CONCEPT OF DEPENDABILITY

EXPLANATORY COMMENTS

The following is for discussion in the April 2009 WG3 meeting on the fundamental concept of dependability with the objective to determine how dependability will be dealt with in the proposed future revision of the top standards for Dependability to be decided in the fall 2009 TC56 meeting.

In this version, a new attempt is made to provide a framework for dependability that is both understandable to the general public but also appropriate for dependability as a technical discipline. With the risk of oversimplifying, it proposes a bridge between the general concept of dependability and the technical discipline by defining several layers:

- An inner core with the core dependability attributes
- A outer layer with the performance attributes that define success

Dependability is then placed in the general context of systems, products and services by recognizing that it enables and enhances the performance attributes that can be relevant to a system.

AN IMPORTANT NOTE: this is not intended to be a new definition of dependability. It can be argued that the formal definition of dependability should describe the technical discipline involved in its application. The purpose of this discussion is to make dependability meaningful in the context of business applications.

DEPENDABILITY IN A BUSINESS CONTEXT

From a business perspective**, dependability describes the extent to which something can be trusted to behave as expected**. Although the concept of dependability can be applied in many different situations, in this context, **it is intended to apply to a technological system, product or service.** (See the section below on what dependability applies to for more explanation.)

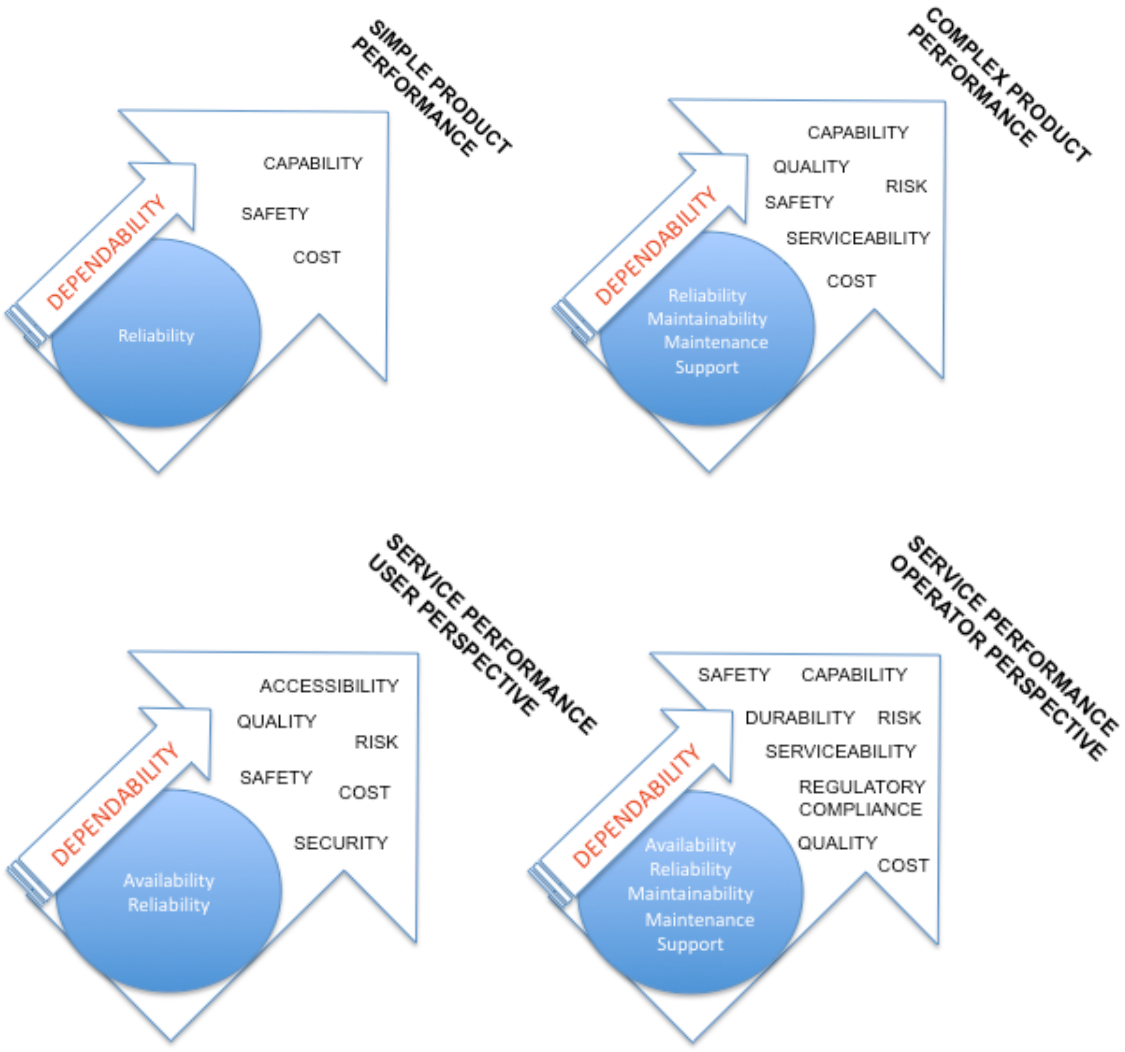
The **success of a technological system, product or service is determined by a number of performance attributes**. These attributes are described by terms such as capability, safety, integrity, durability, survivability, serviceability, risk, quality, environmental sustainability, vulnerability, retainability, accessibility, regulatory compliance, security, cost, disposability and so on.

Dependability is somewhat **unique in that it enables many of them to be achieved**. For example, safety is enhanced when failures are eliminated or minimized. In the past, dependability has been aimed primarily at specific functionality and safety but this now needs to be expanded more broadly. This of course could just be a matter of perception because it can be argued that functionality includes all of these attributes.

It is possible to consider dependability as an independent performance attribute but maybe it is more correct to understand it as **a characteristic that defines how well the basic performance attributes of a system, product or service can be achieved**.

To show this pictorially, one can imagine a core of dependability attributes surrounded by all of the performance attributes of a system, product or service that dependability affects.

For a specific situation, the application of dependability depends on which performance attributes apply. This can be shown in a modified version that shows both the dependability and the performance attributes that are relevant and result in success for the system, product or service. See the examples below.



The stakeholders in a system, product or service are usually referred to as the *interested parties*. The interested parties for dependability include the users of the product or service, the people providing the service or product (operators and maintainers), the public and the owners (or shareholders) who have a financial stake.

The success of the system, product or service is *measured based on the applicable performance attributes relevant from a business context* and varies with the perspective of the various interested parties. Dependability measures are an integral part of the performance measures although they are not the whole. For example, the success of safety performance may be the number of accidents. Some of these will be relevant from a dependability perspective because they occur due to the failure of equipment to perform their required function and others will not such as a design deficiency.

DEPENDABILITY AS A TECHNICAL DISCIPLINE

Core Dependability Attributes

Dependability is an 'umbrella' term that comprises core attributes that describe particular dependability-related aspects of the relevant performance attributes. Traditionally we have described "performance attributes" as "functions" so that has been retained in these definitions.

Reliability is the probability that an item fulfils the required functions for the required duration. Reliability can be considered for an individual function or set of functions (functional mode) which contributes to the service, and an item may exhibit different degrees of reliability for different functions or functional modes. Its reliability usually depends upon the way in which the item is used, so the formal definition requires the 'conditions' (i.e., of use or operation) to be defined. Reliability is related to time (which usually means operating time).

Maintainability is a measure of the ability to perform maintenance under given conditions and indicates the ease with which an item can be repaired. A high degree of maintainability means that repairs consume little time and effort, on average. **Maintenance support** describes various aspects responsible for maintenance, e.g., skill of repair personnel, location of repair facilities, traveling time, time taken to procure spare parts, etc. **Integrated logistic support (ILS)** is the practice of organising all of these aspects in a mutually consistent fashion in order to optimise maintenance.

Availability describes the extent to which an item is operational and able to perform any required function or set of functions if a demand is placed on it. It is derived from **reliability** and **maintainability** (where hardware failure is concerned). **Maintenance support** may also affect availability, since the time required to repair the item depends upon this. There are important differences between the manner in which software is maintained as compared to hardware.

When considering these dependability attributes, focus is usually given to impairments to dependability. There are different ways in which states or events adversely affect dependability. **Failures** are events which occur during the operation of the item when it departs from its required service. There are also instances of **non-conformity** or **defects**, and **faults**. These are states or properties of the item. **Errors** are internal states of a system which may arise from faults. Faults and failures have certain **characteristics** by which they may be classified.

What Dependability Applies To

Dependability can be applied to **systems, products or services** as determined by a specific situation.

Dependability applies to a class or group of descriptors that is formally referred to in IEC as an **item**. Such a general term is used since it is necessary to be able to refer to anything from the simplest 'widget' to the most complex computer system. Dependability most

often refers to the more complex grouping where a service is being performed for a user while its attributes are also applied to lower levels of items.

A system transforms inputs through processes into a product or service by means of resources and processes. For technological applications, the system encompasses **hardware, software and human aspects**.

The system can be seen as providing a service in different situations such as:

- A transportation service such as a railway, airline, bus, pipeline, roads, etc.
- A manufacturing process such as making electronics, processing oil and gas
- A network such as commercial airports, the internet, communications, electric power grid, interconnecting pipelines

The output of a system may also be a **product** as the result of some process that includes specification, design and (where hardware is concerned) manufacture. Increasingly there are **complex systems** of which human operators are considered to be a part, so that the possibility of human error needs to be taken into account, and certain very complex systems which grow ‘organically’ rather than being produced to a clear specification (e.g., the Internet and the world-wide web).

Many items consist of both **hardware** and **software**. If a hardware or software component fails, it is replaced or repaired. If a specification or design fault is discovered, it is corrected, and the system will usually undergo modification during its operating life to remove faults or to improve its performance.

There are important differences between hardware and software that need to be recognised when considering their dependability. Software is intangible. This has important implications for its dependability, for the way in which it fails and for its maintenance. Another important difference between hardware and software is that software does not wear out, nor suffer from other physical causes of failure. Instead, it suffers from systematic failure due to the manifestation of latent faults or bugs introduced by human error during development.

It is important to distinguish between the type of an item or product and an individual example or copy of it in use in the field. Individual examples may exhibit different levels of dependability in use due to operating under different conditions, being subject to different amounts of wear or ageing and due to being at different modification levels.

Management of Dependability

In order for Dependability to be successful, it has to be **managed** within the context of **existing management systems**. The application of dependability techniques over the life cycle of items demands that they be controlled and managed. It is not normally appropriate for separate dependability management systems to be set up and instead existing management structures can effectively be applied to ensure dependability aspects are addressed.

To meet dependability expectations, management has responsibilities to establish dependability-related goals and objectives, integrate dependability processes, provide dependability resources and enable dependability measurement and improvement.

Life Cycle

Any item or type of item goes through a **life cycle** consisting of several phases. Products, hardware, software and systems may entail a different set of **life cycle phases**. In general, the most generic life cycle phases consist of **concept and definition**, **design and development**, **realization and implementation**, **operation and maintenance**, **enhancement or modification**, and finally **retirement and decommissioning**. This is a broader set of life cycle phases than traditionally used for products.

The **life cycle cost** of operating and/or supporting an item is the total cost of developing, manufacturing, or procuring an item, maintaining and supporting it during its operational life, and disposing of it when it becomes obsolete. Several aspects of this cost need to be considered: cost of supply, cost of ownership, and cost of maintenance. Who bears these costs will depend upon the contractual arrangements surrounding an item, e.g., whether it is developed 'in house' or procured from a supplier, whether maintenance is performed by the developer or by a third-party maintenance organization, etc

Human Aspects

The importance of including **human aspects of Dependability** cannot be minimized. Human beings are **users, designers, manufacturers, handlers operators, maintainers**, and perform many other functions related to items. These items can have a very high level of dependability by themselves but this can ultimately be defeated by a lack of attention to human aspects.

Processes, Techniques and Tools for Dependability

The evaluation, assessment and improvement of dependability are achieved by processes, techniques and tools. These can be mainly divided according to the attributes of dependability described above. They are layered from the most general one of processes down to more detailed techniques and tools.

Assessment of Dependability

The assessment of **dependability** and its attributes requires **measurement**. The measurement of dependability from an outside user or business perspective is dependent on the applicable performance attributes. For example, for a transportation service, the user will be concerned with accessibility of the service (availability of space and conformance to the posted schedule) and retainability (on-time arrival) and integrity (properly maintained seating and facilities). Dependability may also be assessed by means of an effectiveness measure that integrates availability, production rate and product quality.

From the point of view of dependability as a technical discipline, the attributes that constitute dependability (**reliability**, **availability**, **maintainability** and **maintenance**

support performance) can be quantified in different ways such as instantaneous and operational measures derived from direct and indirect measures of items in test, operation or maintenance. For example, they can be measured by times of failures, operating time to first failure, duration of intervals of up time and down time, effort (man-hours) expended on maintenance activities, etc.

In the end measurement has to be aimed at the desired audience and not restricted to one point of view.