BEHAVIOR BASED DESCRIPTION OF DEPENDABILITY
Defining a Minium Set of Attributes for a Behavioral Description of Dependability

Jan Rüdiger, Achim Wagner and Essam Badreddin
Automation Laboratory, University of Mannheim, B6, 23-29, Building B, EG, 68131 Mannheim, Germany

Keywords: Fault-tolerant systems, Autonomous systems, Behavioral systems.

Abstract: Dependability is widely understood as an integrated concept that consists of different attributes. The set of attributes and requirements of each attribute varies from application to application thus making it very challenging to define dependability for a broad amount of application. The dependability, however, is of great importance when dealing with autonomous or semi-autonomous systems, thus defining dependability for those kind of system is vital. Such autonomous mobile system are usually described by their behavior. In this paper a minimum set of attributes for the dependability of autonomous mobile systems is proposed based on a behavioral definition of dependability.

1 INTRODUCTION

Complex computing systems, such as network computers, computer controlled plants or flight controll systems need not only to fulfill their functional but also their non-functional properties like availability, reliability, safety, performance, dependability etc. Non-functional properties reflect the overall quality of a system. Besides performance the dependability is getting a more important non-functional requirement of a system.
The dependability is usually understood as an integrated concept (Avizienis et al., 2004b; Avizienis et al., 2004a; Randell, 2000; Candea, 2003; Dewsbury et al., 2003) that further consists of attributes that affect the dependability of the system. The set of attributes and the requirements on each attribute vary from application to application. This makes it hard to define dependability for a broad amount of applications.
The dependability of a system is particularly important when dealing with autonomous or semi-autonomous systems. With an increasing degree of autonomy and safety requirements the requirements for dependability increase hence being able to measure and compare the dependability of these system is getting more and more important.

In this paper a minimum set of attributes for the dependability of autonomous mobile systems is proposed.
This paper is outlined as follows: In Section 2 a description for systems on which dependability is usually defined is presented. Since the dependability definition used throughout this paper is based on a different definition of a system the equivalence of the two system definitions is shown. In Section 3 the different definitions used in the literature are used and again compared to the behavior based definition used throughout this paper. Section 4 summarizes the attributes of dependability and a minimum set of those attributes is proposed based on the behavioral definition of dependability and of the attributes. The paper ends with the discussion of the set in Section 5 and the conclusion.

2 SYSTEM

According to (Randell, 1999; Avizienis et al., 2004b; Avizienis et al., 2004a; Jones, 2003) the system for which dependability will be discussed is described by its

- functional and non-functional properties,

Rüdiger J., Wagner A. and Badreddin E. (2007).
BEHAVIOR BASED DESCRIPTION OF DEPENDABILITY - Defining a Minium Set of Attributes for a Behavioral Description of Dependability.
In *Proceedings of the Fourth International Conference on Informatics in Control, Automation and Robotics*, pages 341-346
DOI: 10.5220/0001650203410346

- the boundaries of the system,
- the environment the system is designed for,
- the system behavior,
- the service the system delivers, and
- its structure.

In Wikipedia a **System** (from the Latin (systēma), and this from the Greek συστημα (sustēma)) is defined as an assemblage of entities/objects, real or abstract, comprising a whole with each and every component/element interacting with or related to at least one other component/element. Any object which has no relationship with any other element of the system, is not a component of that system. A subsystem is then a set of elements, which is a system itself, and a part of the whole system.
In this view it is equal wether a system is connected to another system or to a user, who is again treated as a system.
A system is usually defined by its functional and non-functional properties. The functional properties define specific behaviors of the system or subsystem while the non-functional properties define overall characteristics of the system. Thus, the non-functional properties define properties the system must satisfy while performing its functional properties. Among other things the non-functional properties of a system are: functionality, performance, availability, dependability, stability, cost, extensibility, scalability, manageability, application maintainability, portability, interface, usability and safety. This list is non-exhaustive since the non-functional properties of a system are highly system specific (Torres-Pomales, 2000; Sutcliffe and Minocha, 1998; Franch and Botella, 1998). When systems or sub-systems interact with each other or with their environment the common boundaries of those systems as well as the environment itself must be defined. A system acting well in the specified environment may fail in an environment its was not designed for. The system boundary defines the scope of what the system will be and as such defines the limits of the system.
The behavior of the system is how the system implements its intended function. The behavior of a dynamic system as defined (Willems, 1991) is a time trajectory of the legal states of the system. The legal states of the system are further divided into external and internal states. External states of a system are those which are perceivable by the user or another system. The external states thus define the interface of the (sub-)system. The remaining states are internal.
The service the system delivers is its visible behavior to the user or another system. According to the above definition of behavior this is the time trajectory of its external states.
Last but not least the structure of the system defines how the system is partitioned into sub-systems and how those sub-systems are connected to each other and how the system is „connected" to the environment. The structure of the system also defines how the communication of the sub-systems is organized.
When dealing with autonomous mobile robots the system is often viewed as a black box and described by its behavior. The behavioral approach is very common when dealing with autonomous mobile robots (Brooks, 1986; Michaud, ; Jaeger, 1996). The framework of Willems (Willems, 1991) is used for describing a system by its behavior. In this framework a dynamical system is defined to be „living" in an universe $\mathbb{U}$.

Definition 2.1 *A* dynamical system $\sum$ *is a triple* $\sum = (\mathbb{T}, \mathbb{W}, \mathfrak{B})$ *with* $\mathbb{T} \subseteq \mathbb{R}$ *the time axis,* $\mathbb{W}$ *the signal space, and* $\mathfrak{B} \subseteq \mathbb{W}^{\mathbb{T}}$ *the behavior.*

A mathematical model of a system claims that certain outcomes are possible, while others are not. This subset is called the *behavior* of the system. The behavior $\mathfrak{B}$ is thus the set of all admissible trajectories. The universe $\mathbb{U}$ is the equivalence to the environment as described above and the behavior $\mathfrak{B}$ is the equivalence to function of the system. In (Rüdiger et al., 2007) the definition of a dynamical system is extended by a set of *basic and fused behaviors* $\mathbb{B}$ and by a mission w_m of the system which is the equivalence of the service the system is intended to deliver. Such a system is defined as:

Definition 2.2 *Let* $\Sigma = (\mathbb{T}, \mathbb{W}, \mathfrak{B})$ *be a time-invariant dynamical system then* $B \subseteq \mathbb{W}^{\mathbb{T}}$ *is called the set of* basic behaviors $w_i(t) : \mathbb{T} \to \mathbb{W}$, $i = 1...n$ *and* $\mathbb{B}$ *the set of fused behaviors.*

B is a set of trajectories in the signal space $\mathbb{W}$. The set of basic behaviors *B* of an autonomous system, in contrast to the behaviors $\mathfrak{B}$ of a dynamical system as defined in (Willems, 1991), is not the set of admissible behaviors, but solely those behaviors which are given to the system by the system engineer (programmer).
The mission of such a system is defined as:

Definition 2.3 *Let* $\Sigma = (\mathbb{T}, \mathbb{W}, \mathfrak{B})$ *be a time-invariant dynamical system. We say the* mission w_m *of this system is the map* $w_m : \mathbb{T} \to \mathbb{W}$ *with* $w_m \in \mathfrak{B}$.

A dynamical system can, like the system described above, be divided into subsystem having their own behavior. This definition of system and behavior is used throughout this paper.

3 DEFINITION OF DEPENDABILITY

Beside the other mentioned non-functional properties of a system the dependability is getting a more important non-functional property.
The general, qualitative, definitions for *dependability* used in the literature so far are:

> **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 trust that can be placed on that service. As mentioned before the service a system delivers is the behavior as it is perceived by the user, which in our case is also called the mission of the system.
A more quantitative definition for dependability used in (Avizienis et al., 2004a) is:

> **Dependability** of a system is the ability to avoid service failures that are more frequent and more severe than is acceptable by the user(s).

This definition, however, does not directly include the service the system is intended to deliver nor does it include the time up to which the system has to deliver the intended service.
Derived from the above definitions and the behavioral definition of a system a behavior-based definition for dependability for autonomous mobile robots was introduced in (Rüdiger et al., 2007). This includes the definition of a mission which coresponds with the service mentioned above.

4 ATTRIBUTES OF DEPENDABILITY

According to (Avizienis et al., 2004b; Avizienis et al., 2004a; Randell, 2000) the dependability is an integrated concept that further consists of the attributes (see also Figure 1)

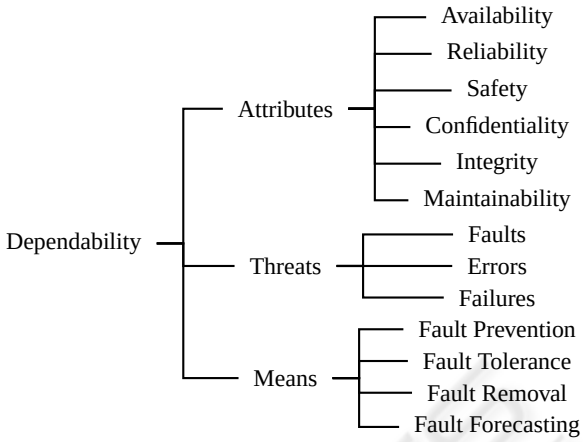

Figure 1: The dependability tree.

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

In (Candea, 2003) only reliability, availability and safety together with security is listed; however, security is seen as an additional concept as described below.
In (Dewsbury et al., 2003) the dependability attributes for home systems are defined as:

- **Trustworthiness** the system behaves as the users expects,
- **Acceptability** a system that is not acceptable will not be used,
- **Fitness for its purpose** the system must fit the purpose it was designed for and
- **Adaptability** the system must evolve over time and react to changes in the environment and the user.

The dependability specifications of a system must set requirements for the above attributes. Based on a specific system the dependability of the system depends on those requirements for a subset or all of the above attributes. Since the (sub-)systems are designed in a behavioral context it is common to also describe the attributes of dependability in a behavioral context or the other way round to describe the requirements for

the attributes on the behavior of the (sub-)system. Before further describing the attributes it is, however, important to define a priority for the attributes.

4.1 Safety

For autonomous mobile robots the main attribute is, or should be, safety. The attribute safety is not to be mistaken with the attribute security which is a combination of the attributes confidentiality, integrity and availability and as thus an additional concept (Samarati and Jajodia, 2000; Cotroneo et al., 2003; Cera et al., 2004). For a comparison of security and dependability see (Meadows and McLean, 1999). Even if the the intended service of the system cannot be fullfilled the safety requirements of the system are not allowed to be violated. Thus, the requirement on the behavior of the system, as defined in section 2, is that it must always fullfill its safety requirements.
From a 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.

In (Rüdiger et al., 2007) an area $\mathfrak{S}$ around the behavior of the system $\mathfrak{B}$ is introduced, which leads to catastrophic consequences when left. Safety of a system Σ is then defined as:

Definition 4.1 *Let $\Sigma = (\mathbb{T}, \mathbb{W}, \mathfrak{B})$, $\mathbb{T} = \mathbb{Z}$ or $\mathbb{R}$, be a time-invariant dynamical system with a safe area $\mathfrak{S} \supseteq \mathfrak{B}$. The system is said to be* safe *if for all $t \in \mathbb{T}$ the system state $w(t) \in \mathfrak{S}$.*

The definition is illustrated in Figure 2. This definition is consistent with the idea that a safe system is either operable or not operable but in a safe state.

4.2 Availability Vs Realiability

Reliability means (Dubrova, 2006):

> 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 $\mathfrak{B}$. In contrast to reliability the availability is defined at a time instant t while the reliability is defined in a time interval.

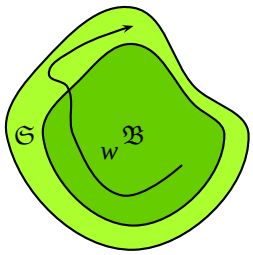

Figure 2: Safety: The system trajectory w leaves the set of admissible trajectories $\mathfrak{B}$ but is still considered to be safe since it remains inside $\mathfrak{S}$.

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

Availability is typically important for real-time systems where a short interrupt can be tolerated if the deadline is not missed. This also holds for autonomous mobile systems. In (Rüdiger et al., 2007) the availability is defined as:

Definition 4.2 *Let $\Sigma = (\mathbb{T}, \mathbb{W}, \mathfrak{B})$, $\mathbb{T} = \mathbb{Z}$ or $\mathbb{R}$, be a time-invariant dynamical system. The system is said to be* available *at time t if $w(t) \in \mathfrak{B}$. Correspondingly, the availability of the system is the probability that the system is available.*

For dependable autonomous mobile systems as defined above requirements for reliability are redundant and can be omitted. In case of reliability and availability it is sufficient to define requirements for the availability.

4.3 Maintainability

A maintainable system is „able to react“ either autonomously or by human interaction to changes in the system and the environment.

> Maintainability is the ability of a system to undergo modification and repairs.

While the requirements for the first two attributes rather passively define the dependability of a system, the maintainability gives the system the ability to react to changes. An event that would reduce or violate the dependability of the system can counteract to recover the dependability. In (Rüdiger et al., 2007) the maintainability is defined as:

Definition 4.3 *A dynamical system $\Sigma = (\mathbb{T}, \mathbb{W}, \mathfrak{B})$ with the behaviors $\mathbb{B}$ is said to be* maintainable *if for all $w_1 \in \mathbb{W}$ a $w_2 \in \mathfrak{B}$ and a $w : \mathbb{T} \cap [0,t] \rightarrow \mathbb{W}$ exist,*

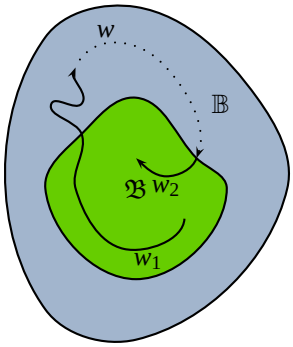

Figure 3: Maintainability: The system trajectory w_1 leaves the set of admissible trajectories $\mathfrak{B}$ and is steered back to $\mathfrak{B}$ with the trajectory $w \in \mathbb{B}$.

with $w' : \mathbb{T} \rightarrow \mathbb{W}$ *defined by:*

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

The definition is illustrated in Figure 3. An autonomous mobile system is said to be maintainable if it is able to steer the system from any trajectory $w \notin \mathfrak{B}$ back to the set of admissible trajectories $\mathfrak{B}$ in time $[0,t]$.

4.4 Confidentiality and Integrity

Confidentiality has been defined by the International Organization for Standardization (ISO) as ”ensuring that information is accessible only to those authorized to have access”. This attribute is very important for systems like operating systems or transaction systems. For autonomous mobile robots, however, this attribute is underpart. If informations of the system will be available un-authorized then this will not reduce the dependability of the autonomous mobile system. For this attribute the functions of the underlaying operating system are used.
When a program is executed on a system it is usually checked whether the program is allow to be runned by the user. *Integrity* ensures that the program flow and the information of the program will not be altered during the execution. Even if a change, wether it was on purpose, by an external or by soft- or hardware failure, in the program flow could be severe this aspect is already covered by the safety attribute.

5 DISCUSSION

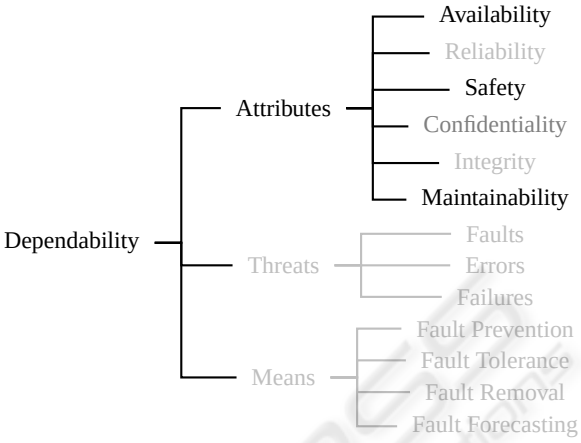

Figure 4: The resulting dependability tree.

The resulting dependability tree for autonomous mobile systems is shown in Figure 4. The requirements for the safety assures that failures in the system will not lead to catastrophic consequences. The requirements for the availability assures that the system is operational at the desired time instances t and finally the maintainability requirements assures that even in case of changes of the system or the environment the system is able to react and modify itself to maintain the dependability of the system.

6 CONCLUSION

Dependability is part of the non-functional properties of a system which reflect the overall quality of a system. Qualitative definitions for dependability like in (Carter, 1982; Laprie, 1992; Badreddin, 1999; Dubrova, 2006) further divide the dependability into attributes. Those attributes are again rather qualitative and also not distinct. Autonomous mobile systems are often described by their behavior. This aspect was utilized in this paper to propose a minimum subset of the attributes of dependability, as defined in (Rüdiger et al., 2007), which are defined quantitative and can still ensure the dependability of the autonomous mobile system.

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.

Brooks, R. A. (1986). A robust layered control system for 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.

Cera, C. D., Kim, T., Han, J., and Regli, W. C. (2004). Role-based viewing envelopes for information protection in collaborative modeling.

Cotroneo, D., Mazzeo, A., Romano, L., and Russo, S. (2003). An architecture for security-oriented perfective maintenance of legacy software.

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.

Franch, X. and Botella, P. (1998). Putting non-functional requirements into software architecture.

Jaeger, H. (1996). Brains on wheels: Mobile robots for brain research.

Jones, C. (2003). A formal basis for some dependability notions.

Laprie, J. C. (1992). *Dependable computing: Basic concepts and terminology*. Ed. Springer Verlag, 1992.

Meadows, C. and McLean, J. (1999). Security and dependability: then and now. In *Computer Security, Dependability, and Assurance: From Needs to Solutions, 7-9 July 1998 & 11-13 November 1998, York, UK & Williamsburg, VA, USA*, pages p.166–70. Los Alamitos, CA, USA : IEEE Comput. Soc, 1999.

Michaud, F. Adaptability by behavior selection and observation for mobile robots.

Randell, B. (1999). Dependability - a unifying concept.

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

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

Samarati, P. and Jajodia, S. (2000). Data security.

Sutcliffe, A. G. and Minocha, S. (1998). Scenario-based analysis of non-functional requirements.

Torres-Pomales, W. (2000). *Software Fault Tolerance: A Tutorial*.

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