BEHAVIOR BASED DEPENDABILITY ESTIMATION
Estimating the Dependability of Autonomous Mobile Systems using Predictive Filter

Jan Rüdiger, Achim Wagner and Essam Badreddin
Automation Laboratory, University of Mannheim, B6, 23-29, Building B, EG, 68131 Mannheim, Germany
ruediger@uni-mannheim.de, a.wagner@ti.uni-mannheim.de, badreddin@ti.uni-mannheim.de

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

Abstract: Dependability is getting a more important non-functional property of a system. Measuring and predicting the dependability is especially important for autonomous or semi-autonomous and safety-critical systems. Since, at least for (semi-) autonomous systems, those systems are usually described by their behavior, a definition for dependability based on the behavior of the system is evident. In this paper the behavioral based definition of dependability was used together with a particle filter to estimate the dependability of an autonomous mobile system.

1 INTRODUCTION

Non-functional properties reflect the overall quality of a system. Beside performance the dependability is getting a more important non-functional requirement of a system. The general, qualitative, definitions for *dependability* used in the literature so far are (in historical order):

> **Military Standard.** (Department of Defense, 1970) A measure of the degree to which an item is operable and capable of performing its required function at any (random) time during a specified mission profile, given item availability at the start of the mission.
>
> **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 definitions have in common that they define dependability on the service a system delivers and the trust that can be placed on that service. The service a system delivers, however, is the behavior as it is perceived by the user, which in our case will be called the mission of the system. They also have in common that they don't define a system independent way of how the measure or evaluate the dependability of a system. Comparing the dependability of different systems, even if a dependability measure for specific systems exists (see (Wilson et al., 2002; Kanoun et al., 2002; Brown et al., 2002; Rus et al., 2002; Cukier and Smidts, 2002; Mukherjee and Siewiorek, 1997; Arlat et al., 1990)), is almost impossible.
According to (Avizienis et al., 2004b; Avizienis et al., 2004a; Randell, 2000) dependability is understood as an integrated concept that further consists of different attributes, threads and means (see Fig. 1). This set of attributes is, however, application specific and thus not fix. In (Candea, 2003) and (Dewsbury et al., 2003) different sets of attributes for evaluating the dependability were proposed. In (Rüdiger et al., 2007b) a reduction of the dependability tree was proposed for the application of autonomous mobile systems. The reduced dependability tree is presented in Fig. 2.

This paper is outlined as follows: In Section 2 a short introduction to the framework of dynamic systems described by their behavior is presented leading to a definion for a system together with a mission, defined in this framework. The section concludes with a definition for a measure for the dependability of this system. Section 2.5 describes different methods of how to apply this definition to actually measure the

dependability. The results of a simulation using particle filter are then presented in Section 4. The paper ends with a discussion of the results in Section 5.

2 BEHAVIOR BASED DEPENDABILITY DEFINITION

2.1 System Definition

In the framework of Willems (see (Willems, 1991)) a system is defined in an universum $\mathbb{U}$. Elements of $\mathbb{U}$ are called outcomes of the system. A mathematical model of a system from a behavioral or black-box point of view claims that certain outcomes are possible, while others are not. The model thus defines a specific subset $\mathfrak{B} \subset \mathbb{U}$. This subset is called the *behavior* of the system.
A (deterministic) mathematical model of a system is then defined as:

Definition 1. *A* mathematical model *is a pair* $(\mathbb{U}, \mathfrak{B})$ *with the universum* $\mathbb{U}$ *- its elements are called* outcomes *- and* $\mathfrak{B}$ *the behavior.*

A dynamical system is a set of trajectories describing the behavior of the system during the time instants of interest in $\mathbb{W}$.
In contrast to the state space representation, like $\dot{x} = f \circ x$, Willems (see (Willems, 1991)) defines a dynamical system as:

Definition 2. *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.*

Furthermore an autonomous system is defined as:

Definition 3. *(Autonomous System) Let* $\Sigma = (\mathbb{T}, \mathbb{W}, \mathfrak{B})$, $\mathbb{T} = \mathbb{Z}$ *or* $\mathbb{R}$*, be a time-invariant dynamical system.* Σ *is said to be* autonomous *if*

$$\left\{ w_1, w_2 \in \mathfrak{B} \text{ and } w_{1(t)} = w_{2(t)} \text{ for } t < 0 \right\} \Rightarrow \{ w_1 = w_2 \}$$

The definition of an autonomous systems states that the future behavior of the system is completely defined by its past trajectory.
This aspect is an important assumption for modeling the system later.

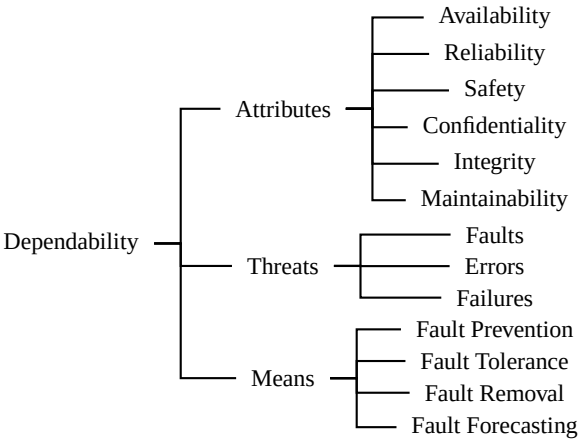


Figure 1: The dependability tree.

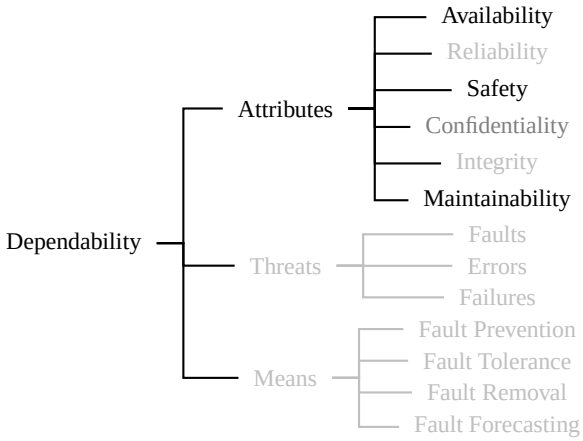


Figure 2: Reduced dependability tree for autonomous mobile systems.

2.2 Behavior and Mission of Autonomous System

To accomplish its task an autonomous system is usuallay given a set of behaviors. In (Rüdiger et al., 2007a) the behavior set of the system was defined as:

Definition 4. *(Behavior) 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 $w_i(t) : \mathbb{T} \rightarrow \mathbb{W}$, $i = 1 \ldots n$ *and* $\mathbb{B}$ *the set of fused behaviors.*

Likewise the mission of the system was defined as:

Definition 5. *(Mission) 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* $w_m : \mathbb{T} \rightarrow \mathbb{W}$ *with* $w_m \in \mathfrak{B}$.

The mission, as defined in (Rüdiger et al., 2007a), is thus just a special trajectory or behavior in $\mathfrak{B}$. Having the system together with a mission mathematically defined is important for a definition of dependability.

2.3 Safe Area $\mathfrak{S}$

Before presenting a definition for dependability, at least the definition for the attribute safety in a behavioral context is needed.

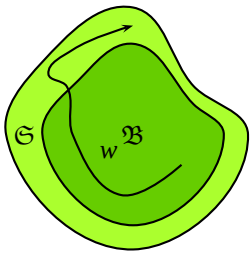


Figure 3: Safety: The system trajectory w leaves the set of admissible trajectories $\mathfrak{B}$ but is still considered to be safe since it remains inside $\mathfrak{S}$

While the other attributes of dependability, like availability, reliability etc., will only be indirectly included in the dependability definition (see Section 2.4 below), the attribute safety, since it is also included in the dependability definitions seen in Section 1, is directly included in the definition (see (Rüdiger et al., 2007a) for a definition of the remaining attributes in a behavioral context).
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.

For the formal definition of safety an area $\mathfrak{S}$ was introduced in (Rüdiger et al., 2007a) and further discussed in (Rüdiger et al., 2007b), which leads to catastrophic consequences when left. This safety area, however, must not be fully contained in the stability region of the system, but $\mathfrak{S}$ is defined to be around $\mathfrak{B}$ ($\mathfrak{B} \subset \mathfrak{S}$). This margin is, like $\mathfrak{B}$, highly system specific, but can be set equal to $\mathfrak{B}$ for a restrictive system.

Definition 6. *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 Fig. 3. Leaving the safe area $\mathfrak{S}$ does not necessary render the system un-operable for the rest of the mission. The above definition of safety permits that the systems trajectory returns to $\mathfrak{B}$ thus making the system fully operable again. This could be achieved be reconfiguration etc.

2.4 Dependability Definition

In (Rüdiger et al., 2007a) the dependability of a system was defined as:

Definition 7. *A time-invariant dynamical system $\Sigma = (\mathbb{T}, \mathbb{W}, \mathfrak{B})$ with the behaviors $\mathbb{B}$ and a mission $w_m \in \mathfrak{B}$ is said to be (gradually)* dependable *in the period $T \in \mathbb{T}$ if, for all $t \in T$, the mission w_m can be (gradually) accomplished.*

To actually measure the dependability of a given system, this definition needs, however, to be further sophisticated. The main idea behind this definition is to look at the dependability as the difference between the mission trajectory w_m and the system trajectory w, which is the evolution of the system state. This, together with the distance to the safety area $\mathfrak{S}$ will be the main idea of a measure for the dependability.
After the system Σ has completed its mission the dependability $\mathfrak{D}$ of this system with this mission w_m can be defined to as:

$$\mathfrak{D}_{\mathfrak{m}} = 1 - \frac{1}{t^*} \int_0^{t^*} d(\tau) d\tau \tag{1}$$

for the continuous case and for the non-continuous case

$$\mathfrak{D}_{\mathfrak{m}} = 1 - \frac{1}{t^*} \sum_0^{t^*} d(\tau). \tag{2}$$

Where t^* is an appropriate normalizing faktor and d is an appropriate measure of the difference between the mission trajectory w_m and the system trajectory w and as such a combination of different distance measurements. Those distance measurements will be discussed in the following.

More important than knowing the dependability of a system after the completion of the mission is to know the dependability during the mission. For this the equation 1 and 2 is split up into a past and a future part. With this the dependability can be computed to be

$$\mathfrak{D}(t) = 1 - \left(\underbrace{\frac{1}{t^*} \int_0^{t} d(\tau) d\tau}_{\text{Past}} + \underbrace{\frac{1}{t^* + \delta} \int_t^{t+\delta} d(\tau) d\tau}_{\text{Future}} \right) \tag{3}$$

in the continuous case and for the non-continuous case

$$\mathfrak{D}(t) = 1 - \left(\underbrace{\frac{1}{t} \sum_0^{t} d(\tau)}_{\text{Past}} + \underbrace{\frac{1}{t_m - t} \sum_{t+\varepsilon}^{t_m} d(\tau)}_{\text{Future}} \right) \tag{4}$$

Computing the $d_i(t)$ is, of course, system and application specific. For the simulation only the distance between the mission trajectory and the system trajectory ($d_m(t)$) and the relative distance between the system trajectory and the safe area $d_{\mathfrak{S}}(t)$ were used, since these both will be used in most of the dependability measures.
The distance between the mission trajectory and the system trajectory was chosen to be the minimum euclidian distance between system state and the mission trajectory.

$$d_m(t) = 1 - e^{-a*\left(\frac{w(t)-w_m(t)}{w_m(t)}\right)^2} \quad (5)$$

The distance measure for safety $d_{\mathfrak{S}}(t)$ was chosen to be a reliable measure even when the mission trajectory w_m itself is close to the safe area $\mathfrak{S}$. The d_S is defined as follows:

$$d_S(t) = 1 - e^{\left(\frac{\min|\mathfrak{S}-w_m(t)|}{\min|\mathfrak{S}-w(t)|}\right)^2} \quad (6)$$

2.5 Measuring the Dependability

For computing the dependability of a system the actual state of the system and for adequate time horizon the future states must be available with sufficient accuracy. To achieve this different techniques are found throughout the literature, among them:

- Using a model of the system and its environment or
- probabilistic approaches like
  - Kalman Filter or
  - Particle Filter

If for the accomplishment of the mission a set of basic behaviors $\mathbb{B}$ rather than only one behavior is available, the minimum d of those behaviors needs to be taken and the future part of dependability thus computes to:

$$\underbrace{\int_{t+\varepsilon}^{t_m} \frac{\min(d(t))^2}{t_m} dt}_{\text{Future}} \quad (7)$$

If the System is further divided into sub-systems, the different measures of those sub-systems needs also to be joined according to the topology of the system.

3 DEPENDABILITY MONITORING AS RECURSIVE STATE ESTIMATION

The formulation of dependability presented above requires estimating the state of the autonomous mobile system and the environment as it changes over time. This information must then be compared to the mission trajectory w_m to compute the dependability of the system.

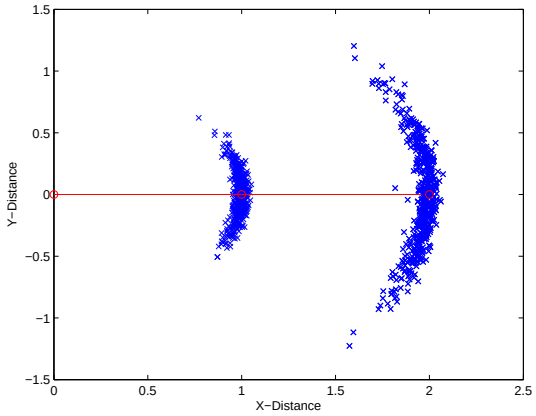


Figure 4: Prediction model of the robot for a translatory movement of 1m and 2m used to predict the dependability of the autonomous mobile system

3.1 Model based State Estimation

Using the mathematical model to compute the dependability of the system is the simplest way. This method, however, can only insufficient deal with changes in the system, which could happen due to system degeneration etc., or changes in the environment. Furthermore mathematical models usually focus on a specific aspect of the system and as thus aren't adequate for computing the dependability. A more sophisticated model of the robot and the environment could compensate this disadvantage with the cost of higher computation time.

3.2 Particle Filter based State Estimation

Since Kalman Filter restricts the state transition and the observation model to be linear functions of the system state, particle Filter are used here to track the state of the autonomous mobile system.
To be able to estimate the dependability with a particle filter, the system is modeled as Markovian, non linear, non-Gaussian. A Sample Importance Resampling Filter (SIR) (see e.g. (Arulampalam et al., 2002),(Chen, 2003)) was then used in a simulation described in the following section to estimate the system state.

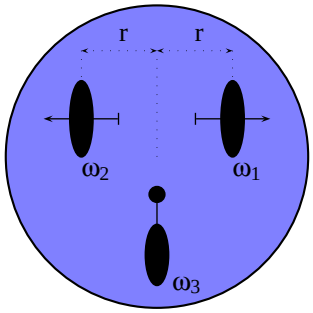


Figure 5: Drawing of the robot used in the simulation. Wheel ω_1 and ω_2 are two independently driven and measured conventional wheels. Wheel ω_3 is an undriven and unmeasured castor wheel.

4 SIMULATION RESULTS

The robot in the simulation has two degree of freedom (DOF) as shown in Fig. 5. For evaluating the dependability of this robot the state (pose)

$$x(t) = \begin{bmatrix} x \\ y \\ \phi \end{bmatrix} \tag{8}$$

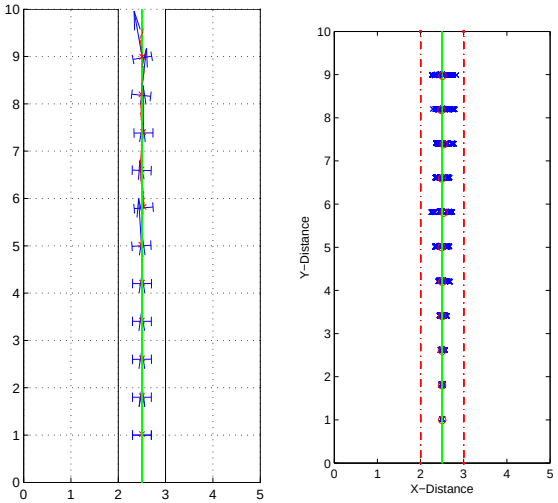
was estimated using a particle filter. The kinematic model of the robot presented in Eq. 9 was used to obtain the prediction model for the movement of the robot.

$$\begin{bmatrix} x_k \\ y_k \\ \phi_k \end{bmatrix} = \begin{bmatrix} x_{k-1} + \delta_s cos(\phi_{k-1}) \\ y_{k-1} + \delta_s sin(\phi_{k-1}) \\ \phi_{k-1} + \delta_\phi \end{bmatrix} \tag{9}$$

In this equation δ_s and δ_ϕ where computed using the movement of the wheels ω_1 and ω_2. A Gaussian noise modell is applied separately to each of the two types of motion because they are assumed to be independent. The resulting prediction model can be seen in Fig. 4 for a translatory movement of 1m and 2m.
The observation model used in the simulation is shown in the following equation.

$$y_k = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} = \begin{bmatrix} \delta_X - r\delta_\phi \\ \delta_Y + r\delta_\phi \end{bmatrix}$$

Where r is the distance between the center of the robot and the contact point of the wheels (see Fig. 5) and δ_X, δ_Y are the motion of the robot in X and Y direction according to the robot coordinate system.
The mission w_m of the system in the simulation (light green line in Fig. 6) was to follow a hallway without colliding with the wall. Noise was added to the wheels to simulate slippage and/or actuator degeneration.



(a) (b)

Figure 6: Simulation Setup. Left image shows the mission trajectory (light green line) of the robot traveling down a hallway (red line). Right image shows the particles used for the state estimation for every 40th time step (blue stars) together with the safe area (dotted red line).

To compute the dependability the distance between the mission trajectory and the robot trajectory ($d_m(t)$) together with the distance between the robot trajectory and the safe area (red line in Fig. 6) relative to the distance between the mission trajectory and the safe area ($d_{\Theta}(t)$) was used to compute the dependability as proposed above. The resulting dependability can be seen in Fig 7. Since a diverge from the mission trajectory also always decreases the distance to the safe area both effects sum up.
In addition to just estimating the system state, the particle filter was also used to predict the future values of the system state and as thus the future dependability of the system. In this setup only the prediction for the next time step was used.

5 CONCLUSIONS

Dependability is of great importance for autonomous mobile systems. Not only for measuring the dependability, but also for comparing it to other missions of the same system or other systems aswell, a formal definition of dependability is important. The definition of dependability used in this paper is based on a mathematical description of the system and its behavior. This property was used in this paper to propose a method for estimating the dependability of an autonomous mobile system using a particle filter.

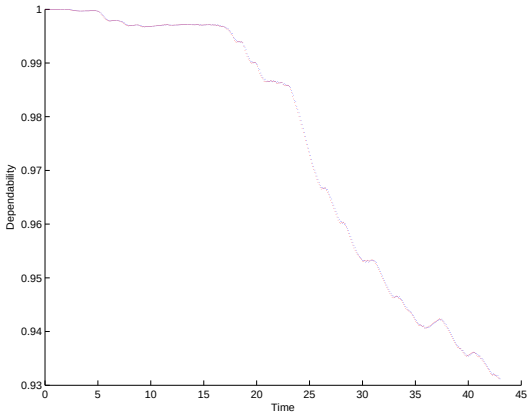


Figure 7: Measured (red) and predicted (blue) dependability of the autonomous mobile system.

REFERENCES

Arlat, J., Aguera, M., Amat, L., Crouzet, Y., Fabre, J.-C., Laprie, J.-C., Martins, E., and Powell, D. (1990). Fault injection for dependability validation: A methodology and some applications. *IEEE Transactions on Software Engineering*, 16(2):166–182.

Arulampalam, M. S., Maskell, S., Gordon, N., and Clapp, T. (2002). A tutorial on particle filters for online nonlinear/non-gaussian bayesian tracking. *Signal Processing, IEEE Transactions on [see also Acoustics, Speech, and Signal Processing, IEEE Transactions on]*, 50(2):174–188.

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.

Brown, A., Chung, L., and Patterson, D. A. (2002). Including the human factor in dependability benchmarks. *In Proceedings of the DSN Workshop on Dependability Benchmarking*.

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.

Chen, Z. (2003). Bayesian filtering: From kalman filters to particle filters, and beyond. Technical report, McMaster University.

Cukier, M. and Smidts, C. S. (2002). Using bayesian theory for estimating dependability benchmark measures. *In Proceedings of the DSN Workshop on Dependability Benchmarking*.

Department of Defense, U. S. o. A. (1970). Military standard - definitions of terms for reliability and maintainability. Technical Report MIL-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.

Kanoun, K., Madeira, H., and Aria, J. (2002). A framework for dependability benchmarking. *In Proceedings of the DSN Workshop on Dependability Benchmarking*.

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

Mukherjee, A. and Siewiorek, D. P. (1997). Measuring software dependability by robustness benchmarking. *IEEE Trans. Softw. Eng.*, 23(6):366–378.

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 minium set of attributes for a behavioral description of dependability. ICINCO.

Rus, I., Basili, V., Zelkowitz, M., and Boehm, B. (2002). Empirical evaluation of techniques and methods used for achieving and assessing software high dependability. *In Proceedings of the DSN Workshop on Dependability Benchmarking*.

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

Wilson, D., Murphy, B., and Spainhower, L. (2002). Progress on defining standardized classes for comparing the dependability of computer systems.