A METHOD OF ORGANIZING DEVICES OF INTEREST TO A USER, IN A MULTIPLE HIERARCHICAL STRUCTURE

FIELD OF THE INVENTION

The present invention relates to a method of managing resources on a network using access control lists.

BACKGROUND OF THE INVENTION

An access control list (or ACL) is a tabulated list that identifies system users and their respective access privileges. This list is established by a systems administrator, and is communicated to the computer's operating system, as a safeguard to the contents of its database. The computer system responds by providing a level of security to the network resource within the server, according to the access control list.

Each network resource has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. Typically, users may be divided into 'role names' and 'user groups'. 'Role names' may be further sub-divided into 'users', 'power users', and 'administrators'.

Access privileges are determined by the role of the system user, and these roles include reading, writing and executing.

Presently, in a manufacturing environment, security is administered by grouping related resources together under one hierarchy, and assigning a particular security setting to the target node, or top of the hierarchy. The security setting set at a particular node will propagate down to its child folders and resources.

In a manufacturing environment set-up, devices of the manufacturing plant are set up in a hierarchical form. The design of this hierarchy is typically set up in a fixed form, for the benefit of usually a single group of users, for example, either the operations or maintenance user groups, and especially for higher management.

For example, a logical hierarchical structure for the operations group will be structured such that each manufacturing step (or logpoint) is a target node, and each equipment used in this step as a child node, and individual devices used within each equipment as the individual devices as seen in Figure 1A.

For a logical hierarchical structure for the maintenance group, as seen in Figure 1B, the hierarchy would have each site as a target node, each area within each site as a first child node, each equipment within each area as a second child node, and each device within each equipment as the individual devices.

As previously explained, security is administered by assigning a particular setting to the target node, and the security set at a particular node will propagate down to its child folders and devices, which results in a very rigid structure.

It is an object of the invention to ameliorate one or all of the above problems.

SUMMARY OF THE INVENTION

According to an embodiment of the invention, there is provided a method of organizing devices of interest to a user, in a multiple hierarchical structure according to the users of such a user, said device of interest selected from a multiple of hierarchical structures, said method including creating a hierarchical structure in terms of folders and sub-folders according to the organizational needs of a user, assigning devices of interest from a pre-existing hierarchical structure to the main folder and sub-folders created in the hierarchical structure, assigning a security setting to the device of interest, wherein the security setting assigned to the said device is the most restrictive security setting of said device in the parent folder of the device of interest, forming a first level of security to the hierarchical structure thus formed.

Preferably, the security settings applicable are any one of the following of

(i) 'read only';
(ii) 'hidden'; or
(iii) 'full control'.

In a preferred method, an administrator can assign a security setting to a main folder or sub-folder of a hierarchy, said administrator security setting forming a second level of security to the hierarchy, on top of the method as disclosed above. Therefore, with two levels of security, accidental and intentional harmful modification of the device will be prevented.

Preferably, the second level of security has precedence over the first level of security.

In a preferred embodiment, the administrator assigned security setting is according to the access rights determined for a specific user or specific user group.

According to another aspect of the invention, there is provided a hierarchical structure organized by a user of devices of interest to said user, said hierarchical structure created according to the methods of creating a hierarchical structure in terms of folders and sub-folders according to the organizational needs of a user, assigning devices of interest from a pre-existing hierarchical structure to the main folder and sub-folders created in the hierarchical structure, assigning a security setting to the device of interest, wherein the security setting assigned to the said device is the most restrictive security setting of said device in the parent folder of the device of interest, forming a first level of security to the hierarchical structure thus formed.

The user created hierarchical structure of above, where in use, a user is able to view the devices organized that have security settings that are 'read only' and 'full access'.

DESCRIPTION OF FIGURES

In order that the invention might be more fully understood, embodiments of the invention will be described by way of example only, with reference to the accompanying drawings, in which:

Figure 1A shows a pre-existing hierarchical structure organized by manufacturing steps;

Figure 1B shows a pre-existing hierarchical structure organized by location;

Figure 2A shows a detailed pre-existing hierarchical structure organized by location;

Figure 2B shows a detailed pre-existing hierarchical structure organized by sensor type;

Figure 3 shows the method of the present invention;

Figure 4 shows the user organized hierarchical structure formed according to the method of the invention; and

Figure 5 shows the administrative view of a user organized hierarchical structure, using a second level security setting of the present invention.

The attached drawings are not necessarily drawn to scale.

DETAILED DESCRIPTION OF THE INVENTION

Reference will now be made in detail to the preferred embodiments of the invention, examples of which are illustrated in the accompanying drawings. The preferred embodiments of the invention are not intended to limit the invention in its broadest aspect to these embodiments. On the contrary, the invention is intended to cover alternatives, modifications and equivalents, which may be included within the spirit and scope of the invention as defined by the appended claims. Furthermore, in the following detailed description of the embodiments, numerous specific details are set forth in order to provide an understanding of the present embodiments.

The present invention relates to a method of grouping each individual device in a manufacturing plant, by placing each device under a multiple of hierarchies. Advantageously, this provides ease of reference for a user, to obtain access to a particular device, regardless of the role of the system user.

For example, as seen in Figure 2A and 2B, an individual device is shown in different and multiple hierarchies. In Figure 2A, the devices are grouped by location of each device, and in Figure 2B, the devices are grouped by sensor types. Therefore, a level sensor 10, is grouped under 'site', 'area', 'distillation', 'tank', and under 'level' in the location hierarchy, and grouped under the child node of pressure sensors 20, and under the target node of sensor types 30, when grouped by sensors.

Similarly, pressures sensor device 11 is categorized under 'site', 'area', 'heat exchanger', 'pressure' and 'pressure tank 1' as seen in Figure 2A, whereas it is categorized under 'sensor types' and 'sensors', in Figure 2B.

This structure is very rigid, and cannot be manipulated according to the needs of a user.

Each individual user will have his own preferred hierarchical structure, according to his job scope, work style or requirements. For example, a level sensor maintenance engineer would want to be able to view and access the level sensors that he is responsible for, within the networked production facility, in a single hierarchical structure. This is more convenient to the user, as compared to searching for all the level sensors using location folders under multiple hierarchical structures, to finally find the devices of interest. The previous method of locating level sensors of interest is very time consuming, especially if this same search has to be done daily.

The present invention relates to a method of organizing devices of interest to a user, in a single hierarchical structure according to the needs of such a user. As seen in Figure 3, this method includes the steps of creating a hierarchical structure in terms of main folders and sub-folders according to the needs of the user, assigning devices of interest from pre-existing multiple hierarchical structures into the folders and sub-folders created, and assigning a security setting to the device of interest, wherein the security setting assigned to the said device is the most restrictive security setting of this device, in the parent folder of the pre-existing hierarchical structure. This method may be repeated as long as a user wishes to create a further hierarchical structure.

In the hierarchical structure created in the method above, devices of interest to a particular user will be presented to him in the single structure thus created, and the

security settings of the device will follow the security settings previously determined by an administrator, and as presented in the pre-existing multiple hierarchical structure.

In the pre-existing hierarchical structure or structures, the devices are organized according to either the location, or type of device forming multiple hierarchical structures. The security setting for each device emulates the security setting of each parent folder of the device. If the number of devices is large, this process may take a very long time, especially where the pre-existing hierarchical structure is very long.

In the present invention, the hierarchical structure created simply takes on the maximum security under the parent hierarchy, where security settings are made. These security settings may be any one of 'read only', 'hidden', or 'full control'.

These security settings may have a second level of security set by an administrator, which is in accordance to a specific user profile, or a specific user group according to the requirements of a user's organization. This security setting would take precedence over the security settings according to the parent folder.

With a hierarchical structure formed according to the method of the invention, a user having a specific user identification will be able to view the user created hierarchical structure of devices, as long as it does not have the security setting of 'hidden'.

As seen in Figure 4, a user created hierarchical structure for maintenance engineer Suzuki would have a main folder named 'Maintenance', a sub-folder named 'Suzuki', and sub-sub-folders named 'Daily' and 'Weekly'. Devices that user Suzuki has to maintain in a daily period will be located in the 'Daily' sub-sub-folder, and devices that Suzuki has to maintain in a weekly period will be located in the 'Weekly' sub-sub-folder.

Depending on the security settings of the individual devices in all the parent folders of pre-existing hierarchical structures, the same security setting will be applied to the device located in the user defined hierarchy, forming a first level of security for a user.

At an administrator level, the method further includes the step of setting a security setting according to a specific user or user group. This security setting takes precedence over the security settings at the first level.

For example, as seen in Figure 5, an administrator may set user folder 'Suzuki' hidden from user Yamada. Therefore, when user Yamada accesses the hierarchical structure, he will not be able to view or access the devices that user Suzuki has created, even though these devices are not set as 'hidden' in the first level of security. The folder named 'Suzuki' is drawn with dashed lines to signify that it is hidden when user Yamada accesses the hierarchical structure formed by the method of the present invention.

The method has been described in the foregoing, specifically in the use for a networked production facility for device management. However, it is to be understood that this method may also be applied in other networked facilities, or in other organizations that wish to manage their networked resources flexibly.

The embodiments have been advanced by way of example only, and modifications are possible within the scope of the invention as defined by the appended claims.

CLAIMS

1. A method of organizing devices of interest to a user, in a multiple hierarchical structure according to the users of such a user, said device of interest selected from a multiple of hierarchical structures, said method including

creating a hierarchical structure in terms of folders and sub-folders according to the organizational needs of a user;

assigning devices of interest from a pre-existing hierarchical structure to the main folder and sub-folders created in the hierarchical structure;

assigning a security setting to the device of interest;

wherein the security setting assigned to the said device is the most restrictive security setting of said device in the parent folder of the device of interest, forming a first level of security to the hierarchical structure thus formed.

2. A method of organizing devices of interest to a user according to claim 1, wherein the security settings applicable are any one of the following of

(ii) 'read only';

(ii) 'hidden'; or

(iii) 'full control'.

3. A method of organizing devices of interest to a user according to any one of claims 1 or 2, wherein an administrator can assign a security setting to a main folder or sub-folder of a hierarchy, said security setting according to any one of claims 2, said administrator security setting forming a second level of security to the hierarchy.

4. A method of organizing devices of interest to a user according to any one of the preceding claims, wherein the second level of security has precedence over the first level of security.

5. A method of organizing devices of interest to a user according to any one of claims 3 or 4, wherein the administrator assigned security setting is according to the access rights determined for a specific user or specific user group.

6. A hierarchical structure organized by a user of devices of interest to said user, said hierarchical structure created according to the methods of any one of claims 1 to 5.

7. A hierarchical structure organized by a user of devices of interest to said user according to claim 6, where in use, a user is able to view the devices organized that have security settings that are 'read only' and 'full access'.