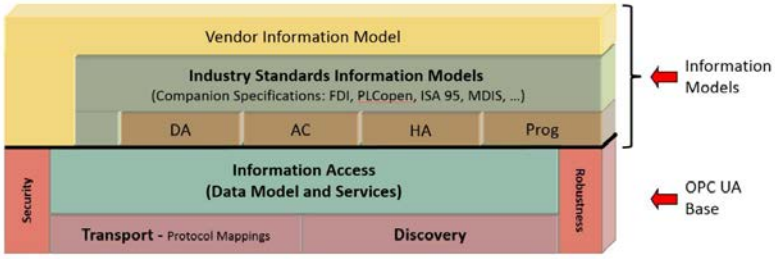


**Figure 4:** OPC UA multi-layered architecture (OPC Foundation, 2020)

The OPC UA Base provides the services Discovery, Transport, Information Access, Security and Robustness. Information models are layered on top of this infrastructure. OPC UA specifies a number of base information models (DataAccess – DA, Alarms&Conditions – AC, and more) that define commonly used objects including both real-time and historical data variables and alarms. (OPC Foundation, 2020)

Further, there shall be Industry Standards Information Models that address a dedicated industry problem, so-called Companion Specifications. The synergy of the OPC UA infrastructure to exchange such industry information models enables interoperability at the semantic level. (OPC Foundation, 2020)

Defining industry information models for transport infrastructure applications would finally make sensor-specific plug-ins obsolete. Austrian road operator ASFINAG has already defined such in its specification PlaPB 800.566.2600 Tunnel – Steuerung but there is no international information model based on OPC UA yet.

However, the problem of lacking interoperability and interchangeability between computers and electronic traffic control equipment from different manufacturers is not new. There have earlier been efforts to standardise communications and data models resulting in protocols like TLSoIP (Germany) or the NTCIP (National Transportation Communications for Intelligent Transportation System Protocol, USA). None of these protocols fits into the OPC UA.

If tunnel and road operators want to push standardisation further, they should jointly with manufacturers develop a Companion Specification for OPC UA.

## 5. REMOTE MAINTENANCE

Remote maintenance allows monitoring, updating, and resolving issues on accessible network devices. Not least because of the savings in travel costs and the better use of resources (staff and technology), remote maintenance reduces cost of operation.

Looking at IoT-enabled sensors there are two aspects of remote maintenance, the first dealing with the actual sensor functionality, the second with the network connection.

It is evident that in case of technical problems remote maintenance enables a remote expert to support configuring or troubleshooting a sensor.

The second aspect dealing with the network functionality of the sensor needs a closer look. Tunnel sensors have a longer lifetime than other IT components in their environment such that manufacturers have to implement functionality to update a sensor's software. If the sensor connects to a corporate network software updates (field updates) may not be as critical as in public networks like the Internet where security issues must be fixed.

Further, software updates can implement new functionality or new communication protocols (field upgrades). This is both an upselling potential for the manufacturer but also a chance for tunnel operators to integrate existing sensors into their changing environments instead of replacing them.

A sensor can be accessed for remote maintenance through its web interface. An unprotected web interface however bears the risk of unauthorised access. Appropriate security measures have to be assessed and implemented. A possible solution is an asset management system that allows a central administration of access rights for all sensors in the network.

## 6. CONDITION MONITORING AND PREDICTIVE MAINTENANCE

Condition monitoring is the process of monitoring parameters of condition in sensors (light source, soiling of optics, temperature, fan rpm, airflow), in order to identify a significant change which is indicative of a developing fault. (Wikipedia: Condition Monitoring, 2020)

Predictive maintenance techniques consider the condition of in-service equipment in order to estimate when maintenance should be performed. This approach promises cost savings over routine or time-based preventive maintenance, because tasks are performed only when indicated. (Wikipedia: Predictive Maintenance, 2020)

Today's tunnel control systems only pick up warnings or errors from installed sensors, data for a condition monitoring is usually "left in the sensor". The purpose of a tunnel control system however is not to analyse indicators within sensors that in many cases only the manufacturer himself can judge. Hence, condition monitoring needs to be handled by a dedicated system. Ideally, all information aggregates into one central system that controls all sensors in a tunnel operator's network.

## 7. DIGITAL QUALITY MANAGEMENT AND DOCUMENTATION

An important task in quality management is the documentation from manufacturing until the sensor is retired. Having access to the sensor offers new opportunities in documentation. The sensor itself could store data and generate reports with information from manufacturing and delivery (serial number, manufacturing date, warranty, configuration, user manual, wiring diagrams) over commissioning to maintenance performed on the sensor.

Reliability statistics derived from condition monitoring helps the manufacturer to improve the future sensor design. The tunnel operator can identify assets with a higher number of failures and take measures.

## 8. ASSET MANAGEMENT SYSTEM

Unleashing the full potential of the aforementioned functions requires an asset management system provided by the sensor manufacturer. This system can be installed on a server within the corporate network of the tunnel operator and/or on a server of the manufacturer.

An asset management system should provide through a web interface:

- Navigation through all assets
- Aggregated and detailed views of all sensors and actuators
- Condition, warnings and errors
- Sensor and network configuration
- Central user rights administration
- Update and upgrade roll-out
- Access to documentation

## 9. CYBERSECURITY

Whenever sensors or actuators in a transport infrastructure connect to a network cybersecurity is one of the major challenges. The term describes the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. While the IoT creates opportunities for more direct integration of the physical world into computer-based systems, it also provides opportunities for misuse. In particular, as the IoT spreads widely, cyber attacks are likely to become an increasingly physical (rather than simply virtual) threat. (Wikipedia: Computer security, 2020)

Discussing cybersecurity is not a topic of this essay. However, none of the discussed technologies adds major new challenges to the cybersecurity in tunnel operators' corporate networks.

## 10. SUMMARY AND CONCLUSIONS

**Figure 5** proposes an architecture for the implementation of the "Tunnel 4.0" that takes into account the components, protocols and cybersecurity issues.

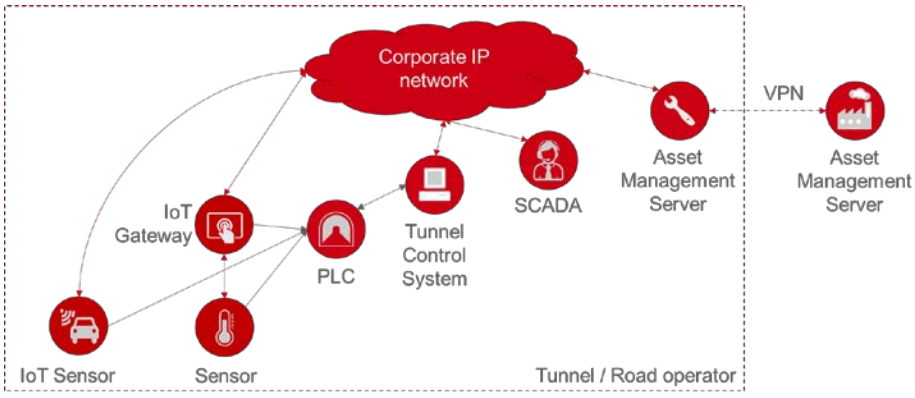


**Figure 5:** Architecture of an IoT-enabled sensor system

Considering that the architecture deals with critical transport infrastructure most of the communication should happen in a "closed" corporate network. IoT sensors, tunnel control systems, SCADA and the central Asset Management Server of the tunnel operator communicate directly via the corporate IP network. Also conventional sensors could be linked to the network via an IoT gateway.

The architecture also allows picking up sensor signals through the conventional path via the PLC to the tunnel control system. Operators and/or system integrators may still want to implement this proven route at least for a period of transition.

In case of necessary software changes, the sensor manufacturer may need to be involved. If concerns regarding cybersecurity prevail and a tunnel operator does not want a permanent data link with the sensor manufacturer a VPN connection could only be established in case of an update or upgrade.

This essay has described how Industry 4.0 and its concepts will sooner or later create a “Tunnel 4.0”. It would be naïve to think that this revolution will bypass transport infrastructure.

Tunnel operators need to rethink their current system architectures. Sensor manufactures will have to deliver the technologies for an efficient implementation of the “Tunnel 4.0”.

Operators, manufacturers and system integrators now need to work together to develop a Companion Specification for OPC UA that allows an efficient integration of sensors into a new or existing transport infrastructure environment.

## 11. REFERENCES

Giacomin, R. (2017). *The revolution of industrial systems and the collapse of a pyramid*. Retrieved from https://viridis.energy/en/blog/revolution-industrial-systems-and-collapse-pyramid

McKinsey. (2016, 04). *Getting the most out of Industry 4.0*. Retrieved from https://www.mckinsey.com/business-functions/operations/our-insights/industry-40-looking-beyond-the-initial-hype

McKinsey Digital. (2016). *Industry 4.0 after the initial hype.* Retrieved from https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/getting%20the%20most%20out%20of%20industry%204%200/mckinsey_industry_40_2016.ashx

OPC Foundation. (2020, 03 03). *UA Companion Specifications*. Retrieved from https://opcfoundation.org/about/opc-technologies/opc-ua/ua-companion-specifications/

OPC Foundation. (2020, 03 03). *What is OPC?* Retrieved from https://opcfoundation.org/about/what-is-opc/

PWC. (2016). *Industry 4.0: Building the digital enterprise.* Retrieved from https://www.pwc.com/gx/en/industries/industry-4.0.html

SMC International Training. (2020, 03 03). *Automation Pyramid*. Retrieved from https://www.smctraining.com/webpage/indexpage/312

Wikipedia: Computer security. (2020, 03 03). Retrieved from https://en.wikipedia.org/wiki/Computer_security

Wikipedia: Condition Monitoring. (2020, 03 03). Retrieved from https://en.wikipedia.org/wiki/Condition_monitoring

Wikipedia: Predictive Maintenance. (2020, 03 03). Retrieved from https://en.wikipedia.org/wiki/Predictive_maintenance