Developments in Dependability Standardization

Thomas Van Hardeveld, M.Sc., P.Eng.
Chair, IEC/TC56 Dependability
Strategic Maintenance Solutions Inc.
Calgary, Alberta, Canada

***Abstract* — This presentation outlines recent developments in standardization of dependability. A major focus for dependability standards relates to the role of large interconnected systems or open systems in today's increasingly integrated global society. This produces challenges to current practices in the field of dependability. These are being addressed in initiatives in TC56 such as a new standard on open systems, the concurrent revision of a number of core dependability standards and increased emphasis on stakeholders, more efficient standards development and communications.**

Keywords—dependability, asset management, risk management, availability, reliability, maintainability, supportability, open systems, IEC standardization

I. Introduction

Dependability is facing new challenges as society and the technology that enables its increasingly rapid progress evolves into new directions. In many ways, this is no different than changes that have occurred in the past but the need to adapt to the major issues that face us are becoming more and more critical to our survival and that of the planet we inhabit.

Dependability concepts are critical for modern trends in an increasingly integrated world that is more and more dependent on interconnected technologies such as the Internet of Things and many areas of infrastructure such as energy, electrical power and transportation [2]. Dependability also promotes clean energy technology applications which encourage energy conservation, include information technology, embrace design principles to reduce, recycle and reuse, advocate the interoperability of system components to achieve simplicity in designs, adopt reusability and utilize applicable commercial-off-the-shelf (COTS) products. In addition to proven dependability tools and techniques, TC 56 is now challenged to provide new or improved methods to deal with the high reliability demands that society now expects.

Today TC 56 covers areas from components to complex systems, networks and open systems and from management aspects to manufacturing. From being mainly focused on Test Analysis and Fix (TAAF), TC 56 now also works with standards covering dependability aspects of product development, design integration, maintenance, risk assessment and obsolescence. There is an increased focus on physical asset management practices where TC 56 standards provide a significant component of how they are implemented.

II. What Is Dependability

A. Definition of Dependability

Dependability is a technical discipline and is managed through life cycle processes involving time-related attributes of availability and its contributing performance attributes of reliability, maintainability and supportability, as well as application specific performance attributes such as recoverability, survivability, integrity and security for products and service dependability evaluation.

The current definition of dependability is the "ability to perform as and when required" with a number of notes that can be found in the IEC Electropedia IEV 192, which also contains many other related definitions.

The following figure tries to illustrate the components of the definition. As mentioned in one of the notes, "Dependability is used as a collective term for the time-related quality characteristics of an item" where time is a general term that also includes measures such as number of cycles, demands, etc. In other words, dependability is concerned with how requirements are able to be achieved over time during all phases of the life cycle. In this definition, the focus is on how Dependability applies to an item, a general term for a hierarchy of hardware and software with human aspects from the simplest component to systems and networks or systems of systems, including open systems.

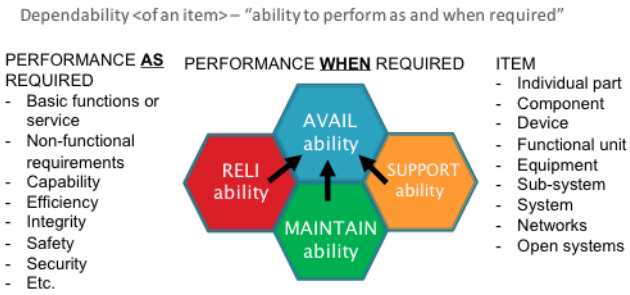

Fig. 1. An interpretation of the definition of dependability

B. The Field of Dependability

Dependability is also used as a collective or umbrella term to describe the framework that is centered on the four major attributes, but also includes management, processes, techniques, risk, etc. The "field of dependability" is used in IEV 192 as the all-encompassing reference to the suite of definitions. In industry, the equivalent term often used is "reliability engineering" or the "big R Reliability." The equivalent term for TC56 is "dependability engineering". In the academic

environment, dependability (or reliability) is seen as a discipline mostly tied to engineering but also information technology or software. On the other hand, management sees it from a business perspective as assurance of asset performance or a service and financial aspects. Users on the other hand relate to the performance or service results that impact them.

Seen in this wider context, dependability can be described as shown in the following figure where the major attributes are surrounded by a cloud of related topics.

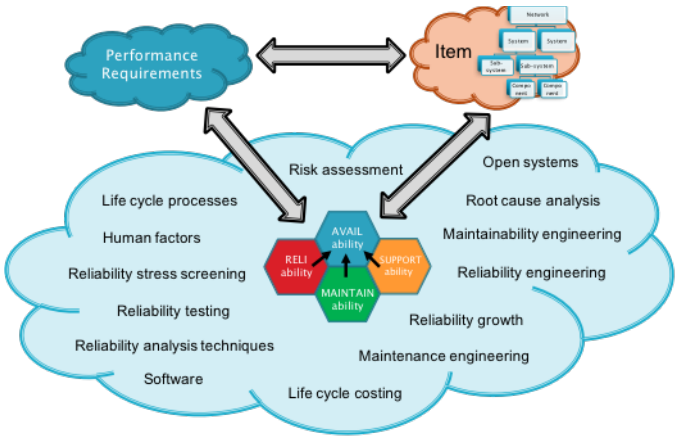

Fig. 2. The field of dependability

C. *Dependability Attributes*

The core of dependability revolves around the time-related (in its broadest sense) characteristics of performance/capability/requirements (again in its broadest sense including functions and service) as they relate to hardware, software and human aspects. This time-related aspect applies to all four characteristics, availability and its contributing attributes of reliability, maintainability and supportability, where all of them have both measurement and other associated properties. (Note: see the IEC Electropedia IEV 192 for exact definitions).

Reliability is associated with the ability to perform without failure. The important measures are failure rate and MTBF but they need to be understood and expressed statistically by distributions and a level of confidence. This works for simpler items but for more complex items averages and even distributions can be very misleading, particularly in actual use when design assumptions for conditions of use and maintenance may be different. For more complex items such as systems, users see this as the ability to maintain service levels without interruption whereas, for open systems, the impact can be very broad and even catastrophic.

Maintainability is the ability to perform maintenance, either preventive maintenance before failure occurs to retain item performance, or corrective maintenance after a failure for restoration. The basic measurement is time to repair (TTR) or mean time to repair (MTTR) with differences as to whether the item is repairable or not. It has the same statistical issues as mentioned above for reliability as well as understanding the difference in application between design/testing (e.g. where maintenance support is always available and logistics are not accounted for) and the practical issues that occur in actual application when it is influenced by supportability.

Supportability deals with maintenance support and the logistics that may be involved in providing maintenance support at the location of the item. It has a number of measures associated with it. The first measure is where it intersects with reliability and maintainability as a component of downtime. Here supportability shows up either as downtime delays in obtaining maintenance support resources such as spare parts or, if maintenance support and associated logistics are perfect, the avoidance of delays that would have occurred without maintenance support and logistics planning. In addition, there are secondary measures for various components of maintenance support, such as spare parts availability, which can also be measured. Supportability inevitably leads us to including maintenance, which also has a set of measures, such as those around maintenance effectiveness and preventive maintenance optimization.

Availability is the final result of the three core attributes and is often measured by downtime. During design, it is often based on reliability and maintainability with the assumption that supportability will be perfect. i.e. no maintenance support is perfectly available and there are no logistic delays. In operation, downtime includes all three core attributes where it results from both the inherent properties of reliability and maintainability and organizational decisions around supportability. Whereas the individual characteristics can only supply their specific components of downtime, availability can provide the total picture by being able to include other parts of downtime that are needed to provide the user/owner with the final understanding of the time-related aspects of the performance/capability of their assets. There are trade-offs to be considered that can only happen when determining the final availability during design but also during utilization. Availability matters greatly since, for many applications, it is the critical component that can be combined with the relevant performance rate connected to business performance such as service levels, production, and ultimately revenue and profitability. For many stakeholders, availability is the essential link to their objectives.

Finally, dependability itself does not have an associated measure although it may be possible to develop a rating system consisting of the attributes and other related factors such as life cycle cost, which may be useful for comparison purposes.

III. Dependability Standardization

A. *Structure of TC 56 Standards*

IEC/TC 56 currently has 54 standards, one Technical Specification and one Technical Report with the current list available on the IEC.ch website. There are various ways to see how they are organized since this is a function of stakeholder needs, applicability in the life cycle, industry application and other factors. The following shows one view of the structure of TC 56 standards.

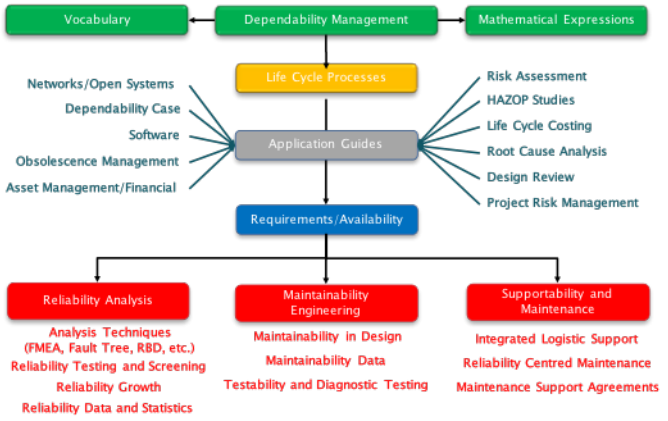

Fig. 3. A general view of the structure of TC 56 standards

B. *IEC Standards Development*

IEC has detailed procedures for standards development that are very similar to those for ISO. There is a structured approach to standards development that is clearly laid out in the ISO/IEC Directives, which are available on the IEC website. Roles and responsibilities are defined for National Committees who can act either as a participating or P member or as an observing or O member. P members appoint experts to Project Teams or Maintenance Teams coordinated by Working Groups to deliver against a prescribed schedule. The following is the basic process for standards development with a shorter process needed for Technical Specifications, Publicly Available Specifications and Technical Reports.

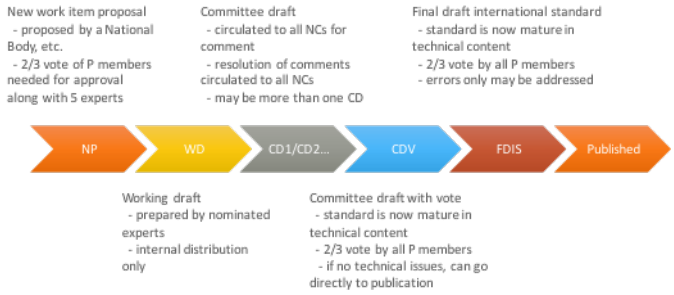

Fig. 4. IEC Process for Standards Development

IV. Dependability and Systems

A. *Classical Systems*

A system as it has been understood in the past is a set of interrelated elements which may comprise a combination of interacting hardware, software, and human elements. In the context of dependability, a system has a defined purpose expressed in terms of intended functions, stated conditions of use, and defined boundaries.

Systems may vary in their complexity structurally and functionally. A system consisting of a single function can be a product. Individual systems or products with a single function can be joined together operating in an environment as interacting systems to form a complex system.

A system is a physical and/or virtual entity. It is necessary sometimes to define a system boundary so that it can be distinguished or separated from other systems. A system interacts with its surroundings or environment to fulfil a specific need or purpose, or to achieve a defined objective. This is accomplished through the interaction of elements representing the required functions designed to meet the intended objective. Determining the required functions designed to meet a specific objective represents the process of developing a system specification. Detailed system design begins only after the functions have been identified.

B. *Open Systems*

Some systems are mainly independent entities with no or limited interaction with other systems. In other cases, well controlled networks have evolved that can achieve dependable functional and service-based requirements due to rigorously and tightly controlled interfaces and configuration. The more recent trend, however, has been a recognition that many systems are not rigorously integrated and have instead to be seen as open systems. This introduces many more unknowns around dependability that have not existed in the past. This impacts hardware dependability but is especially important for information technology and software. Open system dependability focuses on four life cycle process views described in a new standard IEC 62853 Open systems dependability soon to be published.

V. Dependability in the Wider Context

A. *Dependability and Quality*

In the past, dependability has been closely aligned with quality. With quality being the ability to meet requirements, dependability was considered to be a characteristic of quality in that it is concerned with how requirements can be achieved over time. This relationship certainly still exists but dependability is now seen as being more than an aspect of quality but instead has a wider sphere of application.

B. *Dependability and Risk Management*

There is a close link between dependability and risk. Both share the fundamental aspect of uncertainty. Determining the level of risk involves one of the attributes of dependability, namely reliability, as a way of determining likelihood, whereas risk adds consequences as the other component. Risk assessment involves methods and techniques that often use tools developed for dependability.

C. *Dependability and Safety and Security*

Dependability and safety have been linked for a long time. Although dependability does not specifically address safety, it has tools such as FMEA, fault tree analysis and HAZOP studies that assist safety analyses. This linkage continues to be of critical importance.

Security can be seen as being somewhat similar to safety. However, it has much more recently grown in importance, particularly with respect to software security now being at the heart of cyber-physical systems [1].

D. *Dependability and Asset Management*

The most recent touchpoint for dependability is the development of asset management standards under ISO TC 251. These standards cover assets in their broadest sense with

dependability being one of the major "how to" aspects of asset management. Asset management is about how assets are managed within the context of a generic management system with an example being railway asset management from the International Union of Railways [3]. The electrical power sector is also promoting an asset management approach worldwide to achieve consistency in such areas as asset management metrics, risk analysis and prioritization, and indicators to aid asset owner decisions [4].

Dependability management parallels asset management in that it provides the dependability aspects to asset management policy, systems and plans as they fit into the general organizational equivalents. The following figure illustrates this as it is shown in IEC 60300-1, Figure 2 [5].

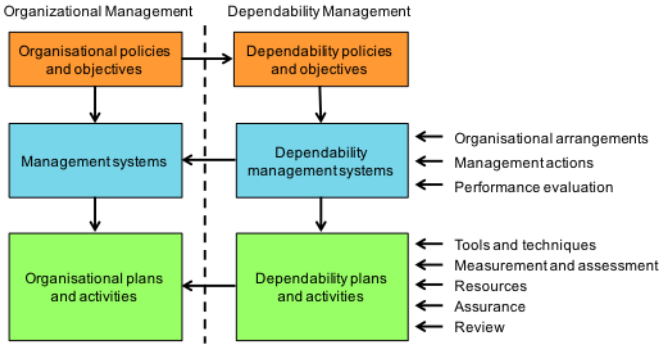

Fig. 5. Dependability Management Systems

VI. Dependability Challenges

A. Stakeholders

This leads us to consideration of the challenges that now face dependability in this rapidly evolving world. Challenges entail factors such as system complexity and analysis, multi-state systems, integration of systems into networks or open systems, organizational and human reliability analysis, software reliability, safety and security, maintenance and infrastructure life assessment and extension [6].

The first challenge is how to engage with our stakeholders. There are many different stakeholders, ones that can generally be divided into these categories:

- designers/implementers of dependability such as reliability, maintainability and supportability experts, statisticians, systems engineers, domain specific engineers, manufacturers and software programmers;
- implementers of dependability such as management, project leaders, test specialists, procurement staff;
- users of assets that are focused on obtaining a service;
- operators of assets that provide the service;
- maintainers that ensure assets retain the functionality of equipment or restore it when it fails;
- regulators that set standards, especially for safety and the environment;
- academia and research organizations;
- other standards organizations.

TC 56 produces generic standards that are intended to be used where applicable, leaving specific industries to produce their own versions where needed. The challenge is how to meet the needs of such a diverse set of stakeholders. TC 56 has recently started to better define who the stakeholders are and to strategize how to more effectively understand and satisfy their requirements.

B. Standards Development

The current pace of standards development follows a typical 3 year cycle for both new standards and maintenance or updating of existing ones. In today's world, this makes it difficult to keep up with evolving developments. And yet, standards deserve careful development and proper international collaboration. IEC is encouraging reducing timelines for standards development or maintenance. One way is to use of online meetings between face to face ones. In spite of the main issue with online meetings that the difference in time zones makes it difficult for some to attend, this has to become more prominent in progressing standards development at a faster pace.

One issue with the current model of standards development is that standards are often not in synch with one another and the updating process is always a bit behind. At the moment for TC 56, this has resulted in a concerted effort to update what is considered as the core standards concurrently. This process involves particularly some re-alignment of content for consistency and minimizing the overlap between these standards.

Another issue is how to obtain consistency with other standards development committees, both within IEC and for external ones such as ISO and other committees or organizations related to dependability.

C. Communication

It is not effective any more for standards committees to rely on the standards themselves to communicate with their stakeholders. Fortunately, communication by electronic means such as websites and the internet facilitates the provision of supplementary information about dependability to a potentially extensive audience. The tools exist for doing this but this adds an additional burden to standards committees to get information out to stakeholders. More effective liaison with other committees and industry interested parties is another important component of communication. Standards committees now need to be much more savvy when it comes to communicating with the outside world.

D. Evolving Technologies

Technologies are evolving at an increasingly faster rate but with shorter life times leading to quicker obsolescence. The impact of climate change, population pressures, environmental concerns, increasing integration between systems, more catastrophic failures and greater reliance on technology to support user expectations all contribute to the need for dependable systems. One of the most important places this is felt is with infrastructure, much of which is reaching the end of its life, requiring major renewal and investment. Another is IoT or the Internet of Things, which is receiving much emphasis [7]. Better ways have to be found for dependability standards to keep up with new technologies.

E. Open Systems

The most crucial arena for evolving technology that is often both innovative and disruptive is with open systems. Within the narrower scope of individual systems, it is still possible, and indeed critical, that the foundations built by dependability be maintained. But for today's systems, it is the outside influences of other systems that interconnect in some way that then exhibit the behaviour of open systems. This is where the greatest risk is of actions that can cause potentially catastrophic failure, particularly for infrastructure.

Some examples are the Internet of Things [8] and the Smart Grid. The need is obviously to ensure dependability requirements are met but this becomes much more difficult if the impact (and even the existence) of other interconnected systems cannot be necessarily established, verified or maintained. Other challenges for dependability are how to characterize dependability for open systems including how to measure dependability in this space although attempts are being made [9].

There are efforts underway to address these challenges, some based on the past and others looking towards the future. One example is a fault tree application that attempts a more classical approach for complex systems [10]. The IEC is leading an effort to evaluate the potential for Global Energy Interconnection where the concepts of open systems will have to be applied [11].

The future is both promising and uncertain. Dependability will continue to play a major role and many challenges and much more work lies ahead of us.

ACKNOWLEDGMENT

The author wishes to recognize the stellar efforts and dedication of the many experts that have contributed to the development of dependability standards over the past 50 years since the formation of the IEC/TC 56 committee on which much of this paper is based. However, in the end the content of this paper expresses the experience, thoughts and opinions of the author and are not intended to necessarily represent those of the IEC.

REFERENCES

[1] WEF World Economic Forum, "Strategic Infrastructure Steps to Operate and Maintain Infrastructure Efficiently and Effectively," Prepared in collaboration with The Boston Consulting Group, REF 180314, April 2014.

[2] ASME, "Cyber-Physical Systems – Maintaining Dependability and Security of Critical Infrastructure", ASME Dynamic Systems & Control, March 2017, Vol. 5 No. 1.

[3] UIC International Union of Railways, "Guidelines for the Application of Asset Management in Railway Infrastructure Organisations," September 2010, ISBN: 978-2-7461-1878-2.

[4] IEC, White paper, "Strategic asset management of power networks," IEC, Geneva, Switzerland 2015, ISBN 978-2-8322-2810-4.

[5] IEC 60300-1:2014, DEPENDABILITY MANAGEMENT – Part 1: Guidance for management and application.

[6] Zio, E., "Reliability engineering: Old problems and new challenges," Reliability Engineering and System Safety 94 (2009) pp. 125– 141.

[7] IEC, "The IEC and the Internet of Things," SMB Newsletter, Issue No. 5 – May 2017.

[8] IEC, White paper, "IoT 2020: Smart and secure IoT platform," IEC, Geneva, Switzerland 2016, ISBN 978-2-8322-3593-5.

[9] Bukowski, L., "System of systems dependability – Theoretical models and applications examples," Reliability Engineering and System Safety 151 (2016) 76–92.

[10] Nguyen, T.P. Khanh, Beugin, Julie, Marais, Juliette, "Method for evaluating an extended Fault Tree to analyse the dependability of complex systems: Application to a satellite-based railway system," Reliability Engineering and System Safety 133 (2015) 300–313.

[11] IEC(4), White paper, "Global energy interconnection," IEC, Geneva, Switzerland 2016, ISBN 978-2-8322-3680-2.