2025 IMEKO TC-6 International Conference on
Metrology and Digital Transformation - **M4DConf 2025**
Benevento, Italy, September 3-5, 2025

Infrastructure requirements for metrological distributed sensor networks

Martin Koval[1], Gertjan Kok[2], Maximilian Gruber[3], Shahin Tabandeh[4], Martin Staněk[1]

[1] Czech Metrology Institute, Okružní 31, 63800 Brno, Czech Republic, martin.koval@cmi.gov.cz, martin.stanek@cmi.gov.cz
[2] Van Swinden Laboratorium (VSL), Thijsseweg 11, 2629 JA, the Netherlands, gkok@vsl.nl
[3] Physikalisch-Technische Bundesanstalt (PTB), Abbestraße 2-12, D-10587, Berlin, Germany, maximilian.gruber@ptb.de
[4] VTT MIKES, Tekniikantie 1, 02150 Espoo, Finland, shahin.tabandeh@vtt.fi

***Abstract* – Distributed sensor networks (DSNs) are increasingly being deployed in various systems, indicating a more active implementation of digitalisation in the field of metrology. DSNs bring a wide range of benefits in the management of processes, where we are now looking not only at real-time monitoring, but also at advanced process optimization based on efficiently acquired data, support in the creation of digital twins, the prediction of future states such as calibration or service maintenance, the usage of artificial intelligence, and much more. For DSNs to operate efficiently and reliably, it is essential to properly establish the network infrastructure and identify the associated requirements at the design phase, including metrological aspects. This paper proposes a structured set of infrastructure requirements and metrological design guidelines that enable long-term reliability, traceability, and data quality in DSNs, and discusses practical approaches to sensor architecture, network topology, calibration strategies, and QA/QC (Quality Assurance/ Quality Control) planning tailored to metrological applications.**

I. INTRODUCTION

Distributed Sensor Network (DSN) is a modern concept where individual sensors are distributed in space and interconnected to efficiently collect, transmit, and process data (measurement data and metadata). This concept is becoming increasingly important in the context of digitalization, particularly in the field of metrology, where it enables more efficient real-time monitoring and control of processes. The deployment of DSNs opens up new possibilities not only for tracking measurement data, but also for data processing, process optimization, digital twins, predictive analytics, and integration of artificial intelligence [1, 2]. DSNs can enable the creation of dynamic models that can respond to current conditions, predict the development of monitored parameters, and positively influence system control. The concept of digital twins is one example where DSNs play a key role. Data collected from distributed sensors allow for constantly updating digital models, improving control and offering advanced opportunities for optimization [1].

DSNs can be found in various applications from Industry 4.0, where they support automation and intelligent control of production lines, through the energy sector (monitoring of distribution systems, smart grids), healthcare (medical devices complex system or wearable devices), to smart cities and environmental monitoring (e.g., air, water, and soil quality monitoring) [3]. In each of these areas, DSNs contribute to improved efficiency, reliability, and sustainability. However, the effective deployment and operation of a DSN is not guaranteed without a properly designed network architecture and clearly defined infrastructure requirements, otherwise, key aspects such as DSN lifecycle and adaptability can be significantly compromised. Factors such as network topology, communication cybersecurity, and scalability as well as metrological considerations with respect to sensor uncertainty, initial calibration and re-calibration strategy greatly influence not only real-time performance, but also the long-term benefits of DSN [3, 4]. The aim of this paper is to analyse key aspects of DSN infrastructure design, highlight the influence of the DSN topology on its performance, and define fundamental requirements necessary for the long-term sustainability and effective operation of a metrological DSN.

II. TERMINOLOGY AND DEFINITIONS

To properly understand the specifics of DSNs, it is necessary to define basic important concepts and the relationships between them. This section only includes terms that are necessary for a better understanding of the context of the article.

DSN architecture: The architecture of a DSN is the overall design, how infrastructure components interact. This is done by designing the logical as well as the physical relationships between these components, specifying access methods and choosing communication protocols.

DSN topology: The topology of a DSN is the graph that represents how measuring devices and computation nodes are linked, either physically or logically.

DSN infrastructure: The infrastructure of a DSN covers the components that are required to develop, operate, monitor, control and support the DSN. These are mainly physical components (i.e., measuring devices, compute nodes, power supplies, networking hardware), but also the required software and network applications.

Node: A node in DSN is a basic functional unit capable of performing measurements, aggregation data, processing data, and communicating with other nodes or a central system.[13]

Sensor: For the purposes of this article, a sensor is considered a physical device that detects, measures, and responds to a specific physical quantity and converts it into a usable signal, typically electrical or digital. In the context of DSNs, a sensor can also be an intelligent sensing unit. This includes additional functions such as signal preprocessing, generation of metadata, bidirectional communication, or embedded firmware, among others.

III. INFLUENCE OF NETWORK TOPOLOGY ON DSN INFRASTRUCTURE

The topology of a DSN describes the way in which individual sensors or sensor networks are interconnected. Standard topologies such as star, tree, mesh, and hybrid structures are well-known in the field, but their impact on the performance and reliability of a DSN is sometimes underestimated. In simple topologies like the star, sensors are directly connected to a central gateway. In tree-based structures, sensors are connected hierarchically through intermediate nodes. Mesh topologies allow nodes to communicate with multiple neighbouring nodes, creating redundant paths and enabling decentralized communication. These configurations help to determine the robustness of a DSN, to visualize data flows, how faults are detected, and many other important information [1,2,6]. The choice of topology directly affects the number of required sensors, the presence of critical points in the network (e.g., huge density of sensors, single points of failure), and the network's ability to detect anomalies either in the monitored process or in the sensor (or sensor nodes) themselves. An effective design of topology enables early identification of issues, whether they are from the object of measuring process, sensor degradation/failure, or communication faults. But an inappropriately chosen topology can lead to blind spots, higher failure rates, or excessive load on specific network segments. Moreover, network topology strongly influences scalability, energy efficiency (especially in wireless systems), latency in data transmission, and overall infrastructure maintainability [1,5]. For these reasons, network topology must be taken as an important design element for the design of a DSN. It determines how well the DSN can perform throughout its lifecycle and how resilient it is to both internal and external influences [2,3,6]. Examples of topologies and their impact on the infrastructure of DSN are the following:

Star topology: In this architecture, all sensors are directly connected to a single central point, typically a gateway or processing unit. This setup allows for simple deployment, efficient communication control, and low data transmission latency. The disadvantage is that the failure of the central unit results in the disconnection/failure of the whole DSN. Star topologies are suitable for smaller networks with a limited number of sensors and a simple physical layout.

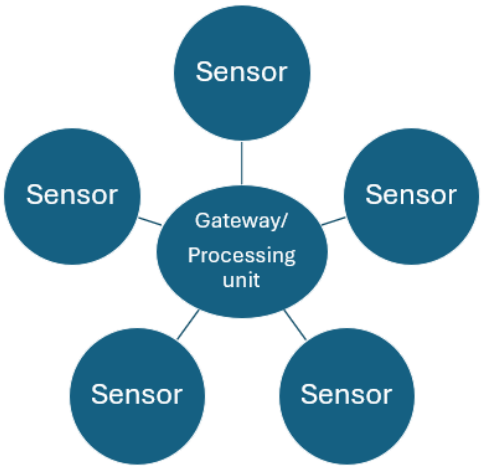

Fig. 1. Example of star topology.

Tree topology: The tree structure has hierarchical levels in which sensors communicate through intermediary nodes (in this case these nodes work as aggregators of data). It is commonly used in applications where the network is logically divided into specific segments. The tree topology facilitates network scalability, but it lacks redundancy and may suffer from increased latency in case of more or deeper branches, which can result in delays in receiving the measuring data or cause faults.

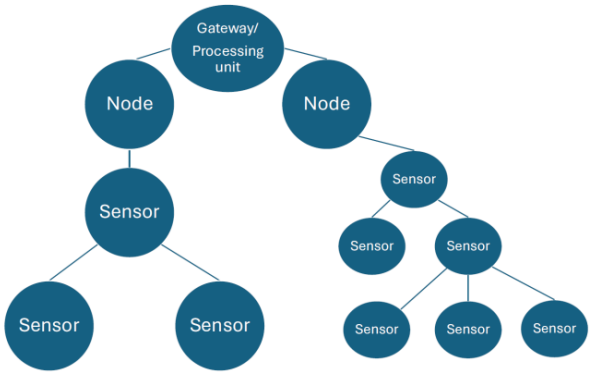

Fig. 2. Example of tree topology.

Mesh topology: In a mesh topology, each sensor can communicate with multiple neighbouring sensors or nodes, forming redundant data transmission paths. This increases the network's fault tolerance and allows for dynamic rerouting in case of sensor failures or environmental changes. However, mesh networks typically require more energy and more complex routing protocols. They are well-suited for applications that demand high reliability or autonomous operation [3].

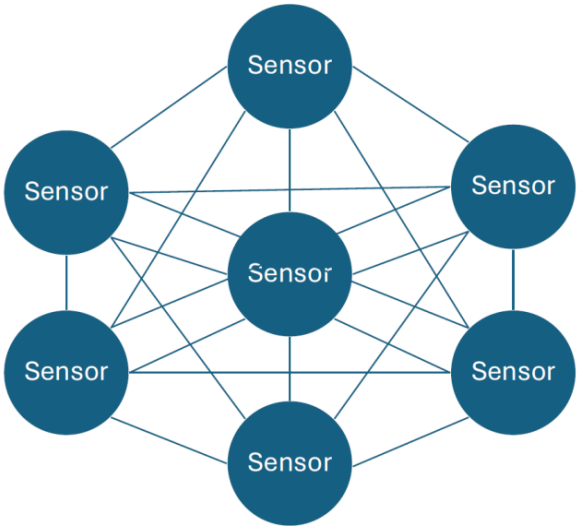

Fig. 3. Example of mesh topology.

Hybrid topologies: In practice, hybrid approaches are most often used, combining the benefits of each topology. For example, tree-mesh structures can balance reliability with energy efficiency while maintaining moderate deployment complexity. Such configurations offer flexibility and adaptability to the specific requirements of the monitored processes where DSN is applied.

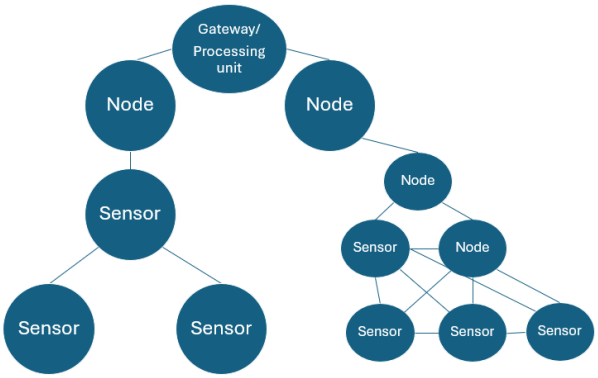

Fig. 4. Example of hybrid topology.

IV. METROLOGICAL ASPECTS OF DSN DESIGN

When designing a DSN with a metrological purpose, it is essential to consider all metrological aspects. The first step is to specify the exact purpose of the network or, in metrological terms, to define the overall DSN measurand, i.e., the quantity of interest that serves as the final output of the DSN. For example, it is important to determine whether the DSN measurand represents a global space- and time-averaged value (e.g., temperature or pollution) or if precise space- and time-resolved data are also of key interest. Additionally, the required measurement uncertainty, along with the spatial and temporal resolution for the measurand, will influence the DSN design and sensor selection. In many cases, the individual sensors in the DSN will measure the same metrological quantity as the overall DSN measurand. However, there are instances where this is not the case. For example, the measurand of the DSN might be the average refractive index over a certain distance, while the individual sensors could be measuring temperature, relative humidity, and CO_2 concentration [7]. When the overall DSN measurand, the type of individual sensors, and the mathematical relationship between sensor values and the DSN measurand are known, it is possible to specify the required uncertainty of the individual sensors. However, it should be noted that correlations in the measurement errors of the sensors need to be carefully considered [8]. Incorrectly assuming that all sensor errors are independent can lead to calculating overly optimistic uncertainties for the DSN measurand. In any case, the combination of multiple data streams requires a common index, usually achieved through synchronized clocks. It is important to evaluate the effects of the implemented time synchronization protocol on the data fusion task at hand, as timestamp uncertainties (e.g., NTP [11]) can be a major part in the uncertainty budget [12].

Another relevant metrological aspect is the expected in-situ behaviour of the sensors, i.e., deployed in the field, the sensors may behave differently than under laboratory conditions. Furthermore, the expected

maximum allowed drift over time should be known. More generally, an initial calibration strategy as well as a metrological QA/QC plan should be designed, where the QA/QC strategy should include a re-calibration plan. The QA/QC-plan may require the inclusion of some high-quality reference sensors and/ or including some redundant sensors in the DSN. As QA/QC can be a major concern for the operation of a DSN over its lifetime, this aspect should be carefully considered in the planning and design phase.

The outputs of a truly metrological DSN should be metrologically traceable, which implies that the individual sensors must also be metrologically traceable and possess a known measurement uncertainty level. If the outputs of a DSN are intended for use in a regulatory context, this can be a significant concern. If the DSN is meant to provide only some qualitative information, the requirements for metrological traceability may be somewhat relaxed; however, an appropriate QA/QC plan is still necessary to ensure that the end-user is not misled by the DSN output and does not base their conclusions incorrectly on, for example, drifting sensors.

A growing body of work shows that several *in situ* calibration strategies, e.g., co-calibration with the neighbouring nodes, consensus calibration, only become viable when the DSN provides sufficient metrological redundancy, i.e. multiple independent observations of the same or strongly correlated measurands within the relevant spatio-temporal window [9] These algorithms exploit the redundant information to solve simultaneously for individual sensor errors and for the measurand field itself; consequently, the expanded uncertainty of the calibrated sensors scales with the degree of redundancy that is preserved [10]. Hence, during the design phase, it is essential to specify a node density that not only meets the desired spatial resolution but also provides the level of redundancy demanded by the chosen calibration strategy and its target calibration uncertainty. The optimum density depends on both the calibration algorithm and the physics of the measurand, as slowly varying or highly correlated fields tolerate larger inter-sensor spacing than fields with sharp and highly localised spatial gradients or rapid temporal dynamics.

V. DSN INFRASTRUCTURE REQUIREMENTS

The effective operation of a DSN depends on a carefully designed infrastructure that takes into account specific hardware, software, and communication requirements. These requirements should be defined during the design phase. The fundamental requirements that need to be considered for any DNS include:

Estimate the numbers or range of used sensors: The number and placement of sensors in a DSN should be determined based on specific targeted processes and take into account measurement accuracy, coverage of the monitored area, or redundancy requirements. ISO/IEC 30141 also recommends considering the scalability of the system so that additional sensors can be added in the future without major changes to the infrastructure.

Types of data collected: Defining the types of data that the sensors will collect is crucial for selecting appropriate sensors and communication protocols. The data should include measured data but may also include derived values obtained by processing the raw data and its measurement uncertainty. In addition to the measured data itself, it is important to collect metadata such as time stamps, sensor identifiers, network topology status, calibration status and other operational parameters depending on the monitored process. This information is essential for proper data interpretation and system maintenance.

Time intervals: It is necessary to determine how often the sensors will collect and send data. These intervals should be defined based on the dynamics of the monitored process and the requirements for data timeliness.

Expected ranges of data values: For each sensor, the data type should be identified and the expected minimum and maximum values defined. This information is important for anomaly detection and sensor calibration.

Distributed computing power: The decision of where data processing will take place (in sensors, nodes, or a central gateway) influences the infrastructure design. Edge computing can reduce latency and network load, while centralized processing can be advantageous for more complex analytics.

Security and Cybersecurity Requirements: DSN security should include data protection during measurement data generation, transmission and storage, as well as device and user authentication, as well as protection against unauthorized access and audit trails in case of operator intervention and all relevant incidents. The ISO/IEC 30141 standard defines requirements for confidentiality, integrity and availability of data, as well as for the protection of personal data.

Network Topology Information: The network topology affects the reliability, latency, and energy efficiency of the DSN. It is necessary to define what type of topology will be used and ensure that the infrastructure is designed with the requirements of the specific process being monitored in mind.

Interoperability: The DSN should be able to work with different devices and services, with an emphasis on standardized interfaces and protocols.

Scalability and flexibility: The architecture should allow for easy expansion of the DSN and adaptation to changing

requirements.

VI. LIFECYCLE OF A DISTRIBUTED SENSOR NETWORK

DSNs are systems that are mostly considered for long-term deployment, requiring a systematic approach to their planning, operation and management throughout their entire life cycle.

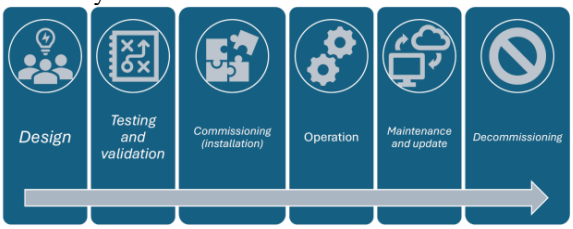

Fig. 5. Lifecycle of DSN

Design phase: This phase sets the network goals, defines the architecture, infrastructure, sensor types, topology, communication, data processing, and security requirements, and considers every known aspect. It also models the operating environment, the expected network load, and plans for scaling.

Testing and validation phase: This phase is essential for the proper functioning of the DSN. Testing includes verification of sensor functionality, compatibility between devices, communication stability and failure tolerance. Simulations of various boundary situations, such as failures, limit values, service (sensor calibration/repair), etc.

Commissioning (installation) phase: physical installation of sensors for monitoring the given process, configuration of nodes and their integration into higher-level systems (e.g., SCADA), or digital twins or cloud platforms. In this phase, communication parameters, security layers are set.

Operational phase: DSN fulfils its main task – data collection and transmission, or local processing. At the same time, continuous monitoring of data integrity, network performance, etc. must be ensured. Early detection of failures, deviations in measurements, or degraded communication quality is also critical.

Maintenance and update phase: This phase includes regular verification of the functionality of all DSN elements, updating of security elements, such as cybersecurity elements. Calibration/service of DSN components, etc. The maintenance interval is set depending on the monitored process, sensor types, and also on the development of cybersecurity (being state of the art in terms of possible attacks).

DSN decommissioning (last phase): includes dismantling components, ensuring secure data handling (archiving, anonymization or total data deletion). This phase should be planned during the design, especially for large-scale or critical applications.

VII. CONCLUSION

Distributed sensor networks are part of the digitalization of metrology. Their ability to continuously monitor processes, process data in real time, and provide data for decision-making, optimization, and prediction makes them a key tool in the field of metrology and its impact on industry, healthcare, and environmental monitoring. However, the successful deployment of DSNs is not only a technical challenge, but also requires a multidisciplinary approach to the design of their infrastructure. As we have shown, it is necessary to take into account the network topology, the number and type of sensors, the method of communication, the location of computing power, and even security requirements already at the design stage. In addition, metrological concerns like the calibration strategy, QA/QC procedures, required uncertainty of the overall DSN measurand and, based on the measurement model and expected sensor uncertainties, the required uncertainty of the sensors should be taken into account. It is equally important to consider the DSN life cycle.

Standards such as ISO/IEC 30141 provide a useful framework and recommendations that can help system designers to create safe and long-term sustainable solutions. It can be stated that DSN have the potential to fully develop and their further development will be increasingly linked to the concepts of digital twins, artificial intelligence and autonomous systems, which places even higher demands on their design and management.

FUNDING STATEMENT

The project (22DIT02 FunSNM) has received funding from the European Partnership on Metrology, co-financed from the European Union's Horizon Europe Research and Innovation Programme and by the Participating States.

REFERENCES

[1] M. Lanza et al., "Towards a Distributed Digital Twin Framework for Predictive Maintenance in Industrial Internet of Things (IIoT)," *Sensors*, vol. 24, no. 8, p. 2663, 2024. [Online]. https://www.mdpi.com/1424-8220/24/8/2663

[2] C. Zhao, Y. Wang, L. Xie, and S. Zhang, "Overview of predictive maintenance based on digital twin technology," *Heliyon*, vol. 9, no. 8, e18385, 2023. [Online].

https://www.sciencedirect.com/science/article/pii/S2405844023017413

[3] IEEE Instrumentation and Measurement Society, *IEEE Std 1451.1-1999: Standard for a Smart Transducer Interface for Sensors and Actuators*. IEEE, 1999. [Online]. https://www.nist.gov/document/information-14511588-v36pdf

[4] International Organization for Standardization (ISO), *ISO/IEC 30141:2018 - Internet of Things (IoT) – Reference architecture*. ISO, 2018. [Online]. https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf

[5] S. Tabandeh *et al.*, Sensor network metrology: Current state and future directions, Measurement: Sensors, (2025), 101798., DOI:https://doi.org/10.1016/j.measen.2024.101798

[6] M. Koval, J. Tesař, M .Havlíček, General Sensor Network application approach, Acta IMEKO, Vol.12 No.1(2023).DOI:https://doi.org/10.21014/actaimeko.v12i1.1409

[7] G. Kok, F. Gugole, A . Seymourk, R. Koops, Improved uncertainty evaluation for a long distance measurement by means of a temperature sensor network, Acta IMEKO, Vol.12 No.1(2023).DOI: https://doi.org/10.21014/actaimeko.v12i1.1411

[8] G. Kok, M.V. Dijk, P. Harris, A. Vedurmudi, Modelling and determining correlations in sensor networks, Measurement: Sensors, 2025, 101793, ISSN 2665-9174, https://doi.org/10.1016/j.measen.2024.101793.

[9] Vedurmudi, A. P., et al. "Automation in sensor network metrology: An overview of methods and their implementations." Measurement: Sensors (2025): 101799.

[10] Harris, P., et al. "Measurement Uncertainty Evaluation for Sensor Network Metrology." Metrology 5.1 (2025): 3.

[11] D. L. Mills, J. Martin, J. Burbank, and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification, " RFC 5905, IETF, Jun. 2010.https://datatracker.ietf.org/doc/html/rfc5905-

[12] Dorst, T., Robin, Y., Eichstädt, S., Schütze, A., and Schneider, T.: Influence of synchronization within a sensor network on machine learning results, J. Sens. Sens. Syst., 10, 233–245, https://doi.org/10.5194/jsss-10-233-2021, 2021.

[13] S. Mahlknecht, J. Glaser, T. Herndl, Pawis: Towards a Power Aware System Architecture for a SoC/SiP Wireless Sensor and Actor Node Implementation, Editor(s): Miguel León Chávez, Fieldbus Systems and Their Applications 2005, Elsevier, 2006, Pages 129-134, ISBN 9780080453644, https://doi.org/10.1016/B978-008045364-4/50058-7.