# Appeal Decision

Appeal No.2020-8184

| | |
|---|---|
| Appellant | Rosemount Incorporated |
| Patent Attorney | TSUKUNI & ASSOCIATES |

Patent Application 2018-551297 “NFC-enabled wireless process communication gateway" Appeal against Decision of Refusal [International Publication on October 5, 2017, WO2017/172403, National Publication of International Patent Application No. 2019-517172A published on June 20, 2019] is decided as follows.

Conclusion

The appeal of the case was groundless.

Reasons

I History of the procedures

The present application was filed as an application with an international filing date on March 21, 2017 (claim of priority under the Paris Convention was received by the Foreign Office on March 31, 2016, in the United States of America), and the history of the procedure is summarized as follows.

| | |
|---|---|
| September 20, 2019: | Notification of reasons for refusal |
| December 17, 2019: | Submission of written opinion and written amendment |
| February 5, 2020: | Decision of refusal by a examiner |
| June 12, 2020: | Submission of Notice of Appeal written amendment |
| February 4, 2021: | Submission of petition. |

II Decision to dismiss the written amendment filed on June 12, 2020

[Conclusion of the decision to dismiss the amendment]

The written amendment filed on June 12, 2020 (hereinafter, “the amendment") is hereby dismissed.

［Reason］

1 Regarding the amendment (details of the amendment)

(1) Description of the scope of claims after the amendment

By the amendment, the recitation of Claim 1 of the scope of claims was amended as follows. (Underlined are the amended parts.)

“A method for connecting a field device to a wireless process communication network, comprising:

bringing the wireless field device into the proximity of the near field communication (NFC) range of a wireless gateway;

establishing a communication connection between an NFC transceiver of the wireless gateway and an NFC tag of the wireless field device;

generating near field communication between the wireless gateway and the wireless field device to automatically load the wireless field device with a join key that can automatically allow the wireless field device to access the wireless process communication network;

and using the join key to enable the wireless field device to communicate on the wireless process communication network.”

(2) Scope of claims before the amendment

The recitation of Claim 1 of the scope of claims as amended by the written amendment dated December 17, 2019, before the amendment, is as follows.

“A method for connecting a field device to a wireless process communication network, comprising:

bringing the wireless field device into the proximity of the near field communication (NFC) range of a wireless gateway;

establishing a communication connection between an NFC transceiver of the wireless gateway and an NFC tag of the wireless field device;

generating near field communication between the wireless gateway and the wireless field device to load the wireless field device with a join key that can allow the wireless field device to access the wireless process communication network;

and using the join key wirelessly to enable the wireless field device to communicate on the wireless process communication network.”

2 Propriety of the amendment

The amendment includes adding the limitation “automatically" to “allow the wireless field device to access the wireless process communication network" which is necessary to specify the invention recited in Claim 1 before the amendment, and adding the limitation “automatically" to “to load the wireless field device" which is necessary to specify the invention recited in Claim 1 before the amendment, and since the field of industrial application and the problem to be solved are identical between the invention recited in Claim 1 before the amendment and the invention recited in Claim 1 after the amendment, the invention falls under Patent Act Article 17-2 (5) (ii), which is intended to restrict the scope of claims.

Therefore, the following is an examination of whether the invention recited in Claim 1 after the amendment (hereinafter, “amended invention") conforms with the provisions of Article 126 (7) of the Patent Act which is applied mutatis mutandis under the provision of Article 17-2(6) of the Patent Act (whether the invention should be patented independently upon the filing the patent application).

(1) The amended invention

The amended invention is as described in 1 (1) above.

(2) Matters described in the cited documents

A Cited Document 2

(A) National Publication of International Patent Application No. 2011-504648A (hereinafter, “Cited Document 2"), which is a document distributed or made available to the public through telecommunication lines before the priority date of the present application cited in the reason for refusal of the original examination, contains the following description with drawings. (Underlined are assigned by this panel.)

“[0019]

Fig. 1 shows a process control/monitoring system 10, which includes host computer 12, high-speed network 14, wireless mesh network 16 (which includes gateway 18 and wireless field devices or nodes 20a-20i), a configuration device 30, and a network computer 32.

Gateway 18 interfaces mesh network 16 and with host computer 12 via the high-speed network 14.

Messages can be transmitted from host computer 12 to gateway 18 via network 14 and then transmitted to selected node of mesh network 16 over one of a plurality of different paths.

Similarly, messages from individual nodes of mesh network 16 are routed through mesh network 16 from node-to-node over one of several paths until they arrive gateway 18 and are then transmitted to host 12 over high-speed network 14.

[0020]

New wireless field devices can be added to network 16 using a joining process. In one embodiment, security within network 16 is predicted on a symmetric join key mechanism. The correct join key must be loaded into a field device so that the device will be accepted by other field devices and by the gateway. The join key must be loaded in a secure fashion, so that another wireless devices within range cannot receive and possibly misuse the join key. Although the join key can be loaded manually into each new field device, manual loading can be prone to error and may expose the cryptographic data to human operators.

[0021]

The goal is to load cryptographic materials, such as keys, into new field devices in a secure fashion. This can be achieved through a secure wireless communication path (as described later in conjunction FIGS.2A and 2B) or a secure wired communication path (as described in conjunction with FIG.3). between gateway 18 and the new field device.

In both cases, configuration device 30 is connected to network 14 along with network computer 32 which provides a graphical user interface (GUI) which may include, for example, a web browser. Configuration device 30 and the GUI on computer 32 allow a technician to interrogate the network security manager (which may be, for example, an application program running on gateway 18 or host computer 12), obtain the correct join key (or other cryptographic material) for the new field device, and securely load the join key into the new field device.

Once the join key and other required information has been loaded, a new field device can be installed in the field, where it can use its stored join key as part of the joining process to become part of wireless network 16.”

(B) Considering the above description and the common technical knowledge of those skilled in the art, it is acknowledged that the following technical matters are described in Cited Document 2.

a The above paragraph [0019] describes that “Fig. 1 shows a process control/monitoring system 10 which includes host computer 12, high-speed network 14, wireless mesh network 16 (which includes a gateway 18 and wireless field devices or nodes 20a to 20i),...".

Then, it can be said that Cited Document 2 describes “a process control/monitoring system provided with a wireless mesh network including a wireless field device".

b The above paragraph [0020] describes that “New wireless field devices can be added to network 16 using a joining process.", “The correct join key must be loaded into a field device so that the device...will be accepted by the gateway." and the above paragraph

[0021] describes that “securely load the join key into the new field device. Once the join key and other required information has been loaded, a new field device can be installed in the field, where it can use its stored join key as part of the joining process to become part of wireless network 16.".

Here, it is apparent that the “new field device" described in the above paragraph [0021] represents the same device as the “new wireless field device" described in the paragraph [0020].

Then, it can be said that Cited Document 2 describes “using the stored join key as part of the subscription process after the join key is loaded into the new wireless field device and adding the wireless field device to the wireless mesh network by having the gateway accept the wireless field device".

c As outlined in “a" and “b" above, it can be said that Cited Document 2 describes a method of “using the join key as part of the subscription process and adding the new wireless field device to the wireless mesh network".

Then, it can be said that Cited Document 2 describes “a method of adding the wireless field device to the wireless mesh network".

(C) From the above (a) and (b), it is acknowledged that the Cited Document 2 describes the following invention (hereinafter, “the cited invention").

“A method for adding the wireless field device to the wireless mesh network, comprising:

in a process control/monitoring system provided with a wireless mesh network including wireless field devices,

adding the wireless field device to the wireless mesh network by having the gateway accept the wireless field device using the stored join key as part of the joining process after the join key has been loaded into the new wireless field device".

B Cited Document 1

(A) International Publication No. WO 2014/205243 (hereinafter, “Cited Document 1"), which is also cited in the reasons for refusal of the examiner's decision and is a document distributed or made available to the public through telecommunication lines before the priority date of the present application, contains the following description with drawings. (Underlined parts are assigned by this panel.)

「[0002] Embodiments of the subject matter generally relate to the field of network devices, and, more particularly, to wireless setup between network devices.

[0003] Near field communication (hereinafter "NFC") technology is a set of standards for allowing communication between compatible devices initiated by bringing the compatible devices into close proximity of each other. NFC may be implemented using radio frequency (hereinafter RF) technology. NFC may be implemented actively or passively. Active NFC includes hardware that transmits an RF signal using a connected power source. Passive NFC, on the other hand, does not have a connected power source, instead relying on power generated from a received RF signal.

(omitted)

[0042] FIG. 1 depicts an embodiment of a set of NFC-enabled wireless devices capable of utilizing NFC to securely facilitate network configuration. FIG. 1 depicts the set of NFC- enabled devices, including a device 102 with passive NFC capability (hereinafter "client") and an access point 104 with active NFC capability (hereinafter "AP"). The range within which a passive NFC capable client may trigger the NFC capabilities of the AP 104 is indicated by the dotted line 106. The client 102 and the AP 104 may each be associated with a public-private key pair (not depicted).

[0043] At stage A, the client 102 is moved into the range 106 within which the AP 104 NFC capabilities are triggered. The specific range 106 may vary between implementations. For example, in some implementations the range may be a few centimeters, while in some implementations the range 106 is small enough that the client 102 physically touches the AP 104. The range 106 may be defined by the particular NFC standard implemented or vary due to design considerations. For example, if reducing power consumption is a design goal, the amount of power available to transmit a signal may be limited, thus reducing the range 106. As a device with active NFC capabilities, the AP 104 generates an RF field that, once a passive NFC device is within range, provides power for the passive NFC device. Thus, when a passive NFC device, such as the client 102, enters the RF field generated by the AP 104, the passive NFC device may communicate with the AP 104.

[0044] At stage B, the AP 104 reads the public key associated with the client 102 from the client 102. To read data from a passive NFC device such as the client 102, the AP 104 encodes a command and transmits the command using an RF signal. The client 102 receives the RF signal, and utilizing the power generated by the RF signal, decodes the command. Further using the power generated by the RF signal, the client 102 transmits the public key.

[0045] At stage C, the AP 104 writes the public key associated with the AP 104 to the client 102. To write the AP 104 public key to the client 102, the AP 104 encodes a write command, as well as the data to write, and transmits the encoded command and data as an RF signal, or as a set of RF signals, to the client 102. The client 102 utilizes the power generated by the RF signal to decode the command and data, writing the AP 104 public key to memory accessible to the client 102.

[0046] At stage D, the client 102 and AP 104 perform a secure network configuration. The client 102 may be implemented such that the client 102 begins the secure network configuration in response to receiving the AP 104 public key. Thus, the receipt of the AP 104 public key may act as the indication that a secure network configuration setup can begin. In some implementations, another command transmitted by the AP 104 indicates that the secure network configuration can begin. In some implementations, the indication may come from another source, such as from a user interacting with a user interface associated with the client 102 or AP 104.」

(B) From the above description, it is acknowledged that Cited Document 1 describes the following technical matters.

(a) The above paragraph [0042] describes that “FIG. 1 depicts the set of NFC-enabled devices, including a device 102 with passive NFC capability (hereinafter, “client”) and an access point 104 with active NFC capability (hereinafter, “AP”)." and the above paragraph [0043] describes that “the client 102 is moved into the range 106 within which the AP 104 NFC capabilities are triggered.", while it describes that “the range may be a few centimeters, while in some implementations the range 106 is small enough that the client 102 physically touches the AP 104.", and therefore, it can be said that the above description “the client 102 is moved into the range 106 within which the AP 104 NFC capabilities are triggered." indicates that the client 102 is brought into proximity of the range within which the AP 104 NFC capabilities are triggered.

Also, the above paragraph [0043] describes that “the AP 104 generates an RF field that, once a passive NFC device is within range, provides power for the passive NFC device…when a passive NFC device, such as the client 102, enters the RF field generated by the AP 104, the passive NFC device may communicate with the AP 104.", and therefore, it is obvious that when communicating, the passive NFC device such as a client establishes a communication connection with the AP.

Then, Cited Document 1 describes that “when a client with passive NFC capabilities is brought into proximity of the range of AP with active NFC capabilities, the client with passive NFC capabilities establishes a communication connection with the AP with active NFC capabilities".

(b) Also, the above paragraph [0045] describes that “To write the AP 104 public key to the client 102, the AP 104 encodes a write command, as well as the data to write, and transmits the encoded command and data as an RF signal, or as a set of RF signals, to the client 102.", and the above paragraph [0046] describes that “the client 102 and AP 104 perform a secure network configuration. The client 102 may be implemented such that the client 102 begins the secure network configuration in response to receiving the AP 104 public key…the receipt of the AP 104 public key may act as the indication that a secure network configuration setup can begin.". Then, the above paragraph [0002] describes that “Embodiments of the subject matter generally relate to the field of network devices, and, more particularly, to wireless setup between network devices.", and therefore, it is apparent that the “secure network configuration set up" in the above paragraph [0046] is a wireless setup between network devices, i.e., a wireless setup between the client 102 and the AP 104, and during wireless setup, it is common technical knowledge that the client 102 accesses the AP 104.

Then, Cited Document 1 describes that “the AP 104 public key is transmitted to the client as an RF signal, and in response to receiving the AP 104 public key, the client accesses the AP 104 to initiate a wireless setup between the client 102 and the AP 104".

(c) Here, it is common technical knowledge that the passive NFC is also called NFC tag and the active NFC is also called NFC reader/writer, and an NFC reader/writer can be said to be an NFC transmitter/receiver, i.e., an NFC transceiver, because it actively transmits to and receives from an NFC tag, furthermore, since the NFC reader/writer of the AP transmits the public key to the NFC tag of the client, it can be said that the client with the NFC tag has established a communication connection with the AP with the NFC transceiver, and the public key is loaded to the client.

In addition, since the client accesses the AP to initiate the wireless setup in response to receiving the AP 104 public key, it can be said that the AP 104 public key is a join key that can automatically allow the client to access the AP.

Then, it is obvious that near field communication is generated between the NFC transceiver of the AP and NFC tag of the client, since the join key is passed as an RF signal, and since the generation of the near field communication is performed by the proximity of the NFC tag of the client and the transceiver of the AP, and the public key is transmitted (loaded) to the client, it can be said that the near field communication between the NFC transceiver of the AP and NFC tag of the client is generated in order to automatically make the client load the public key (join key).

Therefore, it is acknowledged that Cited Document 1 describes a technical matter in which “when a client with an NFC tag is brought into the proximity of the range of an AP with an NFC transceiver, the client with the NFC tag establishes a communication connection with the AP with the NFC transceiver, and a near field communication is generated between the NFC transceiver of the AP and NFC tag of the client in order to automatically load the join key to the client that can automatically allow the client to access the AP".

(3) Comparison and Judgment

Comparing the amended invention and the cited invention, the following can be said.

(A) The “wireless field device" of the cited invention is included in the “field device" of the amended invention and corresponds to the “wireless field device" of the amended invention. Further, since the “wireless mesh network" of the cited invention is provided with the “process control / monitoring system”, the “wireless mesh network" corresponds to the wireless network that communicates for process control / monitoring, i.e., the “wireless process communication network" of the amended invention. And “adding the wireless field device to the wireless mesh network" in the cited invention means connecting the wireless field device to the wireless mesh network.

Therefore, the amended invention and the cited invention are correspondent with that “a method in which a field device is connected to a wireless process communication network".

(B) The “join key" of the cited invention is used when “adding the wireless field device" to the “wireless mesh network". And the “join key" of the cited invention corresponds to the “join key" of the amended invention because the join key is used to allow the gateway to accept the wireless field device. And it is obvious that “adding the wireless field device" to “the wireless mesh network" in the cited invention is done to enable the wireless field device to communicate on the wireless mesh network.

Therefore, the amended invention and the cited invention are correspondent with that “a join key is used to enable the wireless field device to communicate on the wireless process communication network".

From the above, the corresponding features and different features between the amended invention and the cited invention are as follows.

(Corresponding Features)

“A method in which a field device is connected to a wireless process communication network,

and the method comprising the join key being used to enable the wireless field device to communicate on the wireless process communication network”.

(Different Feature)

The different feature is that the amended invention has the matters specifying the invention that “the wireless field device is brought within the range of near field communication (NFC) of the wireless gateway, and a communication connection is established between the NFC transceiver of the wireless gateway and the NFC tag of the wireless field device, and near field communication is generated between the wireless gateway and the wireless field device to automatically load the join key that can automatically allow the wireless field device to access the wireless process communication network, onto the wireless field device”, whereas the cited invention does not have the above feature specifying the invention.

Each of the above differences is discussed below.

As explained in (2) above, the matter “when a client with an NFC tag is brought within the range of an AP with an NFC transceiver, a communication connection is established between the client with the NFC tag and the AP with the NFC transceiver, and near field communication is generated between the NFC transceiver of AP and NFC tag of the client to automatically load the join key that can automatically allow the client to access AP, to the client" is a known technical matter.

Here, it is obvious that in order for the wireless field device of the cited invention to use the join key for communicating on the wireless process communication network, it is necessary to configure settings for that purpose, and automating at least part of the setting work is a problem that should naturally be pursued by a person skilled in the art.

Also, since the cited invention is to join the wireless field device to the wireless mesh network by using the join key to allow the gateway to accept the wireless field device, i.e., to allow the wireless field device to access the wireless mesh network, and the technical matter described in Cited Document 1 is also to allow the client to access AP, i.e., to allow a device called the client to access a network via AP, they are common technical matters in that they automatically allow a device to access the network.

Therefore, in order to solve the problem to automate at least part of the setting work when “the join key is loaded into a new wireless field device" in the cited invention, a person skilled in the art would have easily allowed the wireless field device to access the wireless mesh network automatically, by applying the common technical matters that “when a client with an NFC tag is brought within the range of an AP with an NFC transceiver, a communication connection is established between the client with an NFC tag and the AP with an NFC transceiver, and near field communication is generated between the NFC transceiver of the AP and the NFC tag of the client to automatically load the join key that automatically allows the client to access the AP, to the client”.

And the effects of the amended invention are also merely within the range that would have been predicted by a person skilled in the art based on the cited invention and the technical matter described in Cited Document 1, and cannot be said particularly remarkable.

Therefore, the amended invention would have been easily invented by a person skilled in the art based on the cited invention and the technical matter described in Cited Document 1, thus the appellant should not be granted a patent for the amended invention under the provisions of Article 29 (2) of the Patent Act.

### 3 Closing of Decision to dismiss amendment

Since the amended invention cannot be independently patented at the time of filing the patent application, the amendment violates the provisions of the Patent Act Article 126 (7), which is applied mutatis mutandis in Article 17-2 (6) of the same Act, and therefore it should be dismissed under the provisions of Article 53 (1) of the same Act, the relevant terms of which shall be and applied mutatis mutandis in Article 159 (1) of the same Act.

Therefore, the decision is made according to the conclusion of the decision to dismiss the above amendment.

## III Regarding the Invention of the present application

### 1 The Invention of the present application

Since the written amendment filed on June 12, 2020 was dismissed as described above, the Invention is specified by the matters recited in Claims 1 to 11 of the scope of claims amended by the written amendment filed on December 17, 2019, and the invention as claimed in Claim 1 is as described in “(2) Scope of claims prior to the amendment" in section “1 Regarding the amendment (contents of the amendment)" in “II Decision to dismiss the written amendment filed on June 12, 2020" (hereinafter, “the Invention ").

2 Reason for refusal of examiner's decision

The reason for refusal of examiner's decision includes the fact that the Invention would have been easily invented by a person skilled in the art based on the invention described in Cited Document 2 and the technical matter described in Cited Document 1 below, which were distributed or made available to the public through telecommunication lines prior to the priority claim date of the present application, and because of this reason it shall not be granted a patent under the provisions of Article 29 (2) of the Patent Act.

Cited Document 1: International Publication No. WO 2014/205243
Cited Document 2: National Publication of International Patent Application No. 2011-504648A

3 Cited inventions, etc.

Cited Documents 1 and 2 cited in the reason of refusal for the examiner's decision, and the matters described therein are as described in section “(2) Matters described in the cited documents" in section “2 Propriety of amendment" of “II Decision to dismiss the written amendment filed on June 12, 2020" above.

4 Comparison and Judgment

The Invention omits limitations relating to “the access of the wireless field device to the wireless process communication network" and “loading the join key to the wireless field device" from the amended invention. Since the amended invention, which includes all matters specifying the Invention and corresponds to one with other additional matters, would have been easily invented by a person skilled in the art based on the cited invention and the technical matter described in Cited Document 1, as described in “(3) Comparison and Judgment" of “2 Propriety of amendment" in section “II Decision to dismiss the written amendment filed on June 12, 2020" given above, the Invention would also have been easily invented by a person skilled in the art for the same reason.

5 Regarding the petition

In the petition filed on February 4, 2021, the appellant prepared the following proposal of amendment and also described, “We are prepared to make amendments in order to resolve any indications in the pretrial reexamination report cited in the inquiring of the panel. We would like the panel to examine whether there are any claims that can satisfy the independent patent requirements through these amendments. And we would be grateful if the panel afford us the opportunity to make further amendments”.

<proposal of amendment (underline indicates the amended part.)>

“<Claim 1 after the amendment>
A method for connecting a field device to a wireless process communication network, comprising:

bringing the wireless field device into the proximity of the near field communication (NFC) range of a wireless gateway;

establishing a communication connection between an NFC transceiver of the wireless gateway and an NFC tag of the wireless field device using the wireless gateway;

providing an identifier of the wireless field device obtained from the NFC tag on the network using the wireless gateway;

searching for a join key that allows the wireless field device to automatically access the wireless process communication network using the wireless gateway;

generating near field communication between the wireless gateway and the wireless field device to automatically load the wireless field device with a join key using the wireless gateway;

and using the join key to enable the wireless field device to communicate on the wireless process communication network.

<Claim 5 after the amendment>

A wireless gateway configured to interact with the field device on the wireless process communication network comprising;

an NFC transceiver configured to detect the NFC tag of the field device, connect it to the NFC tag, and provide the identifier of the wireless field device obtained from the NFC tag on the network;

a control unit configured to automatically retrieve the network join key on the wireless process communication network from the process environment network in response to the detection of the NFC tag of the field device to automatically provide the retrieved network join key to the field device using the NFC transceiver;

a wireless process communication module that uses the network join key to allow the field device to communicate on the wireless process communication network."

However, as explained in II above, the amendment should be dismissed,

and as explained in III, 1 to 4 above, the Invention would have been easily invented by a person skilled in the art based on the technical matter described in Cited Document

2 and Cited Document 1 cited as the reason for refusal of the examiner's decision, and therefore no reasonable reason can be found to afford the opportunity for amendment again.

In addition, if it is not clear what “automatically" in Claim 1 relates to, the invention as claimed in Claim 1 is not an independently patentable invention as the recitation of Claim 1 in scope of claims does not conform with the provisions of the Article 36 (6) (ii) of the Patent Act, and therefore the amendment should be dismissed. Further, as explained in III, 1 to 4 above, the Invention would have been easily invented by a person skilled in the art based on the technical matter described in Cited Document 2 and Cited Document 1 cited in the reason for refusal of the examiner's decision, and likewise, no rational reason can be found to afford the opportunity for amendment again.

## IV Closing

As described above, the appellant should not be granted a patent of the Invention under the provision of Article 29(2) of the Patent Act because a person of ordinally skilled in the art of the invention would have easily make the Invention based on the cited invention and the technical matters described in Cited Document 1 before the priority date of the application.

Accordingly, it is not necessary to examine other claims, and the present application should be rejected.

Therefore, the appeal decision shall be made as described in the conclusion.

March 11, 2021

Chief administrative judge: HIROKAWA, Hiroshi
Administrative judge: HONGO, Akira
Administrative judge: KOKUBU, Naoki