ACTA IMEKO
ISSN: 2221-870X
March 2023, Volume 12, Number 1, 1 - 5

General Sensors Network application approach

Martin Koval[1], Marek Havlíček[1], Jiří Tesař[1]

[1] *Czech Metrology Institute, Okružní 31, 63800 Brno, Czech Republic*

ABSTRACT
The paper describes the general approach for Sensor Networks and deals with principled components of Sensor Networks, architecture as well and opportunities for the implementation of current and new technologies. The paper also illustrates an example of the application of the EN 12830:2018 standard.

Section: RESEARCH PAPER

Keywords: Sensor Network; uncertainty measurement; artificial intelligence

Citation: Martin Koval, Marek Havlíček, Jiří Tesař, General Sensors Network application approach, Acta IMEKO, vol. 12, no. 1, article 13, March 2023, identifier: IMEKO-ACTA-12 (2023)-01-13

Section Editor: Daniel Hutzschenreuter, PTB, Germany

Received November 18, 2022; **In final form** March 2, 2023; **Published** March 2023

Corresponding author: Martin Koval, e-mail: mkoval@cmi.cz

1. WHAT IS THE SENSOR NETWORK?

We can imagine a Sensor Network (SN) as a group of sensors that are interconnected in different ways and can create a system that can be understood as a backbone of the processes which need to be monitored and/or optimized. In the system where many different sensors provide a complex overview of the ongoing processes, a model representing such an ensemble can be created. We can refer to this model as to a Digital Twin [1] of the system. The Digital Twin enables a real-time system monitoring, and processes history analysis and effective prediction of future events which can be forecasted with the use of advanced algorithms and AI. The result of such an interplay between the sensor network and the effective feedback control is the minimization of negative events within the system.

2. SENSOR NETWORK STRUCTURE

The basis of the Sensor Network comprises of the Input, Signal Processing and Output. These three areas can be further extended according to their intended use in particular processes. The basic type of the SN consists of sensors of the same type with fixed network topology. These sensors usually send data to the Data Processing Unit in fixed time intervals. The output may consist of the processed measured data with metadata which store additional information about the process history. An example of such process could be a system for temperature monitoring of sensitive goods according to BS EN 12830:2018.

Many more factors have to be taken into account in complex systems, e.g., dynamic topology of the network, Big Data, different sensor types, location of data processing, complex mathematical algorithms, prediction, security, etc. These factors will be discussed in more detail in the following sections.

2.1. Sensor Network Inputs

The Sensor Network may consist of many devices/sensors which can widely differ in numbers, complexity, signal types and data formats. Units of simple sensors as well as thousands of sophisticated devices can both form a structure which can be considered as the Sensor Network. Considering the amount of data collected and processed in such network, we may face challenges with their processing as the amount of data increases.

In such case we talk about Big Data. The Big Data can be well described as the 5 V model: Value, Volume, Veracity, Variety and Velocity. Each "V" has its specific influence on the SN architecture [2].

The Value represents the usefulness of the data. In the SN data hierarchy, the data priority is set from the most to the least important. There is an evident difference in the value of the real measured data, which are used for calculations, and the metadata of measurement data. The Value provides very useful information which can help to interpret data more accurately. One important information category comes from, e.g., alarms. The alarms also have their own hierarchy which defines their roles in informing about the limits of sensors and correct functioning.

The Volume of the data generated in the SN depends on the recording frequency and the number of variables which are recorded. If just the measured data with the corresponding metadata are stored, the amount of such data can reach typically

TB or PB levels. In the case that further data such as text and graphics are transferred, the volume of the data can exceed EB levels and can go even beyond that.

The Veracity represents the quality of information, their uncertainty or accuracy. The information can be inherently inconsistent, non-complete, ambiguous or its reliability can be reduced. These facts form a set of requirements which have to be applied so that it can be decided which data can be used for further analysis.

The Variety in the SN describes different forms of information. The data coming from various types of sensors and appliances can be transferred in either structured or unstructured form. In the first case, the subsequent separation and analysis is relatively easy. The situation is diametrically different for unstructured data. In such case, the data mining, sorting and analysis is more complex which may result in errors in extracted data sets.

The Velocity in the SN is the key parameter which describes the speed of the data transfer and processing. Combinations of various sensors and data structures influence the final data transfer and processing velocity which correlate with the computational power needed. In some applications, a real-time process monitoring is necessary such as in the medical applications or nuclear power plants, where any delay may have fatal consequences.

One of the important aspects which play a crucial role in Inputs is the configuration of the Sensor Network topology [3]. Different time of data delivery from distributed sensors has to be also considered. Another important factor for Inputs, which play an important role, are the dynamic changes of participating sensors. The sensors may be disabled, replaced, maintained, damaged or exposed to disturbances which can possibly have a significant effect on the whole Sensor Network.

2.2. Data Processing

Data Processing can be considered as the core of the Sensor Network. This task can be divided into separate fields which need an individual approach. The Data Processing can include the real measured data as well as the predicted data with their corresponding uncertainty. The data prediction has already become an integral part of the state-of-the-art Sensor Networks.

Data Prediction

The effectivity and reliability of the data prediction are crucial for the modelling of specific missing or corrupted data. Reliable data prediction on different timescales (minutes, hours, days, etc.) and information about their uncertainties are necessary. Another aspect that plays an important role is missing data due to various reasons such as service, calibration, or the failure of sensors. Historical data of Sensor Networks can also be used for the prediction of the network topology in near future. A careful data analysis may help to predict the situations which will occur during the expected events and prepare adequate measures to cope with them, such as maintenance, overloads etc. These data can be modelled with the use of various algorithms based on the Artificial Intelligence (AI). Nowadays, the progress in the AI development is accelerating. It mainly focuses on three areas which can be characterized as learning, reasoning and self-corrections. All these aspects can be directly applied in the SNs. The machine learning focusses on the data mining and creating rules for their conversion into useful information. The machine reasoning aims at searching for the most convenient algorithm from the family of available solutions and its implementation in the particular process. Automated self-correction mechanisms are employed in many processes in order to reach the best results in particular processes. The AI can be divided into different categories based on its capabilities: Artificial Narrow Intelligence (ANI), Artificial General Intelligence (AGI) an Artificial Super Intelligence (ASI). The ANI is frequently used in different applications, the AGI and the ASI are still subjects of research. Another categorization of the AI into four classes is based on its functionality (see Table 1) [4], [5].

Table 1. AI basic categories overview [4], [5].

Type of AI	Use	Example
Reactive AI (type ANI)	effective for simple classification and pattern recognition tasks; incapable of analysing scenarios that include imperfect information or require historical understanding;	Sorting machines
Limited memory (type ANI)	can handle complex classification tasks and use historical data to make predictions; capable of completing complex tasks (e.g., autonomous driving); needs big amounts of training data to learn tasks; vulnerable to outliers or adversarial examples;	Self-driving cars
Theory of mind (type AGI)	should be able to provide results based on an individual's motives and needs; training process would have a lower number of examples than type ANI;	Under research
Self-aware AI (type ASI)	should be aware of the mental state of others entities and itself; it is expected to outperform human intelligence;	Under research

Environment

Another important factor for the Data Processing represents the environment where the data are physically processed. Current technology enables the use of a variety of different virtual environments such as Cloud Computing, remote servers or special-purpose built-in computers. The real location of the data processing influences also the quality of the Sensor Networks.

In the case of virtual environments, the problem with insufficient power is not necessarily the limiting factor. One of the most important parts of the SN is the cyber security of the environment, communication channels and sensors themselves. From the security point of view, the SN begins at sensors. If data reliability shall be guaranteed then all sensors have to be secured from the HW and SW point of view [6]. The HW security is essential in order to prevent any unauthorized change of parts containing the SW, which could possibly compromise the measured data. The HW security can be realized in a non-destructive or destructive way. Any unauthorized access to the sensor/device results in its destruction in the case of a destructive solution [7]. Any fraudulent data manipulation using such damaged sensor is either physically impossible or technically challenging. The non-destructive solutions typically involve different ways of sealing, which indicate an unauthorized access into HW parts. It is worth noting that the availability of technologies which are capable to substitute HW parts is higher than in the past.

Table 2. Example of using Uncertainty evaluation methods [2], [9]-[12].

Uncertainty method	Use
LPU	general uncertainty evaluation for complete datasets;
Monte Carlo	uncertainty evaluation for asymmetric and inadequate datasets;
Shannon's Entropy	determining the amount of missing information on average in a random source;
Fuzziness/Fuzzy Theory	processing of vague or ambiguous datasets for complex models;
Bayesian Statistical Models	they are particularly useful when there exists information about the true value of the measurand prior to obtaining the results of a new measurement

In the case that sensors contain SW it is necessary to deal with the security from the SW point of view which shall include a basic minimum of the integrity check, authenticity and alarms. In the case of more advanced sensors with bi-directional communication where the remote control of sensors is possible, calibration parameters are available, etc., it is essential to secure access rights. If the system parameters can be changed, it is a good practice to use an event logger in order to guarantee the traceability of changes. One of the important factors which help with the data analysis is the presence of the metadata related to the particular data file. This metadata contains additional information which may be essential for a subsequent analysis. One of the most effective ways for the metadata protection represents a blockchain list of records [8]. For the network itself, communication is an essential prerequisite. Hundreds of different communication solutions including protocols and interfaces are now available on the market. Criteria which shall be considered during the SN communication design include energy demand, network type, compatibility, security, open source, etc. The SN design shall also include a risk analysis [9].

Uncertainty Evaluation Methods

Uncertainties in the field of Sensor Networks represent a crucial aspect which should be always taken into account. Each sensor should be considered as an independent device placed in a certain environment and it should be treated as such.

The uncertainty evaluation in the field of metrology is the integral part of all processes where the measurement is realized. Depending on the processes and the field of measurement, the used models can vary substantially. In the case of SNs, the uncertainty evaluation can be challenging. Relatively simple SNs working with basic measurement models and consisting of a few types of sensors represent the case in which the standard procedures can be applied. In the case that the data are collected in regular intervals and only one process is monitored, then it is possible to use The Law of Propagation of Uncertainties (LPU) [10], Monte Carlo [11], etc. In the case of more sophisticated SNs, it is necessary to use mathematical models which are suitable for the particular situation. In the case that some data are not available at the moment or were removed from the data set models like Bayesian statistical models [12], Fuzzy theory, etc., should be used. An overview of commonly used methods for the uncertainty evaluation is shown in Table 2.

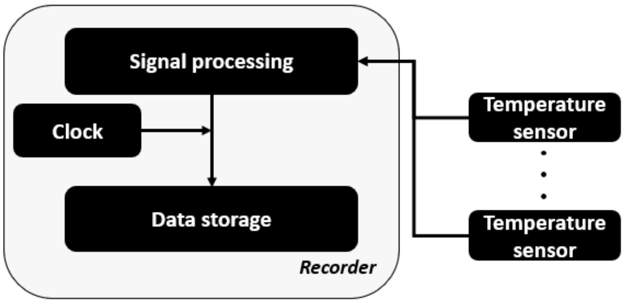

Figure 1. An example of a Simple Sensor Network according to EN 12830:2018.

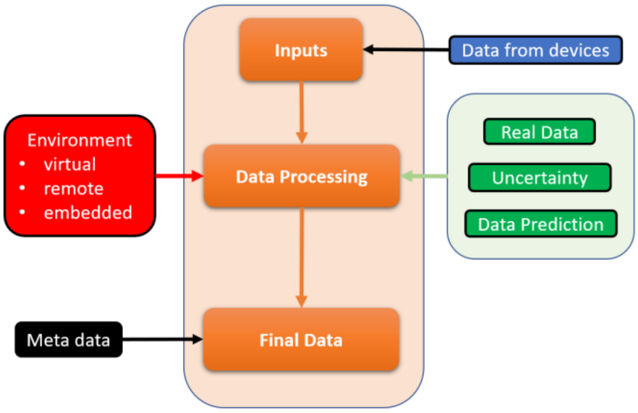

Figure 2. An example of Complex Sensor Network.

2.3. Sensor Network Output

The output of the SN depends on the particular application. Examples shown in Figure 1 to Figure 5 imply that the output can consist not only of the measured data but also contains the metadata which can enable more efficient data processing. The metadata can contain the data directly recorded by the sensors or they can be generated during the data processing (e.g., actual topology of the SN), alarm analysis, event logger messages, sensor IDs, etc. Further utilization of the data depends on the particular application. The outputs can be used in different ways such as process indicators, triggers (process breaks, notifications) or for analyses. Alternatively, the analysis can be directly in a machine-readable format which can be directly used by another SN with minimal changes in the configuration.

3. EXAMPLE OF SENSOR NETWORK

One of the practical examples of the SN realization can be done according to EN 12830:2018 Temperature recorders for the transport, storage, and distribution of temperature-sensitive

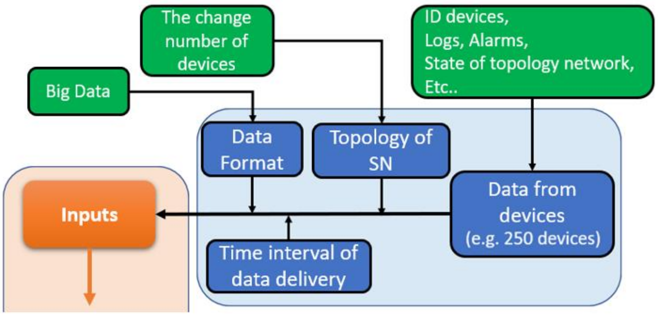

Figure 3. An Example of a Complex Sensor Network – Inputs.

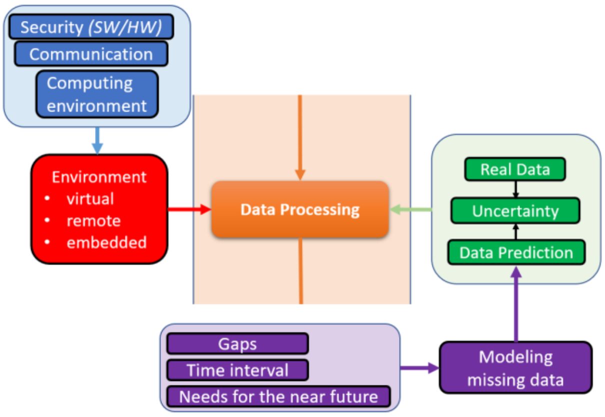

Figure 4. An example of the Complex Sensor Network – Data Processing.

goods [13]. As the name suggests the goal of this norm is temperature monitoring of sensitive goods such as food, pharmaceuticals, blood, organs, biological material, etc. The standard contains practical examples and guidelines for the correct implementations. A simple example is a monolithic temperature recorder which is physically wired to the recorder and is used for monitoring outer and inner space. The data collected is sent to the Signal conditioner and synchronized. The data is subsequently stored in the Base station where it is given the status of relevant data (see Figure 1). An advanced example is a recorder that utilizes cloud services (Figure 6).

It has similar architecture as in the previous case but in addition to it, sensors can communicate with the Base station also wirelessly. It implies that the sensors have to have SW communication modules and space for temporary data storage. Such a system can contain elements that are used for data transfer (e.g. gateway). As a consequence, security cryptographical tools have to be implemented in order to secure transferred data from malicious technical compromise or unauthorized disclosure. In the following step, the relevant data can be transferred into the cloud which usually enables more effective data processing and data management.

The requirements for specific device types are listed in EN 12830:2018. The SW for devices are divided into three classes according to their complexity:

P1- SW is embedded in a closed HW,
P2- SW runs on a general-purpose computer,
P3- SW runs on an external provider of cloud (e.g. SaaS).

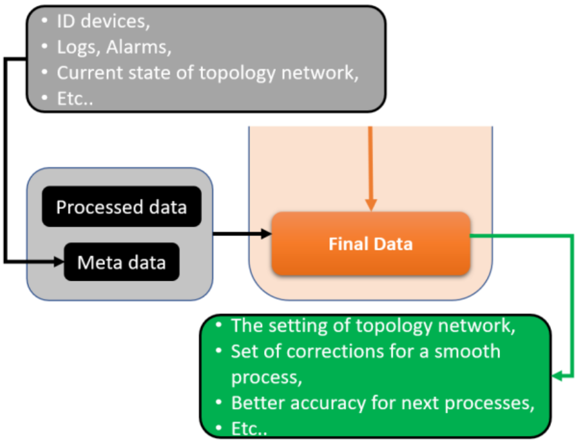
• ID devices,
• Logs, Alarms,
• Current state of topology network,
• Etc..
Processed data
Meta data
Final Data
• The setting of topology network,
• Set of corrections for a smooth process,
• Better accuracy for next processes,
• Etc..

Figure 5. An example of the Complex Sensor Network – Final Data.

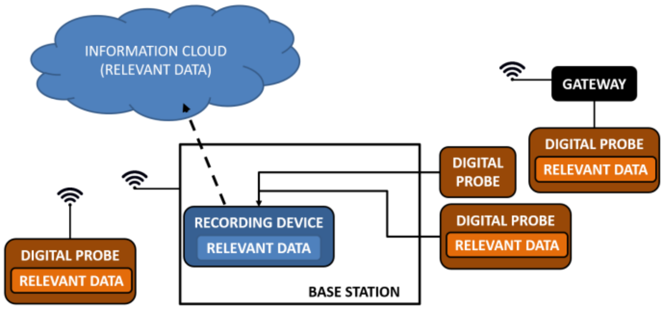

Figure 6. An example of the complex Sensor Network according to according to EN 12830:2018.

Specific requirements focused on functions, data protection, and safety measures are listed for specific types and arrangements. The requirements are based on WELEMC Guide 7.2 [14] and divided into the following blocks:

G - Basic requirements
L - Specific SW requirements for long-term storage,
T - Transmission of relevant information via communication networks,
S - SW separation,
D - Download of relevant SW.

Basic requirements have to be met for all types of P1 and P2. Requirements relevant to block T have to be met for type P3. It is strongly recommended to fulfil the requirements of ISO/IEC 27001 and take into account the requirements for control of the user and communication interface. Complete overview of requirements according to EN 12830:2018 is shown in Table 3.

A complex SN design with requirements applications may look like the one shown in Figure 7.

Table 3. List of requirements according to EN 12830:2018.

Blocks	Requirements
Basic requirements	SW Identification, Influence via user interface, Influence via communication interface, Protection against accidental, unintentional and intentional changes, Parameter protection, SW authenticity and presentation of results.
Specific SW requirements for long-term storage	Completeness of measurement data stored, Protection against accidental of unintentional changes, Integrity of data, Authenticity of measurement data stored, Confidentiality of keys, Retrieval of stored data, Automatic storing, Storage capacity and continuity.
Transmission of relevant information via communication networks	Completeness of transmitted data, Protection against accidental or unintentional changes, Integrity of data, Authenticity of transmitted data, Confidentiality of keys, Handling of corrupted data, Transmission delay, Availability of transmission services.
SW separation	Realization of SW separation, Mixed indication, Protective SW interface;
Download of relevant SW	Download mechanism, Authentication of downloaded SW, Integrity of downloaded SW, Traceability of relevant SW download

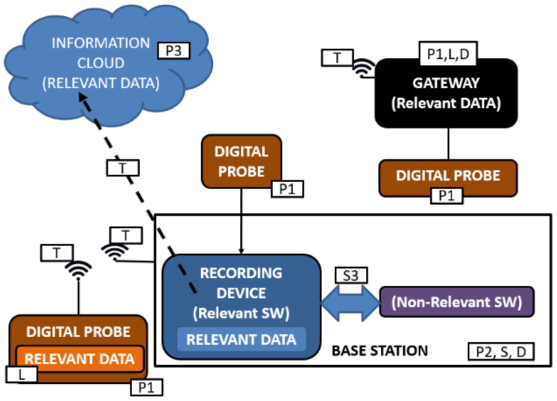

Figure 7. An example of the complex Sensor Network according to according to EN 12830:2018 with application of requirements.

The P1 requirements are applied to sensors, whether they are connected to the base station by hardwired or wireless communication technologies and can also be, for example, on a Gateway. Devices, where P1 requirements are applied, are mostly devices where complex computational power is not required because the tasks of the device are mostly single-purposed such as measurement, data transfer, or storage. The application of P2 requirements can be seen at the Base Station, where there may be a need for final data processing using database systems, or use of static processing where operating systems are used. The P3 application is only for the use of Clouds, where partial responsibility for data security is assumed by the cloud operator, but the manufacturer must be careful how access rights are implemented in combination with the applied user and communication interfaces.

The requirements of block L, are applied in cases where is a need to deal with data storage. It can be sensors or gateways, where it is mostly temporary storage. Or it may be longer-term storage in the Base Station where data needs to be stored for the intended use.

The requirements of block T are applied in cases where data transmission is involved. Figure 7 is shown data transmission between digital probes, base station, gateway, and information cloud.

The requirements of block S (SW Separation) are applied in cases where it is necessary to distinguish between relevant and non-relevant SW, often it is OTS (off-the-shelf) type SW, which was created for general purposes (e.g. various libraries, drivers, etc.). This type of SW can be in base station.

The requirements of block D can be applied to almost any SW where an update is required, it can be sensors or even SW in the Base Station, but it should be ensured that the SW cannot be repaired or updated by an unauthorized person.

4. CONCLUSION

The Sensor Networks are becoming an inherent part of many upcoming technologies, including smart cities, smart grids, complex processes monitoring in industry, autonomous driving, medicine and many other applications.

One of the many examples of SN is the application of EN 12830:2018, for the purpose of process monitoring. When we compare the general approach with what the standard addresses, we can see shortcomings that do not address state of the art options, such as the use of AI, or issues related to network topology. While the standard provides a relatively appropriate approach, it should be pointed out that as new technologies evolve, a wider range of possible applications of technology in SN need to be addressed.

Together with other technologies such as the AI and with the utilization of the Big Data, the SN is becoming an important tool for effectivity optimisation of many processes. The SN has helped to push the limits in metrology towards new effective algorithms in the AI or in challenges in the uncertainty evaluation related to the utilization of the AI as well as in the implementation of solutions for digital transformation.

ACKNOWLEDGEMENT

This work was funded by the Institutional Subsidy for Long-Term Conceptual Development of a Research Organization granted to the Czech Metrology Institute by the Ministry of Industry and Trade. Project number: UTR 22E601104.

REFERENCES

[1] A. Deuter, F. Pethig, The Digital Twin Theory, Project: Asset Administration Shell (Industry 4.0), Munich, 2019. DOI: 10.30844/I40M_19-1_S27-30

[2] R. H. Hariri, E. M. Fredericks, K. M. Bowers, Uncertainty in big data analytics: survey, opportunities, and challenges, Journal of Big Data, 6 (2019), art. no. 44. DOI: 10.1186/s40537-019-0206-3

[3] H. Qi, S. Sitharama Iyengar, K. Chakrabarty, Distributed sensor networks - a review of recent research, Journal of the Franklin Institute, vol. 338, 2001, no. 6, pp. 655-668. DOI: 10.1016/S0016-0032(01)00026-6

[4] H. Khan, Types of AI | Different Types of Artificial Intelligence Systems, 2021. Online [Accessed 13 Match 2023] https://www.researchgate.net/publication/355021812

[5] L. Tucci, A guide to artificial intelligence in the enterprise, R. H. Hariri, E. M. Fredericks, K. M. Bowers, Uncertainty in big data analytics: survey, opportunities, and challenges, Tech Target-Search Enterprise AI: E-Guide, 2021. Online [Accessed 13 Match 2023] https://www.techtarget.com/.

[6] M. M. R. Monjur, J. Heacock, J. Calzadillas, M. D. S. Mahmud, J. Roth, K. Mankodiya, E. Sazonov, Q. Yu, Hardware Security in Sensor and its Networks, Frontiers in Sensors, 3 (2002). DOI: 10.3389/fsens.2022.850056

[7] F. Nekoogar, F. Dowla, R. Twogood, S. Lefton, Secure RFID tag or sensor with self-destruction mechanism upon tampering, United States Patent: Document ID: US 20150339568 A1, 2016.

[8] M. Moni, W. Melo, Jr., D. Peters, R. Mochado, When Measurements Meet Blockchain: On Behalf of an Inter-NMI Network, National Library of Medicine, 2021, DOI: 10.3390/s21051564

[9] ISO/IEC, ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management, International Organization for Standardization, June 2011.

[10] LUM, BIPM, IEC, IFCC, ILAC, ISO, IUPAC, IUPAP, and OIML. Guide to the Expression of Uncertainty in Measurement, JCGM 100:2008, GUM 1995 with minor corrections. BIPM, 2008.

[11] Monte Carlo, BIPM, IEC, IFCC, ILAC, ISO, IUPAC, IUPAP, and OIML. Supplement 1 to the 'Guide to the Expression of Uncertainty in Measurement' – Propagation of distributions using a Monte Carlo method, JCGM 101:2008. BIPM, 2008.

[12] Bayesian Statistical Models, BIPM, IEC, IFCC, ILAC, ISO, IUPAC, IUPAP, and OIML. Guide to the expression of uncertainty in measurement — Part 6: Developing and using measurement models, JCGM GUM-6:2020. BIPM, 2020.

[13] EN 12830:2018 Temperature recorders for the transport, storage and distribution of temperature sensitive goods

[14] WELMEC Guide 7.2, Online [Accessed 13 March 2023] http://welmec.org.