MATISSE: Methodologies and Technologies for Industrial Strength Systems Engineering

IST-1999-11435

MATISSE Handbook

Board-level Storyboard

MATISSE/D10a/1.3

February 2003

Project Information

Project Number	IST-1999-11435
Project Title	Methodologies and Technologies for Industrial Strength Systems Engineering (MATISSE)
Website	www.matisse.qinetiq.com
Partners	Qinetiq -AC
	Centre National de la Recherche Scientifique -SC
	Aabo Akademi University
	Gemplus
	Siemens Transportation Systems
	University of Southampton
	ClearSy

Document Information

Document Title	MATISSE Handbook, Board-level Storyboard
Workpackage	WP1
Document number	D10 (Part A)
Lead Partner	ClearSy
Editor	Thierry Lecomte
Contributors	All Matisse Partners

Version 1.0	initial version
Version 1.3	Comments from partners taken into account

List of Contents

1 Introduction

The core objective of the MATISSE project is the development of industrial-strength methodologies and associated technologies for the engineering of software-based critical systems. These methodologies and technologies will support industry in providing essential services that are highly dependable and therefore lead to increased public confidence and trust in the services.

This document briefly describes the benefits of using the MATISSE methodology and what are its impact on the organisation structure. Data presented in this handbook was obtained from the experience gained in developing the project case studies and from external projects using / extending techniques and methods elaborated in parallel.

2 The MATISSE approach

Over the last 30 years, computer scientists have been developing and advocating the use of rigorous mathematically-based software engineering techniques, so-called *formal methods* http://www.fmnet.info/, that support validation throughout the development life-cycle by providing rigorous specification and design notations as well as proof techniques, model-checking techniques and simulation techniques. Formal methods also allow the complexity of systems to be dealt with through abstraction and modularity. Despite this, the use of formal methods is not widespread in the industry because of various managerial, sociological and technological barriers. One of the major objective of the MATISSE project is to overcome some of these barriers by:

- providing methodologies and associated technologies that are integrated with standard working practices;
- providing further evidence through well-founded evaluation plans that the use of formal methods is cost effective;
- showing how formal methods can help ensure that products and services meet appropriate standards for safety, security and reliability.

3 Keys to success

This chapter draws up an outline of the benefits that are induced by the use of the MATISSE methodology, combining formal methods and existing industrial (best) practices.

3.1 Product quality

The MATISSE methodology enables the development of systems **correct by construction**

by proposing a refinement-oriented approach as a basis for critical system design. Starting from an abstract specification, the system is stepwise refined into a more concrete and deterministic system, leading to a final proved implementation. This constructive approach has been successfully and extensively used by the partners for all the three case studies proposed in the project and also in other application areas (e.g telecommunication network protocols, adaptive routers). The methodology for systems construction by refinement does not rely on a pre-conceived notion of how an implementation may be constructed from a given specification and specific refinement transformation functions.

The MATISSE methodology allows one to obtain **clear requirements** and **specifications**

The main principles to be used for a B development are: to concentrate efforts on the initial phases of development in order to be "as precise as possible, as early as possible", then to make best use of proofs to ensure the initial aims are adhered to. A formal development[1] puts the stress on the specification phase, which is usually longer but leads to documents that are self-sufficient, clear and will not be subject to error-based modifications. Producing quasi-final documents for the first shot reduces the delay of acceptance and allows one to minimise the overriding of two successive phases. Moreover, the delivery of high quality documents would have a positive impact on the final customer and would increase his confidence on the ability of ones organisation to provide good products in time.

The use of formal methods can be restricted to the writing of the documents (statement of work, specification, preliminary design, detailed design), providing a good technical basis for the rest of the project and ensuring a suitable communication among the different partners involved in the development, especially in the case of sub-contractors.

[1] By development, we mean: writing of the specification document, design and code generation.

3.2 Cost/benefit issues

The MATISSE methodology **does not imply** a significant **overhead**

when compared with conventional development, if a dedicated methodology has been previously experimented and adapted to manufacturer's needs. Developing a product using formal methods is comparable, in terms of cost, with developing a safety critical product, as heavy verifications have to be performed alongside the ordinary development process. The MATISSE methodology is model-based, so for similar products[2], the related models may be reused from one product to another with only slight modifications.

In the case of a software development:

- no unit test is required (apart basic machines testing), since proof ensures that every piece of code complies with its specification;
- no functional validation test is required, as proof ensures that top-level properties hold. Nevertheless, tractability between software requirements and abstract model should be manually verified.

3.3 Regulation compliance

The MATISSE methodology allows the development of regulatory compliant equipment.

The use of formal methods is recommended, even highly recommended, when building safety or security-related products, for example EAL7 for information systems and SIL4[3] for railway systems [4], automotive, chemical systems [3], etc.

Certification[4] is eased because:

- Formalism helps one to think about the system and its properties. Formal proof allows one to verify that the behaviour of the system is correct in all the cases, not only in those one has in mind. So bad surprises are unlikely to occur during evaluation and multiple iterations are prevented
- Formal justification of the design choices allow the evaluators to come more quickly to a conclusion, as they do not need to informally prove them. The number of questions is minimised and the duration of the evaluation process is reduced.

[2] Product line for example.

[3] Safety Integrity Level: range 0 to 4, where 4 is the highest level. The Mean Time To Failure of a SIL4 product is about 100 000 years.

[4] Verification of the conformance of a product with its referential.

- The MATISSE methodology is model-based, so for similar products[5], the related models may be reused from one product to an other with slight modifications. In this case, differential evaluation of those models can be performed at minimal cost, as the impact of those modifications can be easily computed and formally verified.

3.4 Competition

The MATISSE methodology helps to maintain competitiveness.

Formal methods are not required by the market, as most of the time, final consumers are not aware of the use/embedding of such methods: application fields are mainly driven by cost reduction. However, depending on the constraints of each domain, the use of formal methods may be positively considered by regulation authorities, for example:

- in the railway domain, most competitors have integrated formal methods into their development process (B at Siemens Transportation Systems and Alstom Transportation, SCADE at CSEE, SDL at RATP, etc.), as safety issues are now of paramount importance.

- in the smartcard domain, many competitors (like Gemplus and Schlumberger) have investigated the use of formal methods (B, coq, PVS, etc.). Their common objective is the building of highest security level products (up to EAL7), when required by banking organisations.

3.5 Teams

The MATISSE methodology does not require development teams to be changed.

Setting up a formal methods activity does not require the complete modification of the existing structure. Functional experts (ako local gurus) need to be inserted into this structure, to advise project leaders, from a strategic point of view (metrics, identification of technological locks, …), and practitioners, from a tactical point of view (modelling, proof, …). Such experts would have at least one year experience in using formal methods. Light training (up to three weeks), immediately followed by full-time practice, is sufficient to have a junior practitioner in a formal methods project. External consultants could provide assistance on some particular aspects of the development (modelling, proof, etc.).

As formal development life cycles are similar to non-formal ones, current management teams need to be lightly trained in order to understand the vocabulary and gain some insights into the specific aspects of formal projects.

[5] Product line for example.

3.6 Technology

The MATISSE methodology comes along with existing, mature tools.

Atelier B [5] and FDR [2] tools, supporting the MATISSE methodology, have been applied on industrial case-studies, up to 100,000 lines for the former. The automatic prover of Atelier B has been designed to demonstrate one proof obligation in 10 seconds or less (mean time), allowing one to prove an industrial-size project in less than one day of computation. Training sessions and support are available for both Atelier B and FDR.

References

1. The B Book: *Assigning programs to meanings*, Abrial, 1996, Prentice-Hall
2. FDR user manual, 1997, Formal Systems (Europe) Ltd
3. IEC 61508-2 : *Dependability – Safety – Prescriptions for programmable electronic systems*
4. EN 50129 : *electronic safety critical signalling systems*
5. Stéria Méditerranée. *Atelier B*. France, 1996.