Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

Behavior Based Estimation of Dependability for Autonomous Mobile Systems Using Particle Filter

Jan Rüdiger Achim Wagner Essam Badreddin *

* *Automation Laboratory, Dept. Mathematics & Computer Science, University of Mannheim, Mannheim, Germany (e-mail: jan.ruediger@ziti.uni-heidelberg.de).*

Abstract: 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 a system is more and more inevitable.
Since autonomous mobile systems are usually described by their behavior it is straightforward to also define the dependability of such a system in a behavioral context. Thus, in this paper, the approach of a behavioral based definition of dependability is used together with a Particle Filter to predict the dependability of an autonomous mobile system at runtime.

In Avizienis et al. [2004a] a taxonomy of Dependability and its threats is presented where the term dependability is seen as an integrated concept that further consists of attributes like availability, reliability, safety integrity etc., threats and means (see Fig. 1).
The list of attributes needed for a dependable system is, however, not fix, see e.g. Candea [2003], Dewsbury et al. [2003], where slightly different attributes for dependability are defined. To evaluate the dependability of a given system one or more of the attributes is usually used, depending on the application.
Depending on the research community and application of the system further attributes are added while other are neglected (see e.g. Rüdiger et al. [2007b]).
Up to now two main approaches can be distinguished:

- the evaluation and validation approach and
- the design approach.

While the first approach tries to measure the dependability on an already built system; the second approach tries to develop techniques for designing dependable hard and software systems.
In Wilson et al. [2002] a classification scheme for dependable systems is proposed based on availability, data integrity, disaster recovery, and security. The system is evaluated against a list of criteria for each dependability factor. The systems are then classified according to their application. This approach, however, lacks a formal method of how the systems are classified or how the attributes are measured and how they influence the classification. This makes, for example, the comparison of dissimilar architectures extremely problematic.
Designing dependable software systems is e.g. covered in Shi and He [2003], Xu et al. [2005], Tichy and Giese [2003]. In Shi and He [2003] the *Software Architecture Model (SAM)*, a formal framework for specifying and analyzing software architecture, is extended to analyze non-functional properties like performance and dependability.
Even if the attributes of dependability are known and accepted, a formal definition for dependability and some of its attributes is still missing. The lack of a formal definition makes the classification and comparison of dependable system nearly impossible. To overcome this problem, a formal definition for dependability is needed not only for measuring and comparing the dependability of an existing system but also for developing techniques for designing new dependable systems. A first formal definition for dependability was therefor proposed in Rüdiger et al. [2007a] solely based on the behavior of the system together with a set of attributes (see Rüdiger et al. [2007b]) adequate for dependable autonomous mobile systems.

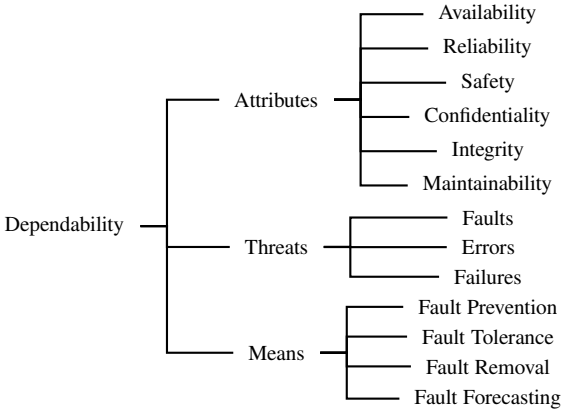

Figure 1. The dependability tree.

When defining the dependability based on the behavior of the autonomous mobile system a filter is needed to predict the future behavior of the system. To predict the future state of a system different algorithm are used, among them *Kalman-Filter*, *Bayesian Filter* and *Particle Filter* (see Chen [2003] for an overview).
The algorithm proposed in this paper to compute the dependability is a continuation of the dependability definition proposed in Rüdiger et al. [2007a]. The proposed algorithm aims to simplify the computation and prediction of the dependability of a system.

The outline of this paper is as follows. In Section 1 the non-formal definitions of dependability are introduced. A short

introduction to the framework of dynamic systems described by their behavior is given in Section 2.1 which is needed to define the elements of the formal dependability definition in Section 2.2 and Section 2.3. A definition for computing the dependability of a system is proposed in Section 3. To be able to estimate the future dependability of an autonomous mobile system a implementation of a Particle Filter is presented in Section 4 which is used in a simulation in Section 4.4.

1. DEPENDABILITY

Dependability is part of the non-functional properties of a system and as such it describes the overall quality of a system. In Rüdiger et al. [2007a] the common non-formal definitions for dependability where used and their ideas transferred to a system defined only by its behavior, which will be described in the following section. Following is a list of the widely used non-formal definitions for dependability (in historical order):

> Carter [1982]: A system is dependable if it is trustworthy enough that reliance can be placed on the service it delivers.
>
> Laprie [1992]: Dependability is that property of a computing system which allows reliance to be justifiably placed on the service it delivers.
>
> Badreddin [1999]: Dependability in general is the capability of a system to successfully and safely fulfill its mission.
>
> 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. The system in our case is a mobile robot and the service this system delivers is the behavior as it is perceived by the user, which in this case is the mission of the mobile robot.

2. BEHAVIOR BASED DEPENDABILITY

2.1 Framework for a theory of dynamical systems

In the framework of Willems (see Willems [1991]) a system is defined in an universe $\mathbb{U}$. 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.
In Willems [1991] a (deterministic) mathematical model of a system is defined as:

Definition 1. A *mathematical model* is a pair $(\mathbb{U}, \mathfrak{B})$ with the universe $\mathbb{U}$ - 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:

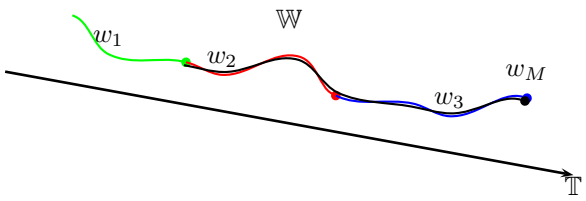

Figure 2. A mission (black line) is accomplished by steering the system to the mission trajectory with the behavior w_1 and then steered along the mission trajectory with the behaviors w_2 and w_3

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.

2.2 Behavior set of an autonomous mobile system

To further investigate the dependability of a system a set of behaviors available to the an autonomous mobile system where defined in Rüdiger et al. [2007a].

Definition 3. 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.

2.3 Mission of a dynamical System

The mission of a dynamical system was defined in Rüdiger et al. [2007a] to be:

Definition 4. 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 $w_m \in \mathfrak{B}$.

The mission of a system was thus just defined as one special trajectory the system trajectory should follow. Note that w_m not necessary needs to be $w_m \in \mathbb{B}$, but only $w_m \in \mathfrak{B}$. Whether the system is able to accomplish the given mission was defined in Rüdiger et al. [2007a] as follows:

Definition 5. A mission $w_m \in \mathfrak{B}$ for a given dynamical system $\Sigma = (\mathbb{T}, \mathbb{W}, \mathfrak{B})$ with the behaviors $\mathbb{B}$ is said to be *accomplishable* by this system if for all $w_1 \in \mathfrak{B}$ there exists a $t \in \mathbb{T}$, $t \geq 0$, a behavior $w \in \mathbb{B}$, $w : \mathbb{T} \cap [0, t] \to \mathbb{W}$ and a behavior $w_2 \in \mathbb{B}$ such that $w' \in \mathfrak{B}$, with $w' : \mathbb{T} \to \mathbb{W}$ 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

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

The definition of a mission and the accomplishment of it is illustrated in Fig.2.

2.4 Safety of a Dynamical System

In case of safety, failures in a system are divided into *fail-safe* and *fail-unsafe* ones. Safety is reliability with respect to failures that may cause catastrophic consequences. Safety is non-formally 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 $\mathfrak{S}$ around $\mathfrak{B}$ was proposed in Rüdiger et al. [2007a], like for example in Badreddin and Abdel-Geliel [2004], Abdel-Geliel and Badreddin [2005], Abdel-Geliel et al. [2005, 2006], which leads to catastrophic consequences when left. This margin is, like $\mathfrak{B}$, highly system specific, but can be set equal to $\mathfrak{B}$ for a restrictive system. The safety area $\mathfrak{S}$ was defined as follows (see Rüdiger et al. [2007a]):

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 $w(t) \in \mathfrak{S}$.

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

3. DEPENDABILITY DEFINITION

After having defined the elements of the non-formal dependability definitions for our system, which are the system itself its boundaries and the mission of the system, a formal definition of dependability for autonomous mobile systems was proposed in Rüdiger et al. [2007a].

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 its mission w_m can be defined as:

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

for the continuous case and for the non-continuous case

$$\mathfrak{D}_\mathfrak{m} = 1 - \frac{1}{t_m} \sum_{\tau=0}^{t} \varepsilon^2(\tau). \tag{2}$$

Where t_m is the mission time and the $\varepsilon^2(\tau)$ is an appropriate quadratic 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 sections.
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

$$\mathfrak{D}(t+\delta) = 1 - \frac{1}{t_m} \underbrace{\left(\int_0^t \varepsilon^2(\tau) d\tau \right.}_{\text{Past}} + \underbrace{\left. \int_t^{t+\delta} \varepsilon^2(\tau) d\tau \right)}_{\text{Future}} \tag{3}$$

in the continuous case and for the non-continuous case

$$\mathfrak{D} + \delta(t) = 1 - \frac{1}{t_m} \underbrace{\left(\sum_{\tau=0}^{t} \varepsilon^2(\tau) \right.}_{\text{Past}} + \underbrace{\left. \sum_{\tau=t}^{t+\delta} \varepsilon^2(\tau) \right)}_{\text{Future}} \tag{4}$$

For computing the future values the $\varepsilon^2(t)$ either a modell of the system, an estimator or a combination of both is used. If for the accomplishment of the mission a set of basic behaviors $\mathbb{B}$ rather than only one behavior is available, the behavior with minimum $\varepsilon^2(t)$ needs to be taken and the future part of dependability thus computes to:

$$\underbrace{\int_t^{t+\delta} \min(\varepsilon^2(\tau)) d\tau}_{\text{Future}} \tag{5}$$

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

3.1 Computing $\varepsilon(t)^2$

For computing the elements of $\varepsilon^2(t) = \Sigma \varepsilon_i^2(t)$ it is not only important to address the distance between the system state and the mission trajectory but also to address the different attributes of dependability discussed in Avizienis et al. [2004b] and defined in a behavioral context in Rüdiger et al. [2007a]. Furthermore, the distance of the system state to the safe area $\mathfrak{S}$ needs also to be taken into account.
All those $\varepsilon_i^2(t)$ depend on the dependability requirements of the system. For simplicity only the distance between the mission trajectory and the system state is used in the following example to demonstrate how the dependability can be measured and predicted with the use of Particle Filter.

3.2 Mission Accuracy $\varepsilon_m^2(t)$

The mission accuracy describes the normalized difference between the mission trajectory and the system state at time t. When evaluating the dependability, $\varepsilon_m^2(t)$ will almost ever be taken into account. Since the error is assumed to be Gaussian distributed the calculation of $\varepsilon_m^2(t)$ is proposed as follows:

$$\varepsilon_m^2(t) = 1 - e^{-1 * \left(\frac{w(t) - w_m(t)}{w_{dev}} \right)^2} \tag{6}$$

The parameter w_{dev} determines how strict a deviation from the desired behavior is judged. The value of this parameter depends on the dependability requirements of the system.

4. DEPENDABILITY PREDICTION

The system trajectory of the system state needs to be sufficiently known in order to be able to predict the future behavior and as thus the dependability of the the system. This can be achieved by a complete model of the system itself together with a complete model of the environment the system is acting in. Since both is rarely available a solution which uses probabilistic algorithms to predict the system state is presented here.
To predict the system state different algorithms are found throughout the literature. Using a Kalman-Filter restricts the state transition and observation model to be a linear functions of the system state. Since we want to examine the dependability of different autonomous mobile systems even the Extended Kalman Filter was neglected in favor of a Particle Filter. This

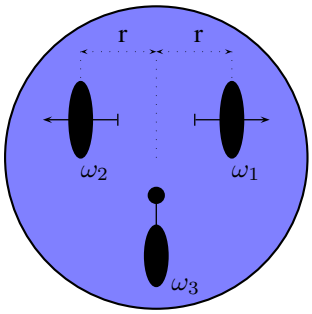

Figure 3. Drawing of the robot used in the simulation. Wheel ω_1 and ω_2 are two independently driven and measured conventional wheels. Wheel ω_3 is an un-driven and un-measured caster wheel.

decision additionally gives us the benefit of being able to examine the dependability of systems described only by a probability distribution function.

For predicting the dependability a filter is needed to compute the probability P for the dependability $\mathfrak{D}$ depending on the system state up to timestep k $x_{0:k}$ and the output of the system k $y_{1:k}$ for the timesteps $1...k$, thus $P(\mathfrak{D}_m|x_{0:k}, y_{1:k})$. Since in the example presented below the dependability is computed as

$$\mathfrak{D}_m(k) = \underbrace{\frac{1}{k}\sum_{0}^{k} d_m(k)}_{\text{Past}} + \underbrace{\frac{1}{k_m - k}\sum_{k+\epsilon}^{k_m} d_m(k)}_{\text{Future}} \qquad (7)$$

computing $P(\mathfrak{D}_m|x_{0:k}, y_{1:k})$ can be reduced to only compute $p(x_k|x_{k-1})$ to indicate that the approach presented here can sufficiently predict the dependability of the system.

To estimate the dependability with probabilistic methods the system is modeled as Markovian, non linear, non-Gaussian state-space model. The system states $\{\mathbf{x}_k; k \in \mathbb{N}\}$ are modeled as a *Markov process* of initial probability distribution $p(\mathbf{x}_0)$ and transition equation $p(\mathbf{x}_k|\mathbf{x}_{k-1})$. Given the process $\{\mathbf{x}_k; k \in \mathbb{N}\}$, the observations $\{\mathbf{y}_k; t \in \mathbb{N}\}$ are assumed to be conditional independent. The model is thus described by

$$\begin{aligned} p(\mathbf{x}_0) \\ p(\mathbf{x}_k|\mathbf{x}_{k-1}) \text{ for } k \geq 0 \\ p(\mathbf{y}_k|\mathbf{x}_k) \text{ for } k \geq 0 \end{aligned}$$

4.1 Motion Model

The robot in the simulation (see Fig. 3) has two degree of freedom (DOF). For evaluating the dependability of this robot the state

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

where x and y are the position of the robot in the floor frame of reference and ϕ is the orientation, is predicted using a Particle Filter. In order to determine the probability distribution of the state of the moving robot a modell of the of the system is needed. The model used in the simulation is:

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

Where δ_s and δ_ϕ are computed using the wheel angular velocity 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.

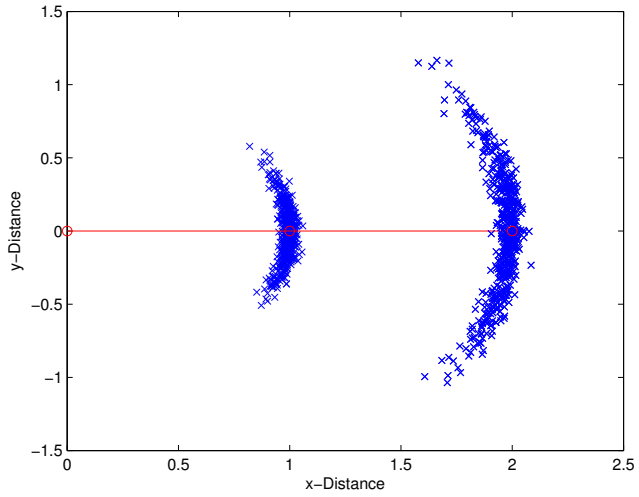

Figure 4. Prediction model (blue crosses) of the robot for a translatory movement of 1m and 2m (red line) used to predict the dependability of the autonomous mobile system

4.2 Observation Model

The observation model used in the simulation is:

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

Where r is the distance between the center of the robot and the contact point of the wheels (see Fig. 3) and δ_X and δ_Y are the distances traveled in X and Y direction transformed from the floor coordinate system into to robot coordinate system.

4.3 Sample Importance Resampling Filter (SIR)

To estimate the system state with a Particle Filter using the *SIR* algorithm the following steps need to be done (see e.g. Arulampalam et al. [2002],Chen [2003])

- sampling from the proposal distribution
- evaluating the weights according to the importance function
- resampling of the weights.

Pseudo-Code of the algorithm used in the simulation is illustrated in Listing 1.

Listing 1. Pseudo-Code of the SIR algorithm used for the simulation

```
FOR p = 1 to numParticles
  % evolve particles using motion model
  x̂_k^(i) ∽ p(x_k|x_{k-1});
  % calculate weights using the observation model
  ω̂_k^(i) = p(y_k|x̂_k^(i));
ENDFOR
FOR p = 1 to numParticles
  % normalize weights
```

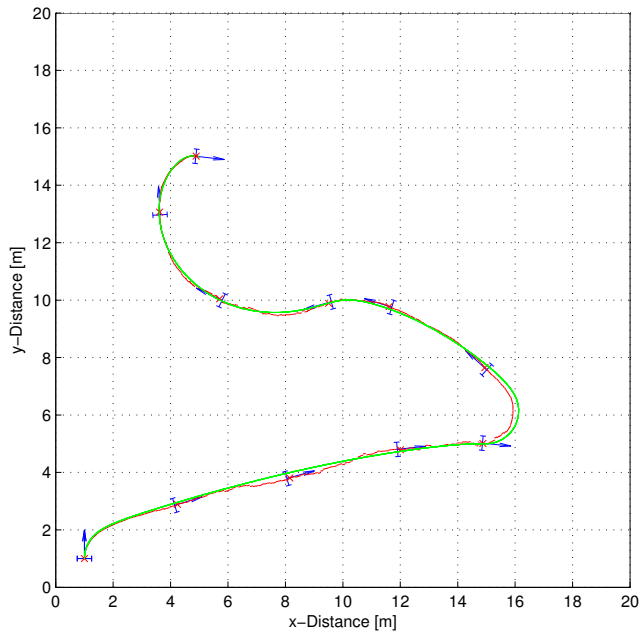

Figure 5. Mission trajectory (green) and estimated trajectory (red) for the autonomous mobile system

$\hat{\omega}_k^{(i)} = \text{normalize}(\hat{\omega}_k^{(i)})$;
ENDFOR
% resample weights
$x_k^{(i)} = resample\_particels(\hat{x}_k^{(i)}, \hat{\omega}_k^{(i)})$;

4.4 Simulation Results

The above discussed algorithm was used in a simulation to demonstrate that the approach of predicting the dependability of an autonomous mobile system using Particle Filter works as expected.
In the simulation, noise was added to the measurement to simulate sensor or actuator degeneration and model uncertainty that would under normal circumstance decrease the dependability of the system.
The mission trajectory given to the system for the simulation is shown as a green curve in Fig. 5 and Fig. 7. The red curve in Fig. 5 denotes the real trajectory of the robot. In Fig. 7 the particles used for estimating the system state for every 40s time step are presented. Finally the dependability of the autonomous mobile system predicted four steps ahead using the Particle Filter (blue curve) together with the measured dependability (red curve) is presented in Fig. 6.
Due to the noise added to the measurement vector to simulate a actuator or sensor degeneration and the control error the dependability of the system decreases during the simulation. Note that the decrease is bigger during turns in the mission trajectory where robot is not able to directly follow the mission trajectory, which is consistent with the assumptions made in the model.

5. CONCLUSION

Dependability is getting a more and more important non functional property of a system. Especially for autonomous mobile systems it is import to measure and predict its dependability. Measuring the dependability according to the service a system

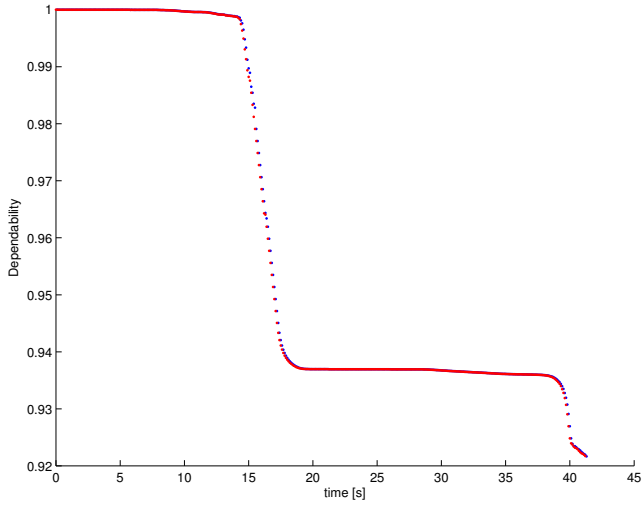

Figure 6. Measured (red) and predicted (blue) dependability of the autonomous mobile system

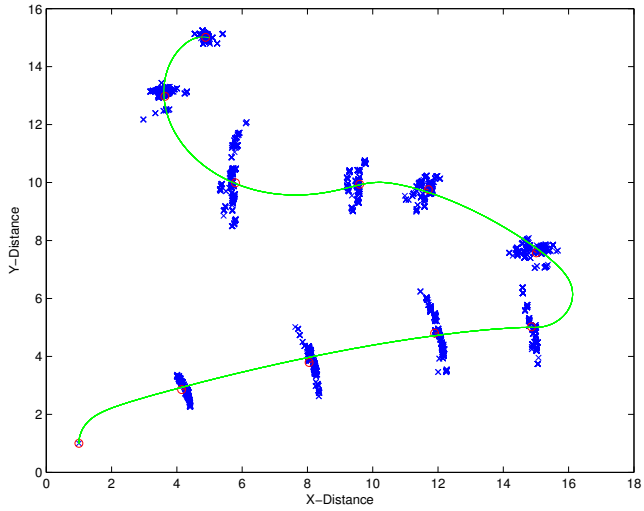

Figure 7. Particles used for the state estimation (blue crosses) plotted for every 40s time step together with the mission trajectory (green)

delivers and thus on the behavior expected by the user is an important step for a system independent dependability measurement. This approach was used in this paper together with a Particle Filter to estimate the future behavior of the system and to compute the dependability at runtime. The results show that the estimated dependability of the system is, at least for this example, close to the dependability measured after the mission. Thus, predicting the dependability for an autonomous mobile system using Particle Filter was demonstrated to be a feasible approach.

REFERENCES

M. Abdel-Geliel and E. Badreddin. Dynamic safety margin in fault diagnosis and isolation. In *European Safety and Reliability (ESREL) conf.*, June 27-30 2005.
M. Abdel-Geliel, E. Badreddin, and A. Gambier. Dynamic safety margin in fault-tolerant predictive controller. In *Control Applications, 2005. CCA 2005. Proceedings of 2005*

IEEE Conference on, pages 803–808, 28-31 Aug. 2005. doi: 10.1109/CCA.2005.1507227.

M. Abdel-Geliel, E. Badreddin, and A. Gambier. Application of model predictive control for fault tolerant system using dynamic safety margin. In *American Control Conference, 2006*, page 6pp., 14-16 June 2006. doi: 10.1109/ACC.2006.1657598.

M. S. Arulampalam, S. Maskell, N. Gordon, and T. Clapp. 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, 2002. URL `http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=978374`.

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

Algirdas Avizienis, Jean-Claude Laprie, and Brian Randell. Dependability and its threats: A taxonomy. 2004b.

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

E. Badreddin and M. Abdel-Geliel. 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, 2-4 Sept. 2004.

George Candea. The basics of dependability, September 2003.

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

Zhe Chen. Bayesian filtering: From kalman filters to particle filters, and beyond. Technical report, McMaster University, 2003. URL `http://math1.unice.fr/~delmoral/chen_bayesian.pdf`.

G. Dewsbury, Ian Sommerville, K. Clarke, and Mark Rouncefield. A dependability model for domestic systems. In *SAFECOMP*, pages 103–115, 2003.

Elena Dubrova. Fault tolerant design: An introduction, March 2006. Draft.

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

Jan Rüdiger, Achim Wagner, and Essam Badreddin. Behavior based definition of dependability for autonomous mobile systems. European Control Conference 2007, July 2-5 2007a. Kos, Greece.

Jan Rüdiger, Achim Wagner, and Essam Badreddin. Behavior based description of dependability - defining a minium set of attributes for a behavioral description of dependability. ICINCO, 2007b.

Tianjun Shi and Xudong He. Dependability analysis using SAM. In *Proc. of the ICSE Workshop on Software Architectures for Dependable Systems*, pages 37–42, June 2003.

Matthias Tichy and Holger Giese. An architecture for configurable dependability of application services. In Rogerio de Lemos, Cristina Gacek, and A Romanowsky, editors, *Proc. of the Workshop on Software Architectures for Dependable Systems (WADS), Portland, USA (ICSE 2003 Workshop 7)*, 2003.

J.C. Willems. Paradigms and puzzles in the theory of dynamical systems. *IEEE Transactions on Automatic Control*, 36(3): 259–294, March 1991. doi: 10.1109/9.73561.

Don Wilson, Brendan Murphy, and Lisa Spainhower. Progress on defining standardized classes for comparing the dependability of computer systems, June 25th 2002. URL `citeseer.ist.psu.edu/wilson02progress.html`.

Lihua Xu, Hadar Ziv, Debra Richardson, and Thomas A. Alspaugh. An architectural pattern for non-functional dependability requirements. In *WADS '05: Proceedings of the 2005 workshop on Architecting dependable systems*, pages 1–6, New York, NY, USA, 2005. ACM Press. ISBN 1-59593-124-4. doi: http://doi.acm.org/10.1145/1083217.1083219.