Internal distribution code:

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

Datasheet for the decision of 7 November 2024

Case Number: T 1933/21 - 3.5.06

Application Number: 16802131.9

Publication Number: 3532926

IPC: G06F9/445, B60R16/02, G06F21/64

Language of the proceedings: EN

Title of invention:
SOFTWARE UPDATE MECHANISM FOR SAFETY CRITICAL SYSTEMS

Applicant:
Harman Becker Automotive Systems GmbH

Headword:
Software update monitor/HARMAN BECKER

Relevant legal provisions:
EPC Art. 84, 56

Keyword:
Claims - clarity (no)
Inventive step - (no)

Decisions cited:

Catchword:

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

Case Number: T 1933/21 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 7 November 2024

Appellant: (Applicant)	Harman Becker Automotive Systems GmbH Becker-Göring-Strasse 16 76307 Karlsbad (DE)
Representative:	Rummler, Felix Maucher Jenkins Liebigstraße 39 80538 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 16 June 2021 refusing European patent application No. 16802131.9 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	M. Müller
Members:	G. Zucka
	K. Kerber-Zubrzycka

Summary of Facts and Submissions

I. The appeal is against the decision by the examining division, dispatched with reasons on 16 June 2021, to refuse European patent application 16802131.9, on the basis that none of the requests satisfied the requirements of Article 56 EPC in view of the following document:

D1: US 2014/075197 A1.

The following documents were introduced by the board:

D3: Archived Internet article "How to verify your Ubuntu download", version of 21 October 2016, URL: https://web.archive.org/web/20161021141955/https://www.ubuntu.org.cn/download/how-to-verify, retrieved by the board on 10 January 2024;

D4: Wikipedia article "File verification", version of 11 October 2016 at 04:08, URL: https://en.wikipedia.org/w/index.php?title=File_verification&oldid=743764901, retrieved by the board on 9 January 2024.

II. A notice of appeal was received on 23 August 2021, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 22 October 2021.

III. The appellant requested that the decision of the examining division to refuse the application be set aside and a patent be granted on the basis of the claims of the main request that was the object of the refusal, or of auxiliary request 1 or 2 filed with the statement of grounds of appeal, or of auxiliary

requests 1 or 2 that were the object of the refusal, now renumbered as auxiliary requests 3 and 4 (the claims according to the main request and earlier auxiliary requests 1 and 2 having been filed on 21 April 2021).

The appellant made a conditional request for oral proceedings.

IV. The further text on file is:

description pages
1 and 3 to 15 as published,
2 and 2a received on 17 December 2019;

drawing sheets
1 and 2 as published.

V. The board issued a summons to oral proceedings. In an annex to the summons, the board set out its preliminary opinion, according to which the appealed decision should be upheld.

VI. The appellant did not respond in substance to the board's preliminary opinion, but withdrew its request for oral proceedings, which were subsequently cancelled.

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

"A software update monitor (102) configured to:
receive, via a first communication channel (118), from a software update component (106), a software update (110, 111);
write the software update (110, 111) into a target memory location (160);

determine a first verification code (122) based on the received software update (110, 111);

receive, via a second communication channel (114) independent from the first communication channel (118), from an update server (104), a second verification code (120) associated with the software update (110, 111);

determine if the first (122) and second (120) verification codes match; and

apply the software update (110, 111) if the first (122) and second (120) verification codes match."

VIII. Compared to the main request, claim 1 of auxiliary request 1 specifies that the target memory location is that of a memory of a control unit connected to the software update monitor.

IX. Compared to the main request, claim 1 of auxiliary request 2 specifies that the second communication channel is independent from a connection of the software update monitor with the software update component.

X. Compared to the main request, claim 1 of auxiliary request 3 specifies that the software update was sent from the update server to the software update component and processed by that component.

XI. Compared to the main request, claim 1 of auxiliary request 4 specifies that the target memory location is in a memory of a control unit, the software update is applied at that control unit, and the software update monitor applies the software update by enabling switching from a previous memory location in a memory of the control unit to the target memory location if the first and second verification codes match.

XII. The wording of the other claims of the main and auxiliary requests is not relevant for the present decision.

Reasons for the Decision

1. *The invention*

The application is in the field of software updating mechanisms for safety critical systems, e.g. in the automotive and aviation industry (description page 1).

The aim of the application is to obtain a secure software update mechanism for such a system (page 2, third paragraph).

To this end, a first verification code is determined on the basis of a software update received via a first communication channel and is compared with a second verification code received via a second, independent communication channel. The software update is applied if the first and second verification codes match (claim 1).

2. *Clarity; Article 84 EPC*

In claim 1 of all requests it is not clear (Article 84 EPC) what is the nature of the claimed "software update monitor", i.e. whether it is a device or (part of) a program, or maybe something else.

3. *Claim 1 of the main request - inventive step Article 56 EPC*

3.1 The reasons for the appealed decision make reference to D1 as closest prior art document. As described mostly in par. [0024], this document discloses a method for validating a content (e.g. software) file to be installed on a vehicle electronic control unit (ECU). A programming tool 68 provides the content file 44 and a digital signature 46 of the content file to the ECU. The digital signature 46 is used to produce a decrypted hash value 78. A hash value 84 is calculated for the content file 44. The decrypted hash value 78 and the calculated hash value 84 are compared. If they match, the content file is considered to be valid and it is installed in the ECU.

3.2 The board agrees with the appellant (statement of grounds of appeal, page 6, first two full paragraphs) that, according to D1, the manufacturing database 56 or the service database 62 provide both the content file 44 and the digital signature 46, i.e. these are not provided via independent communication channels (see paragraph [0022]), and there is no apparent reason why the skilled person would want to adapt the system of D1 in such a way that the manufacturing database only provides the content file and the service database only provides the digital signature to the programming tool.

The board can therefore not follow the reasoning in the appealed decision (point 2.5) in this respect.

3.3 It can nonetheless be observed that the use of two independent communication channels, provided the channel for the (second) verification code is a secure

channel, provides the advantage that no digital signature needs to be generated, a cryptographic hash sum being sufficient, and that such a measure is as such well known (see D4, section "authenticity verification", second paragraph).

3.4 The board however considers that D3 is an appropriate starting point for a more straightforward inventive step analysis.

3.5 D3 discloses a procedure for installing/updating software (see introductory section: the software is an installable ISO image of Ubuntu Linux; the board notes that the installation would according to standard terminology be called an "update" if the installable version is newer than the one existing on the user's computer, and hence such a newer version is considered an "update" within the meaning of the claim).

3.6 The user receives, via a first communication channel, from a software update component, a software update (see title "Ubuntu download": the term "download" implies that the update is received via a download channel, i.e. a "first communication channel", from some download source which can be called a "software update component").

3.7 The software update is written into a target memory location (implied by the fact that the ISO image is downloaded, which necessarily means that it is written to some form of memory of the computer, e.g. a hard disk or RAM).

3.8 The user determines a first verification code based on the received software update (section 4, first

paragraph: the user generates an SHA256 checksum for the downloaded ISO image).

3.9 The user receives from an update server (section 1: "from any of the mirrors") a second verification code (viz. the file SHA256SUMS) associated with the software update.

3.10 The user determines if the first and second verification codes match (section 4: the SHA256 checksum for the downloaded ISO image is compared to the one in the SHA256SUMS file).

3.11 The software update is applied if the first and second verification codes match (introductory section, last sentence: after verification, Ubuntu can be installed).

3.12 D3 leaves open whether the user downloads the second verification code from a second communication channel that is independent from the first communication channel. According to section 1, the SHA256SUMS file is downloaded "from any of the mirrors", which means that the second communication channel might in principle happen to be the same as the first one, i.e. not be independent from it.

3.13 However, a skilled person who wishes to avoid the need of verifying signatures, as is done in sections 2 and 3 in D3, would look for an alternative procedure which avoids this need.

3.14 Document D4 (section "Authenticity verification", second paragraph) shows that it is well known that there is no need to use digital signatures if the cryptographic hash sums are communicated over a secure channel. It is obvious that D4 assumes this secure

channel to be a second channel independent from the first channel, because it assumes that data transmitted over the secure channel cannot be tampered with, and the fact that the authenticity of the software needs to be verified implies that it was delivered over a channel that is less secure.

3.15 Although the nature of the "software update monitor" of claim 1 is not clear (see above), it is assumed that it is intended to comprise some kind of automated construction.

The mere automation of a human activity is however not considered a sign of an inventive step (established case law of the boards, see CLB I.D.9.21.6).

3.16 The skilled person would thus arrive at the subject-matter of claim 1 without showing any inventive activity in the process.

As a consequence, the board holds that claim 1 of the main request does not satisfy the requirements of Article 56 EPC.

4. *Other requests*

4.1 Claim 1 of auxiliary request 1 specifies that the target memory location is that of a memory of a control unit connected to the software update monitor. This is however disclosed by D3, given that the computer of D3 can be considered to be a control unit, and the target memory location in D3 is a memory of the computer (see 3.7 above).

4.2 As regards the feature added in claim 1 of auxiliary request 2, viz. that the second communication channel

is independent from a connection of the software update monitor with the software update component, this would be a result of the skilled person's thinking process described under 3.14 above. It therefore does not render the claim's subject-matter inventive.

4.3 The same can be said for claim 1 of auxiliary request 3.

4.4 The features added in claim 1 of auxiliary request 4 do not render its subject-matter inventive for the reasons already given above.

4.5 As a consequence, the board concludes that none of the requests satisfy the requirements of Article 56 EPC.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

L. Stridde M. Müller

Decision electronically authenticated