Eric Bonjour · Daniel Krob
Luca Palladino · François Stephan
Editors

# Complex Systems Design & Management

Proceedings
of the Ninth International Conference
on Complex Systems Design
& Management
CSD&M Paris 2018

Springer

Complex Systems Design & Management

Eric Bonjour · Daniel Krob
Luca Palladino · François Stephan
Editors

# Complex Systems Design & Management

## Proceedings of the Ninth International Conference on Complex Systems Design & Management, CSD&M Paris 2018

Springer

*Editors*
Eric Bonjour
Université de Lorraine
Laxou, France

Daniel Krob
CESAMES
Paris, France

Luca Palladino
Safran
Magny Les Hameaux, France

François Stephan
Be-Bound
Marnes La Coquette, France

ISBN 978-3-030-04208-0 ISBN 978-3-030-04209-7 (eBook)
https://doi.org/10.1007/978-3-030-04209-7

Library of Congress Control Number: 2018960915



This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

## Introduction

This volume contains the Proceedings of the Ninth International Conference on "Complex Systems Design & Management" (CSD&M 2018; see the conference Web site: http://www.2018.csdm.fr/ for more details).

The CSD&M 2018 conference was jointly organized on 18–19 December 2018 at the Cité Internationale Universitaire de Paris (France) by the three following partners:

1. CESAM Community managed by the Center of Excellence on Systems Architecture, Management, Economy & Strategy (CESAMES);
2. AFIS, Association Française d'Ingénierie Système, the French Chapter of the International Council on Systems Engineering (INCOSE);
3. The Ecole Polytechnique; ENSTA ParisTech; Télécom ParisTech; Dassault Aviation; Naval Group; DGA; Thales "Engineering of Complex Systems" chair.

The conference also benefited from the technical and financial support of many organizations such as Airbus Apsys, Alstom Transport, ArianeGroup, INCOSE, MEGA International, Renault and Thales. Our sincere thanks therefore to all of them.

Then, many other organizations have been involved in the CSD&M 2018 Committee. We would like to thank all their members who helped a lot through their participation during the one-year preparation of the conference.

## Why a CSD&M Conference?

Mastering complex systems require an integrated understanding of industrial practices as well as sophisticated theoretical techniques and tools. This explains the creation of an annual *go-between* forum at European level (which does not exist yet) both dedicated to academic researchers and industrial actors working on

complex industrial systems architecture and engineering. Facilitating their *meeting* was actually for us a *sine qua non* condition in order to nurture and develop in Europe the science of systems which is currently emerging.

The purpose of the "Complex Systems Design & Management" (CSD&M) conference is exactly to be such a forum. Its aim, in time, is to become *the* European academic–industrial conference of reference in the field of complex industrial systems architecture and engineering, which is a quite ambitious objective. The last eight CSD&M Paris conferences—which were all held in the last quarter from 2010 to 2017 in Paris—were the first steps in this direction. In 2017, participants were again almost 250 to attend the two-day conference which proves that the interest for architecture and systems engineering does not fade.

## Our Core Academic–Industrial Dimension

To make the CSD&M conference a convergence point of the academic and industrial communities in complex industrial systems, we based our organization on a principle of *parity* between academics and industrialists (see the conference organization sections in the next pages). This principle was first implemented as follows:

- Program Committee consisted of 50% academics and 50% industrialists,
- Invited Speakers came in a balanced way from numerous professional environments.

The set of activities of the conference followed the same principle. They indeed consist of a mixture of research seminars and experience sharing, academic articles and industrial presentations, software and training offer presentations, etc. The conference topics cover the most recent trends in the emerging field of complex systems sciences and practices from an industrial and academic perspective, including the main industrial domains (aeronautics and aerospace, transportation and systems, defense and security, electronics and robotics, energy and environment, health care and welfare services, media and communications, software and e-services), scientific and technical topics (systems fundamentals, systems architecture and engineering, systems metrics and quality, systemic tools), and system types (transportation systems, embedded systems, software and information systems, systems of systems, artificial ecosystems).

## The 2018 Edition

The CSD&M Paris 2018 edition received 52 submitted papers, out of which the Program Committee selected 19 regular papers to be published in the conference proceedings. A 37% acceptance ratio was reached which guarantees the high

quality of the presentations. The Program Committee also selected 16 papers for a collective presentation during the poster workshop of the conference.

Each submission was assigned to at least two Program Committee members, who carefully reviewed the papers, in many cases with the help of external referees. These reviews were discussed by the Program Committee Co-chairs during an online meeting by 26 June 2018 and managed via the EasyChair conference system.

We also chose several outstanding speakers with industrial and scientific expertise who gave a series of invited talks covering all the spectrum of the conference during the two days of CSD&M Paris 2018. The conference was organized around a common topic: "*Products and Services Development in a Digital World.*" Each day proposed various invited keynote speakers' presentations and a "à la carte" program consisting in accepted papers' presentations and in different sessions (thematic tracks on Day 1 and sectoral tracks on Day 2).

Furthermore, we had a "poster workshop", to encourage presentation and discussion on interesting but "not-yet-polished" ideas. CSD&M Paris 2018 also offered booths presenting the last engineering and technological news to participants.

August 2018

Eric Bonjour
Daniel Krob
Luca Palladino
François Stephan

# Conference Organization

## Conference Chairs

### General Chair

| | |
|---|---|
| Daniel Krob | CESAMES and Ecole Polytechnique, France |

### Organizing Committee Chair

| | |
|---|---|
| François Stephan | Be-bound, France |

### Program Committee Co-chairs

| | |
|---|---|
| Eric Bonjour (Academic Co-chair) | Université de Lorraine, France |
| Luca Palladino (Industrial Co-chair) | Safran, France |

## Program Committee

The Program Committee consists of 21 members (10 academics and 11 industrialists) of high international visibility. Their expertise spectrum covers all of the conference topics.

### Academic Members

### Co-chair

| | |
|---|---|
| Eric Bonjour | Université de Lorraine, France |

**Members**

| | |
|---|---|
| Vincent Chapurlat | Mines Ales, France |
| David Flanigan | Chesapeake INCOSE Chapter, USA |
| Cecilia Haskins | NTNU, Norvegia |
| Neil Handen Ergin | Systems Engineering Penn State University, USA |
| Eric Levrat | Université de Lorraine, France |
| Anja Maier | Technical University of Denmark, Denmark |
| Eduarda Pinto Ferreira | ISEP-IPP, Portugal |
| Donna Rhodes | MIT, USA |
| Zoe Szajnfarber | George Washington University, USA |

**Industrial Members**

**Co-chair**

| | |
|---|---|
| Luca Palladino | Safran, France |

**Members**

| | |
|---|---|
| Ifede Joel Adounkpe | PSA, France |
| Raphael Faudou | Samares, France |
| Davide Fierro | INAF, Italy |
| Annabelle Meunier-Schermann | DGA (State Organization), France |
| Aurelijus Morkevicius | No Magic, Lithuania |
| Frederic Paci | Zodiac, France |
| Amaury Soubeyran | Airbus, France |
| Lawrence Toby | Jaguar Land Rover, UK |
| Lonnie Vanzandt | Sodius, USA |
| Christophe Waterplas | ResMed, Australia |

## Organizing Committee

The Organizing Committee consists of 18 members (academics and industrialists) of high international visibility. The Organizing Committee is in charge of defining the program of the conference, identifying keynote speakers, and has to ensure the functioning of the event (sponsoring, communication, etc.).

### Organizing Committee

#### Chair

| | |
|---|---|
| François Stephan | Be-bound, France |

#### Members

| | |
|---|---|
| Patrick Anglard | Assystem, France |
| Emmanuel Arbaretier | Airbus, France |
| Jean-François Bigey | MEGA International, France |
| Philippe Bourguignon | Engie, France |
| Guy-André Boy | Estia Institute of Technology, France |
| Eric Duceau | Airbus, France |
| Didier Dumur | CentraleSupelec, France |
| Gauthier Fanmuy | Dassault Systèmes, France |
| Pascal Foix | Thales, France |
| Alan Guegan | Sirehna, France |
| Omar Hammami | Ensta ParisTech, France |
| Fabien Mangeant | Renault, France |
| Luca Palladino | Safran, France |
| Pascal Poisson | Alstom Transport, France |
| Alain Roset | La Poste, France |
| Alain Roussel | AFIS, France |
| Richard Schomberg | EDF, France |

## Invited Speakers

#### Plenary sessions

| | |
|---|---|
| Come Berbain | Chief Technical Officer of the French State, DINSIC |
| Manfred Broy | Professor, Technical University of Munchen |
| Yves Caseau | Group Chief Information Officer, Michelin |
| Pierre Chanal | VP Engineering Transformation, Alstom |
| Vincent Danos | Research Director, CNRS |
| Marc Fontaine | Head of Digital Transformation, Airbus |
| Hervé Gilibert | Chief Technical Officer and Quality, ArianeGroup |

**"Methods and Tools" Track**

| | |
|---|---|
| Martin Neff | Chief Architect Systems Engineering, Audi |
| Marie Capron | Engagement Manager and System Engineering, Sogeti High Tech |

**"Design, Manufacture and Operation of Complex Products and Services" Track**

| | |
|---|---|
| Yann Bouju | Project Manager, Virtual and Augmented Reality, Naval Group |
| Olivier Flous | VP Digital Transformation, Thales Digital Factory |

**"Aeronautics" Track**

| | |
|---|---|
| Thierry Chevalier | Chief Engineer Digital Design and Manufacturing, Airbus |

**"Energy" Track**

| | |
|---|---|
| Yannick Jacquemard | R&D Director, RTE |
| Isabelle Moretti | Chief Scientific Officer, Engie |
| Guillaume Brecq | Product Owner, Engie |

**"Healthcare Services" Track**

| | |
|---|---|
| Philippe Baron | Chief Executive Officer, AxDaNe |
| Fabrice Lejay | R&D Product Line Manager, Stago |

**"Transportation & Mobility" Track**

| | |
|---|---|
| Brigitte Courtehoux | Executive Vice President Head of PSA Group New Mobility, PSA |

# Acknowledgements

We would like to thank all members of the Program and Organizing Committees for their time, effort, and contributions to make CSD&M Paris 2018 a top-quality conference. Special thanks go to the CESAM Community team who permanently and efficiently managed all the administration, logistics, and communication of the CSD&M Paris 2018 conference (see http://cesam.community/en).

The organizers of the conference are also grateful to the following partners without whom the CSD&M Paris 2018 event would not exist:

- **Founding partners**
  - CESAM Community managed by the Center of Excellence on Systems Architecture, Management, Economy & Strategy (CESAMES),
  - Association Française d'Ingénierie Système (AFIS),
  - The Ecole Polytechnique – ENSTA ParisTech – Télécom ParisTech – Dassault Aviation – Naval Group – DGA – Thales "Engineering of Complex Systems" chair.
- **Industrial and institutional partners**
  - Airbus Group,
  - Alstom Transport,
  - ArianeGroup,
  - INCOSE,
  - MEGA International,
  - Renault,
  - Thales.
- **Participating engineering and software tools companies**
  - Airbus Apsys,
  - Aras,
  - Dassault Systèmes,
  - Easis Consulting,

– Esteco,
– Hexagon PPM,
– Intempora,
– No Magic Europe,
– Obeo,
– Persistent Systems,
– SE Training,
– Siemens,
– Sodius.

# Contents

# Regular Papers

# Formal Methods in Systems Integration: Deployment of Formal Techniques in INSPEX

Richard Banach[1(✉)], Joe Razavi[1], Suzanne Lesecq[2], Olivier Debicki[2], Nicolas Mareau[2], Julie Foucault[2], Marc Correvon[3], and Gabriela Dudnik[3]

[1] School of Computer Science, University of Manchester, Oxford Road, Manchester M13 9PL, UK
{richard.banach,joseph.razavi}@manchester.ac.uk
[2] CEA, LETI, Minatec Campus, 17 Rue des Martyrs, 38054 Grenoble Cedex, France
{suzanne.lesecq,olivier.debicki,nicolas.mareau,julie.foucault}@cea.fr
[3] CSEM SA, 2002 Neuchatel, Switzerland
{marc.correvon,gabriela.dudnik}@csem.ch

**Abstract.** Inspired by the abilities of contemporary autonomous vehicles to navigate with a high degree of effectiveness, the INSPEX Project aims to create a minaturised smart obstacle detection system, which could find use in a wide variety of leading edge smart applications. The primary use case focused on in the project is producing an advanced prototype for a device which can be attached to a visually impaired or blind (VIB) person's white cane, and which, through the integration of a variety of minaturised sensors, and of the processing of their data via sophisticated algorithms, can offer the VIB user greater precision of information about their environment. The increasing complexity of such systems creates increasing challenges to assure their correct operation, inviting the introduction of formal techniques to aid in maximising system dependability. However, the major challenge to building such systems resides at the hardware end of the development. This impedes the routine application of top-down formal methods approaches. Some ingenuity must be brought to bear, in order that normally mutually hostile formal and mainstream approaches can contribute positively towards system dependability, rather than conflicting unproductively. This aspect is illustrated using two strands of the INSPEX Project.

## 1 Introduction

The contemporary hardware scene is driven, to a large extent, by the desire to make devices smaller and of lower power consumption. Not only does this save materials and energy, but given the commercial pull to make mobile phones increasingly capable, when small low power devices are incorporated into mobile phones, it vastly increases the market for them. The smartphone of today is unrecognisable (in terms of the facilities it offers) from phones even as little as a decade old. This phenomenon results from ever greater advances in system


E. Bonjour et al. (Eds.): CSD&M 2018, *Complex Systems Design & Management*, pp. 3–15, 2019.
https://doi.org/10.1007/978-3-030-04209-7_1

structure, and from the trend to incorporate minaturised sensing technologies that were well beyond the state of the art a short while ago. This trend continues unabated, and also massively propels advances in the Internet of Things.

The availability of such minaturised devices inspires the imagination to conceive novel applications, previously unrealised due to technological barriers. The INSPEX Project is the fruit of one such exercise in imagineering. Taking the autonomous vehicle [15] as inspiration, along with the data fusion that enables autonomous vehicles to elicit enough information about their environment from the data gathered by a multitude of sensors to navigate sufficiently safely that autonomous vehicles 'in the wild' are forseen within a few years [28,35], INSPEX aims to minaturise a similar family of sensors to create a device that offers comparable navigational support to a wide variety of smaller, more lightweight applications.

In the remainder of this paper we do the following. In Sect. 2 we cover the potential application areas for INSPEX, pointing to the key VIB use case that forms the focus of the project. In Sect. 3 we focus more narrowly on the technical elements of the VIB use case. In Sect. 4 we address ourselves to the deployment of formal modelling and verification technologies within the INSPEX development activity. We focus on two areas within which formal techniques were deployed in INSPEX, namely in the power management design and in the data acquisition pathway. Section 5 contains discussion and concludes.

## 2 INSPEX Application Use Cases

Figure 1 gives an indication of the range of applications that the INSPEX imagineering effort generated. The figure is divided into four broad aplication areas. Working left to right, we start with some examples of small autonomous vehicles. Autonomous navigation for these demands the small size, weight and power requirements that INSPEX seeks to provide. Small airborne drones have demands that are very similar, and as their number increases, their navigation and collision avoidance needs increase correspondingly. Considerations of size, weight and power also impinge on humanoid robots and specialised devices such a floor cleaning robots. INSPEX navigation capabilities will also increase autonomy and flexibility of use for factory based transport robots, which have to be prepared to avoid unexpected obstacles, unless their environment is sufficiently tightly constrained.

At the bottom of Fig. 1 we see some examples concerned with large enclosed environments, such as highly automated factories featuring assembly lines consisting of hundreds of robots. To increase the flexibility of reconfiguration of these, increased autonomy in the participating robots is one necessary ingredient. INSPEX, appropriately deployed, can significantly assist in meeting this requirement. The issue becomes the more forceful when the robots involved are

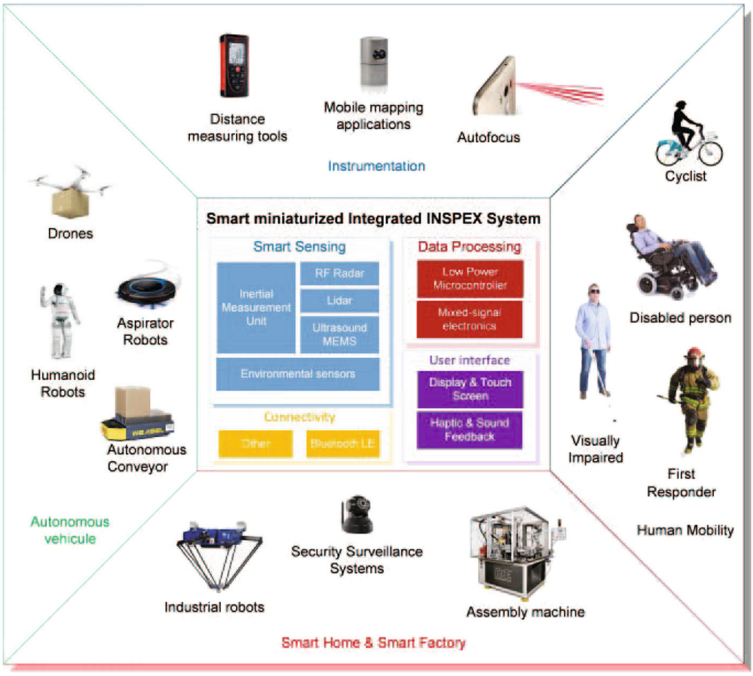


**Fig. 1.** Potential INSPEX use cases.

mobile, since along with the need to be more smart, they particularly need to avoid harm to any humans who may be working nearby. Security surveillance systems, traditionally relying on infra-red sensors, can also benefit from the extra precision of INSPEX.

At the top of Fig. 1 we see some examples concerned with distance estimation. Modern distance measuring tools typically make use of a single laser beam whose reflection is processed to derive the numerical result. For surfaces other than smooth hard ones, the measurement arrived at may be imprecise, for various reasons. INSPEX can perform better in such situations by combining readings from a number of sensors. A very familiar application area for such ideas is autofocus in cameras. These days, camera systems (typically in leading edge phones) employ increasingly sophisticated algorithms to distinguish foreground from background, to make up for varying lighting conditions, and generally to compensate for the user's lack of expertise in photography. INSPEX can add to the capabilities available to such systems.

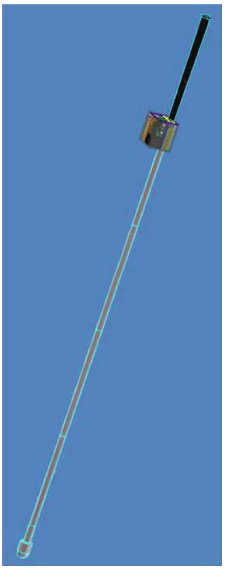

**Fig. 2.** The INSPEX white cane addon.

On the right of Fig. 1 we see the use cases for human centred applications. We see the VIB use case which forms the focus of the INSPEX project, and which will be discussed in detail later. There are also other prominent use cases. The first responder example includes cases like firefighters, who need to be able to enter hazardous environments such as smoke filled rooms, in which normal visibility is impossible. An aid like an INSPEX device can be of immeasurable help, in giving its users some orientation about the space in which they find themselves, without resorting to tentative feeling about, which is what firefighters are often reduced to. Other applications include the severely disabled who may have impediments to absorbing the visual information from their surroundings. And the able bodied too can benefit from INSPEX, when visibility is severely reduced. Although the cases of heavy fogs which reduced visibility to almost zero are thankfully history, today's mega-cities now feature smogs due to different sources of atmospheric pollution which can be just as bad.

## 3 The INSPEX VIB White Cane Use Case

Although a large number of use cases are envisaged for a system such as INSPEX, the primary use case addressed within the INSPEX Project is the smart white cane to assist visually impaired and blind persons. Figure 2 shows a schematic of one possible configuration for the attachment of a smart addon to a standard type of white cane. The white cane application needs other devices to support the white cane addon, in order that a system usable by the VIB community ensues. Figure 3 shows the overall system architecture.

As well as the Mobile Detection Device addon to the white cane, there is an Audio Headset containing extra-auricular binaural speakers and an inertial measurement unit (IMU)—the latter so that an audio image correctly oriented with respect to 3D space may be projected to the user, despite the user's head movements. Another vital component of the system is a smartphone. This correlates the information

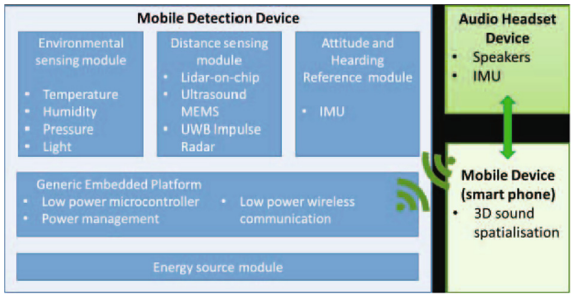


**Fig. 3.** The architecture of the INSPEX system.

obtained by the mobile detection device with what is required by the headset. It also is able, in *smart city* environments, to receive information from *wireless beacons* which appropriately equipped users can access. This enables the whole system to be even more informative for its users.

The white cane add-on contains the sensors that generate the data needed to create the information that is needed by the user. The chief among these comprise a short range LiDAR, a long range LiDAR, a wideband RADAR, and a MEMS ultrasound sensor. Besides these there are the support services that they need, namely an Energy Source Unit, environmental sensors for ambient light, temperature and humidity, another IMU and a Generic Embedded Platform (GEP).

The main sensors are subject to significant development and minaturisation by a number of partners in the INSPEX project. The short range LiDAR is developed by the Swiss Center for Electronics and Microtechnology (CSEM) and the French Alternative Energies and Atomic Energy Commission (CEA). The long range LiDAR is developed by the Tyndall National Institute Cork and SensL Technologies, while the wideband RADAR is also developed by CEA. The MEMS ultrasound sensor is from STMicroelectronics (STM). Cork Institute of Technology (CIT) design the containing enclosure and support services, while the audio headset is designed by French SME GoSense.

The GEP has a noteworthy challenge to confront. Data from the sensors comes in at various times, and with varying reliability. Distance measurements from the sensors are just that, merely distance data without any notion of direction, or orientation with respect to the user. The latter is elucidated by reference to data from the IMU in the mobile detection device. Data from both the IMU and directional sensors is timestamped, since freshness of data is crucial in providing information to the user that is not only accurate but timely. This enables distance sensor data to be aggregated by time and IMU data.

Once the data has been correctly aggregated, it is passed to the module in the GEP that computes the *occupation grid*. This is a partition of the 3D space in front of the user into cells, each of which is assigned a probability of its being occupied by some obstacle. The occupation grid idea is classical from the autonomous vehicle domain, but in its standard implementation, involves intensive floating point computation [28,35]. This is too onerous for the kind of lightweight applications envisaged by the concept of INSPEX. Fortunately INSPEX is able to benefit from a highly efficient implementation of the occupation grid, due to a careful analysis of the computations that are needed to derive a good occupation grid result [13]. The integration of all the hardware and software activities described, constitutes a non-trivial complex systems undertaking.

The wide range of sensors and their concomitant capabilities in the INSPEX white cane application is necessitated by the detailed needs of VIB persons navigating around the outdoors environment (in particular). Although a standard white cane can give good feedback to its user regarding the quality and characteristics of the ground in front of them, especially when the ground texture in the urban environment is deliberately engineered to exhibit a range of standard

textures signifying specific structures [31], it gives no information about hazards to be found higher up. It is a fact of life for VIB persons, that, like it or not, unanticipated collisions with obstacles at chest or head height are an unavoidable occurrence [25]. Many VIB persons are prone to wearing some sort of headgear, more or less involuntarily, to try to mitigate the worst effects of such unanticipated high level collisions. The possibility of alleviating this situation, even in the absence of other use cases, makes for ample justification for the development of INSPEX.

## 4 Formal Modelling and Verification in INSPEX

By now, formal techniques of system development have had a substantial history. After the early years, and the widespread perception that such approaches were 'hard' and did not scale, there was a concerted effort to dispel this view in classic works such as [11,12,19]. It was increasingly recognised, especially in niche areas, that formal techniques, wisely deployed, can add a measure of dependability not achievable by other means.[1] It became recognised that tools, particularly ones that worked in a reasonably scalable way,[2] were key to this [33,34]. This spurred the idea of 'Grand Challenges' in verification, one purpose of which was to both test and further inspire the scalability of tools [23,38,39]. Later surveys include [3,8], and this trend is also evident in [5].

The classic way of applying formal approaches is top-down. One starts with an oversimplified, but completely precise, definition of the desired system. This is then enriched, via a process of formal refinement, to take into account more system detail in order to address more of the system's requirements. Eventually one gets close enough to the code level that writing code is almost a transcription, or the code can be generated automatically.

There are many variations, small and large, on this basic idea. An early account is in [30]. The Z approach is represented by [21,32]; the VDM apporach is in [17,22]; TLA+ is in [24]; Alloy in [1]. There are many others. The B-Method, of which more later, is represented by [2,4,29].

Accompanying these developments grew the subdiscipline of behaviour oriented, or process oriented descriptions of system behaviour. Early references are [7,20,26]. Not long afterwards, it was observed that many process oriented properties of interest for systems conformed to a so-called model checking pattern, and this led to an explosion of research and tool building, since model checking could then be completely automated, leading to tools that could work in a push-button manner, and that could be embedded in development environments, in which they worked 'behind the scenes', i.e. without explicit user control or invocation. Among the tools in this style that have proved to be of interest for the INSPEX project are FDR [16], NuSMV [27], Uppaal [36].

[1] In some niche areas, the recognition came as a direct result of painful and expensive failure, the Pentium Bug and Arianne Disaster being iconic examples.

[2] It became apparent at this time that scalable formal tools were not an impossible dream, even if the degree of scalability was not as great as typically found in conventional approaches.

Whereas all the preceding approaches relied on there being a model of the system that was presented in a relatively abstract language, the growing power and scalability of tools generated an interest in techniques that worked directly on implementation level code. By now there are many well established tools that input an implementation in a given language such as C or C++, and that take this implementation and then analyse it directly for correctness properties [37]. Very often these properties are predefined runtime correctness properties concerning commonly introduced programmer errors, such as (the absence of) division by zero or (the absence of) null pointer dereference. Some however, e.g. [6,9] allow more application specific properties to be checked.

While direct checking of implementations would appear to be a panacea for verification, it nevertheless risks overemphasising low level system properties at the expense of the higher level view. When we recognise that deciding what the system *should be* is always a human level responsibility, and that formal approaches can only police the consistency between different descriptions of the same thing, abandoning the obligation to independently consider the abstract high level view of the system risks abandoning a valuable source of corroboration of the requirements that the system is intended to address. It is this kind of 'stereoscopic vision' on what the system ought to do and to be that constitutes the most valuable contribution that a top-down formal approach makes to system development, quite aside from the formal consistency checking.

In normal software developments, one starts the process with a good idea of the capabilities of software in general, so in principle, it is feasible to use a relatively pure top-down approach. Likewise in most hardware developments that take place at the chip level, one starts the process with a good idea of the capabilities of the technology platform that will be used, and working top-down is perfectly feasible (and in fact is unavoidable given the scale of today's chips). In both of these cases deploying top-down formal techniques (if the choice is made to do so) is feasible.

In INSPEX however, the development of the devices at the physical level is a key element of ongoing project activity, and the low level properties of all the devices used in the INSPEX deliverable are contingent and emergent to a significant extent. This makes the naive use of top-down approaches problematic, since there is no guarantee that the low level model that emerges from a top-down development process will be drafted in terms of low level properties that are actually reflected in the devices available, since the constraints on the system's behaviour that are directly attributable to physics are simply incontestable. As a result of this, the approach to incorporating formal techniques in INSPEX was a hybrid one. Top-down and bottom-up approaches were pursued concurrently, with the aim of meeting in the middle.

The next sections cover how this hybrid approach was applied in two of the INSPEX Project's activities, namely the design of the power management strategy for the mobile detection device module, and in the verification of the data pathway from the sensors to the data fusion application.

### 4.1 Power Management Formal Modelling and Verification

In INSPEX, power management poses a number of challenges. As stated earlier, the concentration of effort in INSPEX is on engineering a suitable outcome at the hardware systems level. Each sensor and subsystem creates its own problems. However they all share a common goal, one common to all mobile systems, of making the smallest demand on the power system that is possible. However, a focus on individual submodules risks paying insufficient attention to issues of coordination. A higher level view offers a number of benefits.

The first benefit is an issue of correct functioning. A naive combination of low level modules, each of them correct in itself, is not guaranteed to generate in a straightforward manner (from a systems level perspective), a globally correct behaviour. For example a submodule might conceivably be left running when it ought not to be running as an unexpected consequence of some complex sequence of events. The second benefit is the issue of global optimality. Focusing on the low level prevents the global optimisation of performance (in this case power saving) by balancing criteria from competing interests originating in diverse submodules.

A formal approach rooted in a higher level view can assist in both of these aspects of the development. Formal techniques are suited *sans pareil* to targeting correctness aspects of a development. Moreover, they are capable of capturing the global consequences of a collection of submodels when they are combined into a single entity, since they do not suffer from the variability of focus that humans can exhibit when they concentrate on one or another aspect of an activity.

Power management design in INSPEX proceeded top-down. From a human perspective this might mean considering broad properties of the power regime first, descending to low level detail at the end — this would fly in the face what has been stated above since what is most incontestable about the design is the low level properties of individual sensors etc. We reconcile these views by observing that formally, 'top level' properties are those that will not be contradicted in subsequent steps of development. This implies that they will be the most primitive rather than the most far reaching among the properties that the system satisfies.

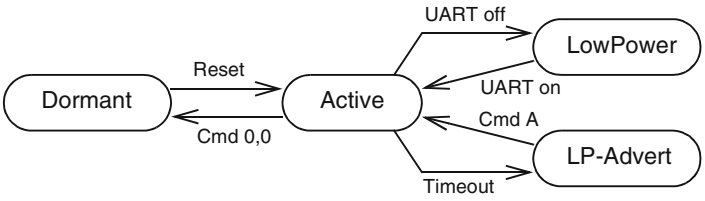


**Fig. 4.** A simplified Bluetooth transition diagram.

The most primitive properties include the state transition diagrams of the various sensors and other components. Figure 4 gives an example of a transition diagram for the Bluetooth submodule, rather drastically simplified from

the description in [10]. To incorporate this into a wideranging formal model we used the Event-B formalism [4]. This enables many levels of abstraction to be formally related to each other via refinement, and is supported by the Rodin tool which features many provers and plugins [29]. A state transition diagram such as Fig. 4 can be captured in Event-B in a fragment like:[3]

```
EVENTS
  Dor2Act
    WHEN  state = Dormant ∧ Reset
    THEN
      state := Active
    END
  LP2Act
    WHEN  state = LowPower ∧
UART_on
    THEN
      state := Active
    END
  LPA2Act
    WHEN  state = LP_Advert ∧
Cmd_A
    THEN
      state := Active
    END
...  ...
  Act2Dor
    WHEN  state = Active ∧ Cmd_0, 0
    THEN
      state := Dormant
    END
  Act2LP
    WHEN  state = Active∧UART_off
    THEN
      state := LowPower
    END
  Act2LPA
    WHEN  state = Active ∧ Timeout
    THEN
      state := LP_Advert
    END
```

A formal model such as the fragment above relates to the low level real time software and firmware as follows. Each event in the model corresponds to a software or firmware command, or an interrupt routine. The guard portion, expressed in the WHEN clause of the event, corresponds to the entry condition code in the command, or scheduler code that checks the cause of the interrupt. The event's THEN clause corresponds to the software command body, or the interrupt handler routine. As stated earlier, capturing all the commands and sources of interrupt enables questions of overall consistency to be examined.

Once the low level integrity has been established, other considerations can be brought to bear. A major element is the quantitative aspect. Event descriptions as above are embellished with numerical data regarding the energetic consequences of executing the event, enabling overall conclusions about energy consumptions to be drawn. Finally, considerations of overall power management policy can be layered onto the formal model and made to correspond with the implementation code.

### 4.2 The Data Acquisition Pathway

Another major area in which formal techniques were deployed in INSPEX to add robustness to the software design was the data acquisition pathway. As

[3] For reasons of the confidentiality of the future commercial exploitation of the INSPEX platform, what is shown here is not actual code.