RUPRECHT-KARLS-
UNIVERSITÄT
HEIDELBERG

International Workshop on the
Design of Dependable Critical Systems

ECOMODIS

Proceedings

of the
International Workshop on the
Design of Dependable Critical Systems
"Hardware, Software, and Human Factors in Dependable System Design"

DDCS 2009

September 15, 2009
Hamburg, Germany

In the framework of
The 28th International Conference on
Computer Safety, Reliability and Security
SAFECOMP 2009

Edited by

Achim Wagner[1], Meike Jipp[1], Colin Atkinson[2] and Essameddin Badreddin[1]

[1] Automation Laboratory, Institute of Computer Engineering, University of Heidelberg
[2] Chair of Software Engineering, University of Mannheim

International Workshop on
the Design of Dependable Critical Systems
September 15, 2009, Hamburg, Germany

Towards a Practical, Unified Dependability Measure for Dynamic Systems

Achim Wagner[2], Colin Atkinson[1], and Essam Badreddin[2]

[1] Lehrstuhl für Softwaretechnik, Universität Mannheim,
68131 Mannheim, Germany
atkinson@informatik.uni-mannheim.de

[2] Automation Laboratory, University of Heidelberg
68131 Mannheim, Germany
{achim.wagner, baddredin@ziti.uni-heidelberg.de}

Abstract. Providing a practical measure of the dependability of dynamic systems, including software systems and components, has been an elusive goal of systems engineers for some time. Measures for static, individual, dependability-relevant properties (e.g. reliability, safety, availability etc.) are well understood, but to date there is no general and widely accepted way of combining these into a single dependability measure that can be used to assess a dynamic system's capability for specific applications. In this paper we present a practical approach for obtaining an Integrated Dependability Measure (IDM) by placing the onus on system developers and users to capture the acceptability of different behavior in the form of acceptability functions rather than by defining (or attempting to define) general purpose combinations of separately determined dependability ingredients (e.g. reliability, safety etc.).

Keywords: Dependability Measure, Dynamic Systems, Behaviour-based System description

1 Introduction

Dependability is a complex concept which attempts to measure the degree to which a user can rely on a system to provide a certain level of service in a certain context [1]. There is general consensus on the various ingredients that contribute towards the dependability of a system such as reliability, safety, availability etc., and these ingredients are well understood [2]. However, even for traditional static systems which exhibit only "hard wired" patterns of behavior as they execute, there is no accepted generic approach for combining these separate ingredients into a single, overall dependability measure, and for dynamic systems which change their state over time it is even less clear how a the overall dependability can be represented by a combination of these attributes. Most of the approaches are related to binary fault models such as fault trees, Markov models or Petri-Nets [3]. These models are functional abstractions of the real system and their coincidence with the real system's behavior is difficult to prove [4]. Since dependability in general can also be defined as the capability of a system to successfully and safely fulfill its mission [5], the purpose of the system must be taken into account explicitly within a dependability measure.

One basic problem with trying to define a single unified measure of dependability from the traditional ingredients (e.g. reliability, safety etc.) is that their combination is highly application specific [6]. Thus, for systems which must satisfy strict safety requirements, safety measures must be given a much higher weighting than other ingredients such as reliability. In contrast, for systems which must satisfy stringent reliability requirements, reliability measures must be given a much higher weighting than other dependability ingredients such as safety and availability etc. The net effect of dependability's sensitivity to application specific requirements is that it is effectively impossible to define a single, generic way of combining the individual measures into a single measure. The definition of single, unified measure has therefore remained elusive.

In this paper we present a practical approach for getting around this problem that switches the onus for combining the dependability ingredients to system developers and users on a case-by-case basis rather than on researchers to find a single generic combination approaches. This is achieved by requiring developers to extend the specification of system behavior with so called "acceptability functions". The approach is based on a behavioral description of the system and the measurement and assessment of the system outputs [5]. In contrast with traditional specifications which merely describe the expected behavior of the system in response to stimuli, a specification enhanced with acceptability functions describes "how well" the range of possible behaviors of the system meet the requirements. In other words, an acceptability function describes (in terms of a value between (0..1) how "acceptable" a particular behavior of the system is for the application in hand. When defining this acceptability function, the system developer has to take into account the appropriate weightings of the different factors such as reliability, safety, performance etc. and give them the corresponding influence on the acceptability value. By moving the problem of weighting the different ingredients to a user-defined acceptability function a single, unified approach can be used to calculate and compare overall dependability measures.

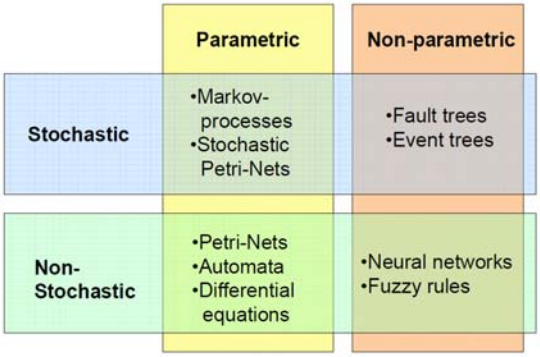
In contrast to the classical reliability engineering approach where the source of faults is not taken into account, in our approach we consider the behavior of dynamic systems. Therefore systems are described using models with uncertainty combining deterministic and stochastic processes. For reliability investigations, our assessment strategy is based on the hypothesis testing approaches commonly used in many disciplines, e.g. metrology and psychology, to determine the level to which a particular hypothesis is valid in a particular scenario. The problem of estimating a system's capability for a new application is then cast as the problem of establishing the likelihood that a given level of service (the hypothesis) will be delivered by a specific system in a given context based on the previous tests performed on that system. Another major advantage of the approach is that it lends itself to use of tests sheets [7] to define and apply the tests used to ascertain the dependability of a system and to document how the acceptability functions are used to calculate the final dependability measure [8].

In this paper we provide an overview of our Integrated Dependability Metric (IDM) approach and explain how system specifications can be enhanced with acceptability functions to combine dependability ingredients in an application specific way. This is demonstrated through a small case study for a dynamic control system.

Theory

There are various different ways to describe dynamic systems, which can be classified as parametric/non-parametric and stochastic/non-stochastic models (see Table 1). In system theory, parametric input-output and state space models are very common, and are often enhanced by additional noise terms to model the stochastic part of the system.

Table 1: Model classification



This kind of model covers a broad range of applications. In contrast to pure stochastic models the output values are generally correlated, i.e. the random noise due a stochastic process is modified by the system transfer function. Thus, not only the distribution in the amplitude but also the distribution over the time domain is an important property of a stochastic variable. Furthermore deterministic output errors can be modelled as a result of parameter errors in the system transfer function. For physical systems, samples are directly related to the time at which the samples are taken, e.g. using a specified sampling rate. For other systems like software systems this sampling time is not obvious. Therefore it may be abstracted using an ordered series of samples instead.

Safety-critical physical states can be represented as internal states in the state space representation. However, as long they can be measured, critical states may be visible as output values of input-output systems. In order to fit the black-box view of many other disciplines, including software engineering the input-output representation for dynamic systems is preferred in this paper.

Dependability Measure

The dependability measure defined in this paper is based on the definition of dependability for autonomous systems [5] and enhanced by an additional stochastic view of the system model. Furthermore, the validation against specified system properties plays a major role. The formal definition of our dependability measure makes the following assumptions:

1. The specification and the realization of a dynamic system are given: i.e. the purpose of the system (usage, mission), the behavioural, structural,

functional and non-functional properties, environmental conditions and system boundaries,

2. The system is operated in an environment with uncertainty, i.e. it is not exactly known if errors in the output behaviour are due to disturbances or system faults.
3. The correctness of known system properties is verified by other means
4. Faults will happen!

The required dependability measure *D* describes the correspondence of the actual system behaviour to its specified behaviour within the system boundaries and according to acceptance criteria. The dependability measure is an objective value and therefore free from any human perception and interpretation. The dependability measure is a functional, which depends on the actual system output behaviour *y*, the specified reference behaviour y_r, system boundaries and acceptance criteria Σ, a mission *u* (finite set of input test trajectories corresponding to the usage of the system) and a number of acceptability functions corresponding to the measured dimension of dependability.

As the Integrated Dependability Measure (IDM) for safety-critical computer controlled systems we propose the (time) discrete function:

$$D_l = 1 - \overline{D}_l = 1 - \frac{\sum_{j=1}^{d}\left[a_j \frac{1}{m} \sum_{k=1}^{l} \overline{A}_j\left(u_k, y_{r,k}, y_k, \Sigma_j\right)\right]}{\sum_{j=1}^{d} a_j} \qquad \textbf{(1)}$$

with normalized acceptability factors $A_j = 1 - \overline{A}_j$ corresponding to the dependability component *j* with dimension *d* and the *k*-th sample of a mission of length *m*. For practical purposes, the acceptability factors $\overline{A}_j$ are normalized functions with values in the interval [0, 1]. The values are added using weighting factors resulting in the overall dependability function. Thus, dependability is a unique normalized value in the range [0, 1] (0 means undependable and 1 dependable) taking account of all possible system impairments during a mission. Both the actual behaviour and the reference behaviour are considered to be the system response on a set of predefined input trajectories called reference missions or usage profiles of the system. The reference behaviour represents the desired (expected) system response during the application of a specific input trajectory. Depending on the concrete system description the test inputs may be fixed trajectories or generated from a test pattern generator (e.g. test sheets or Markov-processes for stochastic systems). Prior to the execution of the test mission the system is initialized. In order to validate specified system properties, a set of criteria Σ related to system behaviour and properties is explicitly included in the acceptability functions. Since performance, safety, complexity, etc. are often concurrent design parameters, the weights must be chosen by the system designer according to the system requirements.

Acceptability factors for dynamic system performance

The definition of errors is domain specific. For instance, in standard software technology only the correctness of a result is important and the error is modelled as a binary decision about the acceptance of the result. However in the scope of safety-critical real-time systems also the gradual degraded state must be considered.

As a basis function for several accessibility measures the relative deviation for sample k

$$e_{rel,k} = \frac{y_k - y_{r,k}}{y_p}, \tag{2}$$

related to the specified (maximum) error y_p can be used. However, $e_{rel,k}$ may have unlimited positive and negative values. Therefore we propose the squared exponential function of e_{rel} for the definition of an acceptability term for the system performance:

$$A_{performance,k} = \exp\left(-\left\| \frac{y_k - y_{r,k}}{y_p} \right\|^2 \right), \tag{3}$$

which has a range of [0, 1] and which is approximately $(1-e^2_{rel})$ for small values of e_{rel}. In case of a non-stochastic dynamic system this term reflects the structural and parameter uncertainty of the modelled system. If the system output is a vector $\boldsymbol{y}$ of dimension d the Euclidian norm is used to determine the absolute value. In the case of stochastic systems e_{rel} can be further evaluated by error statistics getting the meaning of reliability. Depending on how the system is described and what system property shall be highlighted (e.g. reliability or safety) the appropriate element of $\boldsymbol{y}$ must be chosen. In case of reliability, the output value is related to the service the system delivers. In the case of safety, the output value is related to critical system states (see example below). Furthermore, the test mission set must be carefully selected to cover the range of system outputs for the system properties under consideration.

Reliability of dynamic systems

For systems of high reliability the failure rate during normal operation is low. Generally, reliability parameters are determined using a large number of identical parts or many samples on one special system. However, for practical reliability evaluation of one system the lifetime may be shorter than the time needed to take the required number of samples.

The dependability concept presented here constitutes a generalisation of reliability and safety engineering concepts for dynamic systems. Consequently, the dependability measure should also include the special case of the reliability of static systems. Compared to established reliability measures using a binary fault model, here the gradual derivation of the system output can be used to reduce the testing effort.

In order to demonstrate this concept the system is modelled as a deterministic input-output system with stochastic uncertainty. The output value depends deterministically on an input stimulus, described by a constant transfer function known in advance. The output values are superimposed by a pure stochastic process

with independent samples. Thus, the stochastic process corresponds to the deviation of the actual output from the specified output. We assume that non-stochastic and stochastic process can be separated by subtracting both values.

Special case: Reliability of dynamic systems with noise

In contrast to static systems the output value of dynamic stochastic system depends not only on the actual input value, but also on the actual system state, which results from former input values and the initial value of the system. Generally the output values are correlated in the time domain, because independent input values, e.g. white noise, are modified through the dynamic system transfer function. Besides the probability density function (PDF) over the value range, the distribution of the output values over the time, respectively, the frequency spectrum, must be considered. Accordingly, the times where samples are taken must go along a system trajectory.

In this case we propose to collect output data from uncorrelated submissions and treat them as independent sample. To measure the proposed reliability factor it must be assured that the system did not change in between. For software systems, for example, this can be done by re-initialising the system.

Special case: Reliability of stationary systems

In this section the system under consideration is specified as a probabilistic system with the output variable *y*, statistically independent normal distributed output values, a mean value $\mu=0$, and a standard deviation of σ. Furthermore, it is required, that the absolute value of *y* does not exceed the maximum value y_{max} with a probability of P_{sys} for each sample of *y*. Thus P_{sys} is a reliability measure for mean failures per invocation. The conditional probability

$$P(y \le y_{\max} \mid \sigma \le \sigma_0) \le \Phi(y_{\max}, 0, \sigma_0) \quad \textbf{(4)}$$

can be calculated using the cumulative distribution function $\Phi(y_{\max}, 0, \sigma_0)$ according to the normal distribution of *y*, $\mu=0$, and the specified value σ_0 for the standard deviation.

Consequently, the overall probability for an error free system is

$$P_{sys} = P(y \le y_{\max} \wedge \sigma \le \sigma_0) = P(y \le y_{\max} \mid \sigma \le \sigma_0) \cdot P(\sigma \le \sigma_0), \quad \textbf{(5)}$$

i.e. the product of the conditional probability of having no errors $P(y \le y_{\max} \mid \sigma \le \sigma_0) = 1 - \gamma$ and the probability of being in the specified range $P(\sigma \le \sigma_0) = 1 - \alpha$.

Accordingly, we can find an upper limit

$$\overline{P}_{sys} = \overline{P}(y \le y_{\max} \wedge \sigma \le \sigma_0) = 1 - P(y \le y_{\max} \wedge \sigma \le \sigma_0) \le \alpha + \gamma \quad \textbf{(6)}$$

for the overall error-probability (unreliability). Corresponding to the required reliability and the known PDF the σ_0 value is specified during system design. In order to test the system against its specification, it is not necessary to measure the absolute value of the reliability. The α-value indicates the level of confidence the specified reliability has been reached. If the output samples are collected over a number of test missions,

$$\overline{A}_{reliability} = \alpha \tag{7}$$

can be used as an acceptability function for software reliability.

The system validation is now restricted to the test of the output value's distribution parameters, in this example the standard deviation, which can be performed using well known hypothesis tests. We assume that the PDF of the system output is known from long term experience, which is the normal distribution function in our case. Otherwise, tests known from textbooks can be used to test the PDF [9].

The hypothesis H_0: $\sigma^2 \le \sigma_0^2$ shall be validated by falsification of the counter hypothesis H_1: $\sigma^2 > \sigma_0^2$ with a confidence level 1-α, i.e. the probability of accepting H_0 although H_1 is true is less than α.

Since the real value of σ is unknown, the sample standard deviation s over a set of n sampled output values y_i, $i=1..n$ will be used for further calculation.

For a given confidence level α = f($\chi^2_{n-1;\alpha}$) the test condition for rejecting H_1 is given by

$$\frac{(n-1)s^2}{\sigma_0^2} > \chi^2_{n-1;\alpha} \tag{8}$$

with the critical value $\chi^2_{n-1;\alpha}$ of the χ^2-distribution with momentum $n-1$. The value $\chi^2_{n-1;\alpha}$ can be calculated according to the approximation formula

$$\chi^2_{m;\alpha} = m\left[1 - \frac{2}{9m} + y_\alpha\sqrt{\frac{2}{9m}}\right]^3 \approx m\cdot\left[1 + y_\alpha\sqrt{\frac{2}{9m}}\right]^3 \tag{9}$$

of Wilson and Hilferty with the critical value of the normal distribution y_α. Since α decreases more than exponentially with y_α, the number of samples required only increases weakly with decreasing α with

$$n - 1 \approx \frac{\frac{2}{9}y_\alpha^2}{\left[(s/\sigma_0)^{2/3} - 1\right]^2}. \tag{10}$$

In contrast, standard software verification techniques using the zero-error hypothesis need a sample size of the order O(lnα/p) [10], which may be problematic for seldom events with a small probability p. This result is not surprising, because the proposed approach uses the complete information over the distribution of the output samples and not just the binary decision about the acceptance of the sample. Furthermore the assumption of a zero-error system is often not realistic and the measured confidence level corresponds to the error probability of the test and not to a system property. In case of the continuous model the α–value corresponds to the confidence in the specified system and its parameters allowing an estimation of future system behaviour.

If the system output has a mean value $\mu \neq 0$ the complete PDF will be shifted on the y-axis resulting in an increase of the error probability P(μ)/P(μ=0)=1+ϕ. For small

positive values of μ the error probability increases approximate linearly with $\phi=\mu \cdot y_{max}/\sigma^2$. Generally, y_{max} and σ are given by the system specification and μ/σ corresponds to the relative deterministic deviation of the system response e_{rel}, i.e. in the probabilistic case e_{rel} has the meaning of a reliability decrease factor due to the non-probabilistic part of the system.

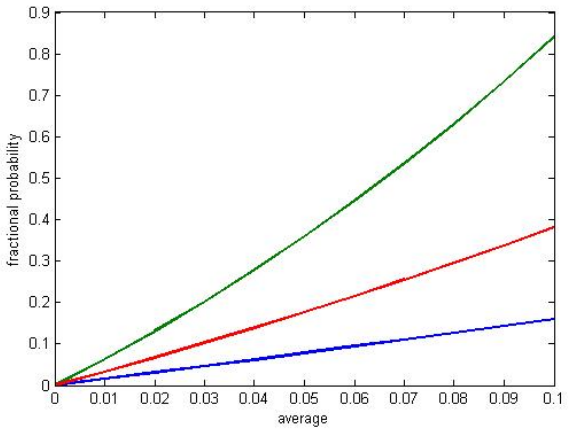


Fig. 2. Relative Increase of the error probability due to shift of the average value (blue line: $y_{max} = \sigma$, red line: $y_{max} = 3\sigma$, green line: $y_{max} = 6\sigma$)

Safety of dynamic systems

Generally, in the literature safety measures are probabilistic concepts based on binary accident events [3][4]. In order to find a safety measure describing the degraded state of a deterministic system the concept of the dynamic safety margin (DSM) is used [11]. In this concept the safety margin is the distance δ to the system boundary given by safety critical physical states, e.g. the pressure in a chemical reactor. In control engineering the measured DSM can be used in order to optimize or to adapt a controller during system operation.

Here, the DSM concept is generalized for safety-critical computer systems as a measure of how far a system is away from the critical state. Using an input-output description of the system, all safety-critical physical states must be accessible from outside the system or subsystem measured by the output value y. Similar to the performance acceptability a safety acceptability factor can be derived utilizing the DSM normalized to specified maximum deviation of the output value y_S.

We propose:

$$A_{safety,k} = \exp\left(-\left\| \frac{\delta_k}{y_s} \right\|^2 \right), \qquad \textbf{(11)}$$

For dynamic systems with additional noise the DSM concept can be treated like the reliability concept, if we replace the maximum allowed deviation of the system output by the DSM. Thus the probability of reaching a critical state can be determined.

Illustrative Example

In order to illustrate the concept of dependability measure a simple heating control system is described in this section. The heating system consists of a radiator, a switching controller and a temperature sensor. The controller gets the desired temperature y_r from the input and the actual temperature y from the sensor. If the difference of both temperatures leaves a specified range the controller switches the radiator ON ($u_k=1$) or OFF ($u_k=0$) corresponding to the control law:

```
initial value OFF
if (yr(k)-y(k))>0.1 && OFF than ON;
if (yr(k)-y(k))<-0.1 && ON than OFF;
```

The radiator temperature has an input-output behaviour corresponding to a first order system (low pass) with a time constant of 2300 s yielding the time-discrete transfer function

$$y_{k+1} = 0.9996 \cdot y_k + 0.3 \cdot u_k + 0.03 \cdot v_k \qquad \textbf{(12)}$$

with the system input u_k (power in watt) and the output y_k (°C), normal distributed white noise v_k, and the sample period Δt. For simplification the index k is used for all variables instead of $k\Delta t$, i.e. $y_k = y(k\Delta t)$. The specified deviation is $\sigma_0 = 0.15$°C. The maximum absolute temperature is $y_{max} = 40$°C. As a test trajectory a biased sinusoidal input is applied with $y_{r,k}=38.5°C+\sin(2\pi \cdot 0.001 \cdot k\Delta t)$, m=1000, $k = 0..m$, $\Delta t = 1$s, and initial output value $y_0 = 38$°C.

The acceptability functions are defined according to (**3**), (**7**), and (**11**) with $y_p=6\sigma_0$, $y_s=\sigma_0$, $\delta=y- y_{max}$. The dependability of dimension d=3 is defined according to (**1**) with the acceptability functions $A_1=A_{performance}$, $A_2=A_{safety}$, $A_3=A_{reliability}$, and weighting $a_1=0.3$, $a_2=0.4$, $a_3=0.3$.

The unacceptability of the reliability factor (α-value) depends on the number of samples taken. In the test case n = 100 samples are taken from independent runs, for one special instance of time. Corresponding to the low-pass behaviour of our system, the output deviation values are correlated in the short time range, leading to smaller s values. In order to get uncorrelated samples, the system relaxation time must be awaited before the samples are taken. The time-dependent α-values are shown in table 2, which increase with time.

Table 2: Sample of the time-dependent standard deviation of the system output and α-value for n = 100.

t (s)	s (°C)	α
10	0.1021	7.9134e-005
100	0.1029	9.6890e-005
1000	0.1047	1.5333e-004

The actual output and the reference output are shown in fig. 3a). The actual output has a noticeable noise in addition to the reference value. Correspondingly, performance acceptability fig. 3b), blue line, is also noisy and the corresponding cumulative function fig. 3b), green line, increases with number of samples accumulated.

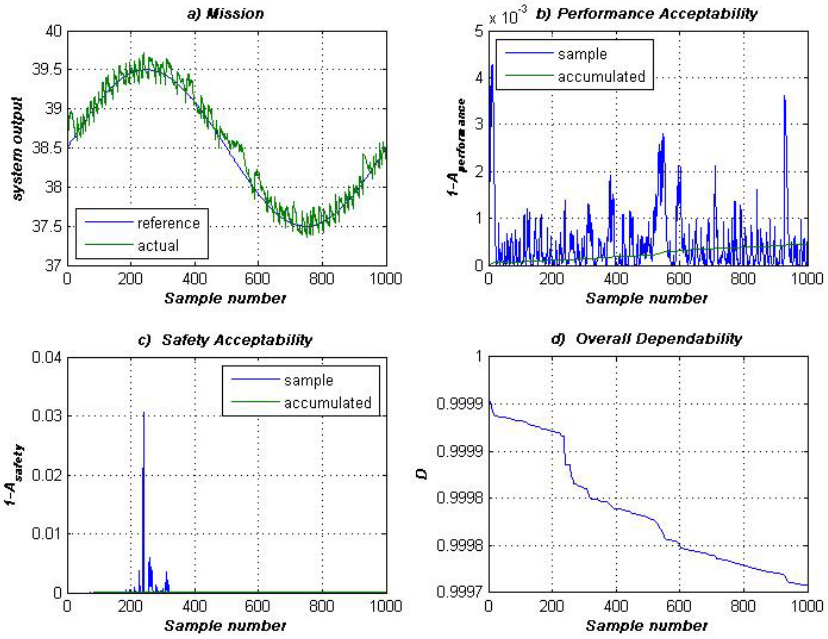


Fig. 3. a) System reference output (green line) and actual output (blue line); **b)** Performance (un)acceptability (blue line) and cumulative value (green line); **c)** Safety (un)acceptability (blue line) and cumulative value (green line); **d)** Overall system dependability.

Fig. 3c) shows the safety acceptability which has peak values in the sample range n=300..400. Within this range the system output has the minimum distance to the maximum system output (see fig. 3a). The overall dependability is plotted in figure 3d). It is obvious that the dependability decreases monotonically. The maximum slope is in the range where the weighted sum of all acceptability terms reaches its maximum as well. Therefore, the peaks in the safety function are visible as strong decreases of dependability.

Conclusion

In this paper an Integrated Dependability Measure (IDM) for dynamic systems was proposed combining acceptability factors for different dependability relevant system properties. The approach is based on a behavioral system description which generalizes diverse system descriptions techniques from different disciplines, e.g. systems, hardware and software engineering, human factor engineering. The measure is suitable for stochastic as well as for non-stochastic system models and related properties. The measure is a functional of the specified behavior represented by the reference output trajectory, the actual behavior represented by the actual output trajectory and a specified mission represented by a test input trajectory. Furthermore criteria are defined by which the system can be validated. Thus, the dependability

measure does not describe the system behavior directly, but how much it deviates from the expected behavior.

The simulation example shows that using the dependability measure (1) the input-output behavior of a system can be validated against its specifications in relation to dependability requirements. As a special case, reliability metrics can also be included in the measure. Considering dynamic systems we have to project the system trajectory by reducing the time dimension to one single value in order to obtain stationary reliability values. Additionally, a method is proposed to validate the reliability by comparing the distribution of output values with a defined probability density function. This approach reduces the number of required samples significantly, which is necessary for a practical application. In this case, the absolute value of the failure probability is not required. In contrast, the deviation of the reliability from the specified value is measure indirectly. This also enables new testing methods to be used. In the future, the unified dependability measure will be applied and evaluated for additional systems covering typical examples of human factor engineering.

References

[1] Laprie, J. C.: Dependability: Basic Concepts and Terminology. Ed. Springer, (1992).

[2] Avizienis, A. , Laprie, J.-C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. on Dependable and Secure Computing, 1 (1):11–33, (2004).

[3] Walter, M., Schneeweiss, W.: The Modeling World of Reliability/Safety Engineering. LiLoLe-Verlag GmbH, Hagen, Germany, (2005).

[4] Rakowsky, U. K.: System-Zuverlässigkeit, Hagen/Westfalen: LiLoLe-Verlag, Paperback, ISBN 3-934447-22-8, (2002).

[5] Rüdiger, J., Wagner A., Badreddin E.: Behavior Based Definition of Dependability for Autonomous Mobile Systems, in Proc. of the European Control Conference 2007, Kos, Greece, July 2-5, 2007, WeD11.4, (2007).

[6] Siewiorek, D. P., Swarz, R. S.: Reliable Computer Systems: design and evaluation. 3rd ed., A K Peter Ltd. Massachusetts, USA, (1998).

[7] Atkinson, C., Brenner, D., Falcone, G., Juhasz, M.: Specifying High-Assurance Services. IEEE Computer, vol. 41, no. 8, pp. 64-71, (2008).

[8] Atkinson, C., Barth, F., Falcone, G.: Measuring the Dependability of Dynamic Systems using Test Sheets, Workshop on the Design of Dependable Critical Systems, Hamburg, (2009).

[9] Weber, H.: Einführung in die Wahrscheinlichkeitsrechnung und Statistik für Ingenieure. Teubner, Stuttgart, ISBN 3-519-02983-9, (1992).

[10] Ehrenberger, W.: Software Verifikation: Verfahren für den Zuverlässigkeitsnachweis von Software, Carl Hanser, München Wien, ISBN 3-446-21624-3, (2002).

[11] Badreddin, E., Abdel-Geliel, M: Dynamic safety margin principle and application in control of safety critical systems. International Conference on Control Applications, volume 1, pages 689–694, Vol.1, 2-4, (2004).