Online Risk Assessment for Safe Autonomous Mobile Robots - A Perspective

H. Voos, P. Ertle *

* Mobile Robotics Lab, University of Applied Sciences
Ravensburg-Weingarten, Germany, (e-mail: voos@hs-weingarten.de).

Abstract: In the near future, mobile service robots are expected to provide services in all spheres of life. They have to execute demanding and complex tasks in a dynamic environment, collaborate with human users in a natural and intuitive way and adapt themselves to varying conditions. The necessary flexible and intelligent behavior however can only be achieved by mobile service robots with a high degree of autonomy. While much effort in research is spent on the investigation and realization of autonomous service robots, it is often neglected that a higher degree of autonomy also results in higher safety requirements, especially if these autonomous robots have to interact closely with human users. This work gives a perspective on the design of safe autonomous service robots using online risk assessment.

1. INTRODUCTION

Mobile service robots are intended to provide services in various domains of life. Herein, the main challenge for the robot is the execution of complex tasks within an unstructured dynamic environment while collaborating with human users in a natural and intuitive way. In order to achieve the necessary highly flexible behavior, mobile service robots must have a high degree of autonomy. The development of autonomous mobile robots has been studied since decades, leading to many published possible approaches and successful implementations, see e.g. Siciliano [2008] for a comprehensive overview. However, although much effort is spent on the investigation and realization of autonomy, it is most often neglected that autonomous robots are also causing new types of safety problems. While a safe stationary robotic manipulator can be obtained by avoiding any collisions with users or the environment (e.g. with the help of a separating safety cage), this is no longer the case for autonomous mobile robots. Here, touching human persons might be even necessary on the one side, while also the pure decisions of the robot, e.g. delivering a requested medicine, could also cause safety-critical situations on the other side.

This work focuses on a perspective for the development of safe autonomous mobile robots. While processes and measures for the design of safety-critical technical systems in general exist, both the structural and behavioral complexity of an autonomous mobile robot requires measures to ensure safety that are far beyond the currently existing approaches. Since passive methods like simulation, testing or software verification and validation turned out to be rather ineffective for the complex control software of an autonomous robot, this approach mainly focuses on a supervisory system as an active method that checks safe operation of the robot during runtime.

The work is organized as follows. First, autonomous robots are identified as safety-critical systems, and current approaches for the development of safe robots are discussed.

Since safety can be interpreted as a special state of the robot-environment-interaction, any method to check safety during operation requires a suitable modeling approach of this interaction. Here, we propose the extended Situation-Operator-Model (exSOM) for this purpose. Using the ex-SOM model, a possible control architecture for a safe autonomous robot will be derived, which includes risk assessment, risk-dependent planning on a deliberative and model-predictive control on a reactive layer. Finally, simulation and experimental results are presented for a first proof of concept.

2. SAFETY ASPECTS OF AUTONOMOUS ROBOTS

2.1 Robots as Safety-Critical Systems

Safety-critical systems are those systems whose failure could result in loss of life, significant property damage or damage of the environment. Therefore, a system is called safe if we can ensure that risks are kept at an accepted level (IEC61508 [2005]). Herein, risk is the possibility of injury, loss or environment incident created by a hazard, while the significance or level of the risk is generally determined by the probability of an unwanted incident and the severity of the consequences. Safety of technical systems is enforced by regulations formulated in laws and directives, and different directives exist for different technical domains. In order to fulfill the requirements of these safety-related regulations, well-established processes and measures for the development of safety-critical systems like air- and spacecrafts or automobiles have been developed, see e.g. Börcsök [2007], including reliability and risk analysis, redundancy, fault and event tree analysis, simulation and testing or formal verification to mention only a few.

Mobile robots have a considerable mass and kinetic energy during operation, they share the same environment with human users and autonomous mobile robots are in addition even enabled to come to own decisions. Therefore, mobile robots and especially those with a higher degree of autonomy are clearly safety-critical systems. Robots in

general belong to the class of machines and therefore are in the scope of the directives EN ISO 13849 for safety of machinery and EN ISO 10218 for industrial robots sharing workspace with humans. However, these directives are mainly considering industrial (stationary) robots, where the general goal of safety is to reduce the collision energy. Therefore, small and weak industrial robots are already certified as safe systems. While the application of heavy and strong industrial robots without a safety cage has been permitted in the past, the new directive EN ISO 10218 also allows automatic operation of (industrial) robots in cooperation with humans. Hereby, the work of humans in the operating range of the robots is enabled through sufficient protection, realized by suitable sensors and automatic control systems. However, mobile robots are so far not directly included in any of these directives, and also autonomous systems are not considered, too.

Some first contributions that are especially focused on the development of safe autonomous mobile robots can already be found in the literature, see e.g. Sommerville [1997], Simmons [2000], Voos [2007] or Wardzinski [2008]. However, most of these papers are mainly focusing on single aspects of this special safety-related problem like software verification, special redundant hardware systems, special software development processes or risk assessment. In this paper, the main focus is on a more comprehensive overall process and system architecture. Nevertheless, the development of safe autonomous mobile robots should first of all also include all the already mentioned well known development processes and measures for safety-critical systems in general, see e.g. Börcsök [2007]. Most of these measures however are passive, i.e. they are applied during the development phase in order to achieve a safe system. This includes a safety-related analysis and a suitable design of the mechanical and electrical/electronic parts. Regarding the software part, the choice of a suitable operating system and programming language could increase safety, but also methods of computer science like programming guidelines, verification and validation of the software etc. could be applied. From a control engineering point of view, robust control methodology also contributes to the passive measures that increase safety of mobile robots.

However, it is typical for all passive safety measures that the possible hazards and failures must be foreseen and included in the safety case during development. In addition, previous investigations led us to the conclusion that software testing, verification and validation is not effective if applied to a complex autonomous robot control system, see e.g. Simmons [2000], Voos [2007]. It turned out that safety is always related to the overall state of the robot and the environment, also including human persons, and it is nearly impossible to foresee all possible interactions between robot and environment at design-time. Nevertheless, also these passive methods should be applied to contribute to the task of designing a safe autonomous robot, however their application alone is not sufficient.

Therefore, it seems to be more promising to add active measures to ensure safety in the case of autonomous mobile robots or autonomous systems in general, see e.g. Wardzinski [2008]. These measures are active during the operation of the mobile robot in order to ensure safety.

During operation, the risk of failure is mainly influenced by the correctness of the state of operation of the robot, the correctness of the application and finally the correctness of the behavior of the robot. The correct state of operation includes correct functioning of the sensors, the computer systems as well as the actuators. Correct application of a robot means that the robot is applied in a specific task as originally intended, i.e. not operated outdoor if originally intended for indoor application. Finally, correct behavior means that the robot is fulfilling its tasks and reaching its goals as planned, also including "safe" behavior. Here, the main focus is on this last aspect, i.e. to find measures that enable the robot to fulfill its tasks and reach its goals while keeping the risk below an accepted level. The related concept is described in the following.

2.2 An Approach for Designing Safe Autonomous Robots

We assume a mobile robot which is intended to move freely in a dynamic environment and to interact with objects and human persons over a longer period of time in order to solve given tasks. During this period of operation, possible hazards could occur creating a certain risk in the previously described sense. The mobile robot will be considered as being safe if at all times during operation the risk is kept below an accepted level (Börcsök [2007]). However, this risk does not only depend on the robot itself but clearly also on the dynamic environment. Therefore, risk assessment is a basic feature of the proposed approach and must be a dynamic process that takes the overall state of the robot and the environment as well as the interaction between robot and environment into account.

That first of all requires a suitable model of the robot-environment-interaction, i.e. a suitable world model. For that purpose, we will apply an extended version of the so-called "Situation-Operator-Model" (exSOM) derived by Söffker [2008], which will be described in more detail in the next section. The core of this exSOM-approach is the assumption that the real world is modeled as a sequence of discrete-time situations and operators. Situations describe the current state of the world comprising the robot and the environment as perceived by the robot. The transition from one situation to the next is caused by operators. The exSOM-based world model is also one of the basic components of the active safety concept. Since it is nowadays widely recognized that efficient robot control architectures are combining reactive control and deliberation to a hybrid deliberative/reactive architecture (Murphy [2000], Siciliano [2008]), this architecture is also adopted here for robot control.

In a hybrid deliberative/reactive architecture, complex and long-term planning tasks based on the world model are solved on a deliberative layer, then the generated plans are executed in a reactive fashion by the activation of a set of suitable behaviors in the underlying reactive layer (Murphy [2000]). These layers are extended in this work in order to achieve the active safety concept. On the deliberative layer, the planning and decision making procedures also take the result of the risk assessment of the current and future predicted situations into account. The generated plans therefore must lead to situations whose risk is always kept under the accepted level. On the reactive layer, the
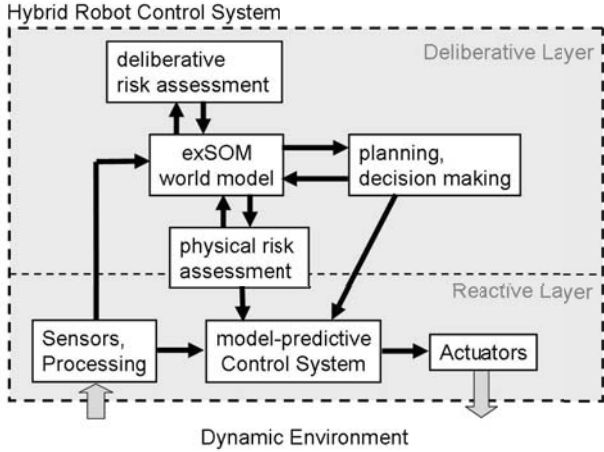
Fig. 1. Structure of the extended hybrid robot control system.

risk assessment of the situations must also be considered during the activation of suitable behaviors. In the proposed approach, this reactive behavior and the coordination of the behaviors is solved by the help of a model-predictive control approach. Hereby, the execution of the plans is formulated as an optimization problem while the safety aspects as a result of the risk assessment are forming constraints. An online optimization finally leads to the optimal action while keeping the safety constraints. The overall structure of this architecture is shown in Fig. 1 and will be further detailed in the following.

3. THE EXTENDED SITUATION-OPERATOR MODEL OF AUTONOMOUS ROBOTS

One of the basic modules of the hybrid robot control architecture and also the basis for risk assessment is the already mentioned exSOM model, which will therefore be explained in more detail. The "Situation-Operator-Model" (SOM) as developed by Söffker [2008] extends classical ideas of the situation and event calculus to a more comprehensive cognitive framework that allows the modeling of the structure of complex scenes. Herein, the reality of the real world, such as a mobile robot in its environment, is mapped to a formal representation. In our work, the SOM approach has been further adapted to robotics and is called extended SOM (exSOM). The core of the exSOM-approach is the assumption that the real world could be understood as a sequence of situations and operators. Since all robots are equipped with digital computer systems which work in a discrete-time manner, this timing model will also be applied to the SOM approach: the robot internally generates the situations at discrete time steps with a constant sampling time ΔT.

Each situation is that extract and internal representation of the real world which is of current interest for the robot. The situation is described by a suitable set of significant facts, the so-called characteristics. The characteristics could be numerical, boolean or linguistic variables, but also more complex data structures like images etc. They include information which is perceived from the external world, i.e. the environment, with the help of suitable sensors and signal processing, and also information of the current physical and cognitive state of the robot, e.g. the

current active goals and plans. The accuracy of the characteristics mainly depends on the considered sensor information. Characteristics can be defined by the developer or autonomously extracted from data by the robot during operation. A situation is generated at each discrete time step $t = k \cdot \Delta T, k = 0, 1, \ldots$, denoted by $S(k)$, and comprises the set of all characteristics $\{C_i(k)\}, i = 1, 2, \ldots, n(k)$. Herein, $n(k)$ is the current number of characteristics, which could change during operation since some new information might arise while other information might become less relevant for the robot. For instance, possible characteristics of a robot could be the current value of the velocity $C_1(k) = v(k)$ and the current main goal $C_2(k) = \texttt{Deliver\_Drug}$.

Changes in the real world are represented by so called operators. The operators are linking the situations in a way that the situation snapshot at any point in time is transferred by an operator to the following situation (Söffker [2008]). In accordance with the previous defined discrete-time description, the operators are assumed to be applied at each time step k and lead to a new situation at time step $k + 1$. Operators could be changes of the characteristics of a situation based on physics and thus described by differential or difference equations. However, operators could also be more abstract changes of the characteristics caused by discrete events or computational algorithms which run in the robot's control system. An operator i at time step k is denoted by $O_i(k)$, where a finite number $i = 1, \ldots, m(k)$ of operators is assumed. At any time step k, several operators could be applied in parallel, which is depicted in Fig. 2. For further details of the underlaying SOM approach, we also refer to Söffker [2008]. The exSOM approach finally offers a possibility to model
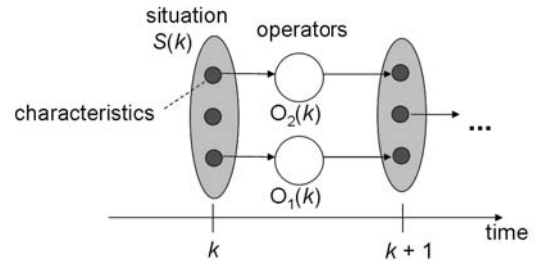

Fig. 2. The basic structure of the exSOM modeling approach.

the robot-environment-interaction in a more formal way in the robot control system. In the following, safety aspects of autonomous robots will be discussed with respect to the exSOM model.

4. CONCEPT FOR SAFE AUTONOMOUS ROBOTS

4.1 Online risk assessment using the exSOM approach

As previously defined, a mobile robot will be considered as being safe if at all times during operation, the risk is kept below an accepted level. In the discrete-time description of the exSOM approach, safety is a property of any situation $S(k)$ at any time step k, and is described by a risk value which is assigned to the situation. This risk value clearly depends on the values of the current set of characteristics $\{C_i(k)\}$ and thus also depends on both robot and environment. A risk value of a situation

describes the probability of an unwanted incident in the future and the severity of the consequences, given the current set of characteristics. In this approach, a risk is only assigned to situations and not directly to operators. Therefore, operators transfer a current situation with a given risk into the next situation with the resulting risk, respectively.

However, the calculation of the risk in a pure mathematical sense as a product of the probability of an incident and the severity of the consequences would be a rather difficult procedure. That would require an enormous effort of numerous experiments and statistical evaluations of the situations. On the other side, it is obvious that also human beings as the most advanced "autonomous systems" are assessing the risk of situations and deciding risk-depending without calculating the risk values in the strict mathematical sense. Here, humans tend to consider risk more as a qualitative property of a situation. For instance, if we should put our hand on a stove without having any more information, we would assign at least a medium risk to this situation, since the stove could be rather hot and burn our hand. However, in that situation we would certainly not be able to calculate the precise risk value of the given situation and base our decision on this.

Therefore, in order to describe the risk of a situation with regard to the related values of the characteristics in the mobile robot application, a qualitative, linguistic approach seems to be more suitable, which could be realized with the help of a fuzzy system. Fuzzy systems are a well established methodology to describe and process qualitative expert knowledge and the whole mathematical background of fuzzy logic is omitted here (see e.g. Levin [1996]). The fundamental elements of a fuzzy system are the fuzzy sets and the rule base. The methodology of the fuzzy sets represents the human interpretation of measured variables. In a fuzzy system, the input variables are interpreted as linguistic variables which are described in linguistic terms. The rule base of a fuzzy system contains a number of IF–THEN–rules which are connecting preconditions and related conclusions both formulated with the help of the linguistic variables.

However, the definition of such a fuzzy system for risk assessment also requires the assignment of a range of values to the risk. Here we assume normalized risk values of a situation $S(k)$ which are real numbers out of the interval between 0 (no risk at all) and 1 (highest risk, i.e. incident is already happening). In addition, if we consider the range of tasks of an autonomous mobile service robot, it seems to be suitable to distinguish between two types of risk: a risk that is mainly concerned with the real physical environment (called physical risk) and a risk which is related to logical decisions of the robot (furthermore called deliberative risk). A look at a service robot which has the task to deliver a medicine, e.g. in the form of a yellow box, could clarify the reason for this interpretation. Since the service robot has to move in the environment of the human user and even has to come quite near to this person, there is always the risk of injury because of a collision between human and robot with a too large kinetic energy. This physical risk always exist and must be taken into account. On the other side, even if the robot moves with a very low velocity minimizing the kinetic energy, also the pure

deliberative capabilities of the robot like decision making could result in a considerable risk for the human user. This would be the case if the robot decides to bring a box without being sure that this is the correct yellow box. In this case, the box might contain another medicine which could be rather dangerous, and there is a considerable deliberative risk. In addition, as already depicted in Fig. 1, the two risk types are considered and processed in different levels of the robot control system, since the physical risk is more related to direct reactions and the deliberative risk is more related to planning and decision making.

Taking these considerations into account, we assign the normalized range of values to the two mentioned risk types $R_{phy}(S(k)), R_{del}(S(k)) \in \mathbb{R}^+$ of situation $S(k)$, i.e. the physical and the deliberative risk:

$$0 \le R_{phy}(S(k)), R_{del}(S(k)) \le 1 \qquad (1)$$

If the risk is interpreted as a linguistic variable, linguistic terms have to be defined such as ZERO, SMALL, MEDIUM, LARGE and V_LARGE, which finally form the fuzzy sets as depicted in Fig. 3 using triangular membership functions.
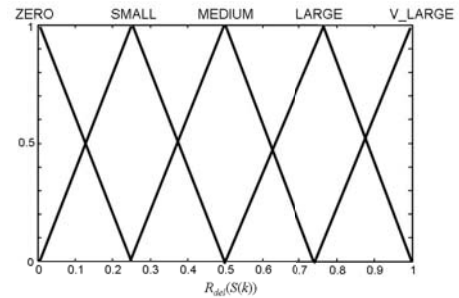

Fig. 3. The fuzzy sets of the linguistic variable $R_{del}(S(k))$.

The input variables of the fuzzy system for risk assessment are the characteristics of the situation $\{C_i(k)\}$ using the exSOM model. Also these characteristics are now interpreted as linguistic variables with assigned linguistic terms and membership functions. Now, the knowledge about the risk of a situation is formulated as the rule base of the fuzzy risk assessment system. Because of the mentioned reasons, we distinguish between a logical and a deliberative risk assessment which are both realized as a fuzzy system, respectively (see also Fig. 1).

The deliberative risk assessment takes that risk into account which is mainly caused by the current goals of the service robot in the actual context. Therefore, the main input variables of this assessment are the goals of the robot and the current sensor information about the environment together with a confidence value. Since the goals are given internally in a deterministic form as results of the planning and decision process, the respective sets are crisp sets. If the only information is the pure goal and no further information is available, the risk of the goal itself also determines the risk of the current situation, i.e. a possible fuzzy rule could be

IF   (Goal=Deliver_Drug)   THEN $R_{del}(S(k))$=LARGE

Herein, the only current information is the existence of a goal to deliver a drug. However, without any further information, this is per se a risky goal and therefore the

deliberative goal is set to a large value. If the vision system delivers the additional information that the object that has been gripped by the robot is a yellow box (which is the correct one) and the confidence of this perception is high, the risk would be assessed as being small:

```
IF   (Goal=Deliver_Drug)  AND  (Conf(Obj_Yellow_Box)=HIGH)

THEN   R_del(S(k))=SMALL
```

The physical risk takes that risk into account which is caused by the physical interaction of the robot and the environment, also including human persons. For instance, the physical risk would be assessed as high, if a detected object is a person (with a high confidence) and the distance is small, i.e.

```
IF   (Distance=SMALL) AND (Conf(Obj_Person)=HIGH)

THEN   R_phy(S(k))=LARGE
```

It becomes obvious from these considerations that the sensor and image processing algorithms also have to deliver confidence values in this realization of an online fuzzy risk assessment.

One remaining question considers the completeness of the safety-related knowledge which is included in the two rule bases of the risk assessment systems. We assume that a first definition of the rule bases is based upon the expert knowledge of the engineers during the design phase. Since this knowledge normally will be incomplete and not cover all possible situations with a considerable risk, learning will be applied in the future realization. Here, reinforcement learning could be a suitable approach, where a human supervisor enters his own risk assessment results with the help of a suitable man-machine-interface during robot actions in simulations or experimental runs.

In the overall robot control system according to the hybrid deliberative/reactive architecture shown in Fig. 1, the two fuzzy risk assessment systems are connected with the exSOM-based world model of the robot. In each situation $S(k)$, the values $\{C_i(k)\}$ of the characteristics are updated and the risk assessment takes place. The resulting values $R_{phy}(S(k)), R_{del}(S(k))$ are calculated and included as additional characteristics in the exSOM-based world model, see Fig. 4. These extended situations are then used by the planning and decision systems on the deliberative layer and the model-predictive control system on the reactive layer.

4.2 Risk-based extension of deliberative and reactive layer

The physical and deliberative risk values which are finally calculated and stored as characteristics in the exSOM world model are then used to influence the next actions of the autonomous mobile robot. On a deliberative layer, the planning and decision process of the autonomous robot is also adapted to the exSOM-based world model leading to a system architecture as described in Ahle [2008]. First, the actual situation $S(k)$ is extracted from the world model. In the exSOM representation of the robot-environment interaction, operators are now applied (and realized) which finally lead to the following situation $S(k+1)$ in the next time step. One or more goals are provided to the system, translated into the exSOM description and formed to a desired situation that the robot finally intends to
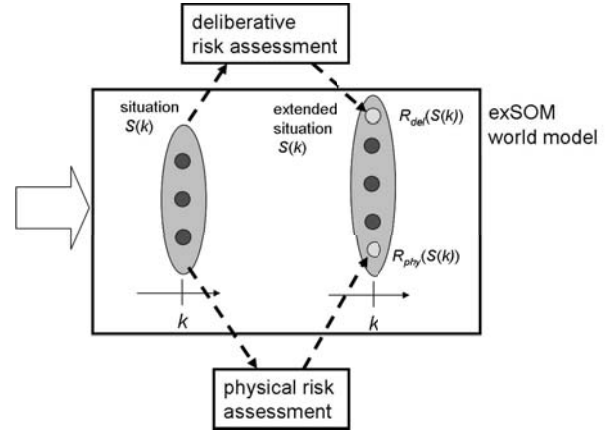

Fig. 4. The online risk evaluation using the exSOM world model.

reach with the help of a sequence of suitable operators. In addition, a knowledge base exists which contains the known operators with probabilities that the application of this operator in a specific initial situation $S_i(k)$ leads to the specific final situation $S_f(k+1)$.

Now, two main processes take place in parallel on this deliberative layer: a planning and decision making process and a learning process. The planning process compares the actual situation $S(k)$ with the generated desired situation $S_d(k+K)$ where K is the planning horizon in discrete time steps. To generate a plan, the information from the knowledge base that includes the operators as well as the risk assessment systems are used. A sequence of operators to reach the desired situation could be found by generating a tree of situations and operators and to conduct deepening depth-first search, see Ahle [2008] (however, any other planning procedure could also be applied). Herein, all generated situations during the planning procedure are always extended by the deliberative risk values. Therefore, the risk values could also be used to form objectives for the planning procedure, e.g. to find that plan that reaches the desired situation while including only intermediate situations with a risk value that is below a threshold (i.e. a "safe plan"). If a plan is generated, the included operators are applied time step by time step and the result of the application is always checked. If the resulting situation is not equal to the situation expected during planning, the operators knowledge data base is updated by a learning process and a new plan is generated. For the details of the learning procedure, we refer to Ahle [2008].

While these generated higher level plans are including the deliberative risk, the physical risk is mainly included in the processes on the reactive layer. The reactive layer gets the higher level plans, e.g. in the form of a desired path given by waypoints or gripping tasks etc. On the reactive layer, these plans are executed with the help of model predictive control algorithms. Model predictive control is a method from control engineering (for an introduction see e.g. Allgoewer [1999]) which is especially suited to include all different types of constraints. The essence of this approach is to optimize, over the manipulatable inputs, forecasts of the behavior of a dynamic process. The forecasting is accomplished with a process model over a finite time interval, the prediction horizon. Only the first

input of the optimal input sequence is injected into the plant and the problem is solved again in the next time step using updated measurements (Allgoewer [1999]). During the optimization, also equality and inequality constraints could be taken into account.

Here, the underlying control tasks of the robot on the reactive layer, e.g. following a path or solving a gripping task, are controlled with the help of suitable formulated model predictive control algorithms. In order to enable the model predictive control approach in realtime on the reactive layer, the physical risk assessment is not applied to all forecasts (which would lead to a rather complex calculation during the realtime optimization), but is used to form differential constraints like maximum values of the velocities, accelerations or turn rates or constraints like minimum distances etc. For instance, if the physical risk in the current situation is assessed as being large (e.g. because the robot is near to a human), the maximum values of the velocities as constraints are set to a low level and a minimum safety distance (if applicable) is also commanded. This finally leads to the realtime execution of the control tasks on the reactive layer while including the safety aspects in a very straightforward way, see also Voos [2009] for details.

5. EXPERIMENTAL RESULTS AND FUTURE WORK

The proposed approach to design safe autonomous mobile robots is currently implemented and tested in a Pioneer 3 DX from ActiveMedia Robotics which is also equipped with a lightweight manipulator from Neuronics and numerous sensors, including a stereo vision systems and a Sick Laser Scanner. The robot control system as proposed also including the exSOM approach is implemented with the help of the SmartSoft Robotic Software framework. A result of the risk assessment during a test scenario is shown in Fig. 5. In this scenario, the service robot is
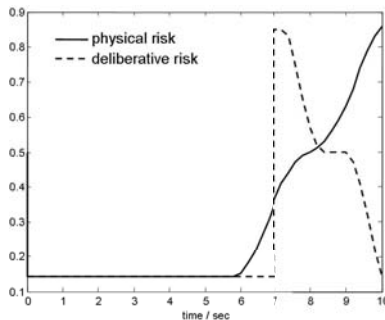

Fig. 5. Online risk evaluation during test scenario.

approaching a human person, and therefore the physical risk is continuously increasing with decreasing distance. However, this leads to a reduced velocity and acceleration because of the model predictive control approach on the reactive layer. At $t = 7$ sec, the robots gets the goal to deliver the medicine in the yellow box. At the same time, the box is perceived by the optical sensors and the image processing system, but the confidence that the perceived box is yellow is calculated as being low at the beginning. The box is gripped and over the next time interval, the confidence that the box is yellow is increasing because the

illumination was getting better. Hence the deliberative risk is decreasing, as shown in Fig. 5.

In Fig. 6, a simulation result of the model predictive control system on the reactive layer is shown. Herein, the task of the considered robot 1 was to follow a defined path given by waypoints commanded from the deliberative layer and to keep a minimum distance of 0.4 m to another moving robot 2. It can be seen that the result is the optimal compromise between path following (left figure) and keeping the safety constraints, i.e. the minimum distance (right figure).
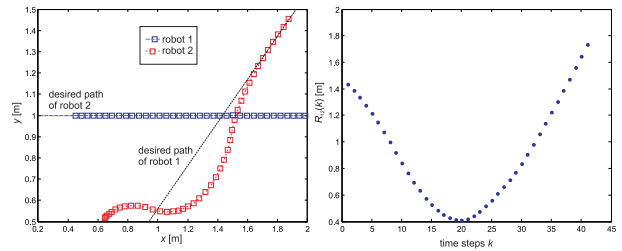

Fig. 6. Result of the model predictive control system.

Besides these first simulations and experimental approaches, further experiments and extensions are currently going on to improve the system and to apply it to more complex real world applications.

REFERENCES

B. Siciliano, O. Khatib (Eds.). *Springer Handbook of Robotics.* Berlin, Heidelberg, New York: Springer, 2008.

Funktional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission, Geneca, Switzerland (2005).

Börcsök, J. *Functional Safety: Basic Principles of Safety-related Systems.* Hüthig Praxis. Hüthig, Heidelberg, 2007.

Voos, H.; Hochgeschwender, N. Verification of Autonomous UAV Systems: A Perspective. In Proc. of IASTED Symposium on Robotic Applications RA 2007, Würzburg, Germany, 2007.

R. Simmons; C. Pecheur; G. Srinivasan. Towards Automatic Verification of Autonomous Systems. In Proc. of IEEE/RSJ Int. Conf. on Intelligent Robots and Systems, Takamatsu, Japan, 2000.

I. Sommerville; D. Seward; R. Morrey; S. Quayle. Safe Systems Architecture for Autonomous Robots. In Proc. of the 5th Safety-critical Systems Symposium, Brighton, UK, 1997.

Wardzinski, A. Dynamic Risk Assessment in Autonomous Vehicles Motion Planning. In Proc. of the 2008 1st Int. Conf. on Information Technology, Gdansk, Poland, 2008.

Söffker, D. Interaction of intelligent and autonomous systems - part 1: Qualitative structuring of interaction. *Mathematical and Computer Modelling of Dynamical Systems* 14, 303318, 2008.

R. Murphy. *Introduction to AI robotics.* Cambridge, Mass.: MIT Press, 2000.

Levin, W. (ed.). *The Control Handbook.* CRC Press, Boca Raton, 1996.

E. Ahle, D. Söffker. Interaction of intelligent and autonomous systems - part 2: realization of cognitive technical systems. *Mathematical and Computer Modelling of Dynamical Systems* 14, 319339, 2008.

F. Allgoewer et al. *Nonlinear predictive control and moving horizon estimation An introductory overview.* In: P. Frank (ed.), Advances in Control, Highlights of ECC99, Springer, London, pp. 391449, 1999.

H. Voos. Model Predictive Collaborative Motion Planning and Control of Mobile Robots including Safety Aspects. In Proc. of the Int. Conference on Advanced Robotics ICAR 2009, Munich, 2009.