A Surveillance and Safety System based on Performance Criteria and Functional Degradation for an Autonomous Vehicle

Andreas Reschka, Jürgen Rüdiger Böhmer, Tobias Nothdurft, Peter Hecker, Bernd Lichte, Markus Maurer

Abstract— **Autonomous driving in urban environments is potentially dangerous since a malfunction of vehicle guidance systems can lead to severe situations for passengers inside the autonomous vehicle and other road users. Therefore both, monitoring the current system operation state by a surveillance system, which is able to detect failures of software and hardware modules, and a safety system, which reacts on these failures immediately, is necessary.**

In this paper an approach based on performance criteria and functional degradation is proposed, which is used in the autonomous vehicle Leonie developed within the Stadtpilot project. The surveillance part of the system collects data from sensors, software modules, hardware, and the vehicle to combine this data with heuristics to performance criteria. Based on these criteria degradation actions are executed to keep the operation of Leonie in a safe state. The safety system can influence driving maneuvers like lane changes and turning maneuvers, modify driving parameters like maximum speed and safe time headway and even force driving maneuvers like emergency stops and controlled stops at the side of the road.

Currently, the safety driver onboard of Leonie is the fallback solution in case of a system malfunction. Using the proposed safety system should reduce the number of situations where the safety driver has to take control over the vehicle though.

I. Introduction

A. Stadtpilot Project

Stadtpilot[1] is a research project at the Technische Universität Braunschweig. The project goal is to drive fully autonomous on the inner city ring road of Braunschweig, Germany. Many different road users, poor GPS reception, traffic lights, intersections, as well as changing road and weather conditions make autonomous urban driving very challenging. The vehicle used in the *Stadtpilot* is a Volkswagen Passat station wagon called *Leonie*, that is equipped with RADAR and LIDAR sensors, and IT infrastructure as described in [1] and [2]. The current research focuses on autonomous lane changes, traffic light interaction and safety, which is aspect of the present paper.

B. Problem Description

A control system for an autonomous vehicle consists of several parts, each characterized by a specific function and specific input values from vehicle and environmental sensors and specific output values to drive actuators. Because of the complexity and criticality of autonomous driving, it is necessary that all involved modules operate reliable to avoid failures in the system or at least to detect maloperation of the control system.

Transparency on system operation needs permanent monitoring of state variables, critical values and parameters as well as information about environmental conditions.

Results from this monitoring are manifold and not every measurement data can be used separately for safety decisions. Therefore, representative *performance criteria* have to be found. These can be applied to degrade the vehicle's functionality, e.g., to limit speed or steering angle. Additionally, considering environment sensors certain driving maneuvers could be prohibited, e.g., if objects on a neighboring lane can not be detected with the environment sensors due to a system failure, a lane change must not be performed. A third action relying on performance criteria are safety maneuvers to avoid dangerous situations, e.g., an emergency stop in traffic flow can be more dangerous than a controlled lane change to the side of the road and a stop there.

The purpose of this paper is to introduce a surveillance and safety system, which monitors system operation, identifies performance criteria for autonomous driving and uses these criteria to influence vehicle control and driving maneuvers. The surveillance is similar to the behavior of a human driver, who should monitor several parameters, e.g., the road and weather conditions, but also technical problems or failures shown by signal lamps in the vehicle's instrument panel.

C. Related Work

Research activities in the field of autonomous driving like [3] and [4] cover mostly functional topics such as environment recognition, sensor data fusion and artificial intelligence (AI) rather then safety aspects. This stands in contrast with advanced driver assistance systems (ADAS). Here, safety plays a major role, because many systems are already in serial development and in production. In [5] a system for supervision and fault-detection for passenger cars is presented. The main difference in ADAS development over developing autonomous driving systems is the possibility to return control of the vehicle to the driver in every situation.

Another field in the automotive industry where redundant fault-detection and fault-tolerance systems [6] are used to compensate the missing mechanical fallback layer, like in an autonomous vehicle where no human driver is present, are drive-by-wire systems [7].

A. Reschka and J. R. Böhmer are with the Institute of Technology, Universität Hildesheim, Marienburger Platz 22, 31141 Hildesheim, Germany {andreas.reschka, boehmer}@uni-hildesheim.de

T. Nothdurft and P. Hecker are with the Institute of Flight Guidance, Technische Universität Braunschweig, Hermann-Blenk-Straße 27, 38108 Braunschweig, Germany {t.nothdurft, p.hecker}@tu-bs.de

B. Lichte and M. Maurer are with the Institute of Control Engineering, Technische Universität Braunschweig, Hans-Sommer-Str. 66, 38106 Braunschweig, Germany {lichte, maurer}@ifr.ing.tu-bs.de

[1] Project website: http://stadtpilot.tu-bs.de/

In all of these fields international standards and guidelines like IEC 61508, IEC 61511, ISO 26262 and MISRA are used for the development of safety critical electrical and programmable systems.

II. Basic concepts

First of all the concept of surveillance, performance criteria and functional degradation shall be defined as well as requirements for their usage. Fig. 1 shows the three steps of the concept. At first measurements are collected and after that they are used for the calculation of performance criteria. Relying on the values of these criteria degradation actions are executed to keep the vehicle in safest operation possible.

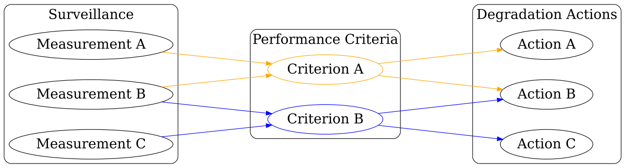

Fig. 1. From single measurement to degradation actions

A. Requirements

Before starting with basic concepts requirements on the safety system shall be discussed. These requirements are mandatory to avoid unwanted influence of any surveillance and safety related functions to normal operation.

- Surveillance modules and integrated surveillance functions must not influence the functional modules in their normal operation. Therefore no changes on any parameters or values of functional modules are allowed, as the surveillance system is only for monitoring. It is additional to functional modules and provides data for safety, but must not alter functional modules.
- Surveillance and Safety functions have to avoid significant additional hardware load, because this could affect the speed of operation of the whole system.
- Integrated surveillance and safety parts must not change cycle times of modules significantly, because this could lead to an increase of the system's reaction time.
- Data Acquisition, calculation of performance criteria and degradation actions have to be executed instantly to react on the current situation and not later than a human driver would react [8].
- As every part in a control system of an autonomous vehicle is necessary for a stable operation, the whole system has to be surveilled. Although not every single calculation can be monitored, most events in the system are time triggered and therefore observable through heartbeats.
- The execution of a degradation action has to improve safety; otherwise it must not be executed.

B. Surveillance

Surveillance is the first part of the proposed concept. Sensor values, heartbeats, cycle times and calculated values are monitored and stored for further use. The sources of the measurements are manifold and most parts of a system provide values which can be surveilled. A main challenge is to detect whether data provided by a sensor is erratic or not. Therefore redundant mesurements as well as model based measurements could lead to more reliable values.

C. Performance Criteria

In this scope performance is the quality of operation of a system or part of a system [9]. As a consequence a performance criterion combines parameters which are important to the quality of operation and it gives a statement of the current operation. The reference for such a criterion is the highest value possible for the quality a system or part of a system can achieve.

In the definition of a performance criterion relevant parameters and their impact on the criterion have to be identified. Each of these parameters is the result of a single measurement. The large number of possible measurements involved in the system makes the creation of a representation of the vehicle's operation difficult and complex. Therefore heuristics, which are rules that define the influence and magnitude of each parameter to each criterion, are set up, e.g., for each degree the outdoor temperature is below 4°C, the value of a criterion representing the road adhesion is decreased by 1.

The definition of heuristics relies on available measurements and performance criteria and data from situations which lead to a deactivation of the GCS.

D. Functional Degradation

Functional degradation [9] is a reduction of the functional range of a system and the reduction of properties of an executed function. That means, a maneuver can be prohibited or its properties can be changed to a safer execution.

Functional degradation relies on performance criteria and heuristics. The performance criteria can be utilized to perform degradation actions, which can be triggered either by a single or multiple criteria. Therefore, heuristics are set up again which combine criteria and their respective values to a statement which degradation action has to be taken and in which magnitude this degradation has to be applied, e.g., if the criterion representing the road adhesion is reduced by 1 the maximum allowed speed is reduced by $0.1\frac{m}{s}$.

These heuristics rely on available criteria and degradation actions and again situations where continuing normal operation of the GCS was not safe.

In the scope of autonomous driving, such degradation actions have to be performed instantly to react on the vehicle's current situation. As traffic situations change fast and failures in the system occur suddenly a fast reaction is very important. Additionally, a degradation action should only be performed if it mitigates the severity of the current situation and does not endanger or scare passengers inside the vehicle or other road users. In some situations a safety driving maneuver could be a worse solution than a continuing operation with a system failure, e.g., In case of a failure in the

GPS/Inertial Navigation System (INS) an emergency brake could be worse than a controlled driving in the current lane until the GPS/INS solution is in normal operation state again.

With functional degradation a behavior similar to a human driver is possible. If the driver feels unsafe in the current situation he reduces speed, increases safety distances or even stops until the conditions get better. To adapt this behavior and to combine it with the benefits of an electronic system the performance criteria are utilized in combination with heuristics to trigger one or several of the following degradation actions.

III. Performance Criteria and Degradation Actions in Leonie

Below follows an explanation of the identified performance criteria and the underlying sensor, vehicle and system parameters in Leonie. After that, degradation actions and their relation to performance criteria are described.

A. Performance Criteria

In the development and testing of Leonie five different performance criteria have been identified, which represent the current state of the vehicle taking into account internal and external measurements. Fig. 2 shows the relations between measurements, criteria and degradation actions. The number of measurements in the surveillance part is simplified in this figure.

1) *Position Accuracy* is an estimate of the current vehicle position. In general a high accuracy of the vehicle's position estimate enables more precise driving maneuvers and leaves less uncertainty. The information used is the state of the GPS/INS unit, the quality of the received GPS signal, the availability of GPS correction data and the state of LIDAR sensors on the sides of Leonie, which detect lane markings.
2) *Grip Value* is an indicator which combines road and weather conditions and vehicle dynamics to indicate the environmental conditions. Basically, it relies on the speed difference of driven front axle and rear axle, the side slip angle, ESC interference, current rain amount and outdoor temperature. A full description of its composition and its usage can be found in [10].
3) *Viewing Area* represents the space around the vehicle which is covered by environmental sensors. To give an estimate about the sensor view, the heartbeats from all sensors are collected and a predefined model is used to estimate the current viewing area.
4) *System Operation Status* contains information about heartbeats and cycle times of all software and hardware modules involved. It is used to verify that all system modules are working properly and in a predefined time range to ensure fast operation. Also vehicle data is considered, which can be critical to system's operation as well, e.g., the voltage of the vehicle's electrical system.
5) *System Reaction Time* is the latency between an external event and the reaction of the vehicle. All cycle times from the detection of an event to a reaction of the actuators of the vehicle are accumulated for its calculation.

B. Functional Degradation Actions

The following degradation actions are executed to keep the operation of Leonie in a safe state.

- With *Modification of Driving Parameters* a direct influence on the longitudinal and lateral controllers is possible. The desired speed and steering angle can be decreased and the safety distance to the sides and the safe time headway can be increased to drive safer.
- With *Modification of Driving Maneuvers* whole driving maneuvers like lane changes or turning maneuvers can be modified by the safety system. This means that a planned trajectory the vehicle should drive can change due to performance criteria values, e.g., the length of a lane change and the speed of the vehicle in the lane change can be modified in the planning step.
- The *Enforcement of Safety Maneuvers* leads to maneuvers that should avoid or mitigate dangerous situations. The options for these actions are manifold and in most situations several safety maneuvers reduce the severity of the current situation. Therefore a decision which safety maneuver should be executed has to be taken.
- In contrast to enforcement of maneuvers, the *Prohibition of Driving Maneuvers* prevents the vehicle from driving maneuvers that can not be planned and observed good enough due to poor performance criteria values. A maloperation of a sensor or a software module could lead to a misinterpretation of the current driving situation and planned maneuvers could rely on these erratic measurements and should be prohibited.

IV. Stadtpilot Architecture

The overall system architecture of the experimental vehicle Leonie is described in [1]. Most of the safety functions are integrated in the Stadtpilot Guidance and Control System (GCS) shown in Fig. 3.

With data acquisition parts of the system information about the environment, road users, vehicle dynamics and vehicle's position is acquired. This information is stored and provided by the Context Model as described in [11]. Based on the provided information and the user inputs a route and driving maneuvers are planned and finally executed with control actions transferred to the vehicle's actuators. The surveillance and safety system is integrated into the GCS and its characteristics are described in the following section. By default the operation of the GCS is configured for good weather and good road conditions.

V. Stadtpilot Surveillance and Safety System

In order to identify performance criteria and functional degradation actions for the autonomous vehicle Leonie, a surveillance and safety system was integrated into the GCS. In Fig. 3 the safety related modules are shown with a red

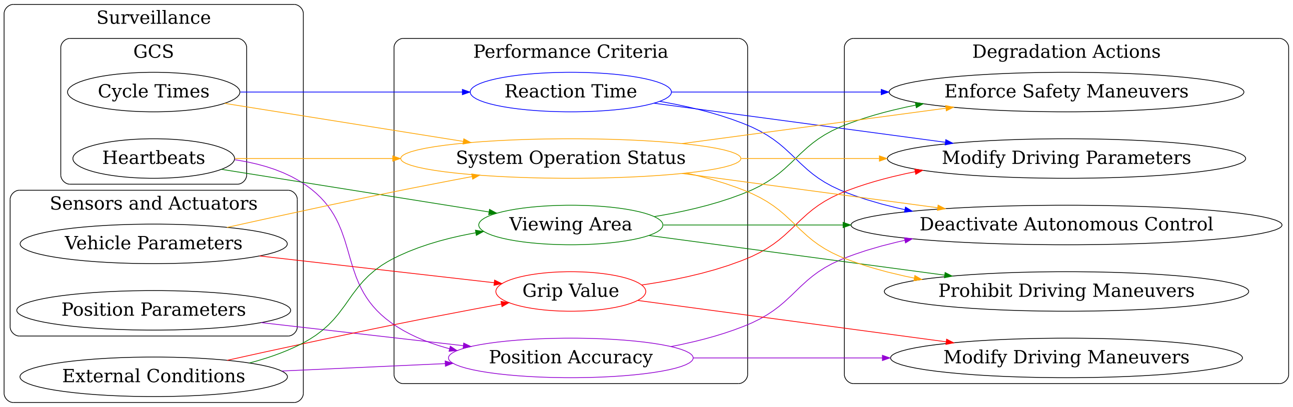

Fig. 2. Relations between acquired data, performance criteria and degradation actions

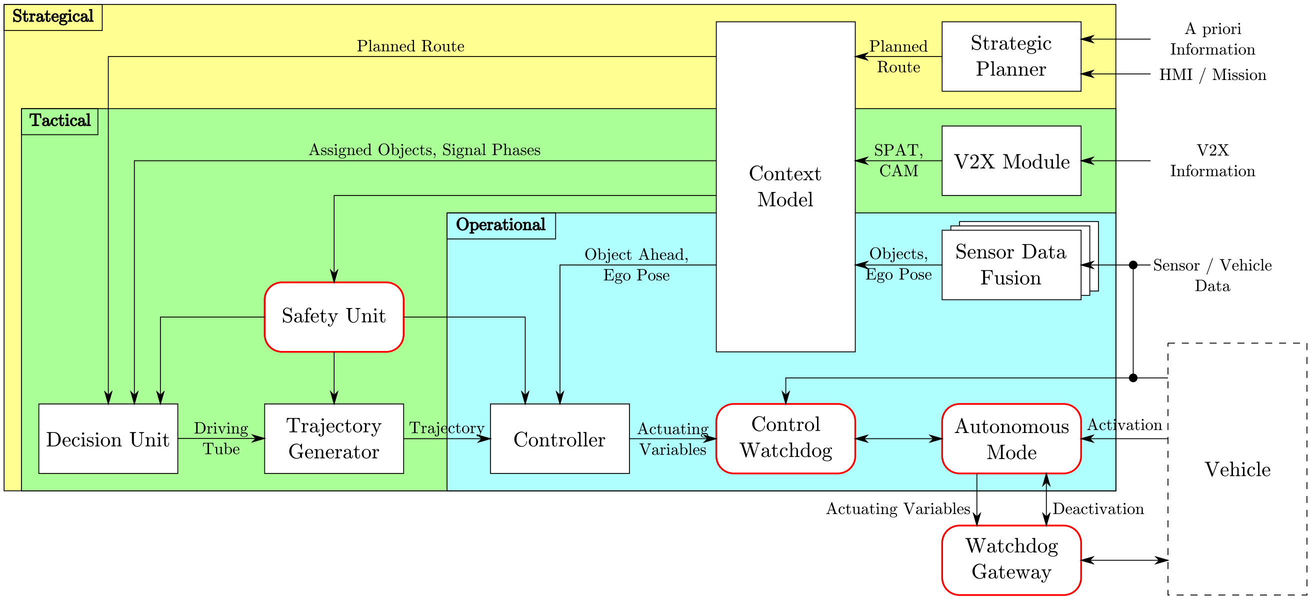

Fig. 3. The hierarchic architecture of the Stadtpilot Guidance and Control System is shown in yellow, green and cyan. The complementary Safety Modules are highlighted with a red border and rounded edges. Connections between modules are simplified.

border and rounded edges. These modules implement the functionality described in Part II and III of this paper.

The structure of the surveillance system is strongly aligned to the Stadtpilot GCS, it is partly additional to and partly integrated in the functional modules of the GCS and consists of four parts.

In almost every part of the GCS important parameters are processed and many of these are monitored by the *Control Watchdog* module and the *Safety Unit* module. These modules are core elements of the surveillance and safety system and collect data from functional modules and sensors, calculate values for performance criteria and execute degradation actions. These actions influence the AI (decision unit, planning modules) and lateral and longitudinal control. The third module for surveillance and safety is the *Watchdog Gateway*, which is the interface between the GCS and the vehicle. Together with the *Autonomous Mode* module the Watchdog Gateway is responsible for the activation and deactivation of the automated vehicle guidance.

A. Control Watchdog

The Control Watchdog is a software component used for monitoring all modules responsible for actuator control, which includes lateral and longitudinal controllers. Additionally it is used to collect heartbeats and cycle times from involved hardware, sensors, and several modules in the low level control and the planning part of the GCS. It is responsible for calculating four of the five identified performance criteria. Fig. 4 shows a simplified version of the Control Watchdog module where input and output are combined to several groups.

The lateral and longitudinal control input is verified within the Watchdog Gateway to ensure its compatibility to the vehicle's actuators. Although this is done in the controller modules as well, it prevents the Electronic Control Units (ECU) in the vehicle from invalid values in a redundant way. Input to the Control Watchdog is described in combination

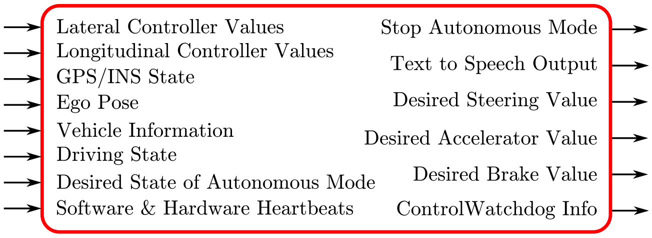

Fig. 4. Input and Output of the Control Watchdog module

with the performance criterion/ criteria to which it is connected below.

Position Accuracy

Due to the position accuracy driving maneuver parameters are modified, driving maneuvers are planned differently and driving maneuvers can be prohibited. The GPS/INS input is used to compare the current estimated position deviation from the INS to thresholds which trigger different events. If a first threshold is reached, a warning is sent via text-to-speech to passengers and the safety driver. If a second threshold is reached the autonomous driving functions are stopped, because a high position error makes autonomous driving in urban traffic too dangerous.

Currently a positioning support for the GPS/INS position via LIDAR is developed and promises better positioning even if GPS reception quality is low [1], [12]. The position accuracy is integrated in the Control Watchdog Info output and submitted to the Safety Unit, because this module influences the planning modules and the controllers.

Viewing Area

The Viewing Area criterion depends on the heartbeats of environmental sensors. If all sensors are operating as expected, the vehicle has an almost 360 degree viewing range with variable width in ranging [13]. Additionally some parts of the viewing area are covered redundant with LIDAR and RADAR. In the future also environment conditions are considered due to their influence in RADAR and LIDAR sensors [12].

Using this criterion it is possible to detect sensor malfunctions and based on this information driving maneuvers relying on failing sensors can be prohibited. Especially in current research on autonomous lane changing this criterion could prevent the vehicle from dangerous lane change maneuvers and in future development it will be important for turning maneuvers with oncoming traffic.

Each of the heartbeats is currently containing sensor data to ensure that the sensor is at least sending data. A verification of this data is not done in the Control Watchdog, but in the perception part of the GCS [13].

System Operation Status

The System Operation Status criterion consists of two parts. The first one is to represent the heartbeats of involved hardware and software, including the GPS/INS. These heartbeats are used to identify parts of the system which are not responding or working any more. They are accumulated and if heartbeats are missing, the Control Watchdog submits a message to stop the autonomous vehicle guidance and to inform passengers and the safety driver about this event. Missing means that in a predefined time span no heartbeat reaches the Control Watchdog.

The second part contains information about the current activation state of vehicle guidance systems, as it is possible to activate longitudinal and lateral control separately. The Autonomous Mode input provides this information which is used to decide if a stop of the automated vehicle guidance is necessary.

System Reaction Time

The System Reaction Time criterion represents an accumulation of the cycle times of all software modules used in the process from detecting an object or event on which the vehicle has to react instantly and the duration until an action is executed by the actuators. The cycle times are calculated by incoming heartbeats. In a predefined process chain of data and the cycle times for each of the modules, the current reaction time can be estimated. The most important reaction on events is to decrease speed, therefore the process chain is based on braking maneuvers.

As the autonomous system should guide the vehicle at least as safe as a human driver [14], this reaction time has to be smaller than 1 second [8]. The System Reaction Time varies because of the large number of modules which process data from environmental sensors to actuators. If the reaction time is higher the vehicle could drive slower and more carefully until the reaction time stabilizes or another degradation action like an emergency stop is necessary.

B. Safety Unit

The Safety Unit combines data from vehicle sensors and vehicle dynamics from the GPS/INS to estimate road and weather conditions in the Grip Value criterion [10]. The main task is to prevent the vehicle from unsafe driving in bad road and weather conditions. Additionally it collects data from the Control Watchdog and the GPS/INS to take safety decisions like reducing the maximum speed or steering angle due to localisation errors.

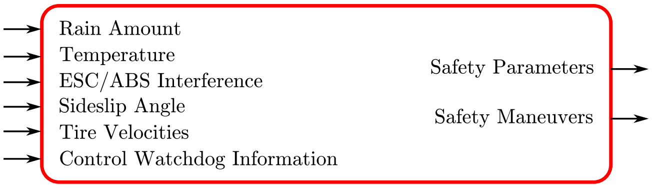

Fig. 5. Input and Output of Safety Unit module

C. Autonomous Mode

Although the Autonomous Mode module is not used to calculate performance criteria, it is a very important part of the safety system. Its input comes directly from the vehicle, the Human-Machine-Interface (HMI) and from the Control

Watchdog. Only if all doors are closed, the Electronic Stability Program (ESP) is activated, and the Watchdog Gateway (description below) and the Control Watchdog signalize that the system and vehicle are in good condition and the driver requests the activation of the automatic vehicle guidance, the Autonomous Mode requests the activation from the Watchdog Gateway.

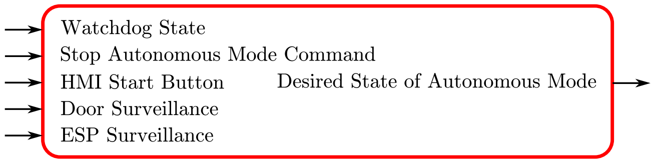

Fig. 6. Input and Output of Autonomous Mode module

D. Watchdog Gateway

The Watchdog Gateway is an ECU which connects the Stadtpilot GCS to the vehicle. It monitors the vehicle's CANs and provides this information about important vehicle parameters. Besides this monitoring function it validates the control values for the vehicle's actuators to ensure a safe actuator control and it limits the steering angle in relation to the current vehicle speed.

Additionally the Watchdog Gateway allows and denies the activation of automated driving functions together with the Control Watchdog and the Autonomous Mode. Therefore information about the GCS system state, from the HMI, the Autonomous Mode state and the vehicle state is considered.

Another very important feature of the Watchdog Gateway is the detection of driver interference in testing autonomous driving systems. Fig. 7 shows its input and output.

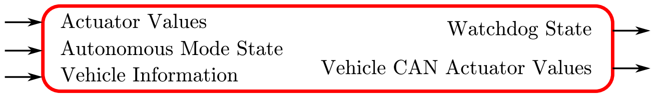

Fig. 7. Input and Output of Watchdog Gateway

VI. Results

The surveillance and safety system is running in Leonie and is collecting most of the relevant values from hardware, software, and sensors. Also the performance criteria are calculated and used for degradation. The current limitation is the differentiation of degradation actions. At the moment only the Grip Value criterion influences the vehicle's maneuvers and all other criteria are used to deactivate the automated vehicle guidance if an error occurs.

Because of the ongoing development on lane changes and traffic light interaction there are no results for safety maneuvers like controlled stops on the side of the road or alternatively planned routes due to poor values of the criteria.

VII. Conclusion

This paper presents an approach how a surveillance system can collect information about the system state of an autonomous vehicle. The information is used to calculate several performance criteria which give a better usable representation of the system state. These criteria are finally used to modify the vehicle's operation if their application improves safety for passengers and other road users.

In the future development of Leonie especially the number of degradation actions has to be increased to react on events in a better way than simply stop the automated vehicle guidance. The first step is an autonomous emergency stop for Leonie followed by a routine to stop at the side of the road to avoid blocking traffic. After such emergency actions self-healing could be a good solution to prevent Leonie from total failure [15].

Acknowledgment

We would like to thank all team members of the *Stadtpilot* project for their work and their help in our research.

References

[1] T. Nothdurft, P. Hecker, S. Ohl, F. Saust, M. Maurer, A. Reschka, and J. R. Böhmer, "Stadtpilot: First fully autonomous test drives in urban traffic," in *14th International IEEE Annual Conference on Intelligent Transportation Systems (ITSC), 2011 IEEE*, Washington DC, USA, 2011, pp. 919–924.

[2] J. M. Wille, F. Saust, and M. Maurer, "Stadtpilot: Driving autonomously on Braunschweig's inner ring road," in *Intelligent Vehicles Symposium (IV), 2010 IEEE*, San Diego, USA, 2010, pp. 506–511.

[3] M. Bertozzi *et al.*, "VIAC: An out of ordinary experiment," in *Intelligent Vehicles Symposium (IV), 2011 IEEE*, Karlsruhe, Germany, 2011, pp. 175–180.

[4] J. Levinson *et al.*, "Towards fully autonomous driving: Systems and algorithms," in *Intelligent Vehicles Symposium (IV), 2011 IEEE*, Karlsruhe, Germany, June 2011, pp. 163–168.

[5] M. Börner and R. Isermann, "Supervision, fault detection, and sensor fault tolerance of passenger cars," in *The 5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, Washington DC, USA, 2003.

[6] R. Isermann, R. Schwarz, and S. Stolzl, "Fault-tolerant drive-by-wire systems," *Control Systems, IEEE*, vol. 22, no. 5, pp. 64–81, 2002.

[7] P. Bergmiller, M. Maurer, and B. Lichte, "Probabilistic fault detection and handling algorithm for testing stability control systems with a drive-by-wire vehicle," in *International Symposium on Intelligent Control (ISIC), 2011 IEEE*, Denver, USA, 2011, pp. 601–606.

[8] G. Johansson and K. Rumar, "Drivers' brake reaction times." in *Human Factors*, vol. 13(1), 1971, pp. 23–27.

[9] H. Kopetz, *Real-Time Systems: Design Principles for Distributed Embedded Applications (Real-Time Systems Series)*. Springer, 2011.

[10] A. Reschka, J. R. Böhmer, F. Saust, B. Lichte, and M. Maurer, "Safe, dynamic and comfortable longitudinal control for an autonomous vehicle," in *Intelligent Vehicles Symposium (IV), 2012 IEEE*, Alcalá de Henares, Spain, 2012, pp. 346–351.

[11] T. Nothdurft, P. Hecker, T. Frankiewicz, J. Gačnik, and F. Köster, "Reliable information aggregation and exchange for autonomous vehicles," in *Vehicular Technology Conference (VTC Fall), 2011 IEEE*, San Francisco, USA, 2011, pp. 1–5.

[12] P. Lindner, E. Richter, G. Wanielik, K. Takagi, and A. Isogai, "Multichannel lidar processing for lane detection and estimation," in *Intelligent Transportation Systems, 2009. ITSC '09. 12th International IEEE Conference on*, St. Louis, USA, 2009, pp. 1–6.

[13] S. Ohl and M. Maurer, "A contour classifying kalman filter based on evidence theory," in *14th International IEEE Conference on Intelligent Transportation Systems (ITSC), 2011 IEEE*, Washington DC, USA, 2011, pp. 1392–1397.

[14] H. Winner, S. Hakuli, and G. Wolf, *Handbuch Fahrerassistenzsysteme*. Vieweg+Teubner, 2009.

[15] D. Ghosh, R. Sharman, H. Raghav Rao, and S. Upadhyaya, "Self-healing systems – survey and synthesis," *Decision Support Systems*, vol. 42, no. 4, pp. 2164–2185, 2007.