An Interdisciplinary Perspective to the Design and Decision Support of Integral Safety Systems

Christian Berger*, Panagiotis Katsaros, Mahdi Bohlouli***, Lefteris Angelis****

**Chalmers | University of Gothenburg, Sweden*
(e-mail: christian.berger@gu.se)
***Aristotle University of Thessaloniki, 54124 Thessaloniki*
Greece (e-mail: {lef, katsaros}@csd.auth.gr)
**** Institute of Knowledge Based Systems and Knowledge Management, University of Siegen,*
D-57068 Siegen, Germany, (e-mail: mbohlouli@informatik.uni-siegen.de)

Abstract: Next generation integral safety systems are expected to provide better protection against traffic accidents by interlinking sensors and actuators of active and passive safety. A series of advanced functions will be used to mitigate collisions and if they cannot be avoided they will at least reduce their severity. We explore the interplay between key technology areas towards a holistic approach in the design and decision support of integral safety systems. First, we refer to the main problems in the design of effective systems and the associated software engineering challenges. Recent advances in sensor data analytics are then explored and their integration with decision support for vehicle control is examined. Finally, we envision that rigorous design techniques based on models for human-machine interaction are essential for achieving adequate performance and robustness of integral safety systems.

Keywords: active control, safety, data streams, sensor systems, decision support systems, formal verification.

1. INTRODUCTION

Integral Safety Systems (ISSs) combine passive safety with active safety systems. The former employ both structural means and subsystems utilising on-board data from e.g. acceleration and yaw-rate sensors, like in the well-known electronic stability systems (ESC). On the other hand, active safety systems rely mainly on volatile data perceived by sensors from a vehicle's surroundings. A typical case of active safety is the current Advanced Driver Assistance Systems (ADAS) aiming to identify critical driving situations and trigger appropriate responses, such as warnings for the driver. ADAS are based on dynamic data and sensor systems for detecting and classifying objects and for tracking the distance from a target.

The combination of systems from both types shall increase the overall traffic safety and at the same time will reduce negative impacts like weight or fuel consumption, if only systems from one type would have been used. It is also foreseen that by connecting passive and active safety systems we can reduce the severity of accidents and their consequences through the optimization of passive safety measures. This integration is a challenging perspective that can be accomplished by a cost-effective combination of recent advances in three different fields: discrete event - hybrid systems simulation, sensor data analytics and decision making support for vehicle control.

The present article adopts this interdisciplinary perspective and examines promising developments in the respective fields that can contribute into a holistic design approach for ISSs.

The simulation is already seen by the automotive industry as an economically feasible means for validating the algorithmic implementations of safety systems. The design and development of ISSs poses significant challenges that are mentioned in Section 2. Sensor data analytics refer to modern techniques and system architectures for handling the huge amount and the heterogeneity of data collected by the sensor systems. Relevant techniques are discussed in Section 3. In Section 4, we present the latest developments in decision support systems and the design challenges for the ISS decision making component. Section 5 focuses on rigorous model-based system design as a viable pathway for the development of trustworthy and optimized ISSs. Recent achievements in the design of embedded systems are examined, as well as appropriate formal models for hybrid systems and human-machine interaction modelling including their interplay in ISS design.

The discussed aspects cannot be considered as an exhaustive coverage of all ISS design problems. However, the key challenges of big sensor-data processing, decision making and heterogeneous system integration are adequately explored.

2. INTEGRAL SAFETY SYSTEMS – SOFTWARE ENGINEERING CHALLENGES

2.1 Usage Scenarios for Simulative Approaches during the Design and Development of ISS

While ISS promise significant enhancements to the overall traffic safety, their design, realization, and evaluation pose new requirements to the development process. The main challenge of these systems is their functional dependency on uncertain and volatile data from the vehicle's surroundings, which is perceived by sensors like cameras, radars, or laser scanners. The validation of their proper functionality by using a small selection of all imaginable situations on proving grounds or on public roads only is not sufficient with respect to reproducibility and accuracy. Furthermore, re-testing these systems on small changes to the requirements specifications or on hardware changes has to take into account all available traffic situations on proving grounds. However, this is not advisable from an economic resources' usage point of view.

Today, automotive Original Equipment Manufacturers (OEMs) use various simulation-based approaches during system design and development, in order to experiment and validate their algorithmic implementations. While their beneficial usage depends obviously on the quality of the models for a system's surroundings and the system's on-board sensors and actuators, the advantage of using them can be pointed out at several spots during the development as outlined in (Berger, 2012).

During the design of these functions, simulative approaches help to analyse and limit design space explorations e.g. for identifying a suitable sensor or determining its mounting position and orientation to achieve the best efficiency for the intended set of use cases. After the start-of-production of the next vehicle generation, simplifications and assumptions about macroscopic movement models of other traffic participants can be improved by feeding data from the field back into the models for the simulation environment. Furthermore, analyses about life-cycle effects of the vehicle can be carried out to get information about their potential impact on a software system; this is of particular interest for the lifetime of sensors that may be changed while parts of the software system remain unchanged; another example is backwards compatibility of communication protocols, which is getting more and more important with respect to systems that rely on vehicle-to-infrastructure and vehicle-to-vehicle communication to realize a specific comfort or even a safety functionality.

2.2 Challenges for Simulative Approaches during the Design and Development of ISS

Firstly, the choice which simulation system shall be used during the design and development depends directly on the questions of interest, which shall be answered. Hereby, one single and unifying simulation system will not be available in the foreseeable future and thus, different and specialized simulations need to be coordinated and integrated to produce the required data; for example, a simulation for validating a pedestrian collision warning system does not need to simulate the potential airflows within the passengers' compartment. Hereby, approaches from the software engineering are required to manage this integration process.

Secondly, as already mentioned before, the benefit of using simulative approaches during the design and development of safety-critical or ADAS depends directly on the quality of the models for the sensors and the vehicle's environment. Hereby, arbitrarily chosen noise models to artificially reduce the perfect quality of simulated sensor data are not enough; instead, better material property models are required to simulate more precisely the detection characteristics of a radar system. Furthermore, lighting and weather conditions must also be modelled accordingly, to analyze a vehicle function's behaviour under various surroundings conditions for a given set of traffic situations.

Next, simulations generate a still growing amount of data that must be analysed to get the desired information. The recorded data might contain hidden interrelations that might be helpful during system validation. Thus, methods for aggregating that data on the one hand to get a quick overview of the software quality of a complex embedded system in general is necessary as described in (Berger et al., 2013). Approaches to search and uncover hidden relations within this recently called "big data" must be developed and applied.

Finally, the design and development of these ADAS and interconnected vehicular systems must also consider the challenges that originate from societal changes: while vehicles were owned and considered as a representative symbol in the last six decades, this perspective of a vehicle is slightly changing nowadays. Thus, the fact that vehicles are more and more regarded as a mobility solution must be considered during the design and realization of ADAS. This apparently not very specific use case has yet an important impact on the average usage profiles of vehicles, which play an important role during the overall design and parameterization of energy management systems.

3. SENSOR DATA ANALYTICS

The problems due to the huge amount and the heterogeneity of data, needed to be processed and analyzed for the design and development of ADAS, cannot be addressed by ordinary statistical methods. In general, there is a need for generic, sophisticated and scalable platforms for supporting information extraction from raw data. These frameworks should implement a mixture of fast algorithms and intelligent techniques in order to extract information from data and present it in forms enhancing decision-making. The simultaneous application of collaborating multidisciplinary methodologies with respect to problems of big data is known as "analytics".

Especially for the safety systems it is important to develop and apply methods for statistical identification and discovery of complex events, i.e. events that summarize, represent, or denote sets of simple events. Complex events are crucial for safety systems, since for example a large number of simple and seemingly uncorrelated and unsynchronized simple events can lead to emergency situation and even to accidents. Complex events cannot be detected by ordinary statistical analyses and there is a need for combined algorithmic and mining techniques.

The related research field is known as Complex Event Prediction and Processing (CEPP) (Adkins et al., 2011). Complex events are represented by data structures which contain, not only the data from each component event, but also the relationships between them with respect to time, causality etc. A formal description of an event with variables and relational operators forms an event pattern, a key concept in CEPP, and involves rules to aggregate, filter, and match low-level events, coupled with actions to generate new, higher-level events (Robins, 2010). In the case of safety systems, CEPP can be used to combine in models environmental and vehicle data which potentially lead to a variety of unanticipated situations. In general, data analytics under the framework of CEPP is beneficial for feeding decision support systems.

The identification and prediction of patterns in data streams involves the utilization of advanced multivariate statistical and data mining methodologies and algorithms such as visual analytics, sampling designs, multiple comparisons tests, time series, data reduction techniques, classification and clustering methods, association rules, optimization algorithms and advanced probabilistic and stochastic causal models such as Bayesian Networks and Structural Equation Models.

A comprehensive platform for a safety system based on sensor data analytics and complex event processing should include three basic components (Hinze et al, 2009): (a) a monitoring component, responsible for event representation, observation and composition of events; (b) a transmission component, responsible for event notification; (c) a reactive component, responsible for triggering a variety of actions based on predefined rules. Therefore, for safety systems, where continuous streams of user data are produced, the first requirement is the efficient monitoring which can be based on longitudinal sampling techniques, dimensionality reduction techniques and recognition of complex events via pattern matching methods. Notification requirements can be based on clustering and classification methods or even to association rules. The third requirement of reactivity requires stochastic models and algorithms able to produce accurate and in-time estimations and predictions of certain critical events.

In general, data analytics can greatly benefit the functionality and the performance of safety systems. As mentioned in (Etzion & Niblett, 2010), the pattern detection in today's systems has to be programmed with details of the specific patterns that need to be detected. The common assumption is that designers know exactly what these patterns are when developing the application, and that the patterns constitute a part of the application specifications. However, in cases as the unwanted situations, that a safety system has to diagnose and prevent, the designers hardly know exactly how a critical event might look like, when first designing the application. In such cases, statistical along with machine learning techniques can be utilized to examine historical events and learn to recognize new patterns.

Another very important use of data analytics is the continuous quality control of the system. Advanced statistical methods and fast algorithms are necessary for the monitoring, and the self-adaptation of the entire system. Hence, data analytics can help to identify malfunctions of individual sensors or even of the whole system and furthermore, they are able to validate the accuracy and efficiency of the decision support systems by getting feedback from them. The quality control component essentially provides intelligence to the system and leads to auto-corrective and self-improvement actions.

The use of statistical and data mining methods has been limited to specific data from specific sources, depending on the application domain. Fortunately, today there are some powerful, open-source and free software tools such as the R statistical language (R Development Core Team, 2009, http://www.r-project.org/), the Predictive Model Markup Language (PMML, http://www.dmg.org/), the WEKA (Hall, et al., 2009) project for data mining, the KNIME (Michael R, et al., 2007) platform for data analytics, and the Apache Mahout (Apache Mahout scalable machine learning and data mining, 2012). These tools offer the opportunity to combine a wide range of statistical methodologies and models that are able to cooperate for processing massive data from heterogeneous sources and producing output for feeding the decision support systems (Williams, 2009).

4. DECISION SUPPORT FOR VEHICLE CONTROL

Decision Support Systems (DSSs) are nowadays one of the core and key components in most novel intelligent software-driven solutions. Their aim is to support key decision makers and domain experts by providing situation aware decision alternatives. Such an aspect should also incorporate learning algorithms, in order to improve the quality of decisions. DSSs can be model-driven, communication-driven, data-driven, document-driven, or knowledge-driven (Hols, 1996) by providing problem-solving expertise saved as facts, rules or similar forms.

The performance of a DSS depends on various factors such as the quality and effectiveness of input data, the decision making algorithms and the provided support for belief revision. In this regard, it is mandatory for ISSs to exclude noisy data and collect the sensor data in the way which can be properly visualized for decision making components. For computerized DSSs, the key question is how to represent the knowledge about the situation (Yang, 2007). This knowledge is about the underlying technical and environmental aspects, and the subjective, individual knowledge and preferences of decision makers.

As shown in Fig. 1, the Decision Support component of an ISS can be based on two main layers: the event and decision layers. By means of Case Based Reasoning (CBR), the system identifies similar cases in the repository of events, in order to provide the required information to the decision layer, for appropriate decisions about the current situation. The key feature in the event layer is the Similarity Template (ST) measurement component. Through a machine learning algorithm, the ST component improves the accuracy of similarity measures based on a feedback cycle from the system design experts about the decision alternatives. "Decision evaluation" and "belief revision" in the decision layer also play an important role in improving the performance and in training the system for better decisions.

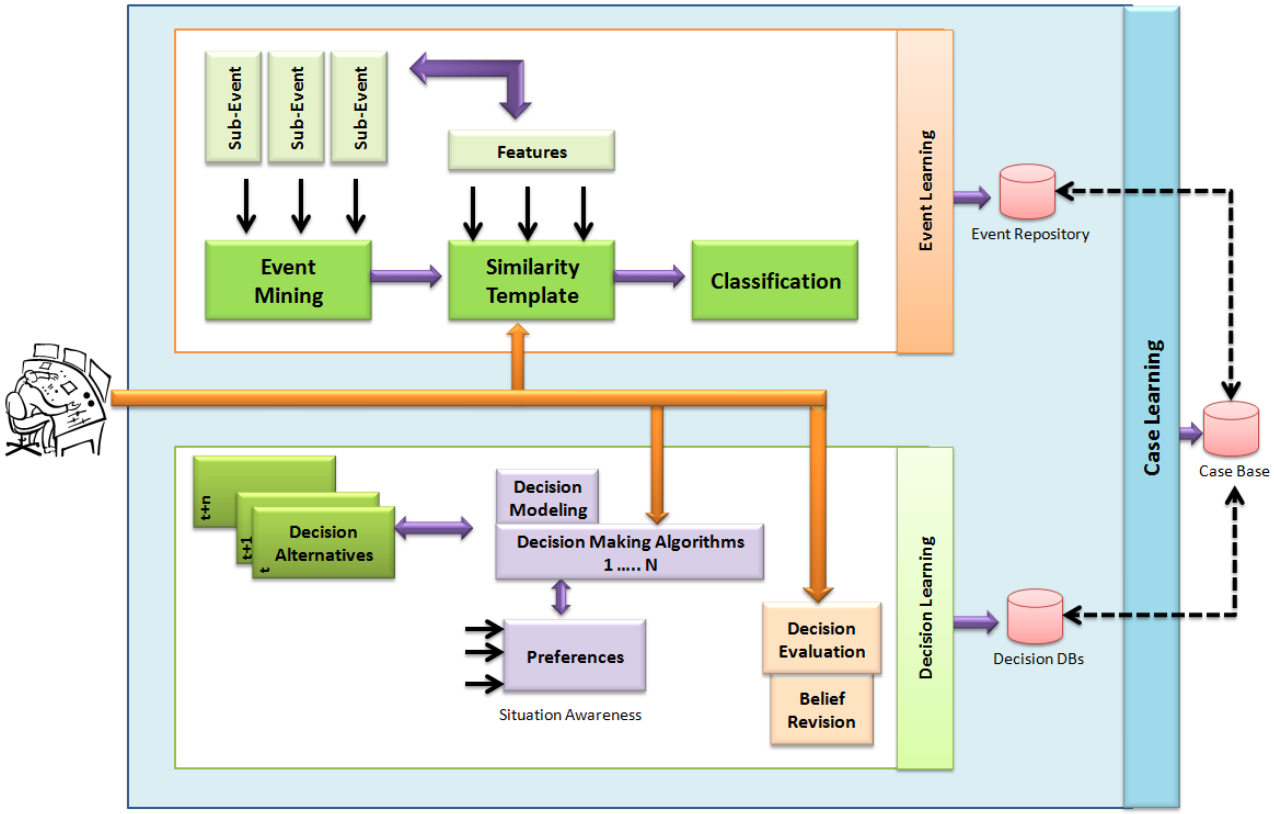

Fig. 1. An overview of the decision making component

There will be two databases in the Decision Support component, namely the event repository and the decision DB. The event repository consists of the historical data about events. The decision DB is about the final decisions and revised solutions towards specific situations.

In the decision modelling component, different criteria such as preferences (e.g. situation awareness), decision alternatives, sensor data and decision evaluation indicators have to be considered. One potential deployment for the data collection from sensors in ISSs is through cloud deployed services (Bohlouli, 2013).

5. RIGOROUS SYSTEM DESIGN

Rigorous design is a cornerstone towards implementing trustworthy and optimized ISSs. Optimization concerns with the system's performance, its cost-effectiveness and the associated tradeoffs, whereas trustworthiness ensures that nothing bad can happen. Most efforts to improve trustworthiness usually result in a non-optimal use of the system's resources. Rigorous design techniques allow balancing the conflicting concerns of trustworthiness and optimality. Moreover, in ISSs the human factor plays a central role in the system's behaviour: his reactions imply state changes in the vehicle's behaviour, which are taken into account during the ISS's autonomous function (Sandberg et al, 2008). We focus on recent advances introducing rigorous methods for system design and human-machine interaction and the challenge of combining them towards the design of trustworthy and optimized ISSs.

In (Sifakis, 2013), the author introduces rigorous system design as "a formal and accountable model-based process leading from requirements to correct system implementations". Accountability refers to the possibility to assert, which among the system requirements are satisfied and which may not be satisfied. The author reviews the main characteristics of successful rigorous design techniques for hard real-time systems and hardware engineering (VLSI design), some of which are used today in the car industry. The success of these techniques is attributed to the coherent and accountable design flows that are enforced by standards, as well as to an extensive use of architectures and design rules, which enable correct-by-construction designs. The main inhibiting factors for applying these practices in the design of complex systems such as the ISSs are the lack of a common component model, the heterogeneity of models of computation (time-triggered and asynchronous event-based), the variety of architectures (sensor system, CEPP and decision making) to be combined and the intractability of synthesis for infinite state systems (the vehicle's behaviour depends on human's reactions and the vehicle's surroundings). To this end, the author is based on the BIP (Behaviour, Interaction, Priority) component framework (Basu et al, 2011) to formalize the design of mixed hardware/software systems, whose behaviour is driven by stimuli from the environment that in turn is affected by their outputs (interactive systems). BIP is the means to realize four

key engineering principles, namely separation of concerns, component-based construction, semantic coherency and correctness-by-construction. The BIP design flow has been successful in numerous embedded system design problems during the past 10 years and we consider it as a highly relevant perspective for ISS design.

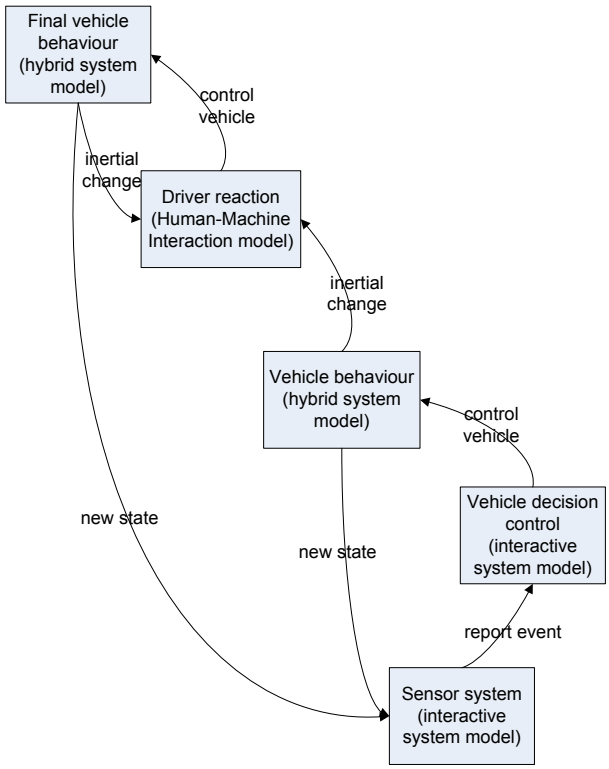

Fig. 2. Formal modelling of driver support functions

In a rigorous design flow such as the one supported by BIP we expect that human reaction in ISS driver support functions will be encoded in appropriate human-machine interaction models that will be combined with hybrid system models (Lunze et al, 2009) for the vehicle dynamics. In (Sandberg et al, 2008), the authors discuss the cause and effect cycle in advanced driver support functions that can be formally represented as shown in Fig. 2. They also point out the importance of generating the same control vehicle actions for identical traffic situations, since any deviation from this principle could cause an unwanted driver reaction. Given this prerequisite for the decision support subsystem and a cognitively plausible formal model of the human behaviour it should be possible to detect or prove the absence of errors emerging from the interaction between the ISS and the driver. Such an analysis will likely yield design improvements for establishing an effective balance between trustworthiness and optimal use of the system's resources.

A valuable source of inspiration for generating this sort of models for human behaviour is the work reported in (Curzon et al, 2007). In that work, the authors are based on results from cognitive psychology in order to derive abstract principles, which are then formalized in higher-order logic. Subsequently, they describe a verification methodology targeting the malfunctioning of interactive systems caused by human actions that can be considered as cognitive slips. However, this is just one of the many recent developments in the area of formal verification for human-machine interaction that we also consider as a highly relevant perspective for the design of effective ISSs.

6. CONCLUSIONS

We presented an interdisciplinary perspective to the design and development of Integral Safety Systems. Important developments in the areas of system simulation, sensor data analytics and decision making were discussed and the challenges towards a holistic design approach for ISSs were considered.

Rigorous model-based system design is a cornerstone, in order to cope with the heterogeneity and the high complexity of ISS subsystems and in order to derive trustworthy and optimized implementations. Recent achievements in the field of embedded systems design were examined and appropriate formal models for hybrid systems and human-machine interaction were considered.

Future work is worth to focus on an ISS case, in order to better understand the problems in the design and development of ISSs, as well as on the pros and cons of existing architectures and the limitations of the considered rigorous design techniques.

REFERENCES

Adkins, J., Bizarro, P., Jacobsen, H.-A., Mavashev, A., Michelson, B. M., Niblett, P., & Tucker, D. (2011). Event Processing Glossary – Version 2.0. The Event Processing Technical Society (EPTS).

Apache Mahout scalable machine learning and data mining. (2012). Retrieved from http://mahout.apache.org

Basu, A., Bensalem, S., Bozga, M., Combaz, J., Jaber, M., Nguyen, T.H., Sifakis, J. (2011). Rigorous Component-Based System Design Using the BIP Framework. IEEE Software, Vol. 28, No. 3, pp. 41-48.

Berger, C. (2012). From Autonomous Vehicles to Safer Cars: Selected Challenges for the Software Engineering. In Ortmeier, F. and Daniel, P. (ed.) SAFECOMP 2012 Workshops, LNCS 7613, pp. 180-189.

Berger, C., Block, D., Hons, C., Kühnel, S., Rumpe, B., Leschke, A., and Strutz, T. (2013). Meta-Metrics for Simulations in Software Engineering on the Example of Integral Safety Systems. In Proceedings des 14. Braunschweiger Symposiums Automatisierungssysteme, Assistenzsysteme und eingebettete Systeme für Transportmittel, pp. 136-148.

Bohlouli, M., Schulz, F., Angelis, L., Pahor, D., Brandic, I., Atlan, D., Tate, R. (2013). Towards an Integrated Platform for Big Data Analysis, Madjid Fathi (Ed.), Integration of Practice-oriented Knowledge Technology: Trends and Prospective, Springer.

Curzon, P., Ruksenas, R., Blandford, A. (2007). An Approach to Formal Verification of Human-Computer Interaction. Formal Aspects of Computing, Vol. 19, pp. 513-550.

Etzion, O., & Niblett, P. (2010). Event Processing in Action. Manning Publications.

Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., & Witten, I. H. (2009). The WEKA Data Mining Software: An Update. SIGKDD Explorations, 11(1).

Hinze, A., Sachs, K., & Buchmann, A. (2009). Event-based applications and enabling technologies. Proceedings of the 3rd ACM International Conference on Distributed Event-Based Systems (DEBS09). Nashville, TN, USA.

Holsapple, C.W. (2007), Decision support systems: a knowledge-based approach, Course Technology Inc.

Lunze, J., Lamnabhi-Lagarrigue, F. (2009). Handbook of Hybrid Systems Control – Theory, Tools, Applications. Cambridge University Press.

Michael R, et al. (2007). KNIME: The Konstanz Information Miner, Studies in Classification, Data Analysis, and Knowledge Organization. GfKL 2007. Springer.

R Development Core Team. (2009). R: A language and environment for statistical computing. Vienna, Austria: R Foundation for Statistical Computing.

Sandberg, A., Sivencrona, H., Torngren, M. (2008). Deterministic Target Selection – Setting Requirements on Speed and Yaw Rate in Automotive Sensor Systems. Proceedings of the 26th International System Safety Conference. Vancouver, Canada.

Sifakis, J. (2013). Rigorous System Design. (In press)

Robins, D. B. (2010). Complex Event Processing. Second International Workshop on Education Technology and Computer Science. Wuhan.

Williams, G. J. (2009). Rattle: A Data Mining GUI for R. The R Journal , 1(2).

Yang, Y. (2007), A framework for decision support systems adapted to uncertain knowledge, Dissertation, University of Karlsruhe, 2007.