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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 April 2021 (15.04.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/069340 A1

(51) International Patent Classification:
G06F 21/56 (2013.01) *G06F 21/81* (2013.01)
G06F 21/85 (2013.01)

(21) International Application Number:
PCT/EP2020/077771

(22) International Filing Date:
05 October 2020 (05.10.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1914519.2 08 October 2019 (08.10.2019) GB

(71) Applicants: **AIRBUS OPERATIONS LIMITED** [GB/GB]; Pegasus House, Aerospace Avenue, Filton, Bristol, BS34 7PA (GB). **AIRBUS DEFENCE AND SPACE GMBH** [DE/DE]; Willy-Messerschmitt-Str.1, 82024 Taufkirchen (DE).

(72) Inventors: **SOULSBY, Hugh**; c/o Airbus Operations Ltd., UK IP Dept., Pegasus House, Aerospace Avenue, Filton, Bristol, BS34 7PA (GB). **WEDGBURY, Adam**; c/o Airbus Operations Ltd., UK IP Dept., Pegasus House, Aerospace Avenue, Filton, Bristol, BS34 7PA (GB). **JONES, Kevin**; c/o Airbus Operations Ltd., UK IP Dept., Pegasus House, Aerospace Avenue, Filton, Bristol, BS34 7PA (GB). **WAHID, Khan-Ferdous**; c/o Airbus Defence & Space GmbH Willy-Messerschmitt-Str.1, 82024 Taufkirchen (DE).

(74) Agent: **ROBINSON, Simon**; Airbus Operations Ltd., UK IP Dept., Pegasus House, Aerospace Avenue, Filton, Bristol, BS34 7PA (GB).

(54) Title: METHOD OF OPERATING A MEDIA SCANNER

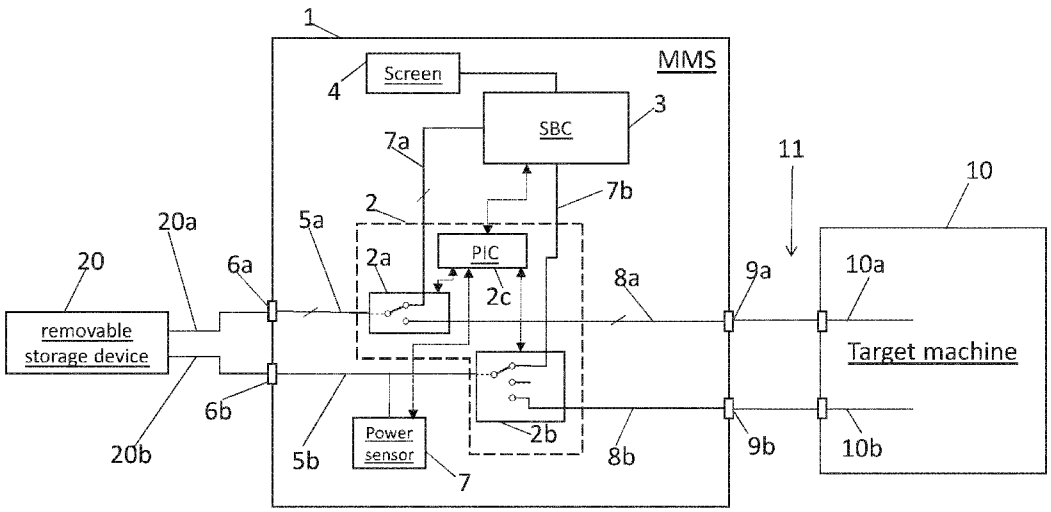


Figure 2

(57) Abstract: A method of operating a media scanner to protect a target machine from malware on a removable storage device. The target machine and the removable storage device each comprise a respective data line, and the media scanner comprises a data switch. Data is scanned on the removable storage device with malware detection software of the media scanner via a first data path, the first data path comprising the data line of the removable storage device connected to the data line of the media scanner by the data switch in a first switching state. After the data has been scanned with the malware detection software, the data switch is operated to switch from the first switching state to a second switching state, thereby disconnecting the data line of the removable storage device from the data line of the media scanner and connecting the data line of the removable storage device to the data line of the target machine. Data is transferred from the removable storage device to the target machine via a second data path, the second data path comprising the data

WO 2021/069340 A1

[Continued on next page]

(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, IT, JO, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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))*

line of the removable storage device connected to the data line of the target machine by the data switch in the second switching state. After the device has been removed, the data switch is returned back to its first switching state.

METHOD OF OPERATING A MEDIA SCANNER

FIELD OF THE INVENTION

[0001] The present invention relates to a method of operating a media scanner to protect a target machine from malware on a removable storage device. The invention also relates to a media scanner configured to perform such a method.

BACKGROUND OF THE INVENTION

[0002] Conventional methods of protecting a target machine from malware on a removable storage device involve installing malware detection software on the target machine. This may not be possible in an industrial environment. A further problem with such conventional methods is that legacy or older target machines may have operating systems that are out of support life so not able to run an up to date version of the malware detection software.

SUMMARY OF THE INVENTION

[0003] According to an aspect of the invention, there is provided a method of operating a media scanner to protect a target machine from malware on a removable storage device, wherein the target machine and the removable storage device each comprise a respective data line, and the media scanner comprises a data switch, the method comprising: a) scanning data on the removable storage device with malware detection software of the media scanner via a first data path, the first data path comprising the data line of the removable storage device connected to the data line of the media scanner by the data switch in a first switching state; b) after the data has been scanned with the malware detection software, operating the data switch to switch from the first switching state to a second switching state, thereby disconnecting the data line of the removable storage device from the data line of the media scanner and connecting the data line of the removable storage device to the data line of the target machine; c) transferring the data from the removable storage device to the target machine via a second data path, the second data path comprising the data line of the removable storage device connected to the data line of the target machine by the data switch in the second switching state; and d) after the removable storage device has been removed from the media scanner, returning the data switch back to its first switching state.

[0004] A further aspect of the invention provides a media scanner comprising a data line, a data switch, malware detection software, and a computer which is configured to operate the media scanner in order to protect a target machine from malware on a removable storage device by the method of the first aspect.

[0005] During the malware scanning step a), since the switches are in their first switching states, the target machine is isolated from the storage device. This is advantageous because it prevents the target machine from being infected by malware from the removable storage device.

[0006] The malware detection software is installed on the media scanner and not on the target machine, making the invention particularly useful in an industrial environment in which installing malware detection software on the target machine may be difficult or impossible. The media scanner can also run up to date versions of the malware detection software, so it can be used to protect a target machine with an operating system which is out of support life.

[0007] Preferably step b) is performed after the data has been scanned with the malware detection software and the storage device passed as safe (for instance with no malware, or any malware removed or quarantined).

[0008] Preferably the media scanner is a mobile device which can be physically coupled to the target machine, physically decoupled from the target machine, and then used to protect another target machine from malware. This enables the media scanner to be used to protect a number of target machines.

[0009] Optionally the target machine and the removable storage device each comprise a respective power line, and the media scanner comprises a power switch, the method further comprising: during the scanning step a), powering the removable storage device via a first power path, the first power path comprising the power line of the removable storage device connected to the power line of the media scanner by the power switch in a first switching state; after the scanning step a), operating the power switch to switch from its first switching state to a second switching state, thereby disconnecting the power line of the removable storage device from the power line of the media scanner and powering down the removable storage device; after the removable storage device has powered down, operating the power switch to switch from its second switching state

to a third switching state, thereby connecting the power line of the removable storage device to the power line of the target machine and powering up the removable storage device via a second power path, the second power path comprising the power line of the removable storage device connected to the power line of the target machine by the power switch in the third switching state; during the data transfer step c), powering the removable storage device via the second power path; and after the removable storage device has been removed from the media scanner, returning the power switch back to its first switching state.

[0010] This switching process ensures that the storage device is powered by the same device that it is communicating with. This is particular advantageous if the storage device is a Universal Serial Bus (USB) device, because the power management of any attached USB device is an important part of the control of that device, affecting connection, operation and disconnection of the USB device.

[0011] Optionally the data switch and the power switch are integrated into a single switch board.

[0012] The powering up of the removable storage device may cause the removable storage device to perform a handshake process with the target machine via the second data path before the data transfer step c).

[0013] Optionally the removable storage device is powered up after the switching step b), so that the second data path is created before the removable storage device is powered up.

[0014] The method may further comprise operating the media scanner to detect a removal of the removable storage device from the media scanner, wherein the data switch and/or the power switch is returned back to its first switching state in response to the detection of the removal. This is advantageous because it prevents an undesirable oscillation which may occur in the absence of such a detection.

[0015] The removal of the removable storage device from the media scanner may be detected by detecting a reduction in power drawn by the removable storage device via the second power path. Alternatively the removal may be detected is some other way, for instance using a physical switch which senses whether the removable storage device is received in a socket of the media scanner.

[0016] The reduction in power may be detected by detecting a reduction in current flow.

[0017] The reduction in current flow may be detected by generating an amplified signal indicative of the current flow, and monitoring when the amplified signal crosses a threshold.

[0018] The method may further comprise operating the media scanner to check whether the media scanner is coupled to the target machine, and operating the data switch in step b) to switch from the first switching state to the second switching state if the check indicates that the target machine is coupled to the media scanner. This is advantageous because it prevents an undesirable oscillation which may occur in the absence of such a check that the media scanner is coupled to the target machine.

[0019] Optionally the media scanner is a mobile device which is physically coupled to the target machine during the data transfer step c), and the method further comprises physically decoupling the media scanner from the target machine after the data transfer step c). This decoupling may be achieved by unplugging a cable, for example.

[0020] The method may further comprise quarantining or removing malware if detected by the malware detection software.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] Embodiments of the invention will now be described with reference to the accompanying drawings, in which:

[0022] Figure 1 is a schematic view of a mobile media scanner (MMS);

[0023] Figure 2 is a schematic view of the MMS of Figure 1 coupled to a removable storage device and target machine, with both switches in their first switching state;

[0024] Figure 3 shows the apparatus of Figure 2 with the data switch in a first switching state and the storage device powered down with the power switch in a second switching state;

[0025] Figure 4 shows the apparatus of Figure 2 with the data switch in a second switching state and the power switch in the second switching state;

[0026] Figure 5 shows the apparatus of Figure 2 with the data switch in the second switching state and the storage device powered up with the power switch in a third

switching state; and

[0027] Figure 6 shows the power sensor.

[0028] DETAILED DESCRIPTION OF EMBODIMENT(S)

[0029] A mobile media scanner (MMS) 1 according to an embodiment of the invention is shown in Figure 1. The MMS 1 is a mobile standalone device. The MMS 1 comprises a Universal Serial Bus (USB) switch board 2, a single board computer (SBC) 3, and a touch screen 4. The switch board 2 comprises a data switch 2a, a power switch 2b and a PIC (Programmable Intelligent Processor) processor 2c that controls the switches 2a, 2b. Alternatively the processor 2c may be another type of controller such as a Field Programmable Gate Array (FPGA). The switch board 2 will work with both USB versions 2 and 3.

[0030] A first MMS data line 5a leads from the data switch 2a to a device data port 6a; a second MMS data line 7a leads from the data switch 2a to the SBC 3; and a third MMS data line 8a leads from the data switch 2a to a target machine data port 9a.

[0031] A first MMS power line 5b leads from the power switch 2b to a device power port 6b; a second MMS power line 7b leads from the power switch 2b to the SBC 3; and a third MMS power line 8b leads from the power switch 2b to a target machine power port 9b.

[0032] The MMS 1 is a mobile device which can be physically coupled to a target machine 10 as shown in Figure 2, then decoupled from the target machine 10 when the MMS 1 is not required. This coupling may be via a USB cable 11 for instance. The target machine 10 has a data line 10a connected to the third MMS data line 8a via the USB cable 11 and the target machine data port 9a; and a power line 10b connected to the third MMS power line 8b via the USB cable 11 and the target machine power port 9b. The USB cable 11 is plugged into one USB port of the target machine, and any other USB ports of the target machine may be disabled.

[0033] The function of the MMS 1 is to protect the target machine 10 from malware on a removable storage device 20 which is plugged into a socket of the MMS 1 so that it is connected to the MMS 1 as shown in Figure 2. The storage device 20 has a data line 20a connected to the first MMS data line 5a via the device data port 6a, and a power

line 20b connected to the first MMS power line 5b via the device power port 6b.

[0034] The SBC 3 runs custom software that is configured to operate the MMS 1 in order to protect the target machine 10 from malware on the storage device 20 by the method described below.

[0035] By default, the data switch 2a and power switch 2b are in first switching states shown in Figure 2. Thus when the storage device 20 is plugged into the MMS 1 as shown in Figure 2, it is powered up via a first power path shown in Figure 2. The first power path comprises the power line 20b of the storage device connected to the power line 7b of the MMS 1 by the power switch 2b in the first switching state.

[0036] The powering up of the storage device 20 causes it to perform a handshake process with the SBC 3 via a first data path shown in Figure 2. The first data path comprises the data line 20a of the storage device 20 connected to the data line 7a of the MMS 1 by the data switch 2a in the first switching state. This handshake process negotiates communications between the storage device 20 and the SBC 3.

[0037] The MMS 1 runs multiple types of malware detection software (virus checkers) such as McAfee (TM) or ClamAV (TM). In this case there are two types, but there may be three or more. After the handshake process is complete, the SBC 3 scans data on the storage device 20 with the malware detection software via the first data path. During the malware scanning step, the storage device 20 continues to be powered via the first power path.

[0038] During the malware scanning step, since the switches 2a, 2b are in their first switching states, the target machine 10 is isolated from the storage device 20. This is advantageous because it prevents the target machine 10 from being infected by malware from the storage device 20.

[0039] If malware is detected by the malware detection software, then the MMS 1 is operated to either quarantine the malware, or remove it from the storage device 20. Quarantining of the malware may involve replacing the malware with an encrypted version of the file which is stored on the storage device 20 along with the encryption key to enable recovery. The process will continue until all the data on the storage device 20 has been checked. The process may then be terminated, or the process may continue if some of the data on the storage device 20 is not malware. The progress of the malware

scanning is shown to the operator by the screen 4.

[0040] After the data has been scanned with the malware detection software, and the storage device 20 passed as safe (i.e. with no malware, or any malware removed or quarantined), then the SBC 3 sends a command to the PIC processor 2c to switch to the target machine. The PIC processor 2c then manages the timing of the switching.

[0041] The PIC processor 2c checks whether the MMS 1 is coupled to the target machine 10 as shown in Figure 2. If not, then the switches 2a, 2b remain in their default first switching states. If the check indicates that the target machine 10 is coupled to the MMS 1, then the PIC processor 2c operates the power switch 2b to switch from its first switching state to a second switching state shown in Figure 3, thereby disconnecting the power line 20b of the storage device 20 from the power line 7b of the MMS 1 and powering down the storage device 20.

[0042] After the power switch 2b has been switched to power down the storage device 20 as shown in Figure 3, the data switch 2a is switched from the first switching state of Figure 3 to a second switching state shown in Figure 4, thereby disconnecting the data line 20a of the storage device from the data line 7a of the MMS 1 and connecting the data line 20a of the removable storage device to the data line 10a of the target machine 10 to form a second data path. This second data path comprises the data line 20a of the storage device 20 connected to the data line 10a of the target machine 10 by the data switch 2a in the second switching state.

[0043] After the data switch 2a has been switched to its second switching state as in Figure 4 with the storage device 20 powered down, the PIC processor 2c operates the power switch 2b to switch from its second switching state to a third switching state shown in Figure 5, thereby connecting the power line 20b of the storage device to the power line 10b of the target machine 10. This causes the storage device 20 to be powered up for a second time via a second power path shown in Figure 5. The second power path comprises the power line 20b of the removable storage device 20 connected to the power line 10b of the target machine 10 by the power switch 2b in the third switching state.

[0044] The powering up of the storage device 20 for a second time causes it to perform a handshake process with the target machine 10, similar to the handshake process

previously described with the MMS 1. This handshake process negotiates communications between the storage device 20 and the target machine 10 via the second data path shown in Figure 5. Note that the storage device 20 is powered up after the data switch 2a has been switched to the second switching state, so that the second data path is created before the removable storage device is powered up for the second time.

[0045] As noted above, after the data has been scanned with the malware detection software, the PIC processor 2c checks whether the MMS 1 is coupled to the target machine 10. If not, then the switches 2a, 2b remain in their default first switching states. This check prevents an undesirable oscillation which would otherwise occur in the absence of the check. Such an oscillation would operate as follows: the storage device 20 is powered down, an attempt to power up via the target machine 10 is performed, no power is available so the switches are returned to their first switching states, the MMS 1 will see this as a new incursion of a storage device and start again, the storage device 20 repeats the handshake and scanning steps with the MMS 1, and so on.

[0046] After the handshake is complete, the data is transferred from the storage device 20 to the target machine 10 via the second data path. During the handshake and data transfer steps, the storage device 20 continues to be powered via the second power path.

[0047] While the storage device is connected to the target machine, the SBC continuously checks whether the storage device 20 has been removed from the MMS 1. When the SBC 3 detects a removal of the removable storage device from the MMS 1, the data switch 2a and the power switch 2b are returned back to their first switching states as shown in Figure 1, in response to the detection of the removal. Again, checking whether the storage device 20 has been removed from the MMS 1 before returning the switches 2a, 2b back to their first switching states prevents an undesirable oscillation similar to the one described above.

[0048] The removal of the storage device 10 from the MMS 1 is detected by a power sensor 7 which is arranged to monitor power being drawn by the first MMS power line 5b. When the power sensor 7 detects a reduction in power drawn by the storage device 10 via the second power path, this is taken by the SBC 3 as an indication that the storage device 10 has been removed.

[0049] A preferred form of the power sensor 7 is shown in Figure 6. The power sensor

7 measures a voltage across a 0.2 ohm resistor 30 in a 0V line 31. The reduction in power is detected by generating an amplified signal indicative of the current flow, and monitoring when the amplified signal drops below a threshold. A device connected signal is held high while the amplified signal is above the threshold, and reset when the amplified signal drops below the threshold indicating that the storage device 10 has been removed. This is monitored by the PIC processor 2c which passes the message on to the SBC 3. This resetting of the device connected signal informs the SBC 3 that the process is complete and the control program run by the SBC 3 can reset the system to await the next storage device to be tested.

[0050] As explained above, the MMS 1 is a mobile device which is physically coupled to the target machine 10 by a USB cable 11 during the handshake and data transfer steps. After the handshake and data transfer steps, the MMS 1 can be physically decoupled from the target machine 10 by unplugging the USB cable 11.

[0051] It is important that the power used by the storage device 10 is supplied by the same device that it is communicating with. This is achieved by the switching process described above. Within PCs/controllers the USB Host Controller chip controls the access to USB devices, it generates a “Port Change Interrupt” that lets the operating system know that a new device is available or that the device has been removed. One of the mechanisms used for the detection is the power management of the USB device.

[0052] As noted above, the target machine 10 is isolated from the storage device 20 during the malware scanning step. At no point is any active component of the MSS 1 (for instance the SBC 3 or PIC processor 2c) connected to the target machine 10.

[0053] The MMS 1 can be used in an industrial environment where USB removable media is used to transfer data between machines and workstations. The MMS 1 is particularly useful in an environment in which malware detection software cannot be installed on the target machine - which is often true in industrial environments.

[0054] Where the word 'or' appears this is to be construed to mean 'and/or' such that items referred to are not necessarily mutually exclusive and may be used in any appropriate combination.

[0055] Although the invention has been described above with reference to one or more preferred embodiments, it will be appreciated that various changes or modifications

may be made without departing from the scope of the invention as defined in the appended claims.

Claims

1. A method of operating a media scanner to protect a target machine from malware on a removable storage device, wherein the target machine and the removable storage device each comprise a respective data line, and the media scanner comprises a data switch, the method comprising:

a) scanning data on the removable storage device with malware detection software of the media scanner via a first data path, the first data path comprising the data line of the removable storage device connected to the data line of the media scanner by the data switch in a first switching state;

b) after the data has been scanned with the malware detection software, operating the data switch to switch from the first switching state to a second switching state, thereby disconnecting the data line of the removable storage device from the data line of the media scanner and connecting the data line of the removable storage device to the data line of the target machine;

c) transferring the data from the removable storage device to the target machine via a second data path, the second data path comprising the data line of the removable storage device connected to the data line of the target machine by the data switch in the second switching state; and

d) after the removable storage device has been removed from the media scanner, returning the data switch back to its first switching state.

2. The method of claim 1, wherein the target machine and the removable storage device each comprise a respective power line, and the media scanner comprises a power switch, the method further comprising:

during the scanning step a), powering the removable storage device via a first power path, the first power path comprising the power line of the removable storage device connected to the power line of the media scanner by the power switch in a first switching state;

after the scanning step a), operating the power switch to switch from its first switching state to a second switching state, thereby disconnecting the power line of

the removable storage device from the power line of the media scanner and powering down the removable storage device;

after the removable storage device has powered down, operating the power switch to switch from its second switching state to a third switching state, thereby connecting the power line of the removable storage device to the power line of the target machine and powering up the removable storage device via a second power path, the second power path comprising the power line of the removable storage device connected to the power line of the target machine by the power switch in the third switching state;

during the data transfer step c), powering the removable storage device via the second power path; and

after the removable storage device has been removed from the media scanner, returning the power switch back to its first switching state.

3. The method of claim 2, wherein the powering up of the removable storage device causes the removable storage device to perform a handshake process with the target machine via the second data path before the data transfer step c).

4. The method of claim 2 or claim 3, wherein the removable storage device is powered up after the switching step b), so that the second data path is created before the removable storage device is powered up.

5. The method of any preceding claim, further comprising operating the media scanner to detect a removal of the removable storage device from the media scanner, wherein the data switch and/or the power switch is returned back to its first switching state in response to the detection of the removal.

6. The method of claim 2 and claim 5, wherein the removal of the removable storage device from the media scanner is detected by detecting a reduction in power drawn by the removable storage device via the second power path.

7. The method of claim 6, wherein the reduction in power is detected by detecting a reduction in current flow.

8. The method of claim 7 wherein the reduction in current flow is detected by generating an amplified signal indicative of the current flow, and monitoring when the amplified signal crosses a threshold.

9. The method of any preceding claim, further comprising operating the media scanner to check whether the media scanner is coupled to the target machine, and operating the data switch in step b) to switch from the first switching state to the second switching state if the check indicates that the target machine is coupled to the media scanner.

10. The method of any preceding claim, wherein the media scanner is a mobile device which is physically coupled to the target machine during the data transfer step c), and the method further comprises physically decoupling the media scanner from the target machine after the data transfer step c).

11. The method of any preceding claim, further comprising quarantining or removing malware if detected by the malware detection software.

12. A media scanner comprising a data line, a data switch, malware detection software, and a computer which is configured to operate the media scanner in order to protect a target machine from malware on a removable storage device by the method of any preceding claim.

13. The media scanner of claim 12, wherein the media scanner is a mobile device which can be physically coupled to the target machine and physically decoupled from the target machine.

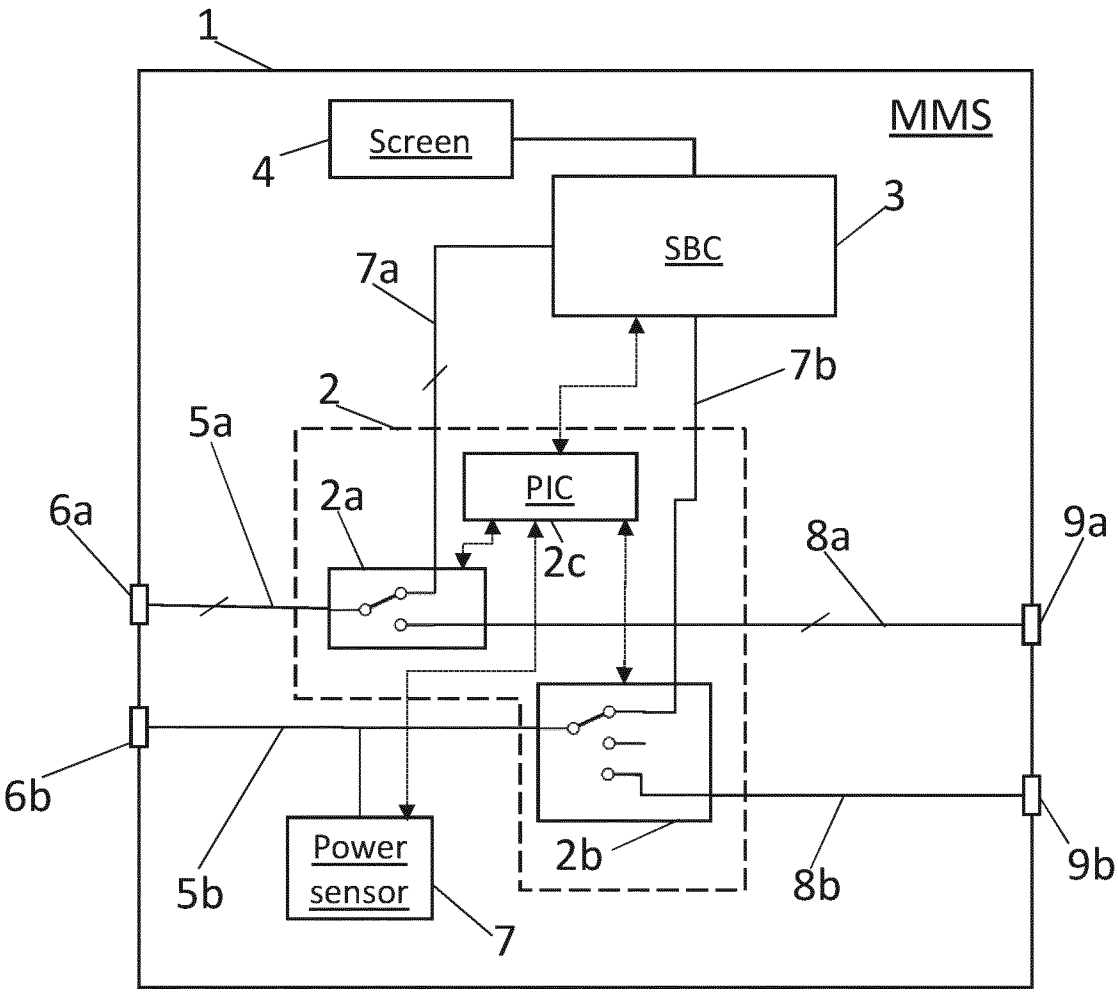

1
MMS
Screen
4
SBC
3
7a
7b
2
5a
PIC
2a
2c
6a
8a
9a
6b
5b
Power
sensor
7
2b
8b
9b

Figure 1

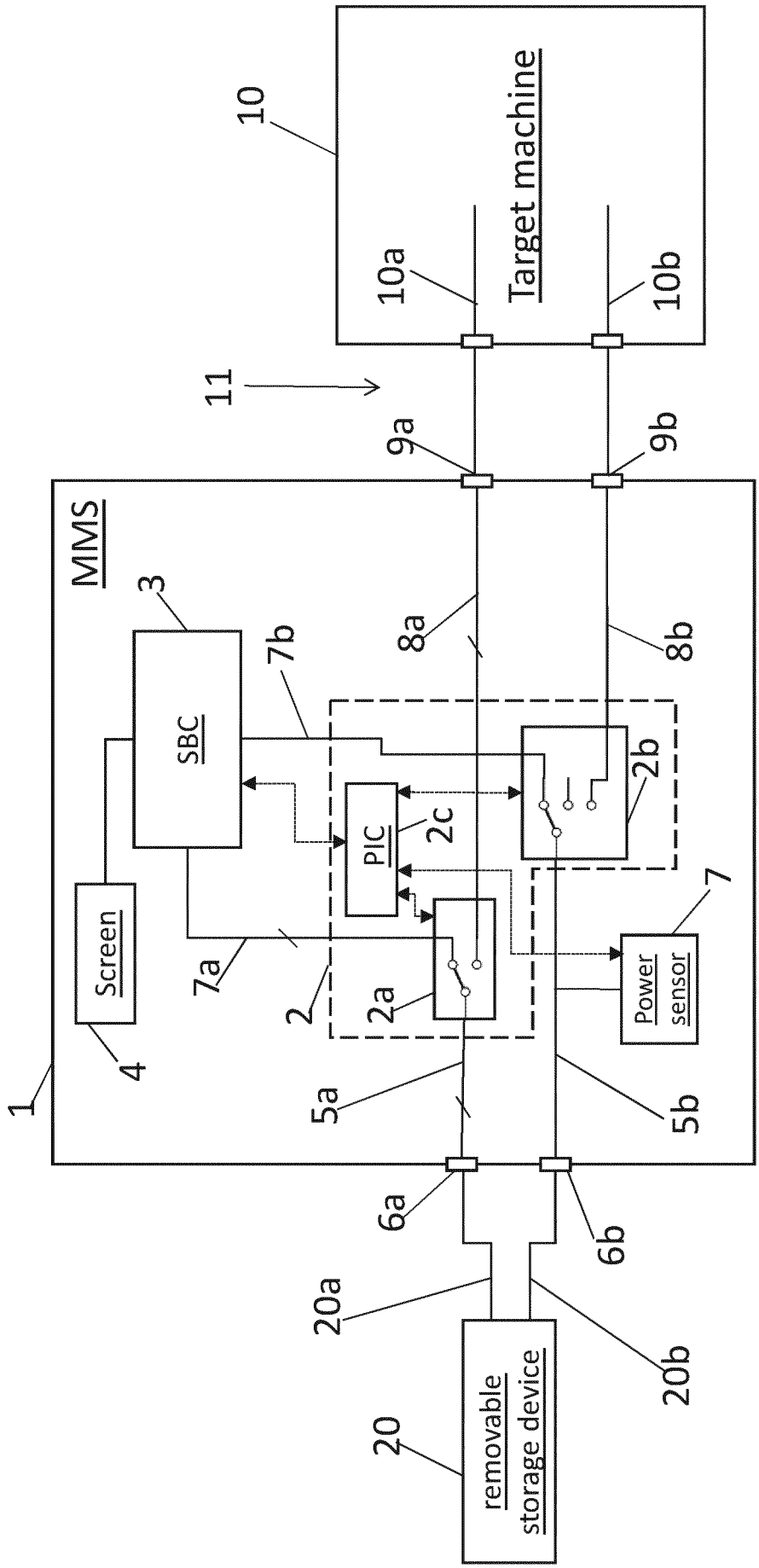

10
Target machine
10a
10b
11
9a
9b
MMS
3
SBC
7b
8a
8b
2b
PIC
2c
Screen
7a
2
2a
7
Power sensor
4
1
5a
5b
6a
6b
20a
20b
20
removable storage device

Figure 2

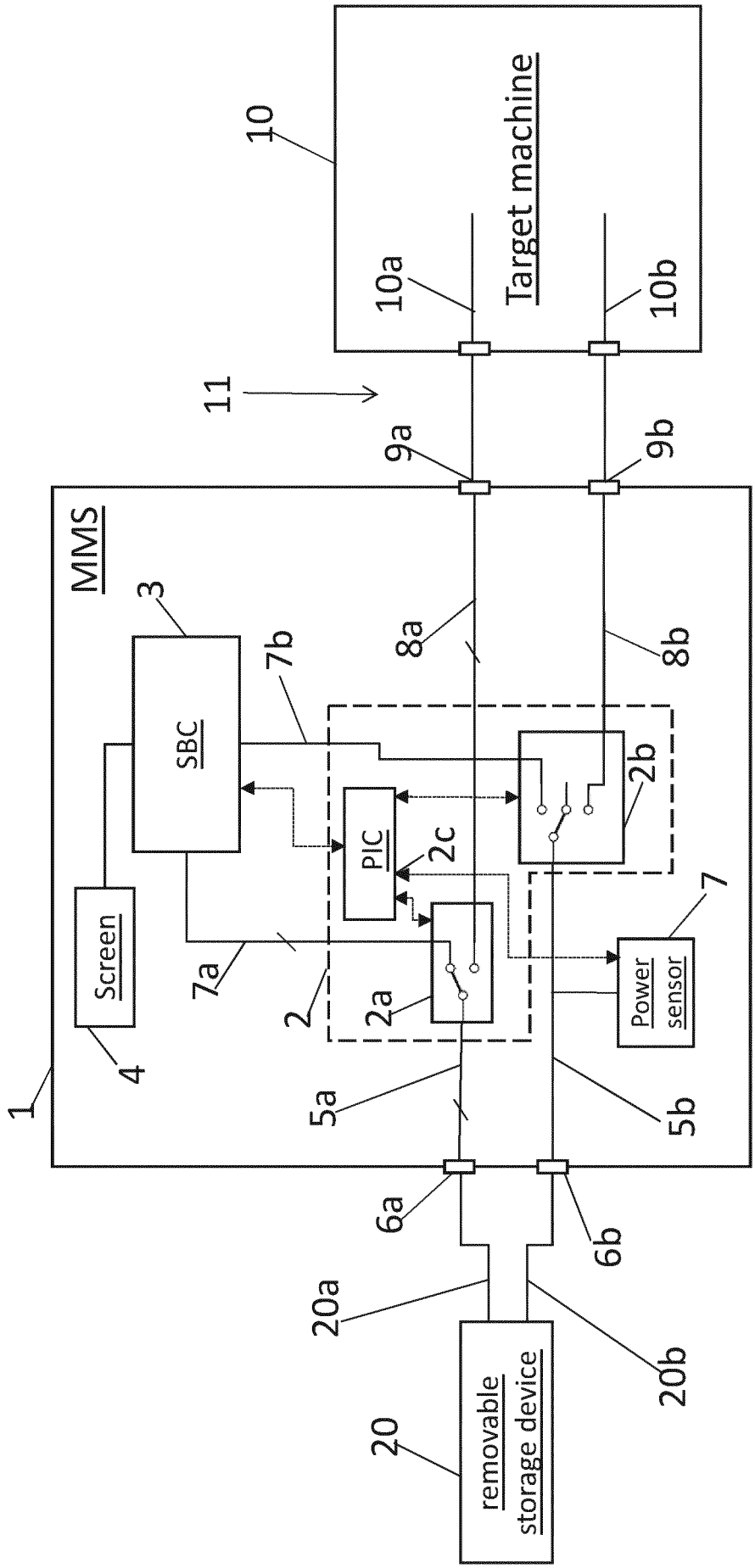

10
Target machine
10a
10b
11
9a
9b
MMS
3
SBC
7b
8a
8b
2b
PIC
2c
Screen
7a
2
2a
7
Power sensor
4
1
5a
5b
6a
6b
20a
20b
20
removable storage device

Figure 3

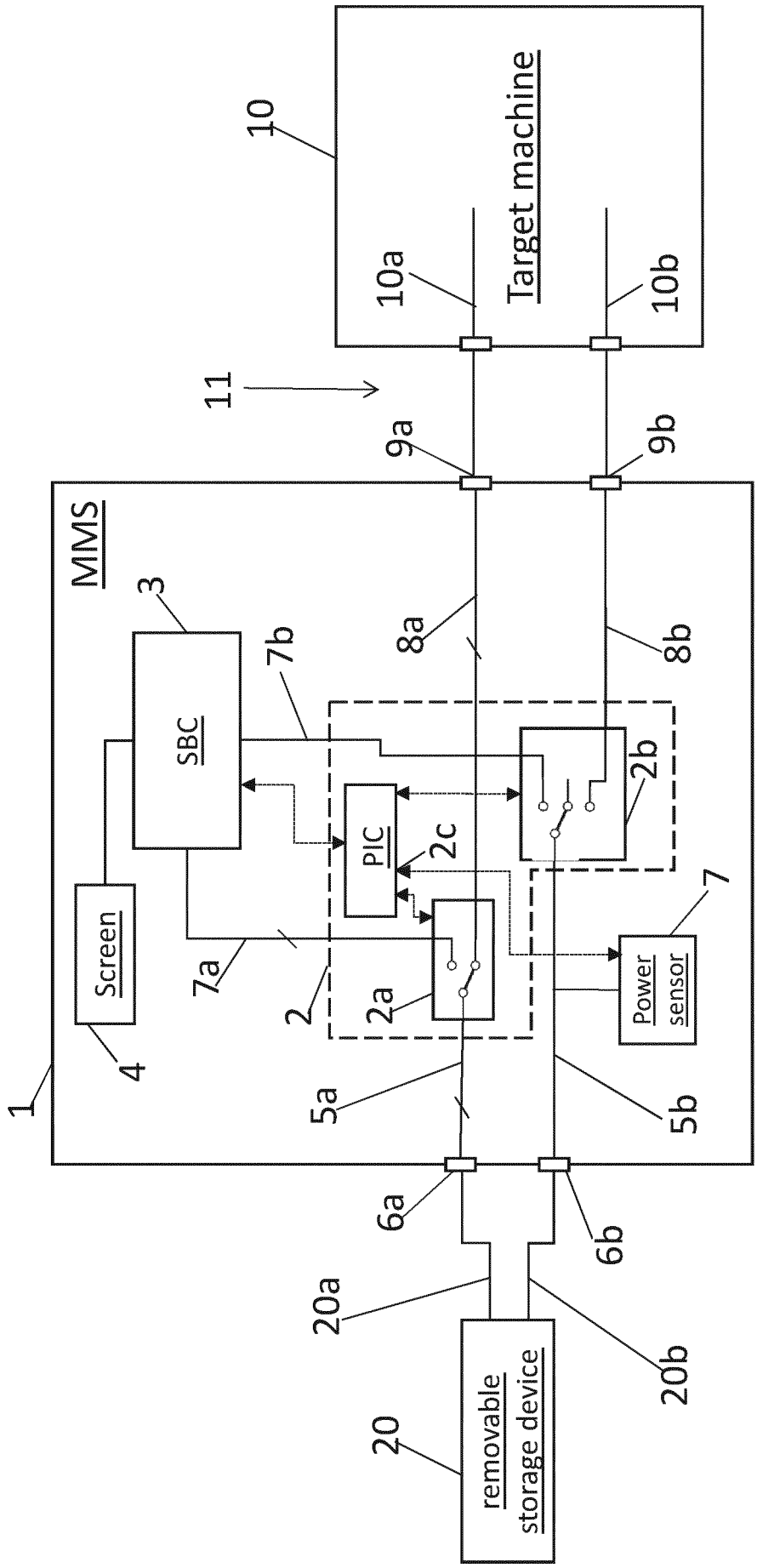

10
Target machine
10a
10b
11
9a
9b
MMS
3
SBC
7b
8a
8b
2b
PIC
2c
Screen
7a
2
2a
7
Power sensor
4
1
5a
5b
6a
6b
20a
20b
20
removable storage device

Figure 4

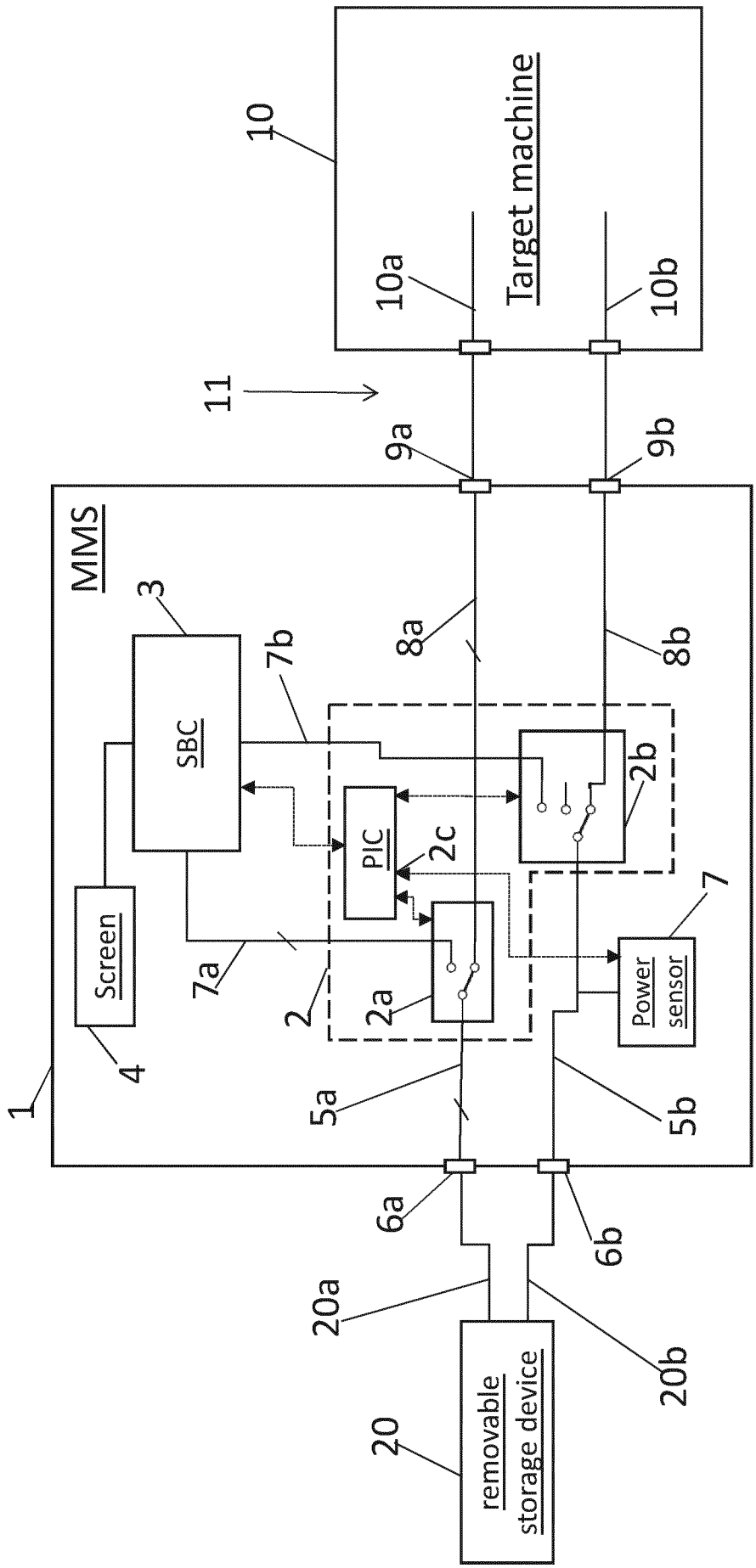

10
Target machine
10a
10b
11
9a
9b
MMS
3
SBC
7b
8a
8b
2b
PIC
2c
Screen
7a
2
2a
7
Power sensor
4
1
5a
5b
6a
6b
20a
20b
20
removable storage device

Figure 5

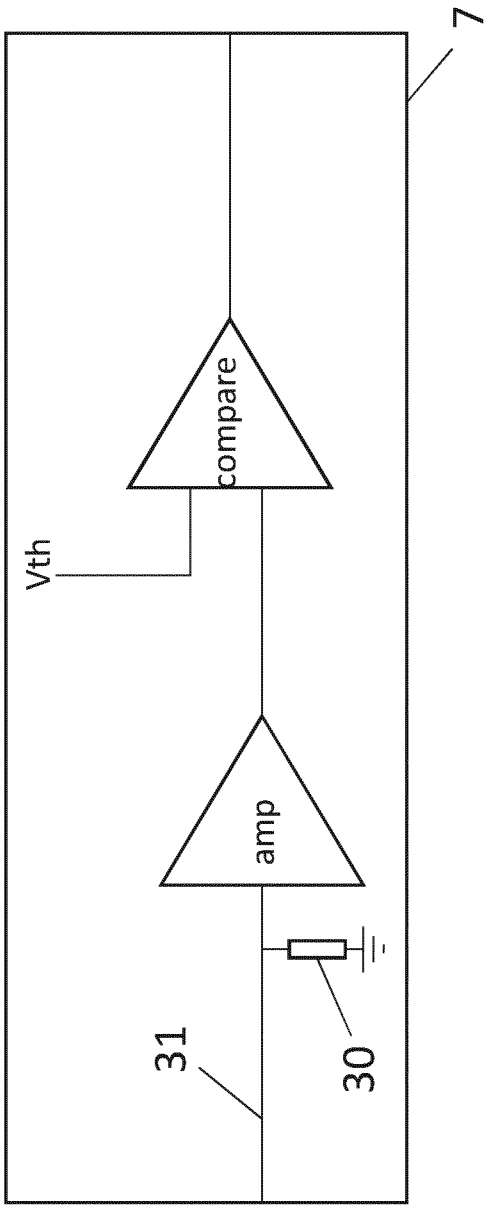


Figure 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2020/077771

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/56 G06F21/85 G06F21/81
ADD.

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)
G06F

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	CA 3 045 109 A1 (HITACHI LTD [JP]) 2 August 2018 (2018-08-02)	1,9-13
Y	figures 1,2,4	5-8
A	paragraphs [0004], [0008] - [0009], [0014], [0022] - [0023], [0042] - [0043], [0048] - [0050], [0052], [0054]	2-4
A	US 2010/011442 A1 (ZHAO SHI-MING [TW]) 14 January 2010 (2010-01-14) paragraphs [0025] - [0029]; figures 5A-5C	2-4
Y	US 2018/097629 A1 (SOFFER AVIV [IL]) 5 April 2018 (2018-04-05) paragraphs [0055], [0146], [0150], [0223]	5-8

☐ 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	Date of mailing of the international search report
9 November 2020	17/11/2020

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	Veillas, Erik

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2020/077771

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CA 3045109 A1	02-08-2018	CA 3045109 A1	02-08-2018
		CN 110050264 A	23-07-2019
		JP 6625077 B2	25-12-2019
		JP 2018124662 A	09-08-2018
		US 2020065488 A1	27-02-2020
		WO 2018139230 A1	02-08-2018
US 2010011442 A1	14-01-2010	US 2010011442 A1	14-01-2010
		US 2010011443 A1	14-01-2010
US 2018097629 A1	05-04-2018	EP 2958047 A1	23-12-2015
		US 2015365237 A1	17-12-2015
		US 2018097629 A1	05-04-2018