We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

4,800
Open access books available

122,000
International authors and editors

135M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS BOOK CITATION INDEX INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

22

Dependability of Autonomous Mobile Systems

Jan Rüdiger, AchimWagner and Essam Badreddin
Automation Laboratory, Dept. Mathematics & Computer Science,
University of Heidelberg Mannheim,
Germany

1. Introduction

Computer systems pervade more and more our everyday life. They are found in workstations, mobile devices and in nearly every device - from consumer products such as coffee-machines to safety critical automotive systems such as cars, industrial production-lines etc. Due to increasing complexity, the controllability of such systems is a serious problem,while impacts and consequences on our daily life are continuously increasing. Therefore, non-functional system properties like dependability became a crucial factor within the computerized product design process. Although common unformal ideas in terms of dependability exist, a formal definition for dependability is still missing. One reason may be the historical growth of the definition of the term dependability, which has been added incrementally by a number of attributes. In the 40ies of the last century, the first computer based on vacuum tube technology with huge failure probabilities (in the ENIAC computer tubes failed every 7 minutes) were constructed, reliability became an issue. Due to increased interaction with the systems later on in the 60ies availability became even more important. Related to the requirements of controlling safety critical plants like nuclear power stations or space crafts the safety property of computer systems where getting into the focus during the 70ies. Internet connectivity, data bases and mobile services were the reason why security, integrity and maintainability have been added to the dependability concept. The state-of-the-art assessment of dependability is based on a binary fault model, which describes components on an operable – not operable basis and a logical error propagation using fault trees, event tress or binary block diagrams (Vesely et al., 1981). Modern approaches like Markov-Chain models (Flammini, 2006) or Stochastic Petri Nets (Filippini & Bondavalli, 2004) capture the time dependent probability of a combination of error states within a system. However, they are not able to detect the origin of an error resulting from the system dynamics. For instance, a light bulb mostly crashes during the switching on phase and not during stationary operation. This error scenario cannot be reflected by pure probabilistic modelling.

A further disadvantage of pure probabilistic models is that they are more or less decoupled from the original behaviour of the system. Thus, finding a valid fault model which starts from the functional model of the system is up to the design engineer. However, even a fault probability equal to zero does not guarantee, that systems operate according to what users expect because the requirements on the dynamic system behaviour are not modelled. Dependability is more than a collection of attributes related to a probabilistic – but static – error description.

Source: Robotics, Automation and Control, Book edited by: Pavla Pecherková, Miroslav Flídr and Jindřich Duník,
ISBN 978-953-7619-18-3, pp. 494, October 2008, I-Tech, Vienna, Austria

This is particularly important when dealing with autonomous or semi-autonomous systems. With an increasing degree of autonomy and safety requirements, requirements for dependability increase. Hence, being able to measure and compare the dependability of a system becomes more and more vital. Since autonomous mobile systems are often described by their behaviour, it is straightforward to also define the dependability of such systems in a behavioural context. To show the link between conventional approaches and to allow the usage existing tools, the proposed dependability model is supplemented by the majority of the dependability attributes described above. The proposed approach of a behaviour based definition for dependability described in this chapter is focused on autonomous mobile systems. Nevertheless, the ideas behind it are more general.

2. Basics of dependable systems

According to (Candea, 2003) a general notion of what dependability is usually understood is summarizes as follows:

> turn your homework in on time, if you say you'll do something then do it, don't endanger other etc.

Computer controlled systems, in our case autonomousmobile systems, do, however, not understand these vague concepts. When it comes to machines we need amore precise understanding and definition of dependability. If system dependability must be expressed and measured in numbers, a formal definition is even more important. This definition must be mostly system-independent in order to have the opportunity to compare the dependability between different systems. Finally, this definition must agree with the general notion of dependability.

This chapter gives a broad overview of what is usually understood under the term *dependability* and discusses the sometimes different definitions of dependability used throughout literature. Based on the aforementioned and in combination with a behavioural system description, a dependability definition for autonomous mobile systems is proposed.

Non-functional properties reflect the overall quality of a system. Beside performance, robustness, usability etc., dependability is getting amore important non-functional system requirement. The general, qualitative, definitions for *dependability* used so far in literature are presented and discussed in the following. The most frequently cited definitions of dependability are the ones introduced by Carter and Laprie which are presented here together with others in chronological order.

Carter (Carter, 1982): A system is dependable if it is trustworthy enough that reliance can be placed on the service it delivers.

Laprie (Laprie, 1992): Dependability is that property of a computing system which allows reliance to be justifiably placed on the service it delivers.

Badreddin (Badreddin, 1999): Dependability in general is the capability of a system to successfully and safely fulfill its mission.

Dubrova (Dubrova, 2006): Dependability is the ability of a system to deliver its intended level of service to its users.

All four definitions have in common that they define dependability on the service a system delivers and the reliance that can be placed on that service. The service a system delivers is the behaviour perceived by the user, which can also be called the *mission of the system*.

Only few further definitions, following the idea of the definitions presented above exist. Among them, the dependability definition of the International Electrotechnical Commission (IEC) ("IEC 60050, IEV 191-02-03: Dependability and quality of service - Part 1: Common terms" see IEC, 1990)[1], the definition from the IFIP 10.4 Working Group on Dependable Computing and Fault Tolerance (see International Federation for Information Processing,) and the definition from the Department of Defence (see Department of Defence, 1970).
These classical definitions of dependability do, however, offer two major drawbacks:

1. They do not define a directly applicable and repeatable way to compute the dependability of a system.[2]
2. The dynamics of the system are not directly taken into account when investigating the dependability of the system. Using the information gained from the mathematical system model, for example, seems obvious when investing the dependability of that system. Neglecting the dynamics of a system means ignoring all information coming from that model. Furthermore the dynamics of a system is crucial for fault scenarios not only in the case of autonomous mobile systems.

In this chapter a theoretical framework is proposed, that does not only describe a dependability definition and dependability means in relation to the dynamics of a system but also presents a repeatable and system-independent way of how to measure dependability.
Dependability is mainly understood as an integrated concept that additionally consists of different attributes (see also Figure 1). According to (Avizienis et al., 2004b; Avizienis et al., 2004a; Randell, 2000) dependability consists of the following attributes:

- **Availability** readiness for correct service,
- **Reliability** continuity of correct service,
- **Safety** absence of catastrophic consequences for both user(s) and environment,
- **Confidentiality** absence of unauthorized disclosure of information,
- **Integrity** absence of improper system state alteration and
- **Maintanability** ability to undergo modifications and repairs.

For further information as to the impact of these attributes on the dependability of the complete system, please refer to (Avizienis et al., 2004a) and (Dubrova, 2006).
Further definitions with slightly different attributes exist in the literature (see i.e. Candea, 2003; Dewsbury et al., 2003). The main idea, i.e. dependability consists of different attributes, is still of value and will be part of the definition proposed below.
The authors would like to express, however, that more than a static aggregation of attributes is needed for the description of the dependability of an autonomous mobile system. These attributes are always related to a static model, even if error propagation is dynamic. The proposal for dependability measurement also includes the attribute approach as a special case for being compatible with the qualitative dependability definitions.
Unfortunately a few of the attributes have different, not necessarily similar, definitions. Still missing is a formal and comprehensive definition for a few attributes.
As for autonomous mobile systems, not all attributes are of equal importance. For a discussion about the set of attributes important for autonomous mobile systems the reader is referred to (Rüdiger et al., 2007b).

---

[1] This definition of dependability is often referred to as ISO 1992 or IEC 50(191)
[2] According to IEC norm the definition is ,,used only for general descriptions in non-quantitative terms"

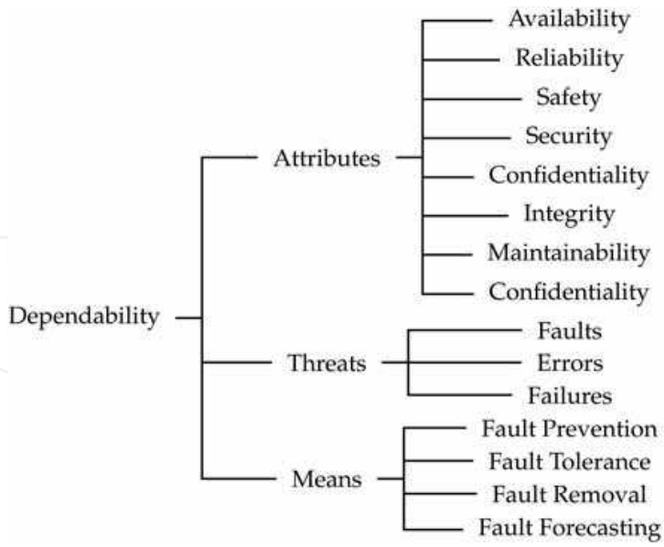


Figure 1. The Dependability Tree

3. Framework for a theory of dynamical systems

In order to develop a formal definition for the dependability of autonomous mobile systems, first of all the following terms

- service,
- system,
- and reliance

mentioned in the non-formal definitions need a mathematical description. Therefore, a formal, mathematical, theory that is capable of describing these terms is needed.

There are different techniques to describe a system mathematicely, that is modeling a system. Among them, the state-space approach can be mentioned, where a system is modelled by a set of input, output and state variables related by first order equations (time domain), and, for example, the frequency domain approach. Another approach is the *Behavioural Modelling* approach (see Willems, 1991) where a system is modelled only by describing its behaviour.

Since the service a system delivers is the behaviour as it is perceived by the user, the later modelling technique was used and is shortly introduced in the following. Additionally, the behaviour based approach is quite common in the field of autonomous mobile robots. This goes back to 1980 where Rodney Brook introduced his subsumption architecture (see Brooks, 1986). Finally, the behavioural modeling approach offers the opportunity to modell the complete system including both environment and user.

Willems (Willems, 1991) defines a system in a universum $\mathbb{U}$. The elements of $\mathbb{U}$ are called outcomes of the system. A mathematical model of a system from a behavioural or black-box point of view claims that certain outcomes are possible, while others are not. The model thus defines a specific subset $\mathsf{B} \subset \mathbb{U}$. This subset is called the *behaviour* of the system. Subsequently, a (deterministic) mathematical model of a system is defined as:

Definition 3.1 A mathematical model *is a pair* $(\mathbb{U}, \mathsf{B})$ *with the universum* $\mathbb{U}$ *- its elements are called* outcomes *- and* B *the behaviour.*

Given the above definition of a mathematical model, a dynamical system is a set of trajectories describing the system behaviour during the time instants of interest in its signal space $\mathbb{W}$.

In contrast to the state space representation, like $\dot{x} = f \circ x$, a dynamical system is defined as:
Definition 3.2 A dynamical system Σ *is a triple* $\Sigma = (\mathbb{T}, \mathbb{W}, \mathsf{B})$ *with* $\mathbb{T} \subseteq \mathbb{R}$ *the time axis,* $\mathbb{W}$ *the signal space, and* $\mathsf{B} \subseteq \mathbb{W}^{\mathbb{T}}$ *the behaviour.*
In the above definition a dynamical system is described by a period of time $\mathbb{T}$, the signal space $\mathbb{W}$ and a set of time trajectories B. The behaviour of a dynamic system is described by a subset B of all possible time trajectories $\mathbb{T} \Rightarrow \mathbb{W}$. For a trajectory (an event) $w : \mathbb{T} \rightarrow \mathbb{W}$ the following applies:

- $w \in \mathsf{B}$ the model allows the trajectory w
- $w \notin \mathsf{B}$ the model forbids the trajectory w

The reader is referred to (Willems, 1991) for examples of this modeling technique.

4. Behaviour-based dependability of autonomous mobile systems

As stated earlier, the service a system delivers is the behaviour as it is perceived by the user. A framework for a mathematical system description according to its behaviour was introduced in the last section.
So far the system and its service, from the dependability definition, can be mathematical described. What remains is a fundamental definition of the *service a system should deliver* and an additional description of the *reliance*, in terms of the service offered, in the given framework. Finally the attributes of dependability as discussed in section 2 need to be defined in the framework (see also Rüdiger et al., 2007a).

4.1 Behaviour and mission of autonomous mobile systems

As afore mentioned, the behaviour of a system is the set of all possible time trajectories of its external states (see section 3). Due to limitations, either deliberately, caused by a fault in the system, or changes in the environment, this set B could be slightly changed or reduced to a set of behaviours actually available to the system. Although it will probably be only a subset of the behaviours of the original system. This set, which may vary over time, will be defined as follows:
Definition 4.1 *Let* $\Sigma = (\mathbb{T}, \mathbb{W}, \mathsf{B})$ *be a dynamical system then* $\mathbb{B} \subseteq \mathbb{W}^{\mathbb{T}}$ *is called the set of* available behaviours $w_i(t) : \mathbb{T} \rightarrow \mathbb{W}$, $i = 1...n$ *to the system at time t.*
Again, the set $\mathbb{B}$ is a set of time trajectories within the original signal space $\mathbb{W}$. For the set $\mathbb{B}$ it must not necessarily apply $\mathbb{B} \subset \mathsf{B}$ since it can also contain trajectories as a result of a fault in the system or a change in the environment not previously modelled. The set $\mathbb{B}$ may also vary over time.
Additionally, the set $\mathbb{B}$ must not cover all trajectories from the set B since due to implementation reasons not all possible trajectories must be available to the system.
Autonomous mobile systems are usually build as general purpose machines that handle different tasks. In the following, these tasks will also be called missions. For estimating the dependability of an autonomous mobile system it is, however, not important to handle all kinds of missions dependable, but only the mission in terms of the *service the system should deliver* or what the system is *intended* to do. Such missions are be defined as:
Definition 4.2 (Mission) Let $\Sigma = (\mathbb{T}, \mathbb{W}, \mathsf{B})$ be a time-invariant dynamical system. We say the mission w_m of this system is the map $w_m : \mathbb{T} \rightarrow \mathbb{W}$ with $w_m \in \mathsf{B}$.

Note that even if an autonomous mobile system is usually build for the handling of different tasks, the actual mission the system has to accomplish is defined as only one special behaviour from the set B.
Thus, the mission, here defined, is just a special trajectory or, more precisely, a special behaviour in B. *Weak controllability* (see Hermann, 1977) is assumed since it does not make any sense to define a mission to a system which by definition is not able to accomplish it.
If the system is capable of fullfilling its mission w_m is defined as follows:
Definition 4.3 *A mission* $w_m \in \mathsf{B}$ *for a given dynamical system* $\Sigma = (\mathbb{T}, \mathbb{W}, \mathsf{B})$ *with the behaviours* $\mathbb{B}$ *is said to be* accomplishable *by this system if for all* $w_1 \in \mathsf{B}$ *there exists a* $t \in \mathbb{T}$, $t \geq 0$, *a behaviour* $w \in \mathbb{B}$, $w : \mathbb{T} \cap [0, t] \rightarrow \mathbb{W}$ *and a behaviour* $w_2 \in \mathbb{B}$ *such that* $w' \in \mathsf{B}$, *with* $w' : \mathbb{T} \rightarrow \mathbb{W}$ *defined by*:

$$w'_{(t')} = \begin{cases} w_{1(t')} & \text{for } t' < 0 \\ w_{(t')} & \text{for } 0 \leq t' \leq t \\ w_{2(t'-t)} & \text{for } t' > t \end{cases}$$

and

$$w'_{(t')} = w_m \quad \text{for } t' > t$$

Based on the definition of controllability according (Willems, 1991) a mission w_m is accomplishable if the system can be steered from any past trajectory (light green trajectory in Fig. 2) to the beginning of the mission trajectory w_m (black trajectory in Fig. 2) and can then be steered along the mission trajectory (red and blue trajectories in Fig. 2).

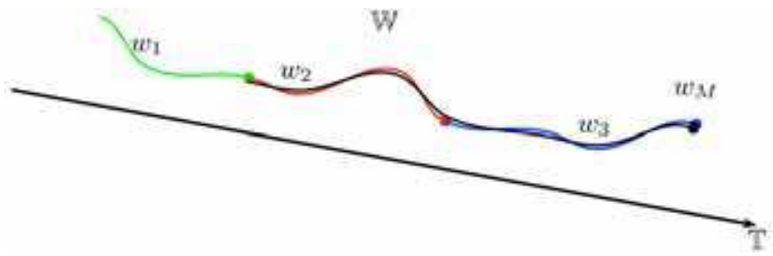


Figure 2. A mission (black line) is accomplished by steering the system to the mission trajectory by behaviour w_1 and subsequently by steering along the mission trajectory with behaviours w_2 and w_3

4.2 Behaviour based attributes of dependability

Before continuing with the definition of dependability for autonomous mobile systems, the basic attributes of dependability must be defined in a behavioural context. Only the main important attributes for dependability of autonomous mobile systems are introduced. Please refer to (Rüdiger et al., 2007a) for an advanced description and (Rüdiger et al., 2007b) for the subset of attributes needed for measuring the dependability of autonomous mobile systems.

4.2.1 Reliability

A common (see e.g. Dubrova, 2006) unformal definition for reliability is:

> Reliability $R|_t$ is the probability that the system will operate correctly in a specified operating environment in the interval $[0, t]$, given that it worked at time 0.

An autonomous system is, thus, said to be reliable if the system state does not leave the set of admissible trajectories B. The reliability of a system can be defined as:

Definition 4.4 *Let* $\Sigma = (\mathbb{T}, \mathbb{W}, \mathsf{B})$, $\mathbb{T} = \mathbb{Z}$ *or* $\mathbb{R}$, *be a time-invariant dynamical system. The system is said to be* reliable *in the period* $[0, t]$ *if for all* $0 \le t_1 \le t$ *the system state is* $w(t_1) \in \mathsf{B}$. *Correspondingly, the* reliability *of the system is the probability that the system is reliable.*

4.2.2 Availability

Availability is typically important for real-time systems where a short interruption can be tolerated if the deadline is not missed.

> Availability $A|_t$ is the probability that a system is operational at the instant of time t.

In contrast to reliability the availability is defined at a time instant t while the reliability is defined in a time interval.

Definition 4.5 *Let* $\Sigma = (\mathbb{T}, \mathbb{W}, \mathsf{B})$, $\mathbb{T} = \mathbb{Z}$ *or* $\mathbb{R}$, *be a time-invariant dynamical system. The system is said to be available at time t if* $w(t) \in \mathsf{B}$. *Correspondingly, the availability of the system is the probability that the system is available.*

4.2.3 Safety

From the reliability point of view, all failures are equal. In case of safety, those failures are further divided into *fail-safe* and *fail-unsafe* ones. Safety is reliability with respect to failures that may cause catastrophic consequences. Therefore safety is unformaly defined as (see e.g. Dubrova, 2006):

> Safety $S(t)$ of a system is the probability that the system will either perform its function correctly or will discontinue its operation in a fail-safe manner.

For the formal definition of safety an area S is introduced, as in (Badreddin & Abdel-Geliel, 2004), which leads to catastrophic consequences when left. In the latter case it is, however, assumed that this *Dynamic Safety Margin* is fully contained in the stability region while S is defined to be around B. This margin is, like B, highly system specific, but can be set equal to B in the case of restrictive systems.

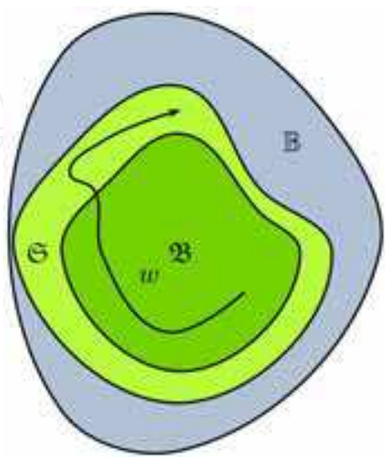


Figure 3. Safety: The system trajectory w leaves the set of admissible trajectories B but is still considered to be safe since it remains inside S

Definition 4.6 *Let* $\Sigma = (\mathbb{T}, \mathbb{W}, \mathsf{B})$, $\mathbb{T} = \mathbb{Z}$ *or* $\mathbb{R}$, *be a time-invariant dynamical system with a safe area* $\mathsf{S} \supseteq \mathsf{B}$. *The system is said to be* safe *if for all* $t \in \mathbb{T}$ *the system state* $w(t) \in \mathsf{S}$.
This definition is consistent with the idea that a safe system is either operable or not operable but in a safe state.

4.3 Behaviour based dependability

Having defined the behaviour of a system and the mission, which corresponds to the service the system should deliver, the dependability of the system can be defined as:
Definition 4.7 *A time-invariant dynamical system* $\Sigma = (\mathbb{T}, \mathbb{W}, \mathsf{B})$ *with behaviours* $\mathbb{B}$ *and a mission* $w_m \in \mathsf{B}$ *is said to be (gradually)* dependable *in the period* $T \in \mathbb{T}$ *if, for all* $t \in T$, *mission* w_m *can be (gradually) accomplished.*

5. Behaviour based dependability measure

The basic idea behind the dependability measure proposed in the last section is to define the dependability based on the behaviour of the system. For this purpose, a desired behaviour, which was called mission $w_m(t)$, was defined for a system and the dependability measure was proposed to be depending on the total of deviation between the actual system behaviour $w(t)$ and the desired behaviour $w_m(t)$. In order to be able to actually measure the dependability this definition must, however, be more sophisticated.

5.1 Requirements for a dependability measure

Before proposing a function for measuring the dependability the characteristics this dependability function should posses are introduced. In the following, the function for the dependability will be called D.

- $\mathsf{D}(t)$ should be a continuous time-dependent function
- $\mathsf{D}(t)$ should be positive, strictly monotone decreasing
- $\mathsf{D}(t)$ should be normalized between 0 and 1, where 1 means dependable and 0 means not dependable
- $\mathsf{D}(t)$ should be a dimensionless quantity

The dependability must be measured during and after the mission, hence the dependability measure $\mathsf{D}(t)$ must be a time dependant function.
The normalization and the non-dimensionalization is obvious in order to achieve a system and unit independent measure. The limitation to the domain between 0 and 1 was chosen so that dependability measure is comperable between different system and application domains.
$\mathsf{D}(t)$ should be strictly monotonic decreasing since a system is less dependable, i.e. un-dependability is more likely to occur, the longer a system runs.

5.2 Definition of dependability measure

The system trajectory $w(t)$ is the evolution of the system state. The distance between this trajectory and the mission $w_m(t)$, together with the distance to the safety area S will be the main idea of the measure for dependability.
After the system Σ has completed its mission, the overall mission deviation D_m of system and its mission w_m is proposed as the sum of all deviations $\varepsilon^2(w(t), w_m(t))$. In the following,

the functional $\varepsilon^2(w(t),w_m(t))$ will be abbreviated as $\varepsilon^2(t)$. Thus, the overall mission deviation can be defined as:

$$D_m = \int_0^{t_m} max_\tau(\varepsilon(\tau)^2)d\tau - \int_0^{t_m} \varepsilon^2(\tau)d\tau \quad (1)$$

Where $\varepsilon^2(t)$ is an appropriate measure of the deviation between mission trajectory w_m and system trajectory w and consequently a combination of different distance measurements, including the distance to the safety area S. The term $max_\tau(\varepsilon(\tau)^2)$ represents the maximum deviation during this particular mission. Those distance measurements will be discussed in detail in the following.

More important than knowing the system dependability after completion of the mission is knowing the dependability during the mission. At time, t the time dependent overall mission deviation $D(t)$ can be measured by means of

$$D(t) = \int_0^{t_m} max_\tau(\varepsilon^2(\tau))d\tau - \int_0^{t} \varepsilon^2(\tau)d\tau \quad (2)$$

Note that the integration limits for the second integral changed from (1) to (2).

In order to calculate $D(t)$ during the mission an estimation for $max_\tau(\varepsilon^2(\tau))$ must be used. This value depends on the distance function $\varepsilon^2(t)$ used and will be discussed together with the calculation of $\varepsilon^2(t)$ in the following.

Furthermore,

$$\int_0^{t_m} max_\tau(\varepsilon^2(\tau))d\tau$$

in (1) and (2) assures that the function for the time dependent overall deviation D is a positive function.

The problem with this function for $D(t)$, is that, besides that it is unnormalized, $D(t)$ is equal to zero if there is no deviation between the desired trajectory $w_m(t)$ and the actual system trajectory $w(t)$. Hence, in this case, the dependability derived from this function would be zero.

5.3 Non-dimensionalization and normalization

Nondimensionalization is a technique for partial or full removal of units from a mathematical equation by a suitable substitution of variables. Normalization bounds the domain of a mathematical function to a given range of values.

Function v with its codomain $[o_{min}..o_{max}]$ can be normalized to a function v' with its co-domain $[n_{min}..n_{max}]$ by the following formula:

$$v' = \frac{v - o_{min}}{o_{max} - o_{min}} \cdot (n_{max} - n_{min}) + n_{min} \quad (3)$$

For the time dependent overall mission deviation (2) the value for o_{min} is:

$$o_{min} = 0 \quad (4)$$

The dependability function, as stated in the introduction to this chapter, should have a co-domain of [0..1], consequently the values for n_{min} and n_{max} should be:

$$n_{min} = 0 \tag{5}$$

and

$$n_{max} = 1 \tag{6}$$

With these values the normalization function is reduced to:

$$v' = \frac{v}{o_{max}} \cdot (n_{max}) = \frac{v}{o_{max}} \tag{7}$$

The value o_{max} for the unnormalized dependability D can be set to

$$o_{max} = \int_0^{t_m} max_\tau(\varepsilon^2(\tau))d\tau \tag{8}$$

If at least one $\varepsilon^2(t) > 0$ for $t \in [0..t_m]$ the normalized dependability $\mathbb{D}(t)$ can be computed from (2) with (7) and (8) to:

$$\begin{aligned} \mathbb{D}(t) &= \frac{\int_0^{t_m} \max_\tau(\varepsilon^2(\tau))d\tau - \int_0^t \varepsilon^2(\tau)d\tau}{\int_0^{t_m} \max_\tau(\varepsilon^2(\tau))d\tau} \\ &= \frac{\int_0^{t_m} \max_\tau(\varepsilon^2(\tau))d\tau}{\int_0^{t_m} \max_\tau(\varepsilon^2(\tau))d\tau} - \frac{\int_0^t \varepsilon^2(\tau)d\tau}{\int_0^{t_m} \max_\tau(\varepsilon^2(\tau))d\tau} \\ &= 1 - \frac{\int_0^t \varepsilon^2(\tau)d\tau}{\int_0^{t_m} \max_\tau(\varepsilon^2(\tau))d\tau} \end{aligned} \tag{9}$$

Nevertheless, the problems with this function are:

1. It only exists if at least one $\varepsilon^2(t) > 0$ for $t \in [0..t_m]$. In other words, it only exists if at least a small deviation between the desired behaviour w_m and the actual behaviour w occurred.
2. It is subject to the calculation of $\varepsilon^2(t)$. Thereby $\max_\tau(\varepsilon^2(\tau))$ cannot be estimated in advance and dependability cannot be computed during the mission.

To finally overcome both problems, a system-independent way for computing $\varepsilon^2(t)$, which is additionally normalized between [0 . . . 1], is proposed.
Having this, $\max_\tau(\varepsilon^2(\tau))$ can be estimated equal to 1 and

$$\int_0^{t_m} \max_\tau(\varepsilon^2(\tau))d\tau \tag{10}$$

can be estimated to

$$\int_0^{t_m} \max_\tau(\varepsilon^2(\tau))d\tau = \int_0^{t_m} 1d\tau = \tau|_0^{t_m} = t_m$$

This finally leads to the desired system independent, normalized function $\mathsf{D}(t)$ of dependability. D can now be computed from (9) to:

$$\mathfrak{D}(t) = 1 - \frac{1}{t_m} \int_0^t \varepsilon^2(\tau) d\tau \tag{11}$$

If a systemindependent way to compute $\varepsilon^2(t)$ between [0 . . . 1] exists this function for the dependability posses all required properties stated at the beginning of this chapter.

5.4 Computing $\varepsilon^2(t)$

For computing the elements of $\varepsilon^2(t)$ it is not only important to address the distance between the system state and the mission trajectory but also to address the different dimensions of dependability such as reliability, availability, etc. For a behavioural definition of these attributes please refer to (Rüdiger et al., 2007a). Furthermore, the distance of the system state to the safe area S also needs to be taken into account.

Thus, $\varepsilon^2(t)$ usually consists of different elements reflecting the different attributes of dependability for this special system. From (2) and (9) it follows that if $\varepsilon^2(t)$ is a combination of different measures $\varepsilon_1^2(t)$ . . . $\varepsilon_n^2(t)$, D (*t*) is calculated

$$\mathfrak{D}(t) = 1 - \left(\frac{\int_0^t \varepsilon_1^2(\tau) d\tau + \cdots + \int_0^t \varepsilon_n^2(\tau) d\tau}{\int_0^{t_m} \max(\varepsilon_1^2)(\tau) d\tau + \cdots + \int_0^{t_m} \max(\varepsilon_n^2(\tau)) d\tau} \right) \tag{12}$$

$$= \left(\frac{\int_0^t \sum_{i=1}^n \varepsilon_1^2(\tau) d\tau}{\int_0^{t_m} \sum_{i=1}^n \max(\varepsilon_1^2)(\tau) d\tau} \right) \tag{13}$$

setting again $\max(\varepsilon_i^2(t)) = 1$, for $i = 1 \ldots n$, this can be reduced to:

$$\mathfrak{D}(t) = 1 - \frac{1}{t_m} \left(\frac{1}{n} \int_0^t \sum_{i=1}^n \varepsilon_i^2(\tau) d\tau \right) \tag{14}$$

As stated in the previous section, $\varepsilon_i^2(t)$ must be normalized and between be [0 . . . 1]. The corresponding function of $\varepsilon(t)$ must be chosen in such a way that 0 means dependable, i.e. the system state $w(t)$ follows exactly the mission trajectory $w_m(t)$, and 1 means not dependable.

In order to compute the different $\varepsilon_i^2(t)$ a special distance measure is proposed derived from the euclidian distance measure between two points $x = (x_1 \ldots x_n)$ and $y = (y_1 \ldots y_n)$

$$d(x, y) = |x - y| = \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}. \tag{15}$$

This measure is, however, not normalized and not necessarily between 0 . . . 1. In order to achieve the remaining two points, too, the following distance measure is proposed derived from (15):

$$\varepsilon^2(w(t), w_m(t)) = 1 - e^{-\frac{|w(t) - w_m(t)|}{w_{dev}}} \tag{16}$$

In (16) $w_m(t)$ is the desired (mission) behaviour and $w(t)$ the actual behaviour of the system. The parameter w_{dev} describes how severely a deviation from the mission trajectory influences the system's dependability. It must be chosen greater than zero and have the same dimension as $w(t)$. The lower w_{dev} is chosen the more a deviation from the desired behaviour is rated (see Fig. 4). The proposed distance measure is therefore dimensionless and normalized between [0 and 1].

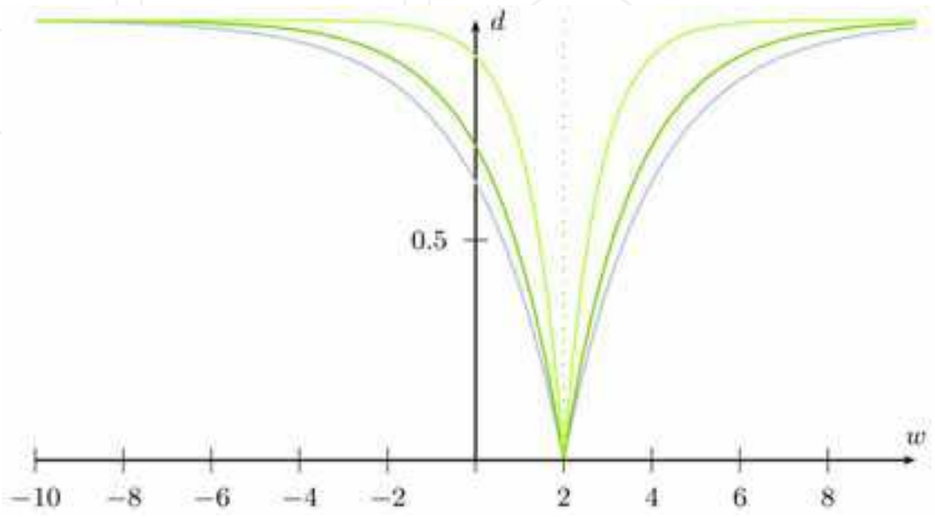


Figure 4. Example of the distance function to compute the different $\varepsilon_i(t)$ with $w_m = 2$ (dotted green line) and $w_{dev} = 1$ (blue), $w_{dev} = 0.8$ (green), and $w_{dev} = 0.4$ (light green)

As the euclidian distance measure, the proposed distance measure $\varepsilon^2(t)$ defines a metric over the space $\mathbb{W}$ since it satisfies all conditions for a metric which are:

1. $\varepsilon^2(x,x) = 0$, identical points have a distance of zero
2. $\varepsilon^2(x,y) = 0$ if and only if $x = y$, identity of indiscernible
3. $\varepsilon^2(x,y) = d(y, x)$, symmetry
4. $\varepsilon^2(x,y) \leq \varepsilon^2(x,z) + \varepsilon^2(z,y)$, triangle inequality

With the aid of this distance measure, the different attributes of dependability can be defined. For $\varepsilon_i^2(t)$ the corresponding euclidian distance measure $d_i(t)$ is used as a basis.

5.5 Mission deviation $\varepsilon_m^2(t)$

The mission deviation describes the normalized difference between the mission trajectory and the system state at time t. For this purpose the afore discussed distance measure is directly used with the euclidian distance d_m between the mission trajectroy and the system state. When evaluating the dependability $\varepsilon_m^2(t)$ is used in most of the dependability measure. The mission deviation $\varepsilon_m^2(t)$ is defined as

$$\varepsilon_m^2(t) = 1 - e^{-\frac{|w(t)-w_m(t)|}{w_{dev}}} \tag{17}$$

Again, $w_m(t)$ is the desired mission trajectory and $w(t)$ is the actual behaviour of the system as described in (16). See Fig. 5 for examples of $d_m(t)$.

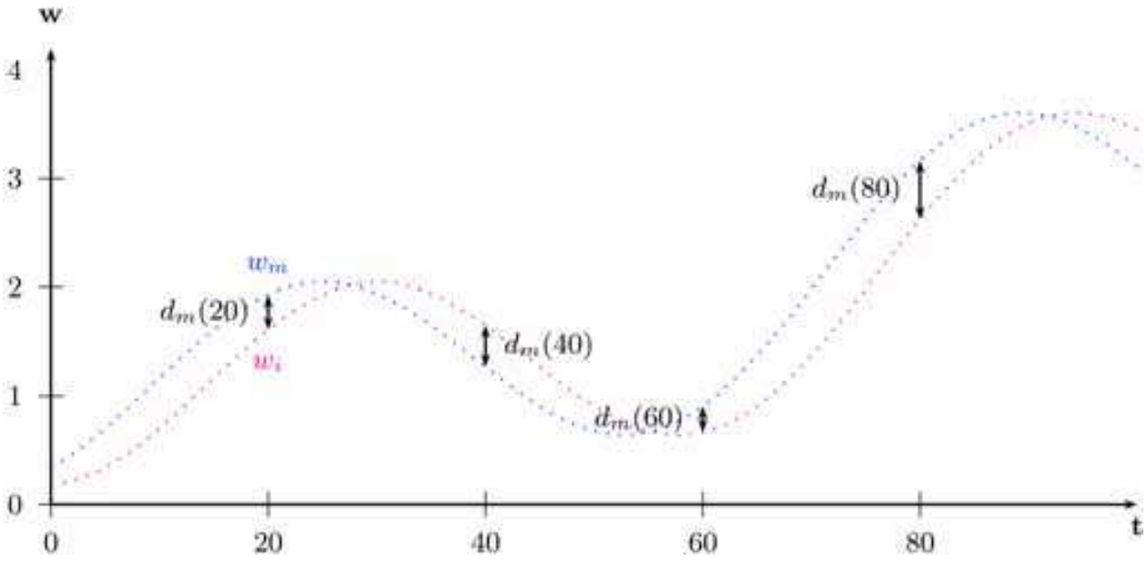


Figure 5. Mission trajectory $w_m(t)$ (blue) and system trajectory $w(t)$ (red) with examples for $d_m(t)$ at different timesteps.

5.6 Safety $\varepsilon_s^2(t)$

Beside the mission deviation $\varepsilon_m^2(t)$ is safety $\varepsilon_s^2(t)$ one of the most important elements of $\varepsilon^2(t)$. As proposed in Section 4.2.3 a safety area S is introduced which when left will lead to catastrophic consequences. The minimum euclidian distance between a system trajectory $w(t)$ and the border of the safety area S at time t will be taken as a basis for the measure of $\varepsilon_s^2(t)$. This distance is called $d_S(w(t))$ and will be abbreviated as follows

$d_S(t)$ for the minimum distance between the actual system states $w(t)$ and the border of the safety area and

$d_{Sm}(t)$ for the minimum distance between the mission trajectory $w_m(t)$ and the border of the safety are at time t.

Obviously $\varepsilon_s^2(t)$ should be 1 when $d_S(t) = 0$, equivalent to the distance between the system state and the safety area being zero.

To be able to adequately cover cases where the mission trajectory $w_m(t)$ itself could be close to the border of the safety area S, not the absolute distance between the actual system trajectory and the border of the safety area $d_S(t)$ is taken but the relative distance between the minimum distance of the actual systemtrajectory and the safety area $d_S(t)$ and the minimum distance of the mission trajectory $w_m(t)$ to the border of the safety area d_{Sm} is taken to compute $\varepsilon_s^2(t)$. Consequently, $\varepsilon_s^2(t)$ is proposed as:

$$\varepsilon_S^2(t) = 1 - e^{-abs\left(\frac{d_S(t)}{d_{Sm}(t)} - 1\right)} \tag{18}$$

Both, $d_S(t)$ and $d_{Sm}(t)$, are greater or equal to 0. The equation for $\varepsilon_s^2(t)$ is only defined for $d_{Sm}(t) \neq 0$. See Fig. 6 for examples for $d_S(t)$.

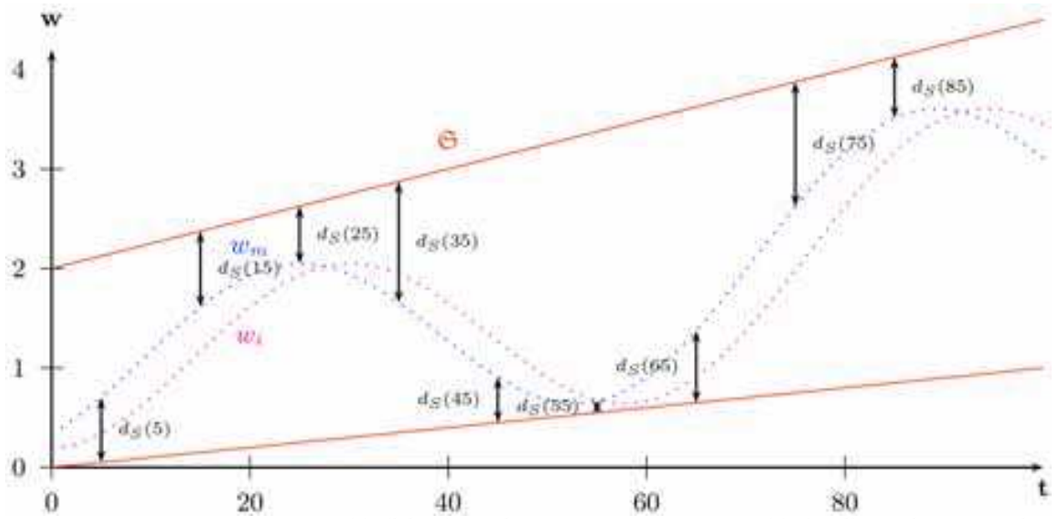


Figure 6. Mission trajectory $w_m(t)$ (blue) and system trajectory $w(t)$ (red) with examples for d_{Sm} the distance between the mission trajectory $w_m(t)$ and the boarder of the safety area S (read lines).

5.7 Timely mission accomplishment $\varepsilon_T^2(t)$

For a number of systems it is not only important that the system adequately follows the mission trajectory but that the system follows the mission trajectory at a given time. A good example for such systems is a heard-lung machine where it is not sufficient that the system gives the right pulses, they must be performed at given timesteps. Another important example, especially in the field of controlling autonomous mobile real-time systems, is the class of periodic behaviours, i.e. velocity control or collision avoidance. In the latter example, the exact time execution of a given behaviour is more important then the exact execution of the behaviour itself.

The calculation of $\varepsilon_T^2(t)$ is of course only possible if $w_m(t)$ is uniquely invertible. For periodic functions, often used on autonomous mobile systems, the uniquely invertible requirement of $w(t)$ can be simplified to a peacewise uniquely invertible requirement.

Let $w'_m(w) : \mathbb{T} \rightarrow \mathbb{W}^{\mathrm{T}}$ be the inverse function of $w_m(t)$ then $\varepsilon_T^2(t)$ is proposed as:

$$\varepsilon_T^2(t) = 1 - e^{-\frac{\left|t - w'_m(w)\right|}{t_{dev}}} \tag{19}$$

As in (16) and (17) the parameter t_{dev} describes how severe a deviation from the mission trajectory influences the dependability of the system. See Fig 7 for an example of $\varepsilon_T^2(t)$

5.8 Reliability $\varepsilon_R^2(t)$

As stated in section 2, reliability $R\,|_t$ describes the probability according to which the system will operate correctly in a specified operating environment in an interval [0, t]. For $\varepsilon_R^2(t)$ this means that $1 - R\,|_t$ describes the probability that the system will fail in the interval [0...t]. Setting $t = t_m$ the latter probability can be directly used and thus $\varepsilon_R^2(t)$ is proposed as:

$$\varepsilon_R^2(t) = 1 - R|_t \tag{20}$$

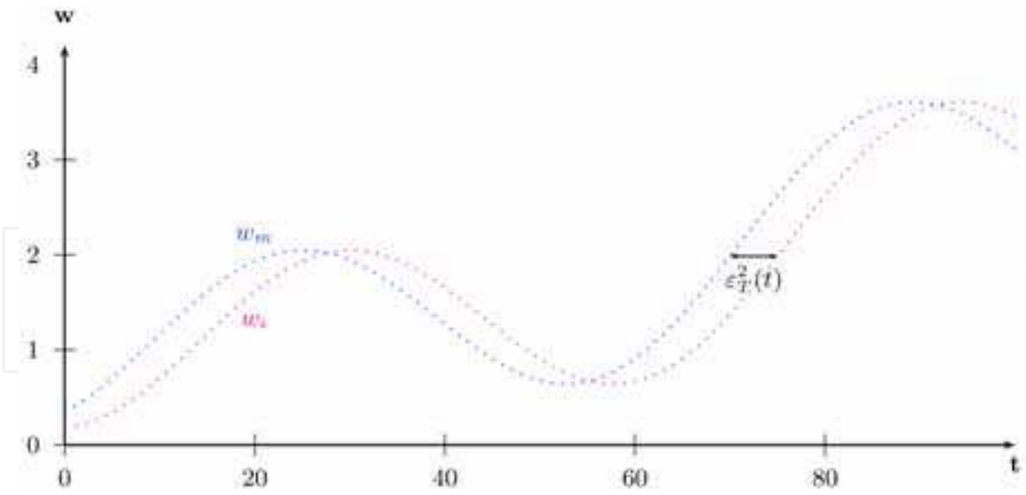


Figure 7. Mission trajectory $w_m(t)$ (blue) and system trajectory $w(t)$ (red) with examples for $d_T(t)$

5.9 Availability $\varepsilon_A^2(t)$

In contrast to reliability, availability is defined at a time instant t while reliability is defined in a time interval. The availability $A|_t$ describes the probability that a system is operational at the instant of time t. As for the reliability, this means for $\varepsilon_A^2(t)$ that $1-A|_t$ describes the probability that the system is not operable at time instant t. This probability can be directly used when computing $\varepsilon_A^2(t)$. Thus $\varepsilon_A^2(t)$ is proposed as:

$$\varepsilon_A^2(t) = 1 - A|_t \tag{21}$$

This definition satisfies two statements about availability mentioned in section 2:

1. If a system cannot be repaired, its availability equals its reliability
2. The integral over the mission time of $\varepsilon_A^2(t)$ in the dependability function equal the average availability, also called interval or mission availability as introduced in section 2.

5.10 Additional $\varepsilon_X^2(t)$

According to the system and its mission, additional measures for $\varepsilon^2(t)$ might be needed to take into account further special requirements with respect to dependability.

As stated earlier, it is important that those $\varepsilon_X^2(t)$ are dimensionaless and are normalized between 0 and 1, where 0 means dependable and 1 means not dependable.

6. Examples for measuring the dependability

To present the adaptability of the dependability definition proposed above, the following two examples may serve as a demonstration.

6.1 Example 1: autonomous transport system

To clarify the behaviour based dependability measurement, an autonomous mobile system with only one position degree of freedom is used. The system is an autonomous

transportation system build to autonomously reach different positions which could be, for example, stopping points on a track. For the dependability measurement only the position on the track is considered in the first example. The velocity and acceleration of the autonomous transportation system will be initially disregarded in this example.

6.1.1 Behaviour based system description

For the dependability measurement proposed in the last section, the system will be modelled as described in Section 3. Since the system only has one position degree of freedom it can only move forward and backward on the track, the signal space of the system is $\mathbb{W} = \mathbb{R}$. The time of interest for this system is $\mathbb{T} = \mathbb{R}^+$.

For the description of the behaviour B, the train model is needed. A simple train model with rolling friction derived from Newtons Law is used for that purpose. According to Newtons-Law, the sum of forces acting on an object is equal to the mass of that object, multiplied by its acceleration. The mass of the train is assumed to be M. The forces acting on the train are, on the one hand, the driving force F_a and, on the other hand the friction force $F_r = \mu F_n$ (μ represents the coefficient of rolling friction, F_n the force parallel to the planes normal). It is assumed that the train only moves in a plane, thus there is no inclination, etc. Consequently, the force parallel to the normal of the plane F_n can be set equal to the force of gravity $F_n = F_g = Mg$, with g being the acceleration due to gravity. A diagram of the system with the forces used in this model is shown in Fig. 8. The system can thus be described according to the following equations.

$$M\ddot{x} = F_a - F_r \tag{22}$$

$$M\ddot{x} = F_a - \mu g M \tag{23}$$

$$\ddot{x} = \frac{1}{M}\left(F_a - \mu g M\right) \tag{24}$$

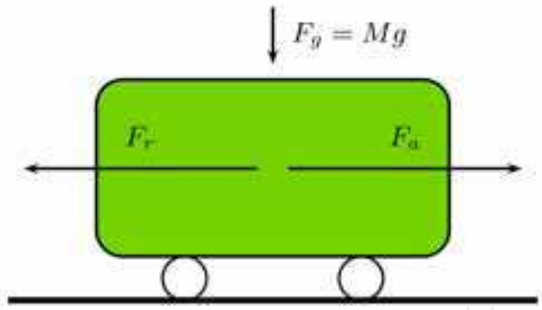


Figure 8. Example of an autonomous transportation system with the forces used to model the system. F_a driving force, F_r friction and F_g gravitation force.

According to the behavioural based approach set forth in section 3, the autonomous mobile transportation system can be described as follows.

Universe $\mathbb{W} = \mathbb{R}$

Time $\mathbb{T} = \mathbb{R}^+$

Behaviour $\mathfrak{B} = \left\{x : \Re^+ \rightarrow \Re | \ddot{x} = \frac{1}{M}\left(F_a - \mu g M\right)\right\}$

The corresponding Matlab Simulink Model is shown in Fig. 9. The position and the velocity of the system are controlled by simple PI-controllers (see Fig. 10 and 11). Of all possible

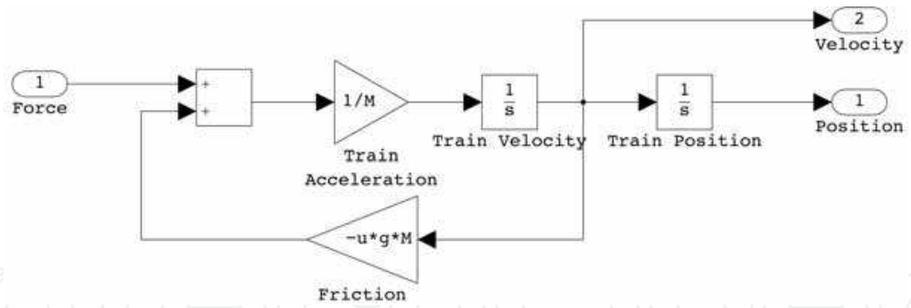


Figure 9. Matlan Simulink model of an autonomous transportation system. M is the mass of the system, μ the friction coefficient and g the acceleration due to gravity

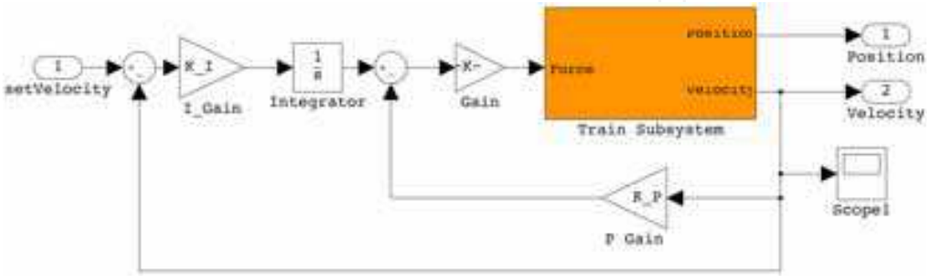


Figure 10. Velocity loop of an autonomous transportation system. The system velocity is controlled by a simple PI controller.

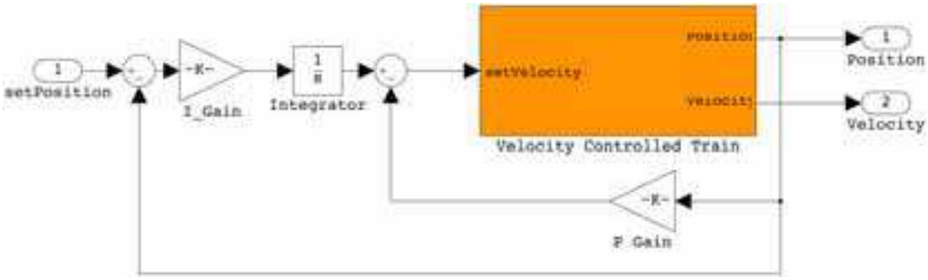


Figure 11. Position loop of an autonomous transportation system. The position of the system is controlled by a simple PI controller

system behaviours from the set B only a subset $\mathbb{B} \subset \mathsf{B}$ is available according to the mass and the maximum possible driving force of the system. In this example it is further assumed that the system is able to completely follow the given velocities and accelerations.

6.1.2 Behaviour based dependability measurement

The mission of the above modelled autonomous transportation system is to reach consecutively different positions on the track. The mission time in this example is set to 2400 time units.

The system should thus accomplish a desired behaviour $w_m(t)$ with its given behaviours $B \subset \mathsf{B}$. The set of desired behaviours for this example is generated with a Matlab Simulink model. For this purpose, the signal builder block is used (see Fig 12) to define different desired positions on the track. The reference signal is fed to the real train system to simulate the actual behaviour (Model in Fig. 8) and also to the reference train system (Reference Model in Fig. 8) to generate the desired behaviour. With the aid of the generated behaviour

in the reference model, this will be taken as the desired behaviour $w_m(t)$ or mission of the autonomous transportation system and used for the computation of the system's dependability. This model shows an example of the different opportunities to measure the dependability of such systems.
At first, it is assumed that the position of the autonomous transportation system can be measured adequately. Consequently it is assumed that the measurement of the position itself does not produce additional errors.
Up till now only system internal errors or deviations were considered as deviations between the reference model and the real system. It is also possible that changes in the model or the environment, as implicitly considered in this case, may occur. Unexpected wearout of wheels, resulting from e.g. a smaller wheel radius can produce errors, and as such lead to a deviation from the desired behaviour, if the position of the train is only measured on the basis of the wheel rotations.

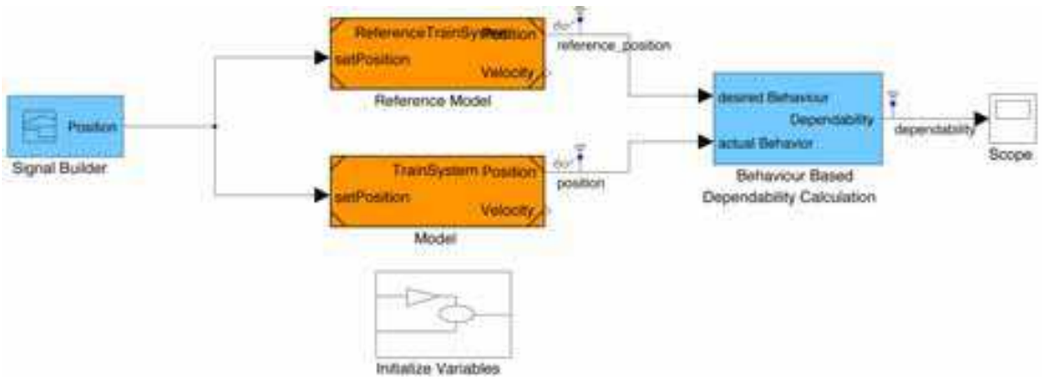


Figure 12. A Matlab signal builder block is used together with a reference and the real system in order to generate the actual and desired behaviour of the system.

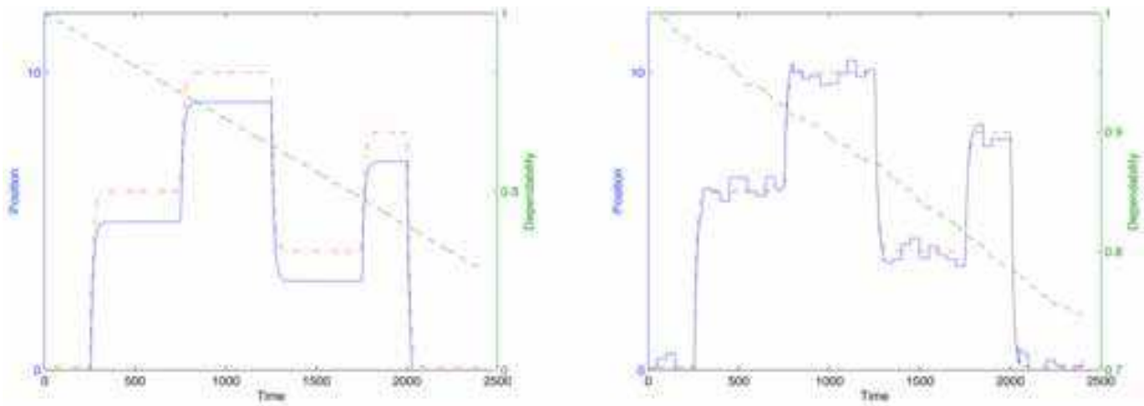
When generating the desired behaviour in this example it is assumed that the system is functioning properly. Thus, the reference model reflects the system adequately. Noise in the sensors, for example, is not explicitly modelled. Of course, this could have been also introduced in the model for a better computation of the desired behaviour.
In the first example, two different simulations are carried out.

1. To simulate an additive error, a constant value is added to the position measurement. This error could be due to faulty initialization, slippage etc, but could also because of an error in the model of such autonomous transportation system.
2. To demonstrate as to what extend noise in sensors or measurement uncertainty affect the dependability of a system, noise is added to the measurement of the position.

The results of the two simulations are shown in Fig. 13. The dotted red line in each case represents the desired behaviour, thus the mission trajectory w_m. The actual system behaviour is shown as blue line. The measured dependability for this example is shown as a dashed green line.

6.2 Example 2: Small train

Since the autonomous transportation system is built for the transport of people and as such represents a safety critical system, system safety is also considered in the second example.
In the second example, besides the position of the system, the velocity is considered when calculating dependability. In addition to the above mentioned two simulations, two other scenarios were added for the computing of dependability.



(a) Aboslut Value added to the position (b) Noise added to the position

Figure 13. Simulation Resutls for Example 1.

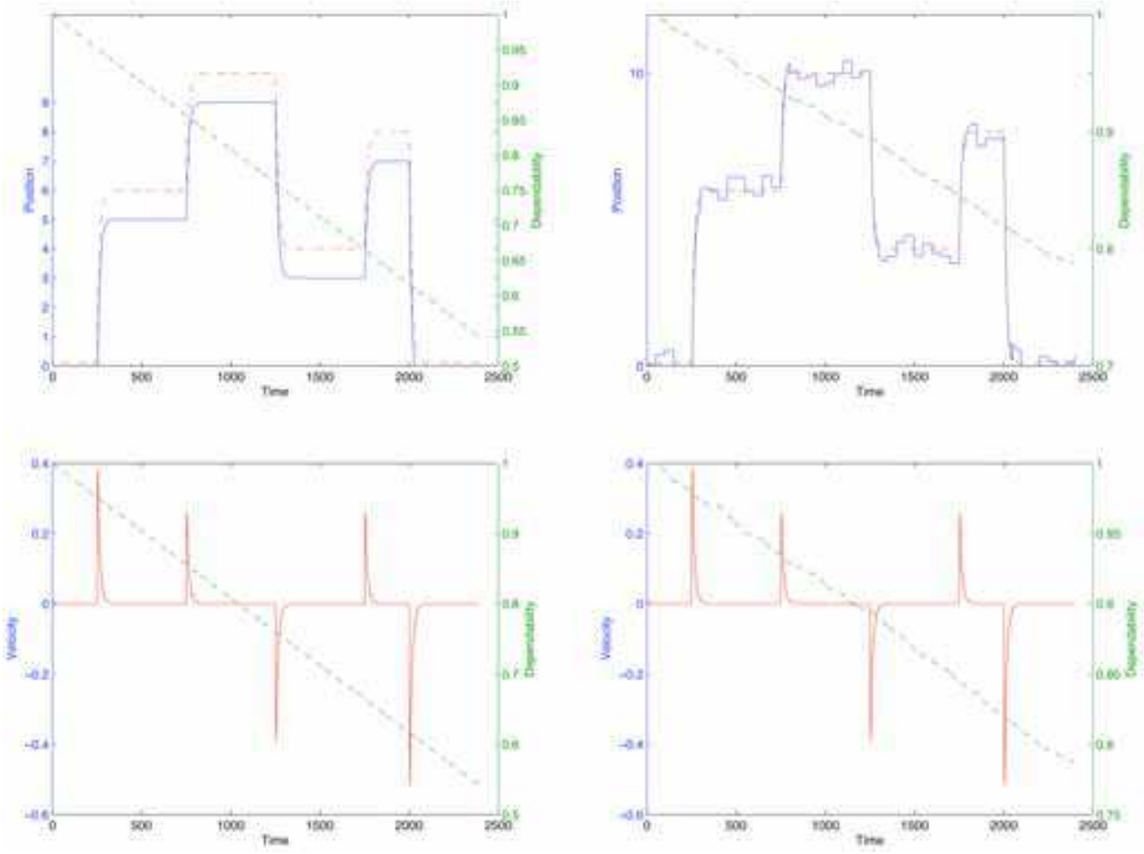


Figure 14. Simulation Results for example 2 with Position and Speed used for the dependability calculation

1. In order to enhance the dependability calculation, a desired and actual behaviour of the velocity was added. For the simulation of parameter errors, which are multiplicative, the velocity of the real system is multiplied by a constant value.
2. A safety area, as proposed, was added for the velocity. Consequently, the relative distance $\varepsilon_s^2(t)$ is also used when computing system's dependability.

For each of these two scenarios, again, both simulations allready used in the first examples where performed. The results of the individual four simulations are shown in Fig. 14 and 15. As in the last figure, the dotted red lines represents the desired behaviour for either the velocity or the position. The actual system behaviour in terms of velocity and position is shown as blue line. The measured dependability for the examples is shown as dashed green line.

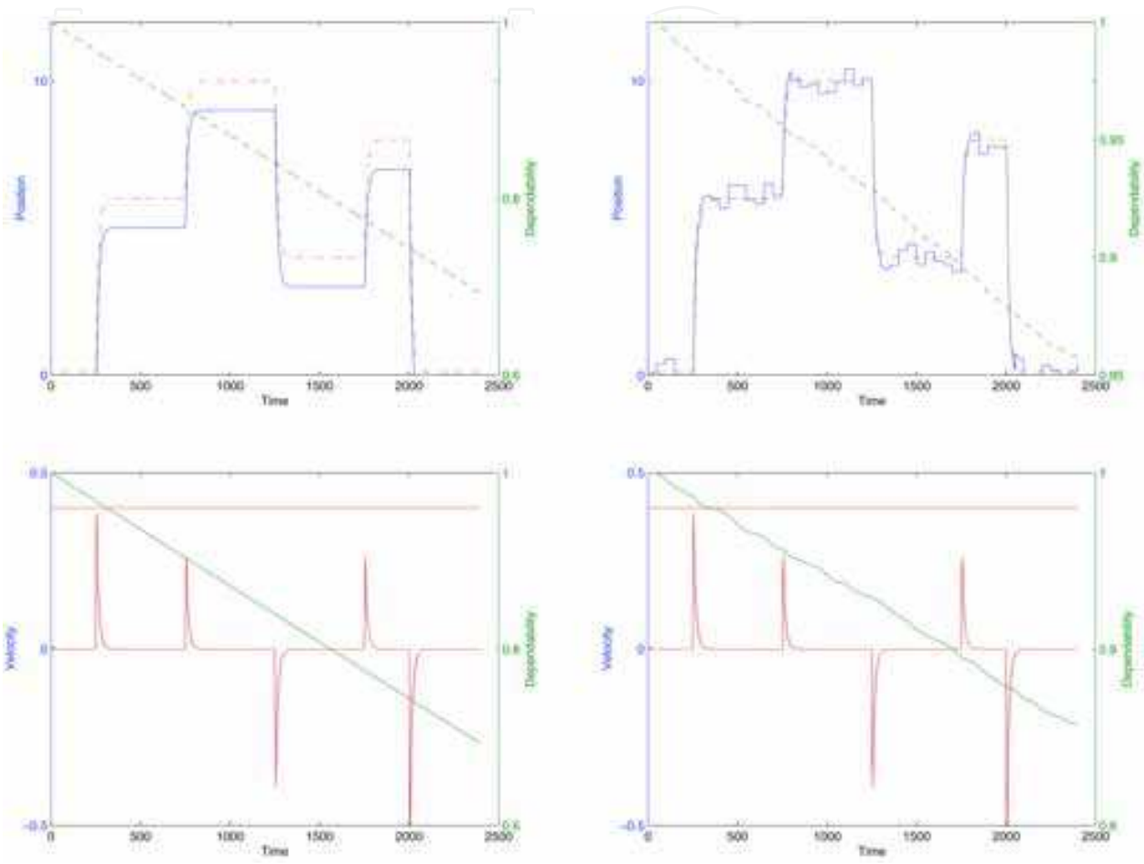


Figure 15. Simulation Results for example 2 with Position and Speed used for the dependability calculation. Additionally a safety area for the velocity is added.

7. Conclusion

There exist numerous non-formal definitions for dependability (see Carter, 1982; Laprie, 1992; Badreddin, 1999; Dubrova, 2006; Avizienis et al., 2004a just to name a few). When applying those non-formal definitions to a specific system the resulting dependability measure usually is only valid for this specific system and only in rare cases transferable to a family of equal systems. Small changes in the system or environment, however, render those measurements usually useless when it comes to measuring or even comparing the dependability of different systems.

Autonomous mobile robots are often described by their behaviour. This aspect was utilized in this chapter for the definition of dependability in a behavioural context in order to obtain an easy to apply and computable formula for the dependability of systems. Since this

formula for dependability is solely based on the behaviour and the mission of a system it can be easily compared with other systems having different missions.
The definition for dependability proposed in this chapter is straight forward, easily applicable and well suited for dependability comparison of different systems.

8. References

Avizienis, A., Laprie, J.-C., and Randell, B. (2004a). Dependability and its threats: A taxonomy.

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

Badreddin, E. (1999). Safety and dependability of mechatronics systems. In *Lecture Notes*. ETH Zürich.

Badreddin, E. and Abdel-Geliel, M. (2004). Dynamic safety margin principle and application in control of safety critical systems. In *Proceedings of the 2004 IEEE International Conference on Control Applications, 2004.*, volume 1, pages 689–694Vol.1.

Brooks, R. A. (1986). A robust layered control systemfor a mobile robot. *IEEE Journal of Robotics and Automation*, 2(1):14–23.

Candea, G. (2003). The basics of dependability.

Carter, W. (1982). A time for reflection. In *Proc. 12th Int. Symp. on Fault Tolerant Computing (FTCS-12)*. FTCS-12) IEEE Computer Society Press Santa Monica.

Department of Defence, U. S. o. A. (1970). Military standard - definitions of terms for reliability and maintainability. Technical ReportMIL-STD-721C.

Dewsbury, G., Sommerville, I., Clarke, K., and Rouncefield, M. (2003). A dependability model for domestic systems. In *SAFECOMP*, pages 103–115.

Dubrova, E. (2006). Fault tolerant design: An introduction. Draft.

Filippini, R. and Bondavalli, A. (2004). Modeling and analysis of a scheduled maintenance system: a dspn approach.

Flammini, F. (2006). *Model-Based Dependability Evaluation of Complex Critical Control Systems*. PhD thesis, Universitá degli Studi di Napoli - Federico II.

Hermann, R.; Krener, A. (Oct 1977). Nonlinear controllability and observability. *Automatic Control, IEEE Transactions on*, 22(5):728–740.

IEC (1990). International electrotechnical vocabulary. chapter 191: Dependability and quality of service.

International Federation for Information Processing. Wg 10.4 on dependable computing and fault tolerance. http:// www.dependability.org/wg10.4/.

Laprie, J. C. (1992). Dependability. Basic Concepts and Terminology. Ed. Springer Verlag.

Randell, B. (2000). Turing Memorial Lecture: Facing up to faults. 43(2):95–106.

Rüdiger, J., Wagner, A., and Badreddin, E. (2007a). Behavior based definition of dependability for autonomous mobile systems. European Control Conference 2007. Kos, Greece.

Rüdiger, J., Wagner, A., and Badreddin, E. (2007b). Behavior based description of dependability - defining a minimum set of attributes for a behavioral description of dependability. In Zaytoon, J., Ferrier, J.-L., Andrade-Cetto, J., and Filipe, J., editors, *ICINCO-RA (2)*, pages 341–346. INSTICC Press.

Vesely, W. E., Goldberg, F. F., Roberts, N. H., and Haasl, D. F. (1981). *Fault Tree Handbook*. U. S. Nuclear Regulatory Commission, NUREG-0492, Washington DC.

Willems, J. (1991). Paradigms and puzzles in the theory of dynamical systems. *IEEE Transactions on Automatic Control*, 36(3):259–294.

Robotics Automation and Control

Edited by Pavla Pecherkova, Miroslav Flidr and Jindrich Dunik

ISBN 978-953-7619-18-3
Hard cover, 494 pages
Publisher InTech
Published online 01, October, 2008
Published in print edition October, 2008

This book was conceived as a gathering place of new ideas from academia, industry, research and practice in the fields of robotics, automation and control. The aim of the book was to point out interactions among various fields of interests in spite of diversity and narrow specializations which prevail in the current research. The common denominator of all included chapters appears to be a synergy of various specializations. This synergy yields deeper understanding of the treated problems. Each new approach applied to a particular problem can enrich and inspire improvements of already established approaches to the problem.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Jan Rüdiger, AchimWagner and Essam Badreddin (2008). Dependability of Autonomous Mobile Systems, Robotics Automation and Control, Pavla Pecherkova, Miroslav Flidr and Jindrich Dunik (Ed.), ISBN: 978-953-7619-18-3, InTech, Available from: http://www.intechopen.com/books/robotics_automation_and_control/dependability_of_autonomous_mobile_systems

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen