

Internal distribution code:

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

**Datasheet for the decision
of 1 July 2021**

Case Number: T 0788/18 - 3.5.07

Application Number: 10090009.1

Publication Number: 2447844

IPC: G06F11/16

Language of the proceedings: EN

Title of invention:

Validating a correct operation of a HMI

Applicant:

Bombardier Transportation GmbH

Headword:

Validating correct operation of a HMI/BOMBARDIER

Relevant legal provisions:

EPC Art. 56

Keyword:

Inventive step - (yes)



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 0788/18 - 3.5.07

D E C I S I O N
of Technical Board of Appeal 3.5.07
of 1 July 2021

Appellant: Bombardier Transportation GmbH
(Applicant) Eichhornstraße 3
10785 Berlin (DE)

Representative: Patentanwälte Bressel und Partner mbB
Potsdamer Platz 10
10785 Berlin (DE)

Decision under appeal: **Decision of the Examining Division of the
European Patent Office posted on 13 October 2017
refusing European patent application No.
10090009.1 pursuant to Article 97(2) EPC**

Composition of the Board:

Chair J. Geschwind
Members: C. Barel-Faucheux
P. San-Bento Furtado

Summary of Facts and Submissions

- I. The appellant (applicant) filed an appeal against the decision of the examining division refusing European patent application No. 10090009.1.
- II. The documents cited in the contested decision included:
D1: DE 199 51 541 C1, published on 26 October 2000
D2: US 2007/0222642 A1, published on 27 September 2007
- III. The examining division refused the application for lack of inventive step of the subject-matter of all claims of the sole request over the prior art disclosed in document D2 combined with the disclosure of document D1.
- IV. With the statement of grounds of appeal, the appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the main request subject of the decision under appeal or, in the alternative, any of the first to fifth auxiliary requests filed with the grounds of appeal.
- V. In a communication in accordance with Article 15(1) RPBA, the board stated that it was of the preliminary opinion that independent apparatus claim 5 and method claim 1 were not clear and lacked support in the description as originally filed, referring to Article 84 EPC, and that the application did not seem to comply with the requirements of Article 83 EPC. The board concurred preliminarily with the examining division decision that independent claims 1 and 5 of the main request were not inventive over a combination of the disclosures of documents D2 and D1 (Article 56 EPC). The board stated that independent claim 5 and

corresponding claim 1 of the first to fifth auxiliary requests did not appear to be inventive over a combination of documents D2 and D1 (Article 56 EPC). The board was inclined not to admit the first to fifth auxiliary requests into the proceedings.

- VI. With a letter of reply, the appellant filed amended main and first auxiliary requests together with amended description pages for each request. It withdrew the previous first to fifth auxiliary requests filed with the statement of grounds of appeal.
- VII. During the oral proceedings, the appellant filed a new main request to replace all the former requests on file which were thus withdrawn.
- VIII. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of claims 1 to 8 of the main request filed during the oral proceedings before the board. At the end of the oral proceedings, the Chair announced the board's decision.
- IX. Claim 1 of the main and sole request submitted at the oral proceedings before the board reads as follows:
"A method of validating a correct operation of a HMI (71), i.e. a human machine interface, located in a driver control arrangement for controlling the operation of the rail vehicle in a rail vehicle, the method comprising the following steps:
(a) receiving input data comprising information about the velocity of the rail vehicle to be indicated by the HMI (71) and supplying the input data to a first processor (69) of the HMI (71), and
(b) processing (73) the input data using the first processor (69) according to a first predetermined

procedure for producing indication data which define the way an indication device of the HMI (71) has to indicate the information about the velocity of the rail vehicle,

- (c) modifying (84) the indication data and obtaining - in a validation mode while a corresponding modification function is enabled - modified indication data to allow for validation of the correct operation of the HMI (71),
- (d) inputting the input data to a second processor (70) and inputting - in the validation mode - the modified indication data to the second processor (70),
- (e) processing (76) in the validation mode the modified indication data according to a second predetermined procedure for checking if the modified indication data are equivalent to the information about the velocity of the rail vehicle to be indicated by the HMI (71) according to the input data received at the data input and outputting a corresponding check result,
- (f) deciding (77) in the validation mode that the validation was successful if the check result of step e) means that the modified indication data is not equivalent to the information about the velocity of the rail vehicle to be indicated and triggering a predetermined fall-back procedure if the validation was not successful,

wherein the first predetermined procedure and the second predetermined procedure are exactly the same predetermined procedures in the validation mode as being performed during normal operation of the HMI (71), when the indication data are not modified."

- X. Dependent claim 2 reads as follows:
"The method of claim 1, wherein, during normal operation, a further validation procedure is performed by performing steps a), b), wherein non-modified indication data obtained in step b) are input to the second processor (70) and the non-modified indication data are checked instead of the modified indication data, and by deciding that the validation was successful if the check result means that the indication data is equivalent to the information about the velocity of the rail vehicle to be indicated."
- XI. Dependent claim 3 reads as follows:
"The method of claim 1 or 2, wherein steps a) to f) of claim 1 are repeated and wherein the indication data are modified in step c) in a different manner."
- XII. Dependent claim 4 reads as follows:
"The method of one of claims 1 to 3, wherein step c) is performed using the first processor (69)."
- XIII. Independent claim 5 reads as follows (itemisation by the board):
"A rail vehicle comprising a HMI (71), i.e. a human machine interface, located in a driver control arrangement for controlling the operation of the rail vehicle, wherein the HMI (71) comprises a display as an indication device (9) and wherein the HMI (71) comprises the following:
(A) a data input (68) for receiving input data comprising information about the velocity of the rail vehicle to be indicated by the HMI (71),
(B) the indication device (9) being adapted to indicate the information to a human,
(C) a first processor (69) which is connected to the data input (68) for receiving the input data,

- (D) a first program (73) implementing a first predetermined procedure for producing indication data which define the way an indication device of the HMI (71) has to indicate the information about the velocity of the rail vehicle, wherein the first processor (69) is adapted to perform the first program (73),
- (E) a modification device (84) adapted to modify the indication data for obtaining modified indication data, thereby implementing a modification function, to allow for validation of the correct operation of the HMI (71), wherein the modification function is disabled during normal operation, but is enabled in a validation mode of the HMI (71),
- (F) a second processor (70), which is also connected to the data input (68) for receiving the input data and which is connected to an output of the first processor (69), for receiving the modified indication data in the validation mode, or to an output of the modification device (84), for receiving the modified indication data in the validation mode,
- (G) a second program (76) implementing a second predetermined procedure for checking in the validation mode if the modified indication data is equivalent to the information about the velocity of the rail vehicle to be indicated by the HMI (71) according to the input data received at the data input and for outputting a corresponding check result, wherein the second processor (70) is adapted to perform the second program (76),
- (H) a decision device (77) adapted to decide in the validation mode that the validation was successful if the check result means that the

modified indication data is not equivalent to the information about the velocity of the rail vehicle to be indicated and adapted to trigger a predetermined fall-back procedure if the validation was not successful,

(I) wherein the first predetermined procedure and the second predetermined procedure are exactly the same predetermined procedures in the validation mode as being performed during normal operation of the HMI (71), when the indication data are not modified."

XIV. Dependent claim 6 reads as follows:

"The rail vehicle of claim 5, wherein the HMI (71) - during normal operation - is adapted to perform a further validation procedure by performing the second program (76) using the second processor (70) in a manner in which the non-modified indication data produced by the first program (73) and optionally by a third predetermined procedure are checked - instead of the modified indication data - for being equivalent to the information about the velocity of the rail vehicle to be indicated by the HMI (71) and in which the decision device (77) decides that the validation was successful if the check result means that the indication data is equivalent to the information about the velocity of the rail vehicle to be indicated."

XV. Dependent claim 7 reads as follows:

"The rail vehicle of claim 5 or 6, wherein the modification device (84) is adapted to modify the indication data in a different manner during repeated validation of the HMI (71)."

XVI. Dependent claim 8 reads as follows:

"The rail vehicle of one of claims 5 to 7, wherein the modification device (84) is part of or implemented by the first processor (69)."

Reasons for the Decision

The application

1. Human machine interfaces (HMIs) are often used to display "safety related information" of, for example, rail vehicles (such as the velocity of the rail vehicle or the braking power of the braking system). If the displayed information is wrong or incomplete, or if the information is not displayed in a manner which can immediately be recognised by the driver, the safety of operation is not guaranteed (description as originally filed, page 1, second text paragraph).
2. In the invention, a main (first) data processor produces indication data. The indication data can either be indicated directly by the indication device without further data processing (e.g. the indication data is a two-dimensional image to be displayed), or there is a (third) procedure (corresponding to a "visualization" function 74) which processes the indication data to obtain data which can be indicated directly by the indication device (e.g. the indication data defines the angle and/or the position of a graphical element, such as an arrow, which corresponds to a measurement value to be indicated, for example a velocity of a rail vehicle) (page 5, last paragraph, to page 6, first two lines).
3. The first data processor may fail for different reasons. The result is a set of indication data which

does not correspond to the information to be displayed as received by the HMI. Therefore, a second processor (the "safety" processor) may be provided to check if the indication data produced by the first processor is equivalent to the information to be indicated by the HMI. It may calculate a characteristic value from the indication data or a part of it, for example a cyclic redundancy check (CRC) value, and compare it with an expected value which corresponds to the information to be displayed by the HMI. If the check result is negative, i.e. there is a difference, a fall-back procedure is immediately triggered, for example the HMI is re-started or the screen is set blank (page 1, last full paragraph; page 6, second full paragraph; page 10, lines 9 to 12).

4. In the invention as defined by independent claims 1 and 5, an additional modification function 84 used "for validation of the correct operation of the HMI" acts on the indication data produced by the first processor. During normal operation, this additional modification function is disabled (page 2, last two lines of the last full paragraph).
5. During validation mode, the data received and processed by the second (safety) processor may be modified or non-modified indication data. When the visualisation function 74 receives the modified indication data, its output to the second (safety) processor 70 should not correspond to the information to be displayed. A checking function 76 should detect this difference and output a corresponding check result to an evaluation device 77. Therefore, if the checking function 76 does not output a check result that there is a difference, evaluation device 77 decides that the validation has failed (page 2, last full paragraph to page 3, point g;

page 10, first full paragraph and last paragraph; Figures 3 and 4).

6. The board finds it more appropriate, in particular for the purpose of comparison with the apparatuses of documents D2 and D1 in the inventive-step assessment, to discuss apparatus claim 5 first.
7. The board refers to the itemisation of independent claim 5 of the main request as shown in point XIII. above.
8. *Basis of the amendments to the claims*
 - 8.1 Claim 5 is based on claims 5 and 6 as originally filed in combination with claims 10 and 11 as originally filed; the paragraph bridging pages 2 and 3 of the description as originally filed (for the validation mode), and page 10, lines 9 to 12 (for the fall-back procedure).
Similar amendments have been made to claim 1, which is mainly based on claim 1 as originally filed.
 - 8.2 Claims 2 to 4 and 6 to 8 are based on claims 2 to 4 and 7 to 9 as originally filed.
 - 8.3 Moreover, claim 5 has been amended to specify that the second processor (70) is connected, for receiving the modified indication data in the validation mode, to an output of the first processor (69) (thus after the visualisation function (74) of Figures 3 and 4, see also point 2. above) or to an output of the modification device (84). This feature covers the alternatives disclosed on page 10, penultimate paragraph, of the description as originally filed.

8.4 The board is thus satisfied that the requirements of Article 123(2) EPC are complied with.

9. *Clarity objections - Article 84 EPC*

9.1 The clarity objections raised in the board's communication have been overcome by the following amendments:

- A decision device (77) has been added to the rail vehicle of claim 5 (feature (H); see objection raised in the board's communication, points 13 and 17)
- The expression "has to indicate the information" has been consistently used in claims 1 and 5 (feature (D); see objection raised in the board's communication, point 14).
- Feature (E) has been further clarified to overcome the board's objection in point 15 of the board's communication.
- It has been specified that the second processor (70) is connected, in the validation mode, to an output of the first processor (69) or to an output of the modification device (84) (feature (F); see objection raised in the board's communication, points 16, 16.1 and 16.2).
- The "enabling and disabling" of the modification function has been defined together with the addition of a validation mode additionally to the normal mode (feature (E); see objection raised in the board's communication, points 18 and 18.1).

10. *Article 83 EPC objections*

10.1 The board's objection under Article 83 EPC no longer applies since the claim has been amended to refer in both features (A) and (G) to the "information about the velocity of the rail vehicle". The board agrees with

the appellant's argument in its letter dated 16 June 2021, on page 7, that the requirements of Article 83 EPC are satisfied, i.e. that a skilled person would be able to implement the invention, in particular to obtain the "information about the velocity of the rail vehicle to be indicated by the HMI" from the input data (see objection raised in the board's communication, points 17.1 and 17.1.1).

11. *Inventive step*

- 11.1 **Document D2** was considered the closest prior art by the examining division. It discloses a display system 10 for use in an aircraft by a pilot which includes a display screen 12 to graphically depict images such as pointers and other indicators, simulated flight instruments and gauges, maps, terrain simulations, alphanumeric characters, etc. (paragraphs [0003], [0005] and [0021]; Figure 1). In the display system 10, a dedicated symbol generator or controller 16 generates and outputs calculated imaging data used to illuminate the appropriate pixels in the display screen 12 and thus create the intended images on that display. The imaging data is derived or calculated by the controller 16 from sensor measurements and other input data obtained from a plurality of aircraft and environmental sensors or other aircraft systems disposed about and throughout the aircraft for ascertaining or "reading" the current values of often dynamically-varying flight control, telemetry, atmospheric, positional, and other aircraft and environmental condition information (paragraph [0021]; Figure 1; paragraph [0023] in conjunction with Figure 2).

Thus, document D2 appears to disclose the preamble and features (A) to (D) of claim 5, except that the vehicle is an aircraft instead of a rail vehicle.

11.2 A comparator processor 32 receives from I/O processor 30 the same sensor inputs and data as rendering computer 34. Instead of generating the data necessary for imaging on display 12 all the fully anti-aliased, alphanumerically and graphically-presented information upon which the flight crew is intended to rely in operating the aircraft, as is required of rendering computer 34, the comparator processor 32 generates the display data for only a limited number - between about 100 and 300 - of specific "points of light" (data points) which are used as test or integrity check points for verifying the accuracy of the display data generated by rendering computer 34 (paragraph [0030]).

If at least the two MSBs (most significant bits) of each of the three RGB (red, green and blue) colour data bytes generated by each of the rendering computer and the comparator processor for a given screen display pixel location are determined to be the same, the rendering computer imaging data for that pixel location is deemed reliable. If the colour data comparison effected by the colour comparator for a particular screen display pixel location determines that the rendering computer and point of light data are not the same or are not otherwise within predetermined acceptable parameters of difference that define a successful comparison, a comparison failure or error signal is generated and provided to the microprocessor interface of comparator processor 32 (paragraphs [0034], [0035], [0039]; Figure 6).

D2 also discloses that, either as a matter of design or operator choice, detection of an error or failure of any subset of the data generated by one of the rendering computers 34 may result in replacement of the entire display field image previously supplied with data from the error-producing rendering computer with the imaging data generated by another rendering computer 34 (paragraph [0040]); this corresponds to the "predetermined fall-back procedure" in feature (H) of claim 5.

The comparison is used to verify that the rendering computer is providing correct, accurate and trustworthy display data upon which the flight crew can confidently rely in their operation of the aircraft (paragraph [0044]).

Consequently, D2 discloses an aircraft flight information graphical display system operationally divided into two basic functional parts: one (the rendering computer) responsible for display availability or reliability, and the other (the comparator processor) which provides or assures display integrity (paragraph [0046]).

The comparator processor of Figure 2 corresponds to the second processor performing the second program implementing the second predetermined procedure as defined by features (G) and (I) with the exception that the first and second procedures of document D1 are not exactly the same since the first procedure implements anti-aliasing, which the second procedure does not (paragraphs [0030] and [0044]). The "indication data" of claim 5 corresponds to the values of the correspondingly-located screen pixels as generated by

the rendering computer for output to the imaging device (paragraph [0044]).

Thus, D2 also discloses part of features (F), (G) and (H).

However, document D2 does not disclose the following distinguishing features of **claim 5**:

(DF1) the vehicle is a rail vehicle

(DF2) there is, in addition to a "normal" operation mode like in D2, a "validation" mode

(DF3) the HMI comprises a modification device (84) adapted to modify the indication data for obtaining modified indication data, thus implementing a modification function, to allow for validation of the correct operation of the HMI, with the modification function disabled during normal operation but enabled in a validation mode of the HMI (71) (corresponding to feature (E));

(DF4) the validation is considered successful if the check result means that the modified indication data is not equivalent to the information about the velocity of the rail vehicle to be indicated

(DF5) the first and second procedures are exactly the same

(DF6) the second processor receives the modified indication data in the validation mode

11.3 The distinguishing features, especially the modification function and the enabling and disabling of the modification function, allow detecting failures not only of the main processor but also of the safety processor.

11.4 The objective technical problem to be solved was identified by the examining division as being "how to

improve the reliability of the validation" (decision, point 1.4). During the oral proceedings before the board, the appellant formulated the same objective technical problem.

In view of the distinguishing features comprising the presence of a "validation" mode, the board reformulates the objective technical problem as how to improve the reliability of assessing the correct operation of a HMI, in a vehicle, for its implementation in a rail vehicle.

- 11.5 The board is not convinced that the distinguishing features are obvious or common general knowledge or that the skilled person would add such features to document D2 without any prompt from another prior-art document.
- 11.6 The board notes that document **D1** discloses an integrated electronic module with at least two similar core circuits, operating in synchronous mode, and a comparator device. The signals of corresponding outputs of the core circuits are fed for mutual comparison to the comparator device which outputs an error signal in the event of a poor match of these signals. The injection of at least one hardware fault at an input of the comparator is controllable. It aims at locating the faulty component in the event of a deviation of the double core circuits from each other (column 1, lines 3 to 11; column 3, lines 7 to 19).

The integrated electronic component of D1 comprises input pins for receiving input data and a first processor (core circuit KK0) connected to the input pins for receiving the input data. A first program performed by the first processor implements a first

predetermined procedure for producing output data ("ou0-1" to "ou0-n") (column 4, lines 20 to 31; sole figure). It comprises a modification device (element "FIN") adapted to modify the output data ("ou0-n") for the purpose of validating the correct operation of the core circuits (column 4, line 68 to column 5, line 7; figure).

The second core circuit (KK1) also receives the input data. A circuit for checking the outputs (OCS) receives the modified output data (column 4, lines 23 to 25; column 5, lines 37 to 54; figure). The checking circuit checks if the modified output data and the output data of the second core circuit are equivalent and outputs a check result (VGS) (column 5, line 50 to column 6, line 3; figure).

In D1, the core circuits are similar and operated in synchronous mode, and the introduction of hardware errors is controllable (column 1, lines 3 to 11; column 7, lines 31 to 33).

11.7 The board recognises that in the apparatus of document D1 there is a normal mode of operation, during which no fault at all is injected, and a validation mode, during which a fault is injected according to a controlled signal (similar to features DF2 and DF3). The first and second core circuits are exactly the same and thus perform exactly the same procedures (corresponding to feature DF5). The modified output is compared with an output of the second core circuit. The second core circuit together with the fault injecting part and the comparator is an entity similar to the second processor of claim 1 (corresponding to feature DF6).

11.8 The appellant has argued that the apparatus of document D1 was not similar to the system of document D2. D1 disclosed an integrated circuit with two identical and synchronously operated core circuits "KK0" and "KK1". These core circuits were identical hardware components in which no software was involved. D1 disclosed very specific error testing by inserting error signals at the level of bits (changing the value of bits). It concluded that the skilled person would not consider implementing, in the system of document D2, an integrated circuit as disclosed by document D1.

11.9 The board concurs with the appellant that the skilled person would not combine document D1 with document D2 for the following reasons.

The system of document D2 should comply with the very strict standards required by the Federal Aviation Administration (FAA) for flight critical airborne equipment to obtain certification of the apparatus and its permitted use on an aircraft (paragraphs [0007] and [0008] of document D2). The comparator processor output data is intentionally insufficient for providing a complete rendered screen display. Instead it is used only as an integrity check on the data produced by the graphics rendering computer. In addition, the comparator calculates only a limited number of data points used in the comparison. Thus, the comparator processor requires far less processing power and fewer executable commands to provide its data processing and comparison functions than does the graphics rendering processor. As a result, FAA certification of the comparator is quicker. Even if rendering engine graphics processors are upgraded, no extensive, if any, subsequent testing and documentation to obtain FAA re-certification is necessary since the associated

comparator processor will generally remain unchanged (paragraph [0010]).

By contrast, the second core component (or double circuit) of document D1 has the purpose of providing redundancy for increasing the security against errors in switching systems or traffic management systems. It is therefore identical to the first core component.

Thus, the skilled person would not consider document D1 to solve the objective technical problem. Even if they did, they would at most implement a fault injection in front of the comparison stage but not use the same circuitry for the comparator processor as for the rendering computer since the aim of the system of document D2 is to reduce the testing and documenting time for obtaining the FAA certification.

11.10 Therefore, independent claim 5, and corresponding independent method claim 1, are inventive over either document D2 or D1, alone or in combination (Article 56 EPC).

11.11 In the board's opinion, the subject-matter of the independent claims is also inventive when taking into account the other cited prior-art documents. The board is thus satisfied that the claims comply with Article 56 EPC.

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 with the order to grant a patent on the basis of claims 1 to 8 of the main request filed during the oral proceedings before the board with the description to be adapted.

The Registrar:

The Chair:



S. Lichtenvort

J. Geschwind

Decision electronically authenticated