The MEFISTO Project

ESPRIT Reactive LTR 24963 Project

Title of Document:	Formal System Specification
Author(s):	David Navarre, Philippe Palanque, Ousmane Sy, Rémi Bastide, Duc-Hoa Le
Affiliation(s):	L.I.H.S. – University of Toulouse 1
Date of Document:	26th October 1999
Mefisto Project Document:	Deliverable 4
Distribution:	INTERNAL
Keyword List:	Interactive cooperative object, formal specification technique, Interactive systems formal specification
Version:	Draft

MEFISTO Partners:

CNUCE, Pisa, Italy

Alenia, Rome, Italy

Dept. of Computer Science, University of York, United Kingdom

DRA, Malvern, United Kingdom

Université Toulouse 1, Toulouse, France

CENA/Sofréavia, Toulouse, France

Associates Partners: University of Siena, Italy — ENAV, Rome, Italy

Title: Formal System Specification	**Id Number: Deliverable 4**

Table of Contents

1 Introduction

The work Package 2 of the project Mefisto is entitled "Formal specification and verification of user interfaces".

As stated in the technical annex, the purpose of this part of the project is to give precise and unambiguous specifications of the tasks to perform in ATC domain, of the possible user behaviour and of the software prototypes to develop. The dimensions of the specifications performed will be suitable to support the development process in an industrial environment. An advantage obtained from the development of these formal specifications will be the possibility to reason about their properties to check whether usability and safety requirements are satisfied.

This deliverable deal with part of work produced in the Work Package 2. More precisely, this part of work concerns formal specification of interactive systems. This deliverable describes a formal specification technique dedicated to the formal specification of interactive systems and its application to an Air Traffic Control en-route case study that has been selected in Mefisto project.

The deliverable is split into three documents:

- Deliv4/1 that corresponds top the working paper WP 2.6. This document presents the exhaustive formal definition of the Interactive Cooperative Objects (ICO) formal specification technique. It encompasses the presentation of several formal specification techniques grounding the ICO formalism. As ICOs can be seen as being at the top of a pyramid of formal specification techniques, we represent here the evolution from basic Petri nets to ICOs through the presentation of Object Petri nets and Cooperative Objects. A small but complete application is then used for exemplifying the various concepts and notations used in the first parts of the document.
- Deliv4/2 that corresponds top the working paper WP 2.4. This document presents the use of the ICO formalism on the Druides application. The Druides application is a prototype for en-route air traffic control featuring data-link communications facilities.

  The aim of Deliv4/2 is threefold:

  - To prove the ability of the formalism to describe behaviour of graphical and dynamic interactive applications,
  - to prove the ability of the formalism to cope with large scale application,
  - to define and apply structuring mechanisms for large specifications.
- Deliv 4/3 that corresponds top the working paper WP 2.5. This document presents the use of the Interactive Cooperative Objects formalism for the specification of the touch screen of Middles Air Traffic Control prototype. The formalism is used as presented in Deliv4/1. As this specification is

complementary to the one of Druides in Deliv 4/2 we often refer to this former specification while presenting Middles functionalities. Middles introduces new features compared to Druides. In particular, it introduces a touch screen called touch spots screen. In this section we present a part of the touch screen specification, in which all the specificities are taken into account. However, in order to make the document simpler and easier to read the complete data link handling and the notion of delayed clearances are not described. In some cases, we add some screen shots extracted from the tool prototyped by CENA to illustrate parts of the rendering.

2 Deliv 4/1: The ICO formal specification technique

This document presents the exhaustive formal definition of the Interactive Cooperative Objects (ICO) formal specification technique. It encompasses the presentation of several formal specification techniques at the basis of the ICO formalism. As ICOs can be seen as being at the top of a pyramid of formal specification techniques, we represent here the evolution from basic Petri nets to ICOs.

This document can be used in different ways:

- As a reference document for the formalism by every person interested in the use of the formalism for the specification of interactive applications,
- As a reference document for people knowledgeable in the field of Petri nets and that would like to understand the underpinning semantics of the ICO formalism.

All the sections of this document follow the same structure. First we present and informal definition of the notation used, then the formal definition is given. This structuring aims at allowing people without a strong background in formal methods to understand the concepts.

The document is structured as follows. Section 1 introduces the basic notions of Petri nets. First the syntax is presented, the its associated semantics is introduced. Section 2 presents the concepts of Objects Petri nets. These concepts are introduced making references to basic Petri nets introduced in the section 3. Section 4 introduces the Cooperative Objects formalism that is based on the Objects Petri nets. Section 5 presents the ICO formalism dedicated to the formal specification of interactive applications. Lastly, section 6 presents a complete example of the use of the ICO formalism on a simple application.

3 Deliv 4/2: Formal Specification of the DRUIDES prototype

This document presents the use of the ICO formalism on the Druides application. The Druides application is a prototype for en-route air traffic control featuring data-link communications facilities. The case study has been provided by CENA and the gathering of information has been performed through various kinds of media:

- the information contained in the WP1-3 describing the case study,
- the video tape which presents the application,
- the reengineering of the prototype.

The aim of this document is threefold:

- To prove the ability of the formalism to describe behaviour of graphical and dynamic interactive applications,
- To prove the ability of the formalism to cope with large scale application,
- To define and apply structuring mechanisms for large specifications.

The use of the formalism follows its formal definition presented in Deliv 4/1.

The document is structured as follow. After a short introduction in section 1, section 2 presents in an informal way the Druides application as well as the structure that has been chosen for the specification. Section 3 presents the specification itself. This section follows step by step the structuring introduced in section 2. Last section (section 4) presents two executions of the specification. One is dedicated to a non-modal interaction while the other one shows how modal interaction is used in one case in the Druides case study and how it has been specified using the ICO formal specification technique.

Druides, as it is a radar screen, allows controllers to handle planes in a graphical way. Using the ICO formalism we describe in Deliv 4/2 most of its features. Indeed, all the possible clearances that can be built using Druides are described in the specification. The data link menu (i.e. how to send data-link requests to planes) is not describe as it is a set of popup menus and submenus, and except the hugeness of its description, it does not present any difficulty to model.

4 Deliv 4/3: Specification of Middles Touch Screen using Interactive Coopertive Objects

This document presents the use of the Interactive Cooperative Objects formalism for the specification of the touch screen of Middles Air Traffic Control case study. The formalism is used as presented in Deliv4/1 that describes the semantics and the use of the formalism. As this specification is complementary to the one of Druides in Deliv 4/2 we often refer to this former specification while presenting Middles functionalities.

Middles introduces new features compared to Druides. In particular, it introduces a touch screen called *touch spots screen*. In the first section of the document we present a part of the touch screen specification, in which all the specificities are taken into account. However, in order to make the document simpler and easier to read the complete data link handling and the notion of delayed clearances are not described. In some cases, we have added some screen shots extracted from the tool prototyped by CENA to illustrate parts of the rendering.

5 Conclusions and future works

This deliverables has presented a new formal specification technique devoted to the specification of real-size interactive systems. This specification technique has been applied to two different case studies in the field of Air Traffic Control.

This deliverable is meant to be read and used as a reference document for the formalism and of its use on real applications.

Future work (that has already started) is twofold:

- The definition and development of tools for supporting the development process of the specifications. These tools will provide support to designer by making easier the edition of the specifications, their inclusion in documents, their modifiability and their use in later phases of the development process such as implementation and testing.
- The definition and development of tools supporting the validation and verification phases of the development process using formal specification techniques. To this end links with formalism used for the description of properties has to be accomplished.

6 The definition of the relations and bridges between formal tasks modelling (see Deliverable 3) and the formal specification techniques. These bridges will allow cross verification, providing thus a coherent cement between usually unrelated views of a same real world.