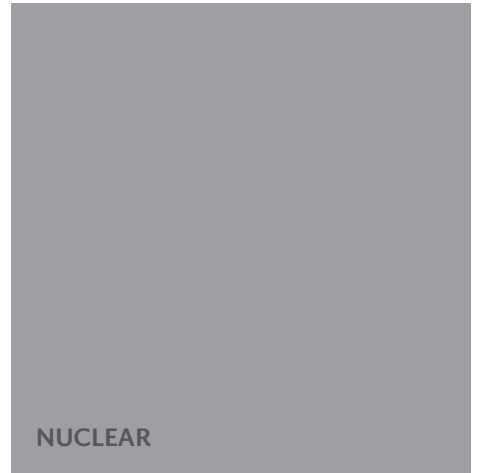


FIELD PROGRAMMABLE GATE ARRAYS IN SAFETY RELATED INSTRUMENTATION AND CONTROL APPLICATIONS

REPORT 2015:112



Field Programmable Gate Arrays in safety related instrumentation and control applications

Nordic Nuclear Power Plants

CATHERINE MENON AND SOFIA GUERRA, ADELARD LLP

ISBN 978-91-7673-112-3 | © 2015 ENERGIFORSK

Energiforsk AB | Phone: +468-677 25 30 | Email: kontakt@energiforsk.se | www.energiforsk.se

Preface

This report is produced by Adelard LLP for Energiforsk within the research program ENSRIC, Energiforsk Nuclear Safety Related Instrumentation and Control systems. The objective of the project was to develop an overview and understanding of the position of safety related systems built on FPGA-technology (Field Programmable Gate Arrays) for nuclear applications. FPGAs have been gaining interest from the nuclear industry for a number of years. Their simplicity compared to microprocessor-based platforms is expected to simplify the licensing approach, and therefore reduce licensing risks compared to software-based solutions. Are FPGA-based systems a realistic alternative in future investment programs in the Nordic NPPs within the next 5 years, considering technological advancement, licensing, market situation etc.?

ENSRIC is focused on safety related I&C systems, processes and methods in the nuclear industry. The three focus areas of the program are emerging systems, life time extension and I&C overall. Information from the program will assist the nuclear industry and the Radiation Safety Authority when analyzing how to replace systems and methods - choosing a new technology or finding a way to stay with the present solution - with maintained safety and promoting a low life cycle cost. The program is financed by Vattenfall, E.On, Fortum, TVO, Swedish Radiation Safety Authority, Skellefteå Kraft and Karlstad Energi.

Summary

This report discusses the use of Field-Programmable Gate Arrays (FPGAs) in safety related nuclear applications, with an emphasis on their use in the Nordic environment.

We first provide some background on FPGAs, and discuss their advantages and disadvantages for use in nuclear applications. We then discuss the use of FPGAs in safety-critical applications, with a particular emphasis on their use and approval in nuclear applications. We identify the major suppliers of FPGA chips and FPGA-based platforms, and discuss their major product families and licensing status. We go on to identify standards used in the development of FPGAs and FPGA-based platforms, as well as standards used in the licensing of these applications. We conclude with a review of the Nordic licensing environment and its position with regards to the use of FPGAs.

We have identified a number of advantages of FPGA-based systems, such as their ability to process independent functions in parallel and hence reduce overall function execution time. Other advantages include the easier separation of logically independent functions, their reduced vulnerability to obsolescence, their security advantages and their ability to constitute a technologically diverse implementation when used alongside a traditional microprocessor-based system.

Disadvantages we have identified include the relatively limited prior experience of the nuclear industry with FPGAs, their unsuitability for some complex functions which include human factors applications, and the potential difficulty in justifying the use of IP cores, or pre-developed FPGA-specific libraries.

Within the nuclear industry, we have identified a number of applications of FPGA usage across multiple regulatory regimes. These include the US regime, where FPGAs have been used in the Wolf Creek NPP, the Diablo Canyon NPP, and proposed for use in the South Texas NPP. The primary platform suppliers in the US have so far been Westinghouse and Toshiba.

In Canada, FPGA-based systems have been incorporated into NPPs since the 1990s, with the Darlington NPP. The primary platform supplier in Canada, and for Canadian companies, has been Radiy. As well as their work in Canada, Radiy are also responsible for supplying a number of FPGA-based systems in Ukraine and Bulgaria.

Other regimes which have accepted the incorporation of FPGA-based elements include China, Japan, Taiwan, South Korea and Sweden. These are discussed in more detail in the report as follows.

Sammanfattning

Rapporten diskuterar användningen av FPGA i säkerhetsrelaterade nukleära tillämpningar, med betoning på deras användning i ett nordiskt perspektiv.

Vi ger först lite bakgrund om FPGA, och diskuterar deras fördelar och nackdelar för användning i nukleära tillämpningar. Vi diskuterar därefter användningen av FPGA:er i säkerhetskritiska tillämpningar, med särskild tonvikt på deras användning och godkännande i nukleära tillämpningar. Vi identifierar de största leverantörerna av FPGA-chips och FPGA-baserade plattformar, och diskuterar deras viktigaste produktfamiljer och licensieringsstatus. Vi fortsätter med att identifiera standarder som används i utvecklingen av FPGA och FPGA-baserade plattformar, samt standarder som används vid licensiering av dessa tillämpningar. Vi avslutar med en genomgång av de nordiska regelverken för licensiering och dess syn när det gäller användning av FPGA.

Table of Contents

1	Introduction	8
2	Background on FPGAs	9
2.1	Technical overview	9
2.1.1	Development process	10
2.1.2	Verification and validation	13
2.1.3	IP cores	13
2.2	FPGA advantages	13
2.3	FPGA disadvantages	15
3	Review of installations in safety-critical applications	16
3.1	FPGA nuclear applications in the United States	16
3.1.1	Wolf Creek Feedwater Isolation System Replacement	16
3.1.2	Diablo Canyon	18
3.1.3	South Texas Project Advanced Boiling Water Reactor	20
3.1.4	AP1000 use in the US	21
3.1.5	NuScale Power Small Modular Reactors (SMRs)	22
3.1.6	San Onofre	22
3.2	FPGA nuclear applications in the United Kingdom	22
3.2.1	Gag Vibration Monitor	22
3.2.2	Hitachi ABWR	22
3.2.3	AP1000	23
3.3	FPGA nuclear applications in Canada	24
3.3.1	Canada Darlington Digital Control Computer (DCC)	24
3.3.2	Darlington	25
3.3.3	Pickering	25
3.4	FPGA nuclear applications in Argentina	25
3.5	FPGA nuclear applications in France	25
3.5.1	EDF 900 MW Series	25
3.5.2	Motorola 6800 Replacement	26
3.5.3	Rady I&C system	26
3.6	FPGA nuclear applications in Japan	27
3.6.1	Advanced Boiling Water Reactor Plant, Japan	27
3.7	FPGA nuclear applications in Ukraine and Bulgaria	28
3.7.1	Rady Digital Platform, and Kozloduy Units 5 & 6, Bulgaria	28
3.7.2	Other systems in Bulgaria and Ukraine	29
3.8	FPGA nuclear applications in Taiwan	30
3.9	FPGA nuclear applications in South Korea	30
3.10	FPGA nuclear applications in China	31
3.10.1	AP1000 variants	31
3.10.2	CAP-1400 and NuPAC	31
3.10.3	Other systems	31
3.11	FPGA nuclear applications in the Czech Republic	32
3.11.1	Temelin NPP	32
3.12	FPGA nuclear applications in Sweden and Finland	32
3.12.1	Olkiluoto	32
3.12.2	Ringhals	32
3.13	FPGAs in non-nuclear applications	33
4	Market availability of FPGAs	35
4.1	Chip suppliers	35
4.1.1	Xilinx	35

4.1.2	Altera.....	36
4.1.3	Microsemi.....	37
4.2	Platform suppliers.....	39
4.2.1	Rady.....	39
4.2.2	Westinghouse.....	41
4.2.3	Lockheed Martin and SNPAS.....	42
4.2.4	Other suppliers.....	44
5	Standards and Nordic environment	45
5.1	General nuclear plant standards.....	45
5.2	Digital I&C equipment in a nuclear power plant.....	46
5.3	Software development methodologies.....	47
5.4	FPGA-specific.....	48
5.5	Nordic standards.....	49
5.5.1	YVL B.1.....	49
5.5.2	YVL E.7.....	50
6	Conclusions	51
7	Glossary	52
8	Bibliography	54
9	Nordic standards and FPGAs	62

1 Introduction

This report discusses the use of Field Programmable Gate Arrays (FPGAs) in safety related nuclear applications, with an emphasis on their use in the Nordic environment. Section 2 provides some background on FPGAs, and discusses their advantages and disadvantages for use in nuclear applications. Section 3 discusses the use of FPGAs in safety-critical applications, with a particular emphasis on their use and approval in nuclear applications. Section 4 identifies the major suppliers of FPGA chips and FPGA-based platforms, and discusses their major product families and licensing status. Section 5 discusses standards used in the development of FPGAs and FPGA-based platforms, as well as standards used in the licensing of these applications. This section also contains a review of the Nordic licensing environment and its position with regards to the use of FPGAs.

2 Background on FPGAs

This section provides some information on the history of FPGAs, on the way in which they are constructed and on the different types of FPGA.

2.1 Technical overview

Field-programmable gate arrays (FPGAs) are high-density logic chips with the ability to simulate any digital logic design. FPGAs contain blocks of logic gates and registers that can be interconnected to produce an application-specific processing function by loading a specific set of gate interconnections into the chip. That is, the logic functions are implemented directly in hardware.

In more detail, FPGAs consist of the following basic architectural entities.

- Configurable logic blocks, which can be used to implement any logic function (e.g. AND, XOR).
- Programmable I/O blocks connected to the configurable logic blocks and serving as electrical interfaces between the FPGA and external components.
- An interconnection grid consisting of wires which link configurable logic blocks together within the FPGA, and link the logic blocks to the programmable I/O blocks.
- Memory to store the application data. This is discussed in more detail below.

All FPGAs require the configuration of the interconnection wires and the logic blocks to be stored in memory. This can be implemented in one of three ways:

- Flash / EEPROM FPGAs store the configuration in non-volatile storage technology. These FPGAs maintain their configuration even without power, and so are ready for use immediately after programming. Flash is the modern evolution of EEPROM, but FPGAs which use both forms are still available.
- SRAM FPGAs store the configuration in volatile RAM cells. The configuration is lost when power is lost, so systems using this type of FPGA are required to store the configuration in external memory. To guard against corruption, these FPGAs calculate and monitor a checksum of their configuration.
- Anti-fuse FPGAs are FPGAs which cannot be re-programmed (that is, the configuration is burned into the FPGA). Like flash FPGAs, they retain their configuration during power loss.

The following table (taken from [1]) identifies the advantages and disadvantages of each of these types.

	SRAM	Antifuse	Flash	EEPROM
Speed	Worst	Best	Worst	Medium
Power	Varies	Near Best	Best	Worst
Density	Medium	Second	Best	Worst
Radiation	Worst	Best	Medium	Medium
Reprogrammable	Yes	No	Yes	Yes

Table 1: Comparison of FPGA types

It is sometimes the case that a system is referred to as an FPGA-based system when it contains both microprocessors and FPGAs. In this report, we focus on FPGA-specific systems, without microprocessors, unless explicitly stated otherwise.

2.1.1 Development process

FPGA development follows a traditional V-model, with associated verification and validation.

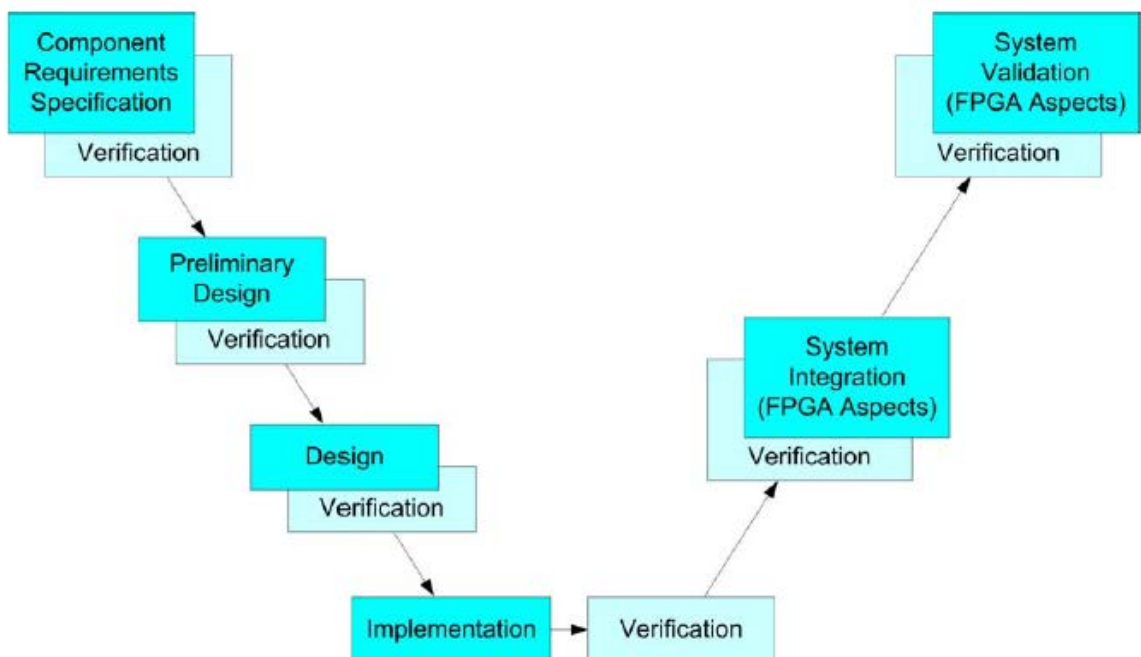


Figure 1: V-model lifecycle for FPGA development [1]

Artefact	Activity
Plant need	
	↗ ↘ Requirements capture
Requirements specification	
	↗ ↘ Design and coding process
HDL source code or schematic diagram Register-Transfer-Level description	
	↗ ↘ Implementation: Synthesis
Netlist (gate-level description)	
	↗ ↘ Implementation: Place and route
Bitstream (binary image to be loaded on to the FPGA)	
	↗ ↘ Instantiation on hardware
Observed execution	

Table 2: Tabular representation of the FPGA development process

Requirements capture

During this phase all requirements which relate to the desired FPGA functionality are specified. Requirements capture for FPGAs is not significantly different to the corresponding activity for any other system. The requirements, which at this stage are circuit-independent, should also be validated.

Design and Coding

In this phase a detailed description of the FPGA functionality is produced. This is analogous to the production of software code to define the functionality of a software system. The FPGA application functionality is typically defined using a high-level hardware description language (HDL), such as VHDL or Verilog, and a number of tools and development kits are commercially available for development and validation of the HDL code. It is also possible to generate the HDL from a higher level description, such as C or Matlab [72] [11]. Schematic diagrams may also be used instead of HDL, but these are typically

only useful for simple cases which are not large-scale or complex [11]. The HDL code (or schematic diagrams) produced from this stage is independent of any particular FPGA chip (this is termed circuit-independence). The most common level of description for the design is Register Transfer Level (RTL) representation, which describes the FPGA functions in terms of the flow of signals between logic blocks.

Implementation

Synthesis is the first step in the implementation phase, where the RTL is then synthesised to a *netlist*. A netlist defines the configuration for the particular FPGA application being designed, by identifying the gates required and their interconnections. This step is also referred to as logic synthesis, and commercial development tools are available for use at this stage. The netlist may be circuit dependent or independent, depending on the tools which are used.

Place and route is the second stage of implementation. This step identifies the best physical positions on the chip for the logic blocks and interconnections. The outcome of this stage is a bitstream, which can then be loaded onto the FPGA to program it.

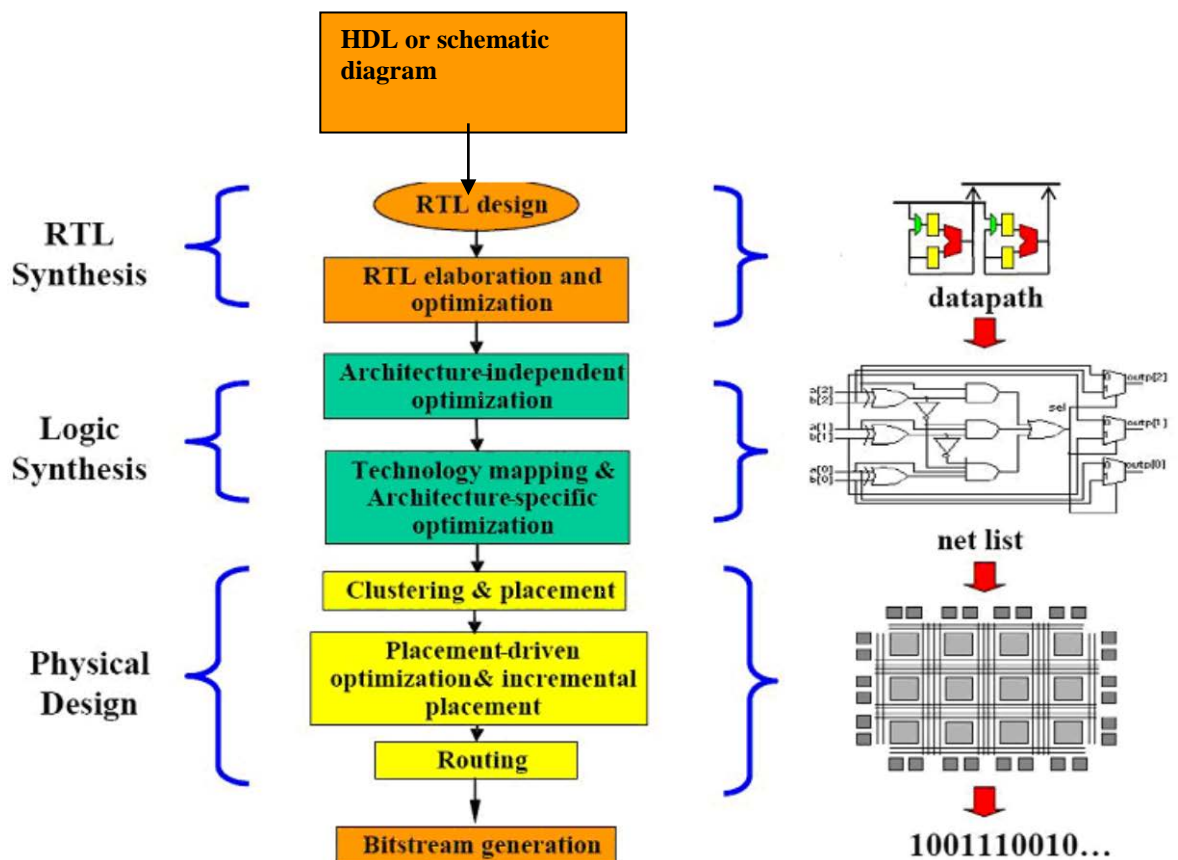


Figure 2: Representation of the design, coding and implementation stages [1]

2.1.2 Verification and validation

Verification of an FPGA-based system is typically undertaken after each stage of development [123]. Integration and validation are considered as part of system integration and system validation [89].

Verification of the requirements is typically performed by documentation review [89]. Verification of the design stage may be performed using a combination of documentation review, testing and formal verification [3]. The testing is usually simulation tests performed on the RTL representation, and is performed to detect logical errors or problems with the functionality. Formal verification may also be undertaken, at this stage. This typically makes use of tools to determine whether the required design properties are satisfied by the RTL [3].

At the implementation stage, simulation is again an important part of verification, and this is the first stage at which the timing aspects can be simulated. Static Timing Analysis (STA) may be used to document best and worst case timing performances and assess the time taken by the relational logic [89]. Formal verification may also be performed to ensure that the netlist is equivalent to the RTL, and black box testing to verify additional aspects relating to the functionality.

2.1.3 IP cores

IP cores are pre-developed libraries for performing certain functions, such as floating-point arithmetic, signal processing or communication protocols. IP cores are provided either by the circuit vendor or by an independent third-party and may be either circuit-dependent (requiring the use of a particular chipset or chip family) or circuit independent. In industry, these are known as "hard" and "soft" IP cores.

Concerns have been raised over the use of IP cores in safety-critical applications, as it may be difficult to assure the design and development to the standard needed. This is discussed further in Section 2.3 and Section 3.

2.2 FPGA advantages

Although FPGAs have been on the market for almost thirty years, their use in nuclear safety-critical applications has not been prevalent over that time. Nevertheless, they present a number of advantages over traditional micro-processor based systems.

Firstly, FPGAs are able to process independent functions in parallel, which can reduce the overall function execution time [72]. The clock cycle time of a microprocessor without this parallel implementation may be too long to meet a short overall function timing requirement.

Another advantage is the easier separation of logically independent functions offered by FPGAs. These are functions which share no logic blocks and no interconnections, and are therefore physically separated on the chip. This means that non-safety related functions can be separated from those which are safety-related, and also that it is easier to demonstrate that independent safety-related functions do not interfere with each other [1]. This can be

difficult on a microprocessor-based system, where these functions execute on a shared operating system and use shared software services. It should be noted, however, that arguments relating to independence of functions are limited, in that there is little physical separation of the relevant logic blocks, and the functions will be vulnerable to common cause failures (e.g. vulnerable to the same hardware failures in the chip itself).

FPGA-based systems are also less vulnerable to obsolescence and more easily portable. The reason for this lies in the development process described in Section 2.1.1. The first stages of these are circuit-independent, and so the logic can be re-used without modification even if a particular chip is discontinued. That is, alternative chips can be used for the FPGA without the need for a full re-qualification of the design [18].

Ready-made IP cores also offer an advantage when it comes to FPGAs. These are pre-existing libraries which can be used for implementing a wide variety of functions, and so reduce development time and effort. IP cores are supplied with differing amounts of verification information, and may provide some additional assurance from being proven in use. However, it should be noted that qualification of these in general may be an issue, and is discussed further in Section 2.3.

FPGAs can also offer security advantages. FPGA-based systems generally do not offer as many avenues for cyber security attacks, in that they do not contain components which are designed to perform generic functions, or which use generic interfaces. These components may be more easily used maliciously or to an unintended purpose. FPGA-based systems therefore reduce the possibility for altering programming or functionality, because these altered functions must be implemented as complete designs, rather than as side-effects of a more general purpose component [73]. Anti-tamper capabilities are also provided by some suppliers, which ensure that if an attempt is made to reverse-engineer the FPGA then it will destroy all information on it [120].

FPGAs are also considered in some cases as easier to justify and qualify than microprocessor-based systems [1] for a number of reasons. Firstly, they may be considered as inherently less complex because the logic is implemented in hardware, with signal paths from input to output. This is in contrast to microprocessors, where the interactions between the shared operating system, software services, peripheral hardware and related drivers must also be considered in a safety justification. Secondly, the US NRC has observed that licensing approval for microprocessor-based systems can be complicated because the internal workings of the microprocessor are proprietary and therefore not available for review [2] [101]. By contrast, the design of an FPGA can be made transparent up to the netlist level by the use of schematic diagrams showing the internal workings.

Finally, FPGAs are suitable for providing a diverse backup to traditional microprocessor-based systems. Diversity is emphasised in many of the applicable standards (see Section 5) and an architecturally diverse system consisting of FPGA-based and microprocessor-based implementations of the same functionality makes an argument of equipment diversity easier to support. However, it should be noted that where the FPGA emulates the

existing microprocessor implementation, the benefits of such technology diversity are less clear [8].

2.3 FPGA disadvantages

FPGAs are not suited to all safety-related applications. There are certain inherent limitations which can prove to be disadvantages when considered against microprocessor-based systems unless these are considered in the design and mitigated against.

The first of these is their relatively limited prior use in the nuclear industry. Because of this, there may be little cultural familiarity with FPGA-based systems, and appropriate standards and guidance have only been recently released. This has historically resulted in situations where licensing approval is delayed or complicated because of a lack of clarity over what is required to justify the use of an FPGA-based system. Although guidance is now becoming available, it is still limited and there is some uncertainty over regulatory expectations and interpretations [75].

A related factor is that, owing to the relatively novel status of FPGAs in the nuclear industry, there is not a large body of evidence regarding their performance in the nuclear field. This can make it difficult to justify a proven-in-use argument, or to select a supplier with the best track record. We note, however, that FPGAs have had a relatively sizeable history in other sectors for safety-related applications, and lessons may usefully be drawn from this, if evidence of this is available.

A third drawback relates to the relatively limited range of suppliers. Although this is now growing, historically this has meant a less diverse range of applications and development tools, which can then have an effect on the ability to justify an absence of common cause failure. The extent to which proprietary tools are verified is also variable, and the development process for these is usually not transparent to users.

FPGAs, while offering an advantage in terms of reduced complexity (see Section 2.2), are not inherently well-suited for complex human factors applications. These applications typically rely on existing pre-developed software, such as user interfaces, menus and windows programs. Such software exists, and has a demonstrable pedigree, for microprocessor-based systems but not for FPGAs to the same extent.

Finally, the use of IP cores in FPGA-based systems can raise concerns in terms of safety justifications. These pre-developed libraries are difficult to justify because they are not transparent, and the development process is typically not available to the user.

3 Review of installations in safety-critical applications

This section provides a review of FPGAs in safety-critical applications, with a particular focus on the use of FPGAs in the nuclear sector. We have categorised FPGA use in this sector according to licensing regime (which broadly equates to a categorisation by country). This is to clarify the different ways in which FPGAs have been approved for use around the world and to provide an overview of the different perspectives of the suitability of FPGAs in nuclear applications.

3.1 FPGA nuclear applications in the United States

3.1.1 Wolf Creek Feedwater Isolation System Replacement

The Wolf Creek NPP is a single-unit, Pressurized Water Reactor (PWR) that has been deployed since 1985 and is operated by Wolf Creek Nuclear Operating Corporation (WCNOC). This example concerns the replacement of the Main Steam and Feedwater Isolation System (MSFIS), a project which began in 2004, and was completed in 2009. It was the first US safety-related use of FPGAs in nuclear plants.

The MSFIS operates the main steam isolation valves and main feedwater isolation valves in the plant, and provides alarm and status information to operators. It responds to actuation signals from the Solid State Protection System (SSPS) and is classed as safety-related (Class 1E) equipment.

The initial replacement project, which was amended due to licensing difficulties, was for a replacement of the reactor protection system (RPS) and Engineered Safety Features Actuation System (ESFAS), comprising:

- MSFIS
- Load Shed and Emergency Load Sequencer
- Balance of Plant ESFAS
- Solid State Protection System
- Thermocouple and Core Cooling Monitor
- 7300 Protection Equipment
- Reactor Vessel Level Indication System

FPGA replacement

The Advanced Logic System (ALS), containing flash-based ProASIC FPGAs from Actel, was used for the MSFIS replacement. It was developed by CS Innovations, a subsidiary of Westinghouse. The FPGA was the APA600-BG4561 [15].

VHDL was used to specify the FPGA functions. The tools used to develop and verify the FPGA were not qualified, although CS Innovations did perform internal V&V to demonstrate that these were fit for purpose [1]. No IP cores were used. The new system was simulated in software, and tuning parameters transferred electronically.

History and licensing

FPGAs were chosen for this project because of previous difficulties in licensing the first option proposed in 2004 - a microprocessor based digital control system which was intended to replace the MSFIS and a number of other systems. The project risks associated with the replacement of all of these systems using a microprocessor was considered too large (given the licensing difficulties already encountered), and FPGAs consequently chosen for the most urgent replacement, the MSFIS.

The Nuclear Regulatory Commission (NRC) determined that the review of the FPGA-based system should be similar to the review of a traditional digital microprocessor system, i.e., that the same criteria would be applied. In particular, the NRC considered that programming in HDL was vulnerable to the same issues and concerns as traditional programming [15]. There was no nuclear guidance or applicable standards that were FPGA-specific at the time.

The ALS was designed to comply with CS Innovations 10 CFR 50 Appendix B QA program, and the FPGA component was assessed against IEEE 603-1991. The FPGA programming was performed in accordance with a version of IEEE 7-4.3.2-2003 adapted for FPGA use. Other standards that the system was assessed against during NRC review included NUREG 0800 Chapter 7, Interim Staff Guidance documents (e.g. ISG #6, "Licensing Process" [16]) and IEEE 1012.

The Wolf Creek FPGA system gained NRC approval in 2009. The Licensing Amendment Request (LAR) was submitted in 2007, and the Safety Evaluation Report [15] that acted as approval was issued in 2009. Information in this SER that could act as future guidance on process and FPGA approval was identified by the NRC staff. This was done with the intention that it should be used as guidance for future safety-related US FPGA projects, owing to a lack of guidance at the time (IEC 61226 had not yet been published) [2]. The SER identified some aspects of the ALS as being approved for MSFIS specifically, and some that gained a "generic" approval. It should be noted that because some approval aspects are specific to the MSFIS use, consequently this does not constitute approval for the ALS in all cases. Some aspects accepted specifically for the MSFIS use included[16]:

- sufficient design diversity
- implementation-specific failure modes and effects
- adequate plant-specific diversity and defence-in-depth
- adequate V&V for a more complex system

Issues identified by NRC as helpful in terms of regulatory approval include [1]:

- functional simplicity of the FPGA
- no use of embedded micro-processor or memory

- segregation of safety and non-safety features, and absence of communication between them
- lack of inter-channel communications

In 2010, a Topical Report [83] was submitted to the NRC to gain generic approval of the ALS and this was granted in September 2013 [84].

Licensing strategy

The developer and regulator communicated often via Topical Report Processes, a method which was considered useful for clarifying regulations and identifying problems [16].

Pre-submittal (Phase 0) meetings allowed the developer to learn about what criteria the NRC would be using to assess the FPGA, and prioritised the discussion of approaches to improve design diversity. These meetings also identified safety aspects for the MSFIS that would potentially be problematic from a generic approval perspective for the entire ALS platform.

Pre-submittal licensing meetings were designed to follow the process, and achieve the objectives, specified in Interim Staff Guidance ISG-06 [43]. These meetings included discussions of ways to systematically eliminate programming error, as well as discuss whether sufficient design diversity was being achieved. Ways to improve diversity identified included [16]:

- use of different or multiple FPGA programming languages
- different FPGA devices or logic synthesis directives
- multiple diverse implementations with redundant channels
- segregation of diverse implementations to mutually independent channels

3.1.2 Diablo Canyon

This example concerns the Process Protection System (PPS) replacement at Diablo Canyon. The Diablo Canyon Power Plant is a pressurised-water NPP in California, consisting of two reactors. Diablo Canyon was first opened in 1985 and is intended to operate until 2025.

The PPS performs Class 1E functions; providing input to the Reactor Trip System and the ESFAS. Each of the two reactors has a separate PPS. These were originally analog systems produced by Westinghouse, but were digitised (also by Westinghouse) in 1994 to provide a microprocessor implementation of the PPS.

FPGA involvement

The FPGA system in question is the Advanced Logic System (ALS) platform as used in Wolf Creek, with some additional design diversity. As discussed in Section 3.1.1 this was developed by CS Innovations, which has since been bought by Westinghouse.

The planned replacement used a combination of microprocessor elements (a Tricon PLC-based platform [28]) and FPGA elements, with the microprocessor being used for those elements of the PPS which do not need additional diversity (i.e., for which other parts of the system provide sufficient diversity under NRC requirements). For the functions that would require additional

diversity (e.g. manual operator intervention, or an additional diverse actuation system), diverse FPGA-based elements are used [2].

All languages, tools and IP cores were identical to those used for the Wolf Creek replacement (Section 3.1.1).

History and licensing

In November 2009 a license renewal application was submitted to the NRC [24]. In June 2011 the NRC issued a Safety Evaluation Report (SER) [25] relating to the license renewal of the Diablo Canyon plant, which did not include the installation of the proposed replacement PPS.

A diversity and defence in-depth (D3) evaluation [23] was performed in 2010 and submitted to the NRC, in order to evaluate whether the proposed FPGA solution met the regulatory diversity requirements [2] [27]. Obtaining NRC approval of the D3 assessment allowed confidence in the chosen design (PLC / FPGA), and thus reduced project risks.

A public meeting was held in October 2013 to discuss the PPS replacement [26]. This allowed discussion between the licensee and regulator prior to the actual evaluation. It was considered to be particularly helpful, particularly when meeting agendas were planned in advance [35].

To support NRC approval of the License Amendment Request, audits were held of the suppliers. In February 2013 an audit of CS Innovations was performed [34] to assess the FPGA portions of the system, while in November 2012 an audit of Invensys was performed to assess the PLC portions (i.e., the Tricon system). The Invensys audit identified some concerns, and a follow-up audit was conducted in June 2014 [33]; consequently as of mid-2014 the system had not yet been approved.

The NRC developed Digital I&C Interim Staff Guidance ISG-06 [43] through a joint working group to provide guidance for modifications of digital I&C systems [35]. The Diablo Canyon PPS replacement was conceived as a pilot project for this guidance, which describes the licensing process that the NRC may want to use to review digital I&C modifications.

ISG-06 identifies different tiers of LAR that can be used [36]. Tier 1 relies on previously-approved topical reports; it is therefore a pre-requisite that the system in question has been generically approved in the previous topical reports. Tier 2 is to be used for systems that have been previously generically approved, but where deviations are made for plant-specific reasons. Tier 3 is where the proposed digital I&C system to be used has no generic approval at all.

Licensing strategies

In accordance with [43], a number of public meetings ("Phase 0") were held to discuss the PPS replacement [26]. These meetings are intended to permit discussion and feedback between the licensee and regulator on issues that may affect the evaluation [35]. In this case, feedback was given on issues that included diversity, communications, maintenance, Class I / II isolation, software and security.

To reduce uncertainty around approval and licensing, Pacific Gas & Energy determined to propose simple solutions where possible, and minimise manual operator interaction as a means of mitigating software CCF. By choosing to use a diverse system (the PPS consists of a Tricon PLC-based system as well as the FPGA-based ALS), this eliminates the need for an additional diverse actuation system [27] [35].

As described above, a diversity and defence in-depth evaluation was submitted to the NRC in 2010, and was approved in 2011 via a Safety Evaluation Report [28]. This formed the basis of the License Amendment Request, submitted in 2011 [29] [31].

The ALS was submitted using a Tier 3 application, as the previous approval for this platform in Wolf Creek was not generic. The response from the US NRC to the Tier 3 application is that the PPS is initially considered compliant and that public health and safety will be protected with NRC approval to make this replacement [32]. The NRC issued an acceptance review [30] in 2012, which enabled them to proceed with the technical review of the system.

In 2010 CS Innovations submitted a topical report [83] requesting generic approval of the ALS [35], which was still pending at the time of submitting the LAR for Diablo Canyon (2011) [31]. The NRC indicated that if this generic approval was granted, then the ALS would be applicable for submission for use in Diablo Canyon under a Tier 1 application [35].

The ALS received generic approval from the US NRC in September 2013 [84].

3.1.3 South Texas Project Advanced Boiling Water Reactor

The South Texas Project (STP) is situated in Texas and operated by STP Nuclear Operating Company. It was opened in 1988 and consisted of two PWRs provided by Westinghouse. In 2006 NRG proposed to build two additional Toshiba Advanced Boiling Water Reactors (ABWR) at the plant.

The Toshiba design being used is equivalent to that discussed in Section 3.6.1.

The FPGA-specific aspects of this design can be found in the Power Range Neutron Monitoring System (PRNMS). This system measures the local neutron flux in the reactor core, calculates the overall reactor flux and provides signals to the rest of the plant including the reactor protection system. The components of the PRNMS which are being implemented using FPGAs are the local range power monitor (LRPM) and the average power range monitor (APRM).

FPGA involvement

The FPGA technology used was proposed to be the Toshiba PRNMS, discussed in Section 3.6.1, and utilising these FPGA chips and techniques.

Owing to the NRC requirements around diversity (which are stronger than those under the Japanese regime), this specific system is amended with additional measures and equipment that provide increased diversity and defence-in-depth [1]. All other languages, tools and IP cores were identical to those described in Section 3.6.1.

History and licensing strategies

Licensing for this was initially sought via submission of topical reports [1], with the first being submitted in March 2008 [47]. A generic topical report for the platform was submitted, as was a later system topical report for the specific application of this platform in the PRNM [48]. The NRC's NRO (Office of New Reactors) was simultaneously reviewing the FPGA system in the South Texas Project [1].

In 2009 Toshiba requested that the NRC stop reviewing the Topical Reports, citing improvements in the development and quality processes that made these no longer relevant [48]. This had the effect of cancelling the generic qualification of the Toshiba platform, although the intent was that the Office of New Reactors would continue to review the FPGA system in the South Texas Project specifically.

In April 2011, NRG Energy announced that it would pull back its investment in the project, attributing this to financial concerns, as well as those relating to the Fukushima accident encountered by its partner, TEPCO [125].

Toshiba submitted a Licensing Topical Report for the FPGA-based I&C systems in 2012 [49], with additional documentation submitted in 2013 [50] and 2014 [51]. The review was currently in process as of 2014, with the development process and platform being reviewed against ISG-06 [51].

It should be noted that there has been some project uncertainty (unrelated to FPGA usage), as since the 2011 decision by NRG Energy, the stakeholders have been considered by the NRC to be primarily foreign-controlled. US NPPs cannot be controlled by foreign companies [124] [44], and hence there has been some regulatory uncertainty. NRC confirmation was provided in 2014 that the proposed ownership by TEPCO was considered acceptable [44].

3.1.4 AP1000 use in the US

The AP1000 is a PWR developed by Westinghouse, and intended for use in countries including the US, the UK (see Section 3.2.3) and China (see Section 3.10).

There are currently two AP1000 reactors under construction in the US: one at Vogtle and one at VC Summer. These reactors use FPGA technology in the Component Interface Modules (CIM), which are Class 1E. The CIM system interfaces between the Protection and Safety Monitoring System (PSMS), the Plant Control System (PCS) and field components [3]. It should be noted that the CIMs are able to be used in a variety of systems, but the first use of this was planned to be within the AP1000 [79].

In addition to the CIMs, the FPGA-based ALS platform is also integrated into the AP1000, and used to provide the Diverse Actuation System (DAS) [3]. It should be noted that, in the US, this DAS is not considered to be safety-related [3] [56]. The language, tools and IP cores used for the ALS are described more fully in Section 3.1.1.

History and licensing strategies

In September 2004 the NRC released a SER [54] that acted as final design approval for the AP1000, and the proposed design certification rule was published in 2005 [55]. Subsequent updates were made by Westinghouse, and approved by the NRC in a series of supplements to the SER [53]. These closed out all open issues associated with the SER.

3.1.5 NuScale Power Small Modular Reactors (SMRs)

NuScale Power together with Rock Creek are considering an FPGA-based reactor protection system [88].

3.1.6 San Onofre

The San Onofre NPP, which is run by Southern California Edison is considering using the NuPAC platform (see Section 3.10.2) for use in its RPS [99].

The functions performed by NuPAC in this case would include the Core Protection Calculators (CPC), Plant Protection System and emergency diesel generator controls.

The detailed designs for this plant are scheduled to begin in 2013 [99].

3.2 FPGA nuclear applications in the United Kingdom

3.2.1 Gag Vibration Monitor

In the UK, one of the nuclear plants has recently replaced the gag vibration monitor system with an FPGA-based system, due to issues of obsolescence [126]. The gag vibration monitoring system assesses the vibration of the gags controlling the flow of coolant gas in the fuel assembly of the nuclear power plant.

The replacement FPGA system performs a Category C function (i.e., a function of the lowest safety category).

3.2.2 Hitachi ABWR

Hitachi are currently in the process of going through a Generic Design Assessment (GDA) [45] for a ABWR. The GDA is a UK assessment process which allows the technical assessment of a reactor design where this has not yet been built nor a site selected [45]. This permits early involvement of the regulators at a stage where designs are still conceptual. Consequently, problems can be identified early, and safety improvements made, without a significant cost to the project or the qualification timescales.

The FPGA system here is identified as the Safety System Logic and Control System (SSLC), which performs Class 1 safety functions [46]. It is responsible for initiating safety protections systems, specifically the RPS, Main Steam Isolation Valve, the Emergency Safety Features (ESF) and the Emergency Core Cooling System (ECCS) [46].

It should be noted that the UK ABWR is a further development of the ABWR in operation and construction for Japan, which does not make use of FPGA technologies [46].

History and licensing strategies

As of 2014, the GDA has progressed as far as an overview of the acceptability of the proposed reactor design concept within the UK regulatory regime. It is noted that as the assessment progresses further, more information will be sought on production excellence of the FPGA-based Primary Protection System [45]. The intention is to produce a draft Topic Report for the FPGA system [46].

The intention is for the FPGA development to comply with IEC 62566 and IEC 61513 [46] [52].

3.2.3 AP1000

A generic design assessment of the AP1000 began in 2007 [60], and was paused in 2011 [57]. At this stage 51 matters had been identified in the GDA [45] [60]. These included concerns over the development process used for the FPGA-based CIM, and over the adequacy and qualification of the tools used to develop the FPGA application.

The FPGA-based technology in the AP1000 is the ALS, a platform developed by Westinghouse. Further details of the development of the ALS and its licensing history can be found in Section 3.1.1 and Section 3.2.3.

At this stage an interim Design Acceptance Certificate was issued, which has the effect that future ONR regulatory efforts will be targeted at the GDA issues that remain. It should be noted that this does not confer regulatory approval.

The GDA assessment process has recently re-commenced [82].

Licensing strategies

A certain difficulty in translating between the US terms of "safety related" or "non safety related" and the UK classifications arose during licensing. As part of this GDA, the ONR raised a concern with the classification assigned to the DAS, namely the claim that it is not safety-related (it is identified as a non-Class 1 system in the Westinghouse Pre-construction safety case report (SCR) [61]). The Office for Nuclear Regulation (ONR) report on the assessment of C&I (together with Westinghouse's own submissions) identify that the DAS contributes to the performance of Category A functions [9]. Although the Primary Protection System is the system primarily responsible for performing this systems, the potential misclassification of the DAS was raised as an initial concern during the GDA, although it was later concluded that the classification of the DAS as a Class 2 system was justified [57].

An issue was raised [58] at this time that the DAS was not sufficiently diverse from the protection and safety monitoring system / CIM, as both use FPGA technologies sourced from the same supplier. As a result of this, Westinghouse changed the design of the DAS to conventional electronics instead of FPGAs [57] [58].

3.3 FPGA nuclear applications in Canada

3.3.1 Canada Darlington Digital Control Computer (DCC)

This example concerns the replacement of the Digital Control Computers (DCCs) used to control the reactors in the Darlington Nuclear Generation Station [1]. These DCCs were originally implemented as PDP-11/70 systems, but by mid-1990s the plant was encountering obsolescence issues and reliability problems.

The reactor itself is a CANDU reactor, with 4 units. The first unit was deployed in 1990. Each unit is controlled by two DCCs in a master / standby configuration [12]. The DCCs control reactor power regulation, steam generator pressure control, alarm annunciation, data display [1].

The technology replaced by FPGAs comprised:

- Countdown registers (CDR) (not safety-related)
- Moving head disks and magnetic tape drives (not safety-related)
- PDP-11/70 CPU, Sequence of Events Monitor, Common Processes Computer, Fuel Handling Computers

The MHD and magnetic tape drives were replaced with the Flexible RM03 Emulated Disk, designed in-house. The CDRs were replaced with an in-house FPGA design that was based on a SRAM type FPGA from Altera.

The other components were replaced with a FPGA PDP-11/70 emulator, developed by QED. The replacement project is being managed by L-3 Communications MAPPS, but QED were responsible for all the FPGA components [1].

The PDP-11 emulator was based on SRAM type FPGA from Xilinx (Virtex 5 family XC5VLX 30/50/110) VHDL was used to specify the functions of the PDP-11 emulator. All tools used and the IP Cores were subject to relevant qualification as per the standards used for this project.

History and licensing strategies

The DCC FPGA emulator was based on a PDP-11/70 FPGA emulator (also from QED) that had been used for over 10 years in the Fuel Handling Systems [1]. It was updated for use in the DCCs.

FPGAs were selected for this project because the original system (DEC CPUs) consisted of a number of complex circuit boards, and could be replaced with a single FPGA. Reducing the chip count in this way meant a reduced MTBF, and also meant that future changes would be less costly.

In this case, use of an emulator meant that the existing software could continue to be run (though this is not an FPGA-specific advantage).

In addition, Ontario Power Generation (OPG) had experience of use with this FPGA emulator, as part of the Fuel Handling Systems. FPGAs had also been used successfully in previous replacement projects.

OPG discussed the project at regular intervals with the regulator, and developed the process for implementation in concurrence with them.

3.3.2 Darlington

CANDU Energy are currently collaborating with Radiy to develop a process for creating FPGA applications for safety-critical functions of the new Enhanced CANDU-6 Reactor (EC-6) [3] [11]. This reactor is a new build project at Darlington [67].

The pilot project for this is the provision of an FPGA solution to safety shutdown system No. 1 (SDS1) and Emergency Core Cooling system of the EC-6 [3] [22].

The platform proposed to implement these reactor trip functions is the Radiy FPGA-based Safety Controller [5].

3.3.3 Pickering

Radiy have also collaborated with CANDU Energy to provide an FPGA-based shut-off rod indicator solution to the Pickering station, operated by Ontario Power Generation's Pickering station [1] [68].

3.4 FPGA nuclear applications in Argentina

Radiy has also won two CANDU bids to supply FPGA-based safety systems to the Embalse NPP in Argentina [22]. This is based on the RadICS platform.

One element of the FPGA equipment was the Windows Alarm Annunciators [76], which are based on the RadICS platform discussed in Section 4.2.1 [69], and another was the PHT Pump Motor Speed Measuring Device [21]. Both of these provide Category A functions.

3.5 FPGA nuclear applications in France

3.5.1 EDF 900 MW Series

This example concerns the 900MW series of nuclear power units in France, operated by EDF. There are 34 of these units, and by 2005 obsolescence issues were beginning to arise in the Rod Control System (RCS) I&C, and in the reactor in-core (RIC) measurement system [17].

The RCS and RIC dated from the 1970s and were considered liable to introduce costly faults [11]. The functions performed by the RCS include generation of control signals to activate the rods, verification of rod position and interface with the HMI and the control & diagnostic unit.

The RCS I&C system was replaced by flash-based FPGAs from Actel (3X3 family, A3P1000). The replacement was developed and implemented by Rolls Royce Civil Nuclear (RRCN). VHDL was used to specify the functions of the FPGA RCS. Place and route was performed using the Designer tool from Actel, while post-synthesis simulation made use of ModelSim (Mentor Graphics). There was no use of IP cores. This was not classified as a safety-related change. No modification of the instrumentation (which is classed as 1E) or the power modules is required [14].

Requirements specification for the project began in 2005, and the first unit was deployed at Tricastin Unit 1 in 2009. In February 2010 the second installation started at Fessenheim Unit 1 [17]. Completion of roll-out to all 34 units is planned for 2020, when the units will be brought back into service.

FPGAs were selected for this project because of the strict timing requirements (1 ms), which is not easy to satisfy with a microprocessor [2]), reliability requirements (RRCN use a very strictly-defined development lifecycle for FPGAs), and for avoidance of future obsolescence issues. In this case, RRCN were also familiar with FPGA technology and internal RRCN standards were used throughout development.

3.5.2 Motorola 6800 Replacement

This example concerns the replacement of the Motorola 6800 microprocessor [1] [2], which performs a range of safety-critical RPS functions in the EDF 1300MW series of plants. The project began in 2008 as a result of obsolescence issues which were being encountered in the plants. This was a result of a lack of spares for the 6800 microprocessor, of which only sufficient for 20 years had been initially purchased [71].

Rolls Royce were responsible for developing the FPGA design used in this system, which was produced as an IP core [17] [78] in 2008. The initial intent was to use existing IP cores (either available as COTS or freeware), and consequently in 2008 a survey was performed of all IP cores that would emulate the 6800 microprocessor as required. The conclusion of this survey was that none of the existing IP cores would satisfy the assurance of quality required for a safety related system, and that furthermore it was not practical to upgrade them to this standard [78]. Consequently, the FPGA emulator was developed without use of pre-existing code.

The FPGA emulator was designed as far as possible to be "licensable" [78]. However, as there were no applicable standards available at the time, Rolls Royce used internal processes that were currently in use in their production and development. These were supplemented by incoming information about IEC 62566 [89], which was being drafted at the time [78], as well as the existing IEC 61226 standard [93].

The verification and validation undertaken by Rolls Royce was based primarily on manual review and testing [78], and made use of the Mentor Graphics HDL Designer verification tool. However, EDF undertook additional formal verification to demonstrate that the emulation was faithful as described [70].

3.5.3 Radiy I&C system

Radiy and EDF have recently signed a contract for supply of an FPGA-based I&C platform [77], which is currently in development. It is expected that this will be based on the RadICS platform, which is discussed further in Section 4.2.1.

3.6 FPGA nuclear applications in Japan

3.6.1 Advanced Boiling Water Reactor Plant, Japan

This example concerns the TEPCO Advanced Boiling Water Reactor plants in Japan, and the replacement of the safety-related (Class 1E) Power Range Neutron Monitoring System (PRNMS) by an FPGA-based system. This project was begun in 2006, and completed in 2007 [72].

The PRNMS measures the local neutron flux in the reactor core, calculates the overall reactor flux and provides signals to the rest of the plant including the reactor protection system. The components of the PRNMS being replaced by FPGAs are the local range power monitor (LRPM) and the average power range monitor (APRM).

The FPGAs used were non-rewriteable FPGAs (anti-fuse) from Actel (A54SX72A and A54SX32A). Toshiba is responsible for the development, installation and qualification of the PRNMS.

VHDL and Verilog were used to program the FPGA, and no IP cores were used. The Actel IDE was used, along with third-party tools including:

- Synplify tool (from Synplicity) to synthesize logic
- ModelSim (from Mentor Graphics) for simulation
- Silicon Sculptor II (from Actel)
- Pinport (from SynapticCAD Sales) to interface between ModelSim and digital hardware

None of these third-party tools were qualified. The Actel IDE itself includes tools to provide the following functionality:

- Netlist viewer
- Place and route
- Static timing analyzer

History and licensing strategies

Toshiba first began using FPGAs in safety-related positions in nuclear power plants in 2004, with radiation monitoring. By 2007 FPGAs were being used by Toshiba in Power Range Neutron Monitoring Systems, and in reactor protection systems. By 2008 there were over 200 of these FPGA-based systems in TEPCO's plants. Toshiba have also used FPGAs to replace the ABWR Startup Range Neutron Monitoring System and reactor trip and isolation systems [11]. Prior to developing the FPGA-based PRNMS for ABR, Toshiba had also developed the Power Range Monitor for Boiling Water Reactors (BWR) [18].

Radiation-hardened FPGAs were deliberately not chosen, as the system was expected to operate in an environment that would not require these. This has historically not affected regulatory approval of NPPs in Japan. Standards used included IEEE 603 (overall safety requirements), IEEE 7.4.3.2-2003 (safety system computers), IEEE 1012 (V&V, and qualification of FPGA logics [18]) and EPRI TR-107330 (hardware qualification). Japan does not require any

specific diversity properties to be satisfied, and consequently there is no need for the PRNMS to offer internal diversity.

None of the tools used for development (either the Actel Integrated Development Environment (IDE) or the third-party tools) were qualified, although review of these was performed internally by Toshiba.

The system was approved by the Japanese regulator once completed, and treated primarily as a hardware based system. Previous experience of these FPGAs in other sectors was crucial to success in gaining regulatory approval. In addition, the choice of FPGAs that were already in use in other sectors (e.g. aerospace) was deliberately made to prolong longevity. In particular, the chip vendor has committed to the US DoD to support these chips until at least 2023 [1]. The wide use of these FPGA chips was also a crucial factor in gaining approval of the Japanese regulator [1].

The PRNMS is also being proposed for use in the South Texas Project Units 3 & 4. More information on the regulatory aspects in the US is available in Section 3.1.3.

3.7 FPGA nuclear applications in Ukraine and Bulgaria

3.7.1 Radiy Digital Platform, and Kozloduy Units 5 & 6, Bulgaria

This example concerns the replacement of the ESFAS in Units 5 & 6 of the Kozloduy NPP. Units 5 (built 1987) & 6 (built 1991) of this plant are PWRs. Units 1 & 2 were shut down in 2004 and decommissioning began in 2010, citing safety concerns. This replacement began in 2008 and was completed in 2010.

There were three redundant ESFAS systems in each of the units (i.e., six in total) which were to be replaced with FPGA solutions. The ESFAS performs automatic actuation of safeguard equipment in response to signals, remote control of actuators, automatic control of actuators and transmission of signals to other systems.

The FPGA platform used is designed, developed and qualified by Radiy, and is identified as the Digital Radiy Platform [19]. The Digital Radiy Platform uses FPGA circuits supplied by Altera (although Radiy have confirmed that where diversity is needed, the diverse redundant circuits are sourced from Actel [4]). SRAM chips (Altera Cyclone) are used for the primary channels, with flash technology (Actel ProASIC3) used for the diverse (redundant) channels where this is required.

The Radiy Digital Platform divides software into upper level (runs on microprocessors using Windows XP) and lower level (FPGAs). All the control functions are performed by the FPGA applications, and the upper level software only handles non-safety related functions [19]. The same division of upper / lower levels applies to hardware, with the lower level cabinets being used to perform safety functions. The lower levels also contain FPGAs that perform microprocessor emulation, in order to use software that would otherwise require a PC. Parts of the Digital Radiy Platform are Category A

(lower level signal forming components [1], and parts are Category B and C (upper level power supplies, redundant computers etc. [1]).

The Altera Quartus IDE is used for programming, with the VHDL functions library "MegaCore". VHDL is used for FPGA design, and C used to develop the code that runs on the FPGA microprocessor emulator. Where diverse FPGAs from Actel are used, the Actel Libero IDE is used for the FPGA programming. IP cores include the Altera and Actel microprocessor emulators, and the Ethernet IEEE 10/100 MBPS interface.

3.7.2 Other systems in Bulgaria and Ukraine

As well as the Kozloduy NPP discussed in Section 3.7.1, Radiy have installed FPGA-based systems in a number of other NPPs in Ukraine and Bulgaria. The systems are both safety-related and non-safety related, and include as of 2014 [21]:

- Reactor Trip Systems (30 of these in Ukraine)
- ESFAS (18 of these in Ukraine and Bulgaria)
- Reactor Power Control and Limitation System (10 of these in Ukraine)
- Rod Control System (RCS - 1 of these in Ukraine)
- Fire Alarm System (9 of these in Ukraine)
- Power Supply for RCS (3 of these in Ukraine and Bulgaria)
- Switchgears (1300 of these in Ukraine and Bulgaria)
- Seismic Sensors (63 of these in Ukraine)

History and licensing strategies in Bulgaria and Ukraine

Radiy first deployed the Digital Radiy Platform in 2003, although they had been providing FPGA-based systems since 1998 [4]. By 2009 there were 17 nuclear power plants in Ukraine and Bulgaria using this platform for:

- Reactor trip systems
- Control rods actuation systems
- ESFAS
- Reactor power control and limitation systems

In the RTS used in the Ukraine, Radiy have been making use of two redundant FPGA systems, sourced from different vendors and programmed using different tools and languages. This would have been an option for the Kozloduy reactors, but was not considered necessary [1].

It is worth noting that Radiy has other FPGA involvement with Kozloduy Units 5 & 6 as of 2012, namely the modernisation of two sets of power supply equipment for the rod control systems and the modernisation of 10 switchgear sets of ESFAS and Nuclear and Conventional Island Control Systems for Units 5 & 6 [4] [21].

In terms of licensing, the FPGA chip was considered to be part of hardware, while the application was considered software [4]. That is, the FPGA was treated as a programmable component, and a modified software lifecycle used [1].

The FPGA-application development followed a V-lifecycle as per IEC 62566, but with modifications for FPGAs as follows [20]:

- Development of signal-forming block diagrams
- Development and integration of electronic FPGA design
- Loading of FPGA design onto the chip

As well as assessment by the Bulgarian authorities for the Kozloduy NPP, the Radiy Digital Platform was assessed by the Ukrainian State Scientific Technical Centre on Nuclear and Radiation Safety (SSTC NRS), which supports the Ukrainian Regulatory Authority. The SSTC NRS were also responsible for assessing all 53 of the FPGA-based safety systems supplied by Radiy to the Ukraine since 2003 [20]. The evaluation process includes the following stages [21]:

- System concept evaluation
- Development planning evaluation
- System requirements evaluation
- System design evaluation
- HW & SW requirements, detailed design, fabrication, test and integration evaluation
- System validation evaluation
- Installation, operation & maintenance evaluation
- Safety Evaluation Report analysis

A gap analysis was performed, comparing IEC and IAEA against the EPRI and IEEE standards, and the conclusion was that the Radiy Digital Platform would also be able to be qualified against US NRC standards [20]. (The new RadICS system has been certified as SIL 3 by Exida [21]).

3.8 FPGA nuclear applications in Taiwan

The Lungmen NPP in Taiwan is an ABWR, constructed by the Taiwan Power Company. As in 2012, there was a proposal to use a FPGA-based design as a possible replacement for the current microprocessor-based protection system. The FPGA chip proposed is the flash-based Actel SmartFusion chip [11].

3.9 FPGA nuclear applications in South Korea

Doosan plan to use FPGAs to perform component interface functions for engineered safety features in new plants currently under construction [1] [22]. In Yonggwang NPP and Ulchin NPP, work is proceeding to replace the PLC based Diverse Protection System (DPS) with FPGA-based controllers in eight power units by 2015 [3] [66]. This is considered to improve the diversity of the plant I&C systems. If this is successful, installation of an FPGA-based PPS will also be considered [66].

Additionally, in the APR-1400 the non-safety related Diverse Protection System and Diverse Indication System are implemented using an FPGA-based platform.

3.10 FPGA nuclear applications in China

3.10.1 AP1000 variants

There are four AP1000 reactors currently being constructed in China: two at Sanmen NPP in Zhijiang, and two at Hiyang NPP in Shandong. Construction of some of these has been completed in 2014, with the remaining construction efforts still scheduled. The AP1000 uses FPGAs as part of the Component Interface Modules, in addition to the ALS platform.

3.10.2 CAP-1400 and NuPAC

The CAP-1400 reactor was conceived as a Chinese derivative of the AP1000. Site preparation began in Shidaowan in Shandong Province in April 2014 [59] with construction expected to begin by 2015 [65]. This example concerns the supply of the I&C system for the CAP-1400 reactor. Development of this began in 2010.

The I&C system for the CAP-1400 reactor is being developed as a joint project between China's State Nuclear Power Automation System (SNPAS) and Lockheed Martin. The platform is known as NuPAC, and is intended to perform Class 1E [64] functions.

History and licensing strategies

NuPAC is based [62] on the functional and physical requirements in [63]. It is intended to be a modular system that can be used for ESFAS, diverse I&C systems, data communications, interlocks and others.

SNPAS and Lockheed Martin submitted the Topical Report [100] in compliance with the guidance in DI&C-ISG-06 [43], and also applied IEEE Std7-4.3.2 [94]. A Topical Report [100] was submitted for generic NRC approval in 2012 [64] and is still in the process of being considered for generic approval [87]. The Chinese regulator, the National Nuclear Security Administration (NNSA) approved the preliminary safety review of the CAP-1400 in 2014 [65].

3.10.3 Other systems

It has been proposed to use FPGAs in the DAS in Units 5 / 6 of the Yangjiang NPP [7]. The platform proposed is the FitRel [10] [7] platform currently under development by CTEC [3]. This is intended to satisfy the diversity requirements of [8], as well as a SIL3 requirement [3].

In addition to this, Triconex (a brand of Invensys Process Systems) are supplying FPGAs for priority logic modules in new plants [1].

China Nuclear Power Engineering Company (CPNE) together with the China National Nuclear Corporation (CNNC) are also evaluating FPGA use in the new version of the CP1000 design, known as the ACP1000. This is derived from the 900MW PWRs described in Section 3.5.1. FPGAs are being considered specifically for the RPS, DAS, ESFAS and Post-Accident Monitoring System. As of December 2014, the ACP1000 had successfully passed the IAEA Generic Reactor Safety Review [128].

3.11 FPGA nuclear applications in the Czech Republic

3.11.1 Temelin NPP

The Temelin NPP is a two-unit PWR in the Czech Republic that has been deployed since 2002. It is operated by CEZ Group. This example concerns the use of FPGAs in the Non-Programmable Logic I&C systems. The project was begun in 1995 and completed in 2000.

The Non-Programmable Logic acts as a safety load interface, communicating between the primary RPS, the Diverse Protection System (DPS) - both of which are implemented via microprocessors - and the Safety Diesel Load Sequencer [21]. The Emergency Diesel Sequencers are also implemented using FPGAs, and have been in operation for over 10 years [72]. The emergency diesel sequencer is classed as a 1E system, while the logic is considered non-safety related [85].

The Emergency Diesel Sequencer used the Actel A14100A FPGA chip [85] and was implemented by Westinghouse [86].

3.12 FPGA nuclear applications in Sweden and Finland

3.12.1 Olkiluoto

Olkiluoto is one of Finland's two NPPs, and is operated by TVO. It has been in operation since 1979 and currently has two BWRs. The third, which makes use of FPGAs, is currently being constructed. It is a PWR known as the EPR, produced by AREVA / Siemens (formerly Framatome) [74].

There has been some delay in constructing this, due to several reasons, including problems with showing independence between the process control and safety automation systems [72].

It is planned to have an FPGA-based backup system to perform some of the main safety automation functions, in order to provide a diverse back up for the microprocessor based systems [72]. The EPR is also proposed for use in France, UK and US, but these versions do not have the FPGA-based backup system [74].

3.12.2 Ringhals

The TWICE project at Ringhals 2 was completed in 2010. This project comprised the replacement of the entire I&C system and the replacement of out-of-date or obsolete components with newer functionality. This was a significant system replacement, although the FPGA involvement was comparatively smaller.

The FPGAs used in the I&C replacement took the form of Component Interface Modules (CIMs) [22], which act as the interface between the primary safety system and the equipment in the plant. These modules were supplied by Westinghouse, following a development process similar to that described in Section 4.2.2.

3.13 FPGAs in non-nuclear applications

FPGAs have been used in safety-related non-nuclear applications for a relatively long time. Some of the most notable applications are in motor control [117], space applications [98], aerospace and aviation, and military use.

Use in the medical sector is another recent application of FPGAs, and suppliers such as Xilinx (Section 4.1.1) and Altera (Section 4.1.2) are currently expanding this. FPGAs are used primarily in medical imaging, particularly in detection and image construction [118]. This has led to the introduction of new techniques, such as Optical Coherence Tomography (OCT), which provides a higher resolution image than those obtainable via magnetic resonance imaging or positron emission tomography (PET) scanning. In particular, a collaboration between the Japan Science and Technology Agency and Kitasato University has produced an FPGA-based system that allows continuous display of 3-dimensional OCT images. Altera, in collaboration with 3D-Computing, has also produced an FPGA-based screening technique that improves the speed of PET scanning, and consequently reduces the radiation exposure to the patient [119].

In aerospace and defence, the major contributions of FPGAs are seen to be in the areas of security information assurance (e.g. anti-tamper capability) and tool usage [120]. However, FPGAs have been used in a variety of systems including radar and sonar imaging, unmanned vehicles and military communications. Faster processing speeds also mean that FPGAs are being used in real-time systems such as improvised explosive devices and weapon systems. Companies such as Altera produce defence-specific FPGA chips, which operate over a wider thermal range and provide a trade-off between computing power and space / power usage.

FPGAs have been used in space applications for over fifteen years, with the major disincentive to further use having historically been the occurrence of radiation-induced Single Event Upsets (SEU) [121]. To address this, many major chip suppliers now make use of radiation-tolerant FPGAs, as discussed further in Section 4.1. ESA has presented a categorisation of the major FPGA suppliers in terms of their readiness (at 2010) to produce FPGAs designed for space applications [122].

space FPGAs




 XILINX®	 Actel®	 ALMEL
<ul style="list-style-type: none"> SRAM-based 0.35 µm-65 nm 	<ul style="list-style-type: none"> Anti-fuse (ONO and M2M) 0.8 – 0.15 µm 	<ul style="list-style-type: none"> Hardened SRAM-based 0.35 – 0.18 µm
<p>Weaknesses</p> <ul style="list-style-type: none"> More SEU sensitive Hardening by design needed at various levels MCGA packages not space qualified yet 	<ul style="list-style-type: none"> Can be programmed only once ITAR applies (RTAX) Parts Cost 	<ul style="list-style-type: none"> Small capacity (40K) available until 2008 New technology not used yet
<p>Strengths</p> <ul style="list-style-type: none"> Unlimited easy reprogrammability Many hard-macros included (DSP, mC, SERDES) 	<ul style="list-style-type: none"> Rad Hard Higher level of Space Qualification Space Legacy 	<ul style="list-style-type: none"> Unlimited easy reprogrammability Non ITAR, fabricated in EU SEU-hardened SRAM/FF/CLK/RST
19 Nov 2010	DCIS 2010	34

Figure 3: Comparison of FPGA suppliers for space applications

4 Market availability of FPGAs

Suppliers can be categorised into two different types: chip suppliers and platform suppliers. Chip suppliers provide the FPGA circuits, typically also with some software for creating the applications. Platform suppliers provide the entire platform for use within a NPP. This includes the application that has been written to run on the FPGA circuit (typically sourced from a chip supplier). Platform suppliers usually provide maintenance and further upgrades.

4.1 Chip suppliers

There are two main chip suppliers in the FPGA market, Altera and Xilinx which together in 2008 held over 89% of the market [13]. Other major suppliers include Microsemi (previously Actel), Atmel, Lattice Semiconductor and QuickLogic. The major producers of SRAM FPGAs include Xilinx, Altera, Atmel and Lattice Semiconductor, while flash FPGAs are primarily produced by Microsemi and QuickLogic. Antifuse FPGAs are rarer, as discussed in Section 2.1, but Microsemi also produce these to a limited extent.

4.1.1 Xilinx

Xilinx is based in California and was founded in 1984. In 2009 it represented 51% of the programmable logic market [39]. Xilinx chips have been used in a number of applications, including the Darlington installation in Canada (Section 3.3.1), space, medical and communication applications.

Major chip families and their use

Xilinx produce four major chip families, ranging from the lower-cost Spartan family, to the mid-range Artix and Kintex families, to the high-density, high-bandwidth Virtex and Virtex Ultrascale. These are all SRAM FPGAs.

In addition to this, Xilinx produce the EasyPath family of FPGAs. These are FPGAs that have been factory programmed and tested for a specific customer application. They are architecturally identical to the Kintex and Virtex families but they are not reprogrammable. This means that the EasyPath FPGAs are cheaper and faster to produce in large quantities.

The use of EasyPath FPGAs takes the following steps [105]:

1. Develop the design using the Kintex or Virtex chips
2. Submit the compiled design to Xilinx for cost reduction
3. Xilinx transfer this design to the EasyPath FPGAs, and send out these to the customer to implement the required design

Xilinx claim an approximate 35% reduction in costs when using EasyPath FPGAs instead of the standard Kintex or Virtex chips [38].

Tools and IP Cores

Xilinx provide IP cores in a number of areas, including video and imaging, memory and controllers, communications, interfaces and mathematical and embedded functions. In addition, Xilinx will also undertake development of custom IP cores.

Xilinx develop the Vivado Design Suite for use in designing and developing applications for their FPGA chips. It provides functionality to integrate IP cores and perform verification and debugging, as well as synthesis and simulation. The Vivado Design Suite includes both C and HDL based high level design abstractions.

In addition to this, Xilinx also continues to offer the ISE Design Suite, which is the forerunner of the Vivado Design Suite. Other tools offered by Xilinx include embedded tools for the creation of firmware, applications, Linux configurations and boot loaders. The Xilinx Certified Safety Design Flow Solution has been certified to meet IEC 61508 by TÜV [131], and consists of:

- FPGA design and verification tools
- IP and devices
- Certificates and reports

4.1.2 Altera

Altera is based in California (Silicon Valley), and released its first PLD in 1984. By 2009 it had approximately 34% of the programmable logic market [39]. Altera chips are used in the automotive, space, military, communications and medical sectors. They were also used in the Darlington installation (Section 3.3.1) and as part of the Digital Radiy Platform (Section 4.2.1).

Major chip families and their use

Altera produce three main families of SRAM-type FPGAs: the low-cost, low-power Cyclone series, the mid-range Arria series, and the large, high-bandwidth Stratix series.

In addition to this, Altera produce Hardcopy ASICs, which are intended to reduce the cost of utilising FPGA-based systems. These ASICs are now offered only for existing designs, and historically have served the same purpose as the Xilinx EasyPath FPGAs in being a high-volume, low-cost method of implementing FPGA-based designs.

Tools and IP Cores

Altera produce a range of IP cores, some of which are designed in-house and some of which are designed, maintained and supported by partners. In-house designed IP cores are provided along with the Quartus software, also developed by Altera for design and development of FPGA applications.

Altera certify the IP cores produced by their partners. This certification ensures the compatibility of the IP cores with Altera designs and updated functions. In addition to this, Altera claim a reduced total cost of ownership for systems implemented using an FPGA-based design [37], citing their

Functional Safety Data Package. This has been SIL 3 certified by TÜV and includes [130]:

- Altera devices
- Diagnostic and standard IP
- FPGA design flows
- Development tools

This certification is claimed to reduce the qualification burden on the developed FPGA components. Altera also cite as factors in this reduced total cost of ownership a faster time to market, an increase in portability, and an enhanced ability (over traditional systems) to handle processing of complex functions.

4.1.3 Microsemi

Actel, the original company, was based in California (Mountain View) and became publicly traded in 1985. In 2010 Actel was bought by Microsemi, who now produce FPGAs for a number of sectors including avionics, military, medical, industrial and automotive. Actel chips have been used in the EDF 900MW installation (Section 3.5.1), the Wolf Creek installation (Section 3.1.1), the ABW Reactor (Section 3.6.1) and also in the Radiy Digital Platform (Section 4.2.1) to satisfy diversity requirements.

Major chip families and their use

Microsemi produce two types of FPGAs: antifuse-based (e.g. Axcelerator) and flash-based (e.g. Fusion, ProASIC3). Fusion FPGAs integrate mixed-signal analog functionality into FPGAs. The antifuse FPGAs are manufactured primarily for space applications, and as such are radiation tolerant. Radiation test data is made available for customer use.

Microsemi also produce two System-on-a-Chip (SoC) FPGAs; SmartFusion and SmartFusion2. These are flash-based FPGAs that are integrated with high-speed interfaces and a complete microprocessor subsystem. That is, they are a combination of an FPGA and a microprocessor on a single chip, which is intended to support safety operations and provide additional features including Ethernet, USB and CAN interfaces. SmartFusion and SmartFusion2 are designed for use in safety-critical applications.

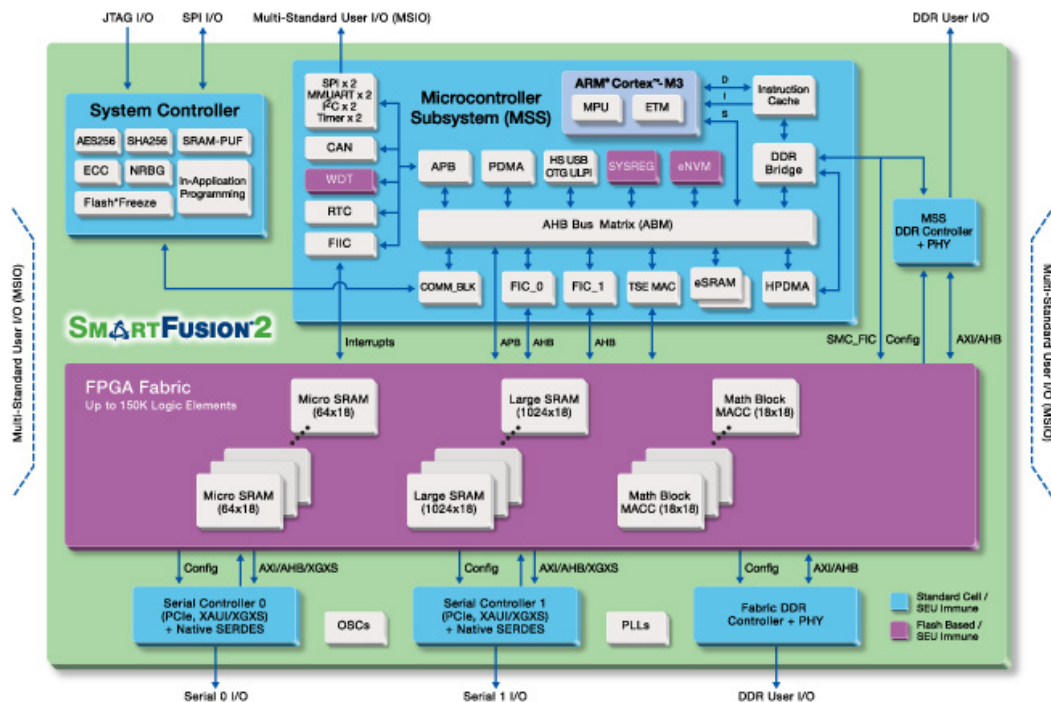


Figure 4: SmartFusion2 layout as depicted in [103]

The safety properties of Microsemi SoC FPGAs include [103]:

- SEU-protection
- built-in self test
- no external configuration device needed
- zero Failure In Time (FIT) rate FPGA configuration

The microprocessor on the SoC FPGA runs a real-time operating system known as SAFERTOS. This has been developed by Microsemi with a design assurance pack containing all necessary artefacts for compliance with IEC 61508, and has been certified as SIL3-compliant by TÜV [104].

Tools and IP Cores

Microsemi provide a range of IP cores, some of which (DirectCores) are designed and verified solely by Microsemi. These offer functionality in the areas of cryptography, firmware protection (e.g. authentication, tamper protection and protection against unauthorised debugging) and shared memory protection. The other type of IP core associated with Microsemi are known as CompanionCores. These are sourced, maintained and verified by a network of Microsemi IP Partners, and have been developed by these third parties specifically for use with Microsemi devices.

Microsemi also offer the Libero IDE for use with their radiation-tolerant FPGAs and antifuse FPGAs. Libero is a software suite used for development, simulation, timing constraint management, modelling and post-route debugging.

Development methods and costs

Microsemi claim a significantly reduced system lifetime cost when using their FPGAs instead of traditional microprocessor systems or FPGAs (particularly SRAM FPGAs) offered by other suppliers. The basis for this claim includes the following [103]:

- Low power: the nonvolatile (flash) FPGAs have comparatively low static and dynamic power consumption
- Low cost of equipment
- Single chip and single voltage – no external device is required to load the FPGA at startup, and unlike SRAM FPGAs, there is no need for additional power on start-up

4.2 Platform suppliers

4.2.1 Radiy

Radiy are currently providing the Embalse system in Argentina, as well as a number of FPGAs in Ukraine and Bulgarian, including Units 5 & 6 at Kozloduy (Section 3.7). They currently have over 90 systems installed in NPPs [21]. Radiy began supply of FPGA-based I&C systems to NPPs in 1998. The second generation of these platforms was developed in 2002, and the third in 2011 [77]. Radiy is also involved in supplying I&C systems to non-nuclear power plants, including the Trypolksa Thermal Plant [21].

Their current platform, the RadICS system, was developed in 2011 [41]. This replaces the Radiy Digital Platform, initiated in 2002 [41]. Radiy produce a range of FPGA-based systems for use in nuclear power plants, all of which are based on the Radiy Digital Platform or RadICS platform [106]:

- ESFAS - complies with applicable national standards in the EU and US
- RCS - first introduced in 2012 in the South Ukraine NPP
- Reactor Power Control and Limitation System (RPCLS) - designed to be compliant with requirements of IEC, IAEA, NRC. If required, can be designed in a configuration that adds extra redundancy.
- Reactor Trip System (RTS) - 28 of these have been produced as of 2014, and are in operation in Ukraine

Development approaches

Before development begins, Radiy prepare and approve the Technical Requirements Specification, Safety Requirements Specification – which includes requirements from relevant nuclear and safety standards – and the System Architecture Description [40].

The preliminary design identifies functional blocks and their interfaces, as well as criteria such as reliability requirements and design traceability. The output of this phase is a textual or graphical representation of high-level design requirements, which acts as input to the detailed design phase. Detailed design takes place after a design review to validate the outputs of preliminary design, and serves to refine the high-level preliminary design. The detailed

design phase involves the production of HDL code or schematic diagrams which implement the design requirements. It is worth noting that large-scale systems typically make use of HDL coding, although in some circumstances schematics may also be produced manually [42] [72].

The detailed design phase concludes with the elaboration of the FPGA components, and the production of the RTL model.

Rady processes follow the major steps outlined in Section 2.1.1.

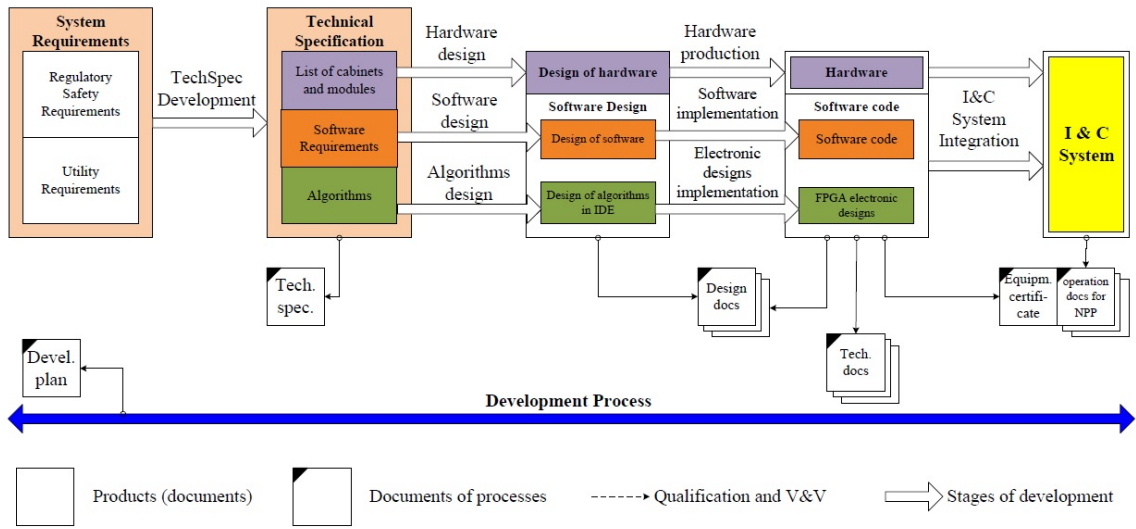


Figure 5: Rady development process as discussed in [76]

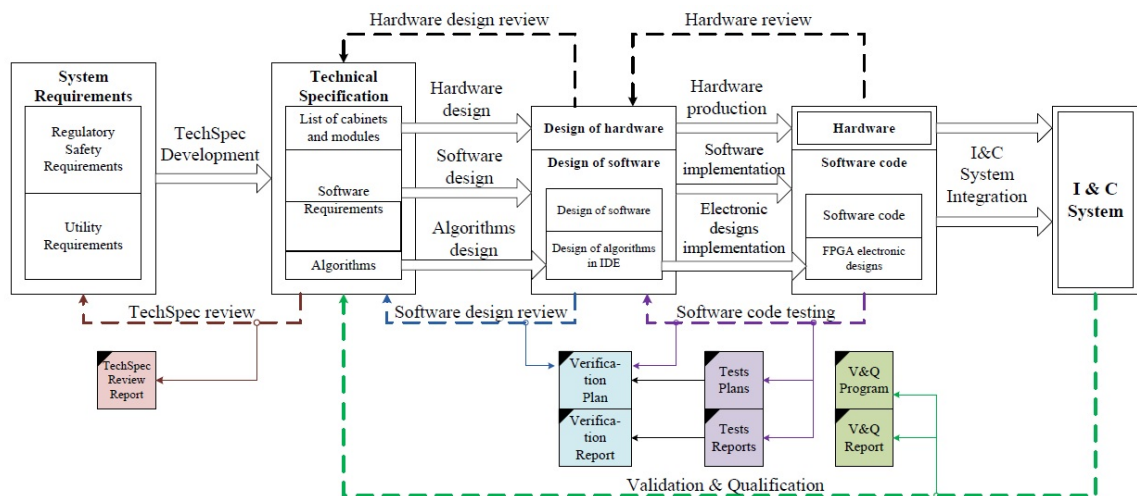


Figure 6: Rady V&V process as discussed in [76]

Tools and licensing

The Rady Product Configuration Tool (RPCT) is used to configure functional block libraries. Rady also make use of the Altera Safety Data Package, which has been TÜV-certified as SIL 3 compliant [76].

The RadICS system has also been certified as SIL3 by Exida [21].

4.2.2 Westinghouse

Westinghouse are the providers of the ALS platform, developed in 2009, and which is currently used in a number of applications, including Wolf Creek (Section 3.1.1) and proposed for use in Diablo Canyon (Section 3.1.2). They also provide the FPGA-based Component Interface Modules (CIM) used in the AP1000 and others, and have provided FPGA-based components to the Temelin NPP(Section 3.11.1).

Development approaches

The Westinghouse design philosophy is to move away from custom designs and towards standardisation [80], using a development approach compliant with IEEE 1012-1998 [81] [82]. Westinghouse implement FPGA development using a waterfall model [81]. A relatively standard project lifecycle is used, consisting of the following stages [107]:

- Planning
- Development
- Manufacturing
- System test
- Installation
- Maintenance
- Retirement

The V&V involves six major aspects: reviews, testing, requirements traceability analysis, checklists, inspection and regression analysis.

Independence is maintained between the development, QA, and test teams [107].

Specific information on the FPGA development is not publicly available, and has been redacted from NRC Topical Reports. However, we are able to confirm that the FPGA logic is assigned a SIL 4 safety integrity level [81].

Licensing

Westinghouse have worked primarily within the US licensing system, gaining first a SER for the ALS to be used in the form of a MSFIS at Wolf Creek [15] and later a SER providing generic approval for the platform [84]. They are also now beginning to work with the IEC set of standards, and have upcoming involvement with TÜV in Germany, and EDF in France.

4.2.3 Lockheed Martin and SNPAS

Lockheed Martin was founded in 1912, and is primarily involved in the space, military, aeronautics and communication sectors. They have had prior involvement with FPGA development, with this being focused mainly on the space sector.

SNPAS is a joint venture between the Chinese State Nuclear Power Technology Corporation (SNPTC) and the Shanghai Automation Instrumentation Corporation Ltd (SAIC), established in 2008 [108]. The scope of SNPAS is intended to be "NPP engineering I&C system design, integration, installation and commissioning and other engineering technical service; NPP I&C equipments complete supply; NPP I&C equipments research and development; NPP I&C system spare parts and operational technical support; System simulation, plant management system, weak current engineering and medium-low voltage electrical equipments and other nuclear power related business." [108].

Lockheed Martin and SNPAS are collaborating to produce the NuPAC platform, discussed in Section 3.10.2.

Development approaches

The development approach used by LM and SNPAS consists of five stages [100]:

- Mission analysis
- System requirements analysis
- System design
- Configuration item development
- V&V

On a general level, FPGA application development is performed using a waterfall model as shown below:

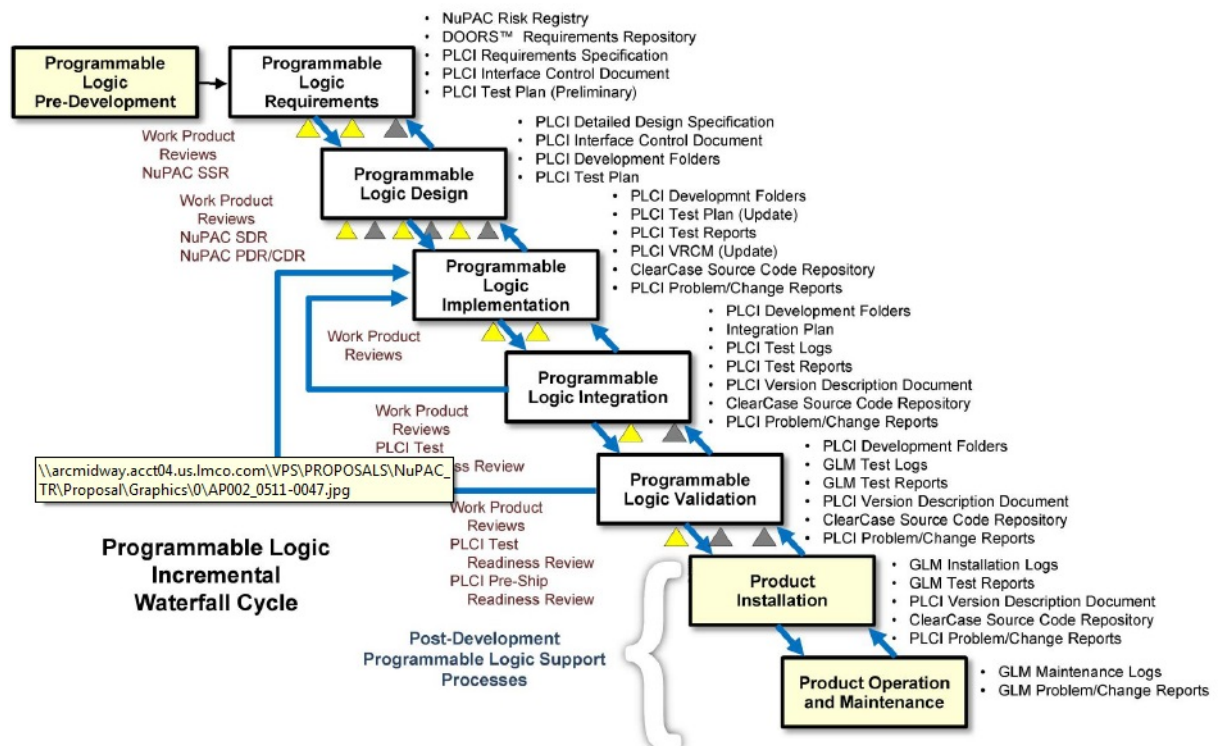


Figure 7: NuPAC programmable logic development as shown in [100]

FPGA verification and validation is intended to demonstrate compliance with the following standards and requirements [100]:

- IEEE Standard 603-1991
- ASME NQA-1-1994
- USNRC Standard Review Plan, BTP 7-14
- RG 1.168, Revision 1
- IEEE Standard 1012-1998
- IEEE Standard 1028-1997
- RG 1.152, Revision 2
- IEEE Standard 7-4.3.2-2003
- DI&C-ISG-06
- NUREG/CR-6101

The NuPAC development approach relies heavily on simulation for V&V, comprising simulation of the VHDL code, simulation after synthesis and simulation after route and layout. Formal verification has also been proposed as a useful supplement to the simulation [109].

More generally, Lockheed Martin typically use directed tests written in VHDL for V&V of FPGA-based systems [97]. They have also created a SystemVerilog / OVM methodology for verification of their space-based FPGA systems, which may be coming into use in nuclear applications [97]. They also typically use tools and support from Mentor Graphics, particularly Questa Verification Management [97].

4.2.4 Other suppliers

We have also identified other suppliers in Section 3, such as Toshiba (Section 3.1.3 and Section 3.6.1), Hitachi (Section 3.2.2), Doosan (Section 3.9) and CPNE (Section 3.10.3). These suppliers use a range of development and verification techniques as introduced in Section 2.1.1. Where information is known about their internal processes and regulatory compliance, this has also been described.

5 Standards and Nordic environment

At the functional level, FPGAs provide implementations of digital hardware and are therefore subject to design considerations such as timing hazards, clock synchronisation and parallel operation. From a development point of view, however, they are closer to software. An FPGA design starts out as source code, which is converted using a complex tool set into a binary image that is loaded onto the device [129].

There is a general consensus in most regulatory regimes that FPGAs should be treated similarly to software for licensing purposes [3] [1]. However, this does not imply that no adaptation is needed, or that FPGA-specific regulations, such as those discussed in Section 5.3, are identical to their software counterparts.

The relevant standards for FPGA development can therefore be divided into four general categories: those relating to general nuclear plant standards, those relating to the use of I&C equipment in nuclear power plants, software development methodologies and FPGA-specific guidance. We have included a representative list of standards in the following section, which have all been explicitly called out by suppliers, regulators or licensees as being used either in previous FPGA development or proposed for upcoming projects. Where a standard has been identified as being of particular significance to a country's licensing regime we have highlighted this.

5.1 General nuclear plant standards

The following standards relate to general design and quality assurance criteria for nuclear plants. Although they do not deal specifically with FPGA-based safety systems, they may be used to inform the development and use of these in a nuclear plant and should be taken into account if they are applicable under the relevant licensing scheme being considered.

- ASME NQA-1-1994
 - This standard describes quality assurance requirements for nuclear facility applications. It is endorsed by the NRC and describes the extent to which documented control is required in specific quality areas.
- IEEE Standard 603 [115]
 - This standard provides a set of functional and design criteria for the power and I&C aspects of a nuclear power station. It is strictly applicable only to safety systems, but in practice can be used as representative of good practice generally in nuclear design and development.
- STUK Guide YVL B.1 [95]
 - This standard details the safety design of a nuclear power plant. More information is given in Section 5.5.1.

5.2 Digital I&C equipment in a nuclear power plant

These standards deal specifically with the use of digital I&C equipment in a safety-related role in nuclear power plants. These standards are more specific than those identified in Section 5.1, and are used within the general context supplied by those identified earlier. Although these standards do not deal explicitly with FPGA-based I&C systems, most of the guidance and requirements they discuss are equally applicable to a FPGA system as a traditional microprocessor system.

- NUREG/CR-7007 [8]
 - This document describes diversity strategies for nuclear power plant I&C systems. It identifies the use of FPGAs as being significant in that they can provide different-technology diversity when used in combination with microprocessor-based systems. Diversity within different types of FPGAs is not discussed in any significant detail in this document. Examples of regulatory regimes for which this standard is applicable include the US and China.
- IEC 61513 [92]
 - This standard identifies and discusses general requirements for I&C systems important to safety in nuclear power plants. It is particularly applicable to digital I&C systems, although its scope is not strictly limited to them. It identifies relevant design criteria, requirements important to safety, and provides guidance and good practice on I&C architecture. This standard also serves to interpret IEC 61508 [102] requirements specifically for the nuclear sector. Examples of regulatory regimes for which this standard is applicable include the UK, France and Canada.
- Digital I&C Interim Staff Guidance [43]
 - This guidance document describes the licensing process for License Amendment Requests (LARs) associated with digital I&C system modifications. It is only applicable to the US licensing regime and, although it does discuss FPGA-based systems, calls out IEEE Std 7.4.3.2 [94] and NUREG CR-7006 [42] as being more generally applicable in these cases. Examples of regulatory regimes for which this standard is applicable include the US.
- IEEE 7.4.3.2 [94]
 - This standard describes IEEE criteria for digital computers in safety systems in nuclear power plants. It is intended to be used as a supplement IEEE Standard 603 [115], and provides additional criteria and requirements that are relevant to digital systems. Examples of regulatory regimes for which this standard is applicable include the US and Japan.
- IEC 61226 [93]
 - This standard provides a categorisation structure for instrumentation and control functions and, by extension, for the systems which perform those functions. It is intended to provide a specific supplement to IEC 61513 [92] by assigning categories (and therefore assurance requirements) to the functions of an NPP based on their importance to

safety. Examples of regulatory regimes for which this standard is applicable include the UK, France and Canada.

- Regulatory Guide 1.152 [113]
 - This document presents criteria for using computers in nuclear power plant safety systems. It is specific to the US regulatory regime and presents one example of a method considered acceptable to design and assure digital safety systems.
- NUREG/CR-6303 [91]
 - This document presents a method of performing diversity and defence-in-depth analyses of reactor protection systems. The purpose of this is to protect against common-mode failure, which has motivated consideration of FPGA-based systems alongside traditional microprocessor systems. Examples of regulatory regimes for which this standard is applicable include the US.
- Regulatory Guide 1.168 [111]
 - This document discusses ways to carry out the verification, validation, reviews and audits for digital computer software used in nuclear power plant safety systems. It identifies industry good practice (at the time of writing).
- NUREG/CR-6101 [114]
 - This document discusses software reliability and safety in nuclear reactor protection systems. It recommends the performance of certain activities during software development, but does not prescribe a particular lifecycle to be used. Examples of regulatory regimes for which this standard is applicable include the US.
- IEC 61508 [102]
 - This standard discusses functional safety of electrical, electronic and programmable electronic safety related systems. It identifies activities to be performed during software development, presents examples of techniques which can be used for assurance of these systems, and includes non-mandatory guidance on different methods of development. Some FPGA-specific guidance is included, such as the description of techniques to avoid introducing faults during FPGA development. Examples of regulatory regimes for which this standard is applicable include the UK.
- STUK Guide YVL E.7 [96]
 - This is discussed in more detail in Section 5.5.2

5.3 Software development methodologies

- IEC 61508 [102]
 - This standard discusses functional safety of electrical, electronic and programmable electronic safety related systems. It identifies activities to be performed during software development, presents examples of techniques which can be used for assurance of these systems, and includes non-mandatory guidance on different methods of development. Some FPGA-specific guidance is included, such as the description of techniques to avoid introducing faults during FPGA development.

Examples of regulatory regimes for which this standard is applicable include the UK.

- IEEE 1012 (see [90])
 - This is the IEEE standard for system and software verification and validation. It is applicable to both hardware and software, including firmware and microcode. Examples of regulatory regimes for which this standard is applicable include Japan, China and the US.
- IEEE Standard 1028 [112]
 - This document presents five different types of software review and audits, including management reviews, technical reviews, inspections, walk-throughs and audits.
- NRC Standard Review Plan BTP 7-14 [110]
 - This standard provides guidance on software reviews for digital computer-based I&C systems. It is specific to the US regulatory regime, and compliance is not mandatory. The guidelines it presents discuss how to evaluate the efficacy of software development lifecycles, and are based on EPRI requirements, NUREG/CR-6101 [114] and a survey of previous license applications. Examples of regulatory regimes for which this standard is applicable include the US.

5.4 FPGA-specific

- IEC 61508 [102]
 - This standard discusses functional safety of electrical, electronic and programmable electronic safety related systems. It identifies activities to be performed during software development, presents examples of techniques which can be used for assurance of these systems, and includes non-mandatory guidance on different methods of development. Some FPGA-specific guidance is included, such as the description of techniques to avoid introducing faults during FPGA development. Examples of regulatory regimes for which this standard is applicable include the UK.
- IEC 62566 [89]
 - This FPGA-specific standard discusses the development of HDL-programmed circuits for systems which perform Category A functions. It is intended to be used in the context of IEC 61513 [92] and IEC 61226 [93], which provide a discussion of general nuclear requirements and the categorisation of systems relative to their importance to safety. Examples of regulatory regimes for which this standard is applicable include France and the UK.
- NUREG/CR-7006 [42]
 - This document presents review guidelines for FPGAs in nuclear power plant safety systems. It is intended to be used with the US regulatory regime, and consists of a compilation of design practices for FPGA development. These can then be used as guidance for reviews of license applications involving FPGA-based systems. There are three types of FPGA design practices identified: hardware design practices, design entry methods and design methodologies. As well as identifying good

practice, this document also highlights potentially unsafe design methodologies and practices. Examples of regulatory regimes for which this standard is applicable include China and the US.

- EPRI TR 1019181 [1]
 - This report presents guidelines on the use of FPGAs in I&C systems of nuclear power plants. It identifies different types of FPGA technology, and the advantages and limitations of FPGAs vs traditional microprocessor-based systems. It also discusses the US regulatory regime and its expectations for FPGA safety justifications, as well as the requirements of IEC 62566 [89]. Finally, this document presents a review of FPGA systems installed in nuclear power plants in all countries.
- EPRI TR 1022983 [2]
 - This report presents some recommended approaches and design criteria for the application of FPGAs in I&C systems of nuclear power plants. It is intended to build on EPRI TR 1019181 [1], and also to incorporate the progress made towards IEC 62566 [89].

5.5 Nordic standards

We have reviewed the SSM regulations in translation [127], and conclude that these do not present any particular difficulties with using FPGAs. They also do not include any specific recommendations for their development, installation or maintenance.

We have also reviewed the regulations of the Finnish nuclear regime as described below. This regime classifies systems into safety classes 1 - 4, and EYT (non-nuclear). Class 1 is the class of systems most important to safety [116].

5.5.1 YVL B.1

This standard discusses the general safety design of nuclear power plants. It is not specific to I&C systems and does not explicitly mention FPGA usage. A major focus of this standard is on management of design, including general design principles, quality control, safety-related design requirements and regulatory oversight of the design.

Although FPGAs are not considered specifically, there are a number of clauses that would appear to be particularly relevant when considering these as options. These are presented in detail in 9 and the major points discussed briefly here.

The standard encourages the consideration of potential technological developments, and the implementation of design solutions using diverse technology. This has been a motivator in many cases for the use of FPGAs in nuclear power plants (see Section 3 for details). A system which makes use of FPGAs as a diverse backup, or in order to address potential equipment obsolescence issues may therefore be simpler to justify compliance with this standard. Similarly, where the standard requires consideration of separation principles, FPGAs offer a degree of separation by design, which may be advantageous.

In terms of verification and validation, this standard also presents few areas of concern in terms of FPGA compliance. The use of simulators as testing aids is recommended, and this is a typical part of FPGA development. Similarly, calculation speed is explicitly identified in the standard as a concern (the calculation of reactor parameters must be performed at a frequency necessary to ensure maintenance of the reactor operating conditions). Calculation speed is identified as an inherent advantage of FPGA systems in certain circumstances, and discussed further in Section 2.2.

There are also some areas of the standard that may need careful consideration when considering FPGA usage. The clauses relating to environmental qualification will need to be assessed, as they require qualification against a number of conditions, including vibration, temperature, pressure, radiation and humidity. While radiation-tolerant FPGAs are relatively wide-spread, the extent to which environmental qualification has been performed will be dependent on the manufacturer selected.

Another potential qualification issue relates to the development and verification tools used. This standard explicitly requires that they are adequately qualified and their safety significance assessed. In the examples seen so far, many FPGA development tools are only assessed internally, and qualification data may not be readily available.

5.5.2 YVL E.7

This standard is concerned explicitly with the electrical and I&C equipment in a nuclear power plant. Although it does not consider FPGAs specifically, there are a (very few) number of clauses which would appear to be particularly relevant when considering these as options. These are presented in detail in Section 9.

The most significant issue here is that of terminology. The standard makes repeated reference to "software-based" technologies and to "software". Historically, the requirements placed on FPGA development have been considered roughly analogous to those placed on software development. However, this is not a universal position (see Section 3.6.1). When using this standard for an FPGA-based system, it is therefore necessary to ensure that the clauses referring to "software" and "software-based technologies" are also explicitly applied to FPGAs.

This standard also identifies the need for qualification evidence relating to the development tools, which as we have discussed in Section 5.5.1 is not always readily available for tools used in FPGA development.

6 Conclusions

In this report we have presented a brief introduction to FPGAs, including a summary of their advantages and disadvantages. We have described a typical FPGA development process and identified how different types of FPGAs can be best used in a range of systems.

We have also performed a review of FPGA installations in safety-critical applications. These range from the earliest FPGA applications in the nuclear industry to systems which are currently under development. We have considered the options available when selecting the technology to be used and the licensing strategy chosen, as well as any lessons learnt. It is obvious from this review that FPGA usage has increased significantly within the last decade, and that licensing problems are becoming less of a concern. The development of FPGA-specific standards such as IEC 62566 [89] has provided clarity about what is required to justify the safety of FPGA-based systems.

We have also performed an assessment and review of the market availability for FPGAs. We have identified the major chip and platform suppliers and described – as far as is publicly available – their development approaches and major product families.

Finally, we have considered the standards used in the above FPGA installations, as well as other international standards which are applicable to FPGA usage. We have identified which of these specifically address FPGAs, and which of these may be applied to FPGAs along with other digital components. We have examined the Nordic standards YVL B.1 and YVL E.7 in detail, and identified those clauses which are particularly relevant to FPGAs. In some cases these are clauses which could be easily satisfied by an FPGA-based system (perhaps more easily than a microprocessor-based system), and in others the clauses represent potential areas of regulatory concern with such systems.

In conclusion, although FPGAs are not new technology, their use in the safety nuclear applications is relatively recent. Nevertheless, FPGAs are becoming more common in the nuclear industry as their advantages are increasingly recognised by the industry. A number of standards and regulations have been and are under development. Although there are still some uncertainties in the licensing requirements, we expect these to decrease as the deployment of FPGAs becomes more common.

7 Glossary

ABWR	Advanced Boiling Water Reactor
ALS	Advanced Logic System
APRM	Average Power Range Monitor
BWR	Boiling Water Reactor
CDR	Count-Down Register
CIM	Component Interface Module
CPC	Core Protection Calculators
DAS	Diverse Actuation System
DCC	Digital Control Computers
DPS	Diverse Protection System
ECCS	Emergency Core Cooling System
ESF	Emergency Safety Features
ESFAS	Engineered Safety Features Actuation System
FPGA	Field-Programmable Gate Array
GDA	Generic Design Assessment
HDL	Hardware Description Language
IDE	Integrated Development Environment
LAR	Licensing Amendment Request
LRPM	Local Range Power Monitor
MSFIS	Main Steam and Feedwater Isolation System
NNSA	National Nuclear Security Administration
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
OCT	Optical Coherence Tomography
ONR	Office for Nuclear Regulation
OPG	Ontario Power Generation
PCS	Plant Control System
PET	Positron Emission Tomography

PPS	Process Protection System
PRNMS	Power Range Neutron Monitoring System
PSMS	Protection and Safety Monitoring System
PWR	Pressurized Water Reactor
RCS	Rod Control System
RIC	Reactor In-Core
RPCLS	Reactor Power Control and Limitation System
RPCT	Radiy Product Configuration Tool
RPS	Reactor Protection System
RRCN	Rolls Royce Civil Nuclear
RTL	Register Transfer Level
SAIC	Shanghai Automation Instrumentation Corporation
SER	Safety Evaluation Report
SEU	Single Event Upset
SCR	Safety Case Report
SMR	Small Modular Reactor
SNPAS	State Nuclear Power Automation System
SNPTC	Chinese State Nuclear Power Technology Corporation
SSLC	Safety System Logic and Control System
SSPS	Solid State Protection System
SSTC NRS	Ukrainian State Scientific Technical Centre on Nuclear and Radiation Safety
STA	Static Timing Analysis
WCNOC	Wolf Creek Nuclear Operating Corporation

8 Bibliography

- [1] Guidelines on the Use of Field Programmable Gate Arrays in Nuclear Power Plant I&C Systems, Epri document 1019181, December 2009.
- [2] Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant I&C Systems, Epri document 1022983, June 2011.
- [3] Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of NPPs, IAEA Nuclear Energy Series, August 2013.
- [4] Lessons learned from using FPGA-based platform for NPP I&C refurbishment, Vladimir Sklyar, 6th International Workshop on the Application of FPGAs in NPPs, IAEA Workshop 2013.
- [5] Use of FPGA-based Components and Systems in CANDU Nuclear Power Plants, John Harber, 6th International Workshop on the Application of FPGAs in NPPs, IAEA Workshop 2013.
- [6] FPGA-based Safety Controller Design and its Application to NPPs, Doosan Corporation, 6th International Workshop on the Application of FPGAs in NPPs, IAEA Workshop 2013.
- [7] FPGA-based DAS System used in Yangjiang Unit 5 / 6, Zhang Chunlei, 6th International Workshop on the Application of FPGAs in NPPs, IAEA Workshop 2013.
- [8] Diversity Strategies for Nuclear Power Plant I&C Systems, NUREG/CR-7007.
- [9] Control and Instrumentation Assessment of the Westinghouse AP1000. (Step 3 of the Generic Design Assessment Process), HSE Division 6 Assessment Report No. AR 09/037-P.
- [10] FitRel Platform Based on FPGA Technology, 5th International Workshop on Applications of FPGAs in Nuclear Power Plants, 2012.
- [11] The Current State of FPGA Technology in the Nuclear Domain, Jukka Ranta, VTT Technology 10, Espoo 12, 2012.
- [12] Darlington Digital Control Computer System Replacement Approach and Experience, http://www.powershow.com/view1/1da9e3-ZDc1Z/Darlington_Digital_Control_Computer_System_Replacement_Approach_and_Experience_powerpoint_ppt_presentation, 3rd International Workshop on the Application of FPGAs in NPPs, IAEA Workshop 2010.
- [13] Feasibility Study of FPGA-based Platforms for Safety Critical Systems, Lawford, M, Bergstra, J., Deng, H., Eles, C., Sullivan, J., Trachimowich, J. McMaster Centre for Software Certification, McSCert Report 3, September 2010.
- [14] I&C Status in France & Recommendations to IAEA, Patrick Salaun, IAEA TWG-NPPIC Meeting, May 2013.
- [15] Safety Evaluation Report Wolf Creek Nuclear Operating Corporation Amendment to Renewed Facility Operating License, Nuclear Regulatory Commission, Amendment No 181, License No NPF-42, March 2009.

- [16] Licensing Field-Programmable Gate Arrays in Safety Systems, Bernard F. Dittman, U.S. NRC, IAEA Workshop 2010.
- [17] Use of FPGA Technology in Implementation of the Logic of the Modernized RCS of the 900 MW EDF Fleet, Julian Bach, NPIC&HMIT, 2010.
- [18] Qualification of Toshiba's FPGA-based Safety Related Systems, Atsushi Kojima, NPIC&HMIT, 2010.
- [19] FPGA-based Technology and Systems for I&C of Existing and Advanced Reactors, E. Bakhmach, International Conference on Opportunities and Challenges for Water-Cooled Reactors in the 21st Century, 2009.
- [20] Design and Qualification of I&C systems on the basis of FPGA technologies, I. Bakhmach, NPIC & HMIT 2010.
- [21] RPC Radiy: FPGA-paved Road to Business Success, Radiy document, September 2014.
- [22] Importance of Modern Instrumentation and Control Systems in Nuclear Power Plants, Oszvald Glockler, Nuclear Safety & Simulation, Vol 4, December 2013.
- [23] Diablo Canyon Power Plant Topical Report, Process Protection System Replacement Diversity & Defence In-Depth Assessment, Pacific Gas & Electric Company, NRC document ML101100647, Rev 0, March 2010.
- [24] Diablo Canyon License Renewal Application, Diablo Canyon Power Plant, November 2009.
- [25] Safety Evaluation Report related to the License Renewal of Diablo Canyon Nuclear Power Plant, Units 1 & 2, US NRC document ML 11153A103, June 2011.
- [26] Diablo Canyon Public Meeting Teleconference Summary, US NRC document ML13329A417, December 2013.
- [27] Digital I&C Upgrades and Regulatory Guidance, Scott Patterson, Instrumentation and Controls Special Section, Nuclear News, 2007.
- [28] Diablo Canyon Power Plant Evaluation for Topical Report Process Protection System Replacement Diversity & Defence-In-Depth Assessment, US NRC document ML110480845, April 2011.
- [29] Diablo Canyon License Amendment Request, US NRC document ML113070457, <http://pbadupws.nrc.gov/docs/ML1130/ML113070457.html>, November 2011.
- [30] Diablo Canyon Acceptance Review of License Amendment Request, US NRC document ML 120120005, January 2012.
- [31] Diablo Canyon License Amendment Request, Pacific Gas & Electric, US NRC document ML11307A331, October 2011.
- [32] Evaluation of the Proposed Change License Amendment Request, US NRC document ML11307A332, October 2011.
- [33] Diablo Canyon Invensys Regulatory Audit Plan, US NRC document ML14126A377, May 2014.
- [34] Diablo Canyon CS Innovations Regulatory Audit Plan, US NRC document ML13029A667, February 2013.

- [35] Diablo Canyon Power Plant Digital Process Protection System Replacement Licensing Experience Using ISG-06, Kenneth Schrader & Scott Patterson, White Paper, http://www.technology-resources.com/White_Papers.html
- [36] Licensing Process for Digital Safety Systems, Norbert Carte, NPIC & HMIT, 2010.
- [37] Lowering the Total Cost of Ownership in Industrial Applications, Altera White Paper, September 2014.
- [38] EasyPath-7 FPGA FAQs, Xilinx document, March 2012.
- [39] Xilinx Third Quarter 2009 Investor Factsheet, Xilinx document, 2009.
- [40] How to Design a FPGA-based I&C, Nuclear Engineering International, 2012.
- [41] Radiy document, <http://radiy.com/en/nuclear/products.html>
- [42] Review Guidelines for FPGAs in Nuclear Power Plant Safety Systems, US NRC document NUREG/CR/7006 ORNL/TM-2009/020, October 2009.
- [43] Digital Instrumentation & Controls Interim Staff Guidance, US NRC document Digital I&C-ISG-06, Revision 1, January 2011.
- [44] Group seeking to build South Texas nuclear reactors passes NRC test, Reuters article, April 2014
. <http://www.reuters.com/article/2014/04/11/utilities-nrg-southtexas-idUSL2N0N31VO20140411> (also <http://public-blog.nrc-gateway.gov/2014/04/22/untangling-foreign-involvement-in-new-reactors/>)
- [45] Summary of the design assessment of Hitachi-GE Nuclear Energy's UK ABWR, Office for Nuclear Regulation, Revision 0, August 2014.
- [46] UK ABWR Generic Design Assessment Chapter 14: Control and Instrumentation, Hitachi document GA91-9101-0101-14000, Revision A.
- [47] Toshiba Topical Report, Toshiba No TOS-TR-GNL-2007-0003, NRC document ML072600331, 2007.
- [48] Toshiba Request to Stop Review, Toshiba No TOS-TR-GNL-2009-0030, NRC document ML091340283, 2009.
- [49] Licensing Topical Report for Toshiba NRW-FPGA-based I&C System for Safety-Related Application, Toshiba document UTLR-0020NP Rev.0, NRC document ML1229A372, October 2012.
- [50] Licensing Topical Report Revision, Toshiba document TOS-CR-FPG-2013-0001, NRC document ML13080A206, March 2013.
- [51] Licensing Topical Report Revision, Toshiba document TOS-CR-FPG-2014-001, NRC document ML14225A051, August 2014.
- [52] Step 2 Assessment of I&C of Hitachi GE's UK ABWR, ONR document ONR-GDA-AR-14-006, Rev 0, August 2014.
- [53] Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design, NRC document, <http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1793/sup2/v1/index.html#abs>, 2011, also <http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1793/>
- [54] Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design, NRC document NUREG-1793,

- <http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1793/initial/index.html>, September 2004.
- [55] NRC Issued Design Certificate for AP1000, NRC website, <http://www.nrc.gov/reactors/new-reactors/design-cert/ap1000.html#ser>
 - [56] AP1000 DAS Planning and Functional Design Summary Technical Report, Westinghouse document APP-GW-GLR-146, NRC document ML102170263, 2010.
 - [57] Generic Design Assessment for the Westinghouse AP1000 nuclear reactor (Step 4 of the GDA), ONR document ONR-GDA-SR-11-002 Revision 0, December 2011.
 - [58] Westinghouse AP1000 GDA Issue: Diversity of PLS, PIMS (inc CIM) and DAS, ONR document TRIM Ref 2011/369299, GDA Issue Reference GI-AP1000-CI-03.
 - [59] Lockheed Martin extends Chinese nuclear cooperation, World Nuclear News, http://www.world-nuclear-news.org/C-Lockheed_Martin_SNPAS_extend_cooperation-1306134.html, June 2013.
 - [60] AP1000 website, ONR, <http://www.onr.org.uk/new-reactors/ap1000/index.htm>
 - [61] AP1000 Pre-construction Safety Case Report, Westinghouse document UKP-GW-GL-732, Rev 2, 2009.
 - [62] Lockheed Martin Nuclear Systems and Solutions, Lockheed Martin document DAL201210006, NRC document ML12299A009, October 2012.
 - [63] Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in NPPs, Epri report TR-107330, December 1996.
 - [64] Submission of Topical Report NuPAC, Lockheed Martin Document Control No NS-LTA-2011-00022, NRC document ML11201A323, June 2011.
 - [65] CAP 1400 Preliminary Safety Review Approved, World Nuclear News, September 2014, <http://www.world-nuclear-news.org/NN-CAP1400-preliminary-safety-review-approved-0909145.html>
 - [66] Planning of Applying FPGA-based Logic Controller in Korea, Yoon Hee Lee, 4th International Workshop on the Applications of FPGAs in NPPs, September 2011.
 - [67] Canada Nuclear Program Instrumentation and Control, Sunil Tikku, IAEA TWG-NPPIC Meeting, May 2013.
 - [68] Radiy Press Release, <http://www.growthmarkets-power.com/contractors/modern-power-systems-bric/rpc-radiy3/>, November 2014.
 - [69] Embalse NPP, Argentina, Life Extension Project, Radiy document 2014.
 - [70] Formal Verification of an FPGA Emulation of the Motorola 6800 Microprocessor, Antoine Druilhe, NPIC & HMIT 2010.
 - [71] Preliminary Validation of an Approach Dealing with Processor Obsolescence, L. Anghel, Tima Lab Research Report ISRN TIMA--RR-03/08-03--FR, 9th IEEE IOLTS, 2003.

- [72] Field Programmable Gate Arrays in Nuclear Power Plant Safety Automation, Lauri Lotjonen, Masters Thesis, Aalto University, 2013.
- [73] Current Issues Associated with the Implementation of Field Programmable Gate Arrays in the Nuclear Power Industry, Steven Arndt, US NRC, NPIC&HMIT, 2012.
- [74] Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update, US NRC document NUREG/CR-6992, 2009.
- [75] Regulatory Perspectives on FPGA Technology, Steven Arndt, US NRC, 7th International Workshop on the Application of FPGAs in Nuclear Power Plants, October 2014.
- [76] Qualification of FPGA-based I&C Applications for NPPs, Anton Andrashov, Radiy, 7th International Workshop on the Application of FPGAs in Nuclear Power Plants, October 2014.
- [77] FPGA-based Applications: Challenges and Drivers, Vladimir Sklyar, Radiy, 7th International Workshop on the Application of FPGAs in Nuclear Power Plants, October 2014.
- [78] Use of FPGA to Face Electronic Component Obsolescence in Software Based Safety I&C in NPPs, Abdellah Hadj and Julien Bach, Rolls Royce, ENC 2010 Transactions (p 55).
- [79] Component Interface Modules, Westinghouse document NA-0105, September 2011.
- [80] Advanced Logic System Post-accident Monitoring System, Westinghouse document NA-0117, July 2012.
- [81] ALS V&V Plan, Westinghouse non-proprietary document 6002-00003-NP, Rev 7, NRC document ML 12332A274, October 2012.
- [82] Email from Stephen Seaman, Westinghouse, 12/11/2014.
- [83] Advanced Logic System Topical Report, CS Innovations document 6002-00301-NP Rev 1, NRC document ML102570797, August 2010.
- [84] Safety Evaluation Report for Topical Report 6002-00301 Advanced Logic System, US NRC document ML13218A979, September 2013.
- [85] FPGA Technology Used at Temelin NPP, Herbert Waage, NPIC&HMIT, 2012.
- [86] Implementing Nuclear Safety Systems with an FPGA Platform, James Beck, Westinghouse ALS-NGSSP-14-014, 7th International Workshop on the Application of FPGAs in NPPs, 2014.
- [87] Lockheed Martin Nuclear Systems and Solutions, Lockheed Martin presentation, 7th International Workshop on the Application of FPGAs in NPPs, 2014.
- [88] FPGA based Protection System for Small Modular Reactors, Jason Pottorf, 7th International Workshop on the Application of FPGAs in NPPs, 2014.
- [89] IEC 62566: Development of HDL-programmed integrated circuits for systems performing Category A functions, Edition 1.0, 2012.
- [90] IEEE Standard for Software Verification and Validation, Summary of IEEE Std 1012 - 2004, IEEE Computer Society presentation, 2008.
- [91] Method for Performing Diversity and Defence-In-Depth Analyses of Reactor Protection Systems, NUREG-CR-6303, 1994.

- [92] IEC 61513: Nuclear Power Plants - I&C for Systems Important to Safety - General Requirements, Edition 1.0, 2001.
- [93] IEC 61226: Nuclear Power Plants - I&C for Systems Important to Safety - Classification of Instrumentation and Control Functions, Edition 2.0, 2005.
- [94] IEEE 7-4.3.2 - IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations, 2010.
- [95] Safety Design of a Nuclear Power Plant, STUK Guide YVL B.1, November 2013.
- [96] Electrical and I&C Equipment of a Nuclear Facility, STUK Guide YVL E.7, November 2013
- [97] Lockheed Martin Success Story,
http://s3.mentor.com/public_documents/success_story/products/fv/success/lockheed_martin_fpga_success.pdf
- [98] Lockheed Martin Press Release: Safety Control Solutions,
<http://www.lockheedmartin.co.uk/content/dam/lockheed/data/mfc/pc/nuclear-systems-and-solutions-nss/mfc-nuclear-systems-and-solutions-nss-pc-03-safety-control.pdf>
- [99] Support for NRC Review of Lockheed Martin NuPAC, Southern California Edison document, NRC document ML112860071, October 2011.
- [100] Licensing Topical Report for Generic Qualification of the NuPAC Platform, Lockheed Martin / SNPAS document NuPAC_ED610000-047-P, Rev B, NRC document ML13289A270, January 2012.
- [101] Wolf Creek Issuance of Amendment Re: Modification of the MSFIS, US NRC document ML ML090610317, March 2009.
- [102] IEC 61508, Functional Safety of Electrical / Electronic / Programmable electronic safety-related systems, 2010.
- [103] Microsemi website, <http://www.microsemi.com/products/fpga-soc/soc-fpga/smartfusion2>
- [104] High Integrity Systems, Wittenstein website,
<http://www.highintegritysystems.com/wittenstein-high-integrity-systems-extends-safety-critical-rtos-support-microsemis-smartfusion2-soc-fpgas/>
- [105] EasyPath-7 FPGAs, Xilinx Product Brief,
http://www.xilinx.com/publications/prod_mktg/EasyPath7-Product-Brief.pdf
- [106] Radix product website, <http://radix.com/en/nuclear/products/fpga-based-safety-and-safety-related-i-c-systems.html>
- [107] ALS Management Plan, Westinghouse document 6002-00000-NP, Rev 7, NRC document ML12332A15, October 2012.
- [108] SNPAS public website, <http://www.snpas.com.cn/en/CompanyBrief/>, 2014.
- [109] Email from Zeng Hai, 14th November 2014.
- [110] Standard Review Plan, Branch Technical Position 7-14, US NRC document ML070670183, March 2007.

- [111] Verification, validation, reviews and audits for digital computer software used in safety systems of nuclear power plants, US NRC Regulatory Guide RG 1.168, February 2004.
- [112] IEEE Standard 1028, IEEE Standard for Software Reviews and Audits, 2008.
- [113] Criteria for use of computers in safety systems of nuclear power plants, US NRC Regulatory Guide RG 1.152, July 2011.
- [114] Software reliability and safety in nuclear reactor protection systems, U.S. NRC, NUREG/CR-6101, UCRL-ID-114839, June 1993.
- [115] IEEE Standard 603 - Standard Criteria for Safety Systems for Nuclear Power Generating Stations, 2009.
- [116] Nuclear Power Plant Systems, Structures and Components and their Safety Classifications, STUK Guide YVL2.1, June 2000.
- [117] Developing Safety Critical Applications that Meet IEC 61508 Standards, Microsemi document http://www.newelectronics.co.uk/image-store/articles/49294%5CSafety_Critical_WP.pdf, March 2013
- [118] FPGAs Advance Medical Imaging, Medical Electronics Design article <http://www.medicalelectronicsdesign.com/article/fpgas-advance-medical-imaging>, October 2011.
- [119] Medical Imaging Using FPGAs, Altera white paper WP-Medical-2.0, July 2010.
- [120] Today's FPGA Trends in Aerospace and Defence Applications, Military & Aerospace Electronics, <http://www.militaryaerospace.com/articles/2011/01/today-s-fpga-trends.html>, December 2014.
- [121] Suitability of reprogrammable FPGAs in space applications, Sandi Habinc, Gaisler Research report FPGA-002-01, Version 0.4, September 2002.
- [122] ASIC and FPGA for space applications, European Space Agency, DCIS keynote presentation, November 2010.
- [123] FPGA-based NPP Instrumentation And Control Systems: Development And Safety Assessment, V.S. Kharchenko, Radiy, ISBN 978-966-96770-2-0, 2008.
- [124] NRC shoots down Texas nuclear plant expansion, news article, <http://bizbeatblog.dallasnews.com/2013/04/nrc-shoots-down-texas-nuclear-plant-expansion.html/>, 2013.
- [125] NRG ends project to build new nuclear reactor, news article, <http://www.dallasnews.com/business/energy/20110419-nrg-ends-project-to-build-new-nuclear-reactors.ece>, April 2011.
- [126] Justification of an FPGA-based System Performing A Category C Function: Development of the Approach and Application to a Case Study, Sofia Guerra, NPIC&HMIT, 2012.
- [127] SSMFS: 2008, Swedish Radiation Safety Authority, <http://www.stralsakerhetsmyndigheten.se/Publikationer/Forfattning/SSMFS-2008/SSMFS-20081/>

- [128] Chinese reactor design passes safety review, World Nuclear News article, <http://www.world-nuclear-news.org/NN-Chinese-reactor-design-passes-safety-review-0812145.html>, December 2014.
- [129] Strategy and Feasibility Plan for HPD / Emphasis Integration, Adelard document D/791/43123/1, v2.0, August 2014.
- [130] TUV-qualified FPGAs for Functional Safety Design, Altera website, <http://www.altera.co.uk/end-markets/industrial/functional-safety/ind-functional-safety.html>, December 2014.
- [131] Xilinx All Programmable Functional Safety Design Flow Solution, Product Brief PB015, July 2014.

9 Nordic standards and FPGAs

The following table identifies those clauses in [95] and [96] which are relevant to FPGAs. We have reproduced the wording, and provided a brief explanation of the relevance of the clause and any minor concerns about the ability of FPGA-based systems to comply.

Clause	Wording	FPGA impact
312	The design of systems important to safety shall be based on a life-cycle model where design and implementation are divided into stages. The life-cycle model shall comprise all successive stages from the determination of the applicable requirements to the operation stage. In particular, the life-cycle model shall include a separate requirement specification stage that precedes the actual design stages.	All FPGA development lifecycles which we have surveyed, across a number of suppliers, satisfy this clause.
340	The accuracy, completeness and consistency of the requirement specification of systems important to safety shall be assessed by experts who are independent of the design and implementation process. The assessment report shall present the observations made as well as a justified conclusion.	Historically, this clause may have presented some concerns due to the relatively small number of people experienced ("expert") in FPGAs. As discussed in Section 2.3, however, this is unlikely to be a current issue.
348	The solutions and methods chosen during the course of the design shall be based on proven technology and operating experience, and they shall be in compliance with the applicable standards. The design shall strive for simplicity. If new solutions are proposed, they shall be validated through tests and experiments.	Although FPGAs may be relatively novel in the nuclear industry, there is a large body of evidence relating to their use in alternative fields, which may aid in a claim that they represent proven technology.
354	Additionally, failure tolerance analyses shall consider human errors and demonstrate that single errors will not prevent the performance of the safety function concerned.	Single Event Upsets (unintentional changes of state in an FPGA) need to be mitigated against. Individual chip suppliers provide a range of

		mitigation against these, which may influence choice of supplier.
404	All the systems, structures and components of a nuclear power plant shall be so designed as to ensure that they perform reliably under design-basis environmental conditions. Environmental conditions to be considered in the design shall include, as appropriate, vibration, temperature, pressure, electromagnetic effects, radiation, humidity, and combinations of these conditions.	Radiation-tolerant FPGAs are available from a number of suppliers, but the extent to which environmental qualification is carried out by suppliers is likely to vary.
407	Every effort shall be made to ensure the independence of the design solutions from any single technology. Due consideration shall be given to potential technological developments in order to enable future replacements of components in a controlled and timely manner.	The use of FPGAs (in conjunction with microprocessors) provides diverse technology as required by this clause. In addition, a number of FPGA replacements we surveyed were prompted by obsolescence of the original microprocessor-based systems.
409	In the design, due account shall be taken of security aspects to minimise potential conflicts between safety and physical protection considerations. Due consideration shall be given to cybersecurity in the design of a nuclear power plant. Specific requirements pertaining to security arrangements are provided in Guide YVL A.11 and those pertaining to information security in Guide YVL A.12.	FPGA-based systems typically do not offer as many avenues for cyber security attacks, in that they do not contain general-purpose components which can be used maliciously or to an unintended purpose.
5205	The safety significance of the information technology tools and testing methods (such as computational software, software compilers and testing tools) used in the design of I&C systems shall be assessed in terms of the end product being designed. The tools used in the design and implementation of safety-classified systems shall be identified. If the quality of a tool or testing method is of direct significance to the proper functioning or failure rate of the end product, it shall be qualified for its	FPGA development tools are not always qualified to external safety standards, and in particular the use of IP cores can be problematic. The need for tool qualification data may influence the choice of supplier.

	intended use. Detailed requirements for the qualification of tools are specified in Guide YVL E.7. Each tool version shall be specifically qualified.	
5209	It must be possible for operators to actuate the systems providing safety functions as well as the I&C functions manually from the control room, if this is deemed necessary to ensure safety.	Although FPGAs are not typically used in systems which have significant HF issues, this requirement should be assessed when considering platform suppliers.
5215	The instrumentation for monitoring the nuclear reactor shall be so designed as to provide sufficiently accurate and reliable input data for the determination of the reactor power distribution and the reactor's thermal margins. Necessary calculations of these reactor parameters shall be conducted automatically and with a frequency necessary to ensure the maintenance of the operating conditions of the reactor.	FPGAs are able to execute functions faster than microprocessors in some cases owing to higher clock speeds.
5252	The factory tests shall cover all system functions and time settings, failure behaviour and, where possible, self-diagnostic functions. Simulators shall be used as testing aids in both the tests intended to demonstrate system conformance and in the actual validation tests. In case of modifications, the need for simulator testing shall be evaluated with due regard to the extent of the modification.	Simulation during verification and validation has been a significant part of all FPGA development lifecycles we have surveyed.

Table 3: Clauses of [95] relevant to FPGAs

Clause	Wording	FPGA Impact
116	The design, manufacture and installation of electrical and I&C equipment and cables of nuclear facilities shall take into account the regulations issued by authorities other than STUK that are in force in Finland. These include safety standards concerning the safety of electrical equipment and occupational safety for electrical work, and the instructions provided by authorities supervising electrical safety (such as standard series SFS 6000: Low-voltage	Although this is unlikely to impact FPGA-based systems specifically, the regulations issued by authorities other than STUK must be considered to determine whether an FPGA-based system can be shown to be compliant with these.

	electrical installations, standard SFS 6001: High-voltage electrical installations, and standard SFS 6002: Safety at electrical work), and the regulations and guidelines concerning machine safety. Compliance with the electrical safety and machine safety legislation is monitored by competent authorities.	
311 - 312	The design, manufacture and testing of I&C equipment in safety class 2 and essential accident instrumentation shall be primarily based on nuclear industry standards and guidelines, if applicable nuclear industry standards exist. The design, manufacture and testing of I&C equipment in safety class 3 shall employ applicable international I&C equipment standards.	Although this clause is no longer a concern, FPGA usage in the nuclear industry has previously been affected by a lack of accepted international standards. The standards shown in Section 5 may all be considered relevant.
338 511 - 512 601 - 651	"Software-based technologies", "software"	These clauses must be taken as applying to FPGA-based systems, as well as to "pure" software systems.
550	Prior to accident condition testing, the test pieces of electrical and I&C equipment and cables shall be artificially aged to correspond to their planned service life.	It is not clear what artificial aging of an FPGA-based system would involve, and compliance with this clause should be discussed with the supplier prior to selection of an FPGA-based system.
571	The third party authorised to perform the type inspection and type conformity assessment of an component shall be a certification body that has been accredited for the conformity evaluation of the applied standards under standard SFS-EN ISO/IEC 17065 [6], or an inspection organisation accredited for a similar task under standard SFS-EN ISO/IEC 17020 [7]. In order to supervise the testing, the certification body or inspection organisation shall have applicable qualifications under standard SFS-EN ISO/IEC 17025 [8]. The	Historically, this clause may have presented some concerns due to the relatively small number of people and organisational bodies with significant experience in FPGAs. As discussed in Section 2.3, however, this is unlikely to be a current issue.

	certification body or inspection organisation shall also be a notified body appropriate for the task.	
625 - 630	Requirements on software tools	FPGA development tools may not be externally qualified to an acceptable standard (although all we have examined are qualified internally). Availability of qualification data on the development tools may influence the choice of supplier.

Table 4: Clauses of [96] relevant to FPGAs

FIELD PROGRAMMABLE GATE ARRAYS IN SAFETY RELATED INSTRUMENTA- TION AND CONTROL APPLICATIONS

Field-programmable gate arrays, FPGAs, are high-density logic chips with the ability to simulate any digital logic design with logic gates and registers. A number of advantages have been identified in this report, for example reduced overall function execution time, easier separation of logically independent functions and reduced vulnerability to obsolescence. Disadvantages identified include the relatively limited prior experience of the nuclear industry with FPGAs, their unsuitability for some complex functions which include human factors applications, and the potential difficulty in justifying the pre-developed FPGA-specific libraries. Within the nuclear industry, a number of applications of FPGA usage across multiple regulatory regimes are described.

Ett nytt steg i energiforskningen

Energiforsk är en forsknings- och kunskapsorganisation som samlar stora delar av svensk forskning och utveckling om energi. Målet är att öka effektivitet och nyttiggörande av resultat inför framtida utmaningar inom energiområdet. Vi verkar inom ett antal forskningsområden, och tar fram kunskap om resurseffektiv energi i ett helhetsperspektiv – från källan, via omvandling och överföring till användning av energin. www.energiforsk.se