

RESILIENT SURVEILLANCE SYSTEM

TECHNICAL FIELD

5 The present invention relates to a method and device for maintaining operation of a surveillance system. The invention particularly relates to a method and device for restoration of the operation of a computer-based surveillance system.

BACKGROUND ART

10

Surveillance systems up until around thirty years ago operate using a combination of analogue and digital devices. A basic surveillance system comprises at least a video camera, a video recorder that records normal or time-lapse video, motion sensors, thermal sensors, microphones etc to record the conditions of the environment which
15 the surveillance system is tasked to monitor.

While the video and audio surveillance data was previously stored on analogue tapes (such as magnetic video and/or audio tapes), data collected by the motion sensors and thermal sensors were typically stored in computer hard disk drives or the like.

20

With the capacity of hard disk drives and computing powers increasing exponentially since the beginning of the twenty first century, and with the costs of manufacturing computers becoming drastically reduced, surveillance systems are now predominantly digital. More specifically, entire surveillance systems can now be built
25 around a single computer or a network of computers. Software applications that are tailored to work with external hardware to collect data from video cameras, motion sensors, thermal sensors, and microphones are installed on the computers. With modern video and audio compression techniques and algorithms, video and audio data that used to be too large to be stored on hard disk drives are compressed to a
30 fraction of their size, and modern high capacity hard disk drives can store up to months or even years worth of surveillance data.

However, when so much reliance is placed on a single computer or a network of computers to provide surveillance and store surveillance data, the reliability of the or

each computer along with their connected hardware (especially the hard drive), plus the stability of their operating system become paramount.

5 Modern computers, powerful as they are, are however known to fail from time to time due to their complexity. Many factors contribute to the failure of a computer, including abnormal ambient temperatures, power surges and interruptions, failure of a piece of connected hardware (such as the hard drive), bugs in the operating system or one of the software applications, and computer viruses.

10 While some computer failures are irrecoverable without human intervention, there are many occasions where a computer can be restored to its functional state without a human engineer having to take it apart. With a computer that runs a surveillance system, such convenience is most welcomed, since the surveillance system may be located where it is inconvenient or cost prohibitive to have a human engineer tasked
15 to monitor and maintain it.

Therefore, there is a need for a method and device that can take over the principal tasks of a human engineer to monitor and maintain a computer that runs a surveillance system.

20

SUMMARY OF THE INVENTION

The principal object of the present invention is to provide a method and device that automatically restores a computer that runs a surveillance system to its functional
25 state in the event of an unexpected failure. There is a further need to allow the restoration process to be initiated and carried out remotely.

According to one aspect of the invention, there is provided a method for restoring operation of a surveillance system comprising a computer running an operating
30 system, the method comprising: providing the computer with a local control unit comprising a microcontroller and a memory module, the local control unit monitoring and storing the status of the computer on the memory module, transmitting the status of the computer from the memory module to a remote server, and restoring operation to the computer when the status indicates the computer is not operating.

The local control unit constantly monitors the status of the computer and determines when it is not operating normally. The local control unit further stores the status of the operating system in the memory module.

- 5 According to one embodiment, the step of the local control unit restoring operation to the computer is initiated by a remote device in communication with the remote server.

In another embodiment, the remote device is a wireless device.

10

The wireless device may be a cellular phone, a tablet or the like communicating wirelessly with the server.

- In yet another embodiment, the step of the local control unit restoring operation to the computer comprises the local control unit rebooting the operating system.
- 15

The microcontroller of the local control unit has access to the electronic switches of the computer, specifically the on/off and reset/reboot switches.

- 20 In another aspect, the step of the local control unit restoring operation to the computer comprises the local control unit restoring the operating system on the computer using a backup image.

- The backup image is a complete copy of the working operating system of the computer.
- 25

In one embodiment, the step of the local control unit restoring operation to the computer comprises the local control unit retrieving the backup image from the memory module.

30

The backup image is stored in the memory module within the local control unit.

According to another embodiment, the step of restoring the operating system further comprises retrieving the backup image from the remote server.

The backup image in this alternative embodiment is stored at the remote server.

According to another embodiment, the surveillance system comprises a digital video recorder system.

5

In yet another aspect, there is provided a local control unit for restoring operation of a surveillance system comprising a computer running an operating system, wherein the local control unit comprises a memory module; a microcontroller to monitor and store the status of the computer on a memory module and restore operation to the computer when the status indicates the computer is not operating; and a modem to transmit the status of the computer from the memory module to a remote server.

10

The modem may be wired or wireless, capable of TCP/IP communication. The modem is also able to encrypt the data prior to transmission and receive encrypted data.

15

According to one embodiment, the microcontroller receives instructions to restore operation to the computer via the modem from a remote device that is in communication with the remote server.

20

In another embodiment, the local control unit is arranged to restore operation to the computer by rebooting the operating system.

In one embodiment, the local control unit is arranged to restore operation to the computer by restoring the operating system using a backup image.

25

In a further embodiment, the backup image is retrievable from the memory module.

According to another embodiment, the backup image is retrievable from the remote server via the modem.

30

According to a further embodiment, the local control unit comprises a backup power supply to maintain operation of the microcontroller and modem in the event of power failure.

According to yet another embodiment, the surveillance system comprises a digital video recorder system.

BRIEF DESCRIPTION OF THE DRAWINGS

5

The invention will be described in conjunction with the following drawing which is only for the purpose of illustrating the embodiments of the present invention, and not for the purpose of limiting the present invention.

- 10 Figure 1 is a system block diagram according to an embodiment of the present invention.

DETAILED DESCRIPTION

- 15 The invention is described in detail in reference to the example below.

In the following example, an embodiment of the present invention is part of a system that monitors and maintains a surveillance system. In this example, the surveillance system comprises at least video surveillance. The system comprises four
20 components and they are: a microcontroller 3, an automated logic software, a security key and a centralized analytic database system. The embodiment of the present invention resides in the local control unit 2, which houses the microcontroller 3. The centralized analytic database system operates at a remote server 6, and can be shared by multiple systems. Each system has its own unique ID so that their data
25 can be stored separately at a remote server 6.

The microcontroller 3 is embedded in the local control unit 2, as per Fig. 1. The local control unit 2 is installed inside the computer 1 that operates the surveillance system. In the present example, a single computer 1 that is assigned a unique ID by
30 the local control unit 2, operates a surveillance system that is connected to video cameras, microphones, motion sensors and thermal sensors. The computer 1 may be running a Windows® based operating system, with a commercially available software that allows it to communicate with and obtain data from the video cameras, microphones, motion sensors and thermal sensors. At the same time, a local control

unit software (not shown) that is installed in the same computer 1 allows the microcontroller 3 to obtain data from the computer 1 itself.

Surveillance data is stored on the computer's hard drive 10, and can also be optionally transmitted to the remote server 6 via an internet connection. The local control unit 2 has a built-in modem with TCP/IP capabilities, allowing it to connect to the internet either via a LAN cable or through cellular connections, such as using GPRS/3G/4G/LTE protocols.

- 10 The automated logic software is embedded within the microcontroller 3, and together, they monitor the status of the computer 1. Specifically, the microcontroller 3, which has a direct connection to the computer 1, collects data from the local control unit software. This data may include status of the motherboard 8, temperature of the motherboard 8, fan speed (of the cooling fans), etc. The
15 microcontroller 3 analyzes the data collected from the local control unit software, and determines what state the computer is in. For example, if the computer's operating system has somehow stalled, the installed local control unit software would cease to output any data. The microcontroller 3, with its independent automated logic software, will not be affected, and can determine that the computer's operating
20 system is no longer running. Since the microcontroller 3 also has direct access to the physical buttons of the computer, such as the on/off switch and the reset/reboot switch, the microcontroller 3, upon determining that the computer is no longer running, can reset or reboot the computer 1 automatically.
- 25 In the event that the microcontroller 3 has attempted to reboot the computer 1, but without success, the microcontroller 3 may determine that the operating system of the computer 1 has been corrupted. When this happens, the microcontroller 3 has the ability to perform system restore on the computer 1. The processes involved in the restoration of a computer's operating system are known to a person skilled in the
30 art, so the details of which will not be described at length in this description.

Typically, the operating system, the backup image of the operating system and the recovery software are stored on a single hard drive 13 in a computer. Even though this practice saves both cost and space, when a virus infection or a catastrophic
35 hardware failure results in the complete erasure of the hard drive 13, both the

backup image and recovery software will be gone. When this happens, system restore will not work. To overcome the above limitation, an embodiment of the present invention stores a copy of the backup image and the recovery software within a memory block 5, which resides within the local control unit 2. That way, even if a catastrophic event erases the entire content of the hard drive 13, the backup image within the memory block 5 will remain intact. The microcontroller 3 can still perform system restore on the computer 1, and potentially return the surveillance system back to its operational state.

In the present embodiment, the operating system of the computer is stored in hard drive 13. Once it has been determined that the operating system has been corrupted, the microcontroller 3 will execute the recovery software, retrieve the backup image from memory block 5 through multiplexer 12, and copy it to hard drive 13.

The EPROM memory 4 within the microcontroller 3 is used to store the statuses of the computer 1, and at the same time, the microcontroller 3 transmits these statuses to the remote server 6. The unique ID of computer 1 ensures that its data will not be mixed with data from other local control units. The transmission may be live or periodical, depending on whether there is sufficient internet bandwidth, and the availability of internet connection.

It can be appreciated that while the EPROM memory 4 and the memory block 5 are two separate components in the present embodiment, it is entirely possible for them to be one and the same, since the microcontroller 3 can easily store the status data in the memory block 5 instead of the EPROM memory 4.

Also, as can be seen in Figure 1, the local control unit 2 has a built-in battery and a charger 9. The local control unit 2 further has a voltage converter 11 to provide its components with operating power. The built-in battery allows the local control unit 2 to continue running in the event of complete power cut off to the computer 1. The local control unit 2 can also report the power cut to the remote server 6.

Another feature of the invention according to the present embodiment of the invention is the microcontroller's ability to retrieve a copy of the backup image from

the remote server 6. That way, the backup image need not be obtained from the memory block 5 of the local control unit 2.

Furthermore, as the statuses of the computer 1 are being stored at a remote server 6, it is possible for the remote server 6 to alert an offsite engineer in the event all the automated processes failed to return computer 1 back to its operation state. The engineer will be informed of the nature of the failure, and can attempt to restore operation to the computer 1 manually or remotely.

For the former option, the engineer would have to examine the computer 1 onsite, and perform diagnostics and repairs as required.

For the latter option, the engineer may use a remote wireless device 7, such as a smartphone or tablet installed with an authorized application, or even a computer containing an authorized application, to wirelessly attempt to restore the computer's operation.

The security key (not shown) mentioned earlier is a unique device paired with a 128-bit encryption certificate key. It allows certain physical access to the system, such as the on/off button or the reset/reboot button of the computer 1. This is an important feature as it can prevent unauthorized shut down of the computer 1 in an attempt to bypass surveillance.

It can be surmised that the above example can usefully assist in the maintenance and recovery of a computer-based surveillance system. Most of the computer's malfunctions can be attended to in an automated manner using an embodiment of the invention, leaving only critical malfunctions to the engineers.

Even though the above example has detailed the invention in a unique embodiment, it is by no means exhaustive. It is therefore to be understood that the invention may be embodied in numerous other ways without departing from the scope of the invention.

CLAIMS

1. A method for restoring operation of a surveillance system comprising a computer (1) running an operating system, the method comprising:
 - 5 providing the computer with a local control unit (2) comprising a microcontroller (3) and a memory module (4, 5);
the local control unit (2)
monitoring and storing the status of the computer (1) on the memory module (4, 5);
 - 10 transmitting the status of the computer (1) from the memory module (4, 5) to a remote server (6); and
restoring operation to the computer (1) when the status indicates the computer (1) is not operating.
- 15 2. A method for restoring operation of a surveillance system according to claim 1, wherein the step of the local control unit (2) restoring operation to the computer (1) is initiated by a remote device (7) in communication with the remote server (6).
3. A method for restoring operation of a surveillance system according to claim
20 2, wherein the remote device (7) is a wireless device.
4. A method for restoring operation of a surveillance system according to any one of claims 1 through 3, wherein the step of the local control unit (2) restoring operation to the computer (1) comprises:
 - 25 the local control unit (2) rebooting the operating system.
5. A method for restoring operation of a surveillance system according to any one of claims 1 through 3, wherein the step of the local control unit (2) restoring operation to the computer (1) comprises:
 - 30 the local control unit (2) restoring the operating system on the computer (1) using a backup image.
6. A method for restoring operation of a surveillance system according to claim 5, wherein the step of restoring the operating system further comprises:
 - 35 retrieving the backup image from the memory module (4, 5).

7. A method for restoring operation of a surveillance system according to claim 5, wherein the step of restoring the operating system further comprises:
retrieving the backup image from the remote server (6).
- 5 8. A method for restoring operation of a surveillance system according to any one of the preceding claims, wherein the surveillance system comprises a digital video recorder system.
9. A local control unit for restoring operation of a surveillance system comprising
10 a computer (1) running an operating system, wherein the local control unit (2) comprises
a memory module (4, 5);
a microcontroller (3) to monitor and store the status of the computer (1) on the memory module (4, 5) and restore operation to the computer (1) when the
15 status indicates the computer is not operating; and
a modem to transmit the status of the computer (1) from the memory module (5) to a remote server (6).
10. A local control unit for restoring operation of a surveillance system according
20 to claim 9, wherein the microcontroller (3) receives instructions to restore operation to the computer (1) via the modem from a remote device (7) that is in communication with the remote server (6).
11. A local control unit for restoring operation of a surveillance system according
25 to claim 9 or 10, wherein the local control unit (2) is arranged to restore operation to the computer (1) by rebooting the operating system.
12. A local control unit for restoring operation of a surveillance system according
30 to claim 9 or 10, wherein the local control unit (2) is arranged to restore operation to the computer (1) by restoring the operating system using a backup image.
13. A local control unit for restoring operation of a surveillance system according to claim 12, wherein the backup image is retrievable from the memory module (4, 5).

14. A local control unit for restoring operation of a surveillance system according to claim 12, wherein the backup image is retrievable from the remote server (6) via the modem.
- 5 15. A local control unit for restoring operation of a surveillance system to any one of claims 9 to 14, wherein the local control unit (2) comprises a backup power supply to maintain operation of the microcontroller (3) and modem in the event of power failure.
- 10 16. A local control unit for restoring operation of a surveillance system according to any one of claims 9 to 15, wherein the surveillance system comprises a digital video recorder system.