Application of Formal Methods in the INSPEX Smart Systems Integration Project

Richard Banach[1], Joseph Razavi[1], Olivier Debicki[2],
Nicolas Mareau[2], Suzanne Lesecq[2], Julie Foucault[2]

[1]School of Computer Science, University of Manchester,
Oxford Road, Manchester, M13 9PL, U.K.
{richard.banach,joseph.razavi}@manchester.ac.uk
[2]Commissariat à l'Énergie Atomique et aux Énergies Alternatives, MINATEC Campus,
17 Rue des Martyrs, F-38054 Grenoble Cedex, France
{olivier.debicki,nicolas.mareau,suzanne.lesecq,julie.foucault}@cea.fr

Abstract. The INSPEX Project aims to create a minaturised smart obstacle detection system, inspired by the sensor constellations that underpin the intelligence of automated vehicle driving systems. Minaturised versions of such systems could find wide application in many contemporary compact smart technologies. The increasing complexity of such systems creates increasing challenges for ensuring their correct operation, inviting the introduction of formal techniques to aid in the maximisation of system dependability. However, the major challenge to building such systems resides at the hardware end of the development, impeding the routine application of top-down formal methods. The experience of the combination of formal modelling and verification techniques with hardware integration techniques in INSPEX is introduced.

1 Introduction

Autonomous vehicles are routinely in the news these days. Videos of cars driving round test tracks have been seen for many years. Videos of cars driving themselves 'out in the wild' are more recent, though increasingly often seen nowadays. This notwithstanding that 'out in the wild' still usually implies an environment that is of a well understood kind, such as a normal urban environment in which the cues for safe navigation are familiar and predictable.

The smart systems on which the safe behaviour of such autonomous vehicles depends relies on a large array of sensors, which feed into a sophisticated computing system that decides on (what it judges to be) future safe dynamics for the vehicle. The notable thing about these integrated systems is that, supported within the vehicle's structure and power supply capabilities, the weight, size and power consumption of the systems themselves are, to first order, immaterial.

However, the concept of a multisensor system, capable of sensing its environment with some precision, and of delivering intelligent feedback on this to a human user, or to a client system, is appealing in many scenarios in which weight, size and power consumption pose much sharper challenges. The aim of the INSPEX Project is to design

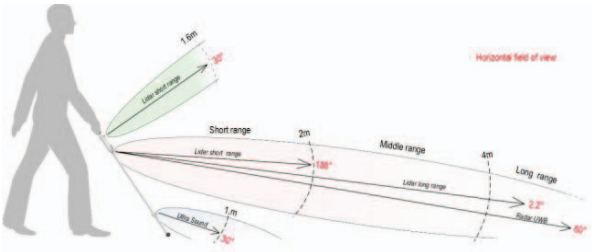

Fig. 1. Schematic of the INSPEX VIB use case.

an integrated, lightweight, minaturised, multi-sensor system capable of functioning in low weight, size and power contexts.

In order to provide a specific focus for the work, INSPEX targets the concept of an assistive aid for visually impaired and blind (VIB) persons. VIB persons typically navigate out in the open using a white cane. A white cane gives good feedback to the VIB person about the texture of the ground in front of them, and this constitutes a rich information source for the user, especially when the environment is familiar.

However, a white cane provides no information about the nature of the user's environment higher up. Injuries caused when a VIB person collides with an object which is not on the ground happen quite frequently, and constitute a notable risk factor for VIB people when navigating, especially in unfamiliar environments. VIB people often wear hats and other headgear, even when they don't particularly want to, to provide a measure of protection against collisions with unknown objects at head height.

The INSPEX Project [3] aims to create an advanced prototype for a device that can be attached to a VIB person's white cane. This will sense the environment and provide feedback to the user about the whole 3D space in front of them, supplementing the information about the 2D terrain in front of the user at ground level, which can be sensed using the white cane alone. Fig. 1 gives a schematic.

To do a decent job of this, the INSPEX device is equipped with a number of sensors, and as a consequence of this, managing and integrating all the information that they provide becomes a task of considerable complexity. To help master this, formal methods were incorporated into the project plan, in order that additional confidence in the design and implementation could be gained by their use. In the following sections we illustrate the novel approach that had to be adopted to achieve a successful outcome for such an enterprise.

2 INSPEX in Outline

The INSPEX concept, adapted to the VIB context, consists of the following components. There is the INSPEX device itself, housed in an attachable block that clips onto the user's white cane. This gathers information from the environment via a collection of sensors: there are short range and long range LIDARs, there is an ultrawideband RADAR, and an ultrasound sensor.

Fig. 2. The complete INSPEX system for the VIB use case.

The information gathered from these sensors is fused, and together with orientation information which captures the disposition of the device in space, is passed via a Bluetooth connection to a smartphone. There is a pair of open air earbuds worn by the user which also contains orientation sensors; the information from these captures the disposition of the user's head in space, and is also passed to the smartphone. The smartphone performs the geometrical computations needed for the generation of aural feedback to the user which is stable in 3D space, despite the movement of the user's head and the movement of the white cane. Fig. 2 gives an illustration of the INSPEX system's components.

The vision for INSPEX opens the door for a wide variety of other application areas for the technology. Many applications can benefit from more accurate information about their environment. Among the more significant of these is the use case of firefighters, who often find themselves in smoke filled, and thus opaque environments. Such use cases will be pursued in due course.

3 The Design Approach for INSPEX

INSPEX is, first and foremost, a hardware systems integration project. Without working hardware, the project achieves nothing. So the overwhelming emphasis in the project is on overcoming the physical challenges in bringing the equipment to life. Everything from the detailed properties of the sensors and their physical signals, to the properties of the main INSPEX device container —with its need for robustness and durability under a variety of weather conditions while at the same time permitting each sensor to transmit it signal and receive the corresponding reflection— takes priority. This imposes an unmistakably hardware-led, bottom-up structure on the project, and makes the typical textbook top-down formal methods approach, focused on functionality without taking low level physical limitations into account, impractical.

4 Modelling and Verification of the Sensor Readings Pathway

The previous section implies that some methodological novelty is inevitable in the use of formal methods in the INSPEX context. In this paper we give an outline of the approach taken in one part of the project, namely the gathering of sensor data and its transmission to the main fusion software.

The information from the sensors is gathered by the acquisition software. This accepts interrupts from the short and long range LIDARs, the RADAR, the US (ultrasound) and the IMU (inertial measurement unit). These need to be timestamped so that the freshness of the data can later be taken into account. At regular intervals, the available fresh data is packaged and transmitted to the fusion software. The fusion software

then uses an approach based on Bayesian estimation to compute an *occupation grid* [2], which is an estimate of which sections of the 3D space in front of the user are occupied by obstacles. The granularity of this estimate is constrained by the quality of the information received and by the bandwidth of the Bluetooth connection to the smartphone.

The unavoidably hardware-led nature of the INSPEX project means that the majority of the design of the acquisition and transmission system are governed by pragmatic hardware and architectural considerations. Accordingly, the formal modelling and verification of this part of the system is, in reality, a process of *abstraction* from implemented code, rather than a top-down design *from* an abstraction. Although mechanised tools for analysis of source code are widely available, those suitable for this application are not free, and so budgetary constraints prevented their employment.

Accordingly, the approach actually used is an eclectic combination of: on the one hand, model building based on informal discussions with the implementation team, the conjecturing of invariant properties of the model and their proof; and on the other, visual inspection of the implemented code, to see how well it matches the invented model. For the former task, Event-B and Rodin [1, 4] has proved to be the most useful approach, especially as the SMT solvers of Rodin make proof an essentially pushbutton activity.

Any discrepancies that are identified, are resolved by discussion with the implementers. Although such an approach cannot hope to match the thoroughness of a fully mechanised approach to verification, we do get the inestimable benefit of a dual perspective on the development, combining traditional imperative design and implementation, with a more abstract and property driven view coming from the abstract modelling and verification.

5 Conclusions

Above, we overviewed the inspiration for INSPEX and the principal features of the project. The increasing complexity of embedded applications today impels a greater focus on matters of correct operation, compared with past practice in this field. The adoption of formal techniques by INSPEX is a telling indication of this increasing trend. The use of formal approaches entails bringing some creativity to align usual practice in the embedded field with usual practice in the formal domain. Further work on the use of formal methods in INSPEX will be reported elsewhere.

Acknowledgement: This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 730953.

The work was also supported in part by the Swiss Secretariat for Education, Research and Innovation (SERI) under Grant 16.0136 730953. We thank them for their support.

References

1. Abrial, J.R.: Modeling in Event-B: System and Software Engineering. CUP (2010)
2. Dia, R. and Mottin, J. and Rakotavao, T. and Puschini, D. and Lesecq, S.: Evaluation of Occupancy Grid Resolution through a Novel Approach for Inverse Sensor Modeling. In: Proc. IFAC World Congress, FAC-PapersOnLine. vol. 50, pp. 13841–13847 (2017)
3. INSPEX Homepage: http://www.inspex-ssi.eu/
4. RODIN Tool: http://www.event-b.org/ http://sourceforge.net/projects/rodin-b-sharp/