Internal distribution code:

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

Datasheet for the decision of 24 March 2021

Case Number: T 2081/15 - 3.5.07

Application Number: 09171333.9

Publication Number: 2172843

IPC: G06F11/16, G06F11/00

Language of the proceedings: EN

Title of invention:
Method and systems for restarting a flight control system

Applicant:
General Electric Company

Headword:
Continuous bank of RAMs for faster fault recovery in a flight control system/GENERAL ELECTRIC

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - after amendment - claim 1 (yes)

Catchword:

Plausible argument of the appellant about the choice of specific, non-obvious hardware implementation, in favour of an inventive step over the prior art (Article 56 EPC).

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 2081/15 - 3.5.07

D E C I S I O N
of Technical Board of Appeal 3.5.07
of 24 March 2021

Appellant: (Applicant)	General Electric Company 1 River Road Schenectady, NY 12345 (US)
Representative:	Openshaw & Co. 8 Castle Street Farnham, Surrey GU9 7HR (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 27 May 2015 refusing European patent application No. 09171333.9 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chair	J. Geschwind
Members:	C. Barel-Faucheux
	M. Jaedicke

Summary of Facts and Submissions

I. The appeal lies from the examining division's decision to refuse European patent application No. 09171333.9, which was published as EP 2 172 843 A1.

The following document is cited in the contested decision:
D1: WO 02/073505, published on 19 September 2002

The examining division decided that the claims of the sole request did not involve an inventive step having regard to document D1 (Article 56 EPC).

II. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the set of claims of a new main request or of either of the new first and second auxiliary requests filed with the statement of grounds of appeal.

III. In a communication following the summons to oral proceedings, the board stated that it was questionable whether or not generalising the expression "during flight controller startup" to "at a predetermined time" in claim 1 of the main and first auxiliary requests constituted or not an "intermediate generalisation" violating Article 123(2) EPC. The board also noted that the wording "during a restart of the processor" in the feature "control transfer of the at least one executable program from the second RAM sector to the first RAM sector during a restart of the processor" in claim 1 of the main and first auxiliary requests appeared to add subject-matter (Article 123(2) EPC). The board gave its preliminary opinion that claim 1 of

the main and first auxiliary requests did not appear to be inventive over D1 and the skilled person's common general knowledge (Article 56 EPC). The board explained why the second auxiliary request did not appear to be admissible and why it considered the wording "transient state" in claim 1 of said request to be unclear (Article 84 EPC). The board stated that it considered claim 1 of the second auxiliary request to lack an inventive step (Article 56 EPC).

IV. By a letter dated 6 January 2021, the appellant filed a new sole request replacing all previous requests. The appellant provided further arguments in support of the allowability of this sole request on file.

V. Oral proceedings were held as scheduled and the appellant was heard on relevant issues. At the end of the oral proceedings, the Chair announced the board's decision.

VI. The appellant's final requests are that the decision under appeal be set aside and that a patent be granted on the basis of the sole request filed by letter of 6 January 2021.

VII. Claim 1 of the sole request reads as follows (itemisation by the board):

(A) A flight control system (100) comprising:

(B) at least one sensor (112) configured to collect data;

(C) a flight controller (110) coupled to said at least one sensor, said flight controller comprising:

(D) a random access memory (RAM) device (144) comprising a continuous bank of RAM,
(D1) said RAM device configured to store at least one executable program in a first RAM sector (150) and a second RAM sector (154) of said continuous bank of RAM,
(D2) wherein said first RAM sector (150) is a low-RAM sector on a low address space and said second RAM sector (154) is a high-RAM sector on a high-address space of said continuous bank of RAM; and

(E) a processor (140) configured to execute the at least one executable program from the first RAM sector (150) to process the sensor data, and to output operational instructions; and

(F) at least one actuator (116) coupled to said flight controller, said actuator configured to receive and execute the operational instructions,

(G) wherein the system further comprises a read only memory (ROM) device configured to store the at least one executable program,

(H) and said processor (140) is further configured to:
(H1) control transfer of the at least one executable program from the ROM device (142) to the first RAM sector (150) and the second RAM sector (154) of said continuous bank of RAM at a startup of said flight controller (110);
(H2) control transfer of the at least one executable program from the second RAM sector (154) to the first RAM sector (150) after an error or fault with the processor (140); and
(H3) reinitialize the processor (140) using the executable program transferred to the first RAM sector

(150) to resolve an error or fault with the processor (140).

VIII. The appellant's arguments, in so far as relevant to this decision, are addressed in detail below.

Reasons for the Decision

Application

1. The application relates to a method for rapidly restarting a flight control system after an error or fault (paragraphs [0001] and [0005] of the published application).

2. For example, an operator's movements of a flight stick are received by a sensor 112 and transferred to a flight controller 110. The controller determines the operations of flight control surfaces of the aircraft that correspond to the operator input. It may also combine the operator input with any other sensor inputs (for example weather-related inputs, altitude input and/or aircraft speed input). In some embodiments, the controller 110 does not receive an operator input, but rather determines the operations of flight control surfaces of the aircraft on the basis of, for example, a pre-programmed flight plan and inputs from the sensor 112. Actuators 116 move the flight control surfaces of the aircraft according to instructions from the controller 110 (Figure 1, paragraph [0012]).

3. The controller 110 includes a processor 140, a read only memory (ROM) device 142 and a random access memory (RAM) device 144 which includes one continuous bank of RAM (Figure 2, paragraphs [0013] and [0015]).

4. The one continuous bank of RAM includes a first sector on the low-address space, referred to as "low-RAM" 150, where executable programs are copied to and where they execute from. It also includes a second sector on the high-address space, referred to as "high-RAM" 154, where programs are placed in a transient state. The programs are copied to the high-RAM 154 and low-RAM 150 from the ROM device 142 (or from a target host system). Upon the occurrence of an event and/or fault, programs are copied from the high-RAM 154 to the low-RAM 150 and executed from low-RAM 150. The processor 140 controls read/write operations between the ROM device 142, the low-RAM 150 and the high-RAM 154 (paragraph [0015]).

5. The flight controller 110 might also include a direct memory access (DMA) engine 162. The DMA engine 162 performs read/write operations between the ROM device 142, the low-RAM 150, and the high-RAM 154 independently of the processor 140. The DMA engine 162 facilitates rapid transfer of data between the memory devices 142 and 144 (paragraph [0016] in conjunction with Figure 3).

6. A software error may interrupt the operation of the processor 140. The software error may be, for example, an event such as a divide-by-zero error, a data access exception or an instruction access exception in the executable program running on the processor 140 (paragraph [0018]).

7. Added subject-matter

7.1 The amendments made by the appellant (based on originally filed claims 5 and 6, and page 7, lines 8 to 14 of the description as originally filed) in reply to

the board's communication have overcome the objections under Article 123(2) EPC.

8. Inventive step

8.1 The examining division considered D1 to be the closest prior art and the board also considers D1 to be an appropriate starting point for the assessment of inventive step.

8.2 Figure 1 of D1 depicts a conventional triple-redundant flight-critical computer architecture that might typically be used on board a spacecraft. Redundant sensors 15 provide inputs to a first computer 11, a second computer 12 and a third computer 13. Each computer includes inputs 17, processing 18 and outputs 19. The outputs from each of the redundant computers 11 to 13 are routed to redundant actuators 16. In addition, the redundant computers 11 to 13 are interconnected by a cross-channel data link (CCDL) 14 which allows the computers to interchange data (paragraph [0003]).

8.2.1 D1 thus discloses features (A), (B), (C), (E) and (F).

8.3 Document D1 relates in particular to a real-time recovery of a flight-critical computer after a single "event upset" (SEU) caused by radiation (paragraph [0060]). D1 explains that energetic particles (for example protons, heavy ions) in space radiation can cause anomalies in electronic equipment, such as flight-critical computers, on-board satellites, spacecraft and aerial vehicles flying at high altitudes. A single energetic particle can deposit enough charge in an integrated circuit to change the

state of internal storage elements and may also cause more complex internal behaviour. The observable state changes can include bit-flips, latched power conditions and short circuits (paragraph [0002]).

8.4 In D1, multiple versions of the same (or similar) computer operational flight programs (OFPs) are run on the same processor and each one of these multiple OFPs is associated with a dedicated memory partition located in a distinct hardware random access memory (RAM) module (i.e. RAM modules 26, 27, 28) to provide *space* redundancy (paragraphs [0011], [0012] and [0037], Figure 2).

A version of an executable OFP is downloaded from a flight-critical computer's non-volatile memory (NVM) 24 to each of the respective hardware isolated memory blocks 70, each hardware isolated memory block being contained on respective banks of system RAM 26 to 28 (paragraph [0038], Figure 3). One of the OFP is designated as the "controller" OFP and the other OFPs are designated as "observer" OFPs. The controller OFP is responsible for controlling devices attached to the flight-critical computer. The observer OFP can be either a copy of the controller OFP or an alternate design that replicates the full states of the controller (paragraphs [0013] and [0037]).

In one embodiment, to provide *time* redundancy, the controller OFP is run, and then each observer OFP is run in a predetermined sequence (paragraph [0039]).

In one aspect of the method in D1, each invalid OFP is recovered by copying a data image of the memory partition associated with a valid OFP (paragraph [0014]). In other words, when erroneous data is

detected in one of the memory partitions, that data is overwritten with fault-free data from an undamaged memory partition (Figure 3; see also claim 1 of D1).

8.4.1 Therefore, D1 discloses the following features:
(D') a random access memory (RAM) device comprising a ~~continuous~~ bank of RAM,
(D1') said RAM device configured to store at least one executable program in a first RAM sector and a second RAM sector of said ~~continuous~~ bank of RAM;

(G') wherein the system further comprises a ~~read only memory (ROM)~~ *non-volatile memory* device configured to store the at least one executable program,

(H') and said processor is further configured to:
(H1') control transfer of the at least one executable program from the ~~ROM~~ *non-volatile memory* device to the first RAM sector and the second RAM sector of said ~~continuous~~ bank of RAM at a startup of said flight controller;
(H2') control transfer of the at least one executable program from the second RAM sector to the first RAM sector after an error or fault with the processor.

8.5 It follows that the features distinguishing claim 1 from the disclosure of document D1 are the following, as also acknowledged by the appellant:

(df1) the bank of RAM is a continuous bank of RAM;
(df2) said first RAM sector is a low-RAM sector on a low-address space and said second RAM sector is a high-RAM sector on a high-address space of said continuous bank of RAM (corresponding to feature D2);
(df3) the non-volatile memory device is a ROM device;

(df4) the processor (140)is re-initialised using the executable program transferred to the first RAM sector after an error or fault with the processor (corresponding to feature H3).

8.6 A ROM as in claim 1 of the application in hand is one example of a non-volatile memory. The skilled person would choose a ROM as an obvious alternative.

Thus the board considers distinguishing features (df3) as obvious to the skilled person.

8.7 D1 discloses that it is known in the art to recover a flight-critical computer via re-initialisation schemes, for example by cycling power ("on-off-on"). D1 teaches that although cycling power to the computer clears some induced errors, it also results in a period of time when the computer is not available for tasks such as spacecraft stabilisation (paragraph [0004]).

8.8 The appellant argued that the invention "may also provide energy efficiency benefits through not necessitating the simultaneous running of the executable program across multiple RAM devices _ as appears to be required by the teaching of D1 with its 'controller' and 'observer' memory banks" (statement of grounds of appeal, last paragraph of page 4).

The board has doubts that "not necessitating the simultaneous running of the executable program across multiple RAM devices" constitutes a difference, and therefore also has doubts that the invention makes it possible to save energy. During the oral proceedings before the board, the appellant stated that the expression "a transient state" of a program meant "a non-permanent state". The board notes, however, that

this does not equate to "a frozen state" or "an un-running state". In particular, in the invention of the application in hand, the executable program stored in the second RAM sector in a transient state might correspond to an executable program running simultaneously with the executable program in the first RAM sector. This would indeed enable a faster recovery after a fault since the state of the program of the second RAM sector and its data, would (almost) correspond to the state of the identical program, and corresponding data, running on the first RAM sector at the time the error occurred.

8.9 The appellant further argued that "[t]he provision of low and high-address RAM sectors within the same continuous bank of RAM would allow for faster copying of the executable program from the high to low RAM sectors compared to D1's requirement for copying the executable program between spatially distinct memory banks" (see statement of grounds of appeal, last paragraphs of page 4 and 6, respectively). The board recognises that, when using distinct memory banks, there is a need to first access the corresponding memory banks (via a corresponding address), in contrast to using the same memory bank.

8.10 In view of the above, the objective technical problem to be solved by distinguishing features (df1), (df2) and (df4) is "how to reduce the elapsed time between the detection of an error and the re-initialisation of the flight control processor" (paragraph [0018] of the published application discusses the effect of the period of time that a flight control system is interrupted due to a software error).

8.11 The appellant argued that, for faster copying, the skilled person would not use low and high-address RAM sectors within the same continuous bank of RAM instead of isolated memory blocks of multiple RAMs as in D1, for the following reasons:
D1 is concerned with the occurrence of "single event latch-ups" (SELs). Specifically, paragraph [0002] of D1 states "[a] latched power condition is an example of a potentially catastrophic fault mode known as a single event latch-up (SEL). A short circuit in an integrated circuit typically results in a hard failure, which is typically mitigated by redundant circuitry. In order to protect a spacecraft against a single flight critical computer failure, redundant computers are typically employed". Furthermore, paragraph [0004] of D1 states that "[i]t is important that each flight critical computer, such as a spacecraft navigation computer, is able to detect and recover from both an SEU and an SEL because an undetected transient fault can possibly diverge to a hard failure".

The appellant argued that the skilled person would not be prompted to modify the system disclosed in D1 so as to use the same (i.e. a single) continuous bank of RAM instead of isolated memory blocks of multiple RAMs since doing so would remove the hardware redundancy present in D1, which appears to be critical in order to recover from SELs and mitigate hardware failures.

8.12 The board notes that D1 states that a conventional method of recovering a flight-critical computer in a radiation environment, without accessing another computer, is to save the state data of the computer, stored in the random access memory (RAM) 26-28, to a radiation-hardened temporary storage while executing the OFP. When a SEU is detected, data is dumped from

the temporary storage back to the random access memory (RAM) 26-28. According to D1, however, this approach fails to preserve data integrity in the temporary storage and can also cause the redundant computers 11 to 13 to lose synchronisation (paragraph [0006]). The method in D1 is based on the concept of analytical redundancy such that it can be implemented in application software without the need for additional radiation-hardened devices (paragraph [0010]). Each of the multiple OFPs is associated with a dedicated memory partition located in a distinct hardware random access memory (RAM) module 26, 27 and 28. D1 stipulates that the effects of an SEU, such as those caused by a cosmic ray event, will manifest themselves in a data value contained in one memory partition (paragraphs [0011] and [0012]). In one aspect, each invalid OFP is recovered by copying a data image of the memory partition associated with a valid OFP (paragraph [0014]).

This means that in D1 the RAM modules 26 to 28 are partitioned in memory partitions (paragraph [0036]). One aspect of the invention of D1 is that a hardware isolated memory block is assigned to the controller OFP and separate hardware isolated memory blocks are assigned to each of the observer OFPs (paragraphs [0037], [0038]).

When erroneous data is detected in one of the memory partitions of one of the RAMs,that data is overwritten with fault-free data from an undamaged memory partition [note from the board: of another RAM, since there is direct mapping of memory addresses between any two given partitions, see paragraph [0058]]. D1 teaches that this recovery scheme allows a flight-critical

computer to recover from an SEU within a single iteration (paragraphs [0042] and [0060]).

8.13 Since claim 1 does not exclude the possibility that distinct multiple RAMs are used, the question is whether or not the skilled person would be prompted to modify the system disclosed in D1 so as to use the same (i.e. a single) continuous bank of RAM instead of, or in addition to, using isolated memory blocks of multiple RAMs.

8.14 The board is of the opinion that, for faster copying, the skilled person could use low and high-address RAM sectors within the same continuous bank of RAM instead of isolated memory blocks of multiple RAMs as in D1, but has doubts that they would.

8.15 The appellant did not contest that, at the priority date, continuous banks of RAM were known but explained that there was no evidence from the identified prior art at hand that it was obvious to implement a continuous bank of RAMs for faster fault recovery in a flight control system.

8.16 The board notes that by using the same continuous bank of RAM, a fault (for example an SEL) might impact the entire continuous bank of RAM, with the consequence that the claimed fault recovery failed. The skilled person would be aware of this disadvantage. Therefore, the appellant's argument that, for want of any relevant teaching in the prior art for this technical field, it was not obvious to implement the claimed solution for faster fault recovery in a flight control system is technically plausible. Consequently, the board considers the subject-matter of claim 1 to be a non-obvious alternative solution, different from a

conventional hardware redundancy configuration as known in the art.

8.17 Therefore, claim 1 of the sole request involves an inventive step (albeit a small one) over D1 and the skilled person's common general knowledge (Article 56 EPC).

Concluding remarks

9. The appellant has overcome the objections raised in the decision under appeal and the board has no further objections against claim 1. However, the board did not examine the remaining claims, the description and the drawings.
The case is thus to be remitted to the department of first instance for further prosecution.

Order

For these reasons it is decided that:

1. **The decision under appeal is set aside.**

2. **The case is remitted to the department of first instance for further prosecution.**

The Registrar: The Chair:

S. Lichtenvort J. Geschwind

Decision electronically authenticated