IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received 15 July 2024, accepted 28 July 2024, date of publication 2 August 2024, date of current version 3 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3438068

RESEARCH ARTICLE

A Framework for Quality Measurements of Intelligent Systems in the Context of Contemporary International Standards

MANSOOR N. ALI[1] **AND MOTEA M. ALJAFARE**[1,2]
[1]Faculty of Computing and IT, Sana'a University, Sana'a, Yemen
[2]Faculty of Computing and IT, University of Science and Technology, Sana'a, Yemen

Corresponding author: Motea M. Aljafare (Mot.AlGaafari@su.edu.ye)

ABSTRACT Intelligent systems (IS) are increasingly prevalent in modern life, and their success or failure heavily depends on their quality and adherence to contemporary international standards. The lack of establishing quality standards for intelligent systems is a significant obstacle for organizations striving for efficient implementation. So, choosing the appropriate standards for intelligent systems is essential for quality control. Quality Measures of Intelligent Systems (QMIS) are defined within specific contexts based on standards. This study aims to describe and discuss the criteria that determine the quality of intelligent systems (QIS) and to analyze the fundamental criteria and techniques for assessing the quality of intelligent systems as well as their impact on the quality of intelligent systems within the context of current international standards to create a general framework for quality. This framework will be used to assess the effectiveness, significance, and applicability of intelligent systems and to gauge the level of intelligence of intelligent systems.

INDEX TERMS Intelligent systems, measure, framework, quality, standards.

I. INTRODUCTION

An intelligent system is a system that mimics some of the qualities of intelligence seen in nature. These include information compression (data to knowledge), learning, adaptability, resilience across issue domains, improved efficiency (over time and/or space), and extrapolated reasoning [1]. QIS aids in enhancing the organization's work processes and information flow, which can improve decision-making [2]. Businesses use intelligent systems because of their capacity to gather, store, organize, process, and distribute vast amounts of data [3]. Intelligent systems give a systematic, methodical approach to solving significant and somewhat complicated issues and obtaining repeatable and trustworthy outcomes. According to several definitions, intelligence is the capacity for comprehension, learning from experience, and understanding. Of course, other definitions exist, such as the ability to understand and remember information, mental prowess, and react rapidly and effectively to novel circumstances [4].

More focus should be placed on standardizing intelligent systems to encourage technical innovation and foster industrial progress. The implementation of artificial intelligence technology and the commercialization of research findings are accelerated through standardization efforts [5]. An intelligent automated system offers services and allows users to use it as much as possible without wasting resources or energy. Several domains represent different types of intelligent systems based on the objective. Reference [6] defined intelligence as a machine's innate quality. The definition of an intelligent computer (or system) possesses some computational ability to behave like a person [7]; nevertheless, the intelligence of a system cannot be determined by a predetermined formula; instead, it should be a composite

The associate editor coordinating the review of this manuscript and approving it for publication was Amin Zehtabian.

indicator that captures how well the system performs in various contexts. As a result, this characteristic has to be flexible and dynamic [7]. An intellectual ensemble is a complex of compatible intelligent systems interacting through an intelligent interface to implement a technological process, social services, transdisciplinary, multidisciplinary research, or a manufacturing cycle [8]. A system must be able to process data, recognize the links between events or objects, perform meaningful tasks, and adapt the information it has learned to a changing environment to be termed intelligent. A typical intelligent system has to possess the following characteristics: Failure-tolerant, Self-correcting, Self-organizing, Adaptive, Mobile, Distributed, Networked, Robust, Context & Situation-aware, Seamless Integration, Validation, and Certification [9]. Different quality criteria may be applicable based on the application and environment in which an intelligent system is utilized. However, it is possible to ensure that intelligent systems are of the highest quality and function well by following the general guidelines and best practices.

II. PREVIOUS RESEARCH

Some current international standards will be discussed to describe the content of each standard, if possible.

The following is survey of the international standards that align with intelligent systems:

A. ITIL(2013)

A productive approach for effectively communicating IT best practices. It focuses on information system quality management about IT infrastructure and production [16].

B. CMMI,(2014)

CMMI identifies three areas of interest: CMMI for Development (CMMI-DEV), CMMI for Services (CMMI-SVC), which is services management-focused, and CMMI for Acquisition (CMMI-ACQ). CMMI-DEV, which was adopted in 2014. The CMMI model is a set of best practices that guide improving and assessing a company's maturity process [16].

C. ISO 9126(2001)

It was created utilizing the McCall and Boehm models, the list of internal and external characteristics of a software product, and the content (Functionality, Reliability, Usability, Efficiency, Maintenance, and Portability) to align the assessment of software or system products with the ISO quality model [1].

D. ISO 25010 (2011)

It is an enhancement to the ISO 9126 Model, which has the quality criteria: Functionality, Reliability, Usability, Efficiency, Compatibility, Security, Maintenance, and Portability that must be modified for AI systems. ISO/IEC has also started an effort to develop a standardized model [11]. It will increase industrial efficiency because it is an international standard that adheres to ISO/IEC 25010 [22].

E. DIN SPEC 92001-1(2019)

It is a freely downloadable standard released in April 2019 by the German organization in charge of standardization (DIN). Its purpose is to give an overview of the AI lifecycle process and the quality standards. Functionality and performance, robustness, and comprehensibility are the three pillars of quality described. To be compatible with current ISO standards, functionality and performance are referred to functional correctness and completeness in this study.

F. SQUARE

The SQuaRE design can help to guarantee the dependability, accuracy, and suitability of intelligent systems for the needs of their intended users. It outlines standards for evaluating the data quality required to train intelligent systems and the models and algorithms used to analyze the data and make judgments or predictions. The SQuaRE design can also help to ensure that the intelligent systems are transparent, understandable, and ethical. It specifies criteria for assessing the fairness, accountability, and transparency of the algorithms and models employed in intelligent systems. Identifying, measuring, and evaluating AI system quality [10].

G. IEEE (ECPAIS –7010™ -2020 - P7014™)

The IEEE principles cover various issues related to intelligent systems, including data protection, openness, responsibility, fairness, and human oversight [15]. They also guide the creation of inclusive, open, and accessible intelligent systems for all users, regardless of socioeconomic status, race, gender, or other traits.

III. PRIMARILY LITERATURE REVIEW

A. INTELLIGENT SYSTEMS

The subject of intelligent systems is complex and subject to debate. From a computational standpoint, a system's intelligence can be defined by its memory, learning, flexibility, adaptiveness, temporal dynamics, reasoning, and capacity to handle imprecise and ambiguous data [12].

B. QUALITY MEASUREMENT

A single metric cannot determine quality. It requires the establishment of characteristics and terms that can be used to define and evaluate quality standards. ISO/IEC 25010 describes two models: A quality model for the product and an actual quality model [13].

C. INTELLIGENT SYSTEMS STANDARDS

Intelligent systems Standards allow different intelligent systems to collaborate and communicate with each other without the need for specific translation or integration. These standards promote quality by outlining requirements for dependability, performance, and safety. These components work together to accomplish common goals. Standards provide best practices for developing, creating, and using intelligent systems. Manufacturers and developers of intelligent systems

FIGURE 1. The criteria for quality measurements of intelligent systems.

can ensure that their products fulfill defined quality criteria by following these standards, which fosters confidence and trust in the systems.

IV. CRITERIA FOR INTELLIGENT SYSTEMS QUALITY

An intelligent system's construction quality can affect its efficacy, safety, and success. When judging the quality of intelligent systems, keep the following points in mind:

1) **Reliability:** Intelligent systems should be reliable and consistent in their performance even under varying conditions. Measuring their reliability is necessary to ensure that they are operating as planned. Failure, time, and environment are the three essential components of dependability. In addition to hardware failure, an IS system's failure events may primarily be attributed to software flaws [14].

Smart systems must be reliable and consistent in their performance, even under different conditions. The reliability of intelligent systems can be measured to ensure that they operate as planned through:

$$\mathrm{Re} = 2 * \frac{\text{precision} * \text{recall}}{\text{precision} + \text{recall}} \tag{1}$$

We can improve the dependability of intelligent systems by taking suitable action after becoming aware of any potential influencing circumstances. For instance, you can select a straightforward goal, real-world representative data, and adequate processing power. For example, suppose we have a binary classification problem where we want to predict whether a given medical test is positive or negative for a disease. We have a dataset of 100 patients, of which 90 are negative and 10 are positive. We train an intelligent system on this dataset and use it to predict the class labels of a new set of 50 patients.

Suppose the system correctly predicts 8 out of the 10 positive patients but also predicts 5 negative patients as positive. Then the TP, FP, and FN values are:

TP = 8, FP = 5, FN = 2, TN = 35 (since the system correctly predicted 35 negative patients); using these values, we can compute the precision and recall:

Recall = TP / (TP + FN) = 8 / (8 + 2) = 0.8; Precision = TP / (TP + FP) = 8 / (8 + 5) = 0.615.

TABLE 1. Reliability characteristics of IS.

Variable	Average	Composite Reliability (ρ)	Cornbrash Alpha (α)
MTTF	0.795	0.886	0.742
MTTR	0.783	0.915	0.861
Availability	0.720	0.928	0.903
growth modeling	0.893	0.962	0.940

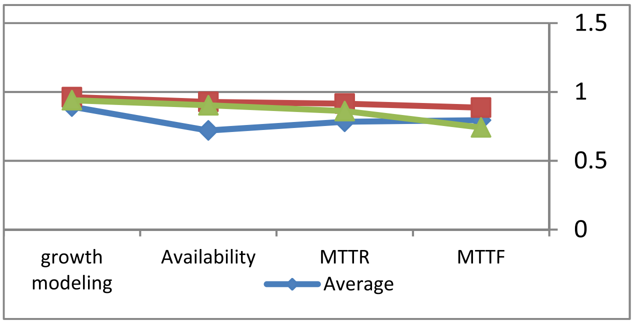

FIGURE 2. shows the reliability of the intelligent systems.

Then, we can compute the F1 score using the formula:

F1 is equal to 2 ∗ (precision + recall) / (precision + recall) = 2 ∗ (0.615 ∗ 0.8) / (0.615 + 0.8) = 0.696.

Therefore, the system's F1 score is 0.696, which measures its overall reliability in correctly identifying positive patients.

2) **Robustness:** Intelligent systems should be able to handle unexpected situations and inputs gracefully without crashing or producing incorrect results, and the system should be able to function effectively even in the presence of unforeseen inputs or changes to the operating environment. Intelligent systems should be robust to errors and unexpected inputs. This means they should be able to continue functioning correctly even when presented with incomplete, corrupted, or otherwise incorrect data. There are two general approaches to robust AI: robust against model errors and robust against unmolded phenomena [16].

It should describe an intelligent system's ability to perform well in any operational environment, even with unexpected inputs or variables, without crashing or delivering inaccurate outputs. It should decide on the alternatives, establish the criteria, determine the relative weights of each criterion, and assess each alternative's criterion. There are four components to the problem:

- Determine the R alternatives
- Set criteria C
- The relative importance (weights) of each criterion rt
- The criterion values for each alternative V Explainability

It can be expressed in the following formula:-

$$\mathrm{Ro} = (\mathrm{Ri} * \mathrm{C})\mathrm{rt} \,/\, \mathrm{V}$$

3) **Explainability:** Users should be able to comprehend how the system operates and why it generates its results.

TABLE 2. General desiderata for helpful explanations of IS.

D1:	Fidelity: The explanation must accurately reflect what the IS performs in practice.
D2:	Include elements like degrees of abstraction, user competencies, and interaction.
D3:	To support a judgment, sufficiency should be able to define language and describe function.
D4:	Minimal construction costs The justification should not dominate the expense of building IS.
D5:	The explanation system's efficiency should not severely slow down the IS.

To determine how explainable intelligent systems are, a variety of methodologies are widely used:

- Local interpretability is a method for determining how a system decides in a particular situation.
- Global interpretability: This method helps us comprehend how a system generally decides.
- User studies: This method asks users to rank the system's explainability.

The review lists five general desiderata for helpful explanations of IS, adding significant perspective to recent work in the field [18].

4) **Usability:** Intelligent systems should be designed to focus on usability and user experience. Usability refers to how well users can use the system to accomplish their objectives. Usability, a crucial component of the whole user experience includes elements like simplicity, adaptability, effectiveness, contentment, and accessibility. Usability is defined via five quality components and identified as a quality attribute [19]: (1) learnability: the simplicity with which new users can operate all fundamental features of the design. (2) Efficiency: the speed at which users can complete tasks once they have become accustomed to the design. (3) Memorability: the simplicity with which users can revert to their previous proficiency in site usage. (4) Errors: the frequency, seriousness, and simplicity of recovering from user-made mistakes; and (5) satisfaction: the fun of utilizing the design.

About three types of usability analysis techniques are available and ranked by several authors as follows:

- Heuristic: These techniques are based on the opinions of usability experts who analyze the system and determine its strengths and weaknesses from an end-user perspective.
- Subjective: These methods are based on the opinions of system users who evaluate operational prototypes and provide feedback on their usefulness.
- Empirical: These methods, which depend on how system users interact with it, work by gathering information about actual system usage.

5) **Scalability:** Intelligent systems should be able to scale to handle large volumes of data and users without sacrificing performance or accuracy. Scalability in intelligent systems is typically measured by their ability to efficiently handle increasing amounts of data, users, or tasks. Scalability is a critical concept in many engineering disciplines and is crucial to realizing operational intelligent systems capabilities. Identify three areas of focus to advance scalable intelligent systems: Scalable management of data and models, Enterprise scalability of intelligent systems development and deployment, and Scalable algorithms and infrastructure [16].

A few key metrics are commonly used to assess intelligent systems' scalability as follows:

- Response time measures the time it takes for an intelligent system to respond to a user request or complete a task. As the system scales up, the response time should remain relatively constant or increase only moderately.
- Throughput: This measures the number of requests or tasks an intelligent system can handle per unit of time. As the system scales up, the throughput should increase proportionally.
- Resource utilization: measures how the intelligent system uses its available resources, such as CPU, memory, and storage, efficiently. As the system scales up, it should be able to use its resources more efficiently to handle the increased workload.
- Availability: This measures the percentage of time that the intelligent system is available and responsive to user requests. As the system scales up, it should maintain a high level of availability to ensure that users can always access it when needed.

6) **Efficiency:** Intelligent systems should be efficient in their use of resources. This means they should be able to produce results quickly and without excessive memory or processing power. Efficiency in intelligent systems is typically measured by how effectively the system can accomplish its intended tasks while minimizing resource usage, such as CPU time, memory, or energy consumption. Optimizing efficiency in an intelligent system often involves a trade-off between accuracy and resource usage. Several key metrics are commonly used to evaluate the efficiency of intelligent systems, including:

- Accuracy measures are the correctness of the system's output or predictions and are critical indicators of efficiency in systems that perform classification, prediction, or other types of data analysis.
- Throughput measures: the rate at which the system can process requests or tasks. It is a crucial indicator of efficiency in systems that handle extensive data or requests.
- Latency measures: the time the system takes to process a request or complete a task. It is a crucial indicator of efficiency in systems that require real-time or near-real-time performance.

7) **Security:** Proper security measures should be implemented to prevent unauthorized access, data breaches, and other security risks. Intelligent systems should be secure from unauthorized access or manipulation. This is especially important for systems that control critical infrastructure or contain sensitive data. Its characteristics include whether the traditional security detection is specific, whether the security

response can ensure timely closed-loop, and whether the security strategy is concerned about accuracy [20].

- Security is a critical aspect of intelligent systems, as these systems often handle sensitive data and perform necessary functions. Several methods and techniques can be used to ensure the security of intelligent systems, including:
- Access control: limits authorized users' access to the system and its data. This can be achieved through authentication, authorization, and multi-factor authentication, which require users to provide credentials or other forms of identification before gaining access to the system.
- Encryption: Encryption involves encoding data so unauthorized users cannot read it. Data encryption, SSL/TLS encryption, and secure communication protocols help protect data in transit and at rest.
- Auditing and logging: Auditing and logging involve recording and monitoring system activity, including user actions, system events, and data access. This can help detect and prevent security breaches and provide a record of system activity for forensic analysis.
- Vulnerability management: Vulnerability management involves identifying and mitigating potential security vulnerabilities in the system, such as software bugs or configuration errors. This can be achieved through regular software updates, patch management, and vulnerability scanning.
- Threat intelligence: Threat intelligence involves gathering and analyzing information on potential security threats, such as malware, phishing, or other attacks. This can be used to proactively identify and prevent potential security threats before they can influence the system.
- Disaster recovery and business continuity planning: Disaster recovery and business continuity planning involves developing and implementing plans for responding to and recovering from security breaches or other system failures. This can help minimize the impact of security incidents and ensure that the system can quickly return to normal operations.

The security threats of intelligent systems can be limited to Sneak Attacks(Se1), Probe or Scan (Se2), Automated Eavesdropping (Se3), Automated password attacks (Se4), spoofing (Se5), denial-of-service attacks (Se6), malware (Se7), physical infrastructure attacks (Se8), human error (Se9), and social engineering (Se10). Assuming that Q is the number of requests of the intelligent system, the wish of the intelligent system can be calculated as follows:

$$\sum\nolimits_{i=1}^{10} \mathrm{Se(i)} \Big/ \mathrm{Q} \tag{2}$$

8) **Fairness:** The system should be designed and implemented to avoid bias and discrimination, providing equal treatment to all users regardless of race, gender, or other characteristics. Intelligent systems should be fair. This means that they should not discriminate against any particular group of people or individuals. Being unbiased toward each person and group concerned might be a broad definition of fairness. Fairness, though, can be viewed in several ways depending on the individual and the situation [21].

To evaluate fairness and permit the comparison of various IS, it is essential to standardize the bias assessment on a linear scale. As a result, we present the Fairness score for the entire system and the Bias Index for each protected property as the accepted benchmarks for evaluating fairness. The following defines the IS fairness score: [21]:

$$\mathrm{FS} = 1 - \sqrt{\frac{\sum_{i=1}^{m} \sum_{j=1}^{n} (\mathrm{Mij} - \mathrm{Mj})\, 2}{\mathrm{mn}}} \tag{3}$$

When i denotes the protected attribute's number, j denotes the fairness metric's number, n denotes the total number of fairness metrics employed, and m denotes the total number of protected attributes taken into account by the AI system. Mij: the value of the ith protected attribute's jth fairness metric, Mj0: The jth fairness metric's ideal value is 1 for ratio metrics and 0 for difference metrics.

9) **Transparency:** Intelligent systems should be transparent to users. This means that users should be able to understand how the system works and why it produces the outputs that it does. Intelligent systems enable decision-making with human-like or even super-human cognitive abilities for specific tasks [22]. According to the growing body of design-based literature on understandable, intelligent systems, deep learning algorithms' lack of transparency hinders user acceptability, making the systems ineffective. Reference [22] Transparency and accountability have attracted increasing interest in providing more effective system training, better reliability, and improved usability [23]. Humans' apprehension about AI predictions frequently prevents the deployment of helpful IS technologies. Because of this, the IS research community has been concentrating on enhancing the transparency of IS judgments by offering justifications [21]. The notion of transparency demands the use of clear, succinct language and various types of transparency. Any information and communication related to the processing of personal data must be easily accessible and intelligible:

- To the developer.
- To the user
- To the community at large
- To provide an expert.
- To facilitate monitoring, testing, and the public.

10) **Accountability:** Intelligent systems should be accountable. This means that there should be a way to hold the developers or owners of the system responsible for its actions. "Answerability" is the obligation to give information about an action taken, explain or justify the taking of that action, and commit to consequential action, including punishment and rectification [21]. Accountability in intelligent systems refers to the obligation of designers, operators, and users to take responsibility for the system's decisions and results.

This includes accountability for whatever damage the system may have caused and accountability for ensuring the system functions safely, justly, and efficiently.

Various accountability models are pertinent in the setting of intelligent systems. Among the essential forms of accountability are:

- Legal accountability is the term used to describe people's or organizations' responsibility under the law for the activities and results of intelligent systems.
- Social accountability: People and organizations have a responsibility known as social accountability to ensure that intelligent systems are created and used in a way that is consistent with society's needs and values.
- Technical accountability is the obligation of people or organizations to ensure that intelligent systems are developed and used safely and securely.

11) **Ethics:** Intelligent systems should be designed and used ethically and responsibly, with attention to bias, privacy, and fairness issues. The system should adhere to ethical principles and values and should not be used to support activities that are illegal, harmful, or unethical; towards the Ethics of Autonomous and Intelligent Systems, the IEEE Standards Association established a global campaign in April 2016. It is impossible to emphasize the importance of this undertaking, which represents a turning point in the development of ethical standards coming from a professional organization with the stature and scope of the IEEE Standards Association. It is also a radical move [24].

A set of rules and principles known as the standards of ethics in intelligent systems has been established to ensure that intelligent systems are created and used responsibly and ethically. Some significant ethical guidelines for intelligent systems include the following:

- Privacy: Intelligent systems should be developed to safeguard the confidentiality of users' personal information. As a result, developers must ensure that data is gathered and handled by recognized privacy standards and laws.
- Safety should be the priority while developing intelligent systems, and the danger of harming people, property, or the environment should be minimal. This is especially crucial for systems like autonomous vehicles or medical equipment that have the potential to hurt people.

Human oversight: Intelligent systems should be built with human monitoring and intervention in mind, especially when making decisions or taking actions that could have a significant impact on people or society as a whole

12) **Accuracy:** Intelligent systems should continually deliver correct outcomes with a low error rate. The way accuracy is measured relies on the type of intelligent system in question and the use case for which it is designed. Here are a few typical techniques for gauging the precision of intelligent systems:

- Classification accuracy (CA): Classification accuracy measures how often an intelligent system classifies something correctly. It is usually determined by comparing the system's predictions to a list of predetermined results or labels.

$$CA = \frac{\text{Number of correct predictions}}{\text{Total number of predictions}} \text{x}100\% \tag{4}$$

- Regression accuracy measures the degree to which an intelligent system's anticipated values match the actual values. It is usually calculated by contrasting the system's predictions with a predetermined set of values.

$$\text{R-squared} = 1 - \frac{\text{Sum of squared residuals}}{\text{Total sum of squares}} \tag{5}$$

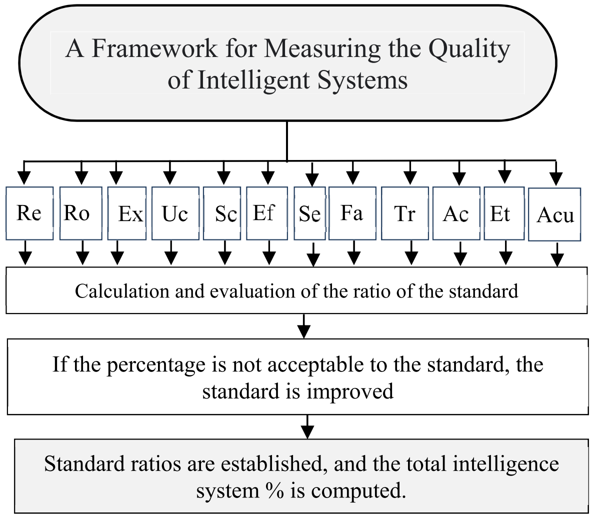

FIGURE 3. Discussion of a framework for measuring the quality of intelligent systems.

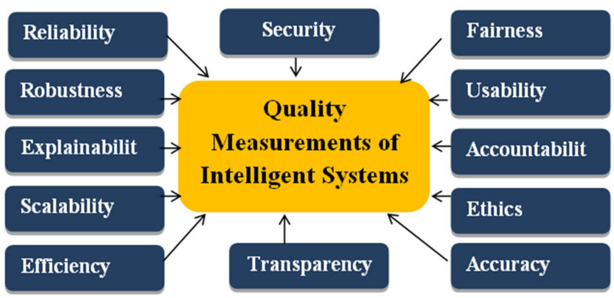

FIGURE 4. Characteristics of measurement standards and their integral connection to form the quality of intelligent systems.

V. PROPOSED FRAMEWORK FOR QUALITY MEASUREMENTS OF INTELLIGENT SYSTEMS

A proposed framework is a list of standards for evaluating the effectiveness of intelligent systems. A standardized quality measurement framework assesses an intelligent system's performance, efficacy, and general quality.

The primary criteria for assessing the quality of intelligent systems are interconnected and frequently reinforce one another. For instance, openness and explainability are crucial to ensure that intelligent systems are fair and do not reinforce prejudice or discrimination. Privacy and security are essential to safeguard user data and prevent illegal access. It is also important to note that each standard's relative value may change depending on the intelligent system's application. For instance, accuracy and explainability may be more crucial in a medical diagnostic system, but user experience and flexibility may be more significant in a recommendation system. Overall, the framework standards for intelligent systems quality measures offer a helpful foundation for assessing and enhancing the performance and efficacy of intelligent systems while also guaranteeing their morality and social responsibility.

VI. CONCLUSION

Intelligent systems (IS) must adhere to standards and quality control to succeed in today's society. Many organizations struggle to use IS effectively due to a lack of clear quality criteria. However, several global standards for software and systems engineering can be applied to the development of intelligent systems. Recent standards, such as the IEEE ECPAIS recommendations and the IEEE 7010-2020 standard, provide a framework for creating AI and autonomous systems that are ethically responsible and aligned with human values.

This proposed framework aims to ensure responsible and accountable development and deployment of intelligent systems, aligning with ethical and societal values. Adhering to this framework can lead to success in various areas of modern life. It emphasizes openness, interpretability, and the consistent exchange of data while encouraging innovation and continual improvement.

REFERENCES

[1] I. Rudas and J. Fodor, "Intelligent systems," *Int. J. Comput., Commun. Control*, vol. 3, no. 3, pp. 132–138, 2008.
[2] W. Y. N. W. Z. Abidin and Z. Mansor, "The criteria for software quality in information system: Rasch analysis," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 9, p. 69, 2019.
[3] T. Knauer, N. Nikiforow, and S. Wagener, "Determinants of information system quality and data quality in management accounting," *J. Manage. Control*, vol. 31, nos. 1–2, pp. 97–121, Apr. 2020.
[4] L. S. V. Pérez, A. F. G. Tornés, E. M. F. Riverón, A. M. S. Hernández, and N. I. P. Galeana, "Software quality methodology to train engineers as evaluators of information systems development tools," *Universal J. Educ. Res.*, vol. 6, no. 12, pp. 2942–2951, Dec. 2018.
[5] N. Trisnawati, Z. Baridwan, and B. Hariadi, "Information system quality influence on organization performance: A modification of technology-based information system acceptance and success model," *Russian J. Agricult. Socio-Economic Sci.*, vol. 72, no. 12, pp. 107–114, Dec. 2017.
[6] S. Aouhassi and M. Hanoune, "Information system quality: Managers perspective," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 8, pp. 493–502, 2018.
[7] R. Gao and L. Tsoukalas, "Performance metrics for intelligent systems: An engineering perspective," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep., 2002, pp. 5–10.
[8] E. Bryndin, "Standardization of artificial intelligence for the development and use of intelligent systems," *Adv. Wireless Commun. Netw.*, vol. 6, no. 1, p. 1, 2020.
[9] P. Dahiya, P. Chaudhary, J. S. Saini, and S. Kumar, "Intelligent systems: Features, challenges, techniques, applications & future scopes," *Intell. Syst. Mobile Adhoc Netw.*, 2007.
[10] F. Schneider and B. Berenbach, "A literature survey on international standards for systems requirements engineering," *Proc. Comput. Sci.*, vol. 16, pp. 796–805, Jan. 2013.
[11] H. Dahar and O. Roudies, "Mapping of quality standards," *Int. J. Innov. Technol. Exploring Eng.*, vol. 8, pp. 2406–2412, 2019.
[12] A. V. Kopyltsov, "Selection of metrics in software quality evaluation," *J. Phys., Conf. Ser.*, vol. 1515, no. 3, Apr. 2020, Art. no. 032018.
[13] Z. Li, S. Wu, H. Zhou, S. Zou, and T. Dong, "Analytic model and assessment framework for data quality evaluation in state grid," *J. Phys., Conf. Ser.*, vol. 1302, no. 2, Aug. 2019, Art. no. 022083.
[14] Y. Hong, J. Lian, L. Xu, J. Min, Y. Wang, L. J. Freeman, and X. Deng, "Statistical perspectives on reliability of artificial intelligence systems," *Qual. Eng.*, vol. 35, no. 1, pp. 56–78, Jan. 2023.
[15] C. Wang et al., "A deep learning framework for predicting tumor proliferation score of breast histopathological images," *IEEE J. Biomed. Health Inform.*, vol. 25, no. 2, pp. 429–440, 2020.
[16] H. Barmer, R. Dzombak, M. Gaston, E. Heim, J. Palat, F. Redner, T. Smith, and N. VanHoudnos, "Robust and secure AI," Tech. Rep., 2021.
[17] R. Hamon, H. Junklewitz, and I. Sanchez, "Robustness and explainability of artificial intelligence—From technical to policy solutions," Publications Office Eur. Union, Luxembourg, Tech. Rep. EUR 30040, JRC119336, 2020, doi: 10.2760/57493.
[18] L. K. Hansen and L. Rieger, "Interpretability in intelligent systems—A new concept?" in *Explainable AI: Interpreting, Explaining and Visualizing Deep Learning*, 2019, pp. 41–49.
[19] A. Dingli and S. Cassar, "An intelligent framework for website usability," *Adv. Hum.-Comput. Interact.*, vol. 2014, no. 1, pp. 1–13, 2014.
[20] R. Yu, "Security framework of artificial intelligence system," *J. Phys., Conf. Ser.*, vol. 1927, no. 1, May 2021, Art. no. 012011.
[21] A. Agarwal, H. Agarwal, and N. Agarwal, "Fairness score and process standardization: Framework for fairness certification in artificial intelligence systems," *AI Ethics*, vol. 3, no. 1, pp. 267–279, Feb. 2023.
[22] J. Wanner, L.-V. Herm, K. Heinrich, and C. Janiesch, "The effect of transparency and trust on intelligent system acceptance: Evidence from a user-based study," *Electron. Markets*, vol. 32, no. 4, pp. 2079–2102, Dec. 2022.
[23] A. Smith-Renner, J. Dodge, C. Dugan, S. Kleanthous, T. Kuflik, M. K. Lee, B. Y. Lim, A. Sarkar, A. Shulner-Tal, and S. Stumpf, "TExSS: Transparency and explanations in intelligent systems," in *Proc. 26th Int. Conf. Intell. User Interface-Companion-IUI Companion*, College Station, TX, USA, Apr. 2021, pp. 24–25.
[24] A. Winfield, "Ethical standards in robotics and AI," *Nature Electron.*, vol. 2, no. 2, pp. 46–48, Feb. 2019.

MANSOOR N. ALI received the Ph.D. degree in technical sciences from the D. Mendeleev University of Chemical Technology, Russia, in 2011. He is currently an Associate Professor and the Head of the Department of Information Systems, Faculty of Computer and Information Technology, Sana'a University, Yemen. He has published many research papers in journals and supervised many master's and Ph.D. theses. His current research interests include the IoT, intelligent systems, DSS, and ES.

MOTEA M. ALJAFARE was born in Ibb, Yemen, in 1981. He received the Bachelor of Science degree, the M.S. degree in computer mathematics from Ibb University, Yemen, in 2003, and the master's degree from Arab Academy, Jordan, in 2012.

From 2004 to 2012, he was a Research Assistant at the University of Science and Technology. Since 2012, he has been with Ibb University, and the Department of Technical Information, University of Science and Technology. He is the author of about 15 lectures. His research interests include artificial intelligence, computational scientific systems analysis, unfreezing, software engineering, and information systems operations and applications.