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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 October 2017 (05.10.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/173053 A1

(51) International Patent Classification:
G01R 31/28 (2006.01) *G06F 13/00* (2006.01)
G06F 11/00 (2006.01) *G06F 15/177* (2006.01)
G06F 11/07 (2006.01) *G06F 21/00* (2013.01)

(21) International Application Number:
PCT/US2017/024971

(22) International Filing Date:
30 March 2017 (30.03.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/317,058 1 April 2016 (01.04.2016) US
15/473,037 29 March 2017 (29.03.2017) US

(71) Applicant: DOBLE ENGINEERING COMPANY [US/US]; 85 Walnut Street, Watertown, MA 02472 (US).

(72) Inventor: ALLISON, Jason, Alexander; 343 Brockelman Road, Lancaster, MA 01523 (US).

(74) Agent: WONG, Frankie; Brinks Gilson & Lione, P.O. Box 10087, Chicago, IL 60610 (US).

(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, DJ, 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, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, ST, 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).

Published:

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

(54) Title: A SECURED METHOD FOR TESTING AND MAINTENANCE OF BULK ELECTRICAL SYSTEMS (BES) ASSETS

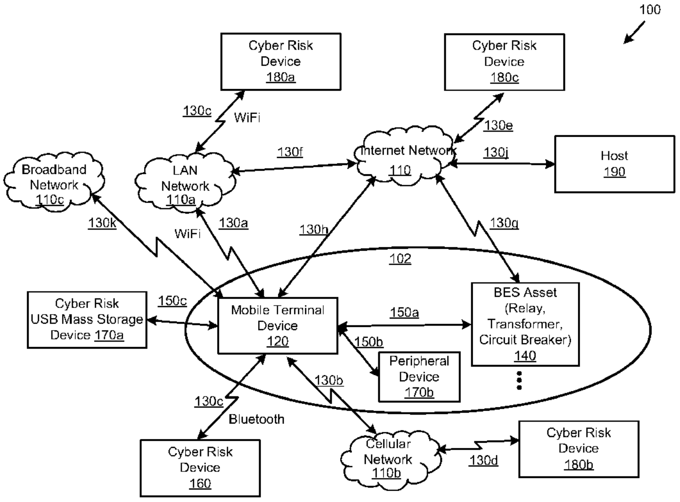

Figure 1

(57) **Abstract**: A method for protecting a mobile terminal device from cyber security threats, including the steps of: detecting that the mobile terminal device is successfully connected only through one or both of a selected physical serial interface connected to a device for facilitating the testing or a wired network interface, which is connected to an electrical utility device. Prior to executing a test routine by the mobile terminal device, switching the mobile terminal device to a test state by: disabling an internal firewall, disabling one or more remaining network interfaces and serial interfaces, such that existing communications or connections are terminated and new communications and connections are prevented. Enabling communication to one or both of the selected physical serial interface and the wired network interface, performing the testing on the at least one electrical utility device according to the executed test routines under control of the mobile terminal device until completion.

A SECURED METHOD FOR TESTING AND MAINTENANCE OF BULK ELECTRICAL SYSTEMS (BES) ASSETS

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Non-Provisional Application No. 15/473,037, filed March 29, 2017, which claims priority to U.S. Provisional Application No. 62/317,058, filed April 1, 2016, the contents of which are incorporated by reference in their entirety.

[0002]

FIELD OF THE TECHNOLOGY

[0003] The present application relates to cyber security protection to a mobile terminal which is configured to perform testing and maintenance of a Bulk Electrical Systems (BES) asset in a substation.

BACKGROUND

[0004] Bulk Electrical Systems (BES) assets (i.e., a power transformer, a current transformer, a circuit breaker, a recloser, a relay, a transformer bushing, a coupling capacitor and a surge arrester etc.) in the electrical utilities industry face significant adversity with cyber security threats and attacks during testing and maintenance test routines run by a mobile terminal which is connected to a network. This adversity creates challenges for the electrical utilities industry which strives to implement secure but reasonable technology policies and practices for field technicians, who manage and test electrical subsystems assets with a mobile terminal which is a microprocessor-based device having one or more communication interfaces.

[0005] For example, any mobile terminal which is installed with an electrical utility test software configured for testing a BES asset (or any electrical device) may be exposed to risks of cyber-attacks, thus may be unable to meet the cyber security requirements as defined by the North American Electric Reliability Corporations Critical Infrastructure

Protection (NERC CIP) standards in the electrical utilities substations.

SUMMARY

[0006] Disclosed below are a method, a mobile terminal device and a non-transitory computer-readable storage medium for protecting a mobile terminal from risks of cyber-attacks for performing testing on a Bulk Electrical Systems (BES) asset (or any electrical device).

[0007] A first embodiment is directed to a method for protecting a mobile terminal device from cyber security threats when performing testing on an electrical utility device. The method includes configuring the mobile terminal device to perform the steps of: executing by at least a processor in the mobile terminal device, test routines instruction code stored in a non-transitory memory to configure the mobile terminal device to perform testing on at least one electrical utility device, wherein the mobile terminal device is configured to: detect that the mobile terminal device is successfully connected only through one or both of a selected physical serial interface and a wired network interface, wherein the selected physical serial interface is connected to a device for facilitating the testing or to another electrical utility device under test and the wired interface is connected to the at least one electrical utility device. Prior to executing a test routine by the mobile terminal device, switching the mobile terminal device to a test state by performing within the mobile terminal device in any sequence, the following: disabling an internal firewall of the mobile terminal device, disabling communication to one or more remaining network interfaces, and disabling connection to one or more remaining unselected physical serial interface for plug-in device port, such that existing communications or connections are terminated and new communications and connections are prevented. The method also includes enabling communication to only one or both of the selected physical serial interface and the wired network interface; and performing the testing on the at least one electrical utility device according to the executed test routines under control of the mobile terminal device until completion.

[0008] The method may further include: upon detecting the completion of the testing on the at least one electrical utility device, switching the mobile terminal device to a network state by performing within the mobile terminal device in any sequence, the following: disabling communication to the one or both of the selected physical serial interface and the wired network interface; enabling the internal firewall of the mobile terminal device, such that new communications or connections are permitted; selecting at least one network interface from among the disabled one or more remaining network interfaces to enable new communications, while keeping unselected one or more remaining network interface and the one or more remaining unselected physical serial interface for plug-in device port disabled; and changing a state mode on a display on the mobile terminal device from the test state to a network state while continue disabling communication to the one or both of the selected physical serial interface and the wired network interface, unless successful connection of one or both of the selected physical serial interface or the wired network interface between the mobile terminal device to the one or both of the device for facilitating the testing or to another electrical utility device under test and the at least one electrical utility device has been detected, wherein the test state mode on the mobile terminal device is being restored.

[0009] A second embodiment is directed to a mobile terminal device that is configured to be protected from cyber security threats when connected to an electrical utility device under test. The mobile terminal device may include a processor. The processor executes test routines instruction code stored in a non-transitory memory. When the processor executes the instruction code, the processor configures the mobile terminal device to perform testing on at least one electrical utility device. In particular, the mobile terminal device is configured to detect that the mobile terminal device is successfully connected only through one or both of a selected physical serial interface and a wired network interface, wherein the selected physical serial interface is connected to a device for facilitating the testing or to another electrical utility device under test and the wired interface is connected to the at least one electrical utility device. Prior to executing a test routine by the mobile terminal device, switch the mobile terminal device to a test state by performing in any sequence, the following: disable an internal firewall of the mobile terminal device, disable communication to one or more remaining network interfaces, and disable connection to one or more remaining unselected physical serial interface for plug-in device port, such that existing communications or connections are terminated and new communications and connections are prevented;enable communication to only one or both of the selected physical serial interface and the wired network interface; and perform the testing on the at least one electrical utility device according to the executed test routines under control of the mobile terminal device until completion.

[0010] A third embodiment is directed to a non-transitory computer-readable storage medium for protecting a mobile terminal device from cyber security threats having stored thereon, a computer program having at least one test routine code section when being executable by at least a processor in the mobile terminal device, configuring the mobile terminal device to: detect that the mobile terminal device is successfully connected only through one or both of a selected physical serial interface and a wired network interface, wherein the selected physical serial interface is connected to a device for facilitating the testing or to another electrical utility device under test and the wired interface is connected to the at least one electrical utility device. Prior to executing a test routine by the mobile terminal device, switching the mobile terminal device to a test state by performing within the mobile terminal device in any sequence, the following: disabling an internal firewall of the mobile terminal device, disabling communication to one or more remaining network interfaces, and disabling connection to one or more remaining unselected physical serial interface for plug-in device port, such that existing communications or connections are terminated and new communications and connections are prevented. The method also includes enabling communication to only one or both of the selected physical serial interface and the wired network interface; and performing the testing on the at least one electrical utility device according to the executed test routines under control of the mobile terminal device until completion.

[0011] Executing the program codes stored in the non-transitory computer-readable storage medium in the mobile terminal device may protect the mobile terminal from cyber security threats through opened cyber space during testing. A person of ordinary skill in the art would recognize that other electrical devices not classified within the utility power device category may also be protected from cyber-attacks when connected to the mobile terminal device using the described method and system for testing. The steps disclosed in the method may be carried out in modified sequences to suit the electrical device test routine.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The accompanying drawings are included to provide a further understanding of the claims, are incorporated in, and constitute as part of this specification. The detailed description and illustrated embodiments described serve to explain the principles defined by the claims.

[0013] Fig. 1 illustrates an exemplary system block diagram illustrating a mobile terminal device performing a test or maintenance task on a BES asset (electrical utility device) in presence of a network environment, according to an embodiment.

[0014] Fig. 2A illustrates the mobile terminal device switching to a “Test State” mode prior to performing testing or maintenance task on a BES asset, according to an embodiment.

[0015] Fig. 2B illustrates the mobile terminal device switching to a “Network State” mode after performing testing or maintenance task on a BES asset, according to an embodiment.

[0016] Fig. 3A illustrates the exemplary steps carried out in the mobile terminal device when switching to a “Test State” mode prior to performing testing or maintenance task on a BES asset, according to an embodiment.

[0017] Fig. 3B illustrates the exemplary steps carried out in the mobile terminal device when switching to a “Network State” mode after performing testing or maintenance task on a BES asset, according to an embodiment.

[0018] Fig. 4 illustrates an exemplary mobile terminal device for performing a test or maintenance task on a BES asset, according to an embodiment.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0019] The various embodiments of the present disclosure are further described in details in combination with attached drawings and embodiments below. It should be understood that the specific embodiments described herein are used only to explain the present disclosure, and should not be construed as a limitation on the claims. Similar features may be referenced back to the prior descriptions in a prior numbered drawing or referenced ahead to a higher numbered drawing.

[0020] Exemplary testing methods and exemplary devices used to facilitate the testing of the BES asset (140) in this disclosure may be provided in details by referring to Doble Engineering's U.S. Application No. 15/457,491 titled "METHOD AND SYSTEM OF APPARATUSES FOR TESTING UTILITY POWER DEVICES" filed on March 13, 2017, to U.S. Application 15/279,032 titled "METHOD AND APPARATUS FOR TESTING UTILITY POWER DEVICES" filed on September 28, 2016, and to U.S. Patent No. 9,482,712 issued on November 1, 2016. The content of which are incorporated herewith by reference.

[0021] Fig. 1 illustrates an exemplary system block diagram (102) illustrating a mobile terminal device (120) performing a test or maintenance task on at least one BES asset (140) (i.e., electrical utility device) in presence of a network environment (100), according to an embodiment. Fig. 4 illustrates an exemplary mobile terminal device for performing a test or maintenance task on the at least one BES asset (140), according to an embodiment. It should be pointed out that more than one BES asset (140) may be simultaneously controlled and tested by the same mobile terminal device (120) through connecting multiple wired network interfaces or in combination with connecting through a selected physical serial interface.

[0022] To help understanding of the described method and operations of the mobile terminal device (120 or 400), Figs. 1 and 4 will both be referred in the following description. Referring to Fig. 4, the mobile terminal device (400) (see Fig. 4) may be a standard portable computing device including at least a CPU processor (420), a memory (440), and a network interface card (460) (see Fig. 4) capable of connecting to one or more respective networks (Internet (110), LAN (110a), Broadband (110c), Cellular (110b), Bluetooth®) LAN through wired connection (130h) or wireless connections (130a, 130b, 130c), through respective COM ports (460a to 460n). The memory (440) may store an operating system (OS) (410), a plurality of applications

(412) and an electrical utility test software (controller program (430)) (see Fig. 4).

[0023] Test routines to various BES assets may be written as executable program codes in a controller program (430), which may be stored on a non-transitory computer-readable storage medium in a mobile terminal device's local memory (440) (such as a ROM, a flash memory, local solid state hard drive) or may be downloaded from a network, from an external USB class mass storage device (170a) (such as a USB flash memory, an optical readable Compact Disc Rom (CD ROM), an external hard disk, or from an external solid state hard drive using a USB interface, to name a few). The executable program codes in the controller program (430)) when executed by the processor (420), may configure the mobile terminal device (400) to carry out the operations under an instrumented finite-state machine (see Figs. 2A-2b, 3A-3B) in either a "Test state" mode or in a "Network state" mode when perform testing on a BES asset (140).

[0024] The mobile terminal device (400) may include one or more communication ports (see Fig. 4, COM Port 1 (460a) ... COM Port n (460n)) for carrying out one or both of wired and wireless network interface connections, and serial interface connections with USB class plugged-in devices. For example, the COM Port 1 (460a) on the mobile terminal device (400) may be a wired network interface (150a) and COM Port 2 (460b) may be connected to a physical serial interface (150b). The wired interface (150a) of COM Port 1 (460a) may be an Ethernet interface and any suitable physical serial interface connection that communicates bidirectional signals in high data rate under a standard communication protocol. The physical serial interface may be a Universal Serial Bus (USB) interface or any suitable serial interface.

[0025] The mobile terminal device (120) may be a regular computer, a laptop computer, a tablet computer, or a dedicated proprietary testing hardware (such as a Doble Universal Controller DUCTM), having a plurality of communication ports as described in Fig. 4, which runs software programs specifically configured to perform electrical utility tests and maintenance on the BES asset. The BES asset (140) itself however, may have its own wireless interface (130) to communicate with a host (190) through the Internet network (110).

[0026] Referring to Fig. 1, when running a test on at least one BES asset (140), the mobile terminal device (120) may simultaneously be connected to one or both of a wired network interface (150a) and a selected physical serial interface (150b), wherein the wired interface (150a) is connected to the BES asset (140) and the selected physical serial interface (150b) is connected to a device (170b) for facilitating the testing or to another electrical utility device under test. The device (170b) for facilitating the testing may be one or more of: a peripheral device, a voltage source and a switch matrix, and the another electrical utility device may be just another BES asset (140).

[0027] The mobile terminal device (120) may connect to a network environment (100) through one or more remaining communication ports COM Port 3 (460c) to COM Port n (460n). The remaining communication ports COM Port 3 (460c) to COM Port n (460n) may be connected to respective network interfaces or to respective USB class plug-in device ports. The respective network interfaces may form network connections with anyone or more of: an Internet network (110) through wired connections (130f, 130h and 130j) and wireless connections (130e, 130g); a Local Area Network (LAN) (110a) through Wireless Fidelity (WiFi) connections (130a, 130c); a broadband network connection (130k), a cellular network (110b) through 4G/LTE packet data radio connections (130b, 130d), and Bluetooth® connections (130c).

[0028] When the mobile terminal device (120) is connected to the network environment (100) while simultaneously performing the testing and maintenance on the BES asset (140), the mobile terminal device (120) may become a target of cyber-attacks by anyone of the remote cyber risk devices (180a, 180b, 180c, 160) through one or more respective network connections (130a, 130b, 130c, 130h) which may spread computer viruses. Computer viruses may also be introduced through plugging in an infected external plug-in device such as a USB class Mass storage device (170a)) to another physical serial interface connection (150c) of the mobile terminal device (120).

[0029] Computer viruses, also known as malware may exist in various types. One well-known type may be a Trojan horse virus, which may contain files capable of replicating themselves and modifying an infected mobile terminal device's programs. In a scenario, the computer virus may taking over control of the infected mobile terminal device (120) by sending commands through the one or both of the selected physical serial interface (150b) or wired interface (150a) to infect the BES asset (140) under test by programming the BES asset (140) to be turned off when receiving a certain command, or damaging the device (170b) facilitating testing, thus may cause disruptions or instability to the electric power grid.

[0030] It is therefore preferable to prior to testing the BES asset (140), isolate the remaining communication ports and from unselected physical serial interface connections (150c) to COM Port 3 (460c) to COM Port n (460n) of the mobile terminal device (120) from external network connections (110, 110a, 110b) as a precaution to protect the mobile terminal device (120) from potential cyber-attacks, thus meeting the cyber security requirements as defined by the North American Electric Reliability Corporations Critical Infrastructure Protection (NERC CIP) standards in the electrical utilities substations.

[0031] Fig. 2A illustrates the mobile terminal device switching to a "Test State" mode prior to performing testing or maintenance task on a BES asset, according to an embodiment. After detecting that the mobile terminal device (120) is successfully connected only through one or both of a selected physical serial interface (150b) and a wired network interface (150a) (e.g., selecting COM Port 2 to connect to the peripheral serial interface (150b) with the device (170b) and selecting and COM Port 1 to connect to the wired network interface (150a) with the BES asset (140)), and prior to executing a test routine by the mobile terminal device (120), the mobile terminal device (120) is switched to a "Test State" mode by performing all of the following steps: disabling an internal firewall (175) of the mobile terminal device, disabling one or more remaining network interfaces (130a, 130b, 130c), and disabling one or more unselected physical serial interface for plug-in device port (150c) such that existing communications or connections are terminated and new communications and connections are prevented. For example, COM Ports 3 to COM Ports n (see Fig. 4) may be disabled.

[0032] Afterwards, enabling communication to only one or both of the selected physical serial interface (150b) and the wired network interface (150a) between the mobile terminal device (120) and the device (170b) and the BES asset (140) only through the selected physical interface or the wired network interface (150a) at COM Port 1 (460a); and performing the testing on the BES asset (140) according to the executed test routines (i.e., controller program (430) under control of the mobile terminal device (120) until completion.

[0033] The BES asset (140) may be an electrical utility device which may be anyone of: a power transformer, a current transformer, a circuit breaker, a recloser, a relay, a transformer bushing, a coupling capacitor and a surge arrester.

[0034] In an embodiment, the physical interface or wired interface (150a) may be an Ethernet interface and any suitable physical interface connection that communicates bidirectional signals in high data rate under a communication protocol.

[0035] In an embodiment, the existing connections or the new connections to the one or more remaining network interfaces (COM Port 3 to COM Port n) may be connections to anyone of: a local area network (LAN) (110a), a wide area network (WAN) or an Internet (110), a Broadband network (110c), a Cellular network (130b), a Wireless Fidelity (WiFi) network (130a), and a Bluetooth® Network (130c) or to the unselected physical serial interface connection (150c) to a plug-in device such as a Universal Serial Bus (USB) Mass Storage device (170a).

[0036] In an embodiment, the method may include determining of device names, port names, and network names prior to the disabling of one or more remaining network interfaces or one or more unselected physical serial interface for plug-in device such that existing communications or connections are terminated and new communications and connections are prevented. The determination of device names, port names or network names may be according to anyone of: net class devices containing “Ethernet” in name, ports class devices containing “COM” in name, Bluetooth® net class devices containing “Wireless” in name, USB class devices containing “Broadband” in name, USB class devices containing “USB Mass Storage Device” in name, and device Firewall (175) with profile rules to grant or deny Public and Private network connection to allow or prohibit data transfer to and from the mobile terminal device (120).

[0037] To summarize, while in the “Test state” mode, the mobile terminal device (120) will disable the device Firewall (175) to deny permission to internal and external remote connectivity for a purpose of eliminating remote attacks and limiting exposure in the event of a compromised system through a data driven, dynamically configured, least permission model. While in the “Test state” mode the electrical utility field technician may therefore securely perform their duties on the BES assets (140) which are high value substation assets. The mobile terminal device (120) may visually display an indication that it is in the “Test state” mode for a purpose of quickly informing the user of the current state the mobile terminal device is in.

[0038] Fig. 2B illustrates the mobile terminal device switching to a “Network State” mode after performing testing or maintenance task on a BES asset, according to an embodiment. Upon detecting the completion of the test routines on the BES asset (140), the mobile terminal device (120) may be switched to a “network state” mode by performing the following steps: disabling communication to the one or both of the selected physical serial interface (150b) and the wired network interface (150a) such that there is no more communication between the mobile terminal device (120) and the one or both of the BES asset (140) and the device (170b) (device for facilitating the testing or to another electrical utility device under test). Of course, if one chooses to, the communication between the mobile terminal device (120) and the one or both of the BES asset (140) and the device (170b) may be maintained. Enabling the internal firewall (175) of the mobile terminal device (120), such that new communications or connections are permitted for selecting at least one network interface (130a, 130b) from among the disabled one or more remaining network interfaces (130a, 130b, 130c) to enable new communications, while keeping unselected one or more remaining network interface (130c) and the one or more remaining unselected physical serial interface (150c) for plug-in device port disabled. Changing a state mode on a display (450) on the mobile terminal device (120) from the “Test state” to a “Network state” while continue disabling communication (150a) to the one or both of the selected physical serial interface (150b) and the wired network interface (150a), unless successful connection of one or both of the selected physical serial interface (150b) or the wired network interface (150a) between the mobile terminal device (120) to the one or both of the device (170b) for facilitating the testing or to another electrical utility device under test and the at least one BES (140) has been detected, wherein the “Test state” mode on the mobile terminal device (120) is being restored.

[0039] When transitioning out of the “Test state” mode to the “Network state” mode, the user of the mobile terminal device (120) is prompted. While in the “Network state” mode, the Firewall (175) of the mobile terminal device (120) is enabled to secure permission for internal and external remote network connectivity, and the electrical utility field technician is precluded from performing their testing duties on the BES asset (140). This exclusion enhances an emphasis on a defense in depth, least permission model for the purpose of mitigating cyber security threats and attacks. While in the “Network state” mode, the mobile terminal device may visually display that it is in the “Network state” mode.

[0040] Fig. 3A illustrates the exemplary steps carried out in the mobile terminal device when switching to a “Test State” mode prior to performing testing or maintenance task on a BES asset, according to an embodiment. The steps in Fig. 3A may be carried out in any sequence without affecting the overall outcome of the “Test State” mode.

[0041] After the mobile terminal device (120) entered into the “Test State” mode, a wired network interface (150a) such as an Ethernet network interface may be enabled in step 302, and one or more Net class devices containing “Ethernet” in name may be read and registered with a permission to connect to a network or to another device such as the BES asset (140) in Fig. 1 in step 304.

[0042] A communication port for a selected physical serial interface (150b) may be enabled in step 306, and one or more Port class devices containing “COM” in name may be read and registered with permission to connect to another device (170b) such as a peripheral device in step 308 for facilitating the testing or to another electrical utility device under test.

[0043] One or more Bluetooth®wireless network ports (such as Bluetooth® Port (130c) in Fig. 2A) may be disabled in step 310, and one or more Net Bluetooth® class devices containing “Wireless” in name may be read and registered with no permission to connect to a Bluetooth® network (130c) in Fig. 1 in step 312.

[0044] One or more Broadband wireless network ports (130k) may be disabled in step

314, and one or more USB class devices containing “Broadband” in name may be read and registered with no permission to connect to the Broadband network (110d) in Fig. 1 in step 316.

[0045] One or more remaining unselected physical serial interface for plug-in device port such as a USB class plug-in device port (150c) may be disabled in step 318, and one or more USB class devices containing “USB Mass Storage Device” in name may be read and registered with no permission to connect to the USB Mass Storage device (170a) in Fig. 1 in step 320.

[0046] One or more Bluetooth® wireless device ports may be disabled in step 322, and one or more Bluetooth® class devices containing “Bluetooth®” in name may be read and registered with no permission to connect to a Bluetooth® device (160) in Fig. 1 in step 324.

[0047] A Windows® Firewall (180) may be disabled in step 326, profiles containing rules on granting “Public and Private” network connection may be denied to prohibit transfer of data to and from the mobile terminal device (120) in step 328.

[0048] Fig. 3B illustrates the exemplary steps carried out in the mobile terminal device when switching to a “Network State” mode after performing testing or maintenance task on a BES asset, according to an embodiment. The steps in Fig. 3B may be carried out in any sequence without affecting the overall outcome of the “Network State” mode.

[0049] After the mobile terminal device (120) entered into the “Network State” mode, the wired network interface (150a) such as the Ethernet network interface may be disabled in step 332, such that the one or more Net class devices containing “Ethernet” in name may not be denied permission to connect to the network or to the BES asset (140) in Fig. 1. In another embodiment, the wired network interface (150a) such as the Ethernet network interface may remain enabled in step 332, such that the one or more Net class devices containing “Ethernet” in name may continue to receive permission to connect to the network or to the BES asset (140) in Fig. 1.

[0050] The selected physical serial interface (150b) connected to the device (170b) communication ports (such as COM Port 2 (460b) in Fig. 4) may be disabled in step

334, and the Port class devices containing “COM” in name may be denied permission to connect to the device (170b) such as a peripheral device for facilitating the testing or the another electrical utility device under test device in Fig. 1. In another embodiment, the selected physical serial interface (150b) connected to the device (170b) communication ports (such as COM Port 2 (460b) in Fig. 4) may remain enabled in step 334, and the Port class devices containing “COM” in name may continue to receive permission to connect to the device (170b) such as a peripheral device for facilitating the testing or the another electrical utility device under test device in Fig. 1.

[0051] The one or more Bluetooth®wireless network ports (such as Bluetooth® Port (130c) in Fig. 2A) may be enabled in step 336, and the one or more Net Bluetooth® class devices containing “Wireless” in name may receive permission to connect to a Bluetooth® network (130c) in Fig. 1.

[0052] The one or more Broadband wireless network ports (130k) may be enabled in step 338, and the one or more USB class devices containing “Broadband” in name may receive permission to connect to the Broadband network (110d) in Fig. 1.

[0053] The one or more remaining unselected physical serial interface (150c) for plug-in device port such as the USB class plug-in device port may remain disabled in step 340, and the one or more USB class devices containing “USB Mass Storage Device” in name may not receive permission to connect to the USB Mass Storage device (170a) in Fig. 1.

[0054] The one or more Bluetooth® wireless device ports may remain disabled in step 342, and the one or more Bluetooth® class devices containing “Bluetooth®” in name may not receive permission to connect to a Bluetooth® device (160) in Fig. 1.

[0055] The Windows® Firewall (180) may be enabled in step 346, such that profiles with rules on “Public and Private” network connection may be granted permission to allow transfer data to and from the mobile terminal device (120).

[0056] All or part of the operations described above in the embodiments may be implemented via instruction code/program (430) stored in a non-transitory computer-readable medium such as a memory (440), which may be a ROM/RAM, a magnetic disk, a solid state hard drive, or an optical disk, which may be executed by the processor (420) in a machine, such as in mobile terminal device (120), a computer, a laptop, a server, or cloud computing infrastructure to perform the operations.

[0057] It will be apparent to those skilled in the art that various modifications and variations can be made to the present disclosure without departing from the scope or spirit of the disclosure. In view of the foregoing, it is intended that the present disclosure cover modifications and variations of this disclosure provided they fall within the scope of the following claims and their equivalents.

What is claimed is:

1. A method for protecting a mobile terminal device from cyber security threats, comprising:

executing, by at least a processor in the mobile terminal device, test routines program codes stored in a non-transitory memory to configure the mobile terminal device to perform testing on at least one electrical utility device, wherein the mobile terminal device is configured to detect that the mobile terminal device is successfully connected only through one or both of a selected physical serial interface and a wired network interface, wherein the selected physical serial interface is connected to a device for facilitating the testing or to another electrical utility device under test and the wired interface is connected to the at least one electrical utility device;

prior to executing a test routine by the mobile terminal device, switching the mobile terminal device to a test state by performing within the mobile terminal device in any sequence, the following:

disabling an internal firewall of the mobile terminal device, disabling communication to one or more remaining network interfaces, and disabling connection to one or more remaining unselected physical serial interface for plug-in device port, such that existing communications or connections are terminated and new communications and connections are prevented;

enabling communication to only one or both of the selected physical serial interface and the wired network interface; and

performing the testing on the at least one electrical utility device according to the executed test routines under control of the mobile terminal device until completion.

2. The method according to claim 1, further comprising:

upon detecting the completion of the testing on the at least one electrical utility device, switching the mobile terminal device to a network state by performing within the mobile terminal device in any sequence, the following:

disabling communication to the one or both of the selected physical serial interface and the wired network interface;

enabling the internal firewall of the mobile terminal device, such that new communications or connections are permitted;

selecting at least one network interface from among the disabled one or more remaining network interfaces to enable new communications, while keeping unselected one or more remaining network interface and the one or more remaining unselected physical serial interface for plug-in device port disabled; and

changing a state mode on a display on the mobile terminal device from the test state to a network state while continue disabling communication to the one or both of the selected physical serial interface and the wired network interface, unless successful connection of one or both of the selected physical serial interface or the wired network interface between the mobile terminal device to the one or both of the device for facilitating the testing or to another electrical utility device under test and the at least one electrical utility device has been detected, wherein the test state mode on the mobile terminal device is being restored.

3. The method according to claim 1, wherein the mobile terminal device comprises anyone of: a computer, a laptop computer, a tablet computer, a portable handheld device or a dedicated proprietary testing hardware,

the at least one electrical utility device comprises anyone of: a power transformer, a current transformer, a circuit breaker, a recloser, a relay, a transformer bushing, a coupling capacitor and a surge arrester; and

the device for facilitating the testing comprises one or more of: a voltage source and a switch matrix.

4. The method according to claim 1, wherein the physical serial interface comprises a Universal Serial Bus (USB) interface or any suitable serial interface, and the wired interface comprises an Ethernet interface or any suitable physical interface connection that communicates bidirectional signals under a communication protocol.

5. The method according to claim 1, wherein the existing connections or the new connections to the one or more remaining network interfaces comprises connections to anyone of: a local area network (LAN), a wide area network (WAN) or an Internet, a Cellular network, a Broadband network, a Wireless Fidelity (WiFi) network, and a Bluetooth® Network.

6. The method according to claim 1, wherein the disabled connection to the one or more remaining unselected physical serial interface for plug-in device port comprises anyone of: a Universal Serial Bus (USB) class plug-in device port and a peripheral device port to mass storage devices.

7. The method according to claim 1, comprising determining device names, port names, and network names prior to the disabling of the one or more remaining network interfaces and the one or more remaining unselected physical serial interface for plug-in device port.

8. The method according to claim 6, wherein the determined device names, port names or network names are according to anyone of: net class devices containing “Ethernet” in name, ports class devices containing “COM” in name, Bluetooth® net class devices containing “Wireless” in name, USB class devices containing “Broadband” in name, and USB class devices containing “USB Mass Storage Device” in name.

9. A mobile terminal device, comprising:

at least a processor executing test routines program codes stored in a non-transitory memory to configure the mobile terminal device to perform testing on at least one electrical utility device, wherein the mobile terminal device is configured to:

detect that the mobile terminal device is successfully connected only through one or both of a selected physical serial interface and a wired network interface, wherein the selected physical serial interface is connected to a device for facilitating the testing or to another electrical utility device under test and the wired interface is connected to the at least one electrical utility device;

prior to executing a test routine by the mobile terminal device, switch the mobile terminal device to a test state by performing in any sequence, the following:

disable an internal firewall of the mobile terminal device, disable communication to one or more remaining network interfaces, and disable connection to one or more remaining unselected physical serial interface for plug-in device port, such that existing communications or connections are terminated and new communications and connections are prevented;

enable communication to only one or both of the selected physical serial interface and the wired network interface; and

perform the testing on the at least one electrical utility device according to the executed test routines under control of the mobile terminal device until completion.

10. The mobile terminal device according to claim 9, wherein upon detecting the completion of the test on the at least one electrical utility device, the mobile terminal device is switched to a network state to perform in any sequence, the following:

disable communication to the one or both of the selected physical serial interface and the wired network interface;

enable the internal firewall of the mobile terminal device, such that new communications or connections are permitted;

select at least one network interface from among the disabled one or more remaining network interfaces to enable new communications, while keeping unselected one or more remaining network interface and the one or more remaining unselected physical serial interface for plug-in device port disabled; and

change a state mode on a display on the mobile terminal device from the test state to a network state while continue to keep disabled communication to the one or both of the selected physical serial interface and the wired network interface, unless successful connection of one or both of the selected physical serial interface or the wired network interface between the mobile terminal device to the one or both of the device for facilitating the testing or to another electrical utility device under test and the at least one electrical utility device has been detected, wherein the test state mode on the mobile terminal device is being restored.

11. The mobile terminal device according to claim 9, wherein the mobile terminal device comprises anyone of: a computer, a laptop computer, a tablet computer, a portable handheld device or a dedicated proprietary testing hardware,

the at least one electrical utility device comprises anyone of: a power transformer, a current transformer, a circuit breaker, a recloser, a relay, a transformer bushing, a coupling capacitor and a surge arrester; and

the device for facilitating the testing comprises one or more of: a voltage source and a switch matrix.

12. The mobile terminal device according to claim 9, wherein the physical serial interface comprises a Universal Serial Bus (USB) interface or any suitable serial interface, and the wired interface comprises an Ethernet interface or any suitable physical interface connection that communicates bidirectional signals under a communication protocol.

13. The mobile terminal device according to claim 9, wherein the existing connections or the new connections to the one or more remaining network interfaces comprises connections to anyone of: a local area network (LAN), a wide area network (WAN) or an Internet, a Cellular network, a Broadband network, a Wireless Fidelity (WiFi) network, and a Bluetooth® Network.

14. The mobile terminal device according to claim 9, wherein the disabled connection to the one or more remaining unselected physical serial interface for plug-in device port comprises anyone of: a Universal Serial Bus (USB) class plug-in device port and a peripheral device port to mass storage devices.

15. The mobile terminal device according to claim 9, further configured to determine device names, port names, and network names prior to the disable of the one

or more remaining network interfaces and the one or more remaining unselected physical serial interface for plug-in device port.

16. The mobile terminal device according to claim 15, wherein the determined device names, port names or network names are according to anyone of: net class devices containing “Ethernet” in name, ports class devices containing “COM” in name, Bluetooth® net class devices containing “Wireless” in name, USB class devices containing “Broadband” in name, and USB class devices containing “USB Mass Storage Device” in name.

17. A non-transitory computer-readable storage medium for protecting a mobile terminal device from cyber security threats having stored thereon, a computer program having at least one test routine code section when being executable by at least a processor in the mobile terminal device, configuring the mobile terminal device to perform:

detecting that the mobile terminal device is successfully connected only through one or both of a selected physical serial interface and a wired network interface, wherein the selected physical serial interface is connected to a device for facilitating the testing or to another electrical utility device under test and the wired interface is connected to the at least one electrical utility device;

prior to executing a test routine by the mobile terminal device, switching the mobile terminal device to a test state by performing within the mobile terminal device in any sequence, the following:

disabling an internal firewall of the mobile terminal device, disabling communication to one or more remaining network interfaces, and disabling connection to one or more remaining unselected physical serial interface for plug-in device port, such that existing communications or connections are terminated and new communications and connections are prevented;

enabling communication to only one or both of the selected physical serial interface and the wired network interface; and performing the testing on the at least one electrical utility device according to the executed test routines under control of the mobile terminal device until completion.

18. The non-transitory computer-readable storage medium according to claim 17, further comprising causing the mobile terminal device:

upon detecting the completion of the testing on the at least one electrical utility device, switching the mobile terminal device to a network state by performing within the mobile terminal device in any sequence, the following:

disabling communication to the one or both of the selected physical serial interface and the wired network interface;

enabling the internal firewall of the mobile terminal device, such that new communications or connections are permitted;

selecting at least one network interface from among the disabled one or more remaining network interfaces to enable new communications, while keeping unselected one or more remaining network interface and the one or more remaining unselected physical serial interface for plug-in device port disabled; and

changing a state mode on a display on the mobile terminal device from the test state to a network state while continue disabling communication to the one or both of the selected physical serial interface and the wired network interface, unless successful connection of one or both of the selected physical serial interface or the wired network interface between the mobile terminal device to the one or both of the device for facilitating the testing or to another electrical utility device under test and the at least one electrical utility device has been detected, wherein the test state mode on the mobile terminal device is being restored.

19. The non-transitory computer-readable storage medium according to claim 17, wherein the mobile terminal device comprises anyone of: a computer, a laptop computer, a tablet computer, a portable handheld device or a dedicated proprietary testing hardware,

the at least one electrical utility device comprises anyone of: a power transformer, a current transformer, a circuit breaker, a recloser, a relay, a transformer bushing, a coupling capacitor and a surge arrester; and

the device for facilitating the testing comprises one or more of: a voltage source and a switch matrix.

20. The non-transitory computer-readable storage medium according to claim 17, wherein the physical serial interface comprises a Universal Serial Bus (USB) interface or any suitable serial interface, and the wired interface comprises an Ethernet interface or any suitable physical interface connection that communicates bidirectional signals under a communication protocol.

21. The non-transitory computer-readable storage medium according to claim 17, wherein the existing connections or the new connections to the one or more remaining network interfaces comprises connections to anyone of: a local area network (LAN), a wide area network (WAN) or an Internet, a Cellular network, a Broadband network, a Wireless Fidelity (WiFi) network, and a Bluetooth® Network.

22. The non-transitory computer-readable storage medium according to claim 17, wherein the disabled connection to the one or more remaining unselected physical serial interface for plug-in device port comprises anyone of: a Universal Serial Bus (USB) class plug-in device port and a peripheral device port to mass storage devices.

23. The non-transitory computer-readable storage medium according to claim 17, wherein the mobile terminal device is further configured to perform: determining device names, port names, and network names prior to the disabling of the one or more remaining network interfaces and the one or more remaining unselected physical serial interface for plug-in device port.

24. The non-transitory computer-readable storage medium according to claim 23, wherein the determined device names, port names or network names are according

to anyone of: net class devices containing “Ethernet” in name, ports class devices containing “COM” in name, Bluetooth® net class devices containing “Wireless” in name, USB class devices containing “Broadband” in name, and USB class devices containing “USB Mass Storage Device” in name.

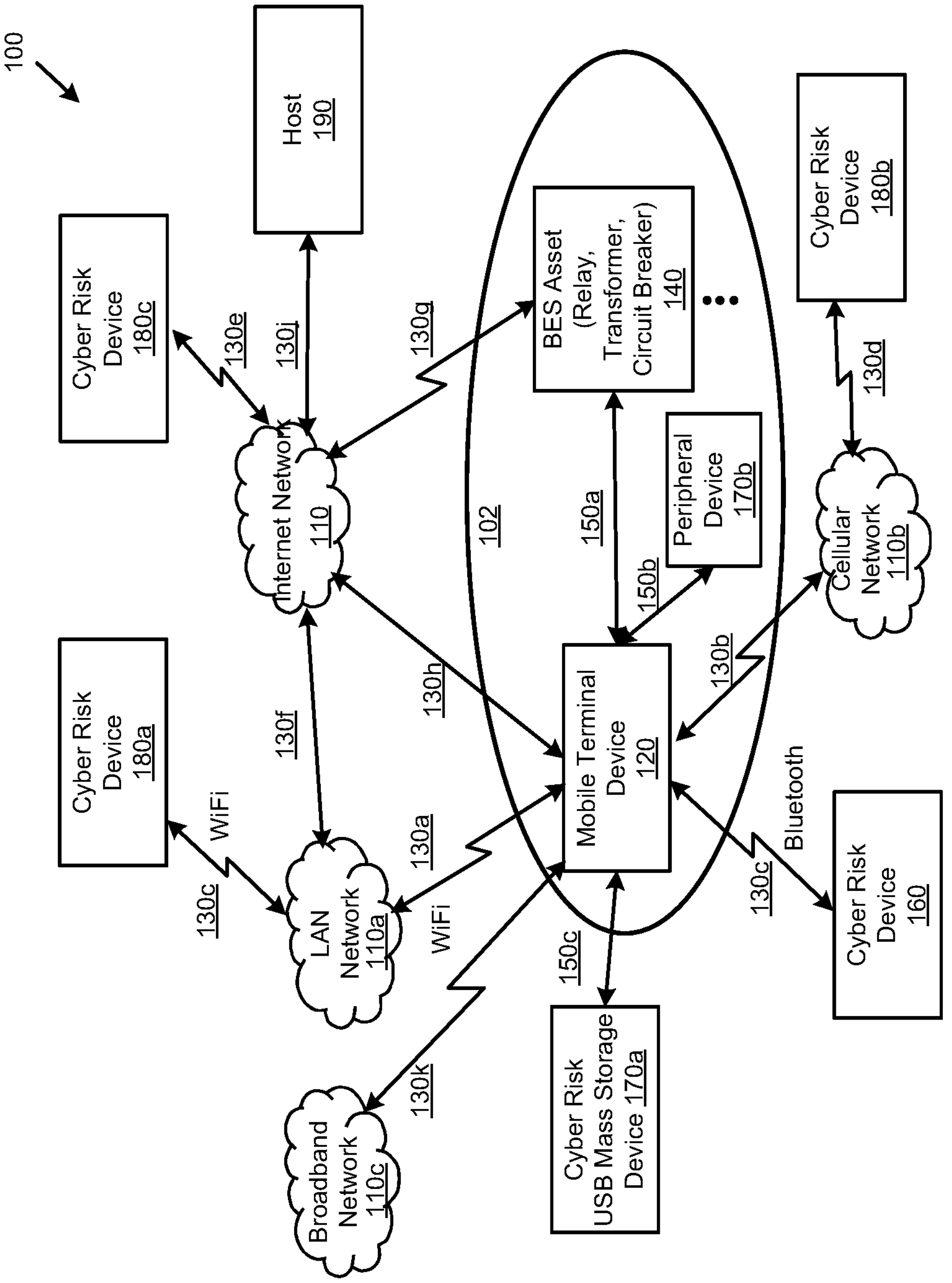
100
Host
190
Cyber Risk
Device
180c
Cyber Risk
Device
180a
Cyber Risk
Device
180b
Cyber Risk
Device
160
Internet Network
110
LAN
Network
110a
Cellular
Network
110b
Broadband
Network
110c
BES Asset
(Relay,
Transformer,
Circuit Breaker)
140
Peripheral
Device
170b
Mobile Terminal
Device
120
Cyber Risk
USB Mass Storage
Device 170a
102
130a
130b
130c
130c
130d
130e
130f
130g
130h
130i
130k
150a
150b
150c
WiFi
WiFi
Bluetooth

Figure 1

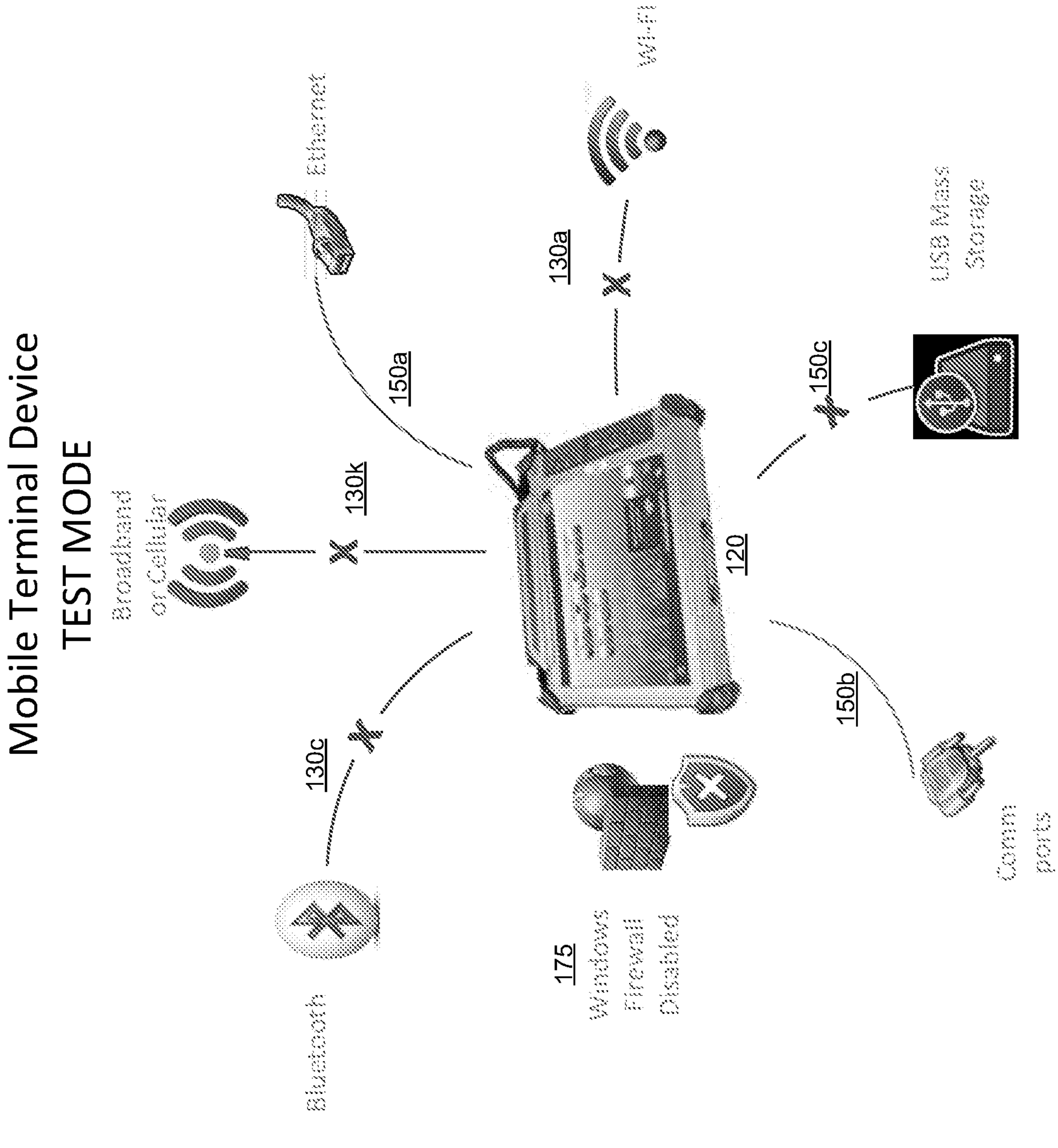
Mobile Terminal Device
TEST MODE
Broadband or Cellular
130k
Ethernet
150a
Wi-Fi
130a
USB Mass Storage
150c
120
150b
Comm ports
175
Windows Firewall Disabled
130c
Bluetooth

Figure 2A

Mobile Terminal Device
NETWORK MODE

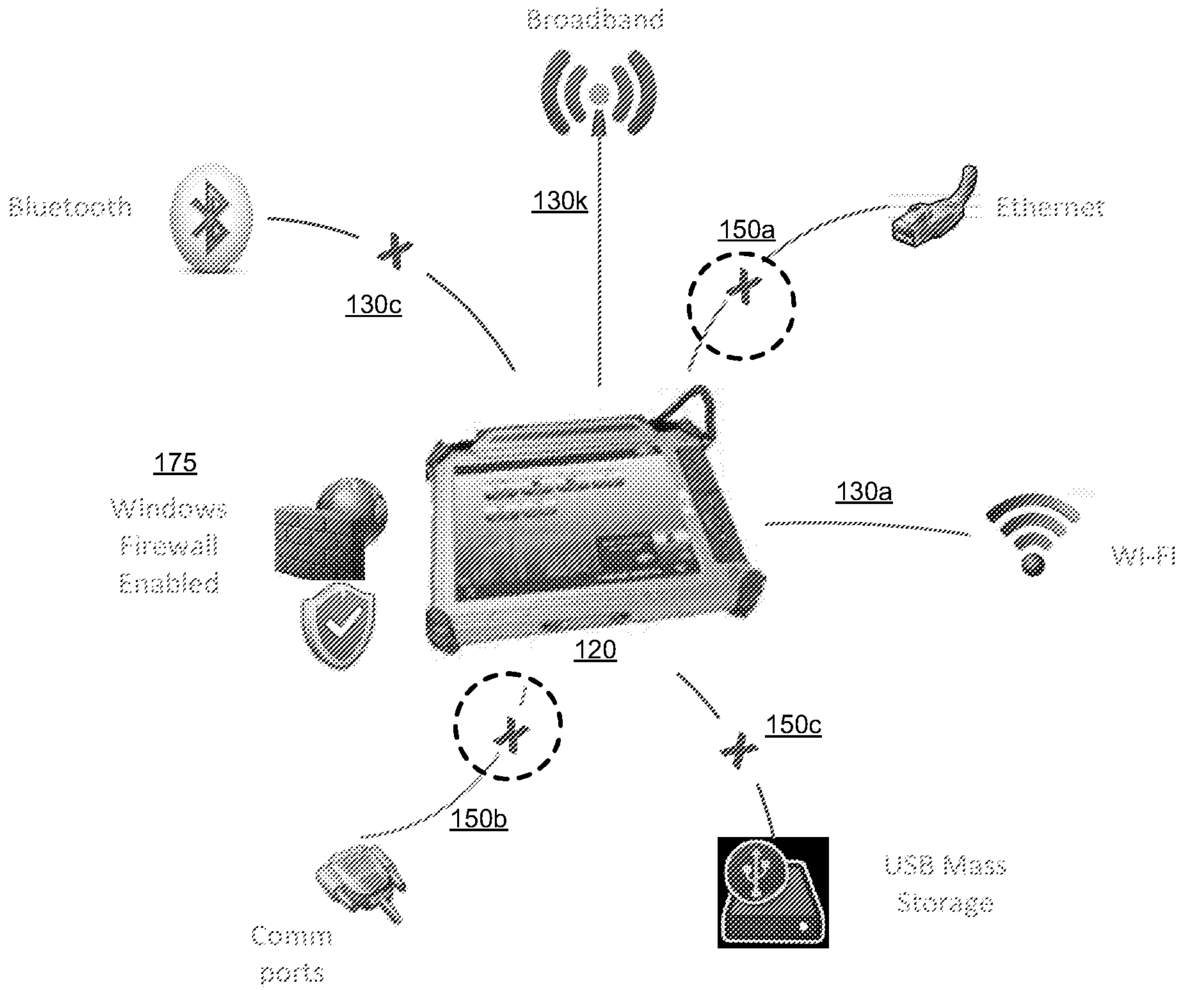

Figure 2B

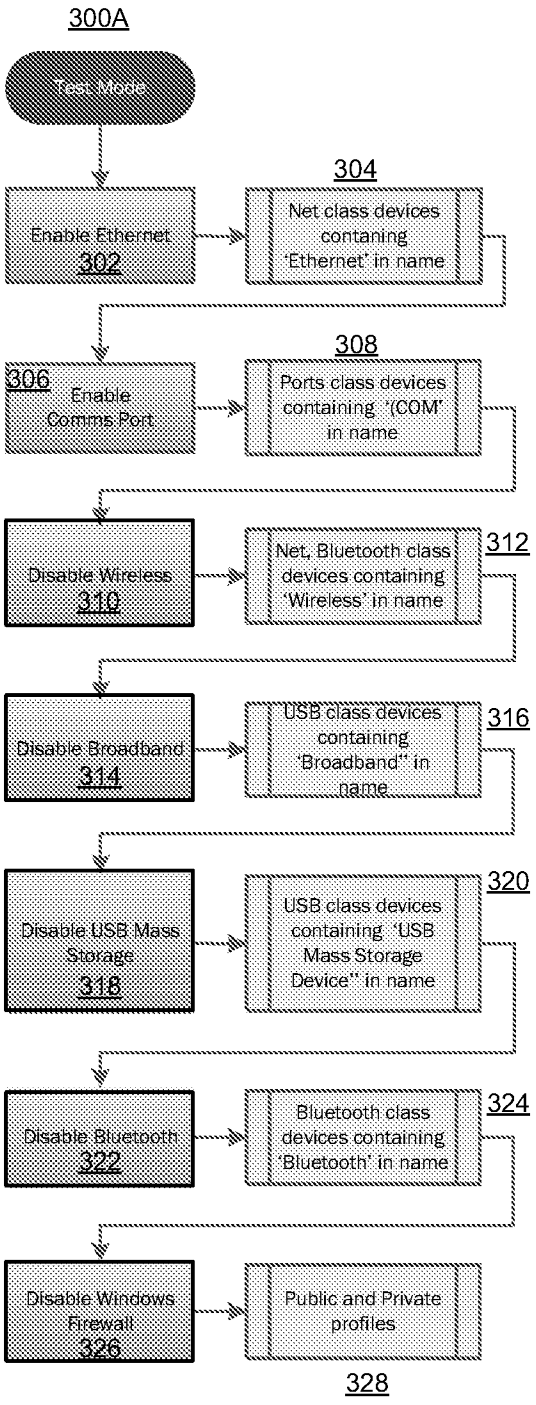
300A
Test Mode
Enable Ethernet
302
304
Net class devices contaning 'Ethernet' in name
306
Enable Comms Port
308
Ports class devices containing '(COM' in name
Disable Wireless
310
312
Net, Bluetooth class devices containing 'Wireless' in name
Disable Broadband
314
316
USB class devices containing 'Broadband" in name
Disable USB Mass Storage
318
320
USB class devices containing 'USB Mass Storage Device" in name
Disable Bluetooth
322
324
Bluetooth class devices containing 'Bluetooth' in name
Disable Windows Firewall
326
Public and Private profiles
328

Figure 3A

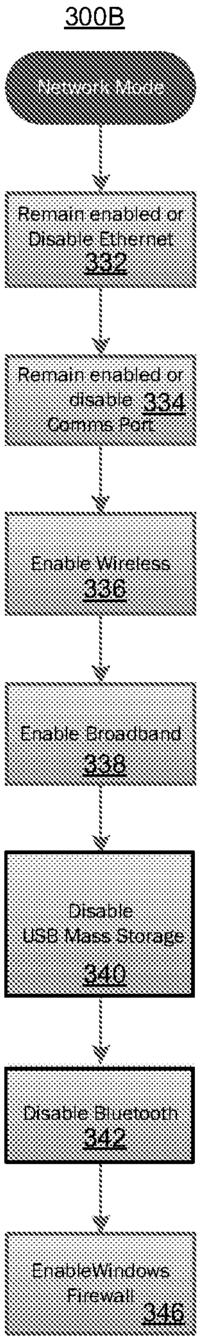

Figure 3B

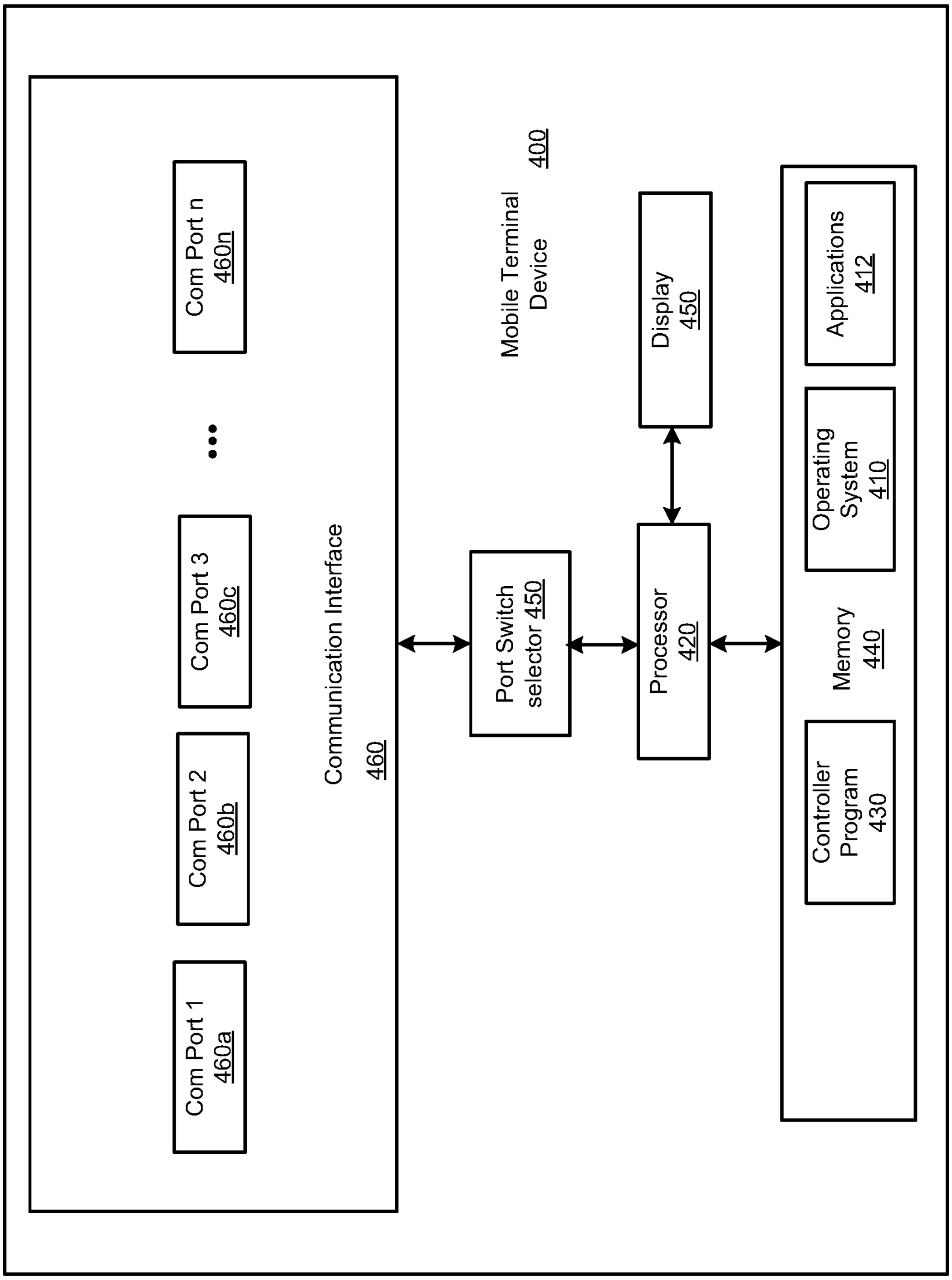
Mobile Terminal Device
400
Communication Interface
460
Com Port 1
460a
Com Port 2
460b
Com Port 3
460c
Com Port n
460n
Port Switch selector 450
Processor
420
Display
450
Memory
440
Controller Program
430
Operating System
410
Applications
412

Figure 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2017/024971

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G01R 31/28; G06F 11/00; G06F 11/07; G06F 13/00; G06F 15/177; G06F 21/00 (2017.01)

CPC - G05B 23/0267; G06F 11/073; G06F 11/0736; G06F 11/076; G06F 21/55; G06F 21/577; H04L 12/2856; H04L 12/2876; H04L 43/50; H04L 51/18; H04L 61/103; H04L 61/3065; H04L 61/6022; H04L 63/14; H04L 63/1425 (2017.02)

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)
See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 434/118; 709/222; 710/33; 714/703; 726/1; 726/23 (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014/0283047 A1 (GENERAL ELECTRIC COMPANY) 18 September 2014 (18.09.2014) entire document	1-24
Y	US 2002/0162059 A1 (MCNEELY et al.) 31 October 2002 (31.10.2002) entire document	1-24
Y	US 2003/0177389 A1 (ALBERT et al.) 18 September 2003 (18.09.2003) entire document	1-24
Y	US 2012/0131157 A1 (GOSPODAREK et al.) 24 May 2012 (24.05.2012) entire document	7, 15, 16, 23, 24
Y	US 2011/0055438 A1 (NAKAGAWA) 03 March 2011 (03.03.2011) entire document	8, 16, 24
A	US 2011/0039237 A1 (SKARE) 17 February 2011 (17.02.2011) entire document	1-24

□ Further documents are listed in the continuation of Box C. □ 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 24 May 2017	Date of mailing of the international search report 16 JUN 2017
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450 Facsimile No. 571-273-8300	Authorized officer Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774