Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 6 October 2015

Case Number: T 0605/10 - 3.5.01

Application Number: 03015860.4

Publication Number: 1496435

IPC: G06F11/267

Language of the proceedings: EN

Title of invention:
Dependable microcontroller, method for designing a dependable microcontroller and computer program product therefor

Applicant:
Yogitech Spa

Headword:
LFSR PSA/YOGITECH

Relevant legal provisions:
EPC Art. 52(1), 56

Keyword:
Inventive step - (no)

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 0605/10 - 3.5.01

D E C I S I O N
of Technical Board of Appeal 3.5.01
of 6 October 2015

Appellant: (Applicant)	Yogitech Spa Via S. Antonio, 3 55049 Viareggio (Lucca) (IT)
Representative:	Marchitelli, Mauro Buzzi, Notaro & Antonielli d'Oulx Via Maria Vittoria 18 10123 Torino (IT)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 6 October 2009 refusing European patent application No. 03015860.4 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Chandler
Members:	R.R.K. Zimmermann
	S. Fernández de Córdoba

Summary of Facts and Submissions

I. European patent application EP 1 496 435 A1, application number 03015860.4, relates to a fault-robust on-chip validation system for microcontrollers.

II. The examining division refused the application for insufficient disclosure of the invention on the basis of the application as last amended by a letter of 4 August 2009. The written decision also mentions lack of inventive step, an objection raised earlier in a communication on the basis of documents US 6 421 790 B1, cited as document D2, and EP 0 251 809 A2, cited as document D5.

III. The appellant (applicant) lodged an appeal in due form and time against the decision and requested the reversal of the decision and subsidiarily oral proceedings. It was alleged that the examining division had not addressed the applicant's arguments properly, and that the decision was not sufficiently reasoned with respect to the objection of insufficient disclosure and the arguments submitted by the appellant in response.

IV. In a non-binding provisional opinion the Board disagreed with the examining division's finding of insufficient disclosure but explained that the appeal was nevertheless not allowable since the subject-matter of claim 1, in all requests before the Board, was obvious in the light of documents D2 and D5. The Board also indicated that it did not identify any violation of the first-instance procedure.

V. Following a reply dated 21 November 2014 and including an additional auxiliary request, oral proceedings were held before the Board on 6 October 2015.

VI. At the oral proceedings, the appellant requested that the decision under appeal be set aside and a patent be granted on the basis of a main request or, in the alternative, of four auxiliary requests, all requests as filed with the letter of 4 August 2009 and containing the feature ", which is a RISC central processing unit," at the beginning of the claim after the feature "a microcontroller comprising a central processing unit (50, 51)". The appellant withdrew the fifth auxiliary request filed with the letter of 21 November 2014 and the objection of lack of reasoning of the decision of the examining division.

VII. Claim 1 of this final main request has the following wording (the structuring of the claim in sections [(a) …], [(aa)…] etc. has been added for convenience of reference):

"1. [(a) A microcontroller comprising a central processing unit (50, 51), [(aa) which is a RISC central processing unit,] a system bus (53) and one or more functional parts (61, 62) comprising interfaces and peripherals (62), and a further fault processing unit (11) to perform validation [(ab) of said central processing unit (50, 51)] wherein said further fault processing unit (11) is external with respect to said central processing unit (51),] characterized in that:
-[(b) said further fault processing unit (11) is different with respect to said central processing unit (51) and comprises at least one module (22, 23, 24) for performing validation of operations of said central processing unit (51) to achieve dependability of

microcontroller operations], [(c) wherein said at least one module includes a shadow register module to make a copy of the register bank of the central processing unit (51)] and [(d) wherein said further fault processing unit (11) includes a reduced version of the ALU/MAC of said central processing unit (51) working with a coded copy of the shadowed registers with a lesser number of bits by implementing ALU/MAC operations on said coded copy having a lesser number of bits to concurrently check the results of the ALU/MAC of said central processing unit (51)],
- [(e) said further fault processing unit (11) comprises one or more modules for performing validation of operations of said other functional parts (61, 62) of said microcontroller (10)]."

According to the auxiliary requests, the following features are inserted at the end of the above-quoted claim respectively as follows:

1st auxiliary request: ", said further fault processing unit (11) including an ALU/MAC supervisor module to make a reduced copy of the integer core of said central processing unit (51)."

2nd auxiliary request: ", said further fault processing unit (11) including an ALU/MAC supervisor module to make a reduced copy of the integer core of said central processing unit (51), wherein said ALU/MAC supervisor module has access to said shadow register module and checks results detected on the ALU write port of said integer core."

3rd auxiliary request: ", said further fault processing unit (11) includes a core interface module and said shadow register module updates said copy of the register bank of the central processing unit (51) based on

memory-to-register data transfers and based on the access to the write port of the Arithmetic Logic Unit of the central processing unit (51) available from said core interface module, said shadow register module to compare register-to-memory transfers with the contents of said copy to detect mismatches."

4th auxiliary request: ", said further fault processing unit (11) including an ALU/MAC supervisor module to make a reduced copy of the integer core of said central processing unit (51), wherein said ALU/MAC supervisor module has access to said shadow register module and checks results detected on the ALU write port of said integer core, said further fault processing unit (11) including a core interface module and said shadow register module updating said copy of the register bank of the central processing unit (51) based on memory-to-register data transfers and based on the access to the write port of the Arithmetic Logic Unit of the central processing unit (51) available from said core interface module, said shadow register module to compare register-to-memory transfers with the contents of said copy to detect mismatches."

VIII. The appellant argued that the invention provided an inventive microcontroller that achieved full dependability, real-time fault control, and a fully and flexibly customisable system-on-chip design with a significantly reduced chip area overhead for the fault processing unit.

Specifically, the invention provided for a dual-processor on-chip microcontroller comprising the main CPU of the microcontroller and a redundant fault processor (further fault processing unit) operating e.g. on a modulo-3 code, implementing a reduced version of

the ALU of the main CPU, for online monitoring of the CPU core. This dual system was able to validate the operations of all failure-prone components of the microcontroller, the CPU, all its registers, and other functional parts like interfaces and peripherals.

In the prior art, the registers of the main CPU were not fully visible and thus not directly accessible by the fault processing unit; faults involving those registers remained undetected. The invention made those registers visible by integrating the fault processing unit on the same chip with the main CPU and by copying the register data of the CPU in a shadow register each time a write operation on one of the processor registers was detected. The register operations could be validated by constantly monitoring the register-to-memory transfers at the write port of the ALU of the main CPU.

The fault processing unit checked the operations of the CPU by means of a reduced copy of the CPU, i.e. by coding the integer core for example on the basis of modulo-3 arithmetic. By using such a reduced copy of the CPU integer core and working with an accordingly coded copy of register data having a lesser number of bits, the validation process was speeded up, achieving an unrivalled balance between dependability and latency of the microcontroller operation.

The invention was particularly useful for monitoring RISC-type of processors as that processor type extensively used its internal registers in read and write operations.

IX. The invention was novel and inventive over the prior art. Document D2 explicitly advised against dual processor systems. Furthermore, it did not mention

shadowing of registers or using a reduced copy of the integer core for detecting faults in the CPU core, which were the salient features of the present invention. In document D2, for example, the secondary redundant processor 18 of the microprocessor system shown in figure 1 had no direct access to the registers of the main CPU 14. This secondary processor was thus not able to perform a full check of the CPU operations and its performance was limited if compared with the invention. The validation method used by the secondary processor was not clearly disclosed in this document; apparently it was not a processor but a linear feedback shift register (LFSR) which was used as a test module. That gap between the invention and the prior art of document D2, i.e. in particular the lack of a reduced shadow register and of a reduced secondary ALU, could not be closed by the prior art, in particular not by document D5.

Document D5 merely disclosed that modulo-3 codes could be used for error detection purposes and provided – at most – some directions in respect of how a modulo-3 copy of the ALU could be constructed. It neither taught nor suggested the use of shadow registers for copying the register bank of the main CPU and to operate on the coded copy of the shadowed data, nor did it disclose how to implement the error detection circuit in a secondary processor for fault processing. Document D5 had clearly in mind the implementation of a single processor referred to as a logic section.

Neither of documents D2 and D5 gave a hint, let alone taught how to combine the main CPU with the redundant secondary processor and the other modules without increasing latency of the microcontroller and

nevertheless maintaining the high fault coverage of the present invention.

Reasons for the Decision

1. The appeal, although admissible, is not allowable since the requests before the Board relate to an invention that does not meet the requirement of inventive step.

2. The relevance of documents D2 and D5 as prior art has not been disputed by the appellant and is expressly endorsed by the Board.

3. Document D2 discloses an embedded microcontroller MCU comprising a dual CPU and a built in self-test (BIST) module (see e.g. D2, figure 1, MCU 10, CPUs 14, 18, BIST 46). In a variant of the dual system, a single main CPU is used, i.e. the optional secondary CPU 18 is eliminated (see column 6, penultimate paragraph; column 7, line 19f.). Relevant as prior art is the validation accomplished by the self-test module BIST 46, applying the well known technique of using a linear feedback shift register (LFSR) 48 for generating signatures of the data streams to be tested through polynomial division.

4. The LFSR 48 of BIST 46 is coupled through bus 12 to the main CPU 14, to memories 36 to 40, and to peripheral units 42 and is arranged to function as a real-time parallel signature analyser (PSA). This LFSR PSA implementation is thus able to signature any type of data streams as well as instruction streams (see D2, column 8, lines 15 to 65). Hence, and since it can interrogate internal registers via a communications

board (see D2, column 8, penultimate paragraph), BIST 46 is able to detect faults in the operation of the main CPU 14. Errors, however, produced by a faulty operation of the CPU core might remain undetected; at least there is no clear indication in document D2 that BIST 46 specifically verifies the health of the CPU core.

5. D2 therefore discloses the following features of claim 1 of the main request: The microcontroller (MCU 10) comprises a central processing unit (main CPU 14), a system bus (bus 12) and one or more functional parts (peripherals 42, memories 36, 38, 40) comprising interfaces (I/O 44; cf. also D2, column 7, lines 7 to 14 and column 10, lines 23 to 25) and peripherals (peripherals 42), and a further fault processing unit (BIST 46, see D2, column 8, line 32f. and column 9, line 2ff.) arranged to analyse and validate various operational aspects of the microcontroller (see D2, column 8, lines 30 to column 9, line 5). The fault processing unit is external with respect to the main CPU (see D2, figure 1), i.e. it is different with respect to said central processing unit; in fact, it operates "with total independence of the 'state of health'" of the main CPU (cf. D2, column 6, line2 ff., column 8, line 46f.). It certainly comprises at least one module, the microprocessor embodied in the PSA itself for example, which performs validation of operations of the microcontroller to achieve dependability of microcontroller operations (see e.g. D2, column 1, line 21f.). Finally, the fault processing unit comprises one or more modules (again the microprocessor embodying the LFSR PSA) for performing validation of the operations of said other functional parts of said microcontroller (see for example column 8, line 51f.). It follows that features (a), except for sub-features (aa) and (ab), as

well as features (b) and (e) are anticipated in combination by the microcontroller of document D2.

6. Besides features (aa) and (ab), the further features (c) and (d) cannot be derived from D2, at least not with sufficient certainty.

7. Regarding feature (c), it is noted that the fault processing unit, BIST 46, is a parallel PSA and thus stores blocks of memory under test in a data register for parallel signature analysis (a high-speed accumulation of memory, for example, see figure 3 data register 106 and column 11, lines 13 to 19 and column 12, line 11ff.). The data register can be said to "make a copy" of the memory blocks, which includes the CPU memory since the "internal registers" can be interrogated by the apparatus for signature analysis (see e.g. D2, column 8, line 37f. and column 8, penultimate paragraph). However, there is no indication that the said data register functions as a shadow memory, i.e. recording data or instructions during program execution for later processing. Feature (c) of claim 1 is hence not fully disclosed by document D2.

8. The following feature (d) begs the question what is meant by "a reduced version of the ALU/MAC of said central processing unit (51) working with a coded copy of the shadowed registers with a lesser number of bits by implementing ALU/MAC operations on said coded copy having a lesser number of bits". This wording is not clear and prompts the reader to consult the description of the invention. Paragraph [60] of the A1-document says: "… includes a reduced version of the ALU/MAC working with a coded copy of the shadowed registers (i.e. with a lesser number of bits), in order to concurrently check the results of the CPU core ALU/MAC

without having a full copy of the ALU/MAC itself." Paragraph [66] says: "… a reduced copy of the CPU Integer Core, including most critical ALU/MAC operations implemented on coded values (e.g. operating on module[sic]-three numbers)."

9. These vague indications imply that the fault detection according to this claim concerns the integer core of the CPU itself and, different from the prior art, is not based on polynomial arithmetic but on estimating the arithmetic results of the CPU core by simulating the core operations in a reduced, for example modulo-three number space. Nevertheless, like the prior art LFSR PSA, it requires a signature generated from register data and a "good" reference value to compare for detecting the fault (see e.g. A1-document, paragraphs [56] "compare… with the reference" and [66] "when a mismatched is detected…").

10. In summary, the distinguishing features of claim 1 of the main request concern the use of a RISC CPU according to feature (aa), the validation of the CPU core itself according to feature (ab), the use of a shadow register module according to feature (c), and the reduced copy of the CPU integer core according to feature (d).

11. Regarding feature (aa), the Board judges that this feature does not provide an inventive contribution over the prior art. At the priority date of the present application, RISC processors had found their way into various devices. They were a normal option also for use in microcontrollers. There was no technical reason that would have deterred a skilled person from using a RISC CPU in a microcontroller of the type shown in document D2. There was also no technical effect achieved which

goes beyond what the skilled person would have expected from using a RISC processor.

12. The appellant argued that the operation of a RISC processor, which heavily relied on internal register operations, posed a particular security problem if the internal registers were not fully visible to the fault detection unit, a problem which had been solved by the invention by providing extended visibility of the internal registers. This argument, however, is not relevant with respect to the prior art of document D2 since already there the fault processing unit has direct access to the data and instruction streams and the internal registers of the microcontroller (see D2, column 8, lines 36 to 37 and lines 60 to 62).

13. Regarding feature (d), that Board judges that this feature does not provide an inventive contribution over the prior art either. Shadowing or mirroring was undisputedly a well-known technique at the priority date of the present application. An inventive contribution, therefore, can only be found in a specific inventive use of the technique, which has not been claimed (and would not be claimable either, considering the invention as disclosed in the application). According to the present claim wording, the shadow register module is included in the fault processing unit to "make a copy of the register bank of the CPU". The fault processing unit then works with "a coded copy of the shadowed registers", i.e. the shadow registers are simply used as an intermediary storage for fault processing. Such an intermediary storage is always an option if data have to be transferred in a system from one component to another component. For example, document D2 proposes storing the CPU system memory and/or registers in a non-volatile memory area for diagnostic purposes (see for example D2,

column 16 line 31ff.). Such considerations invoke obvious options and do not involve an inventive step.

14. Regarding the feature (e), the Board judges that this feature results in an obvious manner from the error detection circuit disclosed in document D5. Starting from the microcontroller of document D2, the skilled person would be faced with the technical problem that the BIST of the prior art microcontroller is not (clearly) able to detect faults in the logic operations of the ALU of the CPU. He or she, therefore, would consult document D5, which promises a error detecting method which precisely and reliably locates errors in the binary operations of an ALU (see Summary of the Invention in D5 at page 2f.).

15. Error detection is achieved by a simple logic section as shown for example in figure 8 of document D5, which only requires access to the CPU registers (see D5, figure 8, operand registers 26, 27) and to reference data to verify those registers (inputs A and B). Since those data are provided by the BIST of the prior art microcontroller, the prior art LFSR PSA can easily be complemented or substituted by the error detection circuit of document D5.

16. This obvious solution implies that the MODULO-3 CALCULATION ELEMENT 68 is a reduced copy of the ALU of the CPU (see D5 page 12, lines 15 to 18). It clearly works on data having a lesser number of bits, namely the 2-bit data produced by the INPUT CODE PRODUCTION CIRCUITs 61, 62, and 73. The combination or use of such an error detecting circuit with the BIST of document D2 does not involve an inventive step.

17. Considering the first and second auxiliary requests, the Board judges that those requests do not add any relevant definitions to claim 1. Defining a "ALU/MAC supervisor module" that does no more than what has already been defined before in the claim does not imply an inventive contribution to the prior art.

18. Considering the third auxiliary request, the Board judges that the request does not add any inventive aspect to the subject matter of claim 1. The extended definitions of the fault processing unit and the liberal register module are obvious in the light of documents D2 and D5. Both documents disclose a "core interface module" (D2: bus interface to main CPU 14; D5, figure 8: circuits 61 and 62). Moreover, the update is based on memory-to-register data transfers (D2 update via bus 12; D5 update via IN1 and IN2) and based on the access to the write port of the ALU of the central processing unit. This last feature is an obvious option if a continuous error control of the CPU or the ALU should take place. Finally, in the error detecting circuit of document D5, the contents of the corresponding ALU registers are compared to detect mismatches (see D5, figure 8, coincidence circuits 63 and 64).

19. Considering the fourth auxiliary request, the Board judges that the request merely summarises the previous requests so that there is lack of inventive step for the reasons already stated above.

20. For the above reasons, the requests before the Board are not allowable, and thus the appeal cannot succeed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

P. Cremona W. Chandler

Decision electronically authenticated