



Your Connection to ICT Research

High-level guidance for Managers Deploying Formal Methods in their Organization

Christophe Ponsard
Jean-Christophe Deprez
Renaud De Landtsheer

FEDER



UNION EUROPEENNE



Wallonie



LE FONDS EUROPEEN DE DEVELOPPEMENT REGIONAL
ET LA WALLONIE INVESTISSENT DANS VOTRE AVENIR.



- Formal methods are great!
 - Technically speaking
- Some industrials have tried, with various success
 - Difficulties not always related to the FM mechanics
- Need to look at how to deploy FM in industry, from an industrial point of view
 - Considering the concrete question of an industrial
- Our contribution: a repository
 - Industry-relevant evidences on FM
 - collected and consolidated throughout Deploy FP7
 - Try to capture the variety of industrial concerns

- A repository of evidence on the deployment of FM in industry
 - Context: the Deploy project
 - Identifying industry-relevant evidences
 - Collecting evidences from deployment stories
- Examining one evidence
 - Impact of FM on a development process
- Related work
- Conclusion

- Ten industrial partners performing FM deployment
SAP, Bosch, Space System Finland, Siemens SAS IMO, XMOS, Critical Software Technologies, AeS Brasil
- Seven major industrial domains where covered:
Aeronautics, Automotive, Business Information Systems, Chip Design/Smartcards, Operating Systems, Space Systems and Mass Transport
- Various FM techniques
Test generation, Proof, model-checking, automated proof, similarity checking, etc.
- 14 deployments observed in Deploy

Identifying relevant roles / viewpoint in industry

- High-Level Managers
 - taking enterprise's strategic decisions and their financial impact
- Project and QA Managers
 - supervising people who actively use FM (in production or R&D), planning projects and performing safety analysis and more traditional QA activities
- Engineers and Analysts
 - People actively using formal methods and tools
- QA Practitioners and safety engineers
 - people who must understand documents involving FM notations but don't need to develop the capabilities to produce them

Identifying high-level topics

- General topics: what are FM?
- Training Scope and Resourcing
- Impact on the Software/System Development Process
 - Impact on quality of product
 - FM at various stage of the development process
 - Impact of introducing a formal method in a process
 - Reuse
 - Migration to FM
- Strengths and weaknesses of tools and tool providers
- External factors : competition, standard bodies, laws


- Filling the topic-role matrix with relevant questions
 - Eg: training – high level managers
 - What is the cost or effort needed to train engineers/analysts to use a new formalism?
- Or answer the same questions under all viewpoints
 - Eg: what is the impact on the process and people involved
- 26 questions answered over 55 identified


← → http://www.fm4industry.org/index.php/Deploying_Event-B_in_a Deploying Event-B in an In...

Fichier Edition Affichage Favoris Outils ?

Google Sites suggérés Accéder à plus de mo...

Log in / create account



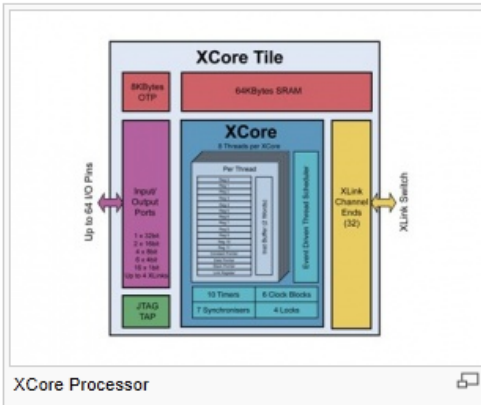
powered by


Page Discussion Read View source View history Go Search

Deploying Event-B in an Industrial Microprocessor Development

[Main](#) -> [DEPLOY Success Stories](#) -> [Micro-electronics#2](#)

Short Description



XCore Processor

The Instruction Set Architecture is a key document for the design of a microprocessor. It is very important to have accurate specification of this because it is the primary reference source for engineers and computer scientists developing and optimizing the compiler tools. Third parties might also want to write their own implementation for microprocessors not licenced with a proprietary micro-architecture. Specification errors can be very subtle and not reveal themselves immediately but many cycles later, so ensuring the quality of such a document is quite a challenge.

The objective of XMOS was to achieve a rigorous review of the natural language specification of the instruction set architecture (ISA) of their XCore processor. XMOS decided to join the DEPLOY Associate program to evaluate how formal modelling and verification could help to provide a high level of quality of their ISA specification. The objective of the project was to see how well Event-B and the Rodin toolset could help producing a rigorous restatement of the XMOS's existing specification, especially to identify errors and omissions.

The project was successful in producing a fully formalised and proved specification. It required some Rodin tools extension to get the right tooling support. In addition the formal model could also be used to generate a reference VM simulator of the ISA to run test suites.

Success Story

Domain CPU

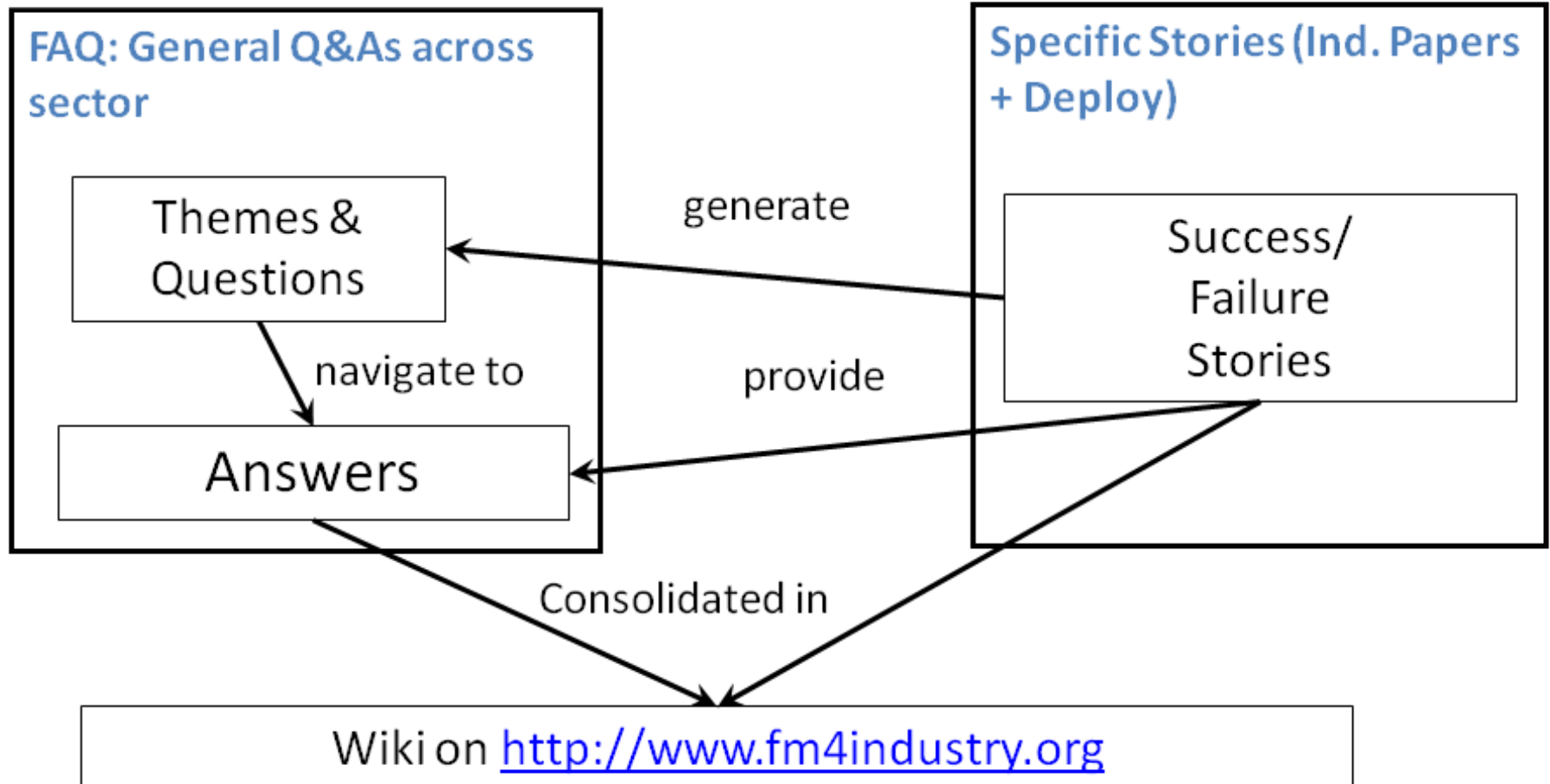
Keywords EventB, micro-electronic circuit, instruction set architecture

Source [XMOS](#)

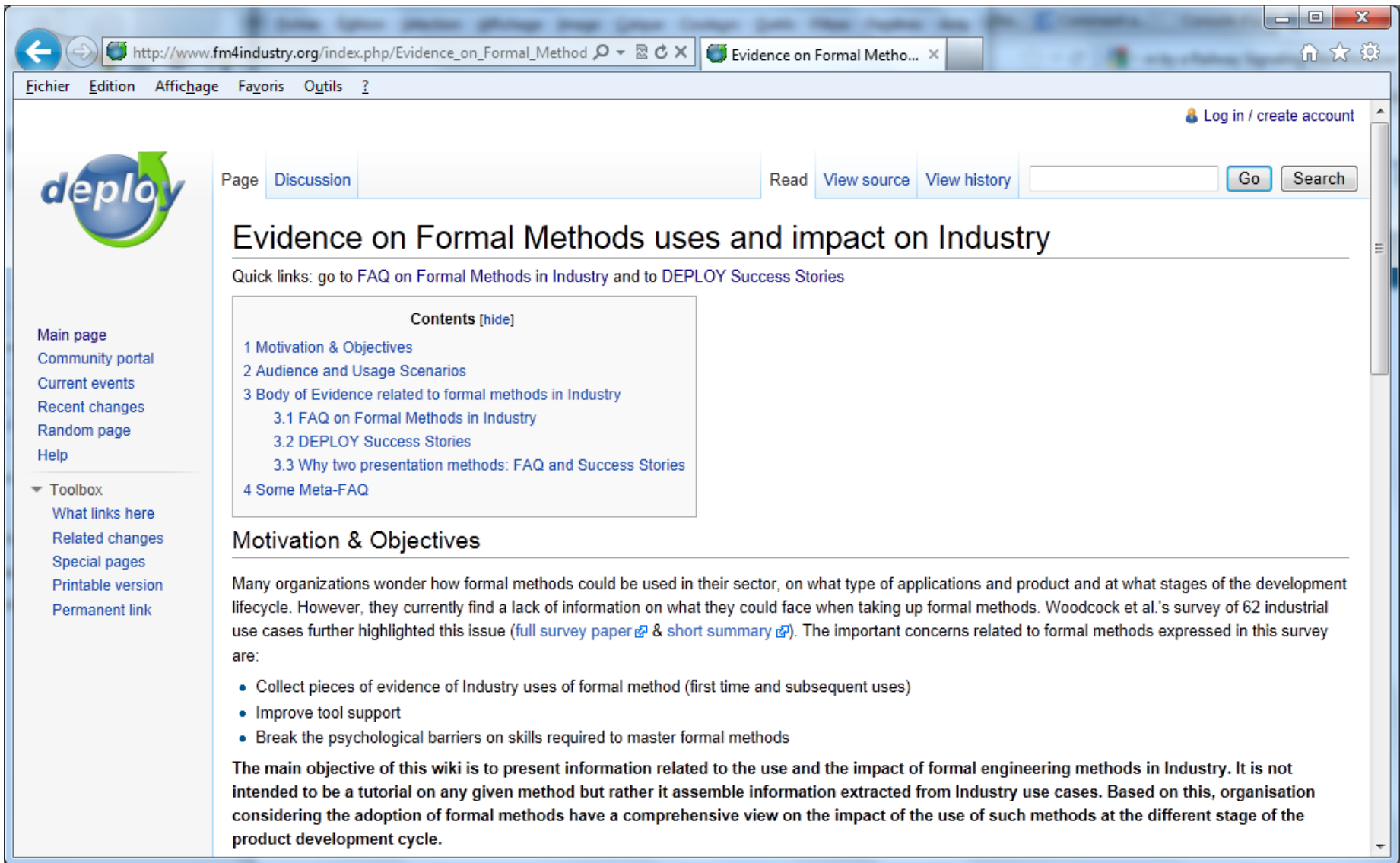
Related FAQ

of Interest to Project and QA Managers

[What is the best way to use formal verification methods to help in the identification of errors at each phase of development tasks?](#)



14 success stories reported in the repository



The screenshot shows a web browser window with the URL http://www.fm4industry.org/index.php/Evidence_on_Forma.... The browser's address bar and navigation buttons are visible. The page content includes a navigation menu with options like 'Eichier', 'Edition', 'Affichage', 'Favoris', and 'Outils'. A 'Log in / create account' link is in the top right. The main content area features a 'deploy' logo, a 'Page Discussion' tab, and a search bar. The title of the page is 'Evidence on Formal Methods uses and impact on Industry'. Below the title, there are quick links to 'FAQ on Formal Methods in Industry' and 'DEPLOY Success Stories'. A 'Contents [hide]' section lists the following items:

- 1 Motivation & Objectives
- 2 Audience and Usage Scenarios
- 3 Body of Evidence related to formal methods in Industry
 - 3.1 FAQ on Formal Methods in Industry
 - 3.2 DEPLOY Success Stories
 - 3.3 Why two presentation methods: FAQ and Success Stories
- 4 Some Meta-FAQ

The 'Motivation & Objectives' section contains the following text:

Many organizations wonder how formal methods could be used in their sector, on what type of applications and product and at what stages of the development lifecycle. However, they currently find a lack of information on what they could face when taking up formal methods. Woodcock et al.'s survey of 62 industrial use cases further highlighted this issue ([full survey paper](#) & [short summary](#)). The important concerns related to formal methods expressed in this survey are:

- Collect pieces of evidence of Industry uses of formal method (first time and subsequent uses)
- Improve tool support
- Break the psychological barriers on skills required to master formal methods

The main objective of this wiki is to present information related to the use and the impact of formal engineering methods in Industry. It is not intended to be a tutorial on any given method but rather it assemble information extracted from Industry use cases. Based on this, organisation considering the adoption of formal methods have a comprehensive view on the impact of the use of such methods at the different stage of the product development cycle.

High-Level Managers

- FM dramatically shifts the workload of a project From late testing to earlier analysis phase
 - because you need to develop a model
- So:
 - Identify adequate workload and progress metrics to estimate costs and deviations of projects using FM
 - Adapt the go/no-go procedure of projects to this new technique
- Danger of early red flagging of project as being over schedule, and indirectly make it augment this deviation due to increased reporting requests from managers.

Project and QA Managers need to properly design the development process and select the most adequate FM such that:

- Claims proven using a formal method are relevant
- The artifact on which a claim is proven is the most adequate one
- Abstractions made to produce a model are verified and valid
- The level of assurance that is delivered by the provers is adequate (soundness, vacuity)
- The formal method is compliant with the targeted standard


Engineers and Analysts

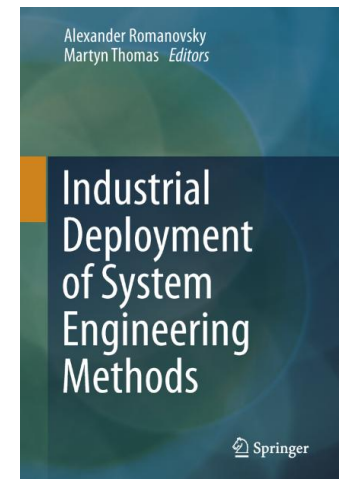
need to

- Develop formal artifacts
- Formally define all the claims to be proven
 - From requirements
 - From standard rules eg: programming rules
- Prove the claims on the artifact
- Exploit the model in the next steps of the development process
 - Eg: code generation
 - Eg: tests oracle / generation.

QA and Safety Engineers need to assess that:

- Proven claims are relevant and have an adequate level of abstraction
- The formal methods have been used in an adequate way. (e.g.: no vacuity)
- (Optional) The model is structured in a way to ease proofs, e.g.: reach a high level of automation

- Evidence repository
 - Built from  experience
 - 10 organizations, of various size, culture
- Addresses concrete industrial-minded questions on FM
- Very difficult to access such info
 - Related to internal process, quality, etc.
- Repository
 - <http://www.fm4industry.org>
 - Chapter in "Industrial deployment of system engineering methods providing high dependability and productivity", A. Romanovsky, M. Thomas (Eds), Springer. April 2013.



- Major success stories in the literature:
 - METEOR [3], Estelle for communication protocols [11], the Mars rover [6], OS driver verification [2] or RTOS design[23], book digests [13, 21]
 - We take a cross-cutting view
- Survey, myth and lesson learned, good practices [16, 14, 5]
 - only give essential Information, and not link it with concrete success stories as proposed in our wiki, and focuses on salient points
- Virtual library of Bowen [4]
 - resources such as formal notations, tools, projects, who's who
- International surveys are also carried out regularly [9, 24].
 - good snapshot of FM adoption, and major barriers/drivers
 - We tried to identify what kind of issues should be better explained, for example the training phase,
 - We tried to take into account all the impacted aspects of a development, e.g. the position of certification w.r.t. the use of FM.

2. Thomas Ball, Byron Cook, Vladimir Levin, and Sriram K. Rajamani, Slam and static driver verifier: Technology transfer of formal methods inside microsoft, In: IFM. (2004, Springer, 2004, pp. 1{20.
3. Patrick Behm, Paul Benoit, Alain Faivre, and Jean marc Meynadier, METEOR : A successful application of B in a large project, In [Wing et al, 1999, pp. 369{387.
4. Jonathan Bowen, Formal Methods Wiki, <http://formalmethods.wikia.com>.
5. Jonathan P. Bowen and Michael G. Hinchey, Ten commandments of formal methods, IEEE Computer 28 (1995), no. 4, 56{63.
6. Guillaume Brat, Doron Drusinsky, Dimitra Giannakopoulou, Allen Goldberg, Klaus Havelund, Mike Lowry, Corina Pasareanu, Arnaud Venet, Willem Visser, and Rich Washington, Experimental evaluation of verification and validation tools on martian rover software, Form. Methods Syst. Des. 25 (2004), no. 2-3, 167{198.
9. Dan Craigen, Susan L. Gerhart, and Ted Ralston, An international survey of industrial applications of formal methods, Z User Workshop, 1992, pp. 1{5.
11. Mariusz A. Fecko, Paul D. Amer, Adarshpal S. Sethi, M. Umit Uyar, Ted Dzik, Raymond Menell, and Mike McMahon, A success story of formal description techniques: Estelle specification and test generation for mil-std 188-220, in FDTs in Practice, 2000, pp. 1196{1213.
13. S. Gnesi and T. Margaria, Formal methods for industrial critical systems: A survey of applications. first edition., John Wiley & Sons, Inc., 2012.
14. Anthony Hall, Seven myths of formal methods, IEEE Softw. 7 (1990), no. 5, 11{19.
16. Peter Gorm Larsen, Odense M, John S. Fitzgerald, and Tom Brookes, Lessons learned from applying formal specification in industry, IEEE Software (1995).
21. A. Romanovsky and M. Thomas, Industrial deployment of system engineering methods, Springer-Verlag New York Incorporated, June 2013.
23. Eric Verhulst, Gjalt G. de Jong, and Vitaliy Mezhyuev, An industrial case: Pitfalls and benefits of applying formal methods to the development of a network-centric rtos, FM (Jorge Cuellar, T. S. E. Maibaum, and Kaisa Sere, eds.), Lecture Notes in Computer Science, vol. 5014, Springer, 2008, pp. 411{418.
24. Jim Woodcock, Peter Gorm Larsen, Juan Bicarregui, and John S. Fitzgerald, Formal methods: Practice and experience, ACM Comput. Surv. 41 (2009), no. 4.



*Thank you
Merci*



Aéropôle de Charleroi-Gosselies
Rue des Frères Wright, 29/3
B-6041 Gosselies
info@cetic.be

www.cetic.be

