S T S A R C E S

Standards for Safety Related Complex Electronic Systems

Annex 14

Innovative Technologies and Designs

ASIC development and validation in safety components

Final Report of WP5

Jean-Luc Durka & Jean-Bernard Givet

INERIS & JAY Electronique

INERIS
INSTITUT NATIONAL DE L'ENVIRONNEMENT INDUSTRIEL ET DES RISQUES

JAY électronique

European Project STSARCES

Contract SMT 4CT97-2191

Table of contents

Figures

Tables

Glossary

Acronyms	Definition
ASIC	Application specific integrated circuit
CPLD	Complex Programmable Logic Device
CPU	Central Processing Unit
EEPROM	Electrically Erasable Programmable Read Only Memory
EMC	Electro-Magnetic Compatibility
EPLD	Erasable Programmable Logic Device
FPGA	Field Programmable Gates Array
HCPLD	High Capacity Programmable Logic Device
MCM	Multi Chip Module
PED	Programmable Electronic Device
PLC	Programmable logic controller
RAM	Random Access Memory
ROM	Read Only Memory
Statecharts	Specification method based on transition systems
SW	SoftWare
WD	Watchdog

1. Summary

The main objective of this work package is to focus the manufacturers view of near-future safety related products.

It joins INERIS as test-house and JAY as manufacturer, and takes into account the foreseeable evolutions in the concepts and designs of safety related systems owing to continuing progress in the electronic technologies, to ensure that future standards do not hinder innovation and progress in safety functions.

As a matter of interest for all professionals involved in safety devices related to machine safe control, manufacturers and Test-Houses, new products are going to appear on the market, which make an increasing use of Application Specific Integrated Circuits. Such products can probably allow to achieve improved performances in terms of speed and compactness, with low costs on the market. However safety requirements must be adapted to this technology all along its life-cycle, from the design by the manufacturer onwards the validation of the product.

A typical product under development was the basis of the study : a single way safety light barrier with a dual ASIC designed for a category 4 certification. The first part deals with techniques and requirements for ASICs design and the second one is based on methods and techniques for ASICs validation.

2. Introduction

Application-Specific Integrated Circuits (ASICs)[1] are used in electronic systems dedicated to the management of safety functions. These complex circuits may incorporate several million transistors, and so cause problems for the evaluation of the functional safety of the systems that include them.

For discrete components (relays, transistors, resistors, capacitors, etc.) the analyst can evaluate the safety level by simulating virtually all the device's fault situations, using a practically exhaustive list of possible failures[1].

For complex electronic circuits such as ASICs, this exhaustive approach is not possible[3]. To evaluate the operational safety characteristics it is necessary to know the failure modes of the components used, and this is not possible for these circuits. The traditional methods of testing performance in the presence of faults are inadequate. It is therefore necessary to tackle the evaluation not only by updating subsequent tests on the finished products but also by extending the field of investigation from the origin of the faults considered: errors of specification, design or production, internal faults, or external effects.

This study describes the integrated circuits used for specific applications, the tests in general, and ways of evaluating safety.

3. New topics in research

3.1. Definitions

- ASIC : is characterised by the small size of the component, the great number of elementary functions, collective process and as the consequence of these characteristics, the impossibility to reach any elementary function if this is not an initial design condition. Also some inside parts can be tested only by an adequate simulation.
- Complex or programmable composant : a monolithic, hybrid or module circuit where the internal connections are not accessible, which satisfies one or more of the criteria below :
    - more than 1000 gates are used in the digital mode,

[1] The term "ASIC" relates more to a design method than to a product. The development of an ASIC necessitates a joint approach by user and manufacturer.

- more than 24 functionally different external electrical connections are available for use,
- the functions can be programmed.

The classic field of microprocessors is split in two structures :

* “von Neumann” the more popular and known structure usually connected with the complete set of instructions (CISC as Complete Instruction Set Computer).
* “Harvard” initial solution for computers and have today a new youth due the research of performances, usually connected with the reduced set of instructions (RISC as Reduced Instruction Set Computer).

If we take in reference the ASIC definition and the relevant component which could be orderly in this classification , microprocessors are in this class. Small size of the component, great number of elementary functions, collective process and as the consequence of these characteristics the impossibility to reach any elementary function if this is not an initial design condition, plus for the microprocessor a particular temporal behaviour as a consequence of the software flow.

3.2. von Neumann versus Harvard block structures

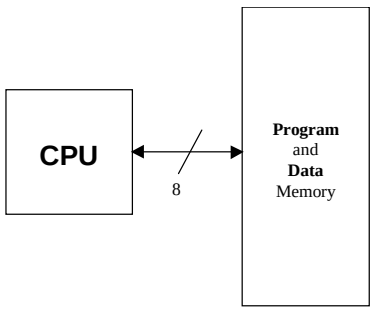


Figure 1 : Von-Neumann (CISC)

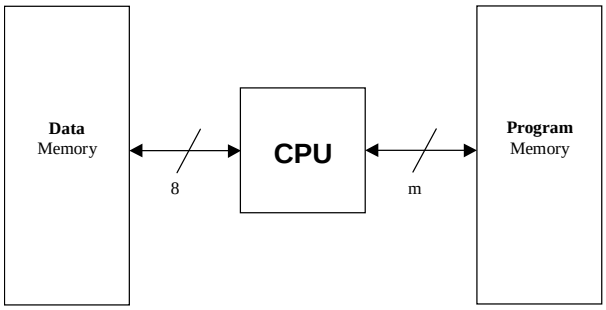


Figure 2 : Harvard (RISC)

m = as a function of memory size

As we can see these structures are different :

- In von-Neuman structure you can explore program memory and make any operation on data memory by by the mean of CPU.
- In Harvard the memory is split in two parts and the CPU can't explore or make operations on such parts.

The testing strategy described in documents such as EN 61508 annex c part 7 is clearly matched with von-Neumann structure. Any tentative to use a Harvard structure with a safety behaviour suppose that particulars means need to be use to reinforce the testing of memory field. The goal is to reach the same coverage testing in the two structures.

3.3. Components design examples

3.3.1. von Neumann

It is obvious that in such structure, if we want to do a check-sum test on the ROM memory area, we can read (R) the current value corresponding to the address CS n-1 in RAM and add by the mean of (ALU) successively the instruction code corresponding to the address n in ROM and Write (W) the new current check-sum value in RAM.

We are also able to imagine sketch calculations for the RAM.(see WP1.2 "Guide for software test").

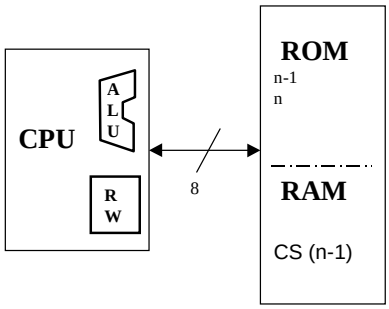


Figure 3 : Von Neumann design example

3.3.2. Harvard classic

In this Harvard classic structure if it is able to test RAM area memory things are impossible for ROM area. In fact the (ALU) execute the successive instructions pointed out by the program counter. We can't read an instruction code corresponding to a choosing address, we can only execute this instruction code by the (ALU). To reach the same testing coverage level than in von-Neumann structure we must imagine other strategy of test. As for example dedicated code for instructions corresponding to a CRC with a hard decoder .

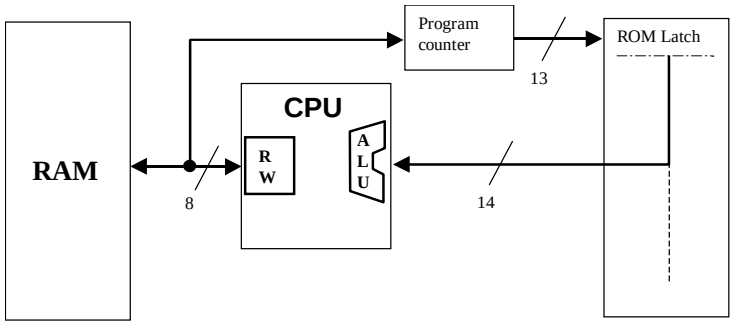


Figure 4 : Harvard classic design example

3.3.3. Harvard with ROM testing capability

In this structure derived from. Harvard classic all the testing strategies are applicable. It is obvious that the same testing method is appicable for RAM testing than in Harvard classic. But for ROM testing , by the mean of table counter we are able to point out any memory cell an execute it by the (ALU) or store it RAM in consequence we can follow this flow ,if we want to do a check-sum test

on the ROM memory area ,we can read (R) the current value corresponding to the address CS (n-1) in RAM and add by the mean of (ALU) successively the instruction code corresponding to the address n in ROM pointed out by the table counter and Write (W) the new current check-sum value in RAM.

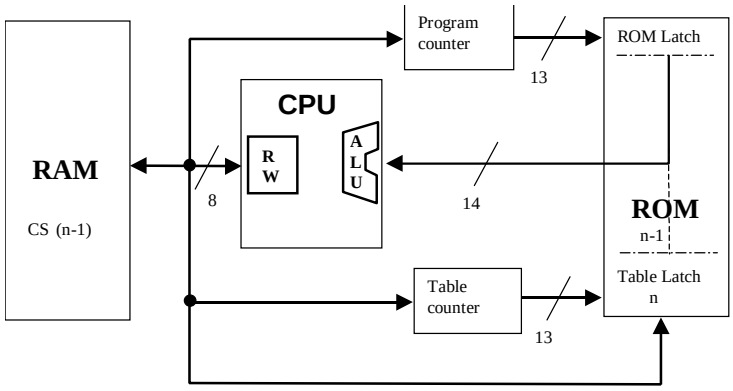


Figure 5 : Harvard with ROM testing capability design example

As describe above von-Neumann and Harvard with ROM testing capability structures are available for use under safety behaviour by using classic bibliographic described testing strategies. Harvard classic need more investigations to imagine adapted testing strategies.

CISC or RISC designation are relevant of instruction set and is not safety relevant.

3.4. Relevant components

ASICs may be divided into three main families : programmable circuits, prediffused arrays, and precharacterised arrays.

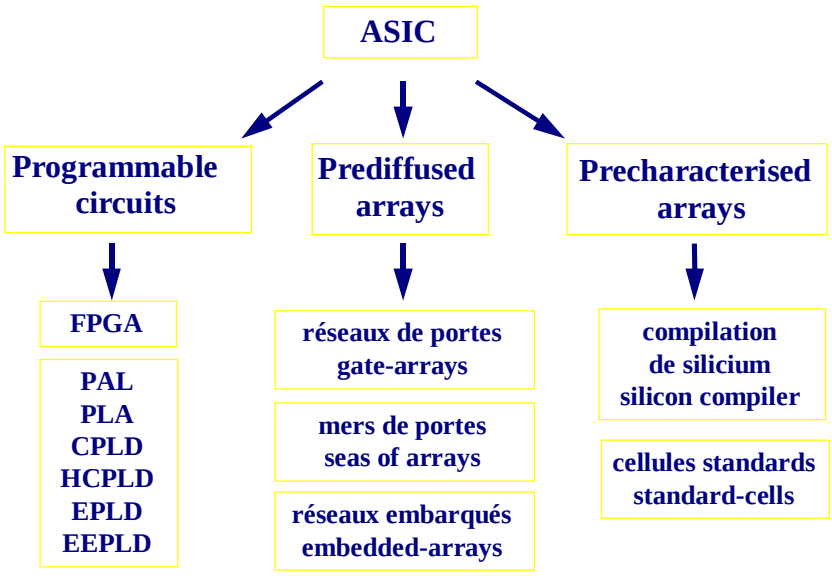


Figure 6 : The families of ASICs

3.4.1. Programmable circuits

Programmable circuits are components made up of matrices of gates, connecting tracks and complex cells such as registers, bistable devices, and so on. The user makes the interconnections between the cells according to his application purposes using a programming tool. The different arrangements of cells, the complexity available and the interconnection technologies used determine the different sub-families of programmable logic devices (PLDs) :

- Programmable Array Logic (PAL) circuits consisted solely of one programmable AND matrix and another fixed OR matrix.

- Programmable Logic Array (PLA) circuits consisted of programmable AND and OR matrices.

These circuits can very easily incorporate more complex cells, but are now obsolete.

- Complex Programmable Logic Device (CPLD) and High Capacity PLD (HCPLD) circuits are a development of PLDs containing a large number of very complex basic cells.

In all these PLD circuits, the cells are interconnected in arrays and the user removes the unwanted connection points by breaking the track. This programming is not reversible.

- The Erasable Programmable Logic Device (EPLD) is a PLD that can be programmed electrically and erased using UV light using the EPROM memory technique.

- The Electrically Erasable Programmable Logic Device (EEPLD) is a PLD that can be programmed and erased electrically using the EEPROM memory technique.

These two sub-families encompass erasable and reprogrammable PLDs, techniques that are very useful in prototyping.

- Field Programmable Gates Array (FPGA) circuits employ two interconnection techniques: the non-melt technique for which the user sets up connection points by breaking down a dielectric (an irreversible configuration) and SRAM for which the configuration of the connections, stored in a ROM memory, is automatically loaded into a solid-state RAM each time the circuit is switched on. The interconnections are made by MOS transistors turned on by commands from the RAM (reconfigurable). They include complex cells such as registers, multiplexers, etc., and represent strong competition for the pre-diffused family.

3.4.2. Prediffused arrays

A prediffused circuit is an incomplete circuit. The deep layers of the component are made beforehand by the constructor. The user designs the interconnections of his circuit in tracks provided for this purpose using a CAD method. The circuit will then be finished by the constructor who creates these connections on a final layer of aluminium. This family is subdivided into three sub-groups :

- Gate Arrays are organised into rows of basic cells and interconnection tracks that are fixed in location and size.

- Seas of Gates or “silicon seas” are circuits with a high density of transistors but no tracks. The interconnections are made on top of these transistors by a special metal layer, giving the user considerable flexibility for defining functions and connections.

- Embedded Arrays offer composite solutions that employ the best features of the various families : the complexity and optimisation of precharacterised circuits, the short development time of prediffused circuits, the high density of seas of gates, and so on.

3.4.3. Precharacterised arrays

With this family, the user has a software library of standard cells that are defined and characterised by the constructor. He chooses the cells necessary for producing the functions required and can design all the interconnection masks. This circuit is more optimised than a prediffused circuit.

The most evolved form of precharacterised circuit is the silicon compilation. This circuit is optimised as regards the parametrisable cells, RAM, ROM, multiplexers, connection of logic functions, and so on, using a description of the component in a high level language.

3.4.4. The technologies

The technology of an ASIC depends on the type of basic transistors it contains. There are six types:

- CMOS, combining high complexity and a good ratio of power consumption to speed. Moreover the protection against Latch-up and electrostatic discharges are ± 200 mA and 4 kV respectively.
- TTL which is practically no longer found in ASICs.
- Bipolar in its very fast ECL version which however is under threat from BICMOS.
- BICMOS which incorporates bipolar and MOS transistors.
- Gallium arsenide (AsGa) that can reach speeds of several GHz with better integration and immunity to noise.
- Silicon on sapphire (SOS) which has excellent resistance to radiation, latch-up and temperature (+ 250°C).

3.5. Favourable and unfavourable criteria

Generally speaking an application developed using an ASIC will be more reliable than one with standard circuits. First of all, reliability is inversely proportional to the number of connections between units and, secondly, low power also means better reliability.

However, for these complex components :

- Knowledge of faults, and any cause/fault correlation, are no more than partial.
- Reducing the physical size of the basic components creates new faults.
- The growing complexity increases the probability that design faults will appear.
- The more limited spread of ASICs compared with standard circuits means that interpreting the feedback of experience is more difficult.

From the technological point of view, the dominant type on the market – CMOS – appears in its stabilised types (1.2 to 0.8 µm) to be the most proven technique as a result of its noise margin, low consumption and good protection against electrostatic discharges and latch-up. These advantages also apply to the BICMOS in applications where higher speed is required.

On the other hand the mediocre noise margin and high consumption do not favour the ECL. The BICMOS or even the AsGa will be preferable.

In terms of safe operation, reliability, testability and consumption, the choice of a family may fall upon non-melt FPGA or EPLD for programmable circuits.

Prediffused arrays are the circuits that offer the best compromise between reliability, consumption and testability, closely followed by the precharacterised arrays.

The electrically reprogrammable circuits such as the EEPLDs are not recommended. They are insufficiently robust with regard to electromagnetic interference (information may be lost).

	Families			
Parameters	Full Custom	Precharacterised	Prediffused	Standard circuits
Testability	1	3	4	5
Reliability	5	4	4	1
Consumption	5	4	4	1

Table 1 : ASIC families scored from 1 to 5

Note: The score 1 is the lowest.

ASIC circuits of very great complexity should be avoided so as not to degrade testability.

All these recommendations can do is to avoid introducing a weak link in a safety application. Validation should be carried out at every stage of the life cycle.

3.6. Point on complexity

- Design

  For ASIC component the input document is the technical specification, software Design and simulation gives the layers. The usual schema generated is only a thinking aid but it is not the viewing of the exact chip result (integrity of compilers).

- Core based ASIC

  Generated blocks are assumed to be „correct by construction“, based on design rules. Pre-layouted or generated macros are process specific but may be ported to different technologies.

- FPGA

  Standard IC, using one-time programmable or re-programmable elements to define the connection between functional blocks and to configure the functionality of the individual blocks. It is not possible to test one-time programmable FPGA completely during production due to the nature of the programmable element.

- Microprocessors

  If for Von Neumann structure some rules are well known (as RAM and ROM testing). These rules are not applicable for Harvard structure. This component is impossible to use in safety application without other strategy of test.

3.7. Failure behaviour

Devising tests for complex integrated circuits necessitates knowledge of how these components fail. Unfortunately, such knowledge and that of the causes/failure correlation are only partial (15% of failures are not characterised on common components). Also, there are very few statistical results specific to ASICs. However their failure modes are practically the same as those of standard circuits, since the technologies and production processes are the same for the two categories.

The following table shows the main causes and failure modes whatever the technology employed.

Failure causes or mechanisms	Consequences
Design	
• Contact omitted	Open circuit (OC)
• Poor interconnections	OC, Short circuit (SC)
• Transistor wrong size	Threshold drift
• Propagation times too long	Logic fluctuations
• Poor threshold setting	Logic fluctuations
Production	
• H_2O, pH in passivation → corrosion	Short circuit
• Displaced atoms in the metal → electromigration	Open circuit
• Ion in grid oxide → contamination	Threshold drift
• Charges on grid oxide → surface charges	Threshold drift
• Poor assembly → broken connections	Open circuit, short circuit
Operation	
• ESD, voltage surge → breakdown of dielectric	Open circuit
• Parasitic ions → drift	Logic fluctuations
• Electrical overload → melting	Open circuit, short circuit
• Spurious electromagnetic signals	Logic fluctuations

Table 2 : Failure causes and modes in integrated circuits

It is interesting to note that the causes of failures show up in a limited number of failure modes :

- short circuits and open circuits at various levels of components (pins, gates, transistors),
- drifts in threshold voltage and logic fluctuations (steady or intermittent reversal of levels).

During production the main failure mechanism is corrosion which shows up mainly as short circuits. In operation, melting caused by electrical overloads leads to short circuits and open circuits at various component levels.

To avoid any unsafe behaviour the following rationale could be used, after choosing the relevant category :

- For external signals we can use the catalogue of single faults which is the annex B of EN 61496-1 [1].
- For internal signals the followings topics need to be analysed :

  [1] Rules of design, including fault simulation, see IEC 61508 [5] and DIN V VDE 801 A2 [6], where some failures are described :

  - signal stucked,
  - loss of a function,
  - loss of time synchronism,
  - components drift,
  - signal unwanted oscillations,
  - intermittent failures.

  [2] Tools of design-compilers integrity, certified versions. Low or high level langage ?

  [3] Suggested safety strutures (e.g. 1998 project report §3.2).

  - Rules of fault detection as already depicted for software (EN 61508, annex C part 7).

  [4] Process stable and known technologie.

  - If there is a change in the process some test or analysis need to be replay as in the design phase.

4. Testing ASICs

4.1. In service tests

The life cycle of an ASIC is shown below : testing is applied at different stages.

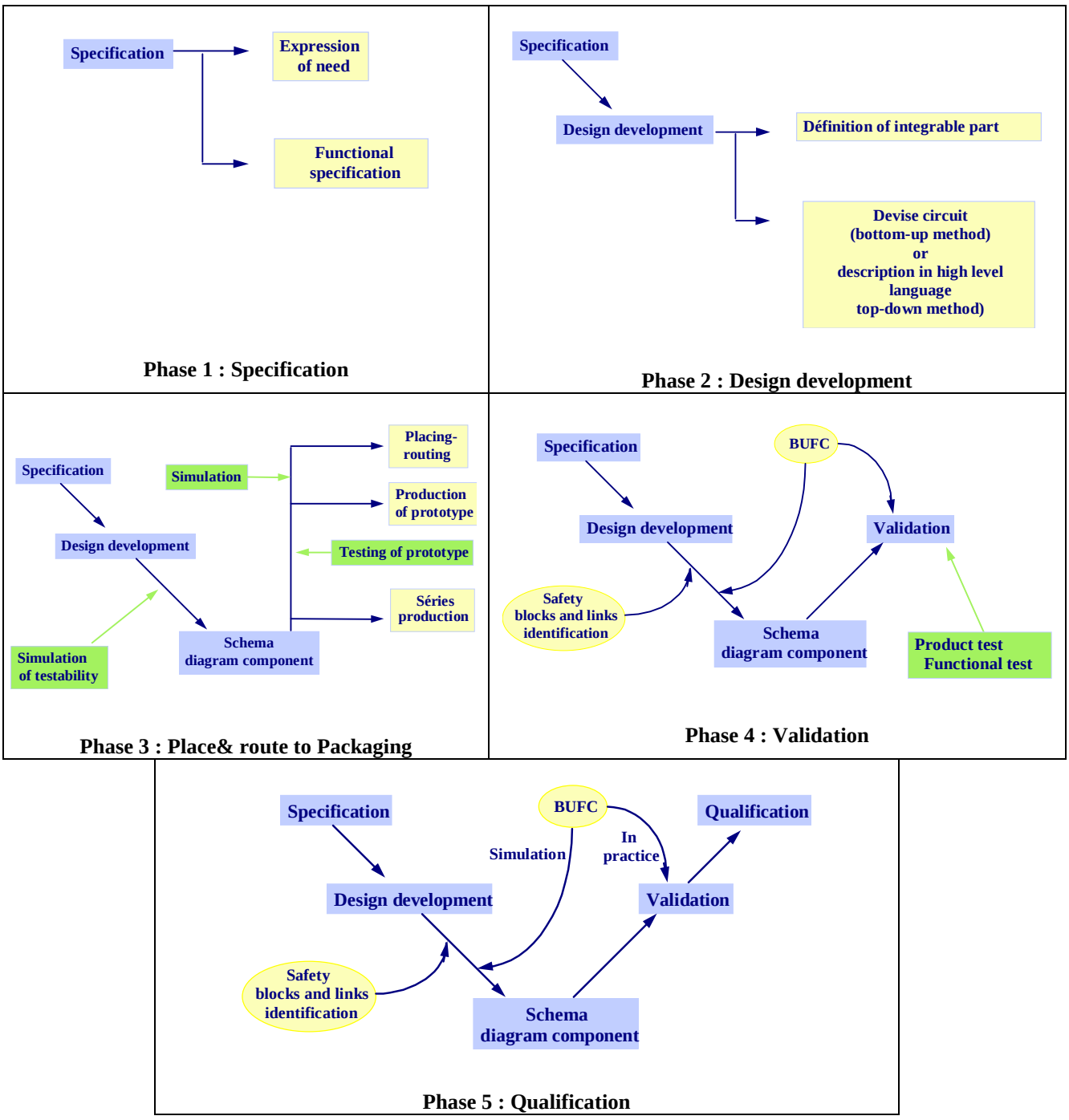


Figure 7 : Life cycle of an ASIC

Note : Behaviour Under Fault Condition (BUFC)

Throughout the life cycle of an ASIC, prototype tests, and checks on time and frequency characteristics, electrical levels, etc. are carried out, together with tests to detect physical anomalies. These tests are more a matter for the silicone producer than the user. However two types of test are of concern to the user or the expert whose task is to analyse a device incorporating an ASIC :

- The functional test. In this type of logic test, a test sequence is applied to the component inputs, which may be in the form of a simulation on the model at the design stage or directly on the circuit on completion of production. Procedures are used to detect the presence of an internal fault at the outputs. At the design stage, this test allows the fault to be corrected after identification. During production, it leads to acceptance of satisfactory circuits or rejection of those that are unsatisfactory.

- The performance test in the presence of internal faults. In this test of integrity, which can be used at the design stage (on a model) or in operation (either on a model or physically), a fault model is simulated or injected into the component or its representation, and the behaviour of its outputs observed. This test is fundamental for safety applications and analyses the ability of the architecture to detect faults.

4.2. Descriptive levels and domains of an ASIC

Tests conducted at different stages in the life cycle of an ASIC will be carried out in different domains that are more or less abstract (models) or concrete (the circuit itself). In addition, different levels of exploration fineness are defined and used according to the need for the test to be representative. These domains and levels are shown on Gajski's Y graph.

The physical domain is the most concrete, and describes the real elements of the chip at different levels of fineness. The structural domain is an abstract domain in schematic form (block or detailed circuit diagrams). The behavioural domain describes the function of the circuit from the most general level (algorithm) to the finest level (transistor).

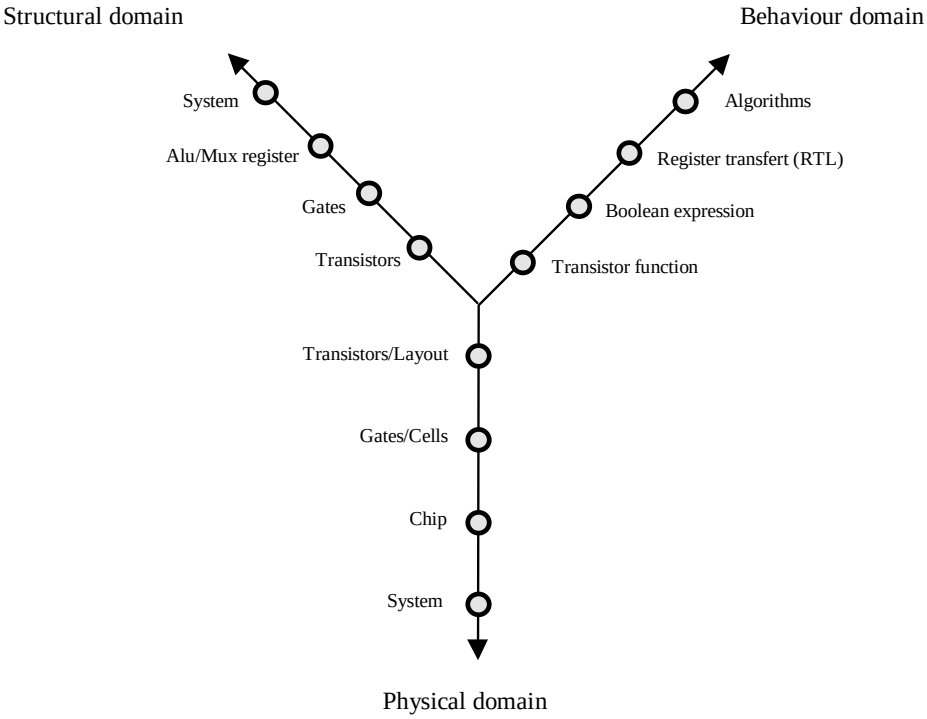


Figure 8 : Descriptive domains and levels for an ASIC

4.3. Fault hypotheses

Owing to the complexity of modern integrated circuits, any exhaustive check on their performance covering all possible faults that could affect them is becoming impossible. Accordingly the philosophy of testing has evolved by comparison with that applying to discrete components, starting from the assumption that a reduced and known set of consequences of faults is sufficiently representative of the physical causes, multiple and unknown faults of these failures.

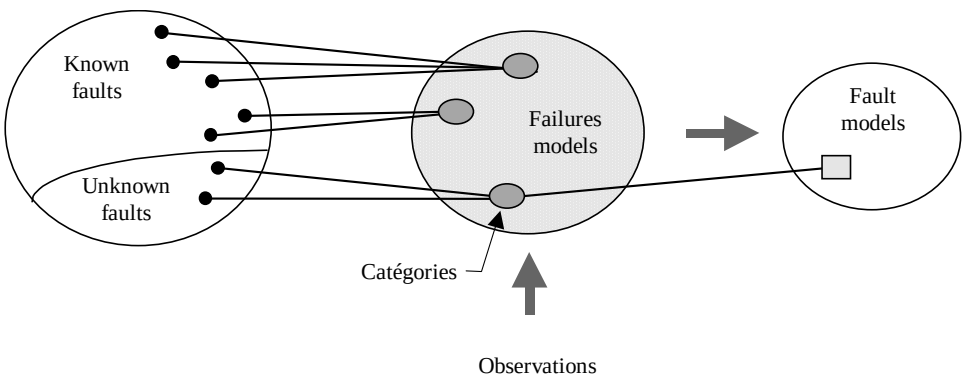


Figure 9 : First fault hypothesis

These failure models are described by a number of fault models according to logic and technological criteria. Reasonable confidence in the test will be obtained by checking that these faults are absent in production, or that they have no effect on normal performance in operation.

A different problem arises when one considers simultaneous faults. The designers of integrated circuits regard these as highly unlikely. As a result, the production tests are based on the second hypothesis according to which the fault is unique.

Finally, a third assumption is that the failure is permanent.

4.4. Fault models

The modes of failure of digital integrated circuits can be placed into four categories : short circuits, open circuits, permanent or intermittent logic fluctuations and the drift of thresholds.

The model of equipotentials stuck at logic levels 0 and 1 is the one most used. It represents about a third of the physical faults identified. Also when this model is applied at “gate” level in the structural domain it is independent of the technology, and the observability of the line affected allows other anomalies to be detected. However this method, although practically exhaustive for bipolar and MOS technologies, is inadequate for CMOS. For this technology, short circuits and open circuits do not necessarily lead to sticking. The outputs may show either analogue behaviour due to threshold drifts, or sequential behaviour. Output short circuits no longer automatically lead to hardwired ANDs or ORs, although “doubtful” output voltages may appear. Finally, threshold drifts and external spurious signals can lead to more or less temporary logic fluctuations.

These phenomena make modelling at transistor level essential, and the following models are used :

- Transistor stuck open. This model represents physical faults such as the absence of source-drain contact, or a broken line. These faults mean that the node concerned remains in the previous state instead of changing over ; this is sequential behaviour.

- Transistor stuck on. In this case, the transistor concerned still conducts regardless of the grid signal. This may be due to a drain-source short circuit or to the threshold voltage being wrongly set. The circuit behaves in an analogue manner. The output voltage can take any value, outside the guaranteed ranges of logic levels, and depends on the value of the external bias resistors used. If this output voltage is very different from that expected, the failure shows up as a logic error (reversal of state).

- Bridging. These models of short circuits at different levels represent spurious links between interconnections due to metal expansion, diffusion errors or breakdowns of insulation between levels. Different types of bridging can be envisaged :

  - between two gate outputs,
  - between two internal nodes,
  - between grid, drain or source of a transistor,
  - between two neighbouring metal levels.

  These bridging models represent analogue behaviour and logic errors.

- Open circuits. The model of a track gap represents either a transistor omitted in the design, or a physical break in the line. Most of the time these faults show up as complex analogue behaviour.

All the fault models presented above lead to short circuits and open circuits at different component levels.

For a circuit subject to an integral line test that is intended to provide a safety function, the following fault models are applicable :

* A short circuit between one diffusion and the next closest diffusion A short circuit between one diffusion and the next closest diffusionv ;
* A broken equipotential: poly-Si and floating grid.

For the thorough production test on a safety component, any short circuits must be at a minimum.

None of these models take into account faults due to spurious electromagnetic signals or radiation. Spurious electromagnetic signals in operation or the erroneous setting of a threshold at the design stage may lead, at the inputs and outputs of a circuit, to intermittent or continuous changes in logic state. These phenomena cannot be absolutely checked by screening and other electromagnetic compatibility precautions, and the design tests may not perceive these threshold faults. We therefore believe it appropriate to consider these problems.

In order to simulate these failures, mainly those resulting from spurious electromagnetic signals, we believe it is useful to propose a model for the change of state of one or more bits at the inputs and outputs. This change of state may be transient, periodic or permanent.

Finally, the different possible short circuits together with internal cross-talk can modify the output signals from an entire system or the outputs from different functional units. We shall see subsequently that the test on the finished product finds it difficult to “penetrate” the interior of a complex component. It therefore seems to us to be important at this stage to consider models of change at functional level : the “black box” system approach or that involving functional modules.

4.5. The functional test at the design stage and on completion of production

The off-line functional test involves applying a relevant test sequence to the inputs of the circuit under test in order to reveal the presence of internal faults at the outputs. Depending on the complexity of the circuit concerned, three approaches to the functional test can be considered :

* The external test.
* The external test on an improved circuit.
* The integral test.

4.5.1. The external test

In this type of test, the tester, comprising the test sequence generator and the functions necessary for observing the outputs, is outside the circuit to be tested.

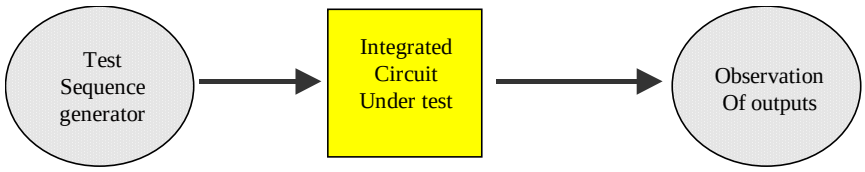


Figure 10 : The external test

The test sequences are generated in a deterministic manner by automatic test program generators. The method most frequently used is “path sensitisation” or the D-algorithm, based upon the sticking model at gate level, and involves finding the input logic sequence or sequences capable of propagating a line sticking fault along an internal path to show up at an observable output.

Another method is the “exhaustive” test, in which the circuit to be tested is regarded as a black box for which only the logic function is known. This involves injecting all the possible combinations of inputs, which total 2^n for a circuit with n inputs. This coarser technique is easy to use but much more involved than the D-algorithm method.

This method is very suitable for simple combinational circuits. However, for practical applications, increasing use is being made of circuits that are both sequential and combinational. For these circuits, the previous methods lead to increasingly complex testers, that are costly and involve prohibitive test times. Also modern circuits can no longer be tested by these methods at nominal speed. It therefore seems necessary to make circuits easier to test.

4.5.2. The external tests on circuits with improved testability

Improving the testability involves modifying the circuit to be tested by incorporating additional functions in it to make the test possible. To do this, action must be taken on the two components of testability : the commandability which represents the ease with which the input sequences can activate the different parts of the circuit, and the observability which determines the ability of the circuit to propagate faults to the output.

There are two approaches to improving testability: ad hoc methods and structured methods.

- Ad hoc methods. These techniques are specific to each application. Two main variants are used :

    * Addition of test points. Unit C is functionally inaccessible from the outside. This unit is rendered commandable by creating the special input E_s and its observability by an output S_s.

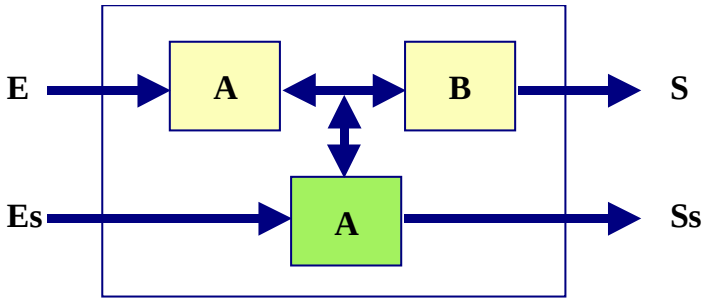
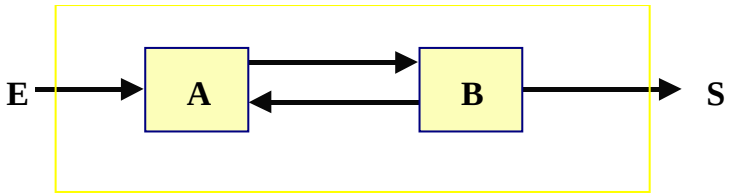


Figure 11 : Adding test points

* Partitioning. This involves partitioning the circuit in which functional or structural units A and B are separated by multiplexers whereby they can be commanded and observed. This technique is relatively easy to do but necessitates about 30% of additional silicon and raises the problem of the integrity of the multiplexers.



Original circuit

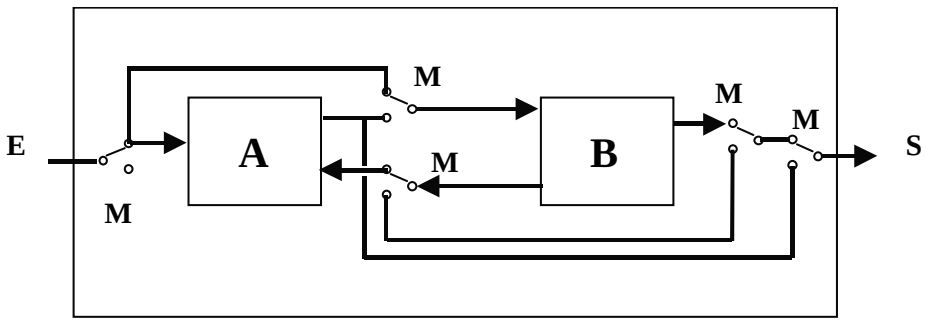


Figure 12 : Testability by partitioning with multiplexers

- Structured methods. These methods can be adapted to any circuit and are particularly suitable for complex combinational and sequential components.

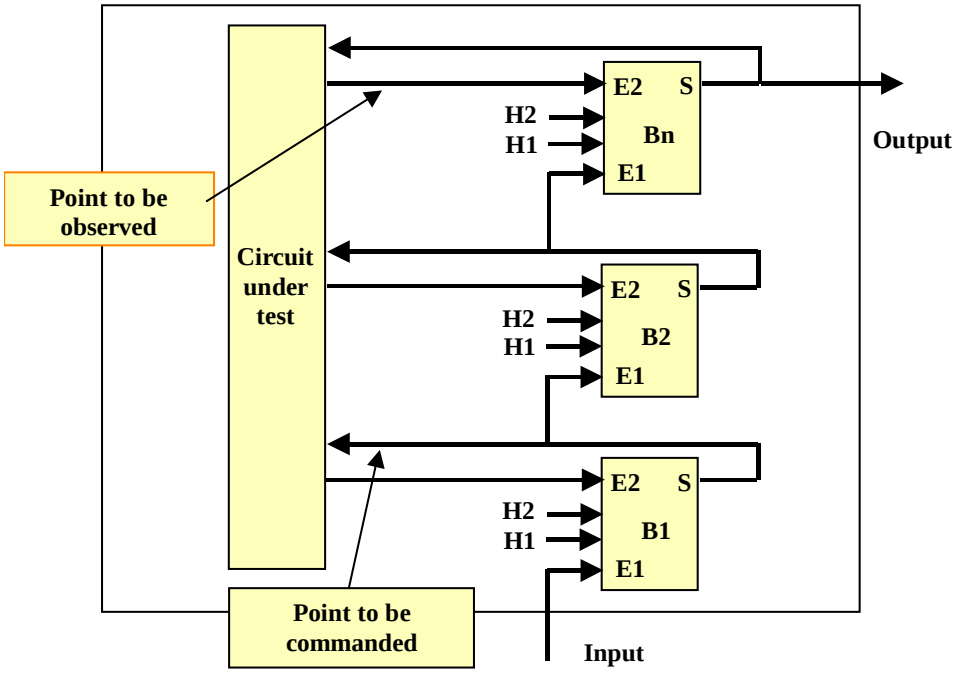


Figure 13 : Structured test method based upon a serial access register

The overall principle is to access all the memory points in the circuit using bistable devices B_1, B_2, … B_n. These bistable devices together form an offset register with serial access. The inputs (commands) are loaded using a clock H_1, and the outputs (observation) by a clock H_2.

Many component manufacturers have developed a number of variants of this structured technique : SCAN PATH of NEC, Level Sensitive Scan Design (LSSD) of IBM, Scan Set Logic of Univac, Random Access Scan of Fujitsu, and so on.

The main attraction of structured test methods is to reduce the test on a sequential circuit to one on a single combinational circuit. The natural registers in the circuit are used as bistable devices in order to constitute the offset register. However the offset logic can use up to 20% of additional silicon and the passage of the data through serial links makes the test relatively long.

4.5.3. The integral test

The integral test, also known as the built-in self-test, involves incorporating in the silicon not only the test facilities but also the tester, encompassing the generation of test sequences and the functions for observing the results. The latter are nearly always based on data compression methods.

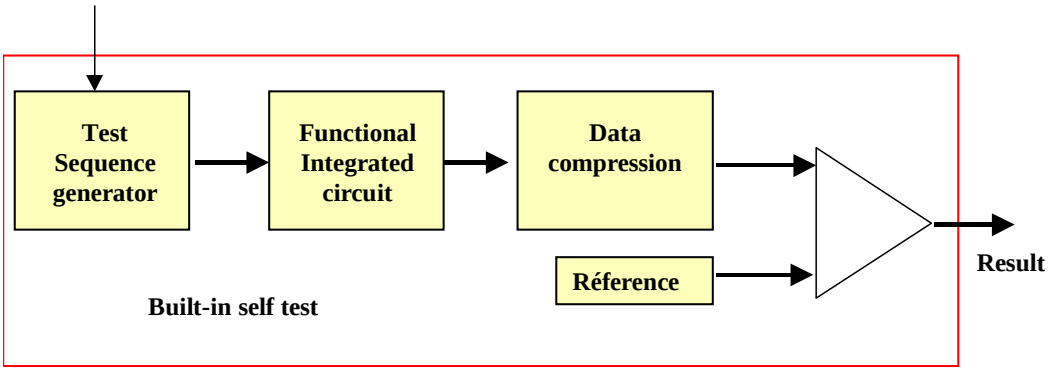


Figure 14 : Built-in self test (BIST

The advantages of this technique are as follows:

- The slowing-down of the test caused by the serial link between tester and circuit is eliminated ;
- Because the tester uses the same technology as the circuit to be tested, the test takes place at nominal speed ;
- It is possible to envisage the exhaustive “black box” test of combinational units ;
- The integral test, subject to certain adaptations, can also be used as an in-line test when the circuit is on a card, whereupon the circuit becomes self-checking in operation.

The decision to install a BIST is subject to the following constraints:

* Additional silicon necessary ;
* Maximum test duration acceptable ;
* Speed of tester ;
* Ease of application ;
* Test quality obtained ;
* Tester cannot be modified once integrated in the silicon.

Various methods can be envisaged for generating the test sequence:

- Data stored in ROM. The test sequences stored in a ROM are applied to the logic units to be tested by internal buses or serial offset register paths (for example SCAN PATH). Sequences are generated in a deterministic and automatic manner. This method is expensive in computer time and in the area of silicon dedicated to the test (storage ROM). It is very suitable for circuits that already have an internal ROM. The test shows good quality but the speed is limited by that of the ROM.

- Exhaustive generation for each unit. This is a simple method that does not require a fine analysis of the circuit. Each internal unit receives an exhaustive set of sequences (2^n possibilities for a unit with n inputs). The generator can be a simple general counter for all the units or there can be one for each unit. The test obtained is of good quality depending on the selected cut-off level, but does require fairly substantial additional silicon.

- Pseudo-random generation. This is the method most used, which involves injecting a pseudo-random test sequence of sufficient length for the test to be relevant into the inputs of the circuit under test. The length of this sequence can be estimated in two different ways :

    * One method is to simulate faults by a random sequence applied to the inputs of the circuits to be tested. The sequence is halted when it is considered that test coverage is adequate. This method requires very long computer time.

    * A second method is based on the concept of the fault that is most difficult to detect. This technique requires fine analysis of the circuit.

  The best known method of pseudo-random generation seems to be the “Built-In Block Observer” (BIBLO) which employs the techniques of both the offset register and signature analysis.

4.5.4. The built-in self test

The BIST test methods described above involved testing the circuit off-line. It is also possible to envisage integrating self-tests on the silicon that can be used in service (on-line test). Various detection mechanisms have been developed. Some are based on LFSR such as cyclic codes and signature analysis, and others could be envisaged : watchdog, detector codes, similarity tests, and so on.

The on-line BIST approach is fairly expensive in silicon and calls for a far-reaching study of the circuit. It is reserved for circuits directly controlling safety functions or applications with a very high level of availability.

4.6. Behavioural tests in the presence of faults

On classics circuits, tests for the effects of single faults shall be carried out on all the relevant components. If further faults occur as a result of the first single fault, the first and all consequent faults shall be considered as a single fault. In order to reduce unnecessary testing where the results of a combination of faults can be precisely defined theoretically, an analysis statement shall be included as part of the test results statement.

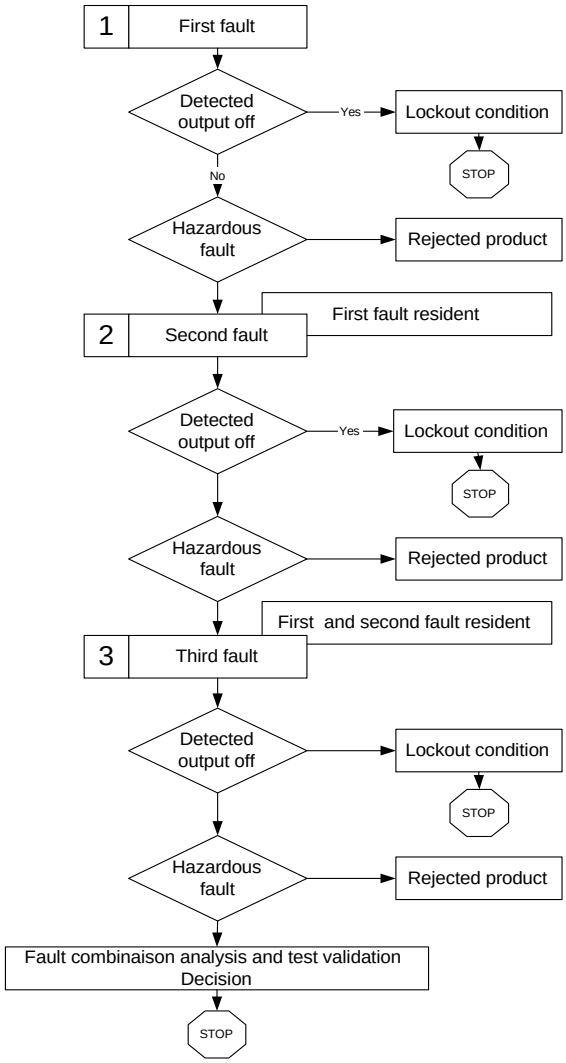


Figure 15 : Faults sequence according category 4 of EN 954

Testing for the accumulation of more than three faults need to be carried out provided that the probability of more than three faults, (largely independent of each other and having to appear in a specific sequence in time), is low.

As far as ASICs are concerned, it is a matter of observing some or all of the output performances when they are affected by an internal fault. This test can indicate the influence of the fault on the circuit functions in terms of functional safety.

There are two possible ways of conducting this test: using software to simulate faults, or physically injecting faults. The growing complexity of ASICs is increasingly imposing the approach involving software simulation of faults on models of the circuit. With this method it is possible to reach fine levels of the component. It involves abstract representations of the circuit which in fact reflect its reality only imperfectly.

The physical injection of faults is the only method that generates anomalies in the real circuit, but the test cannot “penetrate” beyond the connecting pins. It is therefore less detailed than the test by simulation.

4.6.1. Software simulation of faults

The software simulation of faults employs CAD tools, models of the circuit and the fault models used at the design stage. Before simulating faults, it is as well to ensure that the circuit is operating satisfactorily. For this purpose the design tests will be repeated so as to verify the functional characteristics as regards timing, frequency, voltage, current, and so on. The next phase is to simulate faults at different points in the component in order to observe the behaviour at the outputs.

As at the design stage, the models of faults are : sticking equipotentials, open circuits, short circuits at various levels, continuous or intermittent logic fluctuations, perturbations of functions and transistors stuck open or closed.

The test methodology is of the top-down type, with faults initially simulated at system level with the component being generally regarded as a black box. The same tests are then applied to structural or functional units.

4.6.2. Physical injection of faults

The physical injection of faults involves two approaches :

- Creating faults internal to the circuit ;
- The external injection of faults at the component connector.

4.6.2.1. Internal injection of faults

Internal faults can be injected by applying electrical interference to the component supply leads. With this technique, the fault is propagated in a random manner and the results are not reproducible.

4.6.2.2. Injection of faults at the connector

The models of faults generally used are :

* Sticking at 0 and 1 ;
* Sticking at an intermediate value which can resemble the simulation of analogue behaviour in CMOS technology outputs ;
* Line gaps modelling anomalies in this technology ;
* Level inversions and physical bridging which simulate phenomena caused by various types of electrical interference ;
* Changed function at inputs and outputs.

The faults can be applied using the forcing technique. With the component still wired to its card, the fault injected at a pin is propagated over all the lines connected to it.

4.6.3. Improving testability

In complex circuits, the behaviour test in the presence of faults encounters the same problems as the production test. Access to the functional pins alone considerably limits the extent of the test. It therefore seems essential to incorporate Built-In Fault Injection Logic into the silicon. This method involves incorporating, on the signal processing chip, an offset register followed by a decoder which can select the critical nodes in each of the functional units of the processor to be tested.

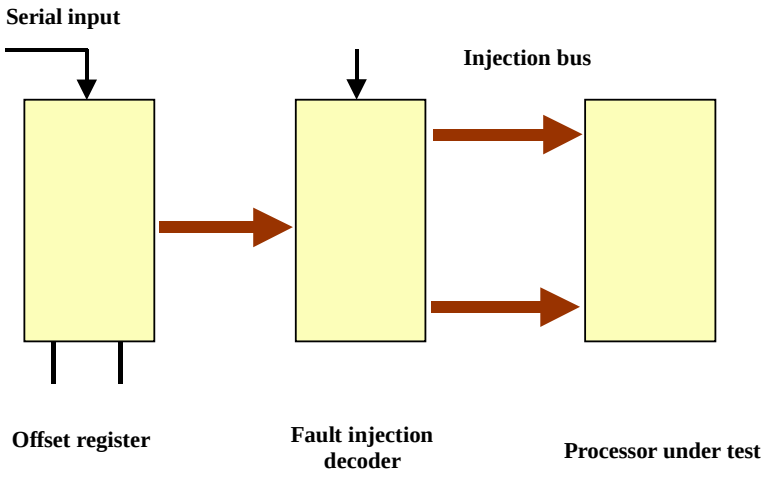


Figure 16 : Built-in fault injector

This ad hoc method seems an attractive approach for memories and processor systems. Its advantages are, first, that it enhances the extent of the test and, secondly, it requires less external test equipment. On the other hand, the preliminary selection of relevant test points is a slow process.

For ASICs of average complexity, adding additional test points would permit greater depth of analysis using the forcing technique.

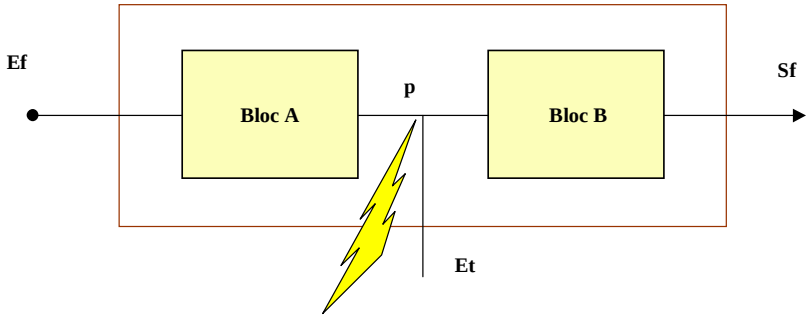


Figure 17 : Additional forcing point

The input E_1 allows the point p to be forced to 1 or 0 or to an intermediate voltage, either continuously or temporarily. This method is very simple and cheap in terms of silicon ; it is very attractive on condition that the relevant test points are well defined and that precautions to limit current are taken on the tester so as not to destroy the circuit being tested.

A variant of this method is to make the inputs and outputs of the functional units accessible from the outside.

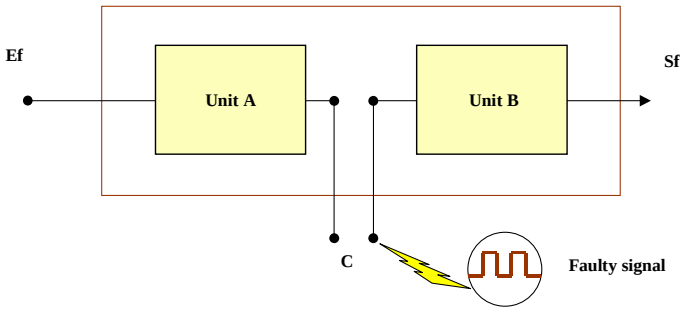


Figure 18 Inserting a faulty signal at an input

4.7. Method for Safety Validation – black-box test

This black-box method is divided in five phases :

- Functional Testing to reveal failures during the specification and design phases ;
- Functional testing under environmental conditions to validate the safety-related system against typical environmental influences ;
- Fault insertion testing to introduce or simulate faults in the system hardware and document the response ;
- Worst case testing to validate the system and the component under highest environmental conditions values.
- Expanded functional testing to check the behaviour of the safety-related system in the event of rare or unspecified inputs

5. Conclusion

The increasingly common use of digital ASICs in electronic systems managing safety functions, such as virtual barriers and two-hand commands, is part of the normal progress of these electronic components.

Indeed the inherent advantages of these circuits – smaller size, lower power consumption, greater speed and reliability, and so on, make them attractive components and they are increasingly replacing standard electronic circuits.

As regards operating safety, the compactness and low consumption of ASICs ensure a more reliable solution than the same design using standard circuits. On the other hand, growing complexity means that less is known about the failure modes of these components. Some 15% of the faults that may affect these circuits are at present unknown.

A critical analysis of the available families and technologies has begun by identifying a few criteria of choice as regards ASICs for safety applications. It is essential to avoid too much complexity as well as the electrically erasable programmable arrays (SARM and EEPLD) which are too sensitive to spurious signals.

Testing should take place throughout the life cycle of an ASIC and take place as follows :

- A functional specification should be drawn up, including a description of the integrable part, the family, chosen technology, characteristics, risk analysis, architectural approaches, testability, and test programs.

- At the design stage, whatever the method used, a high level language scheme should be drawn up. This phase should include a simulation stage for detecting design faults and observing the behaviour of the circuit outputs in the presence of faults.

- During production, it is essential to provide the constructor with the circuit test programs. These tests will be used to determine whether the circuit should be accepted or rejected. The test sequences are prepared using automatic test generation programs. Solutions for improving, first, the testability should be integrated in the silicon (additional test points, partitioning, Scan path, LSSD, BIST, self-checking circuit, depending on complexity) and, secondly, the architecture of self-tests and self-tests outside the ASIC, and even global redundancy.

In this structure one ASIC (1) make the control of the application the other (2) use monitoring informations provided by the application and with a correct phase regarding control orders. Each ASIC use its proper clocks. A link between the to ASICs ensure that the state of the work relevant of each is at the same level or follow a predicted sequence.

The two ASICs can use the same input/output ressource, or two separate relevant of an other level of redundancy.

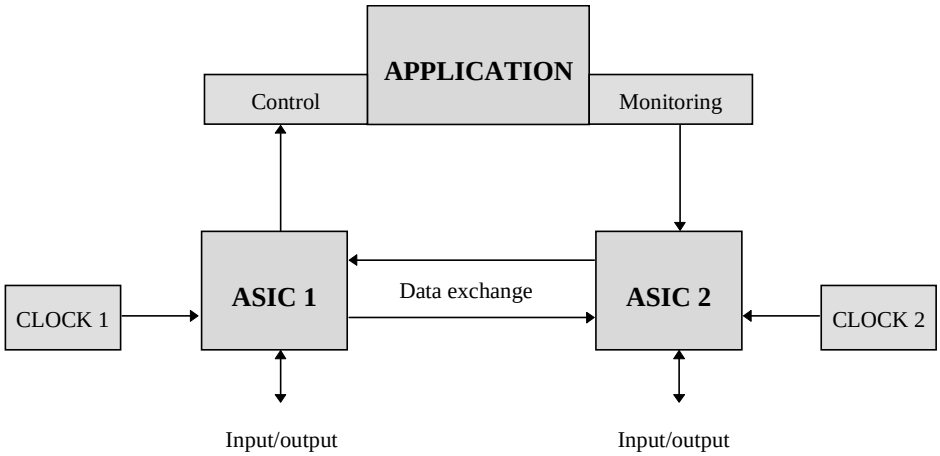


Figure 19 : Redundant structure

All these detection mechanisms should be validated by means of physical fault injection methods using models applicable at connector level : sticking, short circuits and open circuits.

Analysis of operating safety can be broken down into five main phases :

- Verification of the technological and architectural choices, characteristics and safety functions.
- Risk analysis leading to a classification of the level of integral safety.
- Analysis of circuits : safety solutions adopted, study of fault behaviour.
- Simulation of behaviour in the presence of faults on the implanted models using a CAD development tool.
- Validation of the architectural approaches using black box methods :
    - Functional tests ;

* Environmental tests ;
* Physical injection of faults ;
* Environmental tests at the limits ;
* Extension of functional tests to rare situations.

6. Bibliography

[1] IEC 61496-1 : Safety of machinery - Electrosensitive protective equipment - Part 1 : General requirements and tests.

[2] Les circuits intégrés spécifiques (ASIC) dans les applications de sécurité. Analyse et évaluation. C. Vigneron. Les notes scientifiques et techniques de l'INRS, Ed NS0133.

[3] Modes de défaillances des circuits intégrés. Document ISDF du groupe de travail « Mode de Défaillances des Circuits Intégrés », 26 avril 1994.

[4] EN 954-1 - Sécurité des machines : Parties des systèmes de commandes relatives à la sécurité - Partie 1 : Principes généraux de conception.

[5] CEI 61508 : Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité. Ed. 99. Parties 1 à 7.

[6] DIN V VDE 0801 Amendment A2 : Principles for computers in safety-related systems.