ADELARD

FPGAs in Safety Related I&C Applications in Nordic NPPs

Energiforsk/ENSRIC Project

Sofia Guerra, with Catherine Menon and Sam George
27 October 2016

PT/435/150002/3

Exmouth House 3–11 Pine Street London EC1R 0JH
T +44 20 7832 5850 F +44 20 7832 5853 E office@adelard.com W www.adelard.com

Adelard

- **Adelard LLP is an independent product and services company supporting its clients to achieve safe, dependable and secure systems.**
- 29 years of consultancy and training
- Developer of numerous safety standards
- Author of many safety justifications- civil and defence sectors
- Assessed many safety cases - defence and civil
- Developed and assessed critical software
- Research into safety and dependability
- Develops and markets the Assurance Safety Case Environment (ASCE) tool

Outline

- Background
- Are FPGA-based systems feasible for future Nordic applications?
- Implications of FPGA-based solutions in terms of V&V

Background to presentation

- Two projects funded by Energiforsk/ENSRIC on FPGAs
- 2014/2015
  - Investigate whether FPGA-based systems are feasible for future programs in Nordic NPPs
- 2015/2016
  - Implications of FPGA-based solutions (on V&V)

Project aims

- Investigate whether FPGA-based systems are feasible for future programs in Nordic NPPs
- Three major aspects
  - Review of applications
    - Current and historical use of FPGAs across different licensing regimes
  - Market availability
    - Chip suppliers
    - Platform suppliers
  - Standards in the Nordic environment
    - Survey of standards relevant to FPGA use
    - Review and focus on Nordic standards

Outline

- Background
- 1st Project
- 2nd Project

1st Project outline

- Intro: What are FPGAs?
- Task 1: Review of applications
- Task 2: Market availability
- Task 3: Standards in Nordic countries

FPGA introduction

- FPGAs are high-density logic chips that can simulate any logic design
  - Chips contain configurable logic blocks and I/O blocks
  - These are connected to produce a processing function implemented directly in hardware
    - The way the blocks are physically connected defines the function performed

- Three types of FPGA
  - SRAM – configuration stored in volatile memory, so lost on power loss. Requires external memory
  - Flash – configuration stored in non-volatile memory
  - Anti-fuse – non-reprogrammable FPGA where configuration is burnt onto the chip

Regulatory aspects

- FPGA development is similar to software development
  - General consensus among regulatory regimes that FPGAs should be treated as software
- IP cores can be a regulatory concern in safety-critical systems
  - Pre-developed libraries for performing certain functions
    - For example, floating-point arithmetic, signal processing
  - May be provided by chip supplier, or a third party
  - Can be difficult to assure design and development to standard required
    - NB: use is not necessary, as seen in the approach taken by many safety-critical applications

FPGA advantages

- Can process independent functions in parallel and reduce overall function execution time
- RTL is circuit-independent, so reuse on different chips does not require re-qualification of application logic
  - Mitigates potentially costly obsolescence issues
- Separation of logically independent functions
  - Execution independently and in parallel
- Security advantages: FPGAs reduce the possibility of malicious tampering
- Suitability for use in diverse systems with microprocessor based alternative

FPGA disadvantages

- Relatively short history of use in nuclear industry means there is little cultural familiarity with FPGAs
  - Potential problems with licensing – how do you know what you need to do?
- IP cores can be difficult to justify
- Not well-suited for complex human factors applications

Task 1: Review of installations

- Identified safety-related FPGA-based applications in nuclear and non-nuclear sectors
- Nuclear applications categorised by country / licensing regime
  - Identify history of implementation
  - Early experiences and lessons learnt
  - Other options considered
- Includes
  - Sweden and Finland
  - US, UK, France, Czech Rep
  - Ukraine, and Bulgaria
  - Canada and Argentina
  - Japan, China, South Korea
  - Taiwan

Task 2: Market availability and suppliers

- Two types of suppliers: chip suppliers and platform suppliers
- Chip suppliers provide FPGA circuits, also typically software tools for developing FPGA applications
  - Typically supply “families” of chips used for different purposes
- Platform suppliers provide entire platform to NPPs, including FPGA application, interfaces with other components
  - Typically focus on a single major platform, which may be customised to provide different functionality

Task 3: Standards and Nordic environment

- Relevant standards can be divided into four major categories:
  - General nuclear standards
    - STUK Guide YVL B.1, IEEE Std 603
  - Digital I&C equipment in a safety-related role
    - STUK Guide YVL E.7, IEC 61508, IEC 61513
  - Software development methodologies
    - IEEE 1012, IEEE Std 1028
  - FPGA-specific standards
    - Until recently there was little in the way of specific FPGA guidance

Nordic standards

- YVL B.1, YVL E.7 and SSM regulations SSMFS 2008:1
  - Assessed these clause-by-clause to identify areas of concern regarding FPGAs
  - No significant findings – some minor terminology differentiation
  - Can reasonably be used in a framework of FPGA-specific guidance to incorporate FPGAs in nuclear power plants

FIELD PROGRAMMABLE GATE ARRAYS IN SAFETY RELATED INSTRUMENTATION AND CONTROL APPLICATIONS

REPORT 2015:112

Conclusion of first project

- FPGAs may play a role in future modernisation programs of I&C systems in Nordic NPPs
- What are the implications of FPGA-based systems in Nordic NPPs?
  - Focus on verification and validation
  - How do they compare to microprocessor based solutions?

Outline

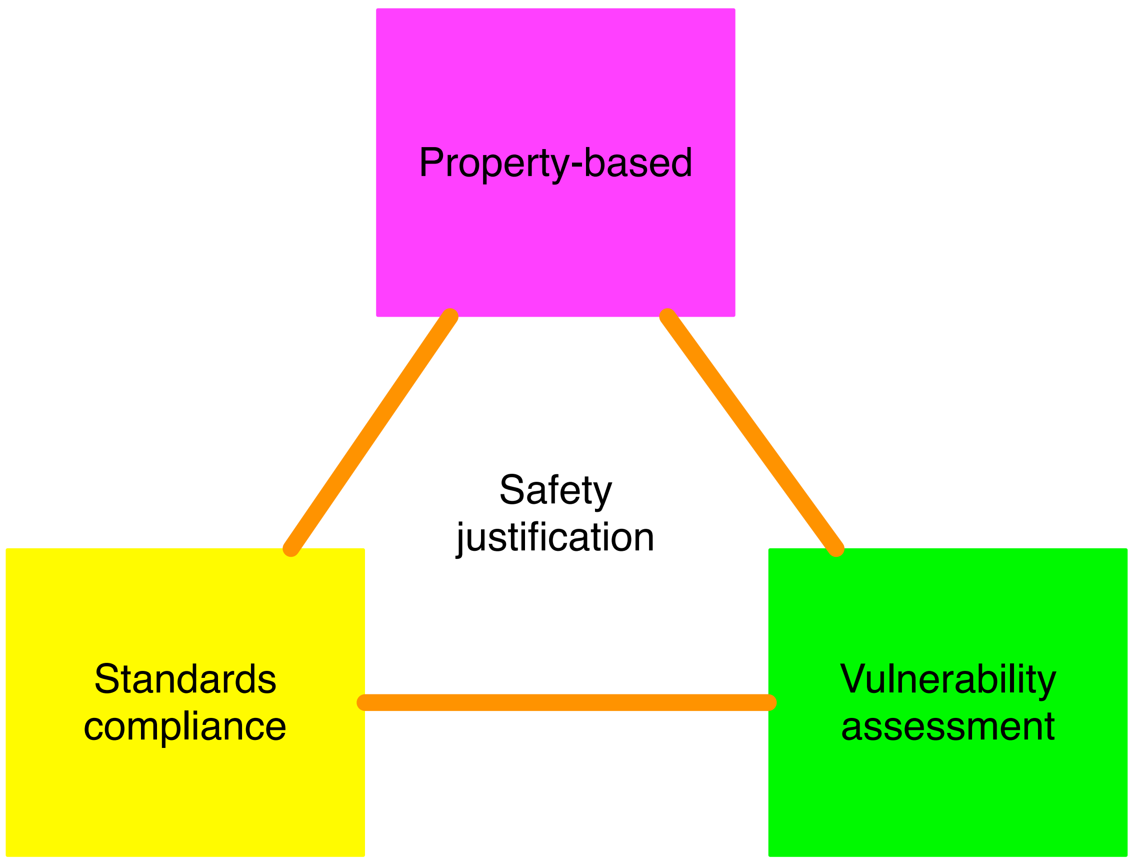
- Background
- 1st project
  - What are FPGAs?
  - Review of applications
  - Market availability
  - Standards in Nordic countries
  - Workshop
- 2nd project
  - Objectives
  - Approach
  - Conclusion

Objective

- Review verification and validation activities needed to implement an application in an FPGA-based product
- Compare with what might be equivalent for a microprocessor based application

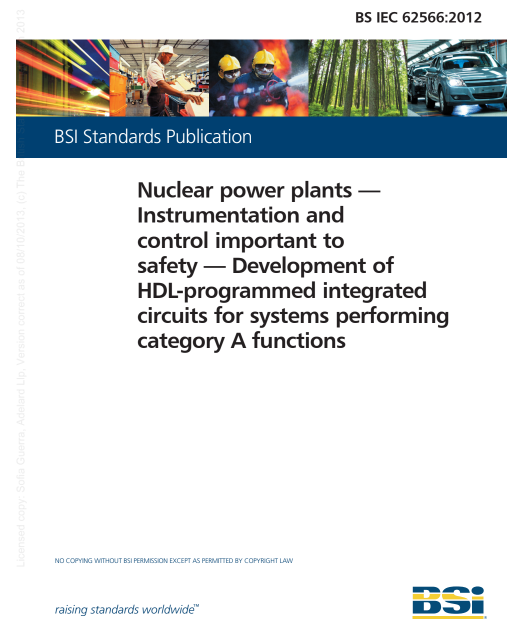
- What does equivalence mean?
  - Different activities have different objectives
  - Different levels of assurance
- Focus on their contribution to the safety demonstration
- Systems implementing safety functions (as Cat A in IEC 61226)

Strategy triangle of safety demonstration



Standards compliance

- Compare verification and validation required by comparable standards for FPGA-based and software-based systems
- IEC 62566 and IEC 60880



Comparison

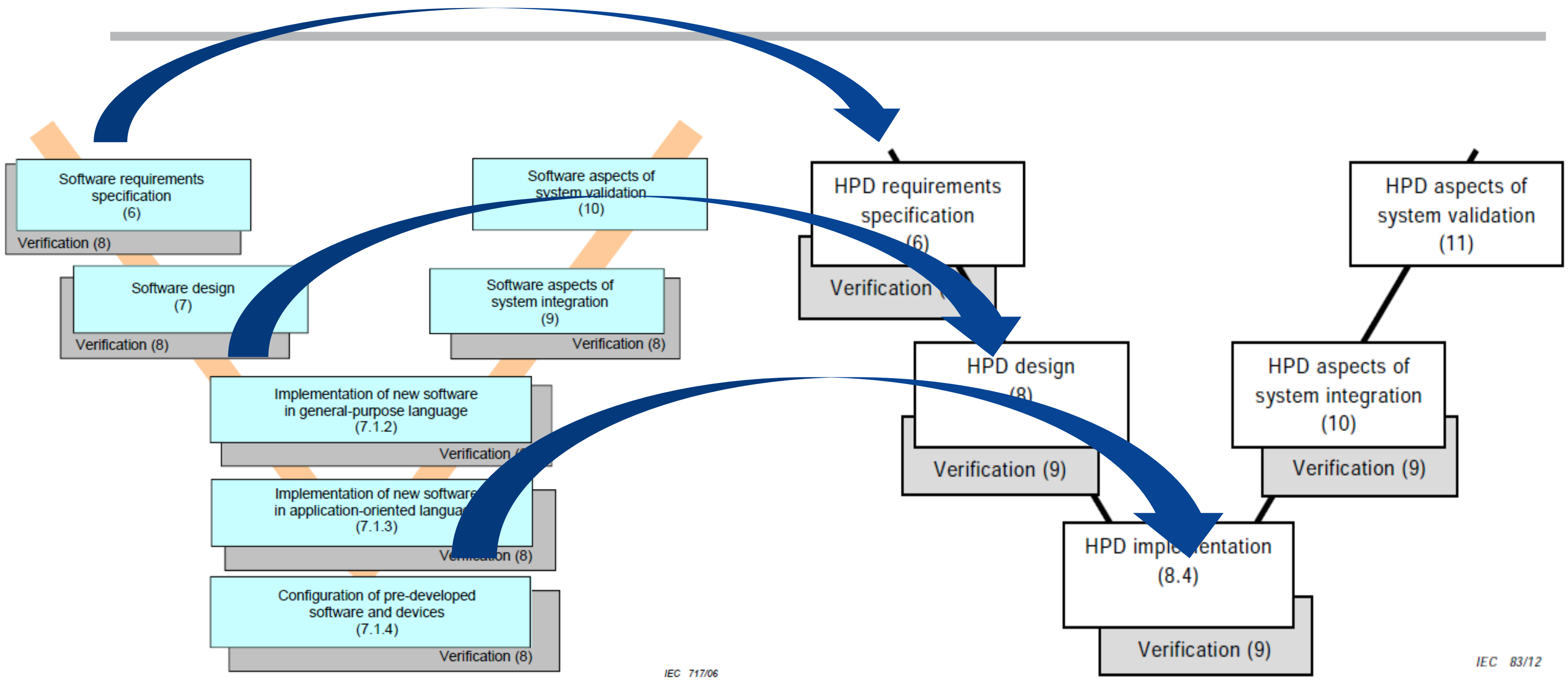


Figure 2 – Development life-cycle of HPD

Figure 3 – Development activities of the IEC 60880 software safety lifecycle

Red – differences

Green – text required for clarity

Black- common

Comparison

	IEC 60880	IEC 62566
Coverage and types	Adequacy of design specification down to module level Decomposition of design into modules wrt technical feasibility, testability, readability, modifiability Code verification to begin with source code analysis then module testing Full testing guidance given in Appendix E Module verification to show that all modules perform intended functions and not unintended functions	Each module to be specifically tested, and all features mentioned in the requirements spec Adequacy of design specification down to module level Decomposition of design into modules testability, understandability, modifiability Static verification to include type / syntax checking, parameter checking, OOR checks, completeness of sensitivity list and cases, detection of dead states and side effects, logical and physical Design Rule Checks Tests should be performed for worst case and best case, and test results documented
Criteria	Test coverage criteria to be justified and documented	Criteria shall be documented and analysed to show sufficiency for requirement spec If a criteria isn't achieved then a justification must be provided
Tools	Automated tools may be used for code verification Tools shall be qualified as per requirements of the standard	
Documentation	Verification plan, established before any verification activities, documents all criteria, techniques and tools Plan includes selection of verification strategies, selection and utilisation of tools, execution of verification, documentation, evaluation of verification results Verification plan shall identify any evidence needed to confirm extent of testing Results of verification shall be documented, including	Verification plan, established before any verification activities, documents all criteria, techniques and tools Plan includes selection and justification of verification strategies, selection and utilisation of tools, execution of verification, documentation, evaluation of verification results All verification strategies to be justified Verification plan to document all tests including goals, criteria and expected results

Standards comparison

- No significant differences
- IEC 62566 less prescriptive about specific documents than IEC 60880
- Some difference on specific requirements due to differences in technology, e.g., static timing analysis

Behavioural properties

- Aims to show that the behaviour of the system or component is met
- The exact set of attributes would need to be defined for the system under consideration

Behavioural properties

Property		Discussion
P1	Functionality	The function performed by the system
P2	Timing	Includes time response, permissible clock frequencies, propagation delays, etc.
P3	Accuracy	Affected by analogue/digital conversion, processing functions, IP cores
P4	Availability	Readiness for correct service, a system-level attribute supported by component attributes
P5	Fault detections and tolerance	Internal detection of faults
P6	Robustness	Tolerance to out-of-normal inputs and stressful conditions
P7	Failure recovery	The ability to recover from failures

Discussion of techniques

V&V area	Microprocessor V&V	FPGA V&V
Techniques/approach	*Description* *Effectiveness/cost*	*Description* *Effectiveness/cost*

Techniques discussed include

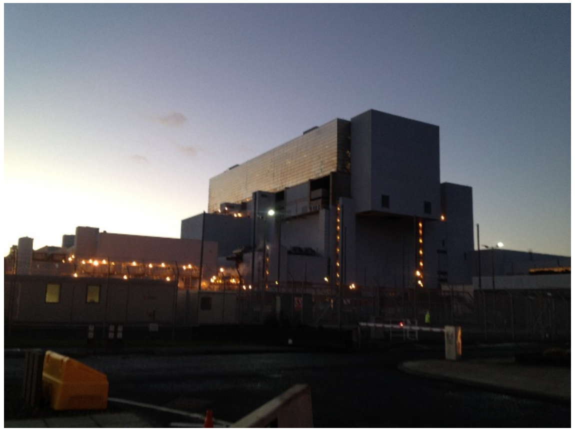
- Code review
- Functional testing
- Formal verification
- WCET
- Static timing analysis
- Response time tests
- etc

Behavioural properties (2)

- Functionality – e.g. multithreaded/concurrent design – difficult to achieve reliably in microprocessor-based systems
- Worst case execution time
- Robustness of hardware and parameters checking

Vulnerabilities

- Vulnerabilities are weaknesses in a system
- They could lead to a hazardous situation, but are not strictly a hazard
- Consider different types of vulnerabilities for FGPA-based systems, and compare with vulnerabilities for microprocessor based systems, and how absence of these can be shown



Format

Vulnerability	FPGA		Microprocessor	
	Explanation	V&V	Explanation	V&V
Timing errors				
Initialisation design errors				
Translation errors				
Incorporation of third-party designs …				

- And technology-specific issues
  - SRAM, Antifuse, Flash

FPGAs - vulnerabilities

- Assume constraints imposed by IEC 62566 hold, e.g.,
  - Synchronous design
  - Adherence to coding rules
- Mainly concern the tools used to refine an HDL specification into a deployed FPGA.
- IEC 62566 mandates that all RTL designs be fully synchronous, if maximum logic propagation times for combinatorial logic do not generate unsynthesisable timing constraints
  - FPGA-specific timing vulnerabilities can in principle be reduced to toolchain vulnerabilities.
- Some vulnerabilities of microprocessor-based solutions are not applicable to FPGAs
  - E.g. processor interrupts

Conclusions

- We compared V&V techniques for FPGAs and microprocessor – based systems
  - Requirements from standards
  - Behaviour based analysis
  - Vulnerabilities associated with the different technologies
- Few significant differences identified as result of standards comparison
- Treatment of timing and concurrency different
- Typical vulnerabilities of microprocessors are absent from FPGAs, but possible issues with lack of transparency of code artefacts
- More comprehensive toolset for FPGAs


VERIFICATION AND VALIDATION TECHNIQUES FOR I&C APPLICATIONS IN NORDIC NPPS
REPORT 2016:268
ENSRIC
Energiforsk