(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 June 2014 (26.06.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/094982 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *G05B 19/418* (2006.01)
H04L 12/24 (2006.01) *H04W 84/22* (2009.01)
H04W 12/04 (2009.01)

(21) International Application Number:
PCT/EP2013/003657

(22) International Filing Date:
4 December 2013 (04.12.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1437/KOL/2012 20 December 2012 (20.12.2012) IN

(71) Applicant: **ABB AG** [DE/DE]; Kallstadter Str. 1, D-68309 Mannheim (DE).

(72) Inventors: **SCHULZ, Dirk**; Hauptstr. 128, 67149 Meckenheim (DE). **KUMAR, Ravish**; Flat no-A101, Saroj Aquila, Srinivas Reddy Layout, AECS Layout, Kundanhalli, Bangalore-560037 (IN). **RUSCHIVAL, Thomas**; Lindenstrasse 4, 88416 Erlenmoos (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

[Continued on next page]

(54) Title: COMMISSIONING SYSTEM AND METHOD FOR A SECURE EXCHANGE OF SENSITIVE INFORMATION FOR THE COMMISSIONING AND CONFIGURING OF TECHNICAL EQUIPMENT

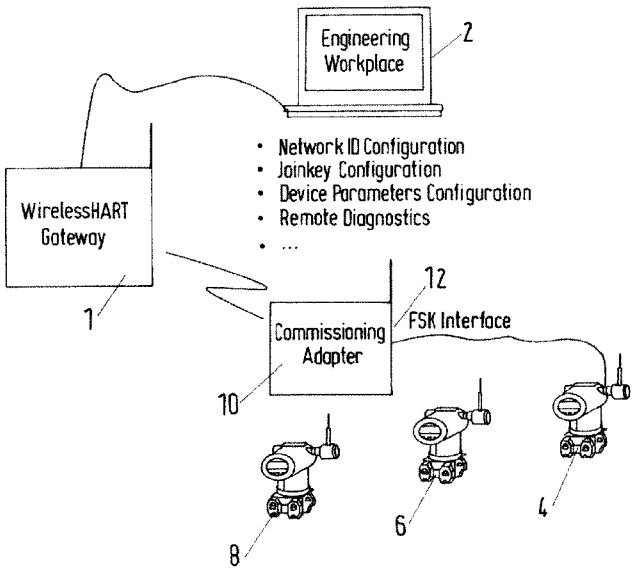

Fig.1

(57) Abstract: The invention relates to a commissioning system and corresponding method for a secure exchange of sensitive information for the commissioning and/or configuring of technical equipment comprising at least two components and/or devices, in particular field devices using communication means to secure a wireless communication, in particular without the need to use higher protocol layers, like for example authentication or encryption functionalities, wherein the communication means comprise a commissioning device and a commissioning network, in particular a commissioning network comprising a regular wireless gateway which in the wireless management system is integrated like a multi-drop wired modem, and/or a key storage device for dedicated join key storage and/or generation is provided, which key storage device comprises a storage unit for a number of key/device and network IDs and is connectable to an engineering client and/or the commissioning device via a wired or wireless short range connection, in particular a handheld and/or USB stick with at least one of a FSK-, RFID-, IR-interface or HMI Port or the like, to receive and/or store one or more join keys and/or ID triples.

WO 2014/094982 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

Commissioning system and method for a secure exchange of sensitive information for the commissioning and configuring of technical equipment

Description

The invention relates to a commissioning system and a method for the secure and/or fail-safe or reliable exchange of sensitive information for the commissioning and configuration of technical equipment, in particular of a plant or process automation system, by means of wireless connections according to the preamble of the independent claims. According to the invention wireless connections which intrinsically seem to be unsecure in real practice, may still be used securely by applying specific communication means, in particular interfaces, and restrictions.

The use of WirelessHART as a new communication standard in industrial automation introduces a number of new challenges compared to classical wired communication, which have to be addressed at an early stage in the respective Device Management System (DMS) during topology engineering and commissioning.

As for wired communication, the DMS requires instances for gateways and devices and must reflect the logical communication topology from the previous network layout. Unlike wired communication, security measures defined in the HART standard introduce additional complexity into the commissioning workflow.

Highlights of the WirelessHART solution are for example the efficient and seamless handling of wireless devices in the DMS; for matters of topology engineering and commissioning, they largely appear just like wired HART devices with the same (even less) effort.

The WirelessHART standard defines mandatory authentication and encryption mechanisms for the wireless communication. It further requires that the related encryption keys are exchanged through secure connections. Wired FSK (Frequency Shift Keying) communication is considered to fulfill this security requirement, are even fully autonomous wireless devices must provide a corresponding interface. Just like any other device parameter, also encryption keys may be pre-parameterized by the device manufacturer.

WirelessHART uses symmetric encryption, namely usage of the same key for encryption and decryption, for the authentication and communication between field devices and wireless access points. Corresponding keys must be available within both the gateway and the field device that wish to communicate.

In the most secure setting, a gateway receives an individual join key per device. To validate a join request, it requires a list of join keys and corresponding device IDs (hardware addresses). There is no way to disable encryption and authentication, but for ease of use the security level can be lowered. A common join key may then be shared between the devices in a network, and any device with a valid key is allowed to join.

Accordingly, during (re-)commissioning or pre-parameterization or installation or putting into operation the WirelessHART - devices must be connected to a "join key source", for example a commissioning station/engineering/handheld, via a secure connection or communication line. Said connection typically is realized via a wired *FSK Modem* connection or a short-range IR connection, which all devices must support, even fully autonomous ones. A HMI (human machine interface) port is also technically possible, but not standardized among manufacturers. Any wired port must be exposed during commissioning, whereby only the non-standard HMI port allows the device to remain closed.

Since existing join keys cannot be read back from any device through any port, the pre-parameterization of keys requires that they are distributed through another chan-

nel, which finally leads to additional effort, potentials and higher risk for mistakes, and diminishes the security.

Similar problems are also valid for the existing Handhelds, which solely allow keys to be entered manually. They have no FDT (Field Device Tool) or FDI (Field Device Integration) integration to exchange the keys with an engineering client.

Therefore, the object of the invention is to provide an enhanced possibility for the secure exchange and easy management of sensitive information of technical equipment and in particular field devices by use of wireless connections, in particular also for wide range exchange.

This object is achieved and solved by a commissioning system for a secure exchange of sensitive information for the commissioning and/or configuration of technical equipment by means of a commissioning device according to the features of claim 1. Advantageous embodiments and developments as well as a corresponding method are disclosed in the description and further claims.

The invention relates to a commissioning system for a secure exchange of sensitive information for the commissioning and/or configuring of technical equipment, in particular field devices of a process automation system or plant automation system, comprising at least two components and/or devices, in particular field devices, using communication means to secure a wireless communication without the need to use higher protocol layers, like in particular authentication or encryption functionalities, wherein the communication means comprise a commissioning device and a commissioning network, in particular a commissioning network comprising a regular wireless gateway which in the wireless management system is integrated like a multi-drop wired modem, and/or a key storage device for dedicated join key storage and/or generation is provided, which key storage device comprises a storage unit for a number of key/device and network IDs and is connectable to an engineering client and/or the commissioning device via a wired or wireless short range connection, in particular a handheld and/or USB stick with at least one of a FSK (Frequency Shift Keying)-, RFID-, IR-interface or HMI (Human Machine Interface) Port or the like, to

receive and/or store one or more join keys and/or ID triples and/or commissioning commands and/or parameters.

The at least two components or devices may be "regular" field devices but also dedicated "care-free" routers, providing an adapter and an energy source, in particular a battery or an accumulator and/or a photovoltaic or solar cell. In particular fully autonomous devices, which in particular are equipped with wireless communication and autonomous energy sources, for example like batteries, which might physically be hard to access because of their site of operation or place of installation, and accordingly do not need or do not have to be accessed or opened and connected through a wired interface.

The communication between devices, in particular field devices , for example from specific and/or special WirelessHART gateways, from WirelessHART handhelds, or from handhelds supporting IR or RFID communication providing near-range communication, wherein a handheld may be any type of smartphone, mobile, tablet PC, netbook, PDA (personal digital assistant) or mobile computer, may be treated as being relatively secure.

Moreover, the system according to the invention, in particular using wirelessHART technology, allows a pre-parameterization or installation or putting into operation / commissioning of wireless – devices, in particular WirelessHART - devices for example by use of a portable commissioning device or station or handheld, in general a portable data processing device or unit, in a secure environment. Secure in the context of this application means with high safety from interception but also a relatively high data or information transfer rate and/or a relatively high data or information transfer quality and/or high connectivity, independent from the circumstances and the environmental conditions in the plant or field.

The system provides a time efficient, in particular with a reduced or minimized join time, flexible, secure and reliable interface or communication interface respectively and access to different type of distributed, in particular wireless or non-wireless, field

devices in particular in a plant or field with a relatively high distance in between the different devices and/or with a relatively high pollution and/or dirt and/or dangerous environment, for example high temperatures and/or pressures, and/or high voltages, so that wired connections or cable connections would require an extended wide range cable net, which cables and/or cable connection might be damaged during operation of the plant and accordingly may not work properly anymore. Furthermore, assembly of the wired network as well as its maintenance will take a lot of effort and material.

Furthermore, the invention allows a reduction of and/or minimizes the join time and/or commission time for one or more field devices arranged in a plant or field in industrial automation industry.

This might be the case for example in an offshore park environment and/or in the oil, gas and minerals site or industry, in particular a roller plant and/or in the chemical or pharmaceutical industry.

Furthermore, the communication means to secure wireless communication comprise properties of a physical layer and/or link layer and/or measurements.

In the context of this invention the term physical layer describes the first and lowest layer in the seven-layer OSI model (Open System Interconnection Reference Model).

The physical layer accordingly comprises all the basic networking hardware transmission technologies of a network and all the necessary means for implementing said technologies and in particular for transmitting raw bits as well as logical data packets over physical link connecting network nodes, whereas the data which have to be transmitted are converted to a physical signal that may be transmitted.

In a further refinement, identification means are provided, which use device identification information to determine the trustworthiness of a communication partner.

In a further refinement, verification means are provided to introduce a verification step executed by a human to yet increase the attained level of security.

According to one embodiment of the system for a secure exchange of sensitive information of technical equipment at least one wireless connection is used, wherein the system comprises communication means which provide or include a commissioning network, in particular a commissioning network comprising a regular wireless gateway which in the wireless management system is integrated like a multi-drop wired modem, wherein said dedicated commissioning network, in particular a WirelessHART Network, uses a well-known Network ID and a shared Join Key and which network is not used for any production purpose whatsoever, and wherein the devices joined in this network are visible to the integration component for the wireless network implemented by the gateway, for example. an FDT (Field Device Tool) communication DTM (Device Type Manager) or an FDI (Field Device Integration) communication device or server, in the same manner as devices connected to an FSK (Frequency Shift Keying) modem, thus any such device may be assigned to the target network, in particular by a commissioning engineer, and to secure this process, the identification information, in particular the device type, the manufacturer, the serial number or the like, or the device proximity to the commissioning network can be used by man or machine to check the legitimacy of the device; the latter is achieved by evaluating receive signal levels and used transmission energy. FSK defines a common frequency modulation technique.

In a further embodiment this commissioning network can be shared between all communication DTMs and/or FDIs and/or communication servers, wherein device assignment is a manual task and accordingly not more than one such DTM (Device Type Manager) or FDI or communication server might be opened at a time and communicates with the gateway.

Furthermore, as part of decommissioning in a further refinement a device is provided which initiates and/or executes a reset of the Network ID and Join Key to the well-known values, a so called soft reset, in particular by demand or request or rule based or signal based.

Generally, in a further embodiment of the invention a device is provided which supports and initiates and/or executes a "hard reset of the security data" to the default values using for example magnetic pins at the respective HMI (Human Machine Interface).

In a further refinement the antenna of the commissioning gateway is enclosed in a radio-shielded tube, in particular made of plastic with embedded metal mesh, and connected via cable to the gateway. When connecting a device, this tube is simply put over the device antenna, resulting in secure and directed or targeted, almost vectored, communication already on the physical layer.

In another embodiment of the invention a handheld is provided, wherein the commissioning network is provided by a wireless handheld. In view of this disclosure and invention the term "handheld" is synonymously used for all type of handheld devices or handheld computer, in particular mobile computers and/or mobile phones and /or cell phones and or smart phones and /or PDA´s and /or handhelds or handheld organizers and or tablet computer, whereas a handheld is a relatively small hand-held computing device with an operating system and a power supply, in particular a battery or rechargeable accumulator power source.

In a further refinement IR (infrared) or RFID (radio frequency identification) connections and near-range communication is supported by the device according to the invention, wherein a handheld or an engineering client is equipped with a corresponding interface and accordingly information can be exchanged securely.

Furthermore, a RFID key storage may be provided, wherein an RFID chip stores the join key. This key can, contrary to WirelessHART, be read from the chip but only from about half a meter of distance, what still seems to be very secure, in particular in view of the risk of tapping or interception. Presuming that the RFID chip still works even in a damaged device, device exchange on location is possible without any connection to the device management system; the handheld can read the key from the old device and download it into the replacement device.

In a further refinement a key storage device for dedicated key storage and/or generation is provided, which contains a storage unit for a number of key/device and network IDs and which is connected to the engineering client and the commissioning device respectively, in particular via USB, to receive a list of key/ID triples.

Furthermore, in the field, the respective commissioning engineer may simply walk by each all wireless devices and establish a connection with each at one time, which will automatically cause the download of the key/network ID pair to a device whose ID is in the list.

In essence this could be a USB stick with any of the previously described interfaces at the other end, like in particular FSK, RFID, IR, HMI Port or the like.

In another embodiment a commissioning/maintenance adapter, in particular a "pre-secured portable wireless" connection device, for an HMI Port is provided as commissioning device, comprising a WirelessHART adapter equipped with an HMI interface so it can be plugged directly onto the device to provide wireless connectivity during commissioning or maintenance.

Furthermore, to be actually able to efficiently use the commissioning adapter, the FDT DTM (Field Device Tool Device Type Manager) for the gateway allows and/or causes the assignment of a roaming role or function to any adapter connected to an FDK or FSK modem. Such a roaming adapter is never associated permanently with a device, which is contrary to the bulk commissioning of adapters, where this is the intended behavior.

Said roaming adapter avoids the need for a handheld when distributing join keys to wireless devices, in particular wireless devices which have their own wireless connection once they have received the keys and/or in hybrid plants, where only some devices use wireless communication technologies, to parameterize the wired devices in the same way as the wireless ones.

According to the invention a secure connectivity over unsecure channels for all variants of key distribution and device parameterization is provided, using either standardized interfaces or the ABB HMI interface.

The commissioning adapter may be used for configuring a wired or wireless device wirelessly. In a further refinement the commissioning adapter is equipped with at least two interfaces, in particular comprising a wirelessHART- and a FSK- interface. The commissioning adapter communicates with the wirelessHART gateway using the wirelessHART interface and device, which needs to be configured, using FSK interface.

The commissioning adapter provides more flexibility and mobility for remotely device configuration and secure handing of network credentials. An exemplary setup is shown in Fig. 1.

In a further embodiment the commissioning adapter is acting in a similar way like the other WirelessHART field devices. It joins the wirelessHART network in the same manner as specified in wirelessHART standard. After joining the network it will be used as remote device configurator.

The device which needs to be commissioned should have connection with commissioning adapter via FSK interface as exemplarily shown in figure 1.

From the engineering workplace the device commissioning related commands can be sent to the commissioning adapter via the wirelessHART Gateway. After receiving the commissioning command, the commissioning adapter will start the device commissioning operation and will send back the command execution result to the engineering workplace via response message.

To provide more extensibility, in a further refinement the commissioning adapter can have at least one of a RFID- or IR- HMI-Port or a combination thereof to establish or provide a connection to the field device which needs to be commissioned.

In advantage, by means of a commissioning adapter a secure network credentials handling may be provided, wherein from an engineering workplace the distribution of device network credentials is initiated and executed in a completely secure manner.

Advantageously a remote device diagnostic and troubleshooting operation is performed, wherein the commissioning adapter diagnoses the field device on the site location and sends the diagnostic information remotely to the network manager.

Furthermore, according to the commissioning adapter, there is no need to change the standard, which in deed means that no changes are required in WirelessHART stack to perform commissioning adapter operation.

Moreover, an easy commissioning is provided by means of the commissioning adapter because device commissioning workflow will be easy as there is no need to use a handheld device for importing/exporting device credentials.

Accordingly the join time of a device may be reduced and/or minimized.

In another embodiment the radio transmissions in the physical layer are influenced without any modification to the field device to restrict the transmissions to a secure area. This is done by various means and at least one of setting transmission power to a level sufficiently high for local communication but low enough so communication cannot be overheard from outside of the commissioning area; encasing at least the antenna, if not the entire device, of device and gateway in a common, shielded housing; restricting the radio direction of device and gateway by shields/reflectors which are not part of the device but for the gateway may be part of a static gateway setup.

The required interaction by the respective user according to the invention is a simple plug & play. Compared to a state-of-the-art handheld no manual parameterization task is needed, no knowledge of join keys is required. By integrating the secure connectivity with the DCS engineering clients, the join keys never need to be exposed or disclosed to a user.

Furthermore, the invention relates to a method for a secure exchange of sensitive information of technical equipment, in particular by use of a system according to the invention as described above, whereas a secure wireless communication between at least two components and/or devices, in particular field devices, is provided and established by using communication means to ensure a secure near-range communication, in particular by restricting communication signals to a secure area and determining if a device is within a certain area and allow communication if it is or refuse to communicate if it is not, without the need to use higher protocol layers, like in particular authentication or encryption functionalities.

Furthermore, to ensure security of the wireless communication properties of a physical layer and/or link layer and/or measurements are processed.

In a further refinement, device identification information is used to determine the trustworthiness of a communication partner.

In a further refinement, a verification step is executed by a human to yet increase the attained level of security.

In another embodiment the radio transmissions in the physical layer are influenced without any modification to the field device to restrict the transmissions to a secure area. As disclosed above, this is done by various means and at least one of setting transmission power to a level sufficiently high for local communication but low enough so communication cannot be overheard from outside of the commissioning area; encasing at least the antenna, if not the entire device, of device and gateway in a common, shielded housing; restricting the radio direction of device and gateway by shields/reflectors which are not part of the device but for the gateway may be part of a static gateway setup.

In a further embodiment the method for a secure exchange of sensitive information of technical equipment is applied to a commissioning network with a wireless gateway

and uses a well-known Network ID and a shared Join Key wherein the devices joined in this network are visible to the respective Communication DTM (device type manager) for the wireless gateway in the same manner as devices connected to an FSK (Frequency Shift Keying) modem, thus any such device may be assigned to the target network, in particular by a commissioning engineer, and to secure this process, the identification information, in particular the device type, the manufacturer, the serial number or the like, or the device proximity to the commissioning network can be used by man or machine to check the legitimacy of the device; the latter is achieved by evaluating receive signal levels and used transmission energy. FSK defines a common frequency modulation technique.

In a further embodiment this commissioning network can be shared between all Communication DTMs and/or FDIs and/or communication servers, wherein device assignment is a manual task and accordingly not more than one such DTM or FDI or communication server might be opened at a time and communicates with the gateway.

Furthermore, as part of decommissioning a device a reset of the Network ID and Join Key to the well-known values, a so called soft reset, is provided.

Generally, it is proposed to support a "hard reset of the security data" to the default values using e.g. magnetic pins at the HMI to initiate and execute the reset procedure and function.

In another embodiment of the invention a handheld is provided, wherein the commissioning network is provided by a wireless handheld. In view of this disclosure and invention the term "handheld" is synonymously used for all type of handheld devices or handheld computer, in particular mobile computers and/or mobile phones and /or cell phones and or smart phones and /or PDA´s and/or handhelds or handheld organizers and or tablet computer, whereas a handheld is a relatively small hand-held computing device with an operating system and a power supply, in particular a battery or rechargeable accumulator power source.

In a further refinement IR (infrared) or RFID (radio frequency identification) Connections and near-range communication is supported by the device according to the invention, wherein a handheld or an engineering client is equipped with a corresponding interface and accordingly information can be exchanged securely.

Furthermore, a RFID key storage may be provided, wherein an RFID chip stores the join key. This key can, contrary to WirelessHART, be read from the chip but only from about half a meter of distance, what still seems to be very secure, in particular in view of the risk of tapping or interception. Presuming that the RFID chip still works even in a damaged device, device exchange on location is possible without any connection to the device management system; the handheld can read the key from the old device and download it into the replacement device.

In a further refinement a number of key/device and network IDs may be retrieved and accessed via a key storage, for example acommissioning and/or handheld device for dedicated key storage and/or generation, which contains a storage unit for said key/device and network ID´s and which is connected to the engineering client to receive a list of key/ID triples.

Furthermore, in the field, a connection with each wireless device may be established at one time, which will automatically initiate and cause the download of the key/network ID pair to a device whose ID is the list.

In essence this key storage/commissioning device or handheld could be a USB stick with any of the previously described interfaces at the other end, like in particular FSK, RFID, IR, HMI Port or the like.

In another embodiment a commissioning/maintenance adapter, in particular a "pre-secured portable wireless" connection device, for a maintenance port is provided, comprising a WirelessHART adapter equipped with an FSK interface so it can be

plugged directly onto the device to provide wireless connectivity during commissioning or maintenance.

Furthermore, to be actually able to efficiently use the commissioning adapter, the FDT DTM (field device tool device type manager) for the gateway allows and/or causes the assignment of a roaming role or function to any adapter connected with an FSK interface. Such a roaming adapter is never associated permanently with a device, it is only used for field device (re)commissioning purpose where this is the intended behavior.

Said roaming adapter avoids the need for a handheld when distributing join keys to wireless devices, in particular wireless devices which have their own wireless connection once they have received the keys and/or in hybrid plants, where only some devices use wireless communication technologies, to parameterize the wired devices in the same way as the wireless ones.

According to the invention a secure connectivity over unsecure channels for all variants of key distribution and device parameterization is provided, using either standardized interfaces or the ABB HMI interface.

The required interaction by the respective user according to the invention is a simple plug & play. Compared to a state-of-the-art handheld no manual parameterization task is needed, no knowledge of join keys is required. By integrating the secure connectivity with the DCS (distributed control system) engineering clients, the join keys never need to be exposed or disclosed to a user.

The further disclosure and explanation of the invention as well as advantageous embodiments and further developments are presented according to at least one illustrative embodiment.

The figure 1 discloses a commissioning system for a secure exchange of sensitive information of technical equipment by use of at least one wireless connection comprising communication means which provide or include a commissioning network, wherein said dedicated commissioning network uses a well-known Network ID and a shared Join Key and which network is not used for any production purpose whatsoever, and wherein the devices 1,4,6,8, joined in this network are visible to the integration component for the wireless network or gateway such as a communication DTM (device type manager) or FDI gateway or communication device package instance for the WirelessHART Gateway 1 in the same manner as devices connected to an FSK (frequency shift keying) modem, thus any such device may be assigned to the target network, in particular by a commissioning engineer.
To secure and simplify this process, the commissioning system for a secure exchange of sensitive information of technical equipment according to the exemplary embodiment of figure 1 comprises at least three field devices 4,6,8 and communication means to secure a wireless communication without the need to use higher protocol layers, like in particular authentication or encryption functionalities, and an engineering client and/or engineering workplace 2, wherein the communication means comprise a commissioning device and a wireless Hart network as commissioning network comprising a regular WirelessHART gateway 1 which in the wireless management system is integrated like a multi-drop wired modem, wherein a commissioning / maintenance adapter 10 for an HMI Port, in particular an FSK interface 12, is provided as commissioning device, comprising a WirelessHART adapter so it can be plugged directly onto the respective field device 4 to provide wireless connectivity during commissioning and/or maintenance, so that no join key or network credentials have to be exchanged.

Accordingly the commissioning adapter 10 may be used for configuring a wired or wireless device wirelessly, wherein the commissioning adapter is equipped with at least two interfaces, in particular comprising a WirelessHART- and a FSK- interface 12, wherein the commissioning adapter 10 communicates with the WirelessHART gateway 1 of the commissioning network using the WirelessHART interface and with the respective field device 4, which needs to be configured and/or commissioned using the FSK interface 12.

Furthermore, the commissioning adapter 10 is acting in a similar way like the other WirelessHART field devices and joins the WirelessHART network in the same man-

ner as specified in WirelessHART standard, wherein after joining the network it will be used as remote device configurator, wherein device commissioning related commands may be send to the commissioning adapter via the commissioning network gateway and in particular the WirelessHART gateway and wherein after receiving the commissioning command, the commissioning adapter will start the device commissioning operation and will send back the command execution result to the engineering workplace via response message.

By means of the commissioning adapter a secure network credentials handling may be provided, wherein from the engineering workplace the distribution of device network credentials is initiated and executed in a completely secure manner.

Furthermore, a remote device diagnostic and troubleshooting operation is performed by the commissioning adapter, wherein the commissioning adapter diagnoses the field device on the site location and sends the diagnostic information remotely to the respective network manager.

According to the method for a secure exchange of sensitive information of technical equipment, in particular by means of a pre-described commissioning system, for a secure exchange of sensitive information of technical equipment comprising at least two components and/or devices, in particular field devices, using communication means to secure a wireless communication without the need to use higher protocol layers, like in particular authentication or encryption functionalities, wherein a commissioning network, in particular a commissioning network comprising a regular wireless gateway which in the wireless management system is integrated like a multidrop wired modem, and a commissioning device is provided, wherein the commissioning device is connected to the field device which has to be commissioned and is connected to the commissioning network so that information can be exchanged and communication can be established between the at least one field device and the commissioning device and/or commissioning network securely, in particular to exchange one or more join keys and/or ID triples and/or commissioning commands and/or parameters.

Moreover the commissioning network is shared between all Communication DTMs, wherein device assignment is a manual task and accordingly not more than one such DTM might be opened at a time and communicates with the gateway.

The present invention also comprises any combination of preferred embodiments as well as individual features and developments provided they do not exclude each other.

Claims

1. Commissioning system for a secure exchange of sensitive information for the commissioning and/or configuring of technical equipment comprising at least two components and/or devices, in particular field devices using communication means to secure a wireless communication, in particular without the need to use higher protocol layers like in particular authentication or encryption functionalities, wherein the communication means comprise a commissioning device and a commissioning network, in particular a commissioning network comprising a regular wireless gateway which in the wireless management system is integrated like a multi-drop wired modem, and/or a key storage device for dedicated join key storage and/or generation is provided, which key storage device comprises a storage unit for a number of key/device and network IDs and is connectable to an engineering client and/or the commissioning device via a wired or wireless short range connection, in particular a handheld and/or USB stick with at least one of a FSK-, RFID-, IR-interface or HMI Port or the like, to receive and/or store one or more join keys and/or ID triples and/or commissioning commands and/or parameters.

2. System according to claim 1, characterized in that the commissioning network is shared between all Communication DTMs and/or FDIs and/or communication servers, wherein device assignment is a manual task and accordingly not more than one such DTM or FDI or communication server might be opened at a time and communicates with the gateway.

3. System according to one of the preceding claims, characterized in that a device is provided which initiates and/or executed a reset of the Network ID and Join Key to the well-known values, a so called soft reset.

4. System according to one of the preceding claims, characterized in that a device is provided which supports and initiates and/or executes a "hard reset of the security data" to the default values using e.g. magnetic pins at the respective HMI.

5. System according to one of the preceding claims, characterized in that a handheld is provided as commissioning device wherein the commissioning network is provided by said handheld.

6. System according to one of the preceding claims characterized in that the at least one field device provides an IR or RFID interface and/or connection and supports near-range communication, wherein the commissioning device, in particular a handheld or an engineering client, comprises a corresponding interface, so that information can be exchanged and communication can be established between the at least one field device and the commissioning device securely.

7. System according to one of the preceding claims, characterized in that a RFID key storage as key storage device is provided, wherein an RFID chip on the respective device stores the join key, which can be accessed and/or read and processed by a short-range connection by means of the commissioning device and/or key storage device, wherein during commissioning the commissioning network join key from an old field device may be accessed/ read and downloaded into a new replacement device.

8. System according to one of the preceding claims 1 to 4, characterized in that a WirelessHART network as commissioning network and a commissioning / maintenance adapter for an HMI Port, in particular a USB port or interface, is provided as commissioning device, comprising a WirelessHART adapter equipped with at least one of a RFID- or IR- HMI-Port or interface, so it can be plugged directly onto the respective field device to provide wireless connectivity during commissioning and/or maintenance, so that no join key or network credentials have to be exchanged. .

9. System according to claim 8, characterized in that to efficiently use the commissioning adapter, the FDT DTM for the commissioning network gateway allows and/or causes the assignment of a roaming role or function to any adapter connected

to an FSK modem, wherein such a roaming adapter is never associated permanently with a device.

10. System according to one of the preceding claims 8 or 9, characterized in that commissioning adapter may be used for configuring a wired or wireless device wirelessly, wherein the commissioning adapter is equipped with at least two interfaces, in particular comprising a wirelessHART- and a FSK- interface.

11. System according to claim 10, characterized in that the commissioning adapter communicates with a wirelessHART gateway of the commissioning network using the wirelessHART interface and a respective field device, which needs to be configured, by using a FSK interface.

12. System according to one of the preceding claims 8 to 10, characterized in that the commissioning adapter is acting in a similar way like the other wirelessHART field devices and joins the wirelessHART network in the same manner as specified in wirelessHART standard, wherein after joining the network it will be used as remote device configurator.

13. System according to one of the preceding claims 8 to 12, characterized in that the device commissioning related commands can be sent to the commissioning adapter via the commissioning network gateway and in particular the wirelessHART gateway and wherein after receiving the commissioning command, the commissioning adapter will start the device commissioning operation and will send back the command execution result to the engineering workplace via response message.

14. System according to one of the preceding claims, characterized in that the commissioning adapter comprises at least one of a RFID- or IR- HMI-Port or interface a combination thereof to establish and provide a connection to the field device which needs to be commissioned.

15. System according to one of the preceding claims 8 to 14, characterized in that by means of the commissioning adapter a secure network credentials handling may be provided, wherein from an engineering workplace the distribution of device network credentials is initiated and executed in a completely secure manner.

16. System according to one of the preceding claims 8 to 15, characterized in that a remote device diagnostic and troubleshooting operation is performed by the commissioning adapter, wherein the commissioning adapter diagnoses the field device on the site location and sends the diagnostic information remotely to the respective network manager.

17. Method for a secure exchange of sensitive information of technical equipment, in particular by means of a system according to claims 1 to 16, for a secure exchange of sensitive information for the commissioning and/or configuring of technical equipment comprising at least two components and/or devices, in particular field devices, using communication means to secure a wireless communication, in particular without the need to use higher protocol layers like in particular authentication or encryption functionalities, wherein a commissioning network, in particular a commissioning network comprising a regular wireless gateway which in the wireless management system is integrated like a multi-drop wired modem, and a commissioning device is provided, wherein the commissioning device is connected to the field device which has to be commissioned and is connected to the commissioning network so that information can be exchanged and communication can be established between the at least one field device and the commissioning device and/or commissioning network securely, in particular to exchange one or more join keys and/or ID triples and/or commissioning commands and/or parameters.

18. Method according to claim 17, characterized in that the commissioning network is shared between all Communication DTMs and/or FDIs and/or communication servers, wherein device assignment is a manual task and accordingly not more than one such DTM or FDI or communication server might be opened at a time and communicates with the gateway.

19. Method according to one of the preceding claims 17 or 18, characterized in that a reset of the Network ID and Join Key to well-known values, a so called soft reset, may be initiated and/or executed.

20. Method according to one of the preceding claims 17 to 19, characterized in that a "hard reset of the security data" to the default values, in particular by using magnetic pins at the respective HMI, may be supported and initiated and/or executed.

21. Method according to one of the preceding claims 17 to 20, characterized in that the near-range communication is provided and supported between the respective field device and the commissioning device, so that information can be exchanged and communication can be established between the at least one field device and the commissioning device securely.

22. Method according to one of the preceding claims 17 to 21, characterized in that join key information are accessed and/or read from a key storage on the field device which has to be commissioned, in particular an RFID key storage, by use of a short-range connection, wherein during commissioning the commissioning network join key from an old field device may be accessed/ read and downloaded into a new replacement device.

23. Process automation system comprising a commissioning system according to one of the preceding claims 1 to 16.

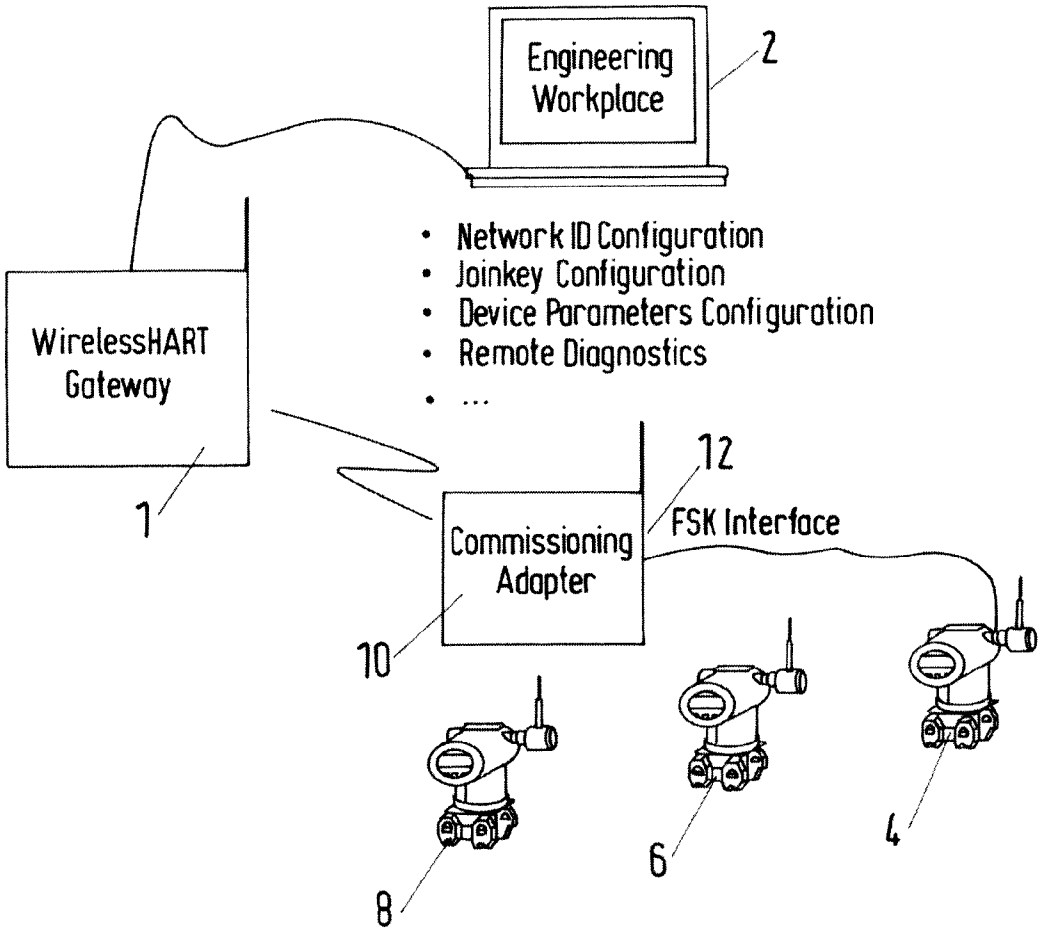
Engineering Workplace
2
• Network ID Configuration
• Joinkey Configuration
• Device Parameters Configuration
• Remote Diagnostics
• ...
WirelessHART Gateway
1
12
FSK Interface
Commissioning Adapter
10
8
6
4

Fig.1

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/003657

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L12/24 H04W12/04 G05B19/418
ADD. H04W84/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W G05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/290351 A1 (TOEPKE TODD MITCHELL [US] ET AL) 18 November 2010 (2010-11-18) paragraph [0009] paragraphs [0017] - [0034]; figures 1,7 -----	1-23
X	US 2012/237034 A1 (KARSCHNIA ROBERT J [US] ET AL) 20 September 2012 (2012-09-20) paragraphs [0016] - [0018] paragraphs [0023] - [0031] paragraphs [0043] - [0053] ----- -/--	1-6, 17-21,23

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 May 2014	03/06/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Ruiz Sanchez, J

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/003657

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Rainer Falk ET AL: "Security Service for the Rollout of Security Credentials in Ubiquitous Industrial Automation Environments", Service Computation 2010, 21 November 2010 (2010-11-21), pages 104-110, XP055073477, Retrieved from the Internet: URL:http://www.thinkmind.org/index.php?view=article&articleid=service_computation_2010_5_20_20033 [retrieved on 2013-07-30] page 107, right-hand column, last paragraph page 108, right-hand column, line 9 - page 109, right-hand column, line 25	1-6, 17-21,23
A	US 2012/036568 A1 (KODAMA KAZUTOSHI [JP]) 9 February 2012 (2012-02-09) paragraph [0050] paragraphs [0061] - [0093]	1-23
A	EP 2 096 505 A1 (ABB RESEARCH LTD [CH]) 2 September 2009 (2009-09-02) paragraph [0004] paragraphs [0019] - [0021] paragraphs [0027] - [0035]	1-23

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/003657

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010290351 A1	18-11-2010	CA 2762092 A1	18-11-2010
		CA 2837940 A1	18-11-2010
		CN 102356366 A	15-02-2012
		CN 102356618 A	15-02-2012
		EP 2430503 A2	21-03-2012
		EP 2430815 A2	21-03-2012
		EP 2605099 A2	19-06-2013
		JP 5399554 B2	29-01-2014
		JP 2012527056 A	01-11-2012
		JP 2012527059 A	01-11-2012
		RU 2011151063 A	20-06-2013
		RU 2011151099 A	20-06-2013
		US 2010290351 A1	18-11-2010
		US 2010290359 A1	18-11-2010
		US 2014036712 A1	06-02-2014
		WO 2010132761 A2	18-11-2010
		WO 2010132799 A2	18-11-2010
US 2012237034 A1	20-09-2012	CN 101855854 A	06-10-2010
		EP 2213030 A1	04-08-2010
		JP 5400788 B2	29-01-2014
		JP 2011504684 A	10-02-2011
		US 2009125713 A1	14-05-2009
		US 2012237034 A1	20-09-2012
		WO 2009064409 A1	22-05-2009
US 2012036568 A1	09-02-2012	CN 102404310 A	04-04-2012
		EP 2418553 A2	15-02-2012
		JP 5170585 B2	27-03-2013
		JP 2012038145 A	23-02-2012
		US 2012036568 A1	09-02-2012
EP 2096505 A1	02-09-2009	DE 102009010730 A1	01-10-2009
		EP 2096505 A1	02-09-2009
		US 2009224906 A1	10-09-2009