



When a Datum Is Not a Measurement: A Doctrinal Account of Metrological Traceability in Engineering Data Systems

Priyanka Singh^{1,*}

¹ Department of Computer Science and Engineering, ITS Engineering College, Greater Noida, Uttar Pradesh 201308

* Corresponding author: priyankas19005@gmail.com

ARTICLE INFO

Article history:

Received: 05-09-2026

Received in revised form: 14-09-2026

Accepted: 15-09-2026

Available online: 17-09-2026

Keywords:

Calibration

Engineering Data Pipelines

Measurement Uncertainty

Metrological Traceability

Sensor Informatics

ABSTRACT

Engineering Informatics considers any input data to have been captured and treated as "data" once it can be saved (stored), graphed, or fed into a predictive model. On the other hand, metrology considers an input value to be a "measurement", only if there exists a defined relationship with a specified unit via a documented, unbroken series of calibrations where each contributes an explicitly quantifiable amount of uncertainty. This conceptual paper uses this distinction to describe how engineering data systems should be developed. It interprets the International Vocabulary of Metrology, the Guide to the Expression of Uncertainty in Measurement, ISO/IEC 17025, ISO 10012, and various digital twin and data quality instruments as mutually limiting resources. The central argument made here is that a pipeline, twin or operational model which omits to identify the units, the calibration status, or the uncertainties associated with the measurements being modeled has not simply lost some useful metadata; it has converted a measurement into a number. There are three tests presented: Unit Continuity Test, Calibration-Chain Continuity Test, and Uncertainty Inheritance Test. A Metrological Integrity Chain is proposed as a small footprint overlay on top of engineering data systems. The reconstruction is theoretical, not a laboratory intercomparison, and it is offered as a completeness criterion for later empirical studies that claim to act on sensor evidence.

1. INTRODUCTION

When an engineer receives a temperature, when he uses a current test sample for training a fault detector, and when a digital twin accepts new vibration data, they all typically receive "data." They become measurements under the definition of measurement by the International Vocabulary of Metrology only when their relation to a reference can be traced via a documented chain; thus, the metrologically traceable property of a measurement result is defined in that vocabulary as the ability of the result to be connected to a reference through a documented continuous chain of calibrations (each contributing to the measurement uncertainty) [1]. That sentence is not a laboratory courtesy. It is a condition on what may later be believed.

Informatics in engineering has good reason to forget that condition. Engineering informatics finds it easier to store numerals rather than chains. The heterogeneity of vendors and the high rate at which data arrive makes finding time to document the chain difficult. Thus, data quality models measure how complete, up-to-date, and consistent each measured field within the database is [2], FAIR stewardship measures findability and reuse [3] and provenance vocabularies track derivation and activity [4]. Those tools do not independently ask whether a value remains a measurement. A findable, provenanced, and valid-in-schema Celsius reading with an unknown last calibration date would be very well governed as a numeral. But it is not yet a piece of engineering evidence in the metrological sense.

Systems designed for use in engineering sit precisely where this forgetting starts to cost money. Pipelines, digital twins, cyber-physical feedback loops, smart operational decisions, and methods in informatics can each consume values from other sources without regard for the fact that the original value had already lost its unit, its calibration status or its uncertainty. Therefore, a digital twin synchronising such a value is faithfully replicating the flow from a source. However, when an operator acts upon that value, an operation that actuates on it commits capital and risk on a number that cannot be reconstructed as a measurement. This paper attempts no further unification of these four components. Rather, we isolate one prior obligation: a datum used as evidence from sensors must be kept as a measurement.

Condition-monitoring practice already shows why the duty is not academic. Stator-current signatures have long been used to detect and grade induction-motor faults, which means that the current sample is being asked to support a severity claim [5]. Internet-of-Things platforms then group, classify, and integrate such samples at scale [6]. If the sample's unit system, instrument identity, and uncertainty are optional, the severity claim and the platform grouping inherit a silent defect. The defect will not appear in an accuracy table. It will appear when two plants, two vendors, or two years cannot be compared.

This article is a doctrinal paper. It reconstructs obligations already present in primary metrological instruments and asks what those obligations do to engineering data systems. It does not report a new calibration campaign. Four questions organise the argument. First, what do the primary instruments actually require of a measurement result? Second, at which ordinary pipeline and twin joins is that requirement stripped? Third, what tests would make the requirement visible inside an engineering data system? Fourth, what follows for design, standards reading, and later empirical work? The contribution is a Metrological Integrity Chain and three tests: unit continuity, calibration-chain continuity, and uncertainty inheritance.

2. DOCTRINAL METHOD

Doctrinal research provides an overview of how to reconstruct a theory based on previous data from documents (i.e., "primary instruments") instead of analyzing new data. The claims that follow are about conceptual obligation, not about a newly measured plant. The primary instruments in legal doctrine are statutes and decisions. In metrology, the primary instruments are vocabularies, guides and laboratory standards, which have previously defined measurement, calibration, uncertainty and competence.

Three classes of source are distinguished. Primary instruments are the VIM, the Guide to the Expression of Uncertainty in Measurement (GUM), ISO/IEC 17025, ISO 10012, and the SI brochure [7]. Secondary instruments are data-quality, provenance, and digital-twin texts that later engineering informatics treats as definitional [2]. Tertiary sources are application papers that show where measurement claims are made in industrial analytics [5]. Doctrine is the work of reading the first class until the second and third can no longer treat a numeral as a measurement by default.

The method is interpretive. It does not claim a systematic map of every 2020-2026 uncertainty paper. Selection favours instruments that laboratories and accreditation bodies already treat as obligatory. Claims that go beyond those instruments are labelled as proposals of this reconstruction.

3. WHAT THE PRIMARY INSTRUMENTS REQUIRE

3.1 Measurement, Result, and Reference

The VIM does not treat measurement as the mere assignment of a number to a thing. A measurement is a process of experimentally obtaining one or more quantity values that can reasonably be attributed to a quantity [1]. A measurement result includes the set of quantity values and other relevant information, and that other information is not optional colour. It includes the unit and, where possible, a statement of uncertainty. Metrological traceability then binds the result to a reference, commonly a measurement unit in the International System of Units, through calibrations [1]. The ninth SI brochure is the public statement of those units and of the constants that now define them [7]. A pipeline that stores 72.4 without a unit has not stored a measurement result. It has stored a token.

This is stricter than a naming convention. Two vendors can both write temperature and still not share a quantity if one scaled a raw count, the other converted from Fahrenheit, and neither recorded the conversion as a calibration or calculation with uncertainty. Data-quality completeness can be satisfied by a non-null field [2]. Metrological completeness is satisfied only when the field still supports the sentence "this value is a quantity value of *this* kind, in *this* unit, obtained by *this* process."

3.2 Uncertainty as Part of the Result

The GUM treats the measurement result as complete only when it is accompanied by a quantitative indication of the quality of the result [8]. Combined standard uncertainty and, where required, an expanded uncertainty with a stated coverage factor are not statistical decorations for a later paper. They are how the result may be compared with a limit, a twin residual, or another laboratory. ISO/IEC 17025 requires laboratories to evaluate measurement uncertainty and to apply the result when relevant to the validity of reported values [9]. ISO 10012 requires an organisation that manages measuring equipment to keep the measurement process capable of achieving the specified metrological requirements [10].

Engineering analytics often replaces that package with a single point. A remaining-useful-life estimate, a predicted load, or a closed-loop set-point is then treated as sharper than the incoming evidence. Digital-twin surveys already warn that many implementations do not declare fidelity or residual uncertainty [11]. The metrological point is prior. Even a perfectly scoped twin cannot inherit an uncertainty that the pipeline deleted.

3.3 The Unbroken Chain

Traceability is a chain – not simply a certificate hanging on a wall. Every link in the traceability chain represents a calibration which ties together an instrument or a measurement standard with a reference point (with its associated uncertainty) [1]. The requirements for competence, impartiality and operational consistency in the organization producing these links are specified in ISO/IEC 17025 [9]. At some point after installation, replacement, drift, or digital filtering of an industrial sensor, the link(s) may have been recorded as such or the traceability chain has broken. Once a traceability chain is broken, there is no way to "reconnect" the chain with an improved accuracy model; rather, the model will fit an historical record of untraceable numbers.

Calibration here includes more than a sticker date. Digital scaling, unit conversion, temperature compensation, and software filters are calculations that change the quantity value. If they are not documented as part of the measurement process, they are silent recalibrations. Provenance languages can record them as activities [4]. They become metrological only when the activity is also given an uncertainty contribution and a reference.

Table 1 contrasts the duty that ordinary informatics quality already states with the stricter duty that the primary metrological instruments impose.

Table 1. *Informatics quality duties and the stricter metrological duties they do not replace.*

Informatics duty already common	What it can certify	What it cannot certify by itself	Metrological duty still owed
Schema validity and completeness [2]	A field is present and typed	That the field is a quantity value	Unit and kind-of-quantity continuity
FAIR findability and reuse [3]	The record can be located and cited	That the record is a measurement result	Documented link to a reference
Provenance of derivation [4]	Who transformed the value	That the transformation was a calibration	Uncertainty contribution at each link
Twin synchrony and scope [12]	The virtual entity was updated	That the update was a measurement	Inherited uncertainty and validity window

The table is the doctrinal claim of this section. Quality, FAIR, provenance, and twin scope remain necessary. They are not sufficient for sensor evidence.

4. WHERE ENGINEERING DATA SYSTEMS STRIP THE MEASUREMENT

4.1 Acquisition That Lands a Count

The first strip is at the device. Many industrial nodes emit scaled integers, vendor codes, or dimensionless features. IEEE's Internet of Things architectural framework insists on cross-domain description rather than on device ingenuity alone [13]. In practice the description often stops at a tag name. Classification and clustering of Internet-of-Things services can then integrate the tag into a platform without integrating its metrological state [6]. The platform has gained a stream. It has not gained a measurement.

Condition-monitoring pipelines illustrate the same join in analogue form. A neural classifier of stator-current faults is only as traceable as the current measurement that feeds it [6]. If amplifier gain, sampling window, and transducer calibration are omitted, the severity grade is a function of a local count. Two motors compared across sites then look different because their chains differ, not because their faults differ.

4.2 Conditioning That Recalibrates in Silence

The second strip is conditioning. Normalisation of units, clock alignment, outlier clipping, and feature extraction are all necessities that must be done in order for this strip to function properly. Each one is a step in the measurement process. Lakes and late-binding transforms treat them as data-science preludes [14]. An undocumented conversion at any time, which creates a new calibration without uncertainty, is a new calibration. Digital-twin frameworks for manufacturing require observable manufacturing elements and an entity that will carry device information [12]. If the communication entity only carries the latest float, the twin's observable is not the plant quantity. It is the last script.

Time is also part of this strip. A measurement result has been indexed to a measurement process that occurred when the instrument was in a stated state. Clock drift, batch windows, and interpolated historians create a new time-quantity pair. Cyber-physical layering that converts connection into information already assumes that such conversion will be accountable [15]. Conversion which cannot state its uncertainty is not information in the metrological sense. It is a smoother numeral.

4.3 Models That Treat Point Estimates as Sharper Than Evidence

The third strip is Learning & Operations. Methods of soft computing & machine learning will allow for closed loop systems to be tuned faster than traditional tuning using classical models [16]. While speed may not provide a unit of measure, an estimated Remaining Life with a precision of 3 digits post-temperature is not an increase in precision due to expanded uncertainty. Enterprise control has been shown to integrate different levels at which recommendations must reside [17]. A "homeless" model can still be accurate; however, it will never be able to support a measurement-based decision if its inputs are untraceable.

In addition, security falls under this category as part of a chain threat instead of a separate subject. Even though certificates have not expired or have been tampered with, altering any portion of the evidence path renders the calibration chain broken [18]. Therefore, integrity of the evidence path represents a metrological requirement and not simply a cybersecurity score.

Each strip displays similarities. Success in Informatics (A Valid Field, A Trained Model, A Live Twin) supports Metrological Failure (No Unit, No Chain, No Uncertainty). When studies are conducted documenting the former while failing to verify the latter they are documenting behavior of software and not the evidence from Sensors.

5. A DOCTRINE OF METROLOGICAL INTEGRITY

5.1 Statement

The doctrine can be stated in one sentence. An engineering data system receives a value as sensor evidence until all three attributes (unit, calibration chain, and uncertainty) remain associated with it. Once any of these items has been removed from association, even if quality, provenance, twin, or operational machinery remain functional they will no longer perform as a measurement system.

Three tests make the sentence operational.

Unit continuity. This involves determining whether the value still represents a quantity value in terms of a unit of measure of a specific type of quantity. If the answer is yes then this would represent a pass. The unit used is either an SI unit or has been converted to an SI unit [7]. A failure would occur when the value being measured is represented by a numerical value alone; when vendor codes are treated as quantities; or when there is an unstated change in units.

Calibration-chain continuity. The question to be answered here is whether the value can be connected to a reference via well-documented paths such as digital transformations and each path is dated and traceable back to the person who performed the transformation [1]. A pass is achieved when there appears to be an uninterrupted link between an operating instrument and the reference using some form of scaling software. A failure occurs when there is no certificate available; when the last certification occurred outside of an acceptable time frame; or when there exists a filter that was applied but not documented.

Uncertainty inheritance. The next test determines if all subsequent uses of the original value provide a quantifiable quality to the results and do not allow them to become more precise than the original evidence without having first made an additional justification for doing so [8]. A pass occurs when at least a standard uncertainty or a declared decision rule is passed along to the user(s). A failure occurs when the results are presented as point estimates and have resolved their inputs without documentation.

Unlike another industrial architecture, the three tests outlined above exist below pipelines, twins and operations as filters that determine how those systems are able to treat values as evidence. These tests are stricter than typical provenance testing since a provenanced value can still lack a unit and/or an uncertainty [4].

5.2 The Metrological Integrity Chain

Figure 1 draws the tests as a chain rather than as a cycle. The chain is directional because a later node cannot restore a link that an earlier node deleted.

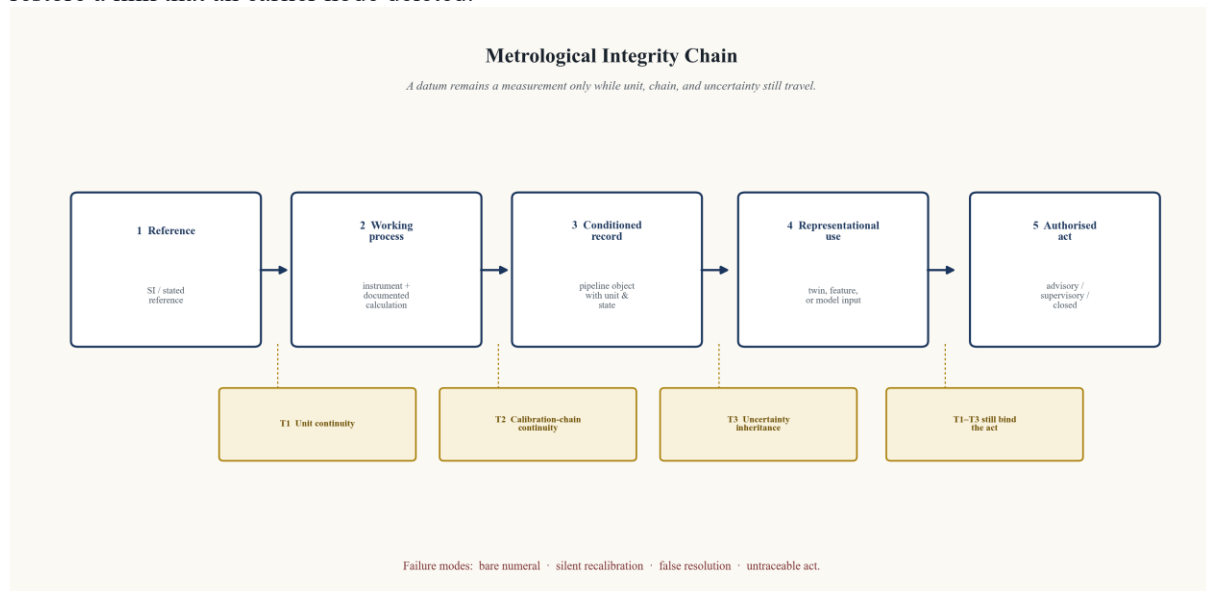


Figure 1. The Metrological Integrity Chain: unit, calibration, and uncertainty must travel from the reference through acquisition and conditioning into any twin or operational act.

Each link in the chain is monitored through one of three tests. The most common types of failure include a single number being recorded during the data collection phase, no alarm sounding when the instrument is recalibrated during the conditioning phase, a wrong value being returned from the model, and some authorized action taking place without the source of the action traceable back to its origin.

The ISO 23247 standard could support the concept presented here with regard to the chain of custody, because it requires the device communication entity to have information regarding the units involved in the measurements made; the state of calibration of those devices; and the uncertainty associated with each measurement, rather than just transmitting a real-time data point [12].

IEC 62264 would also support this concept in relation to the Authorized Act node, provided the Operations Interface will reject any inputs which fail any of the tests [17].

Neither standard would require rewriting for the concepts to be applied. Both standards simply need to be viewed as if a measurement is still a measurement.

5.3 A Compact Vignette

The calibration due date for a vibration accelerometer attached to a gearbox is six weeks away. The accelerometer has a working standard that was the most recent one to calibrate it. The device server emits a 16-bit count. A site script multiplies this counter by a gain stored in a technician's notebook; the results are converted from counts to millimetres/second and then sent to the historian under the tag name GEAR_VIB. A weekly job trains a remaining-useful-life model on the data from this tag and creates a point estimate of 412 hours, which is then sent to an operations dashboard where a supervisor considers it as a trigger for a work order.

The unit continuity will fail unless the type of count and the units of the gain are declared with the record [7]. The calibration chain continuity will fail if there is no dated, attributable link to the gain in the technician's notebook and if there is no way to view the six week time period in the historian [1]. There will be failure of uncertainty inheritance if 412 hours is tighter than any expanded uncertainty that could have been included in writing for either the acceleration or the velocity [8]. Provenance could still name the script and the trainer [4]. The dashboard would still be complete in a data-quality sense [2]. None of that restores

a measurement. The vignette is schematic, not an experiment. It is the form of failure the three tests are built to catch.

5.4 What the Doctrine Does Not Claim

The doctrine does not require every dashboard pixel to carry a GUM budget. It requires that any value used as if it were sensor evidence can, on demand, be expanded into unit, chain, and uncertainty. It does not forbid dimensionless features. It requires that a dimensionless feature not be treated as a quantity value of a physical kind. It does not make every plant a 17025 laboratory. It uses 17025 and ISO 10012 to name competence and process control where the organisation already claims measurement [9]. Claims beyond that (for example a full legal metrology regime for every Internet-of-Things tag) are not made here.

6. DISCUSSION

Designers should attach unit, instrument identity, calibration interval, and a minimum uncertainty marking when the data is acquired (not in a subsequent catalogue) [14]. Scripts used for conditioning the input data should be recorded as measurement process steps and their respective uncertainty contributions. Alternatively, such conditioning scripts should not be allowed to provide twins and actuators. Models consuming sensor evidence should have their uncertainty contribution exposed, and they should not produce a last digit finer than what their uncertainty contribution allows them to [8]. Intelligent operations should consider a failed test as a missing input, not as a missing visualisation.

Models consuming sensor evidence should have their uncertainty contribution exposed, and they should not produce a last digit finer than what their uncertainty contribution allows them to [8].

Intelligent Operations should consider a failed test as a missing input, not as a missing visualization.

For research and design, the implication is narrow. Any studies claiming to have implemented pipelines, twins, or predictive processes using data from plant or product sensors must be able to explain how each of the three tests for these systems can be satisfied or why none of the tests are applicable. This is an issue of completeness, rather than preference for publications focused on lab-based work versus publications focused on computational methods. There could be an empirical follow-up methodology paper providing a compact representation of unit, chain, and uncertainty for very-high rate data streams. Another possible follow-up paper could be a literature review showing how many times papers reporting on digital twins report any uncertainty whatsoever [11].

The limits are those of the genre. There has been no physical measurement of a plant. There has been no inter-laboratory comparison performed. The reconstruction is manufacturing-asset heavy, since there is currently the greatest concentration of sensor-to-actuator claims within this space. Process industries, grids, and vehicles will demonstrate the same tests with just different time scales and different legal-metrology overlays. If such areas identify additional duties beyond those named by the VIM and GUM, then the tests need to be modified. They do not need to be modified simply because some platforms find certification inconvenient.

7. CONCLUSION

Engineering data systems have great capabilities in manipulating numbers, storing those numbers and learning with them, but they lack the capability to manipulate measurements.

The primary metrological instruments already indicate what information a measurement must contain; namely, a quantity value, a unit, a document describing the traceability to a reference point, and an estimate of uncertainty. Quality models, FAIR records, provenance graphs, and twin frameworks cannot supplant this bundle.

These quality models may be able to certify tokens that represent well-managed values that are no longer measurement values.

The purpose of this article was to isolate prior responsibility for engineering informatics.

It proposed three tests (unit continuity, calibration-chain continuity, and uncertainty inheritance) and a Metrological Integrity Chain from reference point through all authorized actions.

Common failures include bare numbers, silent recalibration, false resolution, and untraceable acts.

Future studies will likely provide methods to embed the chain into code; determine the frequency that these chains are broken; demonstrate domains where one of the tests should be rewritten.

REFERENCES

- [1] Joint Committee for Guides in Metrology. (2012). *International vocabulary of metrology: Basic and general concepts and associated terms (VIM)* (JCGM 200:2012, 3rd ed.). BIPM. <https://doi.org/10.59161/JCGM200-2012>
- [2] International Organization for Standardization. (2008). *Software engineering: Software product Quality Requirements and Evaluation (SQuaRE): Data quality model* (ISO/IEC 25012:2008).
- [3] Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., da Silva Santos, L. B., Bourne, P. E., Bouwman, J., Brookes, A. J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C. T., Finkers, R., ... Mons, B. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, 3, 160018. <https://doi.org/10.1038/sdata.2016.18>
- [4] Moreau, L., & Missier, P. (Eds.). (2013). *PROV-DM: The PROV data model*. World Wide Web Consortium. <https://www.w3.org/TR/2013/REC-prov-dm-20130430/>
- [5] Pandey, J. K., & Srivastava, V. (2009). Feed forward neural network for detection and severity evaluation of stator faults in induction motor using stator current. In *International Conference on Control, Automation, Communication and Energy Conservation (INCACEC)*. IEEE.
- [6] Pandey, J. K., Bhuva, D., Bhuva, A., Abbas, S. H., Verma, A., & Moharekar, T. T. (2023). Classification and clustering of Internet of Things (IoT) for integrating IoT services platform. In *2023 IEEE 2nd International Conference on Industrial Electronics: Developments & Applications (ICIDEA)* (pp. 259–262). IEEE. <https://doi.org/10.1109/ICIDEA59866.2023.10295225>
- [7] Bureau International des Poids et Mesures. (2019). *The International System of Units (SI)* (9th ed.). BIPM. <https://doi.org/10.59161/AUEZ1291>
- [8] Joint Committee for Guides in Metrology. (2008). *Evaluation of measurement data: Guide to the expression of uncertainty in measurement* (JCGM 100:2008). BIPM. <https://doi.org/10.59161/JCGM100-2008E>
- [9] International Organization for Standardization. (2017). *General requirements for the competence of testing and calibration laboratories* (ISO/IEC 17025:2017).
- [10] International Organization for Standardization. (2003). *Measurement management systems: Requirements for measurement processes and measuring equipment* (ISO 10012:2003).
- [11] Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital twin: Enabling technologies, challenges and open research. *IEEE Access*, 8, 108952–108971. <https://doi.org/10.1109/ACCESS.2020.2998358>
- [12] International Organization for Standardization. (2021). *Automation systems and integration: Digital twin framework for manufacturing: Part 1: Overview and general principles* (ISO 23247-1:2021).
- [13] Institute of Electrical and Electronics Engineers. (2019). *IEEE standard for an architectural framework for the Internet of Things (IoT)* (IEEE Std 2413-2019). <https://doi.org/10.1109/IEEESTD.2019.8686444>
- [14] DAMA International. (2017). *DAMA-DMBOK: Data management body of knowledge* (2nd ed.). Technics Publications.
- [15] Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters*, 3, 18–23. <https://doi.org/10.1016/j.mfglet.2014.12.001>
- [16] Pandey, J. K., Kotti, J., Parimita, Dhabliya, D., Sharma, V., Choudhary, S., & Anand, R. (2024). Integration of nature-inspired mechanisms to machine learning in real time sensors, controllers, and actuators for industrial automation. In N. Sindhvani, R. Anand, A. George, & D. Pandey (Eds.), *Robotics and automation in Industry 4.0* (pp. 1–25). CRC Press. <https://doi.org/10.1201/9781003317456>
- [17] International Electrotechnical Commission. (2013). *Enterprise-control system integration: Part 1: Models and terminology* (IEC 62264-1:2013).
- [18] Pandey, J. K., Kumar, S., Lamin, M., Gupta, S., Dubey, R. K., & Sammy, F. (2022). A metaheuristic autoencoder deep learning model for intrusion detector system. *Mathematical Problems in Engineering*, 2022, Article 3859155. <https://doi.org/10.1155/2022/3859155>