GATeL et la génération de séquences de tests fonctionnels: impact opérationnel et certification

Pierre Monteil

Juin 2015

pierre.monteil.cn@rolls-royce.com

Trusted to deliver excellence

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Agenda

Introduction to Rolls-Royce Civil Nuclear

Related Software Activities and Testing Challenges

GATeL Deployment and Results

Qualification

Conclusions

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Agenda

Introduction to Rolls-Royce Civil Nuclear

Related Software Activities and Testing Challenges

GATeL Deployment and Results

Qualification

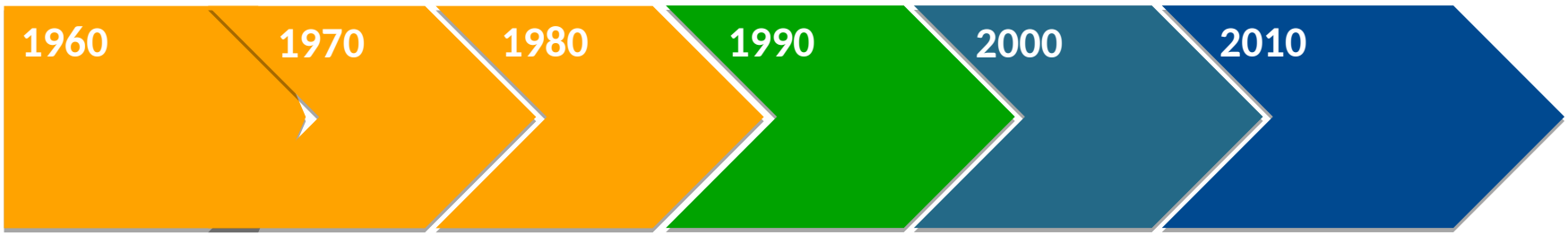
Conclusions

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Our history

A continuous experience on the nuclear market since 1960s

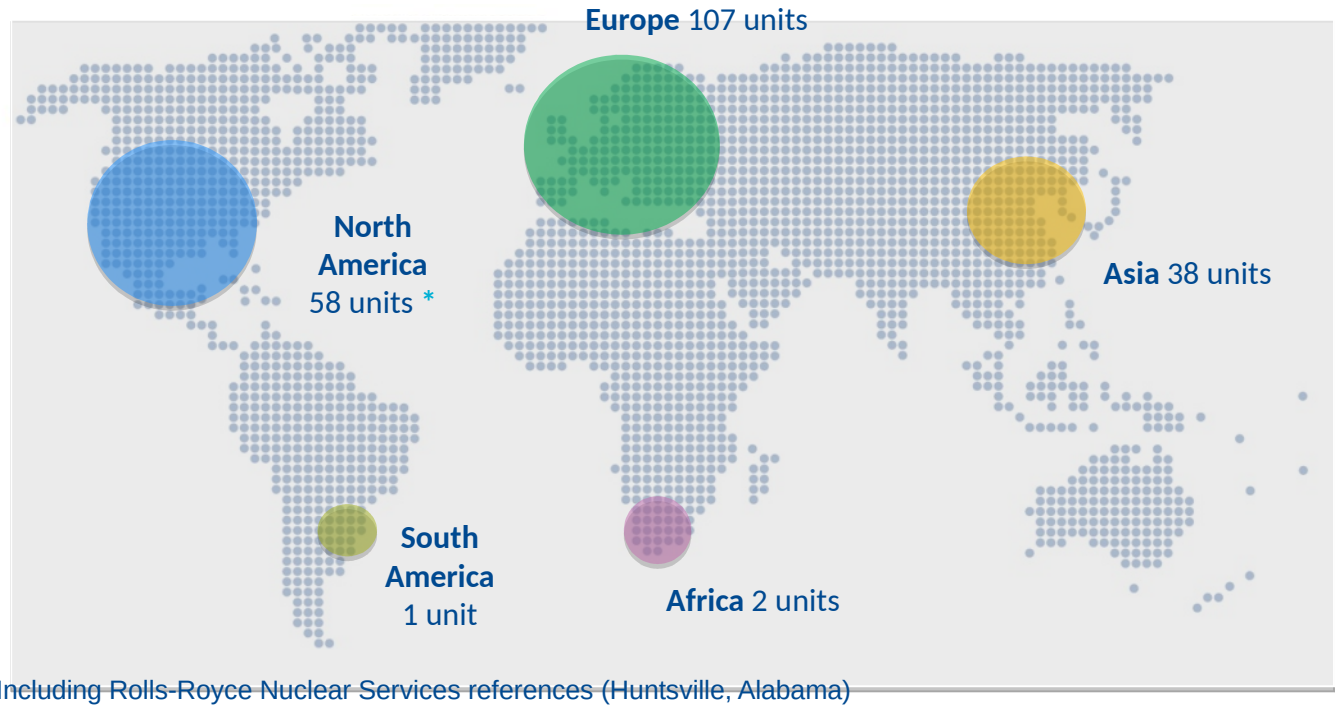


1960	1970	1980	1990	2000	2010
Cooperation with CEA on neutron detection and Multibloc technology	Fessenheim 1 operating with our I&C systems (NIS, RCS, detectors, boronmeter, etc.)	First digital reactor protection system (SPIN) worldwide in Paluel 2	First long term support agreement with EDF for the French nuclear fleet	I&C retrofit of Dukovany VVER reactors from 2000 to 2009	Certification of Spinline technology by NRC, the US safety authority

© 2015 Rolls-Royce Civil Nuclear SAS

Our references

Our systems are present on 200 reactors in 20 countries

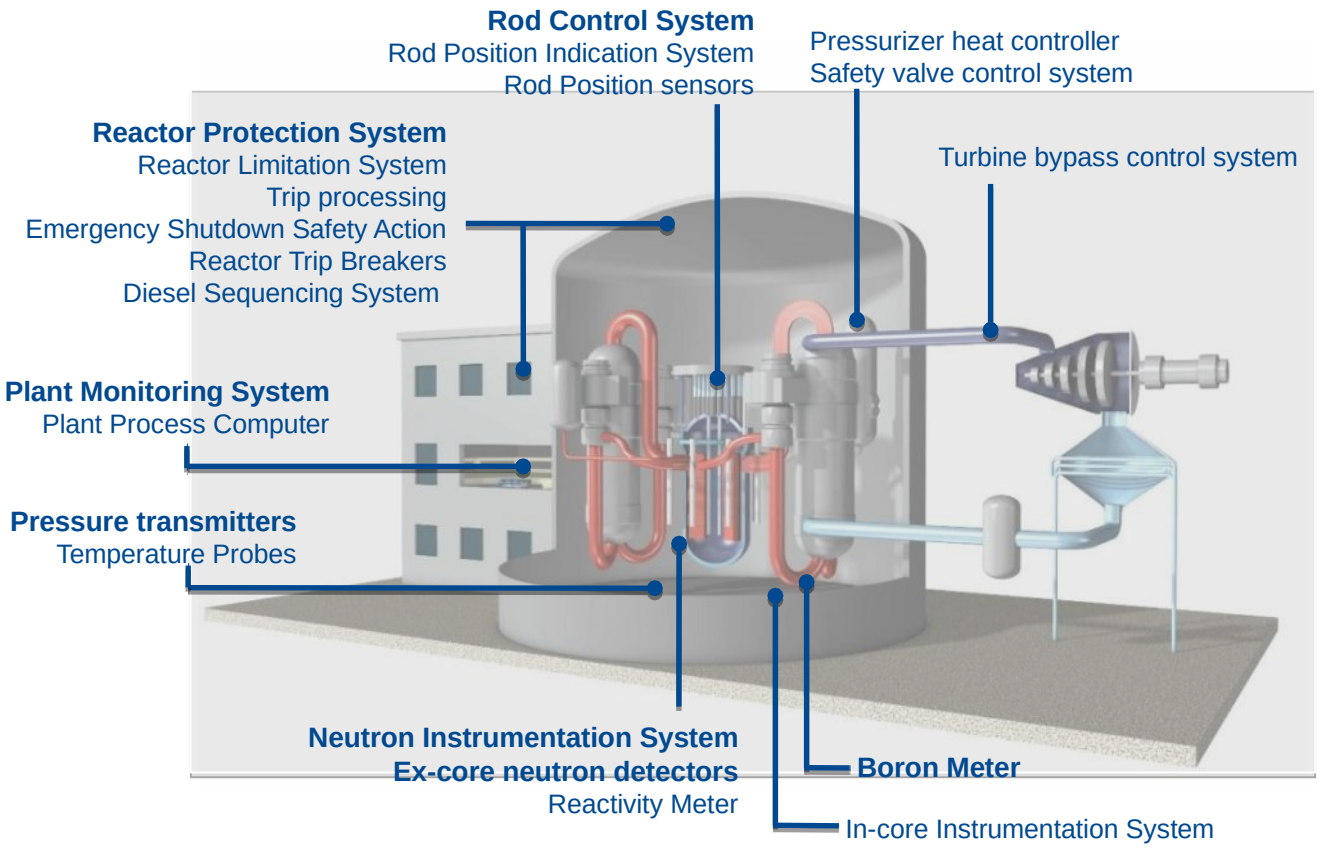


* Including Rolls-Royce Nuclear Services references (Huntsville, Alabama)

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

A complete range of I&C systems



© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Agenda

Introduction to Rolls-Royce Civil Nuclear

Related Software Activities and Testing Challenges

GATeL Deployment and Results

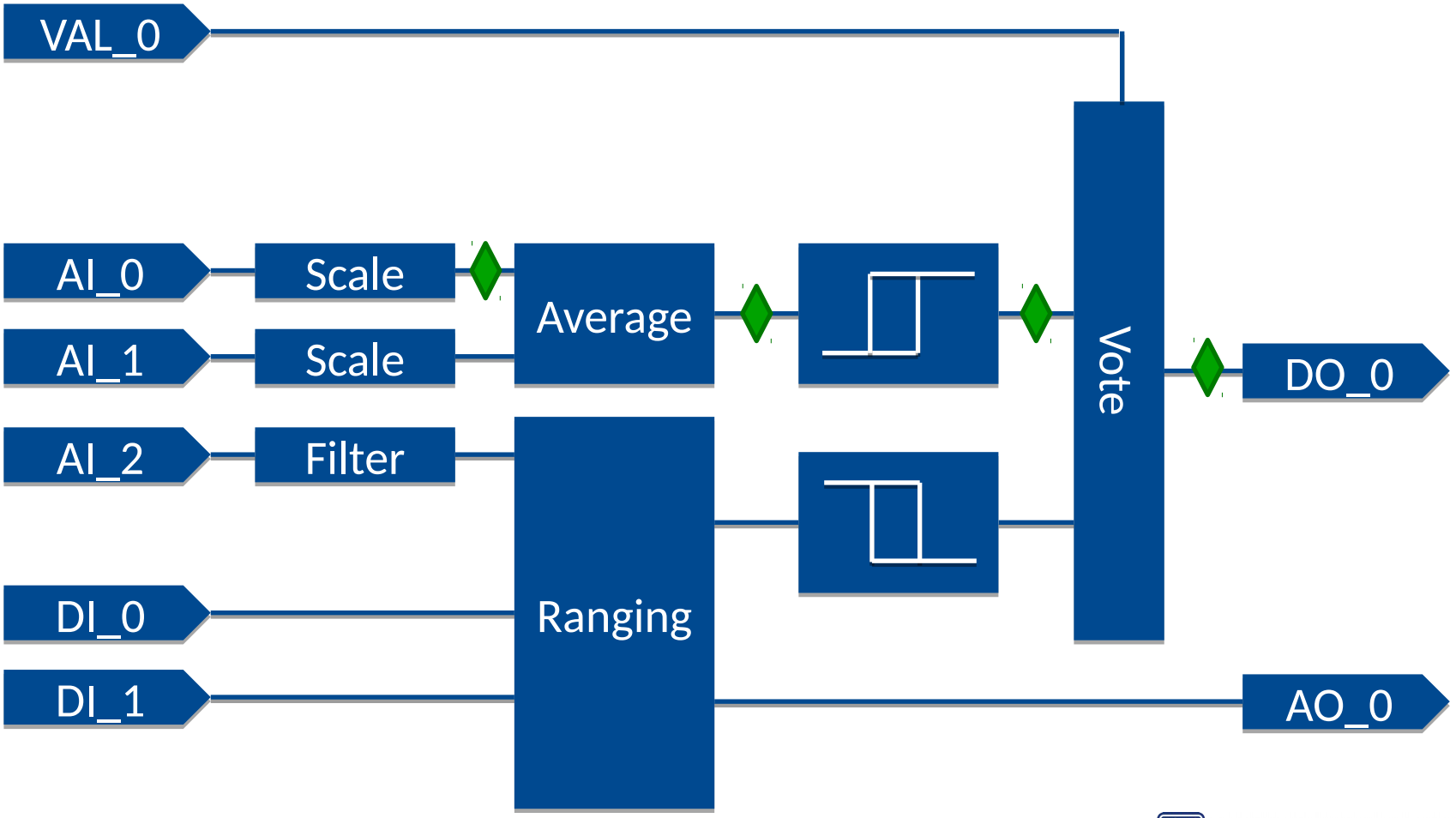
Qualification

Conclusions

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Example of safety I&C processing requirements (1/2)



© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Upstream Requirements and activities

Our system requirements are typically expressed as functional diagrams fixing the structure of the SW design.

Requirements are synchronous functions combining analog and digital inputs, hard-wired or from network. These functions produce safety orders (digital) or specific measures (analog). Some intermediate nodes are visible through the network.

Our two main activities are:

- **Translating these diagrams into SW (using Esterel Scade) adding all the specific safety and technology-related requirements,**
- **Performing exhaustive V&V on these design.**

SW V&V involves quite a lot of testing. Testing effort (as a whole) is more than 50% of the SW cost.

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Test strategy

Test strategy will tell what are the expected transitions we need to check at the output of a given function.

The test engineer needs to find out the right input sequence that will lead to this expected transition.

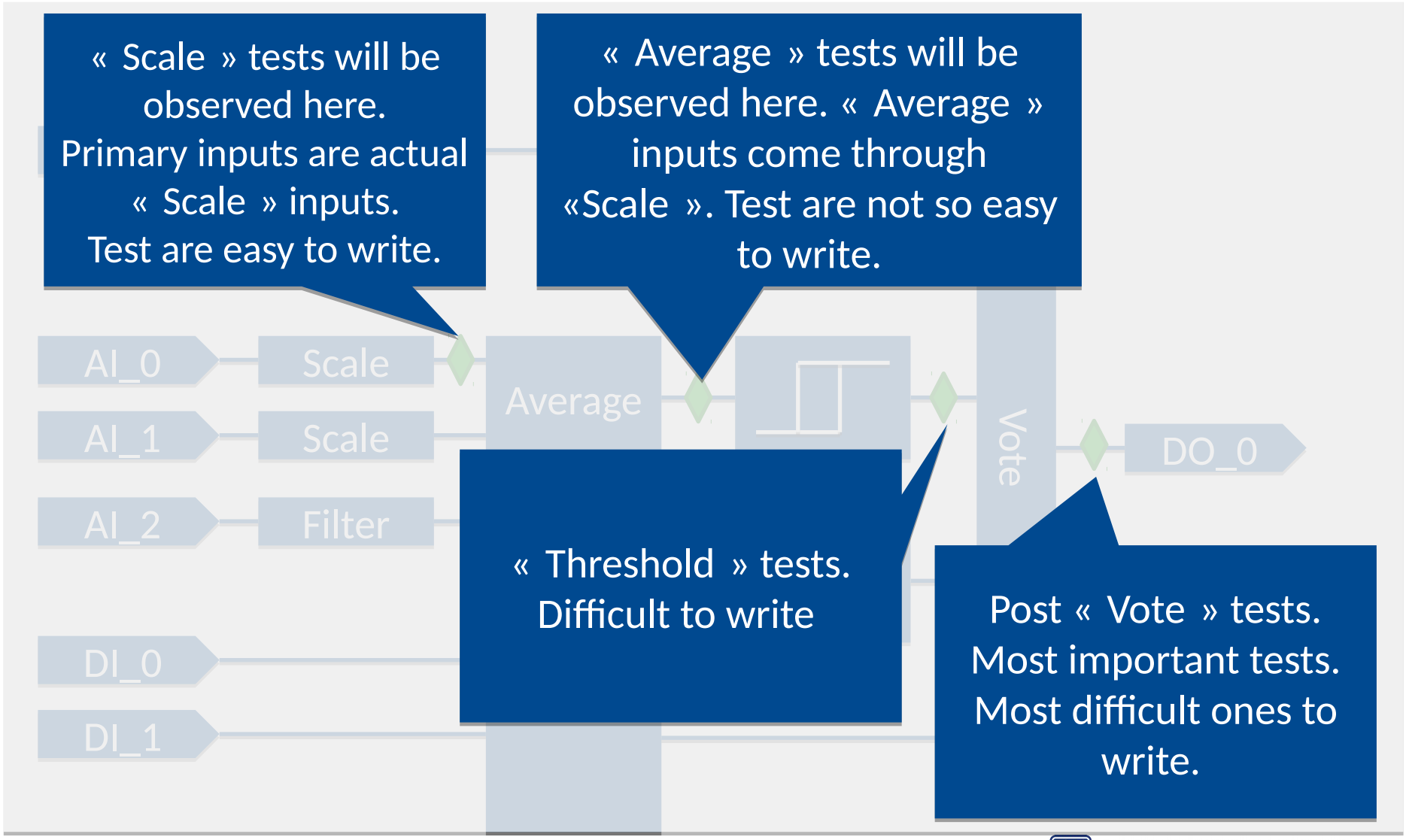
Validation is made in black-box. If the required inputs are primary ones, then it is fairly easy. Otherwise the test engineer needs to take into account all the intermediate functions.

This can become a complex and time-consuming analytical process.

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Test and observation of the results



© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Problem : how to assist test engineering

Assumption: Test strategy is defined out of any tool context.

How to help the test engineer in his process of writing these test sequences in order to:

- **Save time & effort,**
- **Ensure quality (e.g. tests are in line with objectives)**

Working on this question, we initiated our work with CEA on GATeL which is able to produce input sequences for given expected output transitions

- **Without changing test strategy!**

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Solution : GATeL

We initiated an internal R&D project to validate our intuition that Gatel could be used as a test generator on a representative case study (for Neutronic Instrumentation Systems).

We worked alongside with the CEA team to address a couple of issues. They provided support, advices, as well as enhancements.

The R&D project went well (nothing blocking), and we realized that, in case of tool limitation, or any other kind of problem, we would be able to work-around them «by hand » as the strategy was un-changed.

Agenda

Introduction to Rolls-Royce Civil Nuclear

Related Software Activities and Testing Challenges

GATeL Deployment and Results

Qualification

Conclusions

Rolls-Royce

From evaluation to deployment

Technical feasibility

- « Our » ability to model all the functions in Lustre
- « Tool » ability to generate test sequences (e.g. no performance limitations)

Integration in our process

- Confirmation that this solution is test-strategy independent,
- Impact analysis on all the interfaces

Preparation of deployment

- Documentation update (instructions, plans, guides, etc…)
- Development and release of intermediate tools (e.g. test format conversion)

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Application to a real project

Then we decided to go for a real project: the Neutronic Instrumentation System of EDF VD3-1300MW retrofit program.

During the project, we identified and addressed a couple of issues:

- **HW validity combinations not supported by the I/O boards,**
- **Analog signal variations that are physically impossible,**
- **Test documentation was automated, but we had to work on its processing to make it readable « by a human being».**

Good final results:

- **No SW defect identified so far during system validation,**
- **SW and its documentation delivered on schedule,**
- **First-of-a-kind costs partly covered by the savings.**

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Learnings : Positive feedbacks

Requirements quality

- Enforced by an extra modeling stage made by the independent V&V team
- Ensuring clarity and exaustivity

Design exploration

- Generated tests were at times using surprising ways of achieving the objectives
- Allowing to evaluate non-classical ways of thinking the design

Evolution support

- Highly automated process once everything is in place
- Allowing to regenerate all the tests smoothly for last-moment changes

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Learnings : Actual limits and difficulties

Models and Targets

- Working first at model level might hide some limitations/issues
- Which are only visible later on a real target

Mastering Lustre

- Modeling in Lustre needs skills and experience,
- not every V&V engineers are familiar with the language

Mastering Gatel

- Using GATeL requires experience
- which takes some time to get consolidated

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Agenda

Introduction to Rolls-Royce Civil Nuclear

Related Software Activities and Testing Challenges

GATel Deployment and Results

Qualification

Conclusions

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Tool qualification: the IEC 60880 requirements

Our SW development process is aligned with IEC 60880, encouraging test automation tools, given some guidelines.

These guidelines are related to:

- **Tool selection / evaluation prior to use,**
- **Records of tool outputs (exhaustive logs),**
- **Relative criticality of the tool and associated qualification process,**
- **Precautions toward defects introduced by the tool.**

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Formal Tools qualification challenge

For an end user, the reliability of a formal tool is difficult to assess, extremely hard to demonstrate.

If the formal tool is used as a prover, and if these proofs are used for the final validation demonstration, then the tool qualification is a big challenge.

If the formal tool is used as a test generator, and:

- **There is an independent way to ensure the expected results (e.g. through a reference model),**
- **There is a verification process of the generated tests,**

Then there is no need for intensive tool qualification.

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Challenging qualification need

We assume that we are not able to demonstrate Gatel reliability.

So we integrated it in our process in such a way that this demonstration is not required.

We « just » substituted the « manual » test production phase by something assisted by the tool.

We rely our own reference models, as well as our own coverage metrics. We kept all our independent test verification stages.

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Agenda

Introduction to Rolls-Royce Civil Nuclear

Related Software Activities and Testing Challenges

GATeL Deployment and Results

Qualification

Conclusions

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Conclusions

Positive experience, positive project outcome,

Smooth integration within our process, inducing improvements now broadly used,

Ability to produce long/complex test cases within a reasonable timeframe,

Simple qualification/certification process,

Requires specific skills ; maintenance of these skills needs a minimal amount of activity.

© 2015 Rolls-Royce Civil Nuclear SAS

Rolls-Royce

Questions?

Thank-you very much for your attention.

Any questions ?

Rolls-Royce