

Internal distribution code:

- (A) [] Publication in OJ
(B) [] To Chairmen and Members
(C) [X] To Chairmen

D E C I S I O N
of 18 November 1998

Case Number: T 0528/96 - 3.5.1

Application Number: 87400709.9

Publication Number: 0240428

IPC: G06F 11/00

Language of the proceedings: EN

Title of invention:
Fail safe architecture for a computer system

Patentee:
Mirowski, Mieczylaw

Opponent:
Joh. Vaillant GmbH & Co

Headword:
-

Relevant legal provisions:
EPC Art. 101(2), 113(1), 116
EPC R. 57(1), 57(3), 58(3), 67, 68(2)

Keyword:
"Right to comment"
"Oral proceedings"

Decisions cited:
T 0019/87, T 0275/89

Catchword:
-



Europäisches
Patentamt

European
Patent Office

Office européen
des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Case Number: T 0528/86 - 3.5.2

D E C I S I O N
of the Technical Board of Appeal 3.5.1
of 18 November 1998

Appellant:
(Proprietor of the patent) MIROWSKI Mieczyslaw
2405 Velvet Valley Way
Owings Mills
MD 21117 (US)

Representative:
Gutmann, Ernest
Ernest Gutmann - Yves Plasseraud S.A.
3, Rue Chauveau-Lagarde
F-75008 Paris (FR)

Respondent:
(Opponent) Joh. Vaillant GmbH & Co
D-42850 Remscheid (DE)

Representative:
Heim, Johann-Ludwig, Dipl.-Ing.
c/o Johann Vaillant GmbH u. Co.
Postfach 10 10 20
Berghauser Str. 40
42850 Remscheid (DE)

Decision under appeal: Decision of the Opposition Division of the
European Patent Office posted 29 March 1996
revoking European patent No. 0 240 428 pursuant
to Article 102(1) EPC.

Composition of the Board:

Chairman: P. K. J. van den Berg
Members: A. S. Clelland
C. Holtz

Summary of Facts and Submissions

- I. This is an appeal against the decision of the Opposition Division to revoke European patent No. 240 428 on the ground that the subject-matter of independent claims 1 and 23 lacked an inventive step having regard to the disclosure of each of the following documents considered separately:
- D1: Regelungstechnische Praxis, volume 23 (1981) No. 8, pages 268 to 275, Knörnschild:
"Speicherprogrammierbare Steuerungen für den sicherheitstechnischen Einsatz-Anforderungen und Prüfungen"
- D2: EP-B-88 364
- II. The appellant (patentee) lodged an appeal against this decision and paid the prescribed fee. A written statement setting out the grounds of appeal was subsequently received. In this statement the appellant argued that the claims of the granted patent were inventive and that the impugned decision was not based on grounds or evidence on which he had had an opportunity to present comments, Article 113(1) EPC.
- III. Following a communication from the Board the appellant submitted two new sets of claims of first and second auxiliary requests.
- IV. Oral proceedings were held before the Board on 16 March 1997, both parties having requested them.

At the oral proceedings, the appellant requested that the decision under appeal be set aside and that the patent be maintained, either on the basis of the claims as granted (main request), or on the basis of the claims of the first auxiliary request, the second auxiliary request having been withdrawn. Refund of the appeal fee was also requested.

The respondent (opponent) did not appear at the oral proceedings. He had previously, in response to the statement of grounds, referred to the arguments contained in the original grounds of opposition and to the opposition division's decision. He requested that the revocation of the patent be upheld, i.e. that the appeal be dismissed.

V. At the oral proceedings the Board refused the main request and decided to continue the procedure in writing on the basis of the auxiliary request.

VI. Following a communication from the Board, raising issues of clarity, the appellant submitted a revised set of claims for the auxiliary request.

VII. Claim 1 of the main request reads as follows:

"1. A computer system (10), having a processor (14) with an internal register, a storage means (22) for storing at least operation code instructions executable by said processor (14), and a temporary memory (24) storing at least data manipulated by said processor (14), said computer system (10) comprising:

means for verifying the contents of said storage means (22) by applying an algorithm to the stored operation code instructions;

means for testing the integrity of said temporary memory (24);

means for checking the validity of operation of said processor (14) by executing said operation code instructions in discrete subsets and monitoring the condition of said internal register during the execution;

characterized in that:

said means for testing the integrity of the temporary memory (24) includes:

means for saving the current data stored in said temporary memory (24);

means for writing a test pattern into said temporary memory (24) and algorithmically verifying said test pattern; and,

means for restoring said current data in said temporary memory (24);

and in that said computer system (10) further comprises:

means for periodically activating said means for verifying the contents of said storage means (22); said means for testing the integrity of said temporary memory (24), and said means for checking the validity of operation of said processor (14) during the execution of said operation code instructions by said processor (14); said means for periodically activating comprising a timer (T1) which periodically provides a non-maskable interrupt (NMI) to the processor (14) of the computer system (10) and,

means for inhibiting the execution of said operation code instructions by said processor (14) dependent upon the verification of said storage means (22), the testing of the integrity of said temporary memory (24), and the validity check of the operation of said processor (14) by the respective said means for verifying the contents of said storage means (22), said means for testing the integrity of said temporary memory (24) and said means for checking the validity of operation of said processor (14)."

Claim 23 of the main request is an independent method claim having features corresponding to those of claim 1.

VIII: The auxiliary request is based on the following documents:

Description: pages 2, 2a, 2b, as received on 20 May 1998; pages 3 to 13 of the published patent specification

Claims: 1 to 18 as received on 20 May 1998

Drawings: Figures 1 to 5C of the published patent specification

Claim 1 of the auxiliary request reads as follows:

"1. A computer system (10) incorporating a fault tolerant fail safe architecture, having a processor (14) with an internal register, a storage means (22) for storing at least operation code instructions executable by said processor (14), and a temporary memory (24) storing at least data manipulated by said processor (14), said computer system (10) comprising means for periodically activating the following testing means:

means for verifying the contents of said storage means (22) by applying an algorithm to the stored operation code instructions including means for ascertaining whether said algorithm, as applied to said stored operation code instructions, produces a desired result,

means for testing the integrity of said temporary memory (24) including means for saving the current data stored in said temporary memory (24), means for writing a test pattern into said temporary memory (24) and

algorithmically verifying said test pattern, and means for restoring said current data in said temporary memory (24), means for determining whether said test pattern, as written into said temporary memory (24), is algorithmically verified;

means for checking the validity of operation of said processor (14) by executing said operation code instructions in discrete subsets and monitoring the condition of said internal register during the execution including means for initially checking the operation of said internal register and a comparison means for determining whether the condition of said internal register corresponds to a respective predetermined condition for said execution of the discrete subset;

means for inhibiting the execution of said operation code instructions by said processor (14);

means for generating a fail safe trigger signal which is independently actuated by said means for ascertaining, said means for determining and said comparison means, said fail safe trigger signal being applied to said means for inhibiting, the further execution of said operation code instructions by said processor (14) if said fail safe trigger signal is not substantially timely received from said means for generating, characterized in that:

said means for periodically activating comprises a timer (T1) which periodically provides a non-maskable interrupt (NMI) to the processor (14) of the computer system (10), and a timer (T2) for resetting said timer (T1) at regular intervals,

and in that said computer system (10) includes a fail safe trap means being responsive to detection of a fault if that said means for ascertaining does not produce said desired result, said means for determining determines that said test pattern is not algorithmically verified, said means for initially

checking the operation of said internal register is unsuccessful, or said comparison means determines that said predetermined condition of said internal register is not present during the execution of said discrete subset of operation code instructions, to initiate resynchronizing of the operation of said processor (14), and to initiate said testing means, said fail safe trap means further being responsive to detection of more than two faults within the time period of a preselected plurality of successive non-maskable interrupts (NMI) to independently actuate delay of said fail safe trigger signal such that said fail safe trigger signal is not substantially timely generated by said means for generating and is not substantially timely received, thereby causing said means for inhibiting to inhibit the execution of said operation code instructions by said processor (14)."

- IX. The appellant argued that the impugned decision was the first occasion on which he had been informed that the grounds of opposition were considered to prejudice the maintenance of the patent. No substantive communication had been sent before the decision was taken and oral proceedings had not been appointed even though they were clearly appropriate. The violation of the appellant's right to be heard, Article 113(1) EPC, constituted a substantial procedural violation within the meaning of Rule 67 EPC.

As regards inventive step it was argued that the impugned decision did not adopt the problem-and-solution approach and failed to indicate what problem was solved either in the patent or in D1. D1 constituted a catalogue of different safety measures to be performed on a test specimen at the time of manufacturing and was not concerned with operational running. There was no disclosure in D1 of the use of non-maskable interrupts in order to provide a periodic

inhibition of execution of operation code instructions. It had moreover not been shown that all the features of claim 23, the independent method claim, were derivable from D1, nor that the constructional features of claim 1, which defined means to carry out the method of claim 23, were to be found in D1.

Similarly, the discussion of D2 in the impugned decision contained assertions that this document solved the same problem and disclosed the same means as in the patent, but D2 did not in fact disclose all the claimed features and was in any case directed to a fundamentally different problem. Finally, the opposition division had asserted that the features of the dependent claims were obvious but had given no reasoning as to why this was held to be so.

- X. The respondent referred to the arguments contained in their original grounds of opposition and to the opposition division's decision. No comment was made on the claims of the auxiliary request.

Reasons for the Decision

The appeal is admissible.

- 1. *The Right to Comment, Article 113(1) EPC*
 - 1.1 The appellant argued in the statement of grounds that because the opposition division did not issue a communication before the decision was taken there was an infringement of Article 113(1) EPC, which requires that the decision must be based on grounds or evidence

on which the parties concerned have had an opportunity to present their comments. The issue of a communication was argued to be mandatory in the light of Article 101(2) and Rule 58(3) EPC.

1.2 However, the Board notes that no requirement is derivable from the EPC or Rules that the opposition division is obliged to issue a communication, other than in the special case under Rule 71(a) when oral proceedings are appointed. Article 113(1) EPC may be satisfied if the reasoning of the decision has previously been raised and discussed in the proceedings by the parties themselves. As noted in decision T 275/89 (OJ EPO 1992, 126), see point 3.2, an opposition division is not obliged in every case to issue at least one [substantive] communication. In the statement of grounds at page 2, second full paragraph, the appellant observed that the impugned decision "merely referred to passages of the Notice of Opposition". Since the opposition file shows that the appellant was invited to comment on the opposition the requirement of Article 113(1) EPC has been met.

2. *The Right to Oral Proceedings, Article 116 EPC*

2.1 The final paragraph in the patentee's response to the opposition, the last document on the file before the opposition division took its decision, reads as follows:

"Should the opposition division feel that further information is required, the patentee will be pleased to respond in due course, either in writing or during the oral hearing"

- 2.2 The opposition division argued in its decision that this statement did not constitute a request for oral proceedings. In the file as a whole the only other reference to oral proceedings or to an "oral hearing" is to be found in the notice of opposition, in which the opponent makes a conditional request for oral proceedings if the opposition division is minded to reject the main request for revocation of the patent.
- 2.3 The established jurisprudence of the Boards of Appeal (see eg T 19/87 OJ EPO 1988, 268) is that oral proceedings are a very important procedural right and that, whether or not the EPO considers it to be expedient, a party is entitled to oral proceedings upon request. However, a clear request must have been made for such proceedings. In the present case the Board takes the view that the reference in the patentee's response to an "oral hearing", although apparently a reference to oral proceedings within the meaning of Article 116 EPC, does not constitute a **request** for such proceedings. The cited passage seems to assume that oral proceedings will in fact take place even though an appropriate request was never made. Although the opposition division might reasonably have been expected to query whether such a request was in fact intended, the fact that it did not do so does not of itself constitute a procedural violation since the onus to make a clear request is on the party concerned.
- 2.4 In accordance with Rule 67 EPC the reimbursement of appeal fees shall be ordered where the Board of Appeal deems an appeal to be allowable, if such reimbursement is equitable by reason of a substantial procedural violation. Since there was no procedural violation the appeal fee cannot be reimbursed.

3. *Inventive Step (main request)*

3.1 At the oral proceedings it was accepted by the appellant that document D1 relates to a computer system in accordance with the preamble of claim 1 in which operational testing of the system is cyclically effected.

3.2 D1 discloses at page 273, point 2.2.4.1 a cyclically performed ROM test and at point 2.2.4.2, second paragraph a RAM integrity test in which existing data is moved to a second RAM for the duration of the test, i.e. the current data is saved and after testing restored; the test itself is performed by "walking" a bit through the memory, i.e. writing a "0" to all locations and moving a "1" through each location in turn, followed by writing a "1" to all locations and moving a "0" through. This procedure constitutes "algorithmically verifying said test pattern" within the meaning of the claim. It is not explicitly stated that this particular test is performed cyclically, although various other tests, including the alternative RAM test described at point 2.2.4.2, first paragraph are stated to be performed cyclically, and point 2.2.4.5 implies that this is true of all RAM testing. The Board accordingly takes the view that the skilled person would understand the "bit walking" RAM test also to be performed cyclically.

3.3 D1 discloses at point 2.2.4.3 various tests for the registers and the ALU, point 2.2.4.5 also implying that these tests are carried out cyclically. At point 2.2.4.4 a further processor test is described, referred to as a "watch-dog" timer, in which an independent hardware-based timer is used to monitor the time taken

to perform processor operations. This is also said to be combinable with the ROM test, implying it is periodic. From point 2.2.4.5 it can be seen that in the event of an error the processor is switched off, i.e. the execution of opcode instructions is inhibited.

3.4 D1 does not indicate what is meant by performing tests cyclically, nor does it mention the use of interrupts such as a non-maskable interrupt (NMI). In the course of the oral proceedings it was argued by the appellant that from page 6 lines 1 to 10 of the patent it was clear that a pointer register forming part of step 138 in Figure 2D served to initiate the various self-check modules in turn, each in response to a respective interrupt. D1, it was argued, did not suggest carrying out the individual tests in a predetermined sequence; the skilled person seeking to implement D1 might well provide a separate, unsynchronized, cycle for each module and/or might initiate the modules repetitively rather than in sequence, e.g. carrying out five RAM tests for each ROM test. Moreover, any suggestion that the skilled person would provide testing in D1 which was interrupt-driven was ex post facto and depended on an impermissible combination of D1 and D2, the latter showing the use of an interrupt for testing although not an NMI. The skilled person would be prejudiced against interrupt-driven testing in a program where safety was the prime consideration.

3.5 Dealing first with the matter of what the reference to testing "cyclically" in D1 means, it is noted that in point 2.2.4.5 it is stated that the sum of all test cycles must be smaller than the safety-critical process lag of the application. Although this does not exclude parallel and/or asynchronous test cycles with a separate timer controlling each test, the RAM and register testing is dependent on information contained within the ROM (see point 2.2.4.2, last sentence of

first and third paragraphs, and point 2.2.4.3, penultimate sentence). This implies that the ROM cannot be tested at the same time as these devices and that, as each subroutine must be read out in sequence, testing is also sequential. The skilled person could therefore be expected to infer from D1 that testing must be carried out synchronously and under the control of a single timer.

3.6 It is observed that although at the oral proceedings the appellant argued that in the patent each interrupt led to a respective test, so that the tests were carried out in a fixed sequence, claim 1 of the main request does not require that the tests be performed in any particular order. It will be clear from the above discussion that in D1 the tests are activated periodically within the meaning of the claim.

3.7 The only remaining feature of claim 1 is that the processor has a non-maskable interrupt, i.e. an interrupt of highest priority. Such a feature is however standard in modern processors and in view of the importance of integrity testing might be expected to be the interrupt that the skilled man would use to halt normal processing and initiate integrity testing.

3.8 Thus the skilled person, seeking to carry out the teaching of D1, would without the exercise of inventive skill arrive at a computer system having all the features of claim 1.

3.9 Since the subject-matter of claim 1 lacks an inventive step it follows that the same objection applies to claim 23, which is a method claim having the same features as claim 1.

4. *Inventive Step (Auxiliary request)*

- 4.1 Claim 1 of this request includes the feature of "fail safe trap means" which serve, on detection of a failure, to initiate resynchronization of the processor; these means are described in the patent at page 5 lines 18 to 31 in connection with Figure 2C. This procedure is stated to have the advantage that if a fault is only transient then successful resynchronization causes the system to reboot and continue where it left off. Only in the event of a persistent fault, resulting in a failure count of three within 10 interrupts, is the fail-safe condition activated.
- 4.2 The feature of resynchronization on failure detection is not derivable from D1. Nor is it a feature which the skilled person could be expected to incorporate without the exercise of inventive skill. The Board accordingly concludes that the subject-matter of claim 1 of the auxiliary request involves an inventive step having regard to the disclosure of D1.
- 4.3 In its decision the opposition division also considered a second document, D2. This document discloses interrupt-driven self-checking of the internal state of a processor, the interrupts being generated by a counter (60 in Figure 1). If an error is encountered, the processor enters an "interrupt disabled state" in which the further execution of opcode is inhibited, see column 13 lines 9 to 33. From the discussion of Figure 7 at column 12 line 28 to column 14 line 10 it appears that the diagnostic functions which provide for RAM and ROM testing are part of the normal operating cycle of the processor. There is no mention of what happens to the existing contents of the RAM during testing. The effect of an interrupt is described in the passage bridging columns 12 and 13, and in connection with Figure 9 at column 14 line 11 to column 15 line 38; the processor halts its normal operating

cycle, including a halt to diagnostic checking, and enters a subroutine in which the processor registers are themselves checked. D2 accordingly provides for two separate and unrelated forms of self-checking, only one of which is interrupt-driven. If a failure is established the device enters a failure loop; there is no discussion of recovery from a transient failure.

4.4 The Board accordingly concludes that the skilled person, starting out from the teaching of D2, would not arrive at the subject-matter of claim 1 of the auxiliary request.

4.5 Nor does it appear that there is any combination of D1 and D2 which would lead to the claimed invention without the exercise of inventive skill.

5. The Board has noted a number of clerical errors in claim 1 which require correction; at page 1, lines 16 and 17 a definite article has been displaced and at page 2, lines 1 and 2 the text does not make wholly clear that execution of opcode instructions by the processor is inhibited if the fail safe trigger signal is not received in time. The Board also notes that the revised introduction to the description is not wholly in conformity with the revised claims in that it refers at page 2 line 7 and lines 17 to 19 to the invention as encompassing a method of fail safe operation. Moreover, the statement at page 2a, lines 1 and 2 that the cited prior art is not concerned with "fault tolerant architecture in the sense of the present invention" is not considered wholly accurate. For these reasons it is necessary to remit the case to the first instance to enable the required amendments to be carried out.

Order

For these reasons it is decided that:

1. The main request is refused.
2. The decision under appeal is set aside.
3. The case is remitted to the first instance with the order to maintain the patent on the basis of the claims of the auxiliary request after any necessary amendment (see point 5 above).

The Registrar:

The Chairman:

M. Kiehl

P. K. J. van den Berg

