This document includes some recent decisions of the EPO in 2013 with regards to software related inventions and shows relevant extracts from the respective decisions.

T 0862/10 (Notification system/MICROSOFT) of 15.5.2013
Positioning and rendering notification heralds based on user's focus of attention and activity

Inventive step (main request) - no
Inventive step (auxiliary request 1) - yes

Applicant name: MICROSOFT CORPORATION
Application number: 04755824.2
IPC Class: G06F 9/46

Cited decisions: T 1143/06, T 1471/08, T 0643/00

Board: 3.5.06

http://www.epo.org/law-practice/case-law-appeals/pdf/t100862eu1.pdf

The choice of where to put an object on a computer display depending on a value assigned to that object (its "urgency") cannot be considered to have a further technical effect. Furthermore, the movement of the object on the display in response to a change of said value is also considered not to have a further technical effect (see Reasons 3.3.1).

The independent claim of the main request reads as follows:

A notification system, comprising:

an information display object that presents summarized notifications; and

an information controller that receives attentional inputs associated with a user to dynamically generate the information display object on one or more display screens in order to facilitate user processing of the summarized notifications;

wherein the information controller is configured to control positioning of the information display object by dynamically moving the display object closer to the user's focus of visual attention if a notification is determined to be urgent, and

wherein the user's focus of visual attention is determined by at least one of determining the current cursor position, determining the place of an active cursor, using at least one head or

gaze tracking component, using an attention model and determining the user's activity or other input about focus of visual attention including gaze and pose information.

The closest prior art discloses a notification system, comprising an information display object that presents summarised notifications and an information controller that receives attentional inputs associated with a user to dynamically generate the information display object on one or more display screens in order to facilitate user processing of the summarised notifications.

The distinguishing features of the invention are considered:

(1) The information controller is configured to control positioning of the information display object by dynamically moving the display object closer to the user's focus of visual attention if a notification is determined to be urgent.

(2) The user's focus of visual attention is determined by at least one of determining the current cursor position, determining the place of an active cursor, using at least one head or gaze tracking component, using an attention model and determining the user's activity or other input about focus of visual attention including gaze and pose information.

Looking first at the distinguishing feature (1), it is noted that it is largely similar to what was recognised in the appealed decision as distinguishing the subject-matter of claim 1 of the refused main request from the disclosure of the prior art. In the appealed decision (see Reasons 13.4), that feature was simply dismissed as non-technical and it was therefore concluded that there was no inventive step. The board however considers that feature (1) needs to be analysed in more detail. The display of an object near the centre of visual attention of a user (within the "foveal vision"), so that it is more-or-less guaranteed to be seen immediately, or its display simply within the visual field of the user, so that it can be seen, may well be seen as technical effects as compared to arbitrary placement on the screen or on one of a plurality of screens. Thus measures to assess where the user is looking and to place a display object in the light of that assessment do qualify as contributing to a technical effect. However, the board notes that in the case of one screen it is a matter of experience that the whole screen is normally within the field of vision of the user. Further, **displaying a value assigned to an object by means of its relative positioning**, or by moving it on the screen, is clearly a **presentation of information**. Reference is made to T 1143/06, as well as to T 1741/08, from this board in a different composition, which discusses the case law in this area, including the case cited by the appellant in the grounds of appeal, T 0643/00. The particular effects of the claimed invention put forward by the appellant, **"minimising information overload and distraction", cannot be considered technical in nature** according to the case law, being determined by psychological factors and typical to the question of how to present information in a particular context. Overall the board judges that **determining (or attempting to determine) a user's visual focus of attention as a point on a screen and displaying objects in positions relative to that point can be considered to have a technical effect, but that the particular choice of where to display an object dependent on a value assigned to that object (its "urgency") cannot be**. Thus for the question of inventive step the critical question is whether it would be obvious for the skilled person to adapt the notification system of the prior art to take account of the visual focus of attention of the user when placing a notification on the screen.

The prior art choice of when and how to display messages is based on their priority and on the state of the user and may use a different size and either a central or a peripheral location on a screen for a document or alerting window. The present main request claim was not seen as being inventive in view of the prior art. For the inventive auxiliary request please refer to the full decision.

T 0042/10 (Determining relative skills/MICROSOFT) of 28.2.2013
Determining relative skills of players

Inventive step - (no)

Applicant name: Microsoft Corporation
Application number: 06270014.1
IPC Class: G06Q 10/00
Cited decisions: T 1173/97, T 0619/02, T 0717/05, T 1281/10
Citing decisions: T 1281/10

Board: 3.5.01

http://www.epo.org/law-practice/case-law-appeals/pdf/t100042eu1.pdf

The invention addressed controlling an online gaming system so as to keep players interested. It did that by tracking their performance so that suitable opponents could be found.

Claim 1 according to the main request reads as follows:

A computer-implemented method of determining an indication of the relative skill of at least a first player and a second player of a game based on the outcome of one or more such games involving those players said method comprising the steps of:

(i) arranging a processor to, for each player, set statistics describing a probability distribution associated with skill of that player to default values;

(ii) at the processor receiving information about the outcome of one of the games;

(iii) arranging the processor to form and store a factor graph comprising variable nodes and factor nodes, the factor nodes having associated calculation rules, said graph being formed using the received information about the outcome, and arranging the processor to instantiate at least some of the variable nodes with the statistics; and arranging the processor to form and store the factor graph such that it comprises a plurality of first groups of nodes, each first group being associated with a particular player and comprising nodes linked in series; and

(iv) arranging the processor to update the statistics associated with each player by applying message passing to the factor graph using the calculation rules;

(v) arranging the processor to repeat the process of updating the statistics as further game outcomes are received

The basic idea in tracking performance is to represent performance not simply as a score, but as a probability distribution. In practice, Gaussian distributions are used, each represented by its mean and variance. Intuitively, a player with a high mean tends to perform well; a player with high variance will have a large spread of results about the mean, while a player with low variance consistently gets results close to the mean.

The tracking of performance can be applied to teams, as well as to individual players.

As games are played, results are collected and the distributions that represent the players' performances are updated. When the distributions are Gaussian and represented by their means and variances, a straightforward set of update equations results. However, the computational complexity increases as the cube of the number of teams.

The invention deals with that rise in complexity by using "factor graphs". A factor graph performs calculations by passing messages between nodes. Those variable nodes that form the input to an operation pass their values to the operation node. Operation nodes pass their results to output nodes.

The main request defines a method that, based on outcomes of games, calculates indications of the skills of the players, by passing messages between nodes of a factor graph. It is necessary to determine in how far the features of the claim have technical character and so could contribute to inventive step.

The board notes that T 619/02 does **not** say that **all methods of measuring are technical**. It must therefore be assessed whether the measurement can be accepted as technical in the present case.

The term "measurement" is rather broad. It encompasses finding the spectrum of the hydrogen atom, or the salinity of sea water; but also whether one political party is more or less popular than another. In T 619/02, the measurement was of reactions to odours, and it was found to be non-technical. The appellant seeks to distinguish the present case, arguing that the reasons for rejecting the method in T 619/02 do not apply to the present case, because there are no psychological assessments involved.

In the Board's view, the lack of psychological assessments cannot, alone, be determinative. What is needed is a technical problem and a technical solution to it, i.e. a technical effect. However, **judging the skill of a game player does not seem to involve a physical change at all, still less a technical effect**.

The Board, therefore, sees clear reasons for **considering the measurement of performance in games as non-technical**.

The appellant's second argument is based on paragraph 5.9 of T 717/05, in which it is stated that "amusement is the psychological purpose of a gaming apparatus and is the relevant objective technical problem to the extent that the enhanced amusement is achieved by technical features of the claim."

In T 717/05, the deciding Board did indeed hold that the **step of monitoring outcomes of games** was a **technical feature,** but **only in combination with the step of displaying** them (paragraph 5.6 with paragraph 4.5). The displaying step was necessary, since it permitted the player to be informed about the development of the game, thus addressing the problem of maintaining interest (paragraph 5.1). The **present claim**, however, does **not** require the players' scores to be **displayed**, but **only** to be **calculated**. For this reason alone, T 717/05 does not appear to be relevant. A more basic reason is that the ***Board has strong doubts that amusement, even if achieved by technical (in particular, computing and displaying) means, really is a technical problem***. If it were, any dull computer game could be regarded a posing a technical problem that could be solved by any less dull game. The difficulties involved in such a view are evident (the skilled person need not be skilled in a technical art; the effect would be subjective), and the decision has been largely ignored in the jurisprudence of the Boards of Appeal. T 528/07, Portal system/ACCENTURE, not published in the OJ EPO, expressly declined to follow the approach taken in T 717/05.

The appellant's third argument is that **factor graphs**, and the associated message passing algorithm, are technical. They address the **technical problem of speeding up computation**.

In its full generality, **speed of computation is a mathematical problem**. It may be the case that a computer has a particular processor that is particularly good, or particularly poor, at some (class of) operations. Recasting a mathematical method so as to take advantage of what the processor does quickly, or to avoid what it does slowly, **might involve technical considerations**. In such a case, the recast method, when performed on that particular processor, might not be "just" mathematical but also be technical. However, **not all recasting of mathematical methods in order to increase speed are technical**. In the days when people looked up trigonometric functions in tables, recasting a method so as to reduce the number of times the tables had to be consulted might speed up computation, but nothing technical was happening.

The **Board's view regarding technicality can be summarized** as follows.
The overall aim of **keeping players interested is not technical**.
The intermediary aim of **assessing and comparing playing performance is not technical**.
The **representation of performance by probability distributions** and the updating of them, are **mathematical methods**.
The **use of factor graphs** with message passing is a m**atter of mathematics or abstract computer science**.

It is not disputed that suitable computer processors were well known at the filing date (10 February 2006). The skilled person would have been aware that they would be able to carry out the mathematical operations involved in forming a factor graph and passing messages between nodes. Indeed, the method involves the collection of data, possibly large amounts of data, and the carrying out of calculations on it. That is just what computer processors were designed to be good at. It **would, then, have been obvious to use** them. The main request, therefore, cannot be allowed because the method defined in claim 1 does not involve an inventive step.

T 0743/11 (Write allocation/NETWORK APPLIANCE) of 12.4.2013
Extension of a system and method for write allocation within a write anywhere file layout file system

Inventive step - (yes)

Applicant name: Network Appliance, Inc.
Application number: 05738175.8
IPC Class: G06F 17/30

Board: 3.5.01

http://www.epo.org/law-practice/case-law-appeals/pdf/t110743eu1.pdf

The invention concerns an extension to the write anywhere file layout (WAFL) system. In that system, a user's data are stored in logical volumes. A logical volume looks, to the user, like a storage disk, but it is not. Underlying the logical volume is a further storage device.

When data are written in a WAFL system, blocks of the data are assigned block numbers in the logical volume. These logical block numbers are associated with block numbers in the underlying storage. Similarly, when data are read, the user looks for the contents of some particular logical blocks, but actually gets the contents of the underlying blocks.

The underlying storage may, for example, be a physical disk, in the sense of a rotating device with magnetic domains that can be put in one or another state so as to represent stored data. It may, however, be anything that presents the logical volume with the same behaviour. So long as the logical volume sees the behaviour it expects, it will happily "store" data for the user. It does not matter whether the underlying storage really is physical in the sense just outlined, although there must ultimately be some physical storage.

One possibility for the underlying storage is a RAID system. In such a system, data are distributed redundantly over several disks. A user's data block would then be "written" to a logical block, which corresponds to a RAID block, which corresponds to a number of copies in possibly different forms at a number of different locations in different disks.

As explained by the appellant, in prior art WAFL implementations, there was a fixed relationship between logical blocks numbers and RAID addresses. Each logical volume would use a fixed part of the RAID system.

The WAFL system uses a buffer tree to keep track of how data are stored. Each data file is associated with an inode, which comprises pointers to the logical blocks at which the data blocks are stored. If the file is big enough, some of the pointers will not point directly to data, but to "indirect blocks", containing further pointers. By following the pointers from an inode, if necessary passing via indirect blocks, the logical blocks in which the data are stored can be found. Via the fixed relationship between logical blocks and RAID addresses, the logical blocks so identified correspond to specific locations in the RAID system.

Main request, clarity

The Board is satisfied that the terminology of WAFL systems was known to, and would have been understood by, the skilled person. Thus, terms such as "inode" do not require definition in the claims.

The meanings of "physical" and of "aggregate" do require some extra comment. The former can be confusing, because it is sometimes used with its everyday meaning, so that "physical disk" would be something one could pick up, and sometimes with a more abstract meaning, as something that presents appropriate behaviour to some higher layer. The Board is satisfied that the skilled person, who is familiar with WAFL storage, would understand the distinction, and that the more abstract meaning is appropriate for something layered on a RAID plex. Once that has been grasped, the skilled person would correspondingly interpret the term "physical volume block number space," and understand that the aggregate is nothing other than an additional virtualization layer, which covers the whole of the underlying RAID plex, which has its own space of block numbers, and which maintains its own block allocation structures, just as the virtual volumes do. The Board, therefore, considers that the claims are clear.

Main request, inventive step

Claim 1 defines a method of write allocation in which two virtualization layers (the aggregate and the virtual volumes) sit on a RAID plex. Each of them has its own space of block addresses and each maintains its own block allocation structure. When a block is allocated in a virtual volume, a parent block (which will be an inode or an indirect block) is updated so as to include the corresponding block number in the aggregate.

The prior art WAFL system, as set out in the application, is the most appropriate starting point for the assessment of inventive step. That prior art system had a single virtualization layer, and, therefore, a single block allocation structure. The pointers in its inodes and indirect blocks were to blocks within the same virtualization layer, and it was the job of the underlying RAID system to translate those blocks numbers to its own representation.

In contrast to that prior art, the **invention** defined in the independent claims **has the aggregate layered on top of the RAID system**. The **virtual volumes now sit inside container files on the aggregate**. In effect, there are, according to the invention, **two layers of virtualization.** That **allows a more flexible use of the underlying RAID system by the virtual volumes.**

Such a two-layer structure is not part of the prior art WAFL system. Nor do any of the documents cited in the decision under appeal disclose one. In this respect, it is significant to note that the underlying RAID system cannot itself be regarded as a virtualization layer in the way the aggregate is. That is because the RAID system does not concern itself with block allocation structures. That is the job of the file system that makes use of the RAID system.

The **simple addition of a new layer of virtualization would not involve an inventive step**, because successive virtualization has been an important factor in the development of storage devices. Nor, once the decision to add a new virtualization layer has been taken, would the use of the same sort of block allocation structures as those already used be anything more than an obvious choice. **However, the invention does more than add a virtualization layer using the same sort of allocation structures as are already in use**. During write allocation,

it puts (cross-layer) pointers to aggregate allocation structures in the inodes and indirect blocks of the virtual volumes. As a result, when the data are later read, there is no need to convert from the block structures of the virtual volume to the underlying block structures of the aggregate. The **saving during reading is at the cost of more processing during writing**, and of some storage capacity. That is part of the sort of **trade-off that an engineer routinely makes**, but the Board does **not** consider that **every manifestation of a trade-off is obvious simply because the factors traded off are known**. In the present case, **while it would have been obvious to the skilled person to trade off ease of reading against ease of writing and cost in storage, there is nothing to suggest that she would have considered using cross-layer pointers in doing so. None of the prior art suggests cross-layer pointers at all.**

The Board concludes that the subject matters defined in claims 1 and 10 according to the main request do involve an inventive step (Article 56 EPC 1793).

T 1674/09 (Updating firmware/HEWLETT PACKARD) of 7.6.2013
A method of updating firmware without affecting initialization information

clarity (yes)
conciseness (yes)
inventive step (yes)

Applicant name: Hewlett-Packard Development Company, L.P.
Application number: 99115489.9
IPC Class: G06F 9/445

Board: 3.5.06

http://www.epo.org/law-practice/case-law-appeals/pdf/t091674eu1.pdf

The invention relates to updating the firmware of a microprocessor-controlled device without the need to do an overall reset of the system containing the device. When a PC is turned on or reset a system initialization process occurs, for example according to the ISA (Industry Standard Architecture) bus standard or the SCSI (Small Computer System Interface) standard, in which the PC CPU discovers and configures all the system peripheral devices so that they can be individually addressed by the CPU. This involves using what is termed in the claims "device-identification information" to assign "logical device numbers" or "SCSI addresses", collectively termed "configuration information" in the claims, according to the ISA and SCSI standards, respectively. The invention avoids the need for such a system reset when a firmware update is made to a device which may affect the initialization process. To do this, status and configuration information and information which may change during a firmware update are stored in a memory area unaffected by the firmware update. The description sets out two embodiments which differ as to when information is copied to a memory area unaffected by the firmware update. Only the first embodiment, shown in figure 2, is claimed. According to this embodiment, a hard reset or an overall system reset causes device

identification information (step 208) and/or configuration information (step 212) to be saved in a separate portion of memory not subject to change during a firmware update. A subsequent firmware update (step 206) is followed by a "soft reset" (step 204) of the device, but an overall system reset is not required.

The independent claims read as follows:

"1. A method of changing firmware of a device, the method comprising: upon detection of a hard reset or an overall system reset, copying (208) device-identification information which needs to remain unchanged until a next system reset but which may change during a firmware update from a first section of memory that is subject to change during a firmware update to a second section of memory that is not subject to change during a firmware update, and performing (210) a configuration operation using the device-identification information; upon reception of a signal or command to update the firmware, writing new firmware in the first section of memory without changing the second section of memory, wherein the device-identification information changes during the firmware update; after the firmware has been updated, performing (204) a soft reset process comprising tasks involved in a reset process that do not impact the copied information; and using the copied version of the device-identification information during operation, until another hard reset."

"3. A method of changing firmware of a device, the method comprising: upon detection of a hard reset or an overall system reset, performing (210) a configuration operation using a device-identification information, which may change during a firmware update, to obtain configuration information, and saving (212) the configuration information in a second section of memory that is not subject to change during a firmware update; upon reception of a signal or command to update the firmware, changing (206) the firmware in the first section of memory without changing the second section of memory, wherein the device-identification information changes during the firmware update; and after the firmware has been updated, performing (204) a soft reset process comprising tasks involved in a reset process that do not impact the saved information."

The prior art

online documentation relating to developing applications for the "Palm OS" operating system which runs on a "Palm OS" device, for instance a personal digital assistant (PDA)

- concerning system and user interface management (closest prior art)
- concerning memory and communications management

Inventive step

Claim 1 differs from the closest prior art inter alia in the following feature:

a. upon detection of a hard reset or an overall system reset, copying device-identification information which needs to remain unchanged until a next system reset but which may change during a firmware update from a first section of memory that is subject to change during a firmware update to a second section of memory that is not subject to change during a firmware update.

In addition, and contrary to the decision, the subject-matter of claim 1 further differs in the following features:

b. performing a configuration operation using device-identification information;

c. upon reception of a signal or command to update the firmware, writing new firmware in the first section of memory without changing the second section of memory, wherein the device-identification information changes during the firmware update;

d. upon reception of a signal or command to update the firmware, writing new firmware in the first section of memory without changing the second section of memory, wherein the device-identification information changes during the firmware update;

e. the soft reset comprises tasks involved in a reset process that do not impact the copied information and

f. using the copied version of the device-identification information during operation, until another hard reset.

The subject-matter of claim 3 differs from the closest prior art in the following features:

a. upon detection of a hard reset or an overall system reset, performing a configuration operation using a device-identification information, which may change during a firmware update, to obtain configuration information;

b. saving the configuration information in a second section of memory that is not subject to change during a firmware update;

c. upon reception of a signal or command to update the firmware, changing the firmware in the first section of memory without changing the second section of memory, wherein the device-identification information changes during the firmware update and

d. the soft reset comprising tasks involved in a reset process that do not impact the saved information.

According to the appealed decision, the difference features over the closest prior art had no technical effect. The board finds that the **difference features** set out above **solve the technical problems** (see difference feature "b" in claim 1 and difference feature "a" in claim 3) **of building a co-operating system from initially uncoordinated peripheral devices and** (the remaining difference features) **allowing the system to continue to operate without a hard reset after a device firmware update**. Hence all the difference features have technical character and contribute to inventive step. There is no obvious technical problem or solution which would cause the skilled person starting from the closest prior art to add all the difference features set out above in an obvious manner. In particular, **the copying difference feature** (feature "a" in claim 1 and feature "b" in claim 3) **is contrary to the whole philosophy of the memory management of the Palm OS device**, which is to avoid moving data around in memory, and, instead, to access and update data directly in place. Hence the board finds that the subject-matter of claims 1 and 3 involves an inventive step.

T 1630/09 (Medication delivery system/BAXTER) of 17.1.2013
Medication delivery system

Inventive step (yes - after amendment)

Applicant name: Baxter International Inc.
Application number: 02786891.8
IPC Class: G06F 19/00

Board: 3.5.05

http://www.epo.org/law-practice/case-law-appeals/pdf/t091630eu1.pdf

Claim 1 of the main request is directed towards a medication delivery system which comprises a medication delivery device and a handheld computing device. According to claim 1, the handheld computing device has means for reading medication delivery instructions, prescribed medication data and patient data in a machine readable format and for comparing the prescribed medication data and the patient data to confirm a match between the data. With respect to the medication delivery device, claim 1 specifies that this device has multiple delivery channels and that each delivery channel of the medication delivery device has a label with information to uniquely identify the channel in the machine readable format. Claim 1 further specifies that the handheld computing device is capable of communicating the information read in the machine readable format from the label to the medication delivery device so that the appropriate channel is activated.

Claim 1 of the main request submitted at oral proceedings reads as follows:

"A medication delivery system (20) for communicating and matching prescribed medication data from a first label (28) on a medication container (26) holding the medication (27) and patient data from a second label (29) on a tag (24) adapted to be worn by a patient, the first label also containing instruction on delivering the medication, and the medication data, medication delivery instruction, and patient data are provided in a machine readable format, the medication delivery system comprising:

(a) a medication delivery device (30) which is adapted to deliver the medication from the medication container to the patient said medication delivery device having a data port (38) for receiving information and multiple delivery channels (33); and

(b) a handheld computing device (22) having means (36) for reading the medication delivery instruction, the prescribed medication data and the patient data in the machine readable format and for comparing the prescribed medication data and the patient data to confirm a match between the data, the handheld computing device having a transmitter (32) for transmitting the medication delivery instruction from the handheld computing device to the medical device and wherein the medical device is adapted to deliver the medication to the patient according to the instruction,

wherein each delivery channel (33) of the medication delivery device has a third label (31) with the information to uniquely identify the channel in the machine readable format, the handheld computing device capable of communicating the information read in the machine readable format from the label (31) to the medication delivery device so that the appropriate channel is activated."

Inventive step

The only prior art document cited in the decision under appeal, represents the closest available prior art to the subject-matter of claim 1 of the main request and discloses a medication delivery system which comprises a medication delivery device such as an infusion pump and a so-called "medical transaction carrier" (MTC) that contains information concerning past and present medical transactions. In some embodiments, the MTC is an electronic message and no physical device need be used. In other preferred embodiments, the MTC is a handheld computing device such as a PDA. In the latter embodiments, the handheld computing device is used for storing information and transporting the information from one location in a care-giving facility where medications are prepared for delivery to a patient's bedside. There is, however, no teaching or disclosure to the effect that the handheld computing device is provided with means for reading data in a machine readable format and for performing a comparison to confirm a match between items of read data as recited in claim 1 of the main request. There is no identifiable disclosure or suggestion to the effect that the handheld computing device should be provided with such means for reading data in machine readable format. The disclosure concerning the MTC appears to be limited to downloading medical information from the hospital's information systems to the MTC and exchanging data between the MTC and medication delivery devices or "patient specific assets". In the board's judgement, the **prior art neither discloses nor suggests that, in the embodiments where the MTC is realised in the form of a handheld computing device, this handheld computing device should be adapted to permit the capture of data in machine readable format and to perform verification checks on the read data** as recited in claim 1 of the main request. The prior art also fails to disclose that the medication delivery device has multiple delivery channels each of which has a label in machine readable format and that the handheld computing device is used for communicating information read from such a label to the medication delivery device so that the appropriate channel is activated.

Compared to the system of the prior art, the system of claim 1 of the main request thus provides a **handheld computing device which has additional data capture and verification functionality and which further uses this additional functionality to enable the user of the handheld computing device to interact with a multi-channel medication delivery device so as to selectively activate a specific channel of said medication delivery device**.

The modifications to the prior art disclosure required to arrive at the subject-matter of claim 1 of the main request could arguably have been carried out by the skilled person without undue difficulty. However, the **question of obviousness** has to be decided by considering **what the skilled person would have done**, rather than what he hypothetically could have done.

In the board's judgement, the **skilled person starting from the prior art finds no teaching or suggestion in that document which would have led him to perform the specific modifications required to arrive at the subject-matter of claim 1** of the main request.

Neither can the board identify any apparent reason why the skilled person would have been prompted to attempt these modifications on the basis of his common general knowledge. The board therefore concurs with the appellant's submissions to the effect that starting from the prior art it **would not be possible to arrive at the subject-matter of claim 1 of the main request without the use of hindsight**.

In view of the foregoing, the board concludes that the subject-matter of claim 1 of the main request involves an inventive step.

T 1225/09 (Touchscreen controlling medical equipment from multiple manufacturers … of 23.4.2013

Touchscreen controlling medical equipment from multiple manufacturers

Inventive step - main request (yes)

Applicant name: Storz Endoskop Produktions GmbH
Application number: 06026019.7
IPC Class: G06F 19/00

Board: 3.5.05

http://www.epo.org/law-practice/case-law-appeals/pdf/t091225eu1.pdf

Independent claim 1 according to the main request reads as follows:

"1. Medical communication and control system (10) for controlling remotely controllable surgical devices (16, 18, 20, 22), said system (10) comprising:

a bus (12);

a touchscreen (24, 54) being provided with an interface device (23);

a controller (25, 55) for the touchscreen (24, 54), having a controller command protocol;

a first party device (20, 22), having a first command protocol, said first party device (20, 22) controllable by said touchscreen (24, 54);

characterized by

a third party device (16, 18), having a second command protocol different from said first command protocol, said third party device (16, 18) controllable by said touchscreen (24, 54);

the interface device (23), connected between the touchscreen controller (25, 55) and the bus (12), for converting the controller command protocol to the first and second command

protocols, and for transforming inputs received by the touchscreen (24, 54) into commands for controlling the first and third party devices (16, 18, 20, 22); and

the first party device (20, 22) and the third party device (16, 18) each having an interface (15, 17, 19, 21) adapted to provide compatibility between the bus (12) and each device (16, 18, 20, 22)."

The closest prior art on file discloses a networked medical control system which provides the functionality of remotely controlling a plurality of interconnected medical devices using a touchscreen. Each of the plurality of devices in the networking infrastructure contains a corresponding network interface, an embedded controller for communicating bidirectionally, and is connected to a corresponding local display and user interface.

According to claim 1 each of the plurality of devices with its embedded controller uses a particular protocol.

In the most concrete embodiment in the closest prior art, each networked device in the operating room has an embedded controller that is Jini-compliant and capable of communication using standard Jini communication protocols. It explicitly discloses that "any new technology can be incorporated easily into the system by making the new technology Jini compliant". The teaching of the closest prior art is that all connected devices must have embedded controllers using the same command protocol in order to ensure a proper functionality. It does not disclose the use of "third party devices" as defined in the present application and as claimed in claim 1, since those are specified to have a different command protocol. It does not disclose the specific distributed concept of the protocol conversion with the interface device and separate interfaces of the first and third party devices according to claim 1 with their respective tasks of converting the commands between the controller command protocol and the two different command protocols of the first and third party devices and of providing compatibility between the bus and each device. In the prior art the embedded controller is integrated into each medical device of the plurality of devices. This controller, however, is not provided for compatibility between a bus and each device as according to claim 1, but serves the purpose of making the particular medical device Jini-protocol compliant.

Thus, the last two features of claim 1, i.e.

- a third party device (16, 18), having a second command protocol different from said first command protocol, said third party device (16, 18) controllable by said touchscreen (24, 54); and

- the interface device (23), connected between the touchscreen controller (25, 55) and the bus (12), for converting the controller command protocol to the first and second command protocols, and for transforming inputs received by the touchscreen (24, 54) into commands for controlling the first and third party devices (16, 18, 20, 22); and the first party device (20, 22) and the third party device (16, 18) each having an interface (15, 17, 19, 21) adapted to provide compatibility between the bus (12) and each device (16, 18, 20, 22);

are not considered to be disclosed in the closest prior art.

The **technical effect** achieved by these claimed features is considered to be that the conversion of the command protocols is performed separately from establishing bus compatibility of each medical device. This results in the **advantage** that the centralized configuration of protocol conversion is more flexible and can be better modified in the event that new devices involving a new command protocol are to be integrated for touchscreen control.

The underlying objective **technical problem is therefore considered to be to provide for a flexible integration of devices that have different command protocols**.

The closest prior art does not suggest or give a hint in the direction of the solution according to claim 1.

Instead of integrating existing third party devices with a different command protocol**, it leads away from the claimed solution by teaching the use of a particular, i.e. single, command protocol for all devices** and by making each device compliant with this command protocol. Accordingly, it teaches integrating the embedded controller into each medical device of the plurality of devices. In contrast to the claimed solution, this controller is not adapted to provide compatibility between a bus and each device according to claim 1, but serves the purpose of making the particular medical device compliant with the single command protocol. It therefore does not render the claimed solution obvious.

The claimed solution according to the distinguishing features of claim 1 is neither considered to have been notorious knowledge of the skilled person before the priority date of the present application, nor has the examining division provided any support for the assumption that it would have to be regarded as common general knowledge in the field of controlling medical devices.

The closest prior art therefore does not render the claimed solution obvious when combined with the skilled person's common general knowledge.

A further prior art document discloses an interface that allows multiple surgical devices to be controlled from a central input device. The system has a switching interface which couples the input device to the surgical devices (see figure 1). Because each device may require specifically configured control signals for proper operation, adapters or a controller may be placed intermediate and in electrical communication with a specific output channel and a specific surgical device. Thus, for the skilled person, when looking for a solution to the objective technical problem, the **further prior art would suggest that each device has its own specific adapter/controller for command conversion**. It would hence **lead the skilled person away from providing a central command protocol conversion** for logical compatibility according to the distinguishing features of claim 1. Therefore the combined prior art does not render the claimed solution obvious either.

T 1311/10 (Sicherheitssteuerung/BOSCH REXROTH) of 12.4.2013
Maschinensteuerung mit Sicherheitsfunktion

Erfinderische Tätigkeit (Hauptantrag, Hilfsantrag 3 - verneint)
Klarheit (Hilfsantrag 1 - verneint)

Name des Anmelders: Bosch Rexroth AG
Anmeldenummer: 06707010.2
IPC-Klasse: G05B 19/042, G06F 11/00
Angeführte Entscheidungen: T 0641/00

Kammer: 3.5.03

http://www.epo.org/law-practice/case-law-appeals/pdf/t101311du1.pdf

Anspruch 1 des Hauptantrags lautet:

"Programmierbare Steuerung (1) zur Maschinen- und/oder Anlagenautomatisierung wobei die programmierbare Steuerung (1) eine Standard-Steuerung (20) mit Standard-Steuerungsfunktionen und eine Sicherheits-Steuerung (30) mit Sicherheitsfunktionen aufweist und auf Basis eines Personal-Computers PC (10) mit einer PC-CPU (11) und einem PC-Bus (12, 13) aufgebaut ist, wobei der PC (10) mit einem Standard-Betriebssystem betrieben wird und wobei die Standard-Steuerungsfunktionen auf dem PC (10) oder einem PC-Einschubmodul (21) für die Standard-Steuerung (20) realisiert sind,

dadurch gekennzeichnet, dass

die Sicherheits-Steuerung (30) aus einem oder mehreren mit dem PC-Bus (12, 13) verbundenen Sicherheits-Modulen (31, 32) besteht und dass die Sicherheits-Module (31, 32) eine gemäß Fehler- und Ausfallsicherheit sicherheitszertifizierte Hardware und/oder Firmware zur Ausführung der Sicherheitsfunktionen umfassen."

Anspruch 1 des Hilfsantrags 1 weist das weitere Merkmal auf, dass "die Sicherheitsmodule derart ausgelegt sind, dass sie im Fehlerfall autark für sich alleine das Erreichen eines gesicherten Zustands erreichen und sich gegenseitig überwachen, wodurch ein gesicherter Zustand für die automatisierte Maschine und/oder Anlage gewährleistet ist".

Anspruch 1 des Hilfsantrags 3 weist gegenüber dem Anspruch 1 des Hauptantrags die weiteren Merkmale auf, dass "die Sicherheitsmodule derart ausgelegt sind, dass sie im Fehlerfall autark für sich alleine das Erreichen eines gesicherten Zustands erreichen" und "die programmierbare Steuerung (1) als rückwirkungsfreie Kombination aus Standard-Steuerungsfunktionen und mindestens einem Sicherheits-Modul (31, 32) ausgeführt ist, wobei eine rückwirkungsfreie Kombination ein Verhindern eines Auswirkens einer Fehlfunktion der Standardsteuerung auf sicherheitstechnische Merkmale der Sicherheits-Steuerung (30) ist".

<u>erfinderische Tätigkeit</u>

Im Stand der Technik ist ein programmierbares Mikrocomputersystem zum Einsatz in einer sicherheitskritischen Umgebung bekannt, mit einem sicherheitskritischen Prozessor, der

Hard- und Firmware in Form eines "watchdog timer" und eines "power supply monitor" zur Ausführung der sicherheitskritischen Funktionen umfasst; letztere bestehen beispielsweise darin, zu verifizieren, dass die Versorgungsspannung innerhalb vorgegebener Grenzen liegt.

Laut Kammer unterscheidet sich die beanspruchte Steuerung von dem aus dem Stand der Technik bekannten System lediglich darin, dass die Hard- und/oder Firmware der Sicherheits-Module gemäß Fehler- und Ausfallsicherheit sicherheitszertifiziert ist.

Nach Auffassung der Kammer dient die **Sicherheitszertifizierung keinem eigentlichen technischen Zweck**, sondern bringt lediglich zum Ausdruck, dass die Hard- oder Firmware bestimmten vorab festgelegten Sicherheitsanforderungen genügt, indem beispielsweise die Hard- und Firmware übergeprüft wird, ob sie bestimmte Tests besteht. Folglich werden die **technischen Merkmale der Hard- oder Firmware nicht allein aufgrund einer Sicherzeitszertifizierung geändert**. Daher kommt dem Umstand, dass eine Hard- oder Firmware sicherheitszertifiziert ist, für sich genommen **kein technischer Beitrag** zu.

Ausgehend vom nächstliegenden Stand der Technik besteht somit der einzige Unterschied der beanspruchten Steuerung nicht in einem technischen Beitrag. Gemäß der gefestigten Rechtssprechung der Beschwerdekammern (vgl. T 0641/00 (erster Leitsatz), Abl. EPA 2003, 352) kann ein nichttechnischer Beitrag zum Stand der Technik jedoch keine erfinderische Tätigkeit begründen. Folglich beruht die Steuerung gemäß Anspruch 1 nicht auf einer erfinderischen Tätigkeit (Artikel 52 (1) und 56 EPÜ) und der Hauptantrag ist daher nicht gewährbar.

Das weitere Merkmal des Hilfsantrags 3, wonach die Sicherheitsmodule derart ausgelegt sind, dass sie im Fehlerfall autark für sich alleine das Erreichen eines gesicherten Zustands erreichen, drückt nach Auffassung der Kammer **lediglich den Zweck einer Sicherheitssteuerung**, nämlich das zu steuernde System in einer sicherheitskritischen Situation zuverlässig zu kontrollieren, um Schaden zu verhindern, in anderen Worten aus. Für genau diesen Zweck ist der sicherheitskritische Prozessor im Stand der Technik vorgesehen. Somit ist das genannte weitere Merkmal dem SdT sicherheitskritischen Prozessor inhärent und kann daher nicht zur erfinderischen Tätigkeit beitragen.

Auch das weitere Merkmal, wonach die programmierbare Steuerung als rückwirkungsfreie Kombination aus Standard-Steuerungsfunktionen und mindestens einem Sicherheits-Modul ausgeführt ist, drückt **lediglich den Zweck der Sicherheitssteuerung** aus, dass sicherheitskritische Entscheidungen über den Betrieb einer Maschine zwingend separat und unabhängig von der Steuerung der Maschine im Standardbetrieb zu treffen sind, damit jegliche Auswirkung einer Fehlfunktion der Standardsteuerung auf die von der Sicherheitssteuerung zu treffenden Entscheidungen verhindert wird. Daher ist eine Sicherheitssteuerung **zwingend rückwirkungsfrei von der Standardsteuerung** aufgebaut; dieses Merkmal kann daher auch **nicht zur erfinderischen Tätigkeit beitragen**.

Folglich beruht die Steuerung gemäß dem Anspruch 1 des Hilfsantrags 3 nicht auf einer erfinderischen Tätigkeit (Artikel 52 (1) und 56 EPÜ). Der Hilfsantrag 3 ist somit nicht gewährbar.

Klarheit

Das weitere Merkmal, wonach sich die **Sicherheitsmodule "gegenseitig überwachen, wodurch ein gesicherter Zustand für die automatisierte Maschine und/oder Anlage gewährleistet ist**", ist **unklar**, da aus dem Merkmal **nicht zu erahnen** ist, in welchem **Umfang** eine gegenseitige Überwachung der Sicherheits-Module erfolgen soll oder welchen **Einfluss** eine gegenseitige Überwachung auf den gesicherten Zustand einer automatisierten Maschine und/oder Anlage haben soll.

T 1288/09 (Detecting unauthorized transmission/AUDIBLE MAGIC) of 18.4.2013
Copyright detection and protection system and method

Inventive step - yes (after amendment)

Applicant name: Audible Magic Corporation
Application number: 02725522.3
IPC Class: G06F 1/00

Board: 3.5.06

http://www.epo.org/law-practice/case-law-appeals/pdf/t091288eu1.pdf

The invention

The application generally relates to the problem of detecting and acting upon unauthorized transmission of digital works over the Internet. The application proposes to register protected digital works together with so-called "content-based fingerprints" which are obtained from the digital works by extracting a plurality of features from them. Then network traffic is monitored. From each intercepted digital data packet a content-based fingerprint is generated and compared with the registered finger prints so as to determine "a probability that the unknown con tent contains a registered copyrighted work". In case of a match indicating that the data packet contains a portion of a registered work a follow-up check is performed to establish whether the copyright owner may have authorized the transmission. The determination of whether the transmission is authorized is based on the source IP address or the recipient IP address. Based on the result of this determination, especially if negative, appropriate "action" is taken such as re cording, reporting or blocking transmission. The application is particularly concerned with digital works comprising audio data such as music or video, and a method called the Stochastic Audio Matching Mechanism, abbreviated to SAMM, is discussed in detail. However the description is explicit about the fact that digital works can be of any type, including text, software or other digital content. Depending on the type of work, different finger printing methods have to be used which the description refers to as known in the art.

Claim 1 reads as follows.

"A method of identifying transmissions of digital works to detect unauthorized transmissions of the digital works, the method comprising:

maintaining (702) a registry (244) of information identifying registered works including at least one content based fingerprint for each of the registered works, wherein each of the at least one content based fingerprints has a corresponding feature sequence;

monitoring (706) a network for transmission of at least one packet-based digital signal, wherein the transmission comprises a source IP (internet protocol) address, a recipient IP address, and a digital work;

extracting a plurality of features from the at least one packet-based digital signal, wherein the at least one packet-based digital signal comprises audio data, and wherein each feature is a plurality of characteristics of the at least one packet-based digital signal;

generating (732) a content based fingerprint for the at least one packet-based digital signal from the plurality of features, wherein the content based fingerprint of the at least one packet-based digital signal has a corresponding feature sequence;

performing a probabilistic identification comparison between the feature sequence of the content based fingerprint of the at least one packet-based digital signal and the feature sequence of a content based fingerprint of one of the registered works to determine a probability that the digital work in the transmission of the [at] least one packet-based digital signal is a match to one of the registered works;

determining whether the transmission is an authorized transmission, based on at least one of the source IP address or the recipient IP address, if the transmission of the at least one packet-based digital signal includes at least one portion of one of the registered digital works; and

taking action (720, 722, 726) based on the determination."

The prior art

D2 discloses a steganographic system used, inter alia, for the automatic detection of unauthorized transmission of copyrighted digital works, including audio. More specifically, D2 defines a library of so-called universal codes which may be embedded into a digital work - invisibly, but in a way that allows their retrieval by suitable re cognition software - so as to link the work with its pertinent copy right owner. D2 discloses an "Internet tollgate" which would "check in coming video" for the company's "internal signature codes" and certain header information and which would not pass any non-authorized material based on this check. Header information may be information "about the file as a whole" and include information about the author or copy right holder of the data. As an alternative, D2 also discloses "another piece of [the] ... network" which "performs mundane routine monitoring on Internet channels to look for unauthorized transmission of ... proprietary creative property". D2 addresses the problem that "pirates" might modify a protected digital work so that the embedded codes can no longer be recognized and dis closes that this may be acceptable in some situations but not in others. It may be acceptable for the "enablement of authorized action based on the finding of the codes" - because, as the board reads it, a modified digital work will fail to enable the unauthorized action - but may be inacceptable "in the case of 'random monitoring ... for the presence of codes.'" - because the illicit use of modified works will simply be missed.

Claim 1 differs from D2 in two main respects:

a) Identification of digital works according to the claims is based on probabilistic identification of content-based fingerprints rather than on the detection of watermarks as used in D2.

b) The claims specify that an unauthorized transmission is determined based on the source or recipient IP address in addition to the fingerprint matching, whereas D2 discloses that digital data is validated based on watermark detection in combination with the verification of header data, which may include the author and the copyright owner of the digital work.

In the board's understanding however, D2 teaches "mundane routine monitoring" as a different way of employing the watermark-based identification method for transmission control which does not imply or suggest a different identification method (such as fingerprinting) altogether. At the same time, the **board disagrees** with the appellant that D2 **teaches away from** using a different identification method, such as **fingerprinting** in place of watermarking. Rather, the board is of the opinion that the skilled person would always assess possible improvements of a given method or device. The board considers that **watermarking and fingerprinting are well-known ways of identifying a digital object with well-known respective advantages** and dis advantages. Watermarking operates by incorporating "water marks" into a digital object which can be automatically retrieved later on. Fingerprinting in contrast does not incorporate anything in to the digital object but derives an identifier from the given content. The processing requirements for watermarking are typically smaller than those for fingerprinting, but watermarking cannot protect already released digital works and can be removed or disabled, leaving a digital work unprotected. Therefore it would have been **obvious for the skilled person** seeking to **improve** the disclosure of D2 to **consider fingerprinting as an alternative to watermarking to identify digital documents**. Once this choice is made, the board further considers that the claimed use of fingerprints follows obviously, in particular the use of a registry, the calculation of a fingerprint from a digital signal in transmission and its comparison with the registered fingerprints. **Even** the claimed "**probabilistic identification**" is, in the broad interpretation given above, considered to be a **commonly known way of robust fingerprinting**.

The board thus concludes that difference "a" is in sufficient to establish an inventive step over D2.

Regarding feature "b", with reference to the IP addresses, the detection of unauthorized transmission as claimed is based on properties of the network or, more specifically, of the individual network components involved in a transmission. In contrast, D2 only discloses the use of metadata of the digital work itself (header information) and of individuals involved (author, copyright owner). Difference "b" thus **contributes to making the detection mechanism of D2 more network aware**. As part of a network monitoring mechanism as claimed the board finds that this contribution makes a **technical contribution** to the art. The board further considers that the evaluation of IP addresses is not suggested by the use of header information according to D2 nor by any of the other documents on file. Therefore, by virtue of difference "b", the board comes to the conclusion that the claimed matter is based on an **inventive step** over D2 and the available prior art, Article 56 EPC 1973.

T 1512/09 (Content protection/EMMA MIXED SIGNAL) of 20.3.2013

Method and system for protecting content in a programmable system

Keywords: **Inventive step - yes**

Applicant name: Emma Mixed Signal C.V.
Application number: 05006951.7
IPC Class: G06F 1/00, G01R 31/3185, G06F 12/14

Board: 3.5.06

http://www.epo.org/law-practice/case-law-appeals/pdf/t091512eu1.pdf

The independent claim 1 of the main request is directed to:

A method of protecting content embedded in a programmable system, the system having at least one Application Specific Integrated Circuit (ASIC) (12) executing an application,

characterized in that ….

Interpretation of the term "Application Specific Integrated Circuit (ASIC)"

The board considers that for the skilled person both the term "Application Specific Integrated Circuit" and its acronym ASIC have a well-defined meaning. Notably, a "Field-Programmable Gate Array" (**FPGA) is not an ASIC**, although they may both be forms of gate array, since **ASICs do not have re-configurable logic**.

The connections are "hard-wired", i.e. an ASIC is not a programmable logic chip as disclosed in the prior art D1. Thus the board does not agree with the position taken in the appealed decision that the FPGA of D1 is an ASIC as claimed. On the other hand the board considers it well known that an FPGA, together with the necessary configuration memory to program the logic of the FPGA, is a common alternative to an ASIC. Which is used in a particular application depends on a variety of factors, for example the production volume; ASICs are cheap in very large quantities but very expensive in small quantities.

The subject-matter of claim 1 differs at least from the method disclosed by D1 in that (1) an ASIC, rather than an FPGA, (2) executes an application, (3) information "on" (i.e. concerning) the application is stored in non-volatile storage and (4) the non-volatile storage is divided into a region where the protection is applied and an unprotected region that can be accessed in all access modes.

Regarding feature (1), which s**olves the objective problem of providing a protection against reverse engineering**, the board notes that the whole point of the method disclosed in D1 is to protect the configuration memory of an FPGA from unauthorised copying. In fact, the schemes disclosed in D1 are introduced to deal with a transition from ASICs to programmable logic circuitry and it is **not apparent from D1 or otherwise why the skilled**

person would want to transition back to an ASIC whilst still applying a scheme as disclosed in D1. Indeed, whereas FPGAs have such a memory, from which they load their configuration when powered up, **ASICs are permanently configured through hard-wiring and have no need for a similar configuration memory** that would have to be protected against the same kind of design theft.

The appealed decision points out (Reasons 4) that "Furthermore, the present application does not draw a clear distinction between FPGA and ASIC. The feature of reprogramming the device defined by claim 1 points more to FPGA rather than to ASIC, from which the skilled person would expect the logic being "hard-wired" into the chip. The application does not provide a delimiting feature by which the use of an ASIC would show an advantage or a different technical effect over the use of an FPGA". This wording seems to imply that claim 1 would have been drafted keeping in mind at least the possibility of using an FPGA instead of an ASIC, i.e. its subject-matter would really not be that far away from a method that employs an FPGA, as in D1. However, according to the board, **an ASIC is clearly a different thing than an FPGA** and **claim 1 clearly and explicitly refers to an ASIC, not to an FPGA** or some other programmable circuitry. Even if the claim also refers to a "programmable system", the claim's wording leaves no doubt that, in that system, it is not the logic of the ASIC which is programmable in the sense of "re-configurable". In fact, the **logic of an ASIC itself cannot be programmed**, by its very nature. Thus the **claim cannot be construed in this way**. Rather, as is confirmed by the description of the present application, the intention is for the ASIC to be programmable in the sense of carrying out a computer program, in the form of algorithms in the non-volatile memory. The ASIC of claim 1 is therefore clearly distinct from the FPGA of D1.

Thus evidently the claimed subject-matter is not obvious starting from D1.
