Monitoring Approach of Cyber-Physical Systems by Quality Measures

Pedro Merino Laso[1(✉)], David Brosset[1,2], and John Puentes[1,3]

[1] Chair of Naval Cyber Defense, École navale - CC 600, 29240 Brest Cedex 9, France
{pedro.merino,david.brosset}@ecole-navale.fr
[2] Naval Academy Research Institute, École navale - CC 600,
29240 Brest Cedex 9, France
[3] Département ITI - Institut Mines-Telecom, Telecom Bretagne Lab-STICC UMR
CNRS 6285 Équipe DECIDE, CS 83818, 29238 Brest, France
john.puentes@telecom-bretagne.eu

Abstract. Modern cities, industrial plants, cars, trucks, and vessels, among others, make extensive use of cyber-physical systems and sensors. These systems are very critical and contribute to assist decision making. Large data streams are thus produced and analyzed to extract information that allows building knowledge through a set of principles called wisdom. However, because of multiple imperfections, as well as intrinsic, contextual, and extrinsic conditions that alter data, the quality of the generated streams must be evaluated, to determine how relevant they are for decision support. This paper presents a methodology to monitor cyber-physical systems by quality estimation, which defines suitable evaluation characteristics for pertinent analysis. Quality assessment is defined for data imperfections, information dimensions, knowledge factors, and wisdom aspects. The case study of a cyber-physical network of a liquid container training platform is presented in detail, to show how the approach can be applied. Obtained measures are multidimensional, heterogeneous, and variable.

Keywords: Monitoring · Sensor data processing · Multi-source sensor network · Cyber-physical system · Data quality · Information quality

1 Introduction

Cyber-physical systems have become necessary in many realms like transport, manufacturing, home, and cities automation. These systems are composed of sub-systems, which process information and support decision making based on different data sources as sensors, control, and communication systems. Increasingly, multiple systems assist human operators to accomplish efficiently and safely their tasks. To this end, critical monitoring data and information are continuously generated. These fundamental systems are cyber-physical as they interact with the environment making sensor measurements and executing responses

using actuators. Usually, in order to perform external control and monitoring, these systems are also connected to networked stations.

Infrastructure governance is as a consequence completely based on decision-aided or automatic responses, defined by the obtained information, according to a so-called wisdom. Moreover, cyber-physical systems are being developed to improve their performance, conceive new functionalities, or simplify their use. Given the fact that a growing number of these systems are currently deployed, voluminous data streams are permanently produced.

An emerging problem created by such enlarged scale and diversity of systems is the complexity to analyze generated data, taking into account specific operational contexts. Numerous factors can alter collected data and extracted information changing the expected impact on decision support, from innocuous to catastrophic. Therefore, methodologies and models of quality estimation emerge as a possibility to determine, if collected data and extracted information are relevant for decision support.

Our work proposes to address this issue, defining a quality evaluation methodology, identifying which analysis elements are the most pertinent to provide suitable system's streams quality characterization. This evaluation is intended to support decision makers responsible for the corresponding cyber-physical systems. Therefore, if the quality of data, information, knowledge, and wisdom are evaluated with respect to a given operational objective, an adapted response is likely to be given. On the other hand, quality evaluation has several implications. For example, it can be used to discover potential evidence of suspicious anomalies to be further examined by cyber-security tools. It can also permit to identify malfunctions in information systems, or sources that after a qualification, can be trusted and integrated for decision aid, in spite of such imperfections. To provide suitable analyses, quality evaluation must be carried out according to the same functional constraints of the examined system.

Data and information quality have been widely studied in other domains like Management Information Systems (MIS), Web Information Systems (WIS), and Information Fusion Systems (IFS) [11]. However, none of the developed methods can be directly and fully applied to cyber-physical systems. The main reason is that those approaches have been developed for specific data and a particular application. Moreover, the definition of data and information quality assessment is not obvious in cyber-physical streams, given the significant differences in measurement's times and test points. Few other initiatives have conceived automatic quality evaluation methods applied to particular cyber-physical systems, like sensors data for personal health records [9] and wireless sensor networks [4], adapted to very specific user needs.

The proposed contribution relies on three principles. First, quality evaluation of data, information, knowledge, and wisdom are dynamic and derived from intrinsic, contextual, and extrinsic dimensions related to each examined sub-system. Second, quality evaluation is independent of the associated functional task carried out by the sub-system components. Finally, some of the quality evaluation concepts studied by the MIS, WIS, and IFS methods are adapted to

cyber-physical systems. The rest of the paper is organized as follows. A definition of the proposed methodology is presented in Sect. 2. To illustrate how the proposed method could be applied, the case of a liquid tank prototype is studied in Sect. 3. Discussion and conclusions are presented in Sect. 4.

2   Quality of Sensor Streams

This section defines the main components of the proposed quality evaluation method. The key entities are introduced in Sect. 2.1, explaining the difference between data, information, knowledge, and wisdom quality evaluation. Subsections 2.2, 2.3, 2.4 and 2.5 are dedicated to describe separately each quality evaluation approach. In Sect. 2.6, a global quality measurement method is defined integrating the previously defined components.

2.1   Data, Information, Knowledge, and Wisdom

To avoid a well known general confusion regarding the concepts of data, information, and knowledge [14], we consider essential representation notions of the well known DIKW - Data, Information, Knowledge, and Wisdom - pyramid. Its definition can be summarized as know-nothing, know-what, know-how, and know-why, respectively [13].

Accordingly, in cyber-physical systems: data are the streams of bits with no comprehensible sense (know-nothing), including single values, multidimensional signals, and text; information is data with a semantic sense in a context (know-what); knowledge is how this information can be used in a particular case depending on wisdom (know-how); and wisdom is the set of principles, usually created by progressive learning from experiences to explain how information can be transformed into knowledge (know-why). Figure 1 illustrates how these entities interact in the context of the proposed quality evaluation methodology.

Taking into account contextual factors, data and information definitions can be adapted to cyber-physical systems applying:

$$Information = Data + Context_{sub\text{-}system} \tag{1}$$

where the context is formally defined by the corresponding sub-system and system specifications, to be represented as follows:

$$Context_{sub\text{-}system} = Sub\text{-}system_{specs} + System_{specs} \tag{2}$$

The context is defined by the sub-system specifications available in one or several data-sheets and the characteristics of the whole system. Besides, the environment is considered as a variable of the system specifications, *i.e.* where and how it is installed, besides which are its attributes (fixed or variable).

Knowledge is the result of a principle - called wisdom - applied to information. This principle can be for example a mathematical expression, a physical law, or a predefined rule. When knowledge is not fully compatible with the studied

context, it requires to be adapted to preserve coherence. In general, multiple information streams inputs are necessary to create knowledge, represented by:

$$Knowledge = Wisdom(Information) \qquad (3)$$

The proposed method defines a quality evaluation for each one of the described entities. These quality evaluations are presented in the next sections.

2.2 Data Quality

Studies on data quality have been carried out focusing on various application domains. Multiple categories of dimensions identified by data consumers were used in Total Data Quality Management (TDQM) to define what is data quality [12]. The Cost-effect Of Low Data Quality (COLDQ) examined a data quality approach according to some enterprises' needs [6]. Several quality metrics were proposed by the Data Quality Assessment (DQA) [8]. Data Quality in Cooperative Information Systems (DaQuinCIS) was introduced to assist collaborative data quality evaluation [10]. In financial information systems, the Quality Assessment on Financial Data (QAFD) studied how to improve the quality of relevant data [2]. Also, for other types of organizations and businesses, the Comprehensive methodology for Data Quality management (CDQ) searched to enhance efficiency and effectiveness by increasing data quality [1].

On the other hand, from an information processing point of view, data quality can be measured by a characterization of key imperfections as follows [7]:

- **Error** (i_{err})**:** Data are erroneous when values are different from the true data.
- **Incomplete** (i_{inc})**:** Data are not totally supplied.
- **Imprecision** (i_{imp})**:** Data denote a set of possible values and the real value is one of the elements of this set.
- **Uncertainty** (i_{unc})**:** Data cannot be stated with absolute confidence.
- **Unavailable** (i_{una})**:** The system cannot obtain a value because of its limitations or due to missing measurements.

Erroneous data affect the integrity of the system and it should be discarded when detected. As a result, all information obtained from wrong data is also erroneous and its quality evaluation has no sense. Data affected by the other four imperfections preserve its integrity and can still supply valid information.

In some cases, observations should complete identified imperfections to ameliorate quality estimation. For example, data are frequently supplied with correction codes. Corrected data are not imperfect, although corrections may have an impact on quality, depending on the context. Similarly, unavailable data can also be detected when needed environment properties are provided (a condition to point out whenever possible).

2.3   Information Quality

Related specialized studies on information quality are less diverse than those on data quality. For example: the information quality evaluation proposed by the Total Information Quality Management (TIQM) searched to improve business data warehousing and raise benefits [3]; and a methodology for Information Quality Assessment (AIMQ) evaluated and benchmarked information quality [5]. It is nevertheless important to note that studies cited in the previous section, also handle partially the corresponding questions about information quality. Yet, none of them is directly applicable to cyber-physical systems in general.

To specify our information quality evaluation approach, two considerations are underlined. Instead of placing humans as just data consumers and despite the existence of a wide range of automatic processes, cyber-physical networks relate to humans as decision-makers. Besides, given that any information can be part of different tasks, quality evaluation should be task-independent. For this reason, several parameters are necessary to define tasks' quality requirements.

In the absence of a global consensus on basic methodological elements to measure information quality, we concentrate on the most known approaches to define an adapted method for cyber-physical systems. The proposed method consists of customized components of the previously cited TDQM, COLDQ, DQA, DaQuinCIS, QAFD, CDQ, TIQM, and AIMQ approaches. Note that in these works quality dimensions were structured in four groups: intrinsic, contextual, representational, and accessibility. In our case however, the basic quality view relates to sub-systems, which are rarely affected by the representational characteristics. As a consequence, only three groups of quality dimensions are applied. Intrinsic dimensions are defined when sensors are examined separately, without connections. Contextual dimensions are assessed when it is known where the sub-system is installed and what it is measuring. Extrinsic dimensions appear when the sub-system connections are identified.

We define therefore three groups of information quality dimensions, convenient for cyber-physical sub-systems, to manage the lack of specifically designed dimensions in the literature. Namely, the **Intrinsic** category is the group of quality dimensions defined for an isolated sub-system (Table 1). The **Contextual** category includes the quality dimensions that study a sub-system as part of a full system (Table 2). The **Extrinsic** category contains the dimensions that permit to evaluate streams quality considering interconnected sub-systems (Table 3).

2.4   Knowledge Quality

The subjects of knowledge and wisdom quality for networked cyber-physical systems have not been treated in the literature. We propose therefore the corresponding definitions, factors, and aspects, required in the framework of our study. Knowledge is produced by the direct application of wisdom to information. This implies that the quality of knowledge is considerably influenced by both, information quality and wisdom quality. Moreover, in the case of cyber-physical systems some particular factors should also be taken into account:

Table 1. Intrinsic information quality dimensions in cyber-physical systems

ID	Name	Description
id_{sp}	Source precision	The extent to which every information under unchanged conditions show the same results due to the source acquisition
id_{acc}	Accuracy	The extent to which extracted information is close to the true information
id_{obj}	Objectivity	The extent to which information is unbiased, unprejudiced, and impartial
id_{rep}	Reputation	The extent to which information is highly regarded in terms of its source or content
id_{obs}	Obsolescence	The extent to which information is valid through time
id_{fre}	Freshness	The extent to which information is new
id_{tru}	Trust	The extent to which information is trustworthy
id_{acq}	Acquisition cost	The cost to acquire the information
id_{rea}	Readable	The extent to which data used to obtain information are noiseless and intelligible
id_{res}	Resolution	The extent to which data used to obtain information are distanced in sampling
id_{itg}	Integrity	The extent to which information is complete and the provider sub-system is fully available
id_{cns}	Consistency	The extent to which information is presented in the same format
id_{uni}	Uniqueness	The extent to which information is not repeated

Table 2. Contextual information quality dimensions in cyber-physical systems

ID	Name	Description
cd_{rp}	Real precision	The extent to which every information under unchanged conditions shows the same results due to the use of the sub-system
cd_{cla}	Clarity	The extent to which information is comprehensible through other information
cd_{val}	Value-added	The extent to which information is beneficial and provides advantages from its use
cd_{tim}	Timeliness	The extent to which information is expected by the system
cd_{cmt}	Completeness	The extent to which information is know in a complete context
cd_{cnc}	Concision	The extent to which information is compactly represented
cd_{vol}	Volume	The extent to which the volume of information is appropriate for the task at hand
cd_{bel}	Believability	The extent to which information is regarded as true and credible

Table 3. Extrinsic information quality dimensions in cyber-physical systems

ID	Name	Description
ed_{acc}	Accessibility	The extent to which information is available, easily, and quickly retrievable
ed_{sec}	Security	The extent to which access to information is restricted appropriately to maintain its security
ed_{eu}	Ease of utilization	The extent to which information is easy to use and apply to different tasks
ed_{man}	Manipulation	The extent to which an information link is easy to manipulate
ed_{int}	Interpretability	The extent to which information is in appropriate languages, symbols, and units, and the definitions are clear
ed_{cmp}	Compatibility	The extent to which information is comprehensible for different sub-systems
ed_{for}	Format	The extent to which information respects a specific format
ed_{und}	Understandability	The extent to which information is easily comprehended
cd_{red}	Redundancy	The extent to which other sub-systems provide the same information
ed_{coh}	Coherence	The extent to which information is logical with respect to other information

- **Completeness (f_{com}):** The extent to which information sources needed by wisdom are available.
- **Error cost (f_{err}):** The potential cost produced by erroneous knowledge.
- **Relevancy (f_{rel}):** The extent to which knowledge is applicable and helpful for the task at hand.

2.5   Wisdom Quality

Depending on the type of wisdom - mathematical principle, physical law or predefined rule (based on experience) - as well as the related source, attributes, and pertinence, among others, the confidence on wisdom changes. Hence, to evaluate wisdom quality six aspects should be examined:

- **Experience (a_{exp}):** The extent to which wisdom is verified through a defined knowledge put in practice.
- **Confidence (a_{con}):** The extent to which wisdom is highly regarded in terms of its source or content.
- **Accessibility (a_{acc}):** The extent to which wisdom is available, easily retrievable, and modifiable.

- **Interpretability** (a_{int})**:** The extent to which wisdom is clearly defined in appropriate languages, symbols, and units.
- **Security** (a_{sec})**:** The extent to which access to wisdom is restricted appropriately to maintain its security.
- **Completeness** (a_{com})**:** The extent to which wisdom takes into account the variables that influence it.

2.6   Quality Assessment

The proposed quality evaluation methodology (Fig. 1) regulates the transformation of data streams into information and knowledge, depending on the measured quality of each entity. Quality evaluations of DIKW are individual, in order to handle appropriately a large scope of qualification conditions. For instance, a data-set containing several different information elements, which depending on the availability of multiple wisdom principles, can potentially generate various knowledge streams. Therefore, the separate quality evaluation of each particular DIKW sequence contains four unique vectors, specifically: **DQV** (Data Quality Vector), **IQV** (Information Quality Vector), **KQV** (Knowledge Quality Vector), and **WQV** (Wisdom Quality Vector), encompassing previously defined properties related to imperfections, dimensions, factors, and aspects, respectively. Since the evaluation of these properties is rarely exhaustive because of variable unavailability of one or several elements, the proposed method intends to define a complete quality evaluation framework that can be applied according to changing practical conditions.
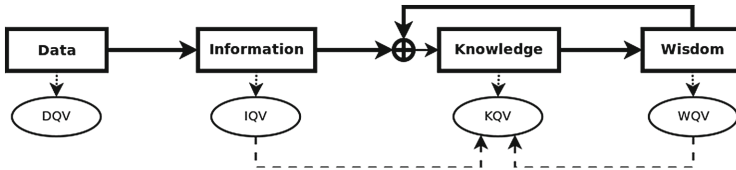

Fig. 1. Entities interactions in the proposed evaluation method.

Depending on the evaluated sub-system, units of quality vectors are likely to vary, depending on the reference system of measurement and the declared attributes' types (Boolean, string, char, word from a dictionary, integer, real, etc.). This fact makes necessary to represent separately the imperfections, dimensions, factors, and aspects, in the evaluation vectors. For instance, to evaluate the quality of a sub-system on which a data stream with K data imperfections (I_i), produces information requiring to examine L dimensions (D_i), leads to the definition of the following **DQV** and **IQV** vectors:

$$\mathbf{DQV} \in \{I_1...I_K\} \tag{4}$$

$$\mathbf{IQV} \in \{D_1...D_L\} \tag{5}$$

By definition, knowledge quality is related to information quality (**IQV**) and wisdom quality (**WQV**). Hence, for a knowledge stream created with M information streams and assessed with N factors (F_i) and **KQV** is defined as:

$$\mathbf{KQV} \in \{IQV_1...IQV_M, WQV, F_1...F_N\} \tag{6}$$

Similarly, wisdom quality formed by P aspects (A_i) defines the following **WQV** vector:

$$\mathbf{WQV} \in \{A_1...A_P\} \tag{7}$$

Additionally, specific constraints identified on the system components should be applied to evaluate quality. These constraints include limitations of the analyzed sub-system, restrictions inherited from other connected sub-systems, or derived from the main system. Whenever different constraints are identified for a given dimension characteristic, quality evaluation is carried out assuming that the sub-system should respect the most restrictive ones (usually related to the need for responses in real time and computational limitations).

3   Simple Case Study

To test the proposed quality evaluation approach we use a cyber-physical platform representing a liquid container subsystem. Such platform commonly used for training on networked control infrastructure, can be found at different scales in cities, homes, industrial plants, or vehicles, to contain liquids like water or fuel. It is composed by two tanks (cisterns): a main tank (Cistern B) and a secondary tank (Cistern A). While the secondary tank fills the main tank using Pump 2, the main tank (smaller than the secondary) provides the liquid to the system. Consumption is simulated by a valve placed at the bottom. To simulate when the main tank is filled, the secondary tank can transfer the liquid contained in the recovery tank by means of Pump 1.

This platform is controlled by a Schneider programmable logic controller (PLC), accessible from a touch screen and through Modbus[1] network commands. Two types of sensors generate data: four discrete sensors (in Cistern A) and one ultrasonic sensor (in Cistern B). Discrete sensors are switches activated when the liquid makes them float. The level of liquid present on the main tank is measured by the ultrasonic sounder. All these components are connected in a local network, which can be linked to remotely monitor and control the whole system. The network schema is shown in Fig. 2, including transmitted information and used protocol for the main connections.

Analysis of system performance is done at a control and monitoring machine connected to the platform network. The system receives **data**, a binary sequence used by communication protocols that is not directly comprehensible.

---

[1] Modbus is an open OSI level 7 protocol developed by Scheinder Electric in 1979 and largely used in SCADA (Supervisory Control and Data Acquisition) systems (http://modbus.org/docs/PI_MBUS_300.pdf).
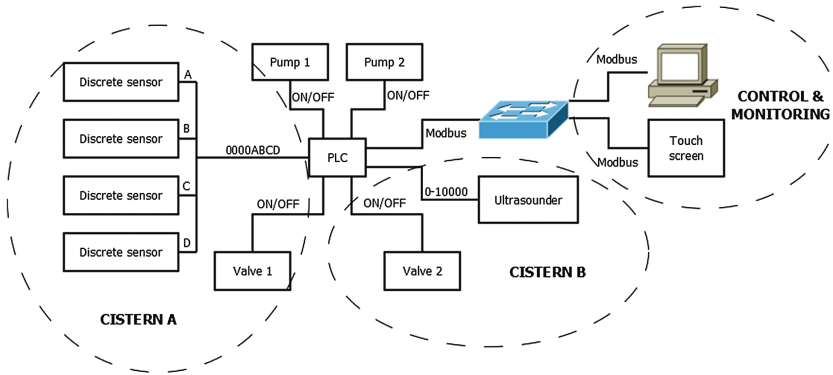
Fig. 2. Training platform network.

This sequence initializes the quality evaluation process. **Information** is defined when a protocol decodes the data and the context gives a meaning to values, making use of the sensors' data specifications and tank size. The resulting information is the measured level of liquid, represented by a comprehensible value (*e.g.* 30 L of liquid). To obtain this information a measure of distance obtained by the ultrasonic sensor is transformed to a measure of volume, according to the tank dimensions. Furthermore, knowing the liquid consumption of the system, its autonomy can also be determined defining related **knowledge** (*e.g.* 20 min). This principle is associated to **wisdom**, specifically the consumption per hour, *i.e.* a vehicle fuel consumption as a function of speed, distance, or type of engine. Once wisdom is defined (*e.g.* 1.5 L/min), knowledge about the autonomy of the system can be calculated. Wisdom will be updated and improved depending on experience, or modified if it does not agree with expected values.

In Table 4, an example of quality evaluation on four contexts, applying the proposed model, is shown. Only the most representative quality elements are indicated to evaluate DQV and IQV. Data quality measures include: Erroneous data marked as true when the CRC (code of cyclic redundancy) provided by the stream cannot be verified; incompleteness detects lost messages using the ID sequence and indicates how many packages are lost. At the information quality level measures take into account: Source precision calculated with the parameters indicated on the data-sheet of the sensor; integrity as the percentage of the sub-system that works properly; uniqueness as a Boolean that indicates if the information is unique for an instant of time; real precision identified as the noise filtered from the signal; timeliness as the difference between the expected and the real time of arrival of the information; format as a Boolean that evaluates if the format is valid; and coherence as the difference between a theoretical behavior of the system calculated knowing the state of pumps and the observed one.

Table 4. Quality evaluation for ultra-sounder

Anomaly	DQV $\{i_{err}, i_{inc}\}$	IQV		
		Intrinsic $\{id_{sp}, id_{itg}, id_{uni}\}$	Contextual $\{cd_{rp}, cd_{tim}\}$	Extrinsic $\{ed_{for}, ed_{coh}\}$
Normal	{false, 0}	{4, 100, true}	{5, 2}	{true, 2}
Foreign objects	{false, 0}	{3, 100, true}	{35, 1}	{true, 2}
DoS attack	{false, 11}	{3, 100, true}	{3, 120}	{true, 5}
Leak	{false, 0}	{1, 100, true}	{15, 0}	{true, 1/35}

An example of a normal behavior is described in the first row: $DQV = \{i_{err} = \text{false}, i_{inc} = 0 \text{ messages}\}$; $IQV = \{\text{intrinsic } \{id_{sp} = 4 \text{ u.}, id_{itg} = 100\%, id_{uni} = \text{true}\}$, contextual $\{cd_{rp} = 5 \text{ u.}, cd_{tim} = 2 \text{ ms}\}$, extrinsic $\{ed_{for} = \text{true}, ed_{coh} = 2 \text{ u.}\}\}$, where 'u.' are the units used by the system, that is, 1 of the 10000 uniformed steps of a full tank. Examples of three different anomalies that deteriorate some dimensions of quality are analyzed in the next three rows. When foreign objects are floating on the liquid, measure precision worsens significantly, *e.g.* contextual $IQV = \{cd_{rp} = 35 \text{ u.}\}$. A DoS (Denial-of-Service) network attack produces the lost of network packages, affecting data incompleteness and increasing information timeliness, *e.g.* $DQV = \{i_{inc} = 11 \text{ messages}\}$ and $IQV = \{cd_{tim} = 120 \text{ ms}\}$. Finally, when a leak is produced the measure of coherence decreases, *e.g.* $IQV = \{cd_{coh} = 1/35 \text{ u.}^{-1}\}$.

Knowledge quality can be defined making use of - $\{f_{err}, f_{rel}\}$ - as: $KQV = \{2, 2\}$, $KQV = \{4, 4\}$, $KQV = \{3, 3\}$, and $KQV = \{3, 3\}$, for the indicated cases respectively, adding relevant factors to previously obtained IQV, as defined in Eq. (6). Completeness is not considered in this case because knowledge is created from a unique source. Defined levels - from 1 to 5 - based on the tank capacity, represent error cost and relevancy. In this particular case, errors' cost make knowledge more relevant and directly related. On the other hand, WQV is static when the system is functioning *e.g.* $WQV = \{a_{exp}, a_{com}\} = \{38, 1\}$ - *i.e.* based on 38 previous cases, only considering the liquid level. Potential costs of wrong decisions resulting from ignoring quality evaluations could be, for instance: blocked pipes if foreign objects are not removed; significant amount of missing values that are not updated if the DoS attack is not detected; and wrong system autonomy previsions if a leak is not fixed.

4   Discussion and Conclusion

Quality evaluation in cyber-physical systems appears as an alternative to monitor systems' operations and adjust if necessary the behavior of sub-systems, as well as to reduce potential risks and costs resulting from wrong decisions. We have proposed a methodology to completely evaluate data, information, knowledge, and wisdom quality. Following an analysis of existing quality measurements in other domains, the proposed approach identifies the most suitable elements

of quality evaluation for cyber-physical systems. Defined knowledge factors and wisdom aspects for quality measurement, not previously conceptualized in the literature, enhance the evaluation to take into account complementary quality evaluation elements. All imperfections, dimensions, factors, and aspects, do not need to be systematically examined to evaluate the quality of a networked cyber-system. Since each element can be separately qualified, dynamic quality evaluations are applied according to the available elements in a given context.

A schematic simplified application of the proposed approach was presented, taking the case study of a cyber-physical system sensor network. It illustrates how the defined quality evaluation components are analyzed. Despite the apparent simplicity of this experiment, obtained results reveal the complexity of evaluating the complete system quality from data to wisdom, at normal and three different possible functioning stages. Resulting measures are multidimensional, heterogeneous, and variable. We also observe the need to encode considerable prior knowledge to facilitate system quality assessment. On the other hand, the interest of global quality measures to monitor cyber-physical systems remains unknown. It is unclear what a single qualification obtained from multiple heterogeneous elements could mean to a decision maker. Further work will consist on extending the proposed approach to other cyber-systems in operational conditions.

References

1. Batini, C., Scannapieco, M.: Data Quality: Concepts, Methodologies and Techniques. Data-Centric Systems and Applications. Springer, New York (2006)
2. De Amicis, B.: A methodology for data quality assessment on financial data. Stud. Commun. Sci. **4**, 115–136 (2004)
3. English, L.P.: Improving Data Warehouse and Business Information Quality: Methods for Reducing Costs and Increasing Profits. Wiley, New York (1999)
4. Guo, J., Liu, F.: Automatic data quality control of observations in wireless sensor network. IEEE Geosci. Remote Sens. Lett. **12**(4), 716–720 (2015)
5. Lee, Y.W., Strong, D.M., Kahn, B.K., Wang, R.Y.: AIMQ: a methodology for information quality assessment. Inf. Manag. **40**(2), 133–146 (2002)
6. Loshin, D.: Enterprise Knowledge Management. The Data Quality Approach. Academic Press, San Diego (2001)
7. Motro, A., Smets, P.: Uncertainty Management in Information Systems: From Needs to Solutions. Springer Science & Business Media, New York (1996)
8. Pipino, L.L., Lee, Y.W., Wang, R.Y.: Data quality assessment. Commun. ACM **45**(4), 211–218 (2002)
9. Puentes, J., Montagner, J., Lecornu, L., Lähteenmäki, J.: Quality analysis of sensors data for personal health records on mobile devices. In: Bali, R., Troshani, I., Goldberg, S., Wickramasinghe, N. (eds.) Pervasive Health Knowledge Management. Healthcare Delivery in the Information Age, pp. 103–133. Springer, New York (2013)
10. Scannapieco, M., Virgillito, A., Marchetti, C., Mecella, M., Baldoni, R.: The DaQuinCIS architecture: a platform for exchanging and improving data quality in cooperative information systems. Inf. Syst. **29**(7), 551–582 (2004)

11. Todoran, I.-G., Lecornu, L., Khenchaf, A., Le Caillec, J.-M.: Information quality evaluation in fusion systems. In: 16th International Conference on Information Fusion (FUSION), pp. 906–913, July 2013
12. Wang, R.Y., Strong, D.M.: Beyond accuracy: what data quality means to data consumers. J. Manag. Inf. Syst. **12**(4), 5–33 (1996)
13. Zeleny, M.: Human Systems Management: Integrating Knowledge, Management and Systems. World Scientific Publishing Co., Pte. Ltd., London (2005)
14. Zins, C.: Conceptual approaches for defining data, information, and knowledge. J. Am. Soc. Inform. Sci. Technol. **58**(4), 479–493 (2007)