Original article
https://doi.org/10.21683/1729-2646-2020-20-4-21-24

Development of the technology dependability automaton (substantiation of standardization regulation)

Nikolay I. Plotnikov, *AviaManager Research and Design Institute of Civil Aviation, Russian Federation, Novosibirsk*
am@aviam.org

Nikolay I. Plotnikov

Abstract. Aim. *This paper presents the development of the dependability automaton. The development is a conceptual description of the automaton as the term structure of a fixed complexity that shows non-contradictory interrelations and clear dependability state transitions of an item. The description of the state structure of the automaton implies subsequent development of a computing device for monitoring the dependability of items of any nature. Unlike in the standard, dependability is defined as a set of states, the measure of concordance with the purpose of an item. The purpose is defined as the property of an object attributed to the natural origin or designed application. In accordance with such definitions, alternative definitions of dependability states have been developed. An observation of the dependability states of an item can be described with a common algorithm. The problem is defined with the help of the automata theory.* **Methods.** *We will call a dependability automaton (DA) a deterministic, fully specified finite-state automaton. In the automata theory, the properties of items are examined in terms of being in states and transitioning between them. Dependability states change in terms of disruption and restoration of item purpose. Such changes can be represented as a directed graph, whose nodes correspond to states, while the edges correspond to transitions between states. As the dependability restoration states are deterministic, they can be represented as processes, i.e. planned, consisting of activities, measures, procedures, operations. The states of disrupted dependability are random, therefore they can be considered as events. Thus, the property of an entity's purpose is observed when the states of dependability are observed that change in events and processes. The automation is described using terms and symbols from standards, as well as alternative definitions of states developed by the author. A review of the appropriate standards is to involve a new terminology. The operation of the dependability automaton reflects transitions and alternative transitions. Restoration is designed as a complete and partially incomplete processes: a) transition from the down state into the up state; b) transition from the down state into the faulty state; c) transition from the down state into the good state. The findings contributed to the development of theoretical and practical dependability of organization, social groups and individuals. The dependability automaton concept includes the development of the engineering design of an expert decision support system for flight operation of an airline.* **Conclusion**. *Technical standards require prior preliminarily philosophical, philological, logical review. Such research is to produce logical proof and substantiation of a set of coordinated, non-contradictory ontological terms: property, state, event, etc. The results will be used in technical standards for the purpose of construction and substantiation of special terms. The paper provides a theoretical and practical substantiation of applying individual provisions of the dependability theory of technology for the purpose of developing the dependability theory of non-digital entities.*

Keywords: *dependability, terminology, standardization, regulation, dependability automaton.*

For citation: *Plotnikov N.I. Development of the technology dependability automaton (substantiation of standardization regulation). Dependability 2020;4: 21-24. https://doi.org/10.21683/1729-2646-2020-20-4-21-24*

Received on: *25.10.2019* / **Revised on:** *20.05.2020* / **For printing:** *18.12.2020*

1. Introduction

In this paper, unlike in the standard [1], dependability is defined as a set of states, the measure of concordance with the purpose of an item. The purpose is defined as the property of an item attributed to the natural origin or designed application. In accordance with such definitions, alternative definitions of dependability states have been developed.

An observation of the dependability states of an item can be described with a common algorithm. The problem is defined with the help of the automata theory [2]. In order to solve the problem, it is suggested to develop a dependability automaton (DA). The development is a conceptual description of the automaton as the term structure of a fixed complexity that shows non-contradictory interrelations and clear dependability state transitions of an item. The description of the state structure of a DA implies subsequent development of a computing device for monitoring the dependability of items of any nature.

2. Development of dependability automaton

Problem definition. We will further call a dependability automaton designated as D (dependability) a deterministic, fully specified finite-state automaton. DA is defined by a set consisting of the following elements:

$D = \{X, S, Y, \delta, \lambda, s_0\}$,

where D is the DA;

X is the input alphabet of the automaton (set of input symbols): $X=\{x_1, \ldots, x_m\}$;

S is the automaton states: $S = \{s_0, \ldots, s_n\}$, s_0 is the initial automaton state;

Y is the output alphabet of the automaton (set of output symbols): *;*

δ is the specified indication of states at a set of input signals, the function of automaton transition from one state into another: $s_j = \delta_i(s_i, x_k)$, where s_j is the subsequent state of the automaton, s_i is the current state of the automaton; x_k is the current input symbol;

λ is the specified indication of states at a set of output signals, the output function: $y_l = \lambda_i(s_i, x_k)$, where y_l is the subsequent output symbol of the automaton, s_i is the current state of the automaton; x_k is the current input symbol.

The conditions are: sets X, S, Y are finite; the output symbol ($y_l \in$ Y) depends on the input symbol $x_k \in X$) and the current state of the automaton ($s_i \in S$); description entries of the automaton are defined at discrete instants in time.

The deterministic automaton: a) from state s_i under the influence of signal x_k transitions into state s_j; at the output, y_h changes to y_1; b) for $(x_i, y_i) \in (X, Y)$ δ and λ are defined.

3. Structure of automaton states

In the automata theory, the properties of items are examined in terms of being in states and transitioning between them. Dependability states change in terms of disruption and restoration of item purpose. Figure 1.

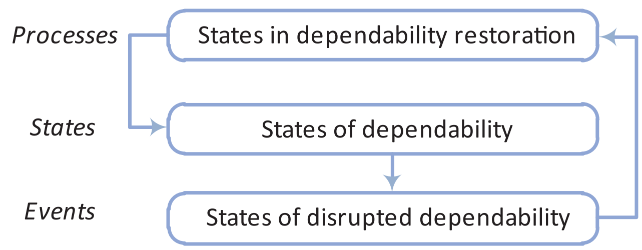

Fig. 1. Observation of dependability

Such changes can be represented as a directed graph, whose nodes correspond to states, while the edges correspond to transitions between states. As the dependability *restoration* states are *deterministic*, they can be represented as processes, i.e. planned, consisting of activities, measures, procedures, operations. The states of disrupted dependability are *random*, therefore they can be considered as events. Thus, the property of an entity's purpose is observed when the *states* of dependability are observed that change in *events* and *processes*.

The automaton is described using terms and symbols of standards [1], [3] and alternative definitions of states developed by the author. A review of the appropriate standards is to involve a new terminology. For instance, the definition of the term "defect" clearly does not correspond to the technical sense. In standard [1], "defect" is defined as the non-compliance on an item with the requirements specified in the documentation. In standard [4], "defect" is defined as non-fulfillment of the requirement associated with the presumed or specified use. The basic states in this paper are set forth as follows (Table 1).

Table 1. States of the dependability automaton

Terms	States	Ω
	maintenance	(s_{mtn})
Processes	repair	(s_{rep})
	restoration	(s_{rest})
	up state	(s_{up})
	perfect state	(s_{per})
States	imperfect state	(s_{imp})
	down state	(s_{dw})
	failure	(s_{fail})
Events	defect	(s_{def})
	degraded state	(s_{deg})

4. Development of DA algorithms

The description of the DA operation consists in the translation of the standard terms into symbolic algorithms suitable for subsequent software development. Let us introduce the following symbols and construct the algorithm of DA operation:

$\overline{D}$ is dependability;

↓D are dependability disruptions;

↑D are dependability restorations;

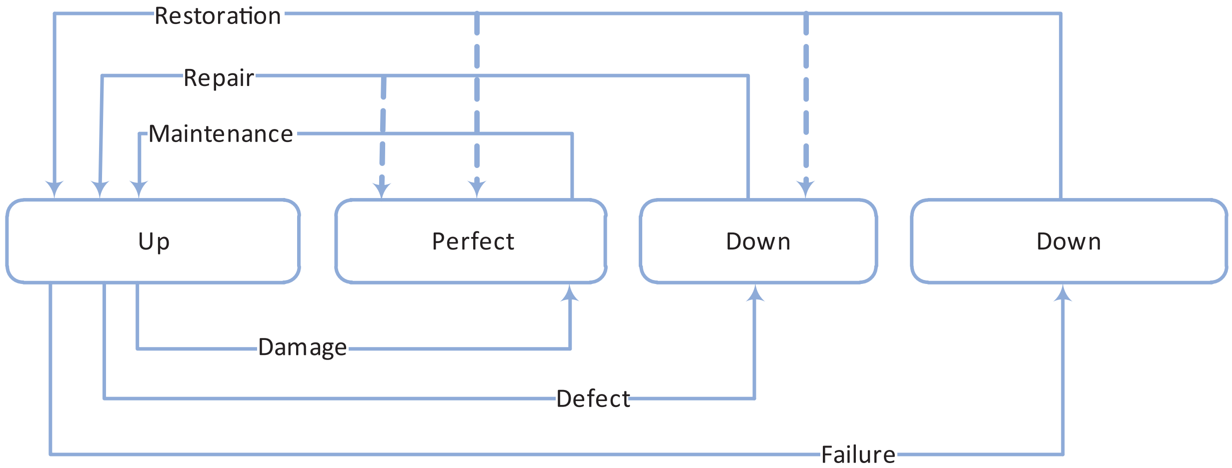

Fig. 2. Conceptual diagram of the dependability automaton

$(s_j \rightarrow s_i)$ are the transitions from the current state into the subsequent state in dependability disruption events;

$(s_j \leftarrow s_i)$ are the transitions from the current state into the subsequent state in dependability restoration processes;

$\overleftarrow{S}$: $(s_{rest} \subseteq s_{rep} \subseteq s_{eng})$ are subsets of dependability restoration states (processes);

$\vec{S}$: $(s_{fail} \subseteq s_{def} \subseteq s_{deg})$ are subsets of dependability disruption states (events);

$(s_j \rightarrow s_i)| \vec{S}$ are transitions amidst dependability disruption events;

$(s_j \leftarrow s_i)| \overleftarrow{S}$ are state transitions amidst dependability restoration events;

DA states are shown in the diagram (Fig. 2).

Dependability states:

$\overline{D}: s_{up} \mid \left(s_{up} \leftarrow s_{eng}\left(s_{per} \leftarrow s_{rep}(\leftarrow s_{rest})\right)\right)$ is the up state by maintenance, repairs, recovery condition;

$\overline{D}: s_{per} \mid \left(s_{per} \leftarrow s_{rep}(\leftarrow s_{rest})\right)$ is the good state by repairs, recovery condition;

$\overline{D}: s_{imp} \mid \left(s_{imp} \leftarrow s_{rest}\right)$ is the faulty state by recovery condition;

$\overline{D}: s_{up} \mid s_0$ is the down state.

States in dependability disruption events:

$\downarrow \mathrm{D}: s_{deg} \mid s_{eng}$ is the damage by maintenance condition;

$\downarrow \mathrm{D}: s_{def} \mid s_{rep}$ is the defect by no-repairs condition;

$\downarrow \mathrm{D}: s_{fail} \mid s_{rest}$ is the failure by no-restoration condition.

States in dependability restoration processes:

$\uparrow \mathrm{D}: s_{eng} \mid \left(s_{up} \leftarrow s_{per}\right)$ is the maintenance for transition from the good state into the up state;

$\uparrow \mathrm{D}: s_{rep} \mid \left(s_{up} \leftarrow s_{per}(\leftarrow s_{imp})\right)$ are the repairs for transition from the faulty state into the up (good) state;

$\uparrow \mathrm{D}: s_{rest} \mid \left(s_{up} \leftarrow \left(s_{per} \leftarrow \left(s_{imp} \leftarrow s_{dw}\right)\right)\right)$ is the restoration for transition from the down state into the up (faulty, good) state.

Discussion. The operation of a DA reflects transitions and alternative transitions. Restoration is designed as a complete and partially incomplete processes: a) transition from the down state into the up state; b) transition from the down state into the faulty state; c) transition from the down state into the good state. The states of DA summarize the resource hierarchy in terms of "restoration" ⊆ "repairs" ⊆ "maintenance". However, all technology dependability standards lack a substantiation of the term hierarchy.

5. Theoretical and practical implementation of DA

The findings contributed to the development of theoretical and practical dependability of organization, social groups and individuals (Fig. 3) [5].

The DA concept includes the development of the engineering design of an expert decision support system (ES) for flight operation of an airline. The ES has functional modules, includes a knowledge base or ES shell, as well as named functional units: information assets transformation system (IATS); module for indicator data analysis and prediction of the states of pilot resources; solver or pilot resources management decision-making module. The DA is represented as the sum of pilot resources (SPR) consisting of three groups of properties of dependability: individual dependability resources (IDR), professional dependability resources (PDR), operational dependability resources (ODR). Such grouping is based upon the structural approach to defining standard terms consisting in the partition of abstract concepts using the example of the category of "dependability".

Using that approach, a base of observation in time has been developed: IDR, the time of human evolution, PDR, the time of employment between ages 20 and 60, ODR, the time from the duration of one flight up to a year. The new SPR structure allows defining various norms and limits, which improves the flight efficiency and safety supervision [6].

6. Conclusion

Technical standards require prior philosophical, philological, logical review. Such research is to produce logical proof and substantiation of a set of coordinated, non-contradictory ontological terms: property, state, event, etc. The results will be used in technical standards for the purpose of construction and substantiation of special terms. For instance, why the term "failure" is larger than the term "damage" in terms of

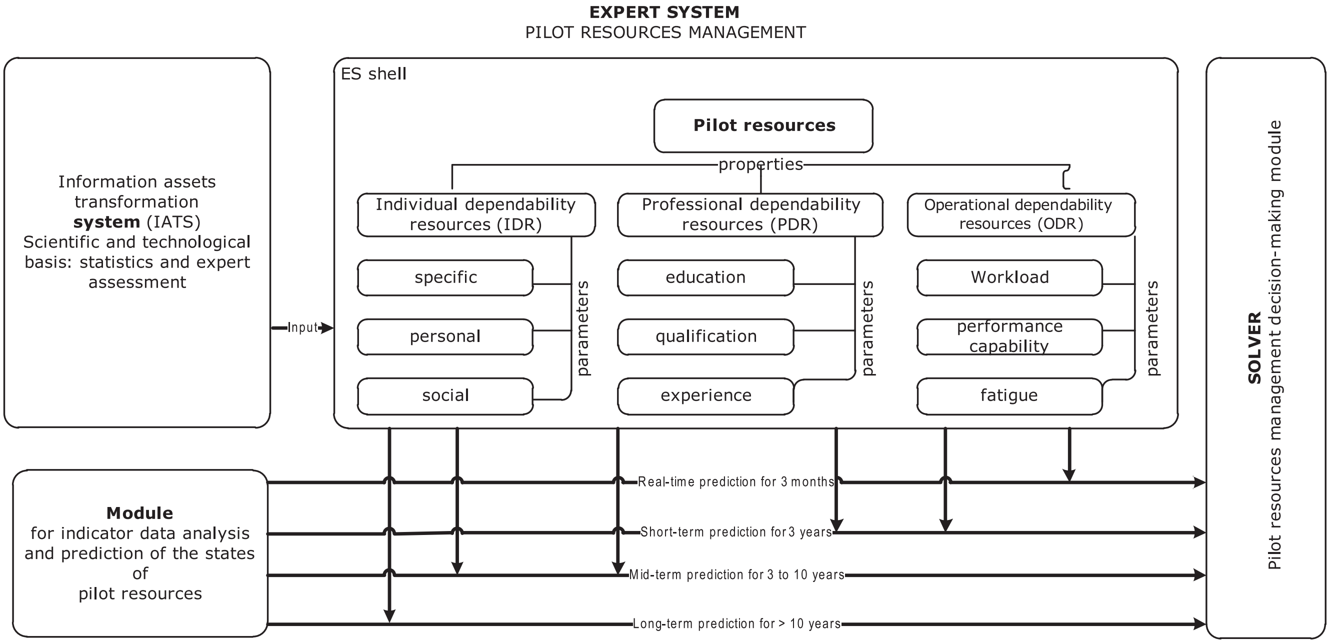

Fig. 3. Dependability automaton of an individual (commercial aviation pilot)

scope and content in the physical and technical senses. The paper provides a theoretical and practical substantiation of applying individual provisions of the dependability theory of technology for the purpose of developing the dependability theory of non-digital entities.

References

1. GOST 27.002-2015. Dependability in technics. Terms and definitions. Moscow: Standartinform; 2016. (in Russ.)

2. Vykhovanets V.S. [Automata theory: a study guide for superior education establishments]. Tiraspol: RIO PGU; 2001. (in Russ.)

3. GOST IEC 60050-113-2015. International Electrotechnical Vocabulary. Part 113. Physics for electrotechnology. Moscow: Standartinform; 2016. (in Russ.)

4. GOST ISO 9000-2011. International standard. Quality management systems. Fundamentals and vocabulary. Moscow: Standartinform; 2012. (in Russ.)

5. Plotnikov N.I. Section 3; Annexes И, К, Л, М, Н. In: [Automated system for prediction and prevention of air accidents in organization and performance of air transportation. Intermediate stage no. 4: Adaptation of developed AS algorithms and software]. Research report, title 2010-218-02-068, state registration no. 01201150118 of 12.01.2011, accession no. 194. Ulianovsk; 2012. (in Russ.)

6. Plotnikov N.I. [Pilot resources. Reliability. A monograph]. Novosibirsk: Aviamanager; 2013. (in Russ.)

About the author

Nikolay I. Plotnikov, Candidate of Engineering, Director General, AviaManager Research and Design Institute, Russian Federation, Novosibirsk, e-mail: am@aviam.org

The author's contribution

The author analyzed dependability standards. Logical analysis of the concept of dependability was performed. The author suggests solving the dependability terminology problem in the automata theory by describing the general algorithm of state transition in the restoration processes and dependability disruption events.

Conflict of interests

The author declares the absence of a conflict of interests.