Dependability and Emerging Technologies
~ draft version 2.1 2020-11~

1. General

As a result of propagation of Information Technology (IT), the world is experiencing a new series of disruptive emerging technologies such as cyber-physical systems (CPS), the Internet of Things (IoT), artificial intelligence (AI), enhanced connectivity driven by 5G, edge computing and intelligence and big data. Correlated with these technologies, modern society needs to drive huge and complex systems, which are often beyond control. While dependability in traditional sense keeps its significance in these emerging technologies, such huge and complex systems are revealing a need for new aspects of dependability.

The purpose of this document is twofold. One is to inform the experts in those emerging technologies of the availability of the IEC series of dependability standards, in order to avoid duplication of effort in each field developing similar standards concerning dependability. Another is to assemble cases for the use of the dependability community to address the socio-technical issues, which are being raised with respect to trustworthiness.

This document is organized as follows.

- **Clause 2** sketches engineering circumstances surrounding dependability.
- An overview of the IEC dependability standards is given in **clause 3**. When a dependability issue arises in some specific engineering field, it would be worthwhile to look at this well-thought-out body of documents. The crucial role of dependability and similar attributes such as trustworthiness is being rediscovered in several emerging engineering areas because issues of reliability, integrity, safety, security and functionality arise everywhere. In the past few decades, IEC has developed a series of dependability standards to enable successful practice in these technologies.
- On the other hand, the emerging technologies have brought about issues which reveal needs for new aspects of dependability. Socio-technological issues such as accountability and interaction with laws and regulation tended to be considered as ethics issues and completely out of scope of technical standards on dependability. Because of recent rise of AI, for instance, a mediator is desired between those ethical requirements and engineering requirements in traditional sense. This topic, as well as how the IEC series of dependability standard is taking a step forward, is addressed in **clause 4**.

2. Background

2.1. Industry and Manufacturing

Business is experiencing a digital transformation of industrial markets with smart manufacturing currently on the forefront. Efforts such as Industry 4.0 represent a revolutionary change in discrete and process manufacturing, logistics and supply chain (Logistics 4.0). These impact industry sectors such as the chemical industry, energy (Energy 4.0), transportation, utilities, oil and gas, mining and metals and other segments, including resources industries, healthcare, pharmaceutical industry and even smart cities.

2.2. Consumers

A major impact for consumers has been the increased speed and availability of the internet, which enables the interconnection of, and remote access to, IoT devices with built-in intelligence that can collect massive amounts of data for further analysis. The largest application of IoT is in smart homes and consumer electronics but even the advent of autonomous transportation will herald fundamental shifts in society.

2.3. IoT

The use of IoT devices is already becoming widespread although they and the business models they are built on are still quite immature. The IEC White Paper [1] provides an outlook on what the current issue in IoT – the development of smart and secure IoT platforms – could involve. As currently defined by ISO/IEC, the Internet of Things (IoT) is “an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react [2].”

The current state of IoT is that it is a mixture of new and legacy devices built on different platforms that hinder interoperability and are often unsuitable for today’s challenges. Key issues for consistent and secure application of IoT are security, safety, integrability, interoperability, composability, data management, analytics and resiliency.

2.4. Artificial Intelligence

AI has many potential benefits but also significant risks and threats to safety, security and operational effectiveness. Enablers of AI are increased computational power, availability of data and improved algorithms while its drivers include cloud computing, edge computing, IoT, big data and consumer acceptance [3].

AI owes much of its recent revival to machine learning, which can be supervised, unsupervised or reinforced learning. Machine learning is embedded in computer vision, anomaly detection, time series analysis, natural language processing and recommender systems while new applications are already underway.

Standardization gaps include harmonized data models and semantics, a common ontology based on data models, verification of artificial intelligence algorithms and benchmarking and evaluation of artificial intelligence infrastructures.

2.5. Edge Intelligence

A new model for computing is evolving which involves extending data processing to the edge of a network in addition to computing in a cloud or a central data centre [4]. Edge-cloud computing models operate both on premise and in public and private clouds, including via devices, base stations, edge servers, micro data centres and networks. It consists of machine learning (ML) and advanced networking capabilities.

3. The IEC series of Dependability Standards

Dependability plays a crucial role in the successful practice of these interrelated technologies. It is supported by standards produced and maintained by IEC/TC 56 Dependability (iec.ch).

IEC/

Key aspects of dependability that contribute to the success of emerging technologies are:

1. **Reliability**. Dependability takes a comprehensive approach to the critical requirement of reliability for IoT devices, computing capabilities including the application of edge computing

and AI, data integrity and interconnectivity between edge devices and the cloud. Dependability is intended to ensure that the entire interconnected system performs as required with respect to reliability [5], maintainability [6], supportability [7] and resultant availability [8].

2. **Risk**. Assessing threats and risks with respect to use of these emerging technologies and their application is supported by an ISO standard on risk management ISO 31000 [9] and a follow-up IEC standard on risk assessment IEC 31010 [10], which references eight more IEC/TC 56 standards.
3. **Safety**. Dependability contributes to safety by assessing risks [10] and enhancing reliability through a number of design analysis standards, including failure modes and effects analysis [11], fault tree analysis [12], Markov analysis [13] and HAZOP studies [14].
4. **System approach**. There are many IEC/TC 56 standards that address the dependability of simpler components, but it also deals with the dependability of systems [15] systems-of-systems, networks [16] and open systems [17]. In particular, open systems (systems that evolve with changing environments) need special consideration to ensure dependability. Reliability testing, especially to ensure components and sub-systems (such as IoT devices) will function properly and safely, is a special focus for IEC/TC 56 standards [18] (and others).
5. **Management and life cycle approach**. It is important to manage dependability [19] and project risk [20] over the life cycle [21]. A critical step is the specification of dependability requirements [22], communication network assessment and assurance [23], and establishing a dependability case for assurance [24]. Four process views are provided by [17] on top of the set of system life cycle processes given by [28].
6. **Obsolescence**. With production and utilization times becoming even shorter with the rapid advancement of technology, managing obsolescence over the entire life cycle is even more crucial [25].
7. **Data and software**. The large amounts of data being produced by these new technologies with software and computing capabilities both at the edge by IoT devices and in the cloud provide new challenges for managing and analyzing data [26] and designing secure software [27].

4. New aspect of dependability — trustworthiness and IEC approach

Recent breakthroughs in AI have prompted several International organizations including OECD, UNESCO COMEST to publish recommendations on the trustworthiness and ethics of AI technology. The concept of trustworthiness seems to have a large overlap with dependability.

These recommendations, because of the nature of these bodies, tend to be stated in the language of the humanities, but they should be implemented technically in the form of, e.g., SC 42 standards. There seems to be a need for a bridge between these two kinds of documents. One of the roles of TC 56 may be to provide such a bridge. There is, for instance, some guidance on consensus building from ethical viewpoint by using the term “fair and equitable manner” [17].

The following subclauses give an overview of trustworthiness as discussed in these recommendations and technical reports, and compare them with IEC dependability standards.

4.1. Trustworthiness in ISO/IEC JTC 1/SC 42 Artificial Intelligence

ISO/IEC JTC 1/SC 42 *Artificial Intelligence* defines trustworthiness in [29] as

> ability to meet stakeholders’ expectations in a verifiable way

Note 1 to entry: Depending on the context or sector, and also on the specific product or service, data, and technology used, different characteristics apply and need verification to ensure stakeholders expectations are met.

Note 2 to entry: Characteristics of trustworthiness include, for instance, reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality, usability.

Note 3 to entry: Trustworthiness is an attribute that can be applied to services, products, technology, data and information as well as, in the context of governance, to organizations.

Compared to TC 56 definition of "dependability", this definition contains "stakeholders". Moreover, the idea of verification comes in here. "To meet stakeholders' expectation" sounds more comprehensive than "to perform as and when required". Reliability and availability, which are considered as core attributes of dependability, appears in the note to the definition. This seems to indicate the similarity of the two concepts.

4.2. Trustworthy AI in EU

EU guideline [30] enumerates three components of "trustworthy AI":

1. it should be **lawful**, ensuring compliance with all applicable laws and regulations
2. it should be **ethical**, demonstrating respect for, and ensure adherence to, ethical principles and values and
3. it should be **robust**, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm.
   Trustworthy AI concerns not only the trustworthiness of the AI system itself but also comprises the trustworthiness of all processes and actors that are part of the system's life cycle.

Dependability in the traditional sense largely corresponds to robustness issues. The Accountability Achievement process view in [17] gives an aspect of the ethical principles as well as consideration to laws and regulations. This shows a recent trend of dependability standard development towards provision of bridge between ethics and engineering.

4.3. Trustworthy AI in OECD

The recommendation [31] identifies five complementary values-based principles for the responsible stewardship of trustworthy AI and calls on AI actors to promote and implement them:

- inclusive growth, sustainable development and well-being;
- human-centred values and fairness;
- transparency and explainability;
- robustness, security and safety; and
- accountability.

"Robustness" here seems close to dependability.

The Consensus Building process view and Accountability Achievement process view provided by [17] address the concern of "human-centered values and fairness" and "transparency and explainability". The former requires fairness and mindfulness, and the latter requires readiness for accountability.

4.4. Ethics of AI in UNESCO COMEST

The study report on ethics in AI [32] suggests twelve generic principles for the development, implementation and use of AI: (1) human rights (2) inclusiveness (3) flourishing (4) autonomy (5) explainability (6) transparency (7) awareness and literacy (8) responsibility (9) accountability (10) democracy (11) good governance (12) sustainability. This document is prepared as a preliminary document; a full-scale document “Recommendation on the Ethics of AI” is planned by UNESCO COMEST.

Accountability Achievement process view provided by [17] seems to be relevant to accountability, explainability and responsibility.

5. References

[1] IEC White Paper, *IoT 2020: Smart and secure IoT platform*, https://www.iec.ch/whitepaper/, 2016.
[2] ISO/IEC JTC 1, *Internet of Things (IoT)*, Geneva, 2014.
[3] IEC White Paper, *Artificial intelligence across industries*, https://www.iec.ch/whitepaper/, 2018.
[4] IEC White Paper, *Edge intelligence*, https://www.iec.ch/whitepaper/, 2017.
[5] IEC 60300-3-1, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*.
[6] IEC 60300-3-10, *Dependability management – Part 3-10: Application guide – Maintainability*.
[7] IEC 60300-3-14, *Dependability management – Part 3-14: Application guide – Maintenance and maintenance support*.
[8] IEC 60300-3-17, *Dependability management – Part 3-14: Application guide – Availability* (currently under development).
[9] ISO 31000, *Risk Management – Guidelines*.
[10] IEC 31010, *Risk management – Risk assessment techniques*.
[11] IEC 60812, *Failure modes and effects analysis (FMEA and FMECA)*.
[12] IEC 61025, *Fault tree analysis (FTA)*.
[13] IEC 61165, *Application of Markov techniques*.
[14] IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*.
[15] IEC 60300-3-15, *Dependability management – Part 3-15: Application guide – Engineering of system dependability*.
[16] IEC 61907, *Communication network dependability engineering*.
[17] IEC 62853, *Open systems dependability*.
[18] IEC 60300-3-5, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*.
[19] IEC 60300-1, *Dependability management – Part 1: Guidance for management and application*.
[20] IEC 62198, *Managing risk in projects – Application guidelines*.
[21] IEC 60300-3-3, *Dependability management – Part 3: Application guide – Section 3: Life cycle costing*.
[22] IEC 60300-3-4, *Dependability management – Part 3-4: Application guide – Guide to the specification of dependability requirements*.
[23] IEC 62673, *Methodology for communication network dependability assessment and assurance*.
[24] IEC 62741, *Demonstration of dependability requirements – The dependability case*.
[25] IEC 62402, *Obsolescence management – Application guide*.
[26] IEC 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*.
[27] IEC 62628, *Guidance on software aspects of dependability*.

[28] ISO/IEC/IEEE 15288, *System life cycle processes*.
[29] ISO/IEC TR 24028, *Overview of trustworthiness in artificial intelligence*
[30] The High-Level Expert Group on Artificial Intelligence in EU, Ethics guidelines for trustworthy AI
https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
[31] OECD, *Recommendation of the Council on Artificial Intelligence*
https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
[32] UNESCO COMEST, *Preliminary study on the ethics of artificial intelligence*
https://unesdoc.unesco.org/ark:/48223/pf0000367823
http://www.unesco.org/new/en/social-and-human-sciences/themes/comest/