

1. (a) **Project title:** Compositional Analysis and Specification of Hybrid Systems
 (b) **Project Acronym:** CASH
 (c) **Principal Investigator:** A.J. van der Schaft (UT-TW)
2. **Summary:** The main aim of the proposed project is to develop a compositional formalism for the specification of hybrid systems. Hybrid systems are systems with interacting discrete and continuous dynamics, as becoming more and more important in computer and control engineering. In line with a strong international trend for cooperation between computer scientists and control engineers on this topic, the project will be carried out as a collaboration between computer science (UT-INF) and mathematics (UT-TW). In particular, the project aims at combining the expertise on the process algebraic specification of discrete systems within formal methods research in computer science with the knowledge on continuous systems as available in mathematical systems theory. The formalism will be based on a process algebraic representation of hybrid automata and compositions, along the lines recently provided in [5] in the case of timed automata. The formalism will be tested on the description and analysis of physical systems with switching topology and of multi-agent control systems. Furthermore, interesting subclasses of hybrid systems will be identified that allow for algorithmic tool support, either with the aid of existing or future tool environments.

3. **Classification:**

Mathematics Subject Classification: 93B99, 93C99, 93C83, 93C85

Computer Science NVI Classification: 3.2, 3.4, 6.3, 6.4, 6.5

4. **Composition of Research Group.**

Name	Research Field	Affiliation	hours/week
Prof. dr. H. Brinksma	Formal Methods Tools	Fac. Comp. Sci. Un. Twente	4
Dr. A.J. van der Schaft	Math. systems th. Nonlinear control Hybrid systems	Fac. Math. Sci. Un. Twente	6
Dr. P.R. D'Argenio	Formal Methods Tools	Fac. Comp.Sci. Un. Twente	p.m.
Dr. J.W. Polderman	Behavioral Syst. Adaptive control	Fac. Math. Sci. Un. Twente	2
OiO (vacancy)		Fac. Math. Sci. Un. Twente	36
OiO (vacancy)		Fac. Comp. Sci. Un. Twente	36

Dr. D'Argenio is a fulltime postdoc in the related STW Progress project HaaST (Verification of Hard and Softly Timed Systems). Because of the potential for substantial synergy between the projects we estimate an effective involvement of about 4 hours/week.

5. **Research School.** The chair of *Formal Methods and Tools* of the Faculty of Computer Science, University of Twente, participates in the Research School of the Institute for Programming Research and Algorithmics (IPA). The *Systems, Signals and Control* Group of the Faculty of Mathematical Sciences, University of Twente, belongs to the Research School of the Dutch Institute for Systems and Control (DISC).
6. **Required funding period:** four years. Envisioned starting date: 01-09-2000.

7. Description of Proposed Research.

(a) *Problem statement and aims.*

During the last decade or so, one can witness a number of convergent trends in systems and control theory on the one hand, and the study of concurrent systems in computer science on the other hand. The theory of computer science and systems and control theory in fact have some common roots from the sixties (cf. the classic on mathematical systems theory by Kalman, Falb and Arbib [15]), in particular the commonality of the concept of input-state-output system, as had then been formulated in systems theory, with the concept of automaton or labeled transition system. Another example is the Springer journal "Mathematical Systems Theory", which in the beginning of its existence tried to combine systems theory with theoretical computer science. In spite of these common roots, however, it is fair to say that since the sixties both disciplines have evolved along almost completely different lines. At the same time, in many application areas computer engineers and control engineers have been working on the same type of problems, each with their own techniques but hardly communicating with each other.

This situation of mutual independence has more recently been challenged by a number of developments. Within computer science it is being realized that information processing systems must be understood and designed in the context of the environment in which they are supposed to function. In a physical environment, as is the case for so-called embedded (computer) systems, computers have to interact with *given* physical components, thus forcing an analysis of the overall (digital *and* continuous) system. This had led to the study of so-called *hybrid systems*, that is, systems with tightly interacting discrete (digital) and continuous dynamics. At the same time, within systems and control theory the prevailing paradigm of constructing a *controller*, processing the output data of the given physical system (the system under control) into signals provided to the actuators of the system, is gradually being recognized to be insufficient and too limited for further developments. Indeed, most of the cost in control system development today is spent on ad-hoc systems integration and validation techniques that rely mostly on exhaustive testing. There is thus a clear need for an analytical framework to deal with software-based control design in a systematic way, again leading to the study of hybrid systems. Publications in the area of formal methods of computer science that reflect this trend are e.g. [1, 8, 10].

From the systems and control perspective it is also becoming clear that "control" should be understood in the much broader context of meeting the control specifications by composing in a structured way the given physical components of the system with additional physical as well as digital components. The notion of 'control by interconnection' has been also stressed in the behavioral approach to systems and control as recently advocated by Willems and co-workers, see e.g. the textbook [17]. In this latter approach, as well as in most current approaches to modelling and simulation of complex physical systems, it is recognized that the framework of interaction by input and output variables (the signal flow point of view) does not always provide the proper level of generality. Instead, a systems or network modelling point of view naturally leads to the consideration of systems with external variables having no a priori input-output structure.

Furthermore, it is recognized by both communities that computer scientists and control engineers often face problems which involve the other field, and whose solution requires an integration of control theory and concepts from computer science. This entails the need for (often hierarchical) specification and analysis of hybrid systems. Without doubt this merging of continuous and discrete dynamics, under the requirement of hierarchical compositionality (modularity) to master the *complexity* of such systems, constitutes a great challenge for the theory of hybrid systems engineering. Some existing work on hybrid systems and their compositionality can be found in [6, 9].

The signalled trend toward collaboration at the scientific level is apparent from the growing number of international conferences and workshops that are devoted to hybrid systems and are increasingly a meeting place for scientists from both communities, such as Hybrid Systems, WODES, CAV, TACAS, etc.; see e.g. the proceedings [22, 23, 24, 25, 26, 27, 28].

(b) *Project Goals*

The proposed project has the following objectives:

- i. The development of a compositional formalism for the specification of hybrid systems, including the coupling of continuous variables of different subsystems. The formalism will be based on a process algebraic representation of hybrid automata and compositions along the lines of [5].
- ii. The development of a proper formal semantical model for the above formalism. The main challenge here will be to combine the discrete and continuous aspects of the model in an elegant and convincing way.
- iii. The study of notions of *equivalent* behaviour in the hybrid setting. This notion has been very important for the analysis of discrete systems in computer science, in particular the members of the family of so-called bisimulation relations [12, 11]. It will be important to see whether this can be usefully combined with notions from the world of continuous control.
- iv. The application of the formalism for the description and analysis of typical hybrid systems, such as physical systems with discrete transitions and control, and multi-agent control.
- v. Determine interesting subclasses of hybrid systems that allow for (interactive) algorithmic tool support for their analysis, by existing or future tool environments.

Below we elaborate on each of these goals.

The first aim of the proposed research proposal is to develop a specification language for a general class of hybrid systems. A successful approach to specify complex information-processing systems is based on *process algebras*, such as CCS, CSP, ACP and LOTOS. Process algebras were conceived for building large concurrent systems as the composition of smaller ones in a structured way. On the other hand, the prevailing description of complex (lumped-parameter) continuous systems is by means of *differential-algebraic equations* (DAE's) involving state variables and external (interaction) variables. Indeed, although differential equations are the standard way to model the dynamics of continuous systems, the *interconnection* of different continuous systems will usually lead to additional algebraic equations constraining the variables of the composing sub-systems. Therefore, it seems logical to develop a syntax for specifying hybrid systems merging process algebras with DAE's. For the much simpler case of *timed* discrete systems an adequate process algebra (called \heartsuit) has been recently provided in [4, 5], and this will be taken as the starting point for the present proposal. Note that indeed timed discrete systems are a special class of hybrid systems, since the continuous dynamics in this case is simply clock dynamics, that is, from the differential equation point of view, $\dot{t} = 1$, with t representing time. Also others have made initial steps in the proposed direction. An extension of CSP for hybrid systems (HCSP) can be found in [3], showing the feasibility of combining discrete and continuous aspects in one compact, compositional notation. A simulation language, χ , based on the combination of CSP and a representation of DAE's was recently presented in [7]. This work shows that also tool support for such hybrid combinations is possible. Although both approaches include semantic models for the respective formalisms ([3] is based on duration calculus, [7] on an operational (scheduling) model), they do not pursue the connections to process algebraic theory in the vein of [5, 4], which we hope will provide the key to an integrated *mathematical* formalism.

The current prevailing paradigm of specifying hybrid systems is by means of *hybrid automata* [1, 8], which provide an essentially monolithic model that lacks the compositionality of process algebraic approaches. Extensions that study the composition of hybrid automata are reported in [6, 9]. The process algebra \heartsuit as developed in [4, 5] covers the description of discrete timed systems by *timed automata*, and it is hoped that it will be possible to develop a process algebra for hybrid systems that in the same way covers hybrid automata. An initial approach to the specification of hybrid systems by means of *equations and inequalities* governing hybrid dynamics has been recently proposed in the textbook [13]. In this approach the continuous dynamics is modelled by DAE's, while the discrete dynamics is described by some form of difference equations, with discrete time parameter being the occurrence of *event times*. Although the description of the discrete dynamics lacks the refined structure given by the use of process algebras, the approach certainly points to important problems in the specification of the syntax and semantics of a hybrid system description. In particular, it shows that the usual notion of hybrid automata is not sufficient for our purposes, since we also want to consider the composition of systems via their *continuous* external variables. In principle it seems feasible, however, to develop suitable forms of parallel composition of hybrid automata that enable such connections, as the result of such continuous synchronisations can be represented by adding extra constraints to the location invariants of the product automaton.

A fundamental concept in the specification of systems by process algebras is the notion of *bisimilarity* [12, 11]. A related idea is also present in the theory of continuous-time input-state-output systems in the notion of *equivalent* systems having the same input-output behavior. However, the notion of bisimilarity is more flexible. A first task in the current project proposal will therefore be to develop a notion of bisimilarity for continuous time systems and for hybrid systems. It is to be expected (like in the case of bisimilarity for timed automata in [5]) that it will be useful to also develop a notion of *structural* bisimilarity for hybrid systems, which is expressed, say, in terms of the defining notions of a hybrid automaton; that is, location invariants and guards, as well as DAE's. It is to be expected that notions of structural bisimilarity of *linear* DAE's will involve concepts of minimality and (controlled) invariant subspaces, as have been studied in linear systems theory, while for general nonlinear DAE's their nonlinear counterparts, see e.g. [16], will play a role. Of course, from a process algebra point of view, the goal is to develop a specification language of hybrid systems together with an equational theory which is sound and complete (for regular behaviours) with respect to the algebra with equivalence relation given by bisimilarity.

An underlying problem in this endeavor will be the development of the *semantics* of a description of hybrid systems. Indeed, as already discussed in [13], the semantics of the standard hybrid automaton model is already not completely unambiguous, certainly if one allows general classes of differential equations describing the evolution of the continuous variables. Also in the framework of EFF's the specification of the semantics is a delicate matter. For non-structural versions of bisimulation, which capture a game-theoretic notion of observable equivalence of non-deterministic behaviours, extended automata models, such as timed and stochastic automata [2, 5], must be mapped to more suitably structured labelled transitions with a (partly) continuous state space. It will be very interesting to see whether on this level connections can be found between notions as bisimilarity and nondeterminism on the one hand, and classical control-theoretic properties as observability and controllability on the other hand.

Although the proposed project in the first instance has the ambitions of a fundamental study, it will be important to have some application areas in mind that can serve as test beds for the theory to be developed. One such application area is formed by the conceptual construction of robotic systems, which are primarily multibody mechanical systems with variable (kinematic and geometric) constraints under the influence of

switching control. Within the control community there is obviously much interest for these systems; see also [18] for some background on their modelling and control, and [19] for similar developments in the context of switching electric circuits. The hybrid dynamics of such systems resulting from the constraints alone has been successfully described in the framework of *complementarity systems*, which are formed by sets of differential-algebraic equations and inequalities, see e.g. [14, 20].

Another application area is formed by *multi-agent control systems*, as now being intensively studied for instance in the context of air traffic control. This is a typical problem of describing in an insightful way the complex dynamics of agents having their own continuous dynamics (e.g. the dynamics of the air plane), communicating with each other and a central operator, under strict safety conditions, see e.g. [21]. Similar problems also appear in the design and control of other transportation systems, see for example the journal special issues [29, 30] for research in these directions.

In the study of complex information-processing systems it has become common knowledge that the application of any formal theory is hopeless without adequate software tool support. It is our intention to identify interesting subclasses of hybrid systems that in principle allow for algorithmic tool support, either with the aid of existing or future tool environments. Also here, however, our approach will be fundamental in the sense that we look at principles and algorithms that define generic support for such system classes. This in contrast to a bottom-up approach, in which one tries to extend concretely existing tools on a mostly pragmatic basis. Where this is possible within the constraints of the project we will strive to illustrate ideas by prototypical implementations.

- (c) *Relevance, history, relation to the field.* As already indicated in the introduction of item (a) in section 7, there is a tremendous interest, in computer science, control engineering, as well as in modelling and simulation, for the development of an analytical framework for the representation, analysis and design of hybrid systems. The research area of what are now called hybrid systems was initiated only about ten years ago, both in computer science and control.
- (d) *Relation with research carried out elsewhere.* Roughly speaking, in computer science the emphasis has been on the specification and analysis of timed automata, and the development of model checkers for this subclass of hybrid systems (e.g., HYTECH at Cornell/Berkeley, KRONOS at VERIMAG Grenoble, UPPAAL at Aalborg/Uppsala and SHIFT at Berkeley), while in systems and control much attention has been paid on notions of switching and variable structure control, the control of hybrid systems via abstraction to discrete-event systems, and the simulation of physical systems with discrete transitions.

The present proposal wants to develop a general framework based on process algebras and DAE's. First steps in this direction have already been made by others [7, 3], illustrating the initial feasibility of the proposed approach. Using the approach for timed en stochastic systems as developed in [4, 5] we intend to study the connections between discrete and continuous aspects on a more fundamental level. We believe such a fundamental study will be very valuable for unifying the theory of hybrid systems, as well as for future tool development.

Both the computer science and mathematics research groups at the University of Twente are scientifically well-connected to the research groups worldwide working on the representation of hybrid systems and the development of tool support for verification and simulation. Brinksma is on the programme committee of CAV2000 and member of the steering committee of the TACAS conferences, Van der Schaft was a member of the programme committee of the second international workshop Hybrid Systems: Computation and Control (HSCC'99). The research group of Brinksma collaborates closely with that of Larsen at Aalborg (home of the Uppaal tool). Larsen will spend a sabbatical year at the University of Twente in the academic year 2000-2001. Van der Schaft

will be one of the two main speakers in the upcoming workshop on Hybrid Control and Automotive Applications, Lund, May 2000, organized by the european ESPRIT project Heterogeneous Hybrid Control (H2C).

On the national level the computer science group collaborates with the group of Feijs and Philips Research on the testing of embedded systems (NWO STW project Cote-de-Resyste), and with the group of Vaandrager at Nijmegen on the analysis of timed and stochastic systems (NWO STW project HaaST). General research on system verification and validation is carried out in the SVC project in collaboration with Groote (CWI) and Lucent in the frame of the Telematica Instituut. The mathematics group collaborates closely with J.M. Schumacher (CWI & KUB) and M. Heemels (TUE) on the modeling and analysis of hybrid systems in the frame of the NWO-SWON Large Project 'Mathematical modeling of open dynamical systems'. Furthermore, Van der Schaft supervises an OiO-project on simulation of (multi-modal) physical systems jointly with P.C. Breedveld (UT, Electrical Engineering).

(e) *Relation with research programme of the group in Twente.*

The proposed project brings together two groups, in different faculties, and the research programme of the project has been devised precisely to stimulate a challenging interaction between these two groups. The proposed project fits very well within the activities of the group in computer science, and can be seen as a continuation of the recent Doctoral Dissertation [5] into the direction of incorporation of continuous dynamics. Considerable synergetic effects are expected from interaction with the current research projects on embedded systems (Cote-de-Resyste, and especially HaaST). The proposed project could profit substantially from the expertise of these projects in the area of tool support and implementation. In turn, the proposed project could contribute a more general and fundamental hybrid systems view to the work on timed and stochastic systems. The *Systems, Signals and Control* group within mathematics has performed fundamental research in various areas of systems & control, including hybrid systems, as illustrated by the recent introductory textbook [13]. Also, the analysis, control and simulation of physical systems with discrete transitions, as well as the theory of behavioral systems, are current research directions in the group, and will provide a stimulating environment for the proposed OiO project.

References

- [1] R. ALUR, C. COURCOUBETIS, N. HALBWACHS, T.A. HENZINGER, P.-H. HO, X. NICOLLIN, A. OLIVERO, J. SIFAKIS AND S. YOVINE. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138: 3–34, 1995.
- [2] R. ALUR AND D. DILL, A theory of timed automata, *Theoretical Computer Science*, 126: 183–235, 1994.
- [3] ZHOU CHAOCHEN, WANG JI, AND A. RAVN. A Formal Description of Hybrid Systems. In *Hybrid Systems III*. R. ALUR, T. A. HENZINGER, E. D. SONTAG, EDITORS. Lecture Notes in Computer Science 1066, 511–530, Springer, Berlin, 1996.
- [4] P.R. D'ARGENIO AND E. BRINKSMA,. A Calculus for Timed Automata (Extended Abstract), In *Proceedings of the 4th International School and Symposium on Formal Techniques in Real Time and Fault Tolerant Systems*, Uppsala, Sweden , B. Jonsson and J. Parrow (eds.), Lecture Notes in Computer Science 1135, 110–129, Springer-Verlag, 1996.
- [5] P.R. D'ARGENIO. *Algebras and Automata for Timed and Stochastic Systems*. Doctoral Dissertation, University of Twente, 1999.

- [6] S. BORNOT AND J. SIFAKIS. On the Composition of Hybrid Systems. In *Hybrid systems: Computation and Control*. S. Sastry and T.A. Henzinger (eds.), Lecture Notes in Computer Science 1386, 69–83, Springer-Verlag, 1998.
- [7] G. FÁBIAN. *A Language and Simulator for Hybrid Systems*. Doctoral Dissertation, Eindhoven University of Technology, 1999.
- [8] T.A. HENZINGER. The Theory of Hybrid Automata. In *Proceedings 11th Annual Symposium on Logic in Computer Science*, New Brunswick, USA, 278–292, IEEE Computer Society Press, 1996.
- [9] N.A. LYNCH, R. SEGALA, F.W. VAANDRAGER, H.B. WEINBERG. *Hybrid I/O Automata*, Report, Computing Science Institute, University of Nijmegen, 1999.
- [10] O. MALER, Z. MANNA AND A. PNUELI. From Timed to Hybrid Systems. In *Proceedings REX Workshop on Real-Time: Theory in Practice*, Mook, The Netherlands, June 1991, Bakker, J.W. de, C. Huizing, Roever, W.P. de, and G. Rozenberg (eds.), Lecture Notes in Computer Science 600, 447–484, Springer-Verlag, 1992.
- [11] R. MILNER. *Communication and Concurrency*. Prentice Hall, 1989.
- [12] D.M.R. PARK. *Concurrency and Automata on Infinite Sequences*. Lecture Notes in Computer Science 104, Springer-Verlag, 1980.
- [13] A.J. VAN DER SCHAFT, J.M. SCHUMACHER. *An Introduction to Hybrid Dynamical Systems*. Springer Lecture Notes in Control and Information Sciences, vol. 251, Springer, London, 2000.
- [14] A.J. VAN DER SCHAFT, J.M. SCHUMACHER. Complementarity modeling of hybrid systems. *IEEE Trans. Automatic Control*, 43: 483–490, 1998.
- [15] R.E. KALMAN, P.A. FALB, AND M.A. ARBIB. *Topics in Mathematical Systems Theory*. McGraw-Hill, New York, 1969.
- [16] H. NIJMEIJER, A.J. VAN DER SCHAFT. *Nonlinear Dynamical Control Systems*. Springer, New York, 1990 (4th reprint 1998).
- [17] J.W. POLDERMAN, J.C. WILLEMS. *Introduction to Mathematical Systems Theory: a Behavioral Approach*. Texts in Applied Mathematics, Springer-Verlag, New York, 1998.
- [18] A.J. VAN DER SCHAFT. *L₂-Gain and Passivity Techniques in Nonlinear Control*. Lect. Notes in Control and Inf. Sciences, vol. 218, Springer-Verlag, Berlin, 1996, p. 168, 2nd revised and enlarged edition, Springer-Verlag, Communications and Control Engineering series, London, 2000.
- [19] G. ESCOBAR, A.J. VAN DER SCHAFT, R. ORTEGA. A Hamiltonian viewpoint in the modelling of switching power converters. *Automatica, Special Issue on Hybrid Systems*, vol.35, pp.445–452, 1999.
- [20] A.J. VAN DER SCHAFT, J.M. SCHUMACHER. The complementary-slackness class of hybrid systems. *Math. Contr. Signals & Systems* 9, pp. 266-301, 1996.
- [21] J. LYGEROS, C. TOMLIN, S. SASTRY. Controllers for reachability specifications for hybrid systems. pp. 349–370 in [30].
- [22] R. I. GROSSMAN, A. NERODE, A. P. RAVN, H. RISCHEL, EDITORS. *Hybrid Systems*. Lecture Notes in Computer Science, vol. 736, Springer, Berlin, 1993.
- [23] P. ANTSAKLIS, W. KOHN, A. NERODE, S. SASTRY, EDITORS. *Hybrid Systems II*. Lecture Notes in Computer Science, vol. 736, Springer, Berlin, 1995
- [24] R. ALUR, T. A. HENZINGER, E. D. SONTAG, EDITORS. *Hybrid Systems III*. Lecture Notes in Computer Science, vol. 1066, Springer, Berlin, 1996
- [25] P. ANTSAKLIS, W. KOHN, A. NERODE, S. SASTRY, EDITORS. *Hybrid Systems IV*. Lecture Notes in Computer Science, vol. 1273, Springer, Berlin, 1997

- [26] O. MALER, EDITOR. *Hybrid and Real Time Systems*. Lecture Notes in Computer Science, vol. 1201, Springer, Berlin, 1997.
- [27] S. SASTRY, T.A. HENZINGER, EDITORS. *Hybrid Systems: Computation and Control*. Lecture Notes in Computer Science, vol. 1386, Springer, Berlin, 1998
- [28] F.W. VAANDRAGER AND J.H. VAN SCHUPPEN ,EDITORS. *Hybrid Systems: Computation and Control*. Lecture Notes in Computer Science, vol. 1569, Springer, Berlin, 1999.
- [29] P. ANTSAKLIS, A. NERODE, GUEST EDITORS. Special Issue on Hybrid Control Systems. *IEEE Transactions on Automatic Control*, vol. 43, 1998
- [30] A. S. MORSE, C. C. PANTELIDES, S. S. SASTRY, J. M. SCHUMACHER, GUEST EDITORS. Special Issue on Hybrid Systems. *Automatica*, Vol. 35, 1999.

8. Expected use of Instrumentation.

Computing Equipment, Software Tools.

9. Work programme.

Year 1 (INF and TW):

- The candidates will follow a selection of appropriate courses in formal methods and systems and control (such as the graduate courses offered by IPA and DISC).
- Familiarisation with problem area.
- First design of a process algebraic model and formalism for hybrid systems.

Year 2 (INF and TW):

- Development of adequate notions of equivalence.
- Syntax and semantics of a process algebraic formalism for hybrid systems.

Year 3 TW:

- Formalisation of systems theory of hybrid systems; observability and controllability.
- Case study in physical systems with variable topology.

INF:

- Identification of hybrid systems that allow algorithmic tool support.
- Definition of tool functionalities and algorithms.

Year 4 TW:

- Case study in multi-agent control systems.
- Completion of thesis.

INF:

- Definition of tool architecture, preliminary prototype implementation.
- Completion of thesis.

10. Requested Budget

2 OiO positions (1 TW, 1 INF).

H. Brinksma is the envisioned promotor for the OiO at the Faculty of Computer Science. A. J. van der Schaft is expected to be promotor for the OiO at the Fac. of Mathematical Sciences.

11. Literature.

The literature that is directly related to this project is formed by [4, 5, 13, 14]. These references may be found in the references at the end of the ‘Description of Proposed Research’.