A Model-Based Testing Process for Enhancing Structural Coverage in Functional Testing

Yanjun Sun, Gérard Memmi and Sylvie Vignes

CNRS LTCI, Télécom ParisTech, Université Paris-Saclay

yanjun.sun@telecom-paristech.fr

Feburary 26, 2016

Outline

Introduction

Introduction

- For safety critical systems, it is cost-effective to perform verification on models of the system developed in upstream design phases.

Introduction

- For safety critical systems, it is cost-effective to perform verification on models of the system developed in upstream design phases.

- Initiated by French nuclear industry since 2012, the "CONNEXION" project proposes a unique tool chain to automate as much as possible the functional verification on models of the I&C (Instrumentation & Control) system.

Introduction

- For safety critical systems, it is cost-effective to perform verification on models of the system developed in upstream design phases.
- Initiated by French nuclear industry since 2012, the "CONNEXION" project proposes a unique tool chain to automate as much as possible the functional verification on models of the I&C (Instrumentation & Control) system.
- This article presents a new MBT process leveraging model checking to enrich functional verification. Coverage based test generation is combined with functional requirements to ensure the functional reality of new test.

CONNEXION: key figures

CONNEXION: partners

I&C System of a Nuclear Power Plant

I&C System of a Nuclear Power Plant

- The I&C system of a Nuclear Power Plant is composed of several hundreds of **Elementary System** (**ES**).

I&C System of a Nuclear Power Plant

- The I&C system of a Nuclear Power Plant is composed of several hundreds of **Elementary System** (**ES**).
  - 8000 binary signals and 4000 analog signals

I&C System of a Nuclear Power Plant

- The I&C system of a Nuclear Power Plant is composed of several hundreds of **Elementary System** (**ES**).
  - 8000 binary signals and 4000 analog signals
  - over 10 000 I&C sub-functions and 300 I&C cabinets

I&C System of a Nuclear Power Plant

- The I&C system of a Nuclear Power Plant is composed of several hundreds of **Elementary System** (**ES**).
  - 8000 binary signals and 4000 analog signals
  - over 10 000 I&C sub-functions and 300 I&C cabinets

- Each ES is a set of circuits and components performing an essential function to the operation of the nuclear plant.

I&C System of a Nuclear Power Plant

- The I&C system of a Nuclear Power Plant is composed of several hundreds of **Elementary System** (**ES**).
  - 8000 binary signals and 4000 analog signals
  - over 10 000 I&C sub-functions and 300 I&C cabinets

- Each ES is a set of circuits and components performing an essential function to the operation of the nuclear plant.
  - **Process**: physical infrastructure

I&C System of a Nuclear Power Plant

- The I&C system of a Nuclear Power Plant is composed of several hundreds of **Elementary System** (**ES**).
  - 8000 binary signals and 4000 analog signals
  - over 10 000 I&C sub-functions and 300 I&C cabinets

- Each ES is a set of circuits and components performing an essential function to the operation of the nuclear plant.
  - **Process**: physical infrastructure
  - **Functional Diagram** (**FD**): control of the Process

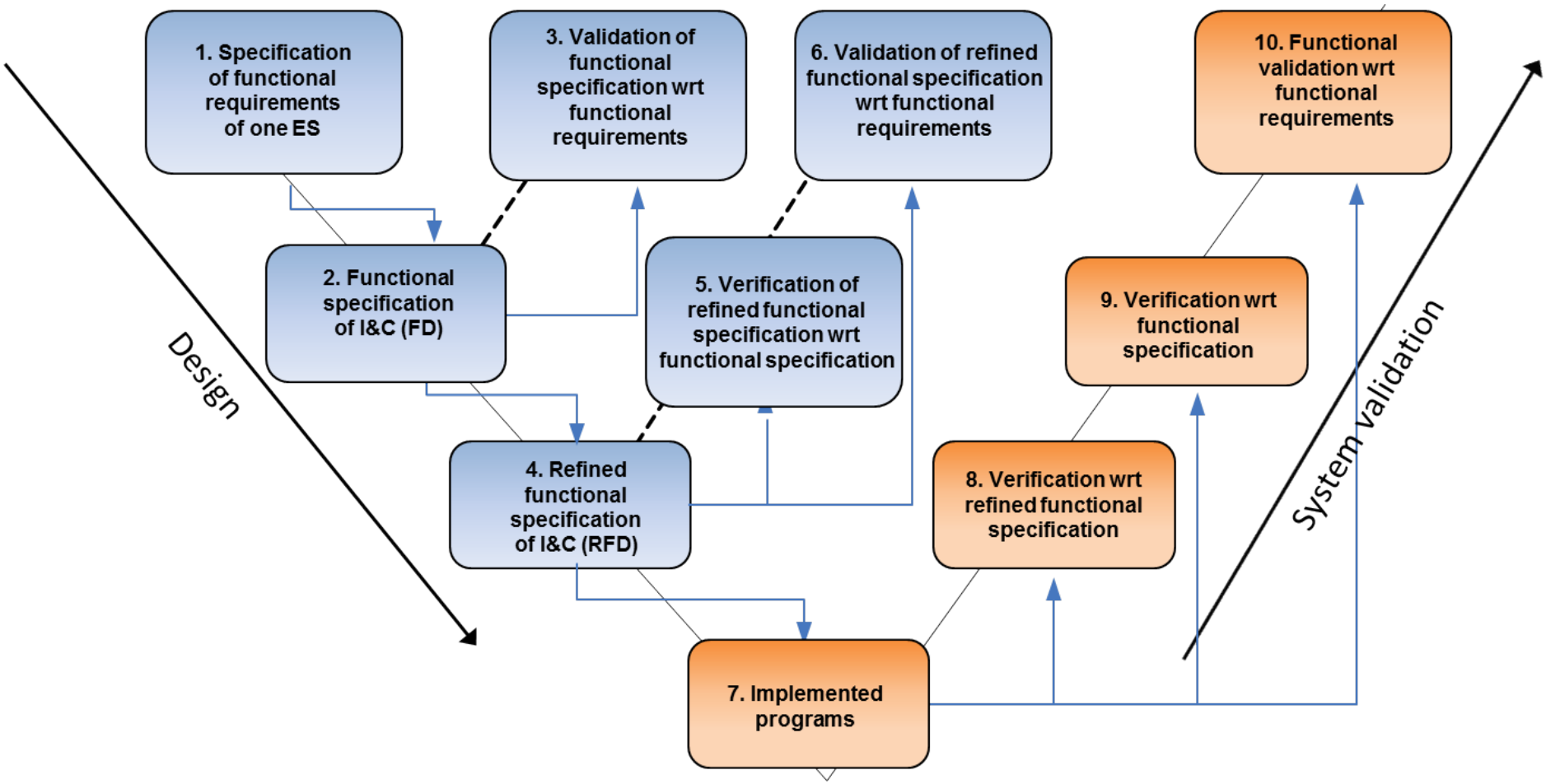
I&C System of a Nuclear Power Plant

- The I&C system of a Nuclear Power Plant is composed of several hundreds of **Elementary System** (**ES**).
  - 8000 binary signals and 4000 analog signals
  - over 10 000 I&C sub-functions and 300 I&C cabinets

- Each ES is a set of circuits and components performing an essential function to the operation of the nuclear plant.
  - **Process**: physical infrastructure
  - **Functional Diagram** (**FD**): control of the Process
  - **Refined Functional Diagram** (**RFD**)

Triple V life cycle of one ES

The traditional V cycle is enriched by two sub-cycles:



A unique tool chain

Category	Tool
System modelling tool	*Papyrus/SysML*
	Dymola/Modelica
	SCADE Suite/Scade
Functional test generation tool	*Interval*
	MaTeLo
Model checker	*GATeL*
Coverage monitoring tool	*SCADE QTE*
Model execution environment	*ALICES*
Test observer (oracles)	*ARTiMon*

Table: The verification tool chain in "CONNEXION"

A unique verification tool chain

Category	Tool
System modelling tool	*Papyrus/SysML*
	Dymola/Modelica
	SCADE Suite/Scade
Functional test generation tool	*Interval*
	MaTeLo
Model checker	*GATeL*
Coverage monitoring tool	*SCADE QTE*
Model execution environment	*ALICES*
Test observer (oracles)	*ARTiMon*

Table: The verification tool chain in "CONNEXION"

Related work on test generation with model checking

Related work on test generation with model checking

- A model checker is normally used to analyze all reachable states of a model and search for property violations. In case of a violation detected, a counterexample is returned.

Related work on test generation with model checking

- A model checker is normally used to analyze all reachable states of a model and search for property violations. In case of a violation detected, a counterexample is returned.
- The counterexample contains test date that forces the model to reach a state where the violation occurs. It can be used to construct test cases.

Related work on test generation with model checking

- A model checker is normally used to analyze all reachable states of a model and search for property violations. In case of a violation detected, a counterexample is returned.
- The counterexample contains test date that forces the model to reach a state where the violation occurs. It can be used to construct test cases.
- A rich literature on coverage based test generation with model checking:
  - Rayadurgam et al.(2001): formalization of various structural coverage criteria to challenge a model checker
  - Eniou et al.(2013), Heimdahl et al.(2003): automatic test generation by model checking to satisfy structural coverage criteria

A new model-based testing process (1)

A new model-based testing process (1)

- Definitions:
  - **Branch**: a unit of the model coverage measurement, whatever the coverage criterion chosen (DC, MCC, MC/DC, etc...).

A new model-based testing process (1)

- Definitions:
  - **Branch**: a unit of the model coverage measurement, whatever the coverage criterion chosen (DC, MCC, MC/DC, etc...).
  - **Reachability check**: whether a branch can be covered by any test case.

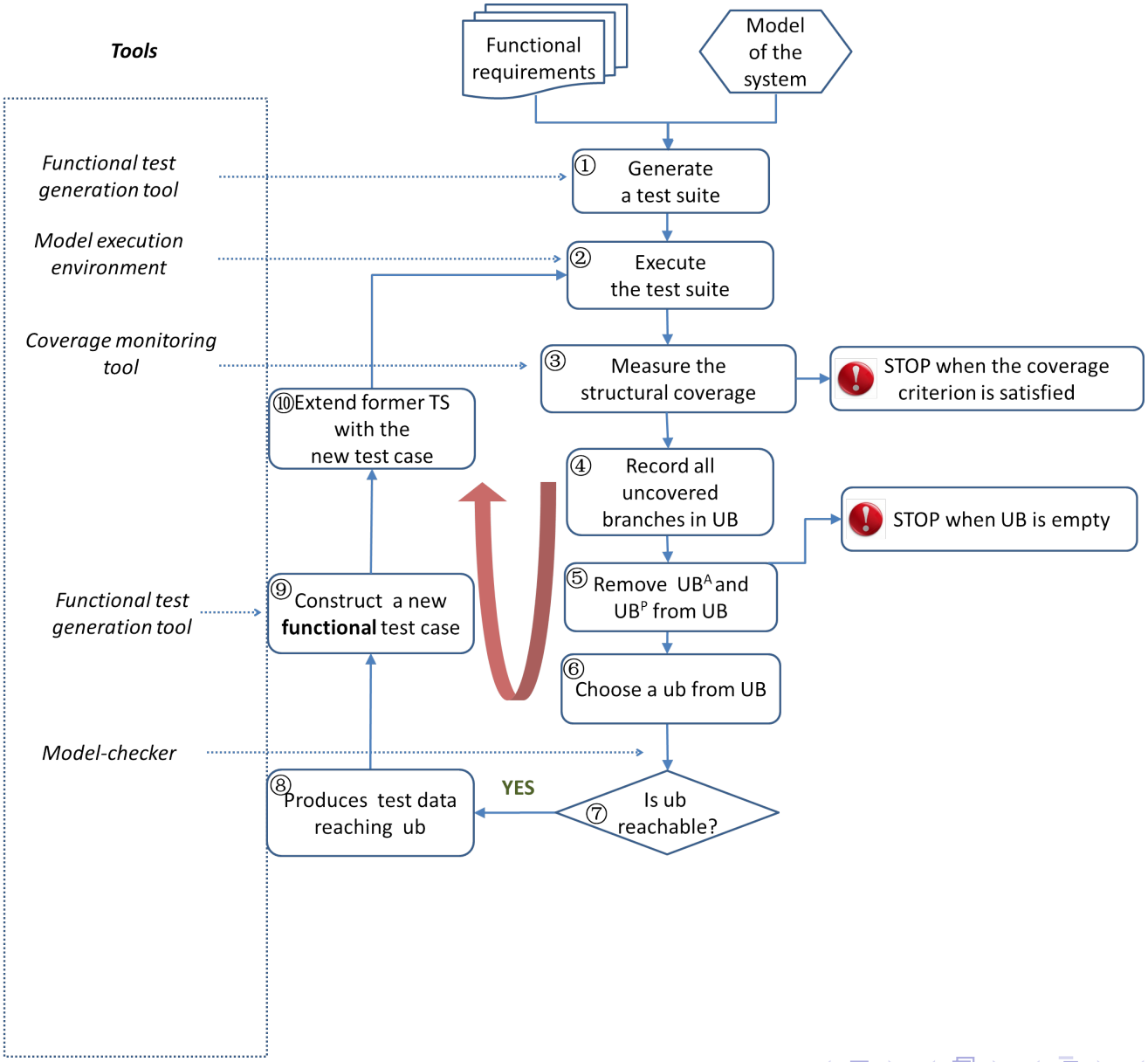
A new model-based testing process (1)

- Definitions:
  - **Branch**: a unit of the model coverage measurement, whatever the coverage criterion chosen (DC, MCC, MC/DC, etc...).
  - **Reachability check**: whether a branch can be covered by any test case.
- Fantachi et al.(2004) proposes a procedure to perform reachability check on every uncovered branch. Either establishes that the branch can not be covered, or produces a test case that covers the branch.

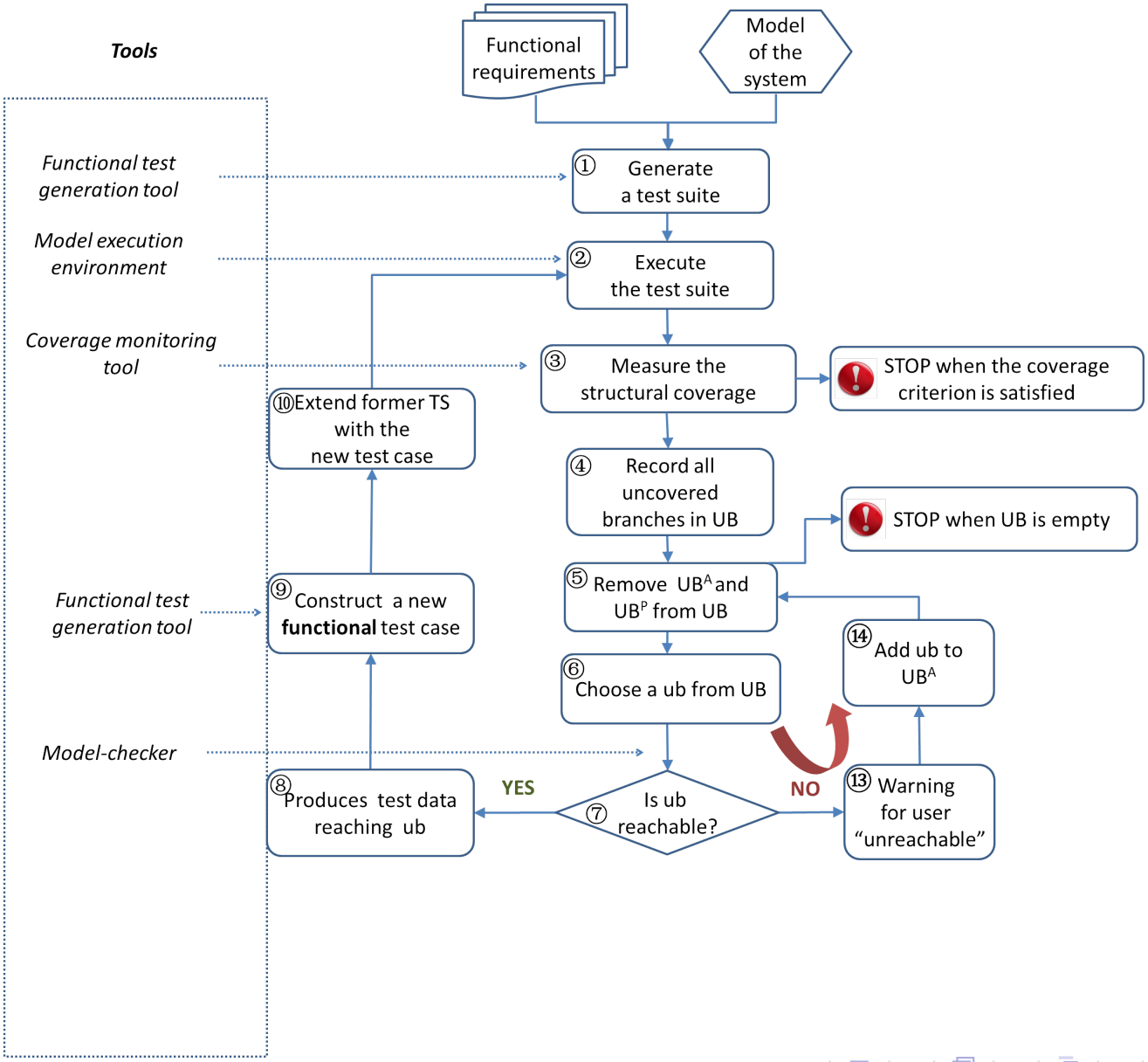
A new model-based testing process (1)

- Definitions:
  - **Branch**: a unit of the model coverage measurement, whatever the coverage criterion chosen (DC, MCC, MC/DC, etc...).
  - **Reachability check**: whether a branch can be covered by any test case.
- Fantachi et al.(2004) proposes a procedure to perform reachability check on every uncovered branch. Either establishes that the branch can not be covered, or produces a test case that covers the branch.
- In addition to this procedure, our process:
  - highlights the functional reality of the coverage based test generation by model checking;
  - takes into account that the model checker can have a "time out";
  - designed in particular for a complex system composed of sub-systems modeled in different formats.

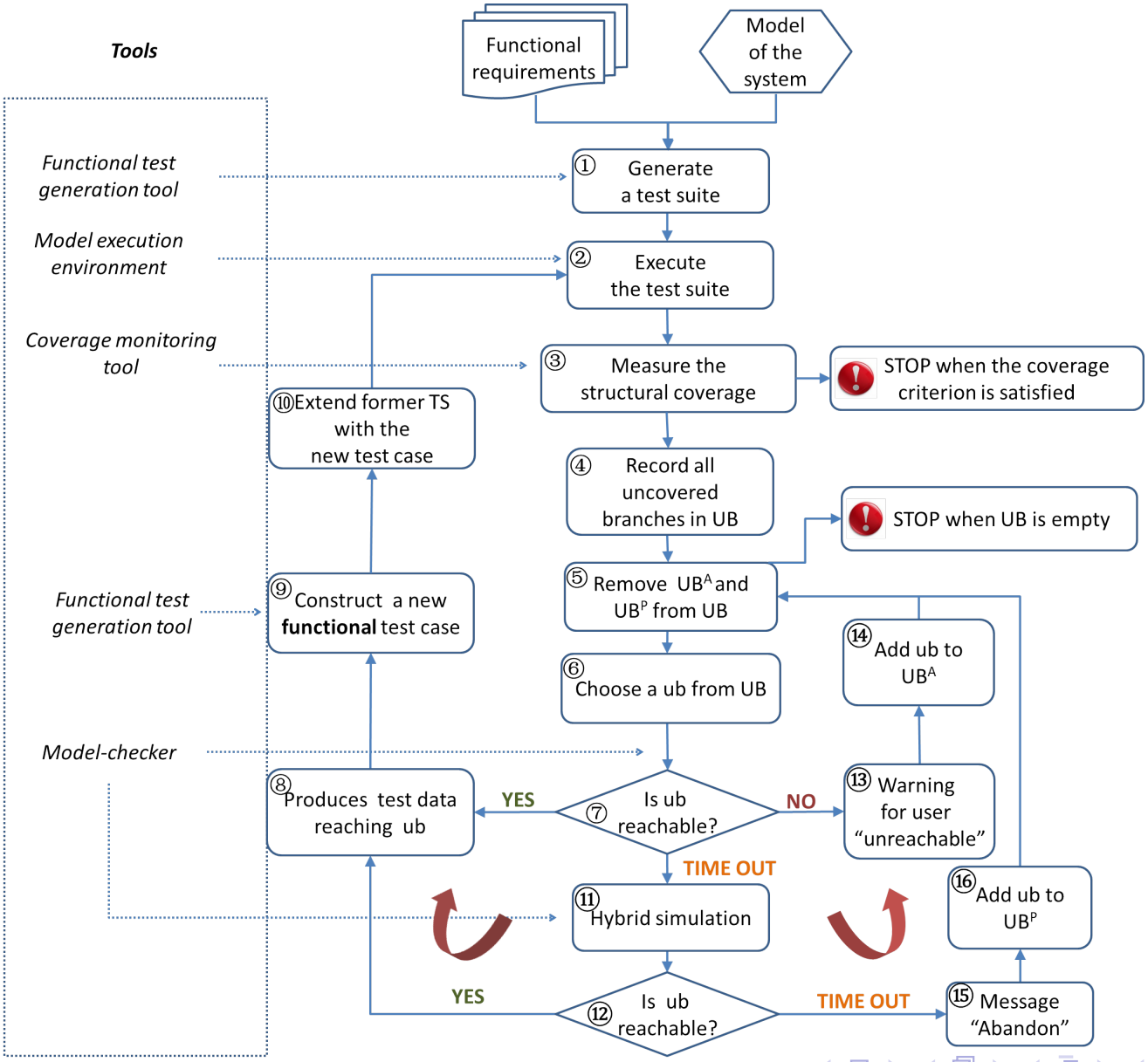
A new model-based testing process (2)



A new model-based testing process (2)



A new model-based testing process (2)



Challenges with respect to "CONNEXION"

- Construct a test case at the ES level from test data generated by GATeL requires knowledge of both the functional requirements and the testing techniques and tools.

Challenges with respect to "CONNEXION"

- Construct a test case at the ES level from test data generated by GATeL requires knowledge of both the functional requirements and the testing techniques and tools.

- Equivalence of transformation between models:
  - recreate FD and RFD in *SCADE Suite*
  - transforme Scade models into Lustre models

Conclusion

Conclusion

- This article presents a model-based testing process directed by structural coverage and functional requirements. The unique tool chain provided by “CONNEXION” enables our process.

Conclusion

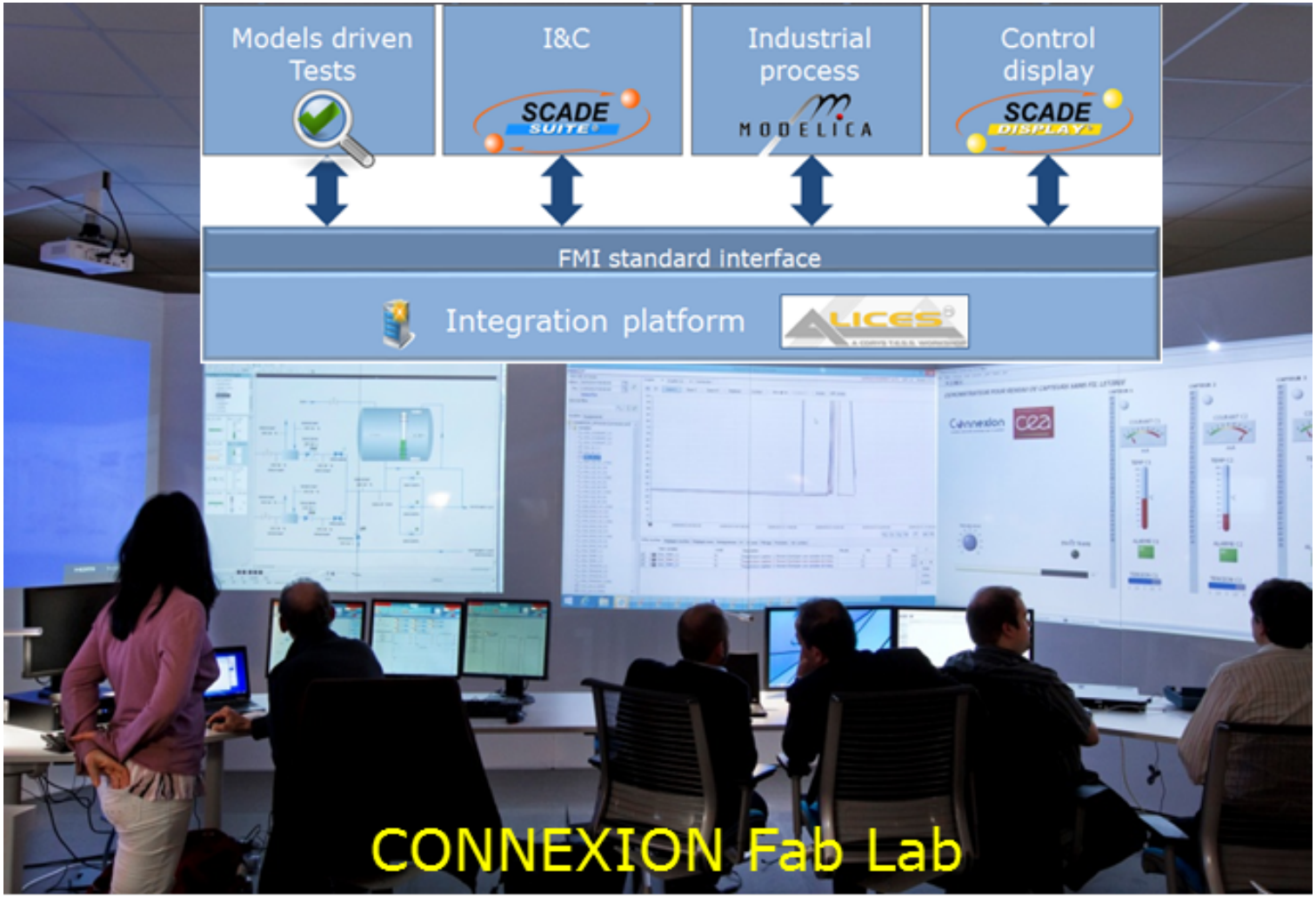
- This article presents a model-based testing process directed by structural coverage and functional requirements. The unique tool chain provided by “CONNEXION” enables our process.

- The “CONNEXION” project has determined a progressively complex case study where our process is being applied.

Conclusion

- This article presents a model-based testing process directed by structural coverage and functional requirements. The unique tool chain provided by "CONNEXION" enables our process.
- The "CONNEXION" project has determined a progressively complex case study where our process is being applied.
- Future work includes research on reducing test cost by reusing some test cases after changes being made to the system. The proof of model transformation equivalence remains an open question.

CONNEXION Fab Lab: a step toward Industry 4.0



Acknowledgment

The authors would like to thank the engineers of EDF who are part of the "CONNEXION" project: Maxime Neyret and Gaëtan Robin as well as other project partners providing tools and valuable advice: Benjamin Blanc from CEA (*GATeL*), François-Xavier Dormoy and Luc Coyette from Esterel Technologies (*SCADE* tool set), François Chastrette from ALL4Tech (*MaTeLo*).

References

Enoiu et al.(2013)

Automated test generation using model-checking: an industrial evaluation

ICTSS 2013

Rayadurgam et al.(2001)

Coverage Based Test-Case Generation Using Model Checkers

IEEE 2001

Heimdahl et al.(2001)

Auto-generating test sequences using model-checkers: A case study

3rd International Workshop on Formal Approaches to Testing of Software 2003

Fantechi et al.(2004)

Enhancing Test Coverage by Back-tracking Model-checker Counterexamples

Electronic Notes in Theorectical Computer Science, vol. 116, 143–158, 2004

The End
Thank you!