Reliability Engineering and System Safety 151 (2016) 76–92

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

System of systems dependability – Theoretical models and applications examples

L. Bukowski

The University of Dabrowa Gornicza, Poland

ARTICLE INFO

Available online 6 November 2015

Keywords:
Dependability engineering
System of systems
Uncertainty
Risk
Vulnerability
Resilience
Process continuity

ABSTRACT

The aim of this article is to generalise the concept of "dependability" in a way, that could be applied to all types of systems, especially the system of systems (SoS), operating under both normal and abnormal work conditions. In order to quantitatively assess the dependability we applied service continuity oriented approach. This approach is based on the methodology of service engineering and is closely related to the idea of resilient enterprise as well as to the concept of disruption-tolerant operation. On this basis a framework for evaluation of SoS dependability has been developed in a static as well as dynamic approach. The static model is created as a fuzzy logic-oriented advisory expert system and can be particularly useful at the design stage of SoS. The dynamic model is based on the risk oriented approach, and can be useful both at the design stage and for management of SoS. The integrated model of dependability can also form the basis for a new definition of the dependability engineering, namely as a superior discipline to reliability engineering, safety engineering, security engineering, resilience engineering and risk engineering.

1. Introduction

This article is based on the keynote lecture delivered by the author at the European Safety and Reliability Conference ESREL held in Wroclaw (Poland) in 2014. The main theme of this lecture was a unified model of dependability and resilience for complex systems. Following series of discussions with conference participants as well as our own reflection and experience [13–20], there was developed a new, broader and deeper version of this lecture, which constitute the content of this article.

Reliability engineering as a scientific discipline was born in the mid-1950s, and has been developing particularly rapidly since it was integrated into risk assessment methodology in 1970s [65,99]. With the increasing complexity of systems having a multi-dimensional character, namely: structural, spatial, temporal and disciplinary, as well as growing levels of uncertainty and risk, classic methods of assessing reliability have become insufficient. In-depth analysis of the situation at the end of the first decade of the 21st century was presented by Zio within the work [99].

In the areas of technical sciences, particularly fast-growing ones (such as computer science), at the end of the 20th century there began to form concepts of a comprehensive approach to the issues covered by reliability engineering and extended additionally by problems related to safety and security of systems [3,8,48,49,55,57,67,78,85,87]. There has been proposed a concept of dependability, as a collective term to describe the availability of a system, and its influencing factors, namely: reliability, maintainability and maintenance support performance [35]. Over time, new concepts of the term "dependability" were created, focused on the specific nature of the field in which they could be applicable. As a result of these works there began to emerge in the IT area, on the basis of reliability engineering, its generalised version – dependability engineering [27,38]. A significant advantage of this concept, especially for systems with high complexity, is its service delivery orientation and risk related approach, but disadvantage can be represented by its close fit to the specificity of computer area.

Another problem was related to the difficulty of defining the relationship between the concept of dependability and other similar concepts, such as: survivability [8], trustworthiness [8] and resilience. That problem applies especially to this last concept, associated with rapid development of a new, emergent knowledge discipline – resilience engineering [4,9,25,33,34,50,52,58,59,61,62,68,71,72,89,92]. The reason for such a large interest in this area appears to be primarily due to the growing importance of the threats and hazards of the type "LSLIRE" (large scale, large impact, rare events) [6,71,83,84,90]. Events of this type are particularly dangerous for system of systems such as critical infrastructure [27,46,47,64,68,98] and global supply chains [11,13,21–24,42,51,56,59,63,70,71,77,79,80,88,89].

Thus, it is fully justify to seek an opportunities to generalise the concept of "dependability" in a way, that could be applied to all types of systems, especially the system of systems, operating

E-mail address: lbukowski@wsb.edu.pl

http://dx.doi.org/10.1016/j.ress.2015.10.014
0951-8320/

under both normal and abnormal work conditions. The first step towards solving this problem, according to the author, is to predefine the basic concepts, principles and models existing in this field and based on the methodology of a systemic and process approach, on the grounds of system engineering [1,12,43,44,73] and system of systems engineering [28,29,32,37,50,74,82,87,98]. Subsequently, there should be developed the overall concept of dependability, applicable to all complex engineered systems, in particular, such as large scale and ultra large scale systems.

In Section 2, the concept of system of systems (SoS) and its main attributes is analysed, in terms of the general systems theory. The SoS is described with the teleological model by the function *P* and the function *G*. These two functions are taken for the primary measures of system performance and correspond to well known in the area of applied sciences – the effectiveness (function *P*) and the efficiency (function *G*). In Section 3 there are the main existing concepts of system dependability, that is: availability related probabilistic approach, availability and credibility related probabilistic-deterministic approach and concept of dependable service delivery as a risk related approach. In Section 4, on the basis of the considerations presented in Sections 2 and 3, there is a proposed generalised model of dependability, intended for its application in system of systems, particularly within complex socio-technical systems of the network organisations type. Finally an integrative concept for system of systems dependability assessment and management is developed, and, based on a static as well as a dynamic approach, the framework for evaluation of system of systems dependability proposed.

2. System of systems as an object of investigation

The first step toward defining the term “system of systems” is based on the foundations of the general systems theory and the systemic approach. Then, we will use Ackoff's behavioural approach to define different types of systems and their characteristics. Next, based on the concept of process approach, the terms: process and process organisation will be clarified. Finally, in association with ideas of complexity and emergence, the concept of a "system of systems" and network organisation will be defined.

2.1. The concept of the system in terms of general systems theory

Systems sciences have developed a new scientific paradigm called holism, that is, systemic approach. Systemic approach looks at the whole through the role and function of parts in the whole, taking into account the relationship of cause and effect (often undisclosed, non-linear and distant in time). It is characterised by a turn:

- from an emphasis on the part, to focusing attention on the whole,
- from a static structure, to a dynamic and process structure,
- from a metaphor of a hierarchical structure or a linear chain to the metaphor of a network,
- from the desire for an absolute truth to the approximate description.

The foundation for the systemic approach is systems thinking [10,12,31,43,91], based mainly on synthetic research procedure which, somewhat simplified, can be reduced to three following steps:

- Identification of the entire system, which includes the examined elements (e.g. subsystems).
- Evaluation and description of the system properties and its behaviour in time.
- Determination of the properties of individual system elements and their behaviour in time, taking into account the impact of these elements on the implementation of system functions.

The main task of this kind of synthesis is not a clear and precise identification of the system structure, but rather gaining knowledge about its behaviour in time and – in particular – about its functions. Thus, the cognitive emphasis of systemic synthesis is placed at explaining (what?) and understanding (why?) the behaviours and functions of the system, with a particular emphasis on variability in time, while an analytical approach focuses on determining static (fixed in time) structural characteristics of the system.

Systemic approach gained significance in recent decades, due to the growing number of the so-called large-scale problems. These include important issues in both defence and civilian systems, in terms of production and services, and examined from different perspectives – technical, economic, social, environmental and political. The root of these problems lies in complex interactions between the elements and states of the system, as well as unpredictable changes in the environment caused by forces of nature (natural disasters) or deliberate criminal and terrorist activity. Large-scale problems lead to the phenomenon of "the mess", defined by Ackoff. In his book [2] he defines “the mess” as a state of an organisation (a system) caused by a combination of unexpected and interrelated situations that pose a threat (danger) or a chance (opportunity) to the organisation. A lack of response to the mess, or limiting oneself to partial (non-systemic) solutions can lead to a deep crisis or even a total destruction and collapse of the entire system. Classic methods of solving such problems are generally ineffective, which is a result of the so-called circular logic effect, among others. This effect consists in the fact that in complex systems with a large number of interactions between elements and state variables, certain system states can be both the causes and effects of changes taking place in the system. This makes it difficult to identify both the problem itself and the causes that could have lead to it.

The practical implementation of the idea of a systemic approach is now possible thanks to the dynamic development of information technology. It requires a synergetic cooperation in numerous areas using a variety of methods and tools, e.g. in accordance with the so-called $\mathbf{C^4I^2}$ principle, whose name is an acronym for the following terms: **C**ommand, **C**ontrol, **C**ommunication, **C**omputer, **I**ntegration, **I**ntelligence. The main objective of this rule is to support decision makers in handling unexpected situations, which they have never had to deal with.

During the work on the development of general systems theory, a number of proposals have been made for defining the concept of the system. In "An Approach to General Systems Theory" [43], Klir made a critical analysis of the applied ways of defining systems and proposed a new approach to the problem, which he referred to as inductive approach (as opposed to deductive approach dominating in that time). This approach was based on distinguishing four basic features of systems, namely: the resolution level of examined system values (i.e. the accuracy and frequency of measurement), behaviour over time (variability of system values observed over time), relations stable over time (the relationships between system values that are stable over time) and properties describing these relations. As a result, a classification of definitions was created. It includes the following five types (classes):

1. A given system is a set of values examined at a certain resolution level.
2. A system is a set of values representing the variability of values under consideration over time.