Chapter 1

Extrait du Rapport de l’équipe S3

Team leader  I. Demeure (P).

Team members  P. Busch (Technician), P. Dax (DE), B. Dupouy (MC), S. Gadret (CE), S. Gardoll (CNRS engineer), J. Hugues (MC), G. Mouret (Research engineer), E. Najm (P), L. Pautet (P), S. Vignes (MC), S. Tardieu (MC)

PhD students  E. Borde (12/06–), X. Grehant (10/06–), H. Ha Duong (10/06–), I. Hamid (02/05–05/08), J. Hugues (10/02–09/05), Z. Kazi-Aoul(10/03–2/08), G. Lasnier (10/08–), S. Naqvi (10/02–12/05), G. Paroux (CIFRE 10/04–06/09), I. Perseil (10/05–), X. Renault (1/2007–), T. Vergnaud (10/03–11/06), B. Zalila (10/05–11/08).

Post-docs, and sabbaticals  P. Feiler (CMU-SEI 04/08–06/08).

1.1 Objectives

Adaptable middleware
Existing middleware technologies for Mobile Ad hoc Networks applications (MANet) or Distributed Real time Embedded Systems (DRE) (such as TAO) provide general purpose execution platforms targeting a large spectrum of application domains. Their complex design patterns induce large memory footprints and execution overheads but also produce systems that are difficult to analyse and verify.

Our research is precisely aimed at addressing this pitfall. Our goal is to produce a verifiable and highly configurable middleware factory. The sought and delivered factory should be based on a flexible, modular and versatile architecture that allows for the automated generation of middleware instances matching specific application requirements. This endeavour involves also the design and delivery of predefined or automatically generated components that support specific distribution and communication functions. The factory should allow for the verification of these individual components as well as their sound integration in the delivered middleware.

General purpose middleware also fail to resolve MANet specific needs. A MANet is a self-configuring network of mobile nodes connected by wireless links. MANets are highly dynamic. Changes may impact network topology in many ways - nodes may become out of reach of each other, or may have energy failures. Hence servers must be redundantly distributed over the nodes. The supporting middleware must manage dynamic service location and routing. Thus they must monitor the topology and adapt with appropriate actions. They must also preventively manage power consumption by monitoring and balancing node activities. These are the goals we pursued in designing middleware for MANets.

Model driven development
Our main endeavour is to define and build a development process, endowed with a supporting transformational tool chain, that aims at producing systems that faithfully implement high-level requirements. Mode Driven Engineering (MDE) is a key enabling technology: models are versatile as they can describe various software and system engineering artefacts: from requirements down to resources, platforms, application components, infrastructure components, etc. The applicability of MDE to Distributed Real time Embedded Systems (DREs) has not been properly addressed yet by the research community.

Our aim is precisely to bring the potential benefits of MDE to reality in the realm of DREs and safety critical systems. Thus, the sought and delivered tool chain has distinctive features that are hard to obtain in DREs.

Cost reduction and higher quality are to be achieved by extending the automatic code generation capabilities to distributed code and to the automatic deployment of the system. It is to be achieved also by allowing for the integration of predefined components (COTS) in the transformational process. Such an automatic code generation allows to produce the optimized and analyzable components of PolYORB-HI, our DRE AADL middleware (previously described). System quality and correctness is to be enhanced by the use of formal verification of both the functional (deadlock/starvation non-appearance) and non-functional (schedulability, response time) properties of systems.

The delivered process should address and integrate the different domains of expertise that are involved in building complex space and avionics systems, from requirements capture, through formal modeling and property assessment, down to the final implementations.

1.2 Main Results

1.2.1 Adaptable Middleware

Faculty I. Demeure, J. Hugues, L. Pautet.

Main events and external collaborations Summer school on Real Time Systems (ETR 09) by L. Pautet, France Telecom R&D, TAI/Thales, SC2/Thales, Agence Spatiale Europeenne (TOS-EME/ESA), Peter Feiler (SEI/CMU), Fabrice Kordon (LIP6/UPMC). Member of the SAE (Society of Automotive Engineers) ADL (Architecture Analysis Design Language) standard committee.

Projects ANR Flex-eWare, IST ASSERT, contracts with ESA and AdaCore RNRT-Transhumance, IST-POPEYE STREP, Contract with Orange R&D.

Adaptable middleware for distributed real time embedded systems

We study the problem of middleware engineering in the context of distributed real-time embedded (DRE) systems [77].

To tackle the middleware development complexity, we defined the schizophrenic middleware architecture. It makes it possible, for the first time, to instantiate simultaneously several distribution models with an excellent code reuse ratio compared to other approaches [38]. PolyORB, an implementation of this highly configurable architecture [39], is now industrially supported by AdaCore.

PolyORB is one of the very few middleware platforms to have been modelled and verified on some non-trivial configurations using Petri nets (collaboration with LIP6/UPMC) in order to assess

http://www.adacore.com/home/products/gnatpro/add-on_technologies/distributed_systems
1.2. MAIN RESULTS

properties like deadlock free, livelock free or buffer dimensioning [76]. To improve the analysability of both the DRE system and its middleware, we decided to comply with the Ravenscar profile, a concurrency model for use in High-Integrity systems [39]. We also decided to use the Architecture Analysis and Description Language (AADL) (collaboration with SEI/CMU) to support our new design process for DRE systems [7].

We revisited PolyORB and the schizophrenic architecture [44] to define PolyORB-HI. It takes advantage of AADL to precisely deduce deployment and configuration information to automatically generate optimized and analyzable middleware components [71]. This AADL executive platform was one of the main results of the IST project ASSERT leaded by the European Space Agency, but also of the ANR Flex-eWare project. For instance, THALES reduced by a factor of 500 the memory footprint of executables produced with a concurrent approach. PolyORB-HI associated with our code generators is currently the first AADL execution platform for producing both Ada, C or RTSJ DRE systems.

We are studying the impact of new trends towards more complex DRE systems, like hierarchical partitioning as well as the duality of the safety and security features on middleware architecture. POK has enriched PolyORB-HI with safety (ARINC) and security (MILS) features coming from partitioned systems [24]. To our knowledge, POK is the first open-source kernel providing both ARINC and MILS services. In the context of ANR Flex-eWare, we also made architectural improvements to enforce mode-based reconfiguration [18].

Adaptable middleware for collaborative applications over MANets

We designed and prototyped adaptable middleware solutions for Mobile Ad hoc Networks (MANets) providing support for collaborative applications. This led us to the following contributions.

Publish-subscribe system for MANets. Chapar is an event system designed for MANets [51]. It supports event persistency to resist transient disconnections and network partitioning. Following a cross-layer approach, Chapar relies on the Multipoint Relays (MPRs) defined in the OLSR MANet routing protocol as distributed brokers, and uses the OLSR routing table to disseminate the events. The support of persistency coupled with the cross-layer approach taking benefit from the OLSR MANet routing protocol, make Chapar quite unique.

Data-sharing system for MANets. Our system uses a predictive algorithm based on semantic information about the user and the data and previous access patterns to decide how to proactively replicate data. It creates enough replica to prevent data loss in case a peer unexpectedly disappears or a partition occurs. To this end, we proposed a stable group creation algorithm based on long lasting connectivity. While data sharing systems for MANET already exist, both the use of semantic information and of temporal stability are new in this domain. We illustrated the interest of the proposed algorithms by studying how a wiki service on MANETs would benefit from them [33], [32].

Energy-aware middleware for MANets. We proposed architectural guidelines, mechanisms and algorithms to design an energy aware middleware for MANets [7]. Each middleware module is designed with various level of functioning. When the energy level is high, the middleware provides all functionalities. When the energy level decreases, the functionalities are degraded in order to preserve the battery. The experiments performed showed a reduced energy consumption of about 20 % for the experiments conducted with ciphering and non acknowledged transport.

Open source software. Our contributions were prototyped and integrated to either one of the two platforms developed within the framework of POPEYE an IST STREP Project, and Transhumance an ANR RNRT project. Both platforms are available as open source software on Sourceforge. These developments were consucted jointly with our Transhumance and POPEYE partners and in particular with THALES present in both projects.

Innovative demonstrators. Finally, another contribution of this work lies in the cooperation with digital media designers (SES department) in order to propose innovative services, such as the above mentioned treasure hunting game, as demonstrators [28], [25].

A flexible architecture for the adaptation of composed multimedia

We proposed and prototyped PAAM (Provision of AdApTable Multimedia composed documents) a
service oriented architecture for the adaptation of multimedia documents to user preference and context. A novelty in PAAM, with respect to related work, is that adaptors are offered as shared resources by the participants; hence PAAM is an example of peer-to-peer collaboration overlay that provides all the functionalities to declare, look for, select and compose adaptors located at participating peers. For the project purpose, we extended WSDL (Web Services Description Language) to describe adaptors in order to make them easily declared, looked-up and composed. We proposed a complete adaptation chain that was implemented using the web services technology [?].

1.2.2 Proof Based and Model Driven Developments

Faculty J. Hugues, E. Najm, L. Pautet, S Vignes.

Main events Organisation of AFADL’06 by S. Vignes; Neptune’08 et ’09 by J. Hugues, S Vignes; FORTE’06, SDL’07 and ICSSEA’08 by E. Najm; IEEE/IFIP RSP’09 by J. Hugues

Projects and ACI FIACRE, ANR Flex-eWare, IST ASSERT, contracts with ESA and AdaCore, ANR EDEMOI

Model based development for distributed real time embedded systems

We have built a combined expertise in modular middleware, formal modelling and software engineering. This wide range of expertise helps in delivering a full toolchain targeting the development of DREs.

We chose the AADL (Architecture Analysis and Design Language) as our pivot modelling language. AADL is an Architecture Description Language (ADL) well suited for DRE’s. We have taken a leading position in the standardisation of this language, proposing several contributions to the core AADLv2 standard, and taking the lead on the definition of some annexes on data modeling, integration of programming languages, and on the integration of ARINC653 for the modeling of avionics system.

Based on AADL, We have designed a “Verification Driven Engineering” [52] process, where one iterates in order to enable verification at model level. We have shown that we need multiple formal methods to support the full engineering process. Therefore, we explored different tracks:

We adopted the Ada Ravenscar profile as one of our target patterns towards code generation, for its robustness and suitability for high-integrity systems as well as for its deterministic behaviour and its schedulability analysis capabilities.

We have defined the Ravenscar Meta Model (RMM) that we endowed with a formal semantics in order to make the generated code amenable for verification [35]. We have also defined a novel “deterministic” intertask communication pattern that we proved to be sound (cooperation with INRIA) [34]. We developed a prototype: ARC, to validate our transformations [6] [36]. We studied in collaboration with LIP6, the possibility to use Colored or Timed Petri Nets as another tool to support verification [66, 65], and with UBO the possibility to perform high-level schedulability analysis of DREs.

We studied in collaboration with CMU/SEI the possibility to express safety and security properties on AADL model. We defined an AADL annex (REAL) [?] to express design patterns mandated by ARINC or MILS.

Ocarina [55] is the Open Source platform software that gathers our AADL tools and contributions. Ocarina has been tested and validated by academic and industrial partners as part of our funded R& D projects IST-ASSERT and ANR Flex-eWare in collaboration with ESA and Thales. Ocarina provides also a method for the integration of other modeling frameworks like SCADE or Simulink.

Proof based orchestration of web services

We defined a novel approach for the sound orchestration of services, based on expressing jointly behaviours and their types [27]. We proposed (1) Orcharts (orchestration charts) to define session based services and (2) Typecharts to support session types with complex interaction patterns that generalise the request/response interaction paradigm defined in BPEL. We defined an
algorithm for deciding behavioural well typedness and showed that it guarantees an important safety property: in all states of any configuration of well typed orchestr, all exchanged messages are expected and understood by their target partner.

Model based approach for formalising security properties
Our main contribution is a method to formalize security properties derived from the Goal-Oriented Requirements meta-method [57]. In this method, we match goals with security properties (for instance preventive security measures). We have adopted multiple notations to capture these properties: Natural language, a UML security profile, and formal methods (B and Z). Graphical UML descriptions are readable by domain experts and are used to support validation activities whereas formal methods are needed to support verification. Formal models are used to check the consistency of the documents and to generate test scenarios. The UML and formal models are tightly linked so as to make sure that "what you validate is that you verify".

We have applied our RE process and method to the domain of airport security (cf. EDE-MOI Project). However, various domains including safety critical embedded system or ambient and pervasive adaptation, are concerned by confidence in the security properties and will be confronted with certification activities.

1.3 References

1.3.1 ACL: Articles in ISI-Indexed Journals


1.3.2 ACLN: Articles in Other Refereed Journals


1.3.3 ACTI: Articles in Proceedings of International Conferences


[67] N. Richard, S. Tardieu, and S. Yamada. Cascaded Generic XCS to Learn About Remind-
ning Preferences. In International Workshop on Learning Classifier Systems, Londres, An-

generating tailored distribution middleware for embedded real-time systems. In ERTS’06,

lications from their Architectural Description. In 12th International Conference on Reli-
able Software Technologies - Ada-Europe 2007, volume LNCS, pages 155–167, Geneva,
Switzerland, June 2007.

[70] B. Zalila, J. Hugues, and L. Pautet. An Improved IDL Compiler for Optimizing CORBA

International Symposium on Object-oriented Real-time distributed Computing (ISORC’08),

property preservation in high-integrity real-time systems. In OSPERT 2007 — Workshop
on Operating Systems Platforms for Embedded Real-Time applications, pages 35–39, Pise,

1.3.4 OS: Books and Book Chapters

[73] LNCS 4229, editor. Formal Techniques for Networked and Distributed Systems, Heidelberg,
Germany, September 2006. Springer.


systèmes à large échelle. Lavoisier, France, 2008.

Paris (France), 2006.