Spinline - FPGA and µProcessor based platform

Taken and sharing advantages of both worlds

Julien BACH,
Rolls-Royce Civil Nuclear SAS

AIEA FPGA workshop 2016 – Lyon, France - October 2016

Trusted to deliver excellence

Rolls-Royce

Main objectives

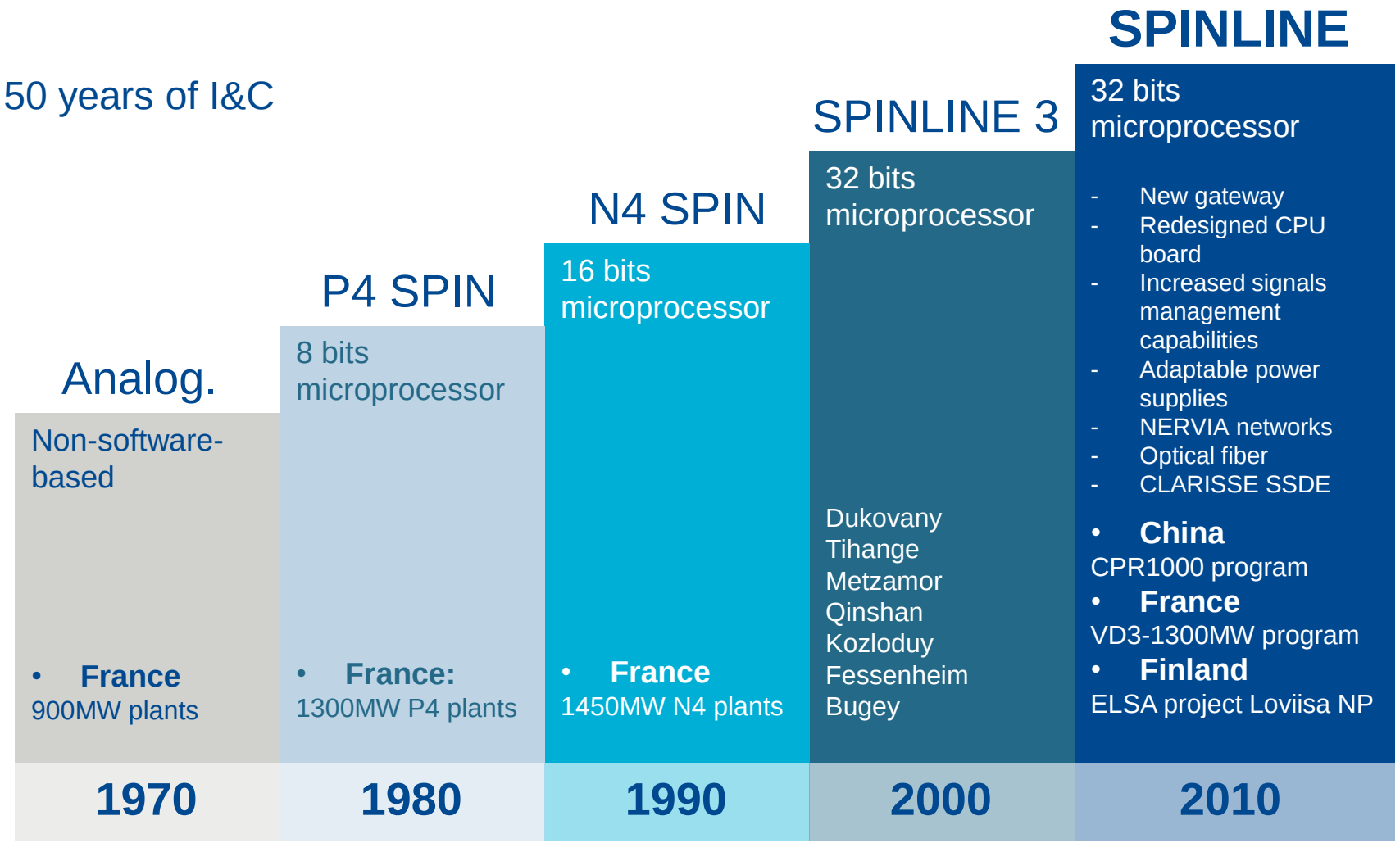
Spinline : the Rolls-Royce I&C Software based nuclear safety platform dedicated for category A functions

Overview of the software aspects

Overview of embedded FPGAs aspects

Licensing of Spinline in different Regulatory frameworks

Spinline the 4th digital generation

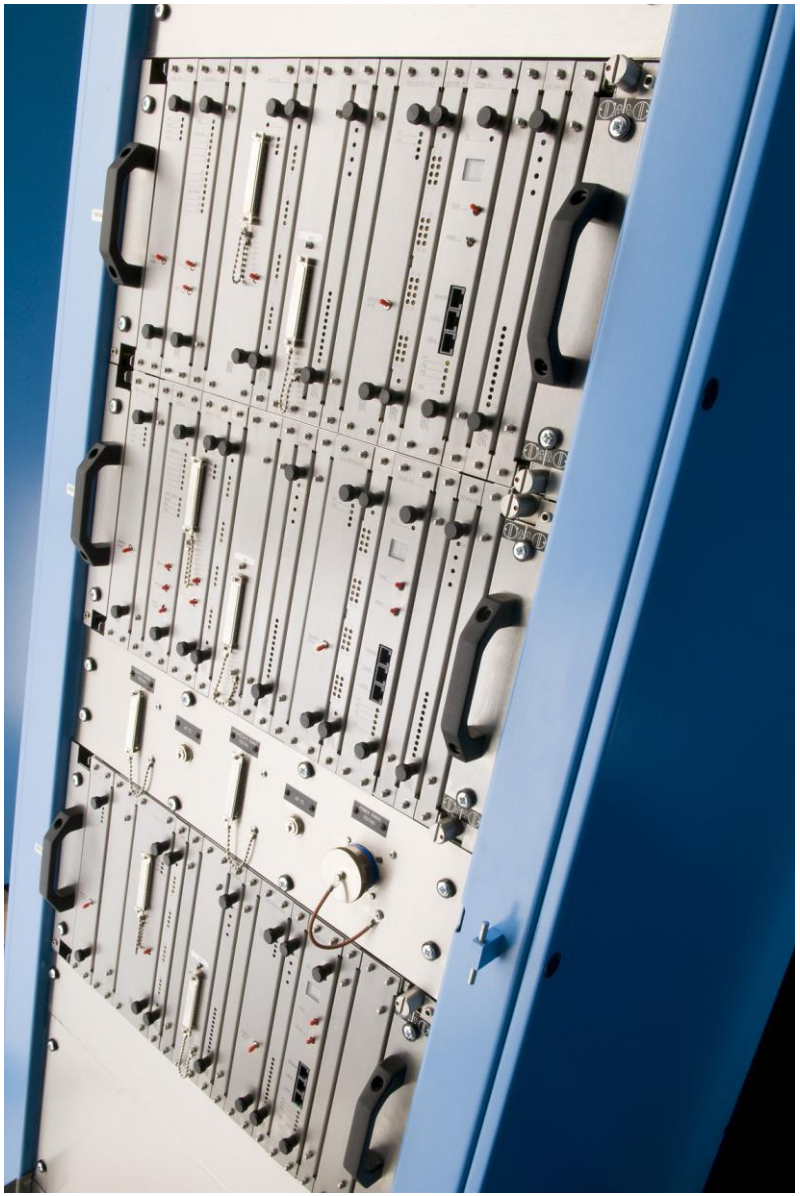


Rolls-Royce

Spinline platform

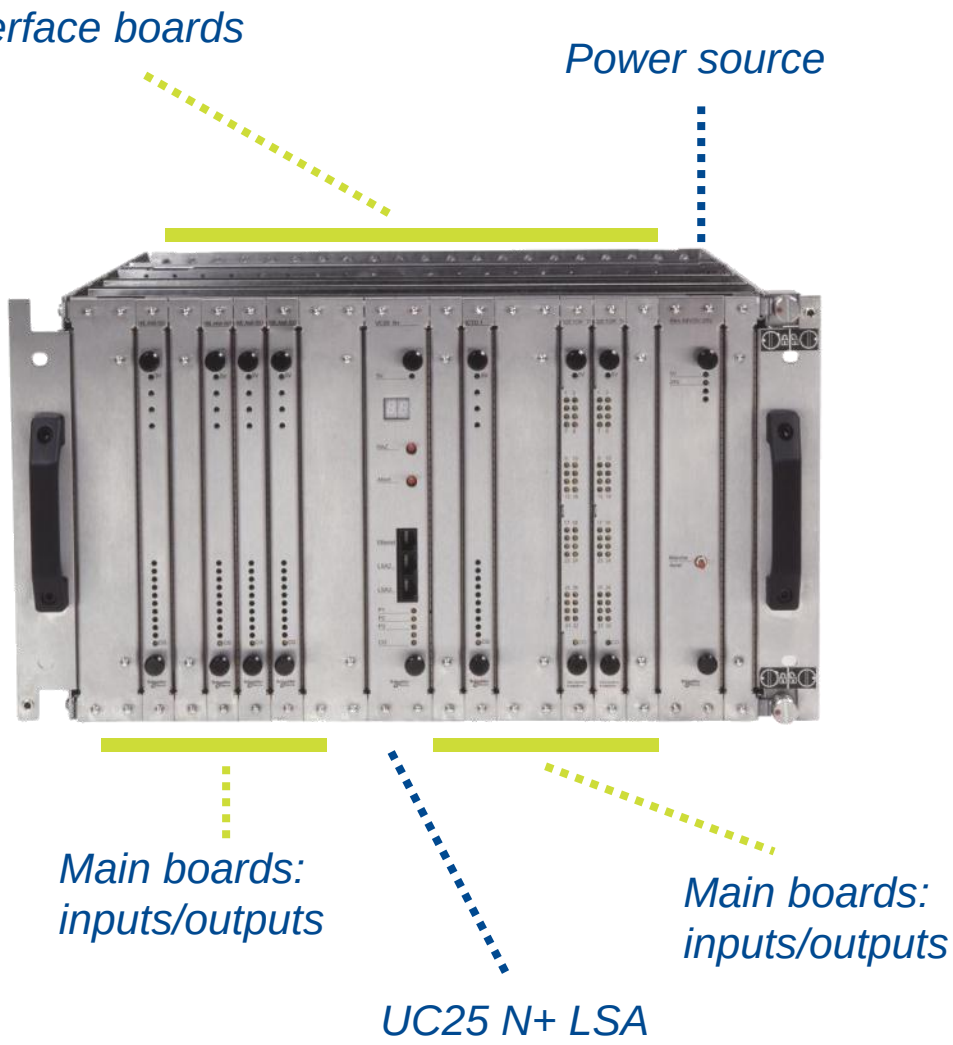
the Spinline components:

- The components of the generic platform software are:
  - The standardized, Class 1E configurable Operational System Software (OSS)
  - The Class 1E application-oriented library of re-usable software components,
  - The Class 1E software embedded in “intelligent” boards
  - A non-Class 1E set of tools integrated in a System and Software Development Environment ((CLARISSE), used to design and configure the systems and equipment software.
- Spinline embedded FPGA for electronic functions
- Spinline hardware boards, modules, racks, cabinets



Rolls-Royce

Spinline processing rack



Rolls-Royce

Spinline software

A Spinline software is composed of two parts:

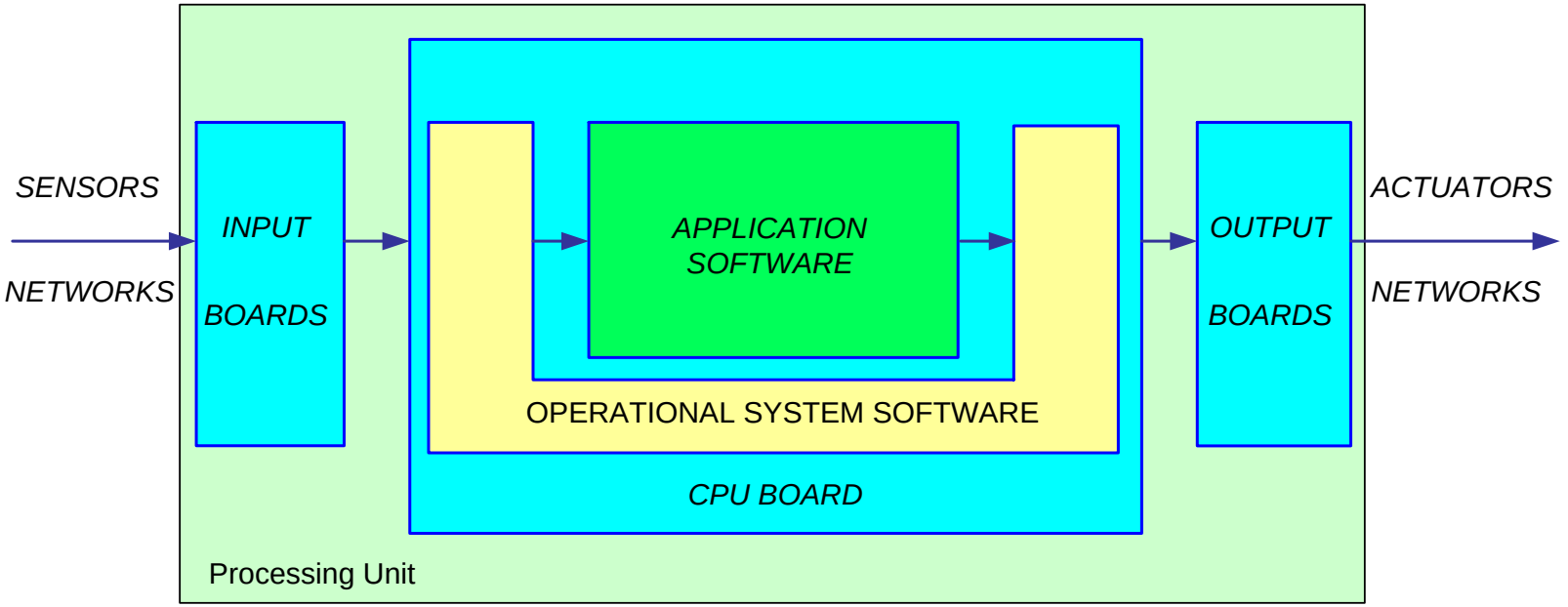
- The “Operational System Software” (OSS) is standard,
  - Is has been developed according to IEC 60880 and comes as a software component to be used on the CPU boards of the processing units.
  - It is ready for use after a simple configuration to fit the needs of the customer I&C systems. It provides basic functions like communication, data acquisition or services to be used by the application software

- The “application software” is specific and must be developed by a dedicated team.
  - It implements the Equipment Functional diagrams (the plant specific application)

Rolls-Royce

Spinline software

The software Installed on a Processing Unit



Rolls-Royce

Spinline software

Main characteristics :

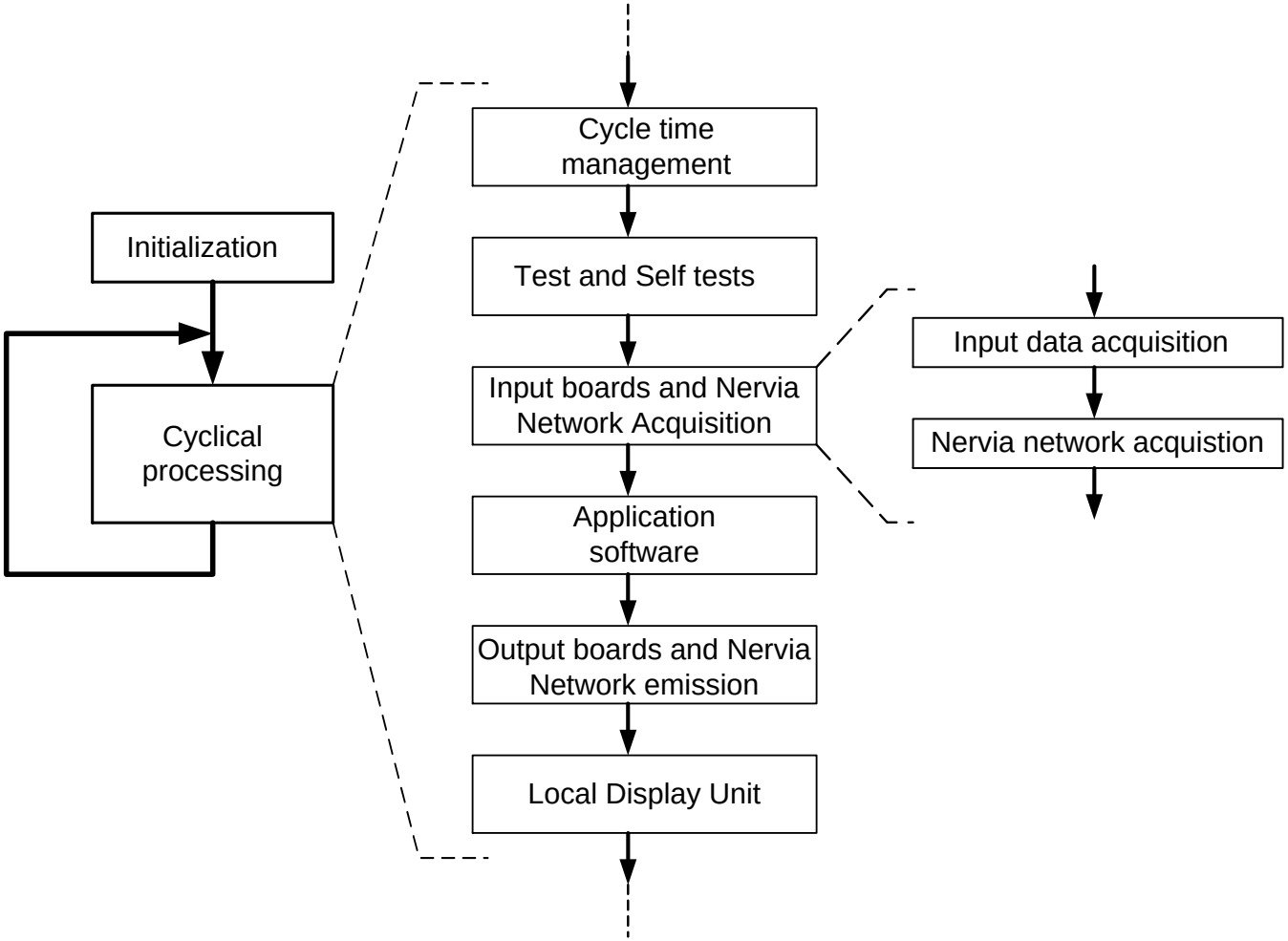
- no use of interrupts
- no dynamic memory allocation
- no support for event driven multi-tasking
- Modular, structured and simple
- functions embedded restricted to the only need of the operation of the equipment and the I&C safety functions
- perform and manage self-tests
- include defensive programming where appropriate
- ensure safety oriented features (when a failure is detected)

- Entirely designed, verified and validated according to IEC 60880

Rolls-Royce

Spinline software

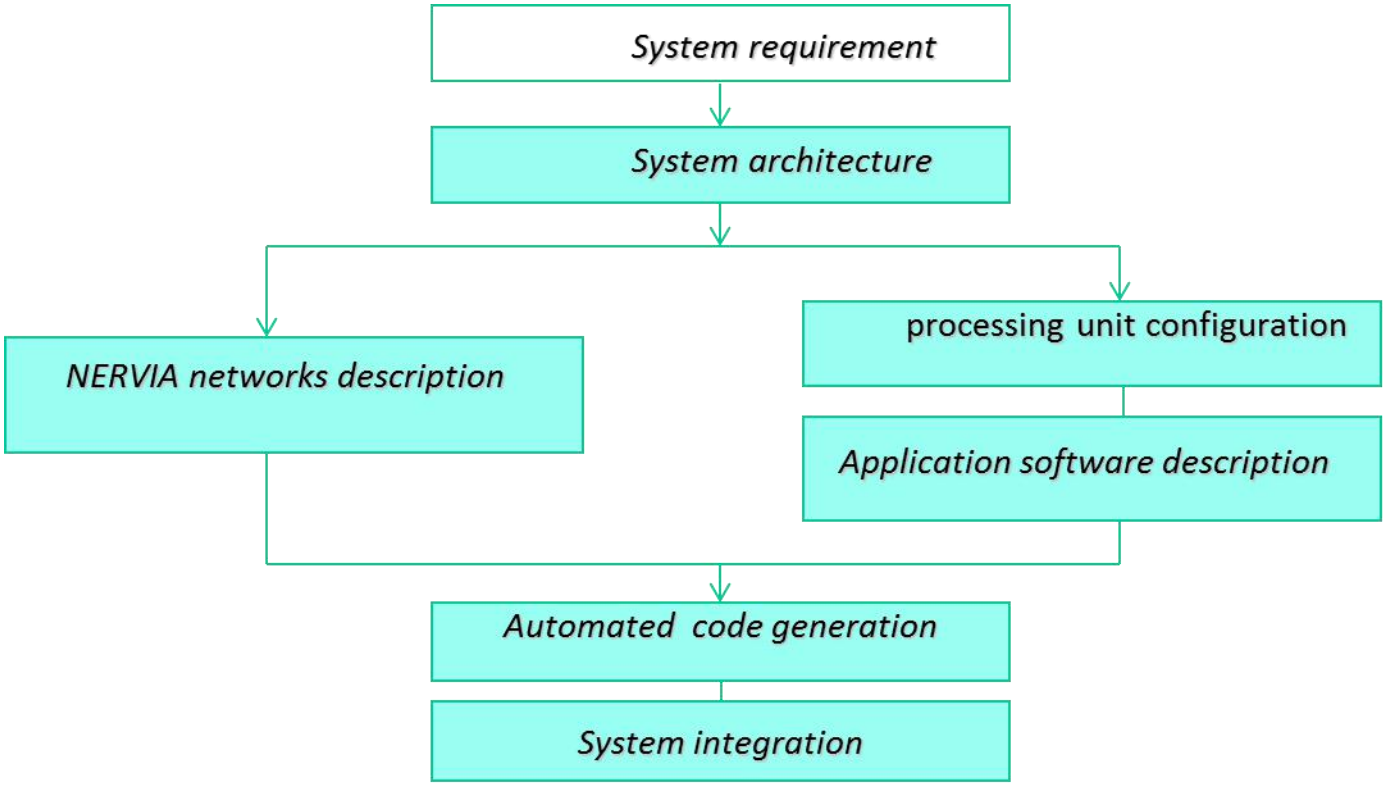
Sequential, cyclic and fully deterministic execution of functions



Rolls-Royce

Spinline software

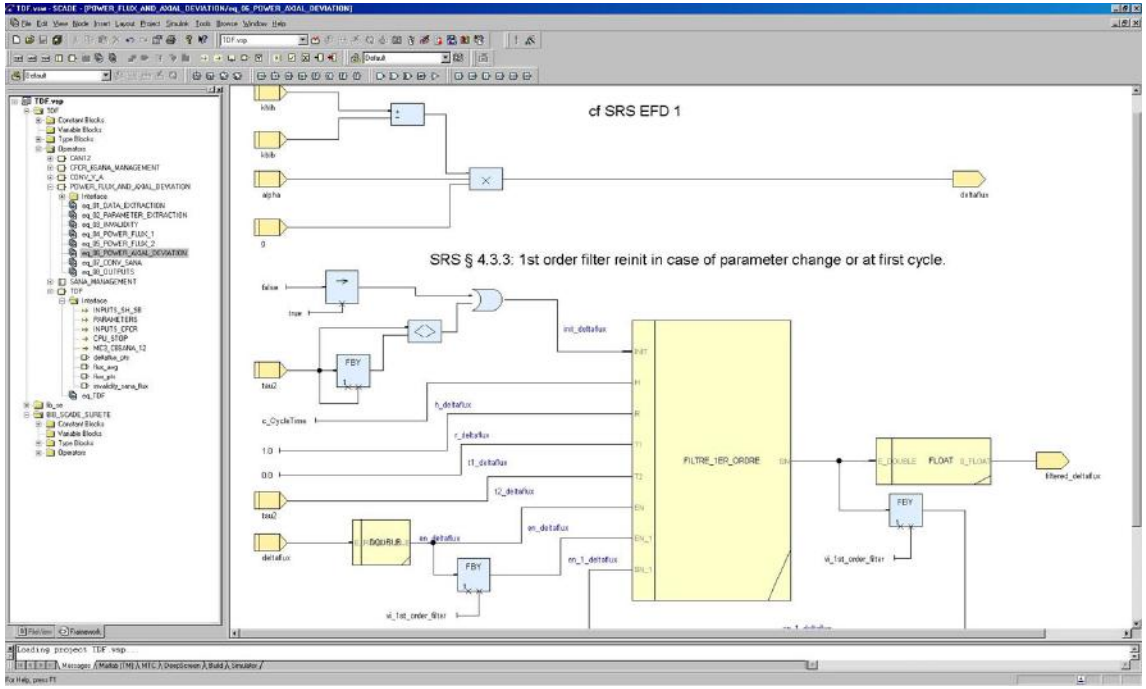
The SW development process with Clarisse SDDE



Rolls-Royce

Spinline software

Plant specific application development with Scade



- controlled language : no loops, no interrupts, no dynamic memory allocation
- includes semantics checks : completeness, type consistency, initial data, deadlock
- used in critical systems (Airbus, Eurocopter, railways signalling)
- compliant with requirements of IEC60880

Rolls-Royce

Spinline software

CLARISSE SDDE - Software binary production

Input of data

Application functions description

Hardware & networks configuration

SCADE editor

Configuration tool

Compiling & Assembling

Building

SCADE C code generator

ANSI C compiler

680x0 Assembler

Operational system software

Linker

binary code generator

Executable software

Secured operation
- Defensive programming
- Write-protected software
- Physical access to the CPU board is needed for modifications

Rolls-Royce

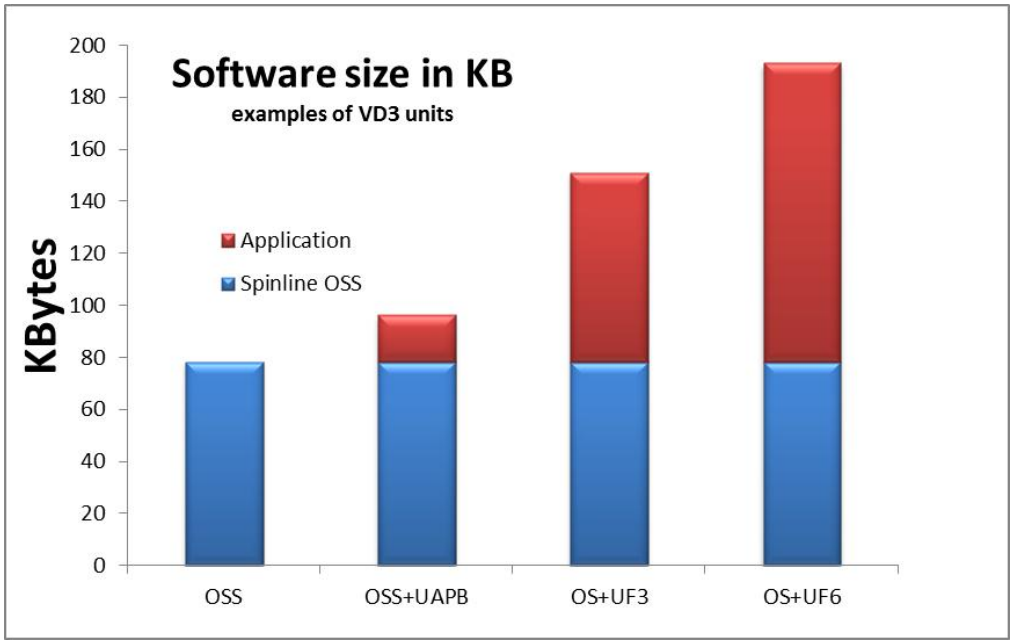
Spinline software

Final characteristics for assessments

Safety and Transparency

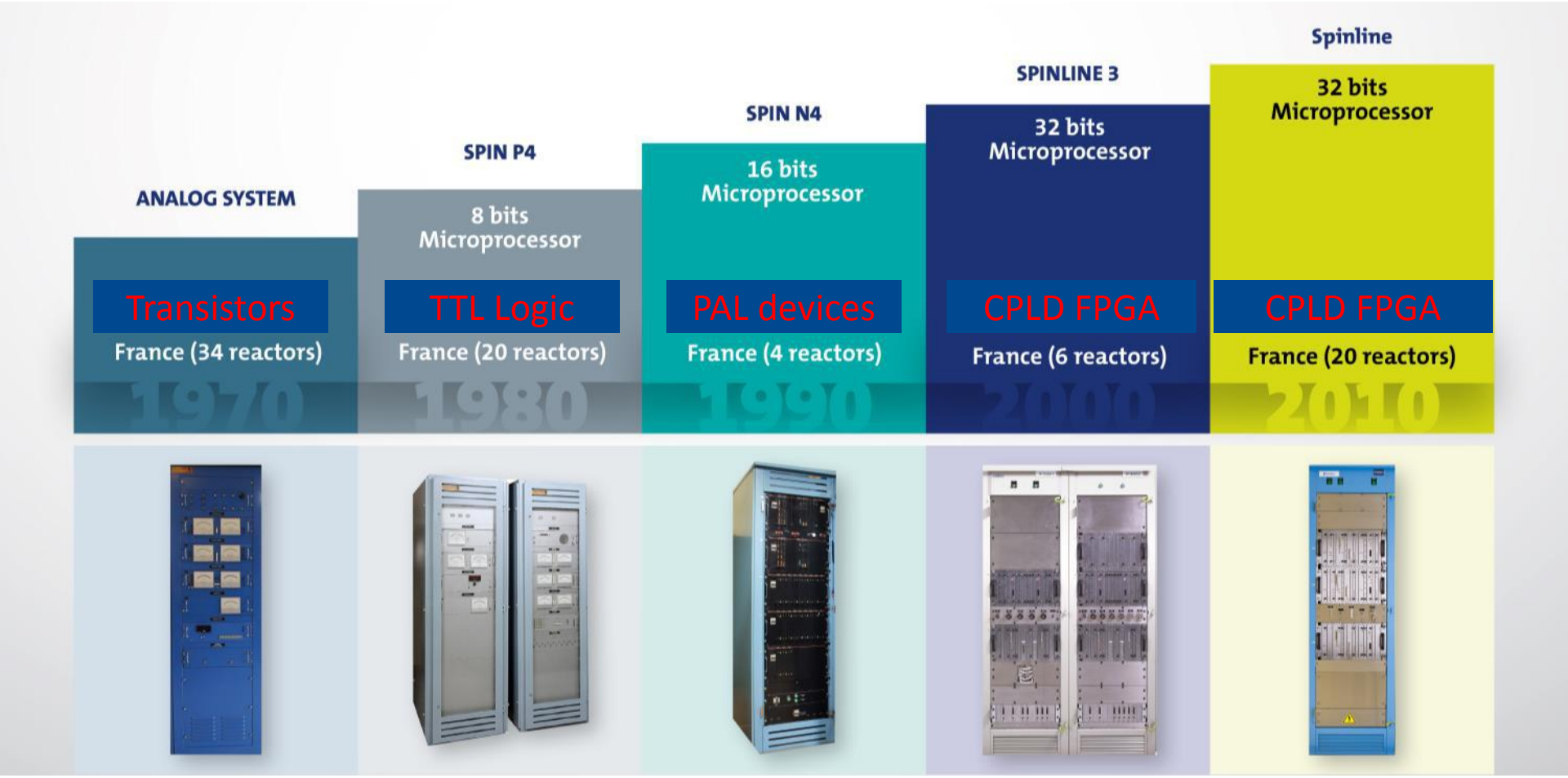
- All safety software components are available and reviewable
- C language are commonly known and tools exist for third parties evaluation
- Function block diagrams description are close to specifications and easy to ready
- No Safety software black boxes

Size



Rolls-Royce

Historical use of FPGA at Rolls-Royce I&C



Rolls-Royce

FPGA at Rolls-Royce I&C

FPGAs used to provide hardware design solutions ranking from

- simple electronic functions internal to hardware devices (in the context of dedicated hardware or programmed logic boards)
- implementation of complex application functions

In the design of electronic boards :

- existing boards, boards foreseen to be refurbished and additional new boards.

Higher level of complexity used for specific non safety equipment

- ex Implementation of rod control system – cycler (France 900MW)

Rolls-Royce

Design of electronic boards for class 1 equipment

32 Actuator Board design

FPGA

Previous actuator board:
1 microprocessor + logic circuits;

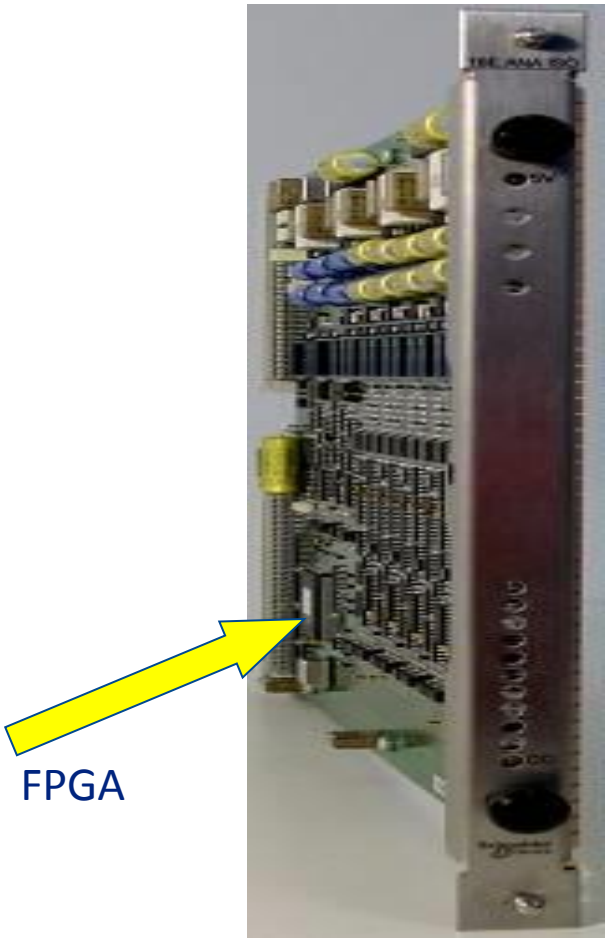
New actuator board (on the left):

- Electronic function implemented in an Actel FPGA
- 30 000 gates
- Performs the following functions :
  - Bus interface
  - Processor interface (registers)
  - Surveillance of the outputs, using a short impulse test
  - Board self-tests
- All other components on the board are analog components

Rolls-Royce

Design of electronic boards for class 1 equipment

16 analog inputs board



Previous analog board: 1 microprocessor + logic circuits; 6 analog channels per board

New analog board:

- The electronic function is implemented into an Actel FPGA
- 40 000 gates
- Performs the following functions :
  - Interface with the bus
  - Interface with the processor (dual ported ram)
  - Control of acquisition (16 inputs in 1 ms)
  - For each input, processing of the input value for gain and offset adjustment, performed by an Arithmetical and Logic Unit
  - Board self-tests
- All other components on the board are analog components

Rolls-Royce

Design of electronic boards for class 1 equipment
FPGA Design Flow

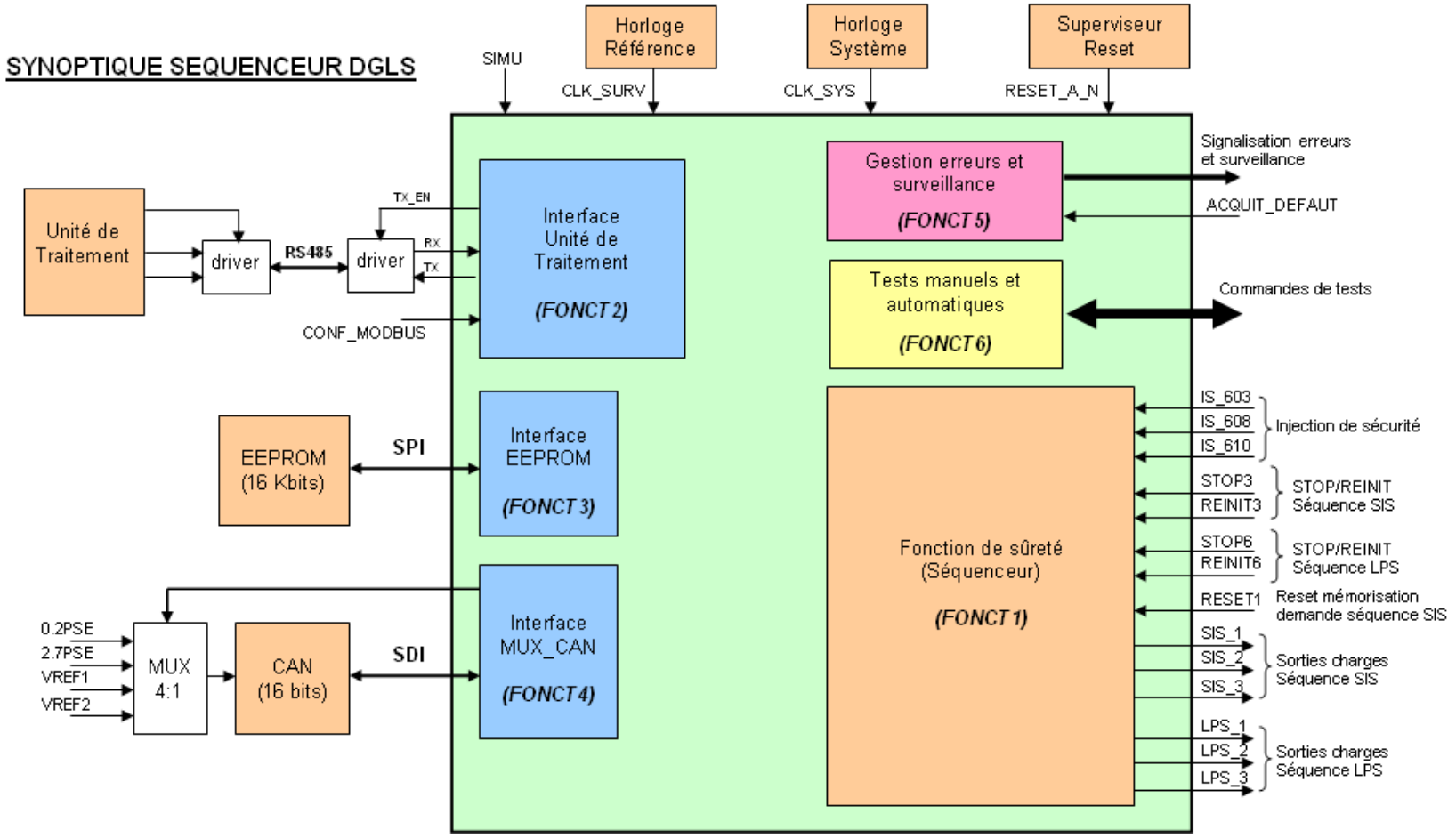
- Successfully used for all electronic functions design
- Compliant with IEC62566
- Entirely and exclusively applied in the Hardware electronic department
- **Applied to more than 15 class1 boards**

Board Design Process :
- simulation ,
- prototypes tests (PROTO1, PROTO2, …)

Rolls-Royce

FPGA Thoughts about a Class 1 application (R&D)

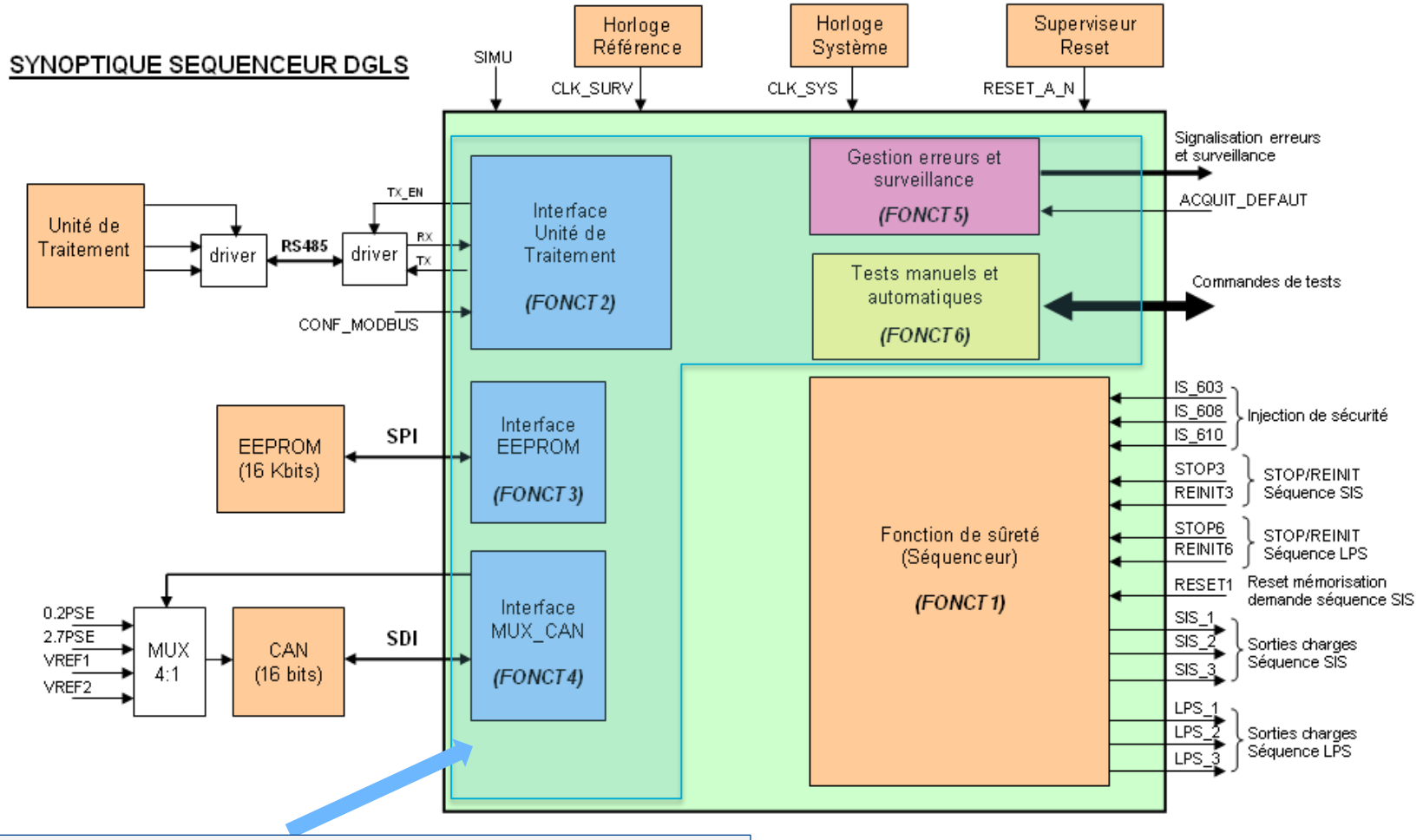
Top level specification of a Diesel Generator Load Sequencer



Rolls-Royce

FPGA Thoughts about a Class 1 application (R&D)

Top level specification of a Diesel Generator Load Sequencer



Equivalent to an Operational System Software

Rolls-Royce

FPGA thoughts about the use of the technology

- **Clear advantages for electronic functions**
  - Flexibility and ease for implementing hardware functions
  - Reduction of discrete components, higher board reliability
  - Replacement of sensible components (adjustment pot)
- **Need for skills attention**
  - Design and test activities require dedicated skills with electronic hardware background rather than System or software background
  - Coding HDL differs significantly from software coding
  - Architecture of the FPGA and targeted design within the FPGA must be well understood and drives the design beyond the functions to implement
- **Need for technical attention**
  - No ease for floating point format calculation, developing an FPU is needed,
  - no mathematic functions, no algebraic, no Elementary transcendental functions
  - Embedded self tests, Definition of safe states,
  - Partitioning, separation, local specific redundancy, parallel propagation
  - Design and testing tool behavior
  - Parameter handling (conditions for updates)

About licensing of Spinline

3 cases:

- UNITED STATES, US NRC*:*
  - Spinline : safety evaluation of the Spinline generic platform,
- FRANCE, ASN/IRSN:
  - EDF - VD3 1300MW : Plant specific project

    20 NPP refurbishment currently in deployment phase,
- FINLAND, STUK,
  - FORTUM - ELSA project : Plant specific project

    refurbishment of I&C systems at the Loviisa NPP in progress

Rolls-Royce

Spinline generic assessment - US NRC (1)

NRC RAIs LTR and documentation reviews :

The NRC staff submitted 3 sets of Requests for Additional Information (RAIs) representing 67 questions/comments covering:

- Process and procedures :
- Technical clarification

- All topics explained, understood and accepted by the NRC

NRC Factory audit:

- NRC one week audit with IRSN France as an invited party to share the audit content and outcomes
- aimed to more communications about procedures, complex technical information and access to low-level details.

US NRC audit report :
"The audit team lead indicated that all audit objectives were satisfactorily met. No open items or concerns were identified."

Rolls-Royce

Spinline generic assessment - US NRC (2)

the US NRC evaluation in a nutshell:

- In 2009, Rolls-Royce submitted the initial LTR for the acceptance evaluation
- In 2010, the evaluation project was launched by the US NRC
- The NRC staff submitted 3 sets of RAIs filled-in by Rolls-Royce
- The NRC performed hardware qualification audit and factory audit

- **In September 2014, the NRC finalized the SER**

US/NRC : “No generic open items or unusual plant-specific open items are needed to be addressed by an applicant or licensee referencing the topical report”

Rolls-Royce

VD3 1300 MW project : EDF- IRSN/ASN (1)

Specific licensing aspects for the software

- EDF fully independent software testing
  - all final VD3 1300 MW software source code
  - quality assessment of the code
  - robustness assessment of the code
  - 3 different departments of EDF involved

- IRSN fully independent additional software testing
  - Selected final software testing
  - dedicated purposes for IRSN

- **no critical issue are identified**

Rolls-Royce

VD3 1300 MW project : EDF- IRSN/ASN (2)

the VD3 1300 MW project in a nutshell:

- Rolls-Royce started the project at end of 2010

- The overall licensing in 2 parts:
  - the generic Spinline platform
  - plant specific project
- 180 documents licensing related,

This project is currently the world largest I&C modernization program

- **At the end of 2014, the final assessment of IRSN has been officially published :**

IRSN : “The Spinline platform is fully suitable for the development of class 1 equipment and for category A functions.”

Rolls-Royce

LOVIISA ELSA project : FORTUM - STUK (1)

“Independent Type approval” of the Spinline platform:

- The type approval process aims to get certificates from a third party independent from the supplier
- Accreditation ISO 17020, ISO 17025 or IS0 17065
- Rolls-Royce contracted the activity with the German company “ISTec TUV Rheinland”
- The assessment covered in detail more than 40 documents completed by more than 150 referenced documents
- It has started in mid 2014 and has been finalized for all existing parts in September 2016
- **4 certificates : Hardware, Software, software tools, FPGA**
- **Completed by the Type approval report**


Inspection Certificate

Inspection certificate regarding Type Approval based on the assessment of the equipment design and the quality management of manufacturing for the digital safety I&C platform Spinline

Certificate No 968/INS 126.00/16

Client / Certificate Owner Rolls-Royce Civil Nuclear SAS 23, chemin du Vieux Chêne 38246 Meylan Cedex France

Product Digital safety I&C platform Spinline to be used for nuclear safety systems (requesting framework: Finnish regulation - ELSA project)

Type designation Spinline platform software consisting of the following components:
- Operational system software (OSS)
- Application-oriented library of re-usable software
- Software embedded in the NERVIA communications board (firmware to implement the communication protocol) and software embedded in the ICTO pulse input board (firmware to implement acquisition of pulses)

The detailed list of the Spinline design criteria and of the components of the Spinline platform software is given in the Inspection Report 968/INS 126.00/16

Standards applied for inspection IEC 61513:2011, IEC 61500:2009, IEC 60880:2006

Inspection Results The independent inspection according to ISO/IEC 17020 has been passed successfully without functional remarkers. The Spinline platform software is suitable for application in safety systems of nuclear power plants. The Spinline platform design criteria and software comply with the requirements of the standards IEC 61513:2011, IEC 60880:2006 and IEC 61508:2009 regarding its documentation and development life cycle. The detailed assessment results, the assessed documents with the issue date and the software components with the version data can be found in the Inspection Report 968/INS 126.00/16.

Inspection Period 2014-06-17 - 2016-09-15

Validity The validity of the Spinline digital platform inspection and of the corresponding certificate is limited to five years.

Cologne, 2016-09-15

Dipl.-Ing. Heinz Gall

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Inspection Body of TÜV Rheinland Industrie Service GmbH
Business Area Energy Systems and Automation
Business Field Automation - Functional Safety www.tuv.com/nuclear

Accredited by DAkkS as Inspection Body acc. to DIN EN ISO/IEC 17020:2004

www.tuv.com

TÜVRheinland®
Precisely Right.

ISTec-TUV : “The report confirms that the Spinline and the hardwired platform conform to their specifications, and that the design and manufacturing processes are adequate to ensure high quality I&C products for implementation in systems important to safety in nuclear power plants.”

Rolls-Royce

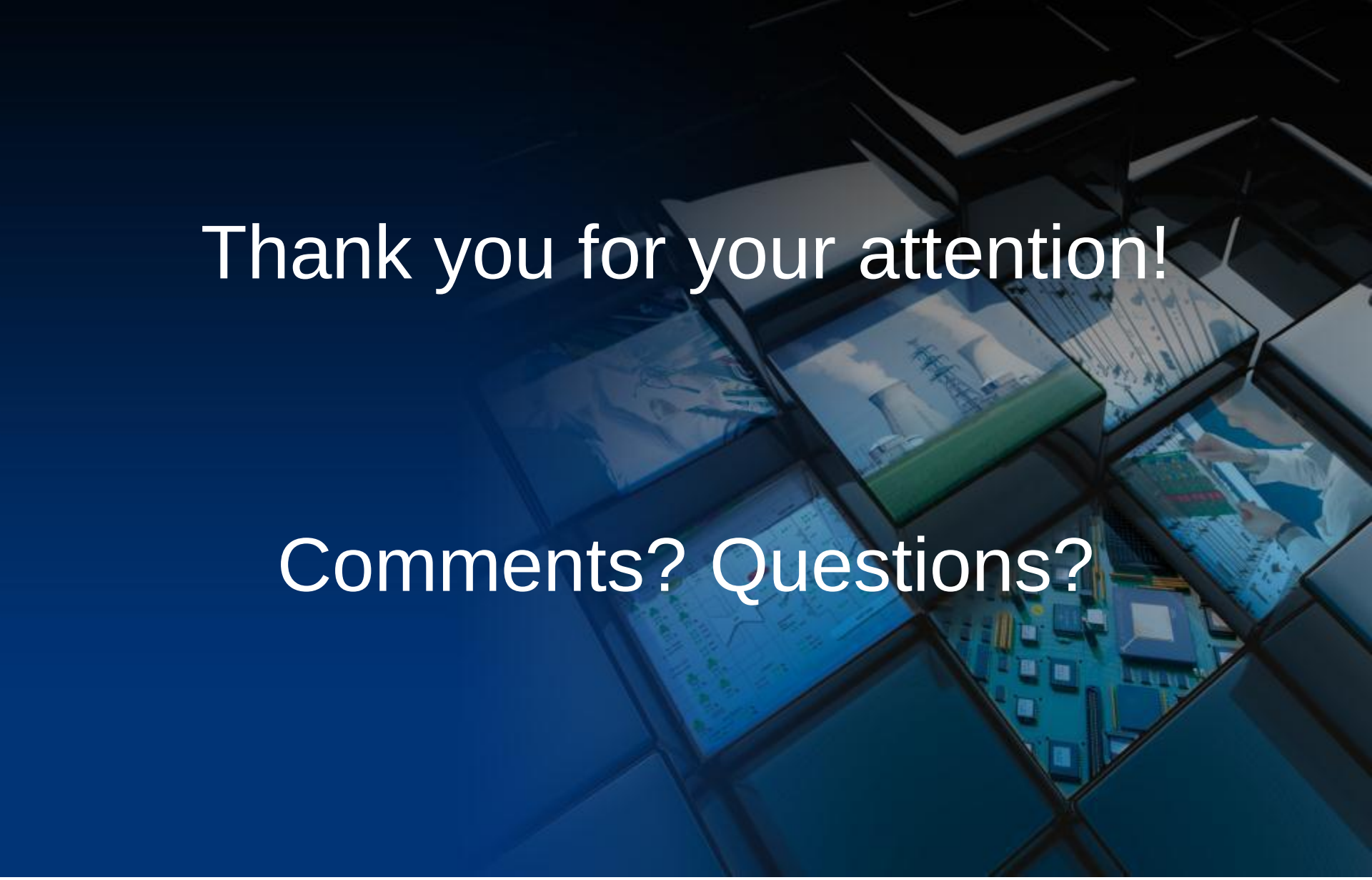
Conclusion

- **Both worlds, FPGA based or Software based, have their specific advantages and may be used to implement targeted functions,**
- **Both can be used efficiently and consistently for their most relevant field.**
- **A platform initially and entirely designed for nuclear I&C systems remains certainly a significant factor for safety demonstration.**

- **Spinline, including both technologies, has shown to be fully licensable within different international Regulatory frameworks**

- **The highest level of confidence stands certainly on the easiness:**
  - **to provide the safety evidences of the solutions**
  - **to reach the best common understanding among the stakeholders.**

Rolls-Royce



Thank you for your attention!

Comments? Questions?