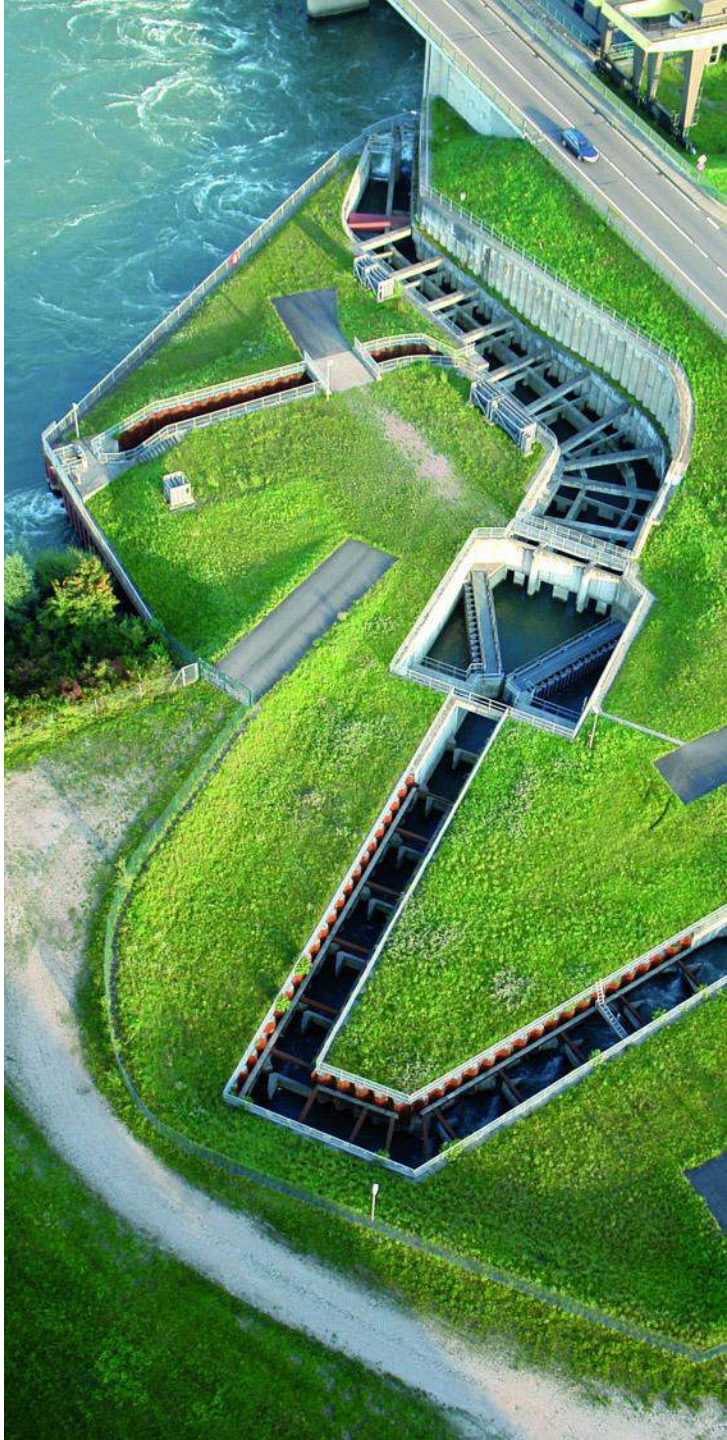
8th Workshop on the Application of FPGAs in NPPs

FPGA-Based I&C Systems : Unraveling Myths from Reality



EDF Nuclear Engineering Division, Basic Design (SEPTEN)

Alexander Wigg (alexander-john.wigg@edf.fr)
Ludovic Pietre-Cambacedes (ludovic.pietre-cambacedes@edf.fr)

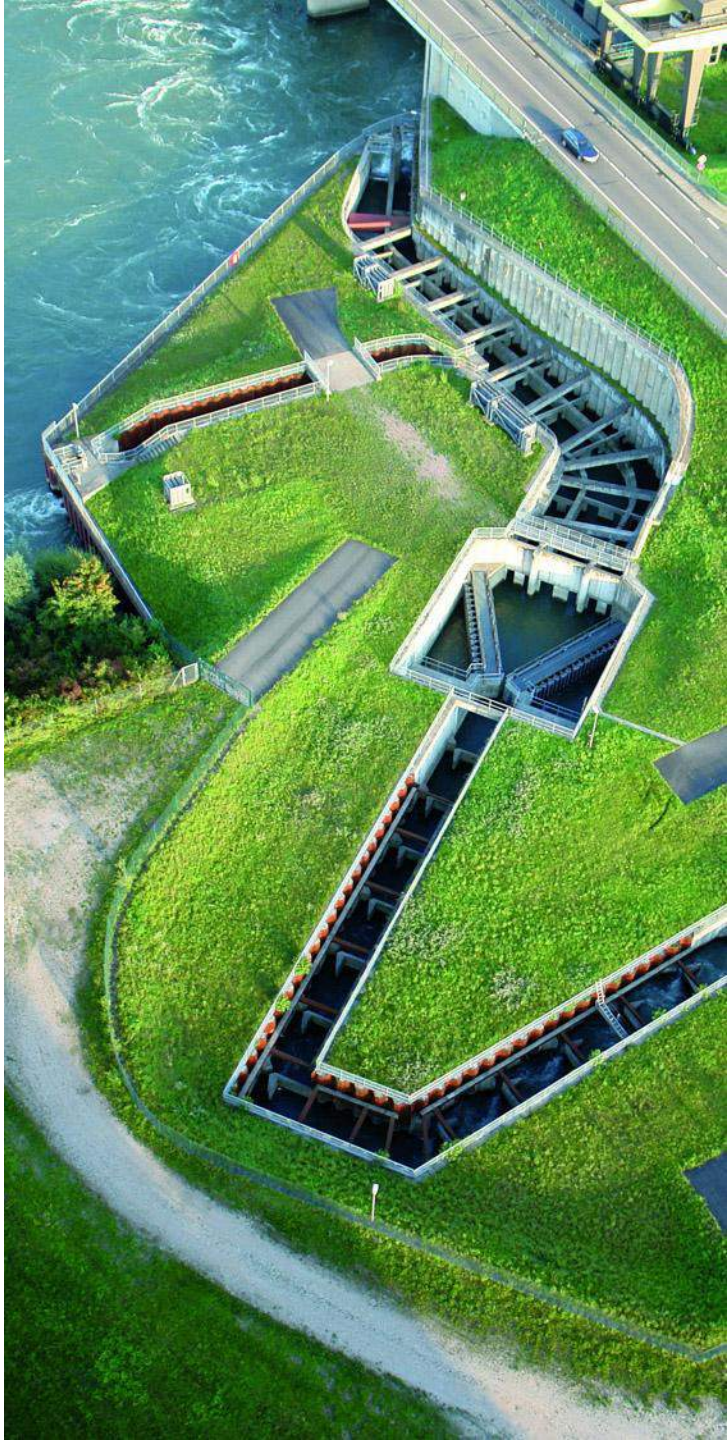
Presentation Plan :

1. Introduction

2. Key differences between FPGAs and microprocessors

3. Thematic analysis

4. Conclusions and recommendations



Introduction and objective

- Objective : To challenge biased information and misconceptions regarding FPGAs, to promote critical analysis and open discussion based on facts and real world experience.

  - *EDF does not support or promote the use of one particular technology over another.*

Introduction and objective

The problem with how FPGAs are regarded in the nuclear industry :

Theme	In the beginning…
Qualification	No software so easy to qualify
Cybersecurity	Immune to viruses
Deterministic behaviour	Pure hardware solution so deterministic behaviour
Performance	Faster response times
Obsolescence	Transferrable code, no obsolescence issues

Introduction and objective

The problem with how FPGAs are regarded in the nuclear industry :

Theme	In the beginning…	Now…
Qualification	No software so easy to qualify	Difficult to qualify, but at least there is no operating system with FPGAs
Cybersecurity	Immune to viruses	Viruses are not the only issue, but FPGAs have certain advantages
Deterministic behaviour	Pure hardware solution so deterministic behaviour	Pure hardware solution so deterministic behaviour
Performance	Faster response times	Faster response times
Obsolescence	Transferrable code, no obsolescence issues	Code is transferrable, but FPGAs do, in fact, become obsolete

Introduction and objective

The problem with how FPGAs are regarded in the nuclear industry :

Theme	In the beginning…	Now…
~~Qualification~~	~~No software so easy to qualify~~	~~Difficult to qualify, but at least there is no operating system with FPGAs~~
~~Cybersecurity~~	~~Immune to viruses~~	~~Viruses are not the only issue, but FPGAs have certain advantages~~
~~Deterministic behaviour~~	~~Pure hardware solution so deterministic behaviour~~	~~Pure hardware solution so deterministic behaviour~~
~~Performance~~	~~Faster response times~~	~~Faster response times~~
~~Obsolescence~~	~~Transferrable code, no obsolescence issues~~	~~Code is transferrable, but FPGAs do, in fact, become obsolete~~

Presented in this manner, the offered “advantages” in fact have very little to do with FPGA technology.

Key differences between FPGAs and microprocessors

- Whether the fundamental distinction between hardware and software matters or not will need to be determined on a national level through discussions between equipment suppliers, plant operators and regulatory bodies :
  - *At EDF, this distinction is not of huge importance.*
  - *IEC nuclear standards define **objectives**, rather than **means** (contrary to IEC 61508). Qualification is simply a demonstration that the process has been followed and that the objectives are met.*
  - *Either FPGAs or microprocessors allow the objectives to be fulfilled, **subject to suitable design and implementation of the technology.***

- The fundamental differences in operating principles can however have an impact on the choice of technology for a particular application.

Thematic Analysis – Simplicity and deterministic behaviour

- It is true that FPGA-based platforms do not use operating systems...
- …but neither do their “rival” software platforms (i.e. 1E platforms).
- The main difference is the absence of *task schedulers*, used in common operating systems. Task schedulers manage requests for resources from applications and introduce uncertainty into system behaviour.
- Both software and FPGA-based 1E platforms have system code, essential for platform management tasks, auto-tests etc..
- The absence of ‘operating systems’ or ‘unused functionalities’ is a requirement according to IEC standards, regardless of the technology.
- Software-based 1E nuclear I&C platforms are completely different to COTS platforms.

Software ≠ Operating System

Thematic Analysis – Simplicity and deterministic behaviour

- Arguments for simplicity seem to be based on an older and idealistic understanding of FPGAs.
- Modern FPGAs and the associated tools are extremely complex, comprising millions of logic elements and flip-flops, the final implementation of which can be difficult or impossible to control.
- Poorly designed clock signals in FPGAs can result in unpredictable behaviour, even in synchronous designs.
- The need to apply “software-like” standards results from this complexity, not from the similarity of the development processes.

Pure hardware ≠ deterministic behaviour

Thematic Analysis – Obsolescence

- The COTS market drives functionality and the need for complexity .
- COTS suppliers also *want* their products to become obsolete.
- This makes COTS generally unsuitable for nuclear applications.
- This mechanism applies to microprocessors **and** to FPGAs.

The same principles apply for nuclear products, although cycles are longer due to the smaller market, certifications, which discourage design changes, as well as long term maintenance contracts with suppliers.

- In modern FPGAs, the use of vendor-specific functionalities is inevitable for all but the simplest of functions. Proprietary IPs have become their main selling point.
- The utility will typically have no influence in how code is written, how portable it is, nor will they have the rights to implant it on different hardware, even if it is possible.

Software and HDL can <u>both</u> be designed to be portable

Thematic Analysis – Cybersecurity

Common Argument	Analysis
"FPGA-based systems are less vulnerable to cyber-attacks than microprocessor-based ones"	For attacks targeting executable code, FPGAs may have some advantages, but other attacks are in fact much more common.
"FPGA-based systems can be designed without high-level, general purpose components which are easily attacked"	No 1E platform is designed using general purpose components.
"FPGA re-programming can be possible only by physical access, or anti-fuse FPGAs can be used"	A software platform could also be designed in this way. Very few products use anti-fuse FPGA technology.
"IP cores can be verified to be free of hidden or unnecessary capabilities"	What is true for HDL is also true for software. For class 1, black box components are prohibited. For class 2 or 3, which may use COTS, access to source code may not be allowed, whether it's software or HDL.

Thematic Analysis – Licensing and qualification

Problem : How to treat FPGAs compared to software?

- In France, software-based protection systems were qualified well before appropriate software standards existed.
- Such real-world experience is essential for the development of relevant and industrially applicable standards.
- The need for software standards arose from increasing complexity of systems.

Therefore, the need for FPGA standards is a result of their complexity, not of their "resemblance" to software, despite the fact that they are in the end purely hardware.

Processes/standards should be *as rigorous as they are for software*, but *adapted to the specific nature of FPGAs*.

Conclusion and recommendations

- In COTS components, FPGAs and microprocessors are used concurrently in a complementary fashion. FPGAs are fundamentally better for some applications (parallel high-speed processing), and microprocessors for others (floating point).
- Software-based safety platforms also use FPGAs for some peripheral tasks, and vice-versa, due to their suitability for them.

FPGAs and software are not rivals, they are different.

- Improved portability, simplicity and deterministic behaviour: these arguments are based on an older and idealistic understanding of FPGAs, and perhaps a lack of knowledge of current software-based safety platforms, which bear little resemblance to the COTS with which FPGAs are so often compared.
- The choice of technology alone tells you very little about your final system.

The decision to use FPGAs or not should be based more upon the functional requirements of the system, and less upon the hope of them being an easier option to qualify than software.

Conclusion and recommendations

	In the beginning…	Now…	After analysis
Qualification	No software so easy to qualify	Difficult to qualify, but at least there is no operating system with FPGAs	Technology independent. Design dependent
Cybersecurity	Immune to viruses	Viruses are not the only issue, but FPGAs have certain advantages	Technology independent to an extent. Design dependent
Deterministic Behaviour	Pure hardware solution so deterministic behaviour	Pure hardware solution so deterministic behaviour	Technology independent. Design dependent
Performance	Faster response times	Faster response times	Technology independent. Design dependent.
Obsolescence	Transferrable code, no obsolescence issues	Code is transferrable, but FPGAs do, in fact, become obsolete	Technology independent. Design dependent.

FPGA-BASED I&C SYSTEMS: UNRAVELING MYTHS FROM REALITY (POSTION PAPER)

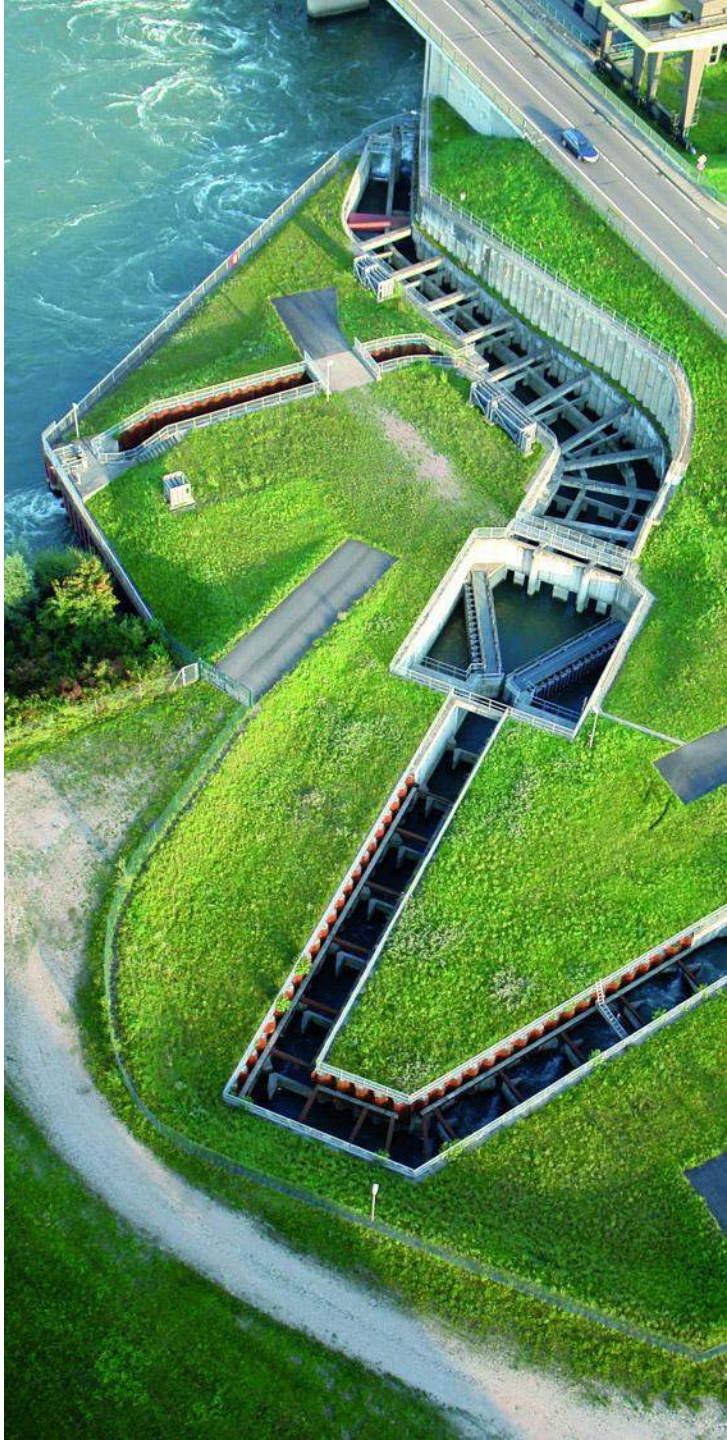
Alexander-John Wigg, Ludovic Pietre-Cambacedes
EDF Nuclear Engineering Division, Basic Design (SEPTEN)
12-14 avenue Dutriévoz, 69628 Villeurbanne, France
{alexander-john.wigg, ludovic.pietre-cambacedes}@edf.fr

ABSTRACT

This article presents a critical analysis of FPGAs compared to microprocessors with regards to their fundamental differences and, importantly, to their use in systems for nuclear power plants based on this technology. This analysis covers in particular the following issues: safety, performance, maintenance, cybersecurity, obsolescence, renovations, licensing and qualification. The resulting advantages and disadvantages of FPGAs compared to microprocessors are often presented in an over-simplified manner. This situation can create confusion regarding the distinction between properties that are inherent to the underlying technology and those that depend upon the specific product. This article provides explanations and analyses to inspire a deeper understanding of the aforementioned issues, and to help readers to better unravel myths from reality regarding FPGA-based I&C systems.

Key Words: FPGA, I&C, cybersecurity, digital, licensing

Thank you for your attention.



EDF Nuclear Engineering Division, Basic Design (SEPTEN)

Alexander Wigg (alexander-john.wigg@edf.fr)
Ludovic Pietre-Cambacedes (ludovic.pietre-cambacedes@edf.fr)