International Electrotechnical Commission

IEC Technical Committee No 56: Dependability

Dependability and Emerging Technologies

General

The world is experiencing a new series of disruptive emerging technologies. The main components of this technology revolution are cyber-physical systems (CPS), the Internet of Things (IoT), artificial intelligence (AI), enhanced connectivity driven by 5G, edge computing and intelligence and big data.

This is evidenced both in manufacturing initiatives such as Industry (or Industrie) 4.0 that many are characterizing as a 4th industrial revolution as well as consumer-related developments such as smart homes, enhanced monitoring with predictive maintenance and health care.

In this rapidly changing environment, dependability is taking on an even more crucial role that impacts critical areas such as functionality, safety, security and reliability. Among others, IEC is taking a proactive approach to standardization and conformity assessment to enable successful implementation of these technologies. In addition to the substantial benefits that this revolution will have, there are new challenges related to the vulnerabilities inherent in technologies such as IoT that require special and innovative solutions.

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 revolution 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, pharma and even smart cities.

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.

IoT

The use of IoT devices is already becoming widespread although they and the business models they are built on are still quite immature. An IEC White Paper [1] provides an outlook on what the next big step 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.

Artificial Intelligence

AI is another disruptive technology that 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 drivers of artificial intelligence, cloud and edge computing, IoT, big data and consumer acceptance [3].

AI is most closely associated with machine learning, which can be supervised, unsupervised or reinforced learning. Current machine learning systems are 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.

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.

The Role of Dependability

Dependability will play an important role in the successful implementation of these interrelated technologies. It is supported by standards produced and maintained by IEC/TC 56 Dependability (iec.ch). Key aspects in which dependability contributes 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 (where an open system is one that is only loosely connected to other systems) are vulnerable from a security perspective so 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].
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].

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*.