An Evidence Repository of Formal Methods for Industry

Deploy Federated Event – Fontainebleau – March 1st 2012

Jean-Christophe Deprez
Christophe Ponsard
Renaud De Landtsheer
CETIC - Belgium

Motivation

ACM Survey by Woodcock, Larsen, Bicarregui and Fitzgerald's (62 FM Industry Projects):

- **Collection of FM Evidence in Industry**
- Tooling Support
- Subsequent Usage of FM
- Psychological Barrier and Skills Req. (Inhibitors)

Collection of FM Evidence can also address last 3 points

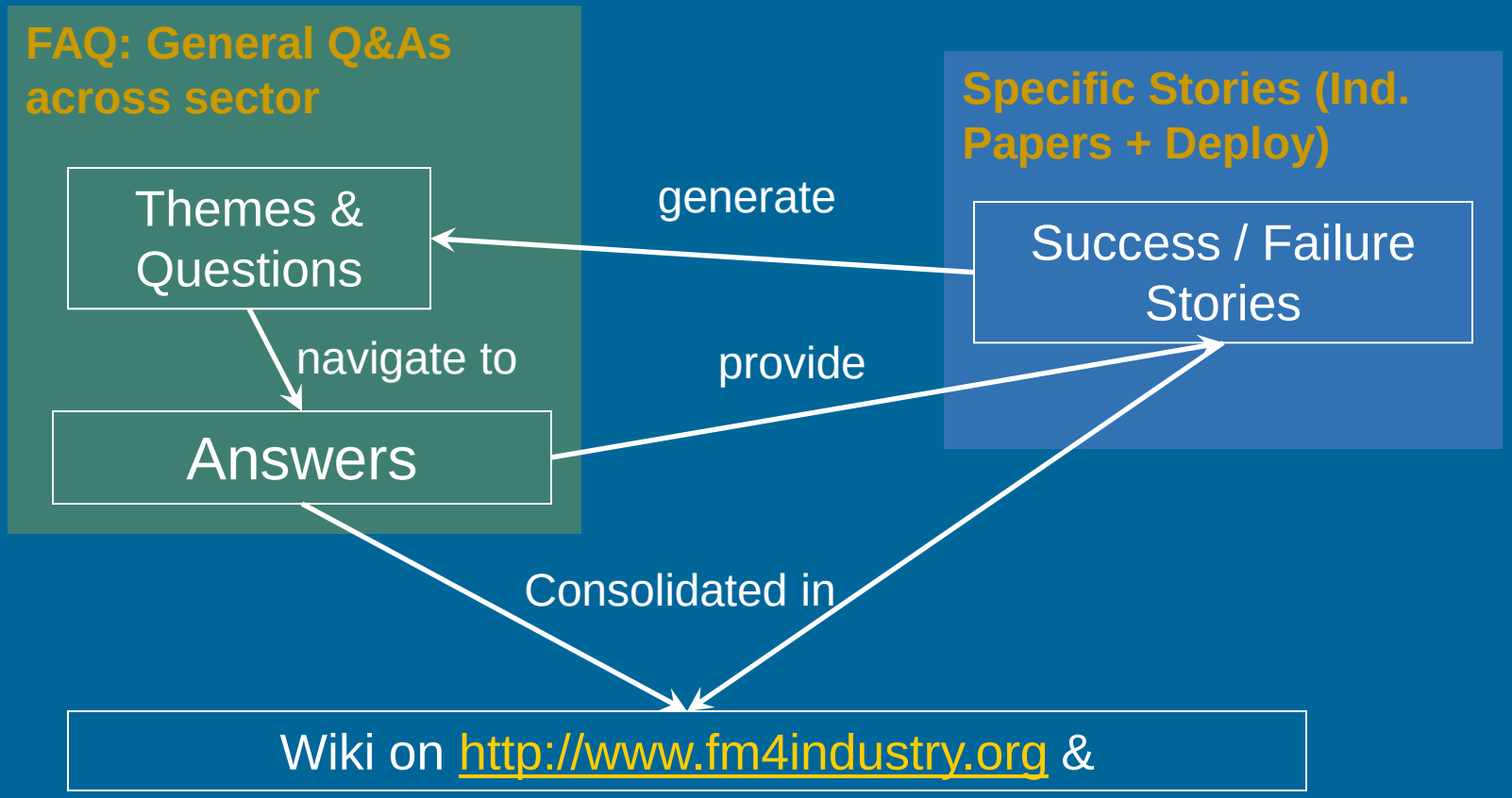
What about Case Study Articles

- Great First Step

But

- Focus on application of
  1 FM in 1 particular Industry case
- Usually Hard to understand how to integrate
  - with other FM approaches
  - In other Industry cases

Capturing & Presenting Pieces of Evidence



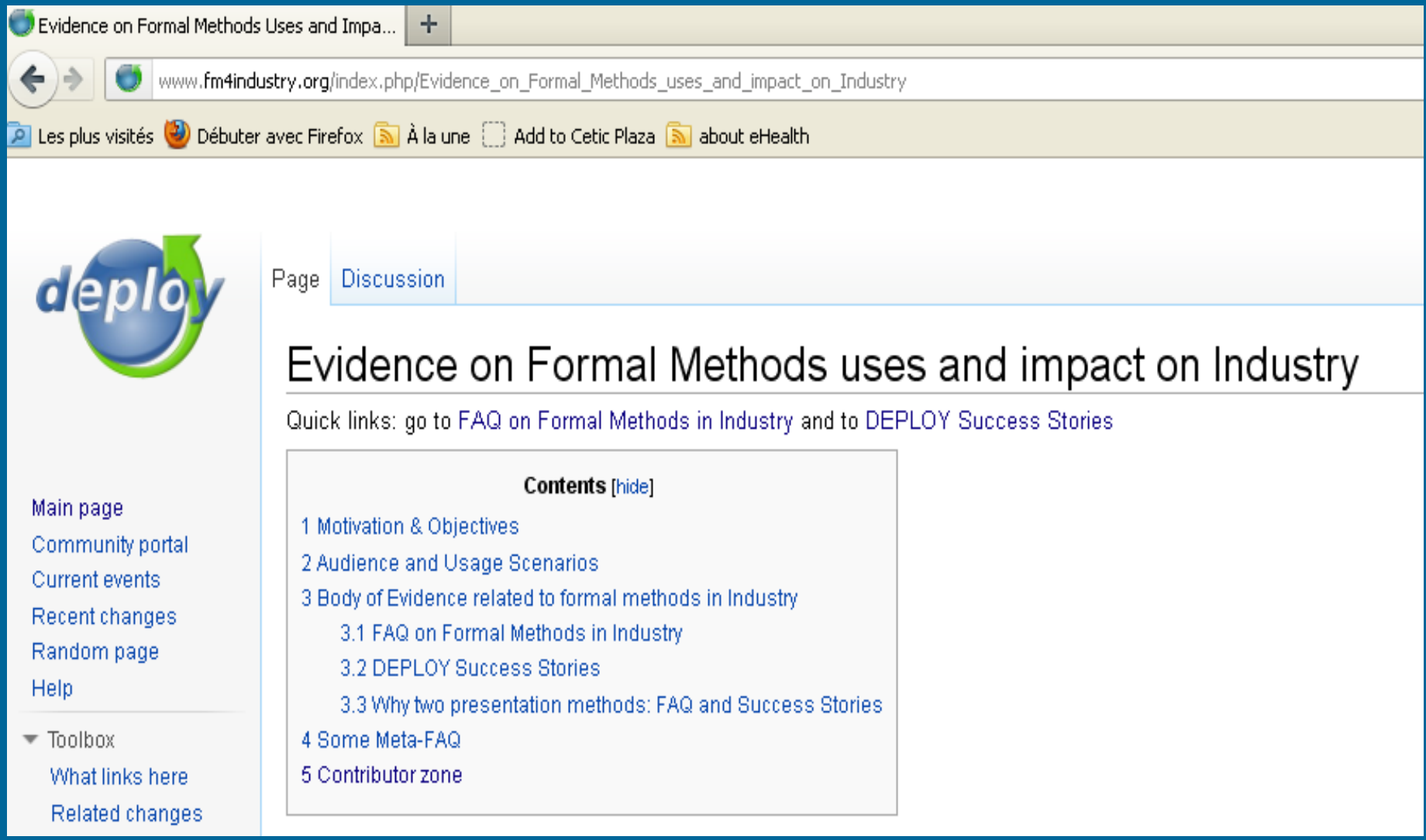
http://www.fm4industry.org is open for external contribution. See how later in talk

Themes

- Impact on an organisation with regards to **training scope and resourcing**
- Understanding the impact on the *Software/System Development Process*
  - The impact on the **quality of a product developed using formal methods**,
  - The capability to **exploit formal models** at various stages of the development process,
  - The capability to perform **reuse across development projects** when formal methods are used, including reuse of formal and proven artefacts
  - The capability to **phase the learning** of a formal method in an organisation and eventually to **limit the scope of who** must understand and become an expert in a formal method
  - The capability to **phase the migration** to using a formal method (given the existence of products not initially developed using formal methods)
- **Known strengths and weaknesses of tools** associated to a formal method as well as the **quality of support by tool providers**
- **External factors advocating take-up** (from competition, standard bodies, laws) of formal methods
- **General topics of concerns related to formal methods in Industry**

Role Breakdown (for classifying questions)

- **High-Level Managers**: enterprise's strategic decisions and their financial impact
- **Project and QA Managers**: Managers of people who actively use FM (in prod or R&D)
- **Engineers and Analysts**: People who will actively use FM
- **QA Practitioners**: people who review and use documents expressed using FEM notation


Evidence on Formal Methods Uses and Impa...
www.fm4industry.org/index.php/Evidence_on_Formal_Methods_uses_and_impact_on_Industry
Les plus visités
Débuter avec Firefox
À la une
Add to Cetic Plaza
about eHealth
deploy
Page
Discussion
Evidence on Formal Methods uses and impact on Industry
Quick links: go to FAQ on Formal Methods in Industry and to DEPLOY Success Stories
Contents [hide]
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
5 Contributor zone
Main page
Community portal
Current events
Recent changes
Random page
Help
Toolbox
What links here
Related changes

Talk:Evidence on Formal Methods uses and impact on Industry

Main page
Community portal
Current events
Recent changes
Random page
Help

Toolbox
What links here
Related changes
Atom
Special pages
Printable version
Permanent link

Search terms: Search Sorting order: last modified first Go

Contents

Thread title	Replies	Last modified
Add usage scenario	0	08:56, 5 February 2012
Other dimension of the success story classification	0	01:01, 5 February 2012
Idea: add a glossary	1	13:51, 10 December 2011

Add usage scenario

Usage scenario from the DEPLOY book chapter

Cponsard 08:56, 5 February 2012

Other dimension of the success story classification

JC suggests to also report by "FM tools and tool providers" Some good candidates: Systerel (rodin), ClearSy (atelier b), Sparx Systems (just look at the tools)

Actually we had it on the private wiki: 'Success Stories by FAQ Themes' and Tools is a dimension of the classification

Cponsard 00:33, 5 February 2012

Answering FAQs (with Deploy success stories)

- SSF → Training Scope and Resourcing
  - Training people with no FM background
- SAP → Control Impact of Formalism
  - Hiding FM behind a domain specific notation
- Siemens → External Factor – Certification
  - Qualification of FM Tool used in dev. Process for IEC-50128
- Bosch → Exploiting models
  - Problem Frames to bridge informal requirements and formal models

SSF → Training Scope and Resourcing

What is a reasonable rate of progression when learning a new formalism (depending on whether one has previous experience with formal methods or not)?

Training People With No FM Background

- Guiding Hypotheses
  - For developers and analysts with no background in Formal Modelling, a training programme and/or individual coaching needed to become autonomous with Event-B modelling and proofing takes about XXX months and requires YY% of effort (per engineer) over that period.
- Answer from SSF
  - SSF trained **a senior engineer and a junior programmer** with no Formal Modelling background
  - Training = **3-day training** with Prof. expert in Event-B given + Independent Learning with **access to SSF internal expert**
  - Training Lasted **2 to 4 Months.** Both trainees practices by solving exercises similar to Zurich Introductory Block Course spending between **25% and 50% of their time**

NOTE: None of these exercised required manual proofs (all proof obligations for these simple exercises can be solved automatically)

Siemens → External Factor – Certification

- **What is the position of standards regarding formal methods in my industry segment?**

- **Answer for railway/metro lines (Siemens)**
  - IEC-50126/128 /129 series, derived from EN-61508 (defining SIL levels)
  - Software in **IEC-50128**
    - Mentions **Formal Methods/Proofs as relevant technique/measure for data preparation techniques**
    - **“Recommended" for SIL levels 1 and 2**
    - **"Highly Recommended" for SIL levels 3 and 4**
  - **Barrier of the “well-established recommended practices”** (e.g. testing)
    - Consequent work for 1st time certification (e.g. B for metro lines)
    - After Can become an established practice
  - On-going revision (2011) : tool classes and associated requirements
    => Siemens involved in qualifying their data validation tool + the standardisation working group

- **Related success stories: ProB efficiency for data verification (published) and qualification process for production (on-going)**

SAP → Control Impact of Formalism

- **Can the use of a formal method be hidden from most of development and management teams except to a few selected experts who will use it (perhaps even without other team members knowing)?**

- **Answer:**
  - Some facts:
    - Domain Specific Language are quite adopted (e.g. VHDL, BPMN...)
    - Many **DSL are only semi-formal** (meta-model based) and lack formal semantics
  - **Combining DSL and FM** is beneficial because:
    - FM give/demand a precise semantic to/from DSL, **enabling reasoning and verification** using available formal tools
    - Empower current DSL users **without need to train** to the underlying FM
  - Requires to develop mapping between DSL and FM *and back*

- **Related success story**: Adoption Eased by Using Formal Models behind Domain Specific Notations (published paper)
  - Show how SAP could translate BPMN-like notation in Event-B, perform checks and provide explanations

Status in Evidence Collection (# from Private wiki)

	Total	Done	ToDo
# of FAQ themes	9	9	?
# of role-based FAQ	52	17	8
# of success/failure stories	11	9	2
# of working hypothesis identified	*101*		
# of working hypothesis of interest	*59*		

13 FAQ and 9 success stories migrated to http://ww.fm4industry.org

? = open for discussion

A few Authors and Tools mentioned

- Leuschel (Train)
- Heitmeyer (Nuclear)
- Drusinsky (Mars Rover)
- Ferrari (Metro)
- Woodcock (Survey)
- Wheeler (Tools)
- …

- Rodin
- ProB
- AtelierB
- NUSMV
- Polyspace
- SCR
- …

Have you done Industry Case Studies?

If so, check if we cite your work or tool in our evidence repository. If not, let us know.

Why, What, How to contribute

Why?

- To easily gain leverage

→ Share Results with Industry Players

→ Guide Future Research

→ Compare/Contrast with Similar Effort

What?

- Submit comment on public FAQ
  - Point to missing info
  - Write new segment of answers
- Suggest new FAQ or new structure of answers
- Submit new success/failure stories
- Join the internal editorial board (after Deploy)

visit http://www.fm4industry.org

Remaining Issues

- Raise interest from readers with different level of expertise
- Capture feedback from Industry readers
- (near) Self-sustaining FM evidence repository
- Controlled Editing by an Editorial Board
- Close Integration with “ACM Surveys”

Last 2 points → Discussed with FME

Visit http://www.fm4industry.org

Deploy Federated Event – Fontainebleau
March 1st 2012

Jean-Christophe.Deprez@cetic.be
Christophe.Ponsard@cetic.be
Renaud.DeLandtsheer@cetic.be
CETIC - Belgium