UDC 004.41

G. SCHNÜRER

Institute for Safety Technology (ISTec), Garching, Germany

SPECIFICATION OF REQUIREMENTS FOR THE IMPLEMENTATION OF ASICS AND FPGA IN I&C SYSTEMS IMPORTANT TO SAFETY IN GERMAN NPP

This paper gives an overview concerning the design as well as the verification and validation of Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGA) in German NPP which are applied to carry out I&C functions. The qualification procedures dealt with are restricted on ASICs without any microcontroller core. Thus these ASICs are implemented on the basis of a hardware configuration, generated by development tools. Presently, just that kind of ASICs are relevant for German NPP. Dependent on the different safety categories, recommendations concerning the qualification level and procedures are elaborated which have to be achieved for ASICs and FPGA. Requirements are also introduced for the implementation of ASICs and FPGA in I&C systems important to safety, which are in accordance with German and international regulations and guidelines as well as additional specific requirements. Additional, important aspects within the framework of the expert judgement for upgrading of safety relevant I&C by ASICs and FPGA are dealt with. These aspects are of general character and are mainly focused on suitability test procedures and robustness requirements of ASICs and FPGA.

ASIC, FPGA, VHDL, I&C, validation

Introduction

The high safety standard in German nuclear power plants requires a consequent and formal assessment procedure for all systems and components important to safety in view of reliability and functionality. This paper deals with different safety aspects, whether application specific integrated circuits (ASICs) or field programmable gate arrays (FPGA), respectively, are performing safety functions with the same quality level like conventional hardwired I&C systems and components. Because of ASICs and FPGA actually do have an innovative character for German nuclear power plants, safety relevant requirements and guidelines are to elaborate on the basis of already existing national and international nuclear standards in view of hardware qualification procedures and the adoption of application specific issues, like tool validation.

Therefore, already well known properties like robustness against radiation and the determinable functional status, even in case of system failures or faults are promoting the innovation of ASICs and FPGA in German nuclear power plants. Furthermore, the determination and quantification of reliability data of ASICs seems to be possible by well established methods like a failure mode analysis; provided the ASIC application is based on a fixed logic without any micro-controller core.

Last but not least it should be possible to replace and to renew components (electronic cards or sub-assemblies) in electronic cabinets important to safety without affecting the overall I&C concept and design. This eases also the licensing and assessment efforts, provided the new ASIC based component is qualified by type test and suitable test procedures. The redesign of hardwired I&C components by means of sub-assemblies and its qualification is the main focus of this paper.

Software programmed ASICs are not implemented in German NPP, and are not treated in this paper. Consequently these ASIC based components consist of a hardware configuration designed by ASIC development software tools.

An additional concept besides ASICs is the use of FPGA. FPGA contain pre-configured functional blocks, which are to connect by the user to the desired logic via a configuration procedure. This paper presents also information concerning verification, validation and qualification of FPGA based components in view of the redesign of hardwired I&C components by FPGA based sub-assemblies.

1. Layout, design and construction of ASICs

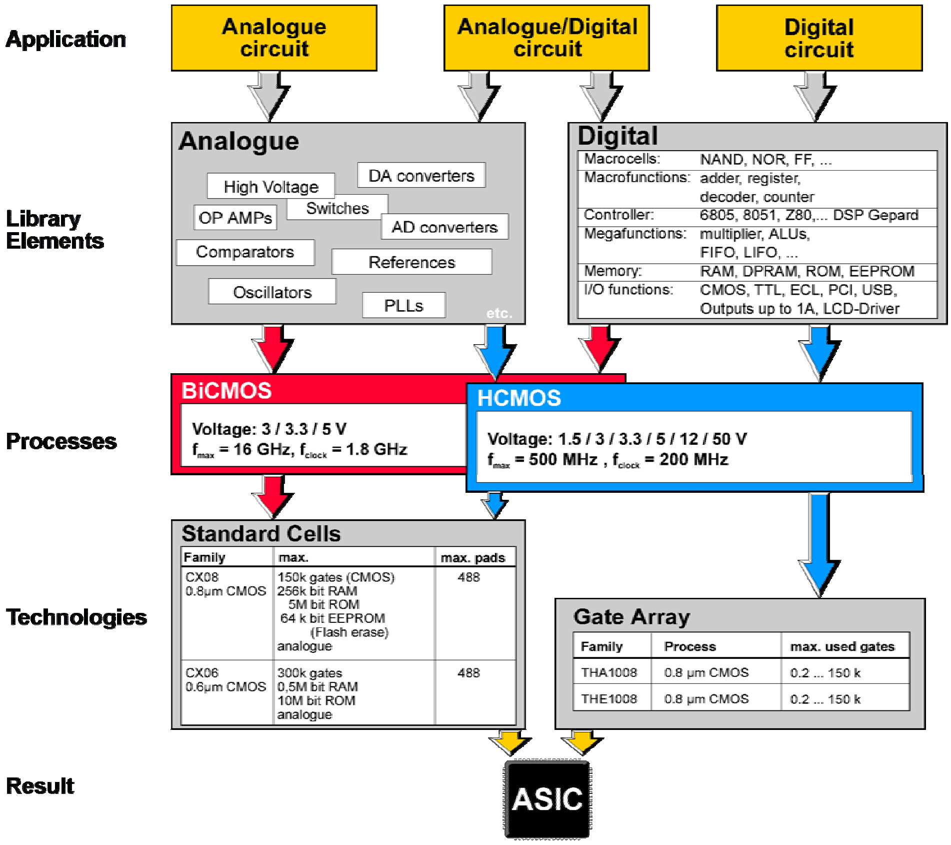
The design flow for safety related ASIC can be performed by different methods and procedures. Examples are the full custom, macro core, standard cell and gate array design flow. Within the full custom design flow each element of the core has to be designed according to the applicant specification. This procedure offers great flexibility but demands the highest effort. The other procedures (macro core, standard cell and gate array design flow) do have a lower effort because of already dedicated elements located in a library.

Analog to the programming languages like FORTRAN, PASCAL and C++, hardware specific languages for ASICs are established. Advantages of the hardware description language (HDL) are:

- The language is the interface communication between designers.
- A formal specification via the language is possible.
- The language supports the documentation of the development.
- The design can be simulated.
- The design is in-dependant from the technology.
- The language is the basis for an integrated and automatized development process.

At present, the language VERILOG is very common in the USA whereas VHDL is more common in Europe. The efficiency of both hardware description languages is comparable.

The design flow (e.g. via VHDL) is characterized as follows:



Macrocells:	NAND, NOR, FF, ...
Macrofunctions:	adder, register, decoder, counter
Controller:	6805, 8051, Z80,... DSP Gepard
Megafunctions:	multiplier, ALUs, FIFO, LIFO, ...
Memory:	RAM, DPRAM, ROM, EEPROM
I/O functions:	CMOS, TTL, ECL, PCI, USB, Outputs up to 1A, LCD-Driver

Standard Cells

Family	max.	max. pads
CX08 0.8µm CMOS	150k gates (CMOS) 256k bit RAM 5M bit ROM 64 k bit EEPROM (Flash erase) analogue	488
CX06 0.6µm CMOS	300k gates 0,5M bit RAM 10M bit ROM analogue	488

Gate Array

Family	Process	max. used gates
THA1008	0.8 µm CMOS	0.2 ... 150 k
THE1008	0.8 µm CMOS	0.2 ... 150 k

Fig. 1. Overview of the ASIC-development-process

According to the task description the specification should be elaborated in VHDL-language. After this the development of the task on VHDL-modules will follow. These VHDL-modules are to be simulated successfully on the test bench. The simulation is followed by the syntheses-procedure (design will be transferred to the target technology). The syntheses delivers the net list, which has to be simulated in the test bench and evaluated against the specification. This test is followed by the procedure Place and Routing which results in a back-annotation net list (which has to be verified again in the test bench).

1.1. Verification flow

The parallel to the ASIC development (implementation flow) realized verification flow is essential. Each ASIC design step has to be verified against the specification of this step.

1.1.1. Verification of the ASIC design

The complete verification of circuits with approximately more than one Mio. gates seems to be a problem because of a linear increasing number of gates results in an exponential increase of simulation vectors. Hence, the test-duration also increases due to the number of gates. Because of this demand there are quite a lot of simulation and verification tools offshore available. But up to now even for VHDL-versions there is no 100 % test coverage carried out. Furthermore, neither the design tools nor verification tools are qualified according to the nuclear standard. That is why different verification tools from different (in-dependant) producers should be applied.

1.2. Validation against the specification

Besides the verification after each design step the validation against the specification is important. Following validation methods are practiced due to the design and safety relevance for ASICs.

- Functional testing (of the specified function).
- Functional testing under (operational respectively) environmental conditions.
- Interference immunity testing
- Fault injection testing.
- Expanded functional testing (robustness testing).
- Surge immunity testing (power supply, signal acquisition).
- Black box testing.
- Statistical testing (for failure rates).
- Worst case testing (in view of robustness).

The following figure shows the verification and validation tests needed according to the design basis:

Phase	Validation Tests								
	Functional Testing	Funct. Testing under environ. conditions	Interference Immunity Testing	Fault injection Testing	Expanded Functional Testing	Surge immunity Testing	Black Box Testing	Statistical Testing	Worst Case Testing
Specification	░ Note (1)								
Design-Description	▓ Note (2)			▓ Note (6)	▓ Note (2)			▓ Note (2)	
Implementation I	▓ Note (2)	▓ Note (4)		▓ Note (6)	░ Note (2)			▓ Note (2)	░ Note (4)
Implementation II	░ Note (2)	▓ Note (4)	░ Note (5)	▓ Note (6)					▓ Note (4)
Production				Note (7)					
Post Production	░ Note (3)	░ Note (3)	▓ Note (5)	░ Note (3)	░ Note (3)	▓ Note (5)	▓ Note (8)	░ Note (3)	░ Note (3)

□ Test in this phase is not effective

░ Test in this phase has a limited benefit

▓ Test in this phase is recommended

Fig. 2. Validation tests according to the design basis

2. Layout, design and construction of FPGA

Field programmable gate arrays (FPGA) are pre-prepared hardware cores which can be configured to the desired circuit by the applicant through a software-based configuration. FPGA architecture consists of periodical identical configurable logic blocks (CLBs) to realize logical functions. FPGA are also containing wiring resources for connecting the different CLBs. These wiring resources must be configured to realize the desired function on the FPGA. For FPGA four different architectures: symmetrical arrays, row-based arrays, hierarchical PLD (Programmable Logic Device) and sea-of-gates are known.

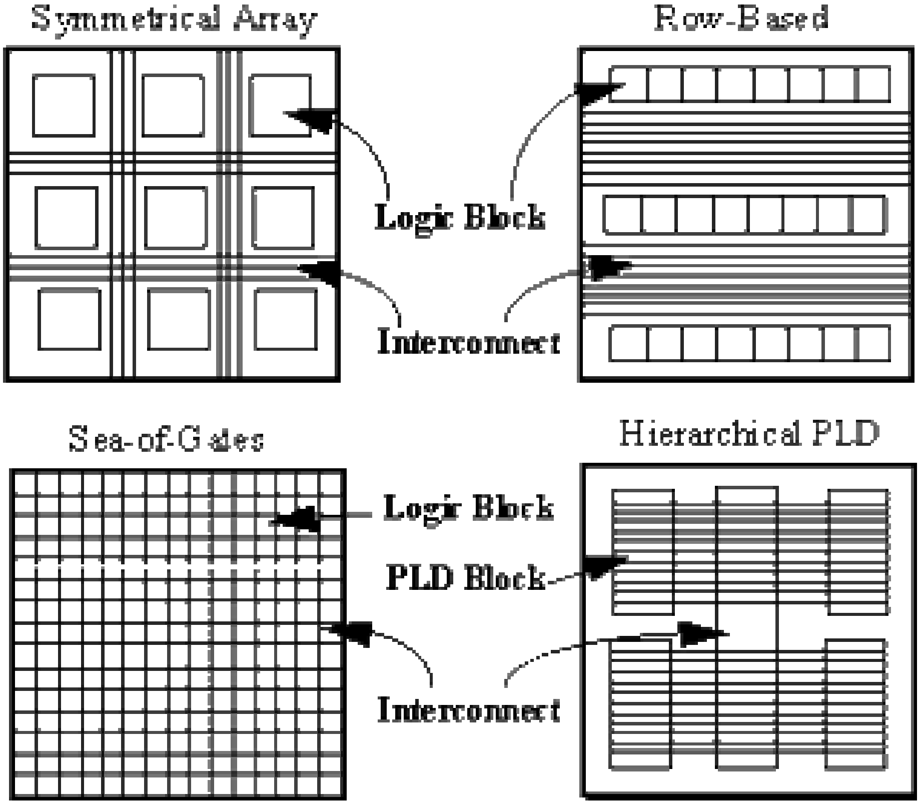


Fig. 3. Architectures of FPGAs

Therefore four different design technologies are applicable. The design of FPGA has in comparison to ASICs some special characteristics:

- The amount of configurable CLBs is limited. That is why just a limited amount of functionality can be realized.
- The functionality of CLBs is in view of different functions also limited.
- The limited amount of wire resources restricts the functionality.
- The delay time for signals in FPGA is not negligible.

2.1. Design steps of FPGA

First step: Design input

Based on the specification and the library sets of the FPGA target system by a hardware description language the circuit has to be developed and described. The result of this step is a net list.

Second step: Plan and Rout

The net list will be converted into a bit stream file which is needed for the configuration of the FPGA. Therefore, the logical blocks needed must be chosen and placed and the connections between the logical blocks must be routed.

Third step: Verification

Within this step the verification of the design will be followed by tests and simulation. For the verification a set of tools is available.

Fourth step: Programming

After successful verification the bit stream file will be routed.

2.2. Verification and Validation of FPGA

For ASICs as well as for FPGA it can be stated, that for its functionality in German NPP during normal operation no software routine is needed. Hence, the verification of a program code is also not necessary. Within the layout and design process several different software based design and verification tools for elaboration and testing of the configuration files are to be applied. Consequently these tools must be assessed within the type testing or suitability test procedure at least. It is characteristic for type testing of FPGA that the completed specification set just after configuration with the help of configuration tools via the FPGA can be operated and tested. That is why it has to be proven that the established set of configured FPGA is operated exactly due to the specification. Consequently in Germany FPGA are presently just a prototype solution from the point of view of an implementation in the reactor safety system.

3 Robustness of ASICs and FPGA

Robustness can be separated in:

- robustness against environmental conditions.
- functional robustness against input signals, which deviates from the specification as well as loads outside the specification.

3.1. Robustness against environmental conditions

- General aspects

Concerning environmental impacts, the following parameters should be taken into account.

- Climatic impacts like temperature, moisture, atmospheric pressure, (natural) radiation and light sources.
- Impacts via the power supply like over voltages (spikes) and low voltages, frequency deviation, power interrupts and crest factor.
- Mechanical impacts like vibration, earthquake, strokes, mechanical acceleration or delays.
- Accident conditions.
- Electromagnetic interference.
- Specific operational conditions like increased radiation exposure.

- Special aspects (for CMOS-technology)

The special aspects are mainly focused on the CMOS-technology as well as Micro/Nano Technology of ASICs and FPGA. The CMOS-technology as well as high package density result in a sensitivity against over voltages and electrostatic discharge. Consequently:

- The protection measures and devices against over voltages and electro magnetic impacts are to be adopted by means of strengthen.
- The realisation of ASICs in a rough technology of 1.2 µm instead of 0.25 µm technology can improve the resistance against over voltages.
- Measures to improve the power supply availability are to be evaluated because even a short loss of power supply results in the loss of functionality.
- The operation of digital circuits can demand an additional external fan-cooling facility.
- Because of the low masses of ASICS and FPGA mechanical impacts do have a lower influence than for conventional hard wired systems.

3.2. Functional Robustness

- General aspects

Functional robustness against input signals which deviate from the specification can be achieved by following measures:

- Despite of a deviation of the input signal level from the lower or upper signal specification the functionality of the system remains.
- While deviation of the input signal level out of the specification switch-over procedures will ensure the functionality.

- In case of input signal levels out of the specification prevention measures will keep the system in a safe state.

Nevertheless possible measures and device for achieving robustness are numerous and complex.

- Special aspects

The measures mentioned below are also essential in view of prevention of common cause failures.

- Requirements according to fault tolerance must be specified for the concrete application. Therefore faults and failures on the chip as well as on the chip environment must be taken into account. Self test and self diagnosis procedures are very helpful in this sense.
- ASICs and FPGA normally do have pulsed circuits. Robustness in view of timing and deviation of timings must be investigated.
- Tests in view of functional robustness should be established in accordance with the assessor. For instance the failure modes must be defined.
- Tests for faulty input signals as well as faults on the chip itself must be elaborated. The latter ones should also be recognised by development tools.
- The complex algorithms for the failure management should also be recognised on the system level (the chip level is not sufficient).
- For redundant functions ASICs and FPGA should be developed and designed by diverse tools.
- It has to be ensured, that FPGA after implementation cannot be booted by another configuration file.
- According to the requirements of IEC 61511-2 “Functional safety of instrumented systems for the process industry, part 2: Guidelines in the application of part 1” following aspects are relevant for achieving robustness:
- Diverse algorithms.
- Diverse validation of input and output data of the chip.
- Diverse failure management routines.
- Different types of data, structures and local memories.
- Diverse laboratories and subroutines.

4. Assessment of an upgrading of already existing hardwired safety relevant I&C via modern ASIC respectively FPGA in compatible applications

For the assessment national requirements, international requirements as well as the German nuclear standards must be taken into account. These requirements do not cover all safety aspects of ASICs and FPGA. That is why additional special requirements for the application of ASICs must be introduced. Therefore actually a new IEC standard concerning the selection and use of Complex Electronic Components (CEC) in the design of I&C systems performing Category A functions. Following aspects are therefore of relevance:

- It has to be assessed, that ASIC faults do not cause secondary failures.
- It has to be assessed, whether EMI during operation of the system can effect the safety function.
- It has to be assessed, whether the design recognises also test procedures.
- One main topic of the assessment should be the verification and validation of the ASIC (FPGA). Qualified development tools should be used for the layout and design.
- It has to be assessed, whether the ASIC (FPGA) is operated without any software (by means of micro controller core). If not, software specific requirements e.g. according to IEC 60880, IEC 60987, RSK Guideline must be applied.

Concerning FPGA it should be assessed that after implementation the booting of another configuration file is not possible. According to the safety relevance after the feasibility investigation, FPGA solutions should be replaced by ASIC solutions.

5. Conclusions and outlook

The replacement of conventional hard wired electronic boards (sub-assemblies) via ASICs (FPGA) seems to be possible provided the redesigned sub-assemblies on basis of ASICs (FPGA) fulfil all suitability test requirements. The confirmation of suitability in the practical application is eased, because in German NPP a redesigned ASIC (FPGA) sub-assembly has a pin-compatible and function-compatible adaptation within the already existing I&C system concept. There is a trend in the nuclear industry, that, besides the effort in qualification, the application of ASICs will be forced.

Acknowledgement

This paper is an excerpt out of an investigation performed for the German Federal Ministry for Environment, Nature and Conservation and Reactor Safety (BMU): “Compilation of safety relevant aspects in view of the implementation of application specific integrated circuits in systems important to safety”.

Literature

1. IEEE Std 610.12-1990 "Standard Glossary of Software Engineering Terminology".

2. RSK-Leitlinien (Guidelines of the German Reactor Safety Commission) für Kernkraftwerke mit Druckwasserreaktoren vom 14.04.1982, Fassung 23.08.1996.

3. IEC 61326-1. "Electrical equipment for measurement, control and laboratory use - EMC-requirements".

4. IEC 60880. Software for computers in the safety systems of Nuclear Power Stations, 2006.

5. IEC 60987 Programmed digital computers important to safety for Nuclear Power Stations December 1989.

6. IEC 61513 Nuclear Power Plants – instrumentation and control for systems important to safety – general requirements for systems. March, 2001.

Поступила в редакцию 14.02.2008

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.