

INFORMATION MONITORING SYSTEM AND METHOD FOR INDUSTRIAL CONTROL DEVICE NETWORK, COMPUTER-READABLE STORAGE MEDIUM, AND COMPUTER DEVICE

TECHNICAL FIELD

The present disclosure relates to but is not limited to the fields of industrial automation, informatization and computer, and in particular, to an information monitoring system and method for an industrial control device network, a computer-readable storage medium, and a computer device.

BACKGROUND

The industrial control device plays an important role in industrial informatization. It is widely used in industry, power, energy, transportation, water conservancy, public utilities, and production enterprises. The industrial control device can control a wide range of objects, such as production processes, mechanical devices, vehicles, experimental facilities, instruments, living facilities, and household appliances. The industrial control device guarantees the normal operation of industrial facilities through automated monitoring, command, control, and adjustment of work processes, and is an important part of the country's critical infrastructure and information systems.

With the advent of Industry 4.0 and the convergence of industrialization and informatization, the security of traditional industrial control device networks (also known as industrial control security) has become a tough challenge for enterprises and countries and garnered greater attention.

Therefore, it is necessary to propose a technical solution for effective information monitoring of the industrial control device network.

SUMMARY

The present disclosure is intended to solve the above problem.

According to a first aspect of the present disclosure, an information monitoring system for an industrial control device network is provided includes:

- a data acquisition module, configured to obtain device information of a network device in the industrial control device network;

- an information scheduling engine module, configured to receive the device information and store the device information into a database; and

- a database, configured to store the device information.

The information monitoring system for an industrial control device network according to the present disclosure further includes:

- a web service provision module, configured to provide a web service for monitoring the device information for a user.

The information scheduling engine module of the information monitoring system for an

industrial control device network according to the present disclosure includes:

- an acquisition scheduling model module, configured to receive the device information; and
- a database module, configured to store the device information into the database.

The web service provision module of the information monitoring system for an industrial control device network according to the present disclosure includes:

- a user interface (UI) module, configured to provide the user with a UI for inputting a monitoring operation instruction and displaying monitored device information; and
- a backend module, configured to forward the monitoring operation instruction to the database and forward the monitored device information to the UI module.

The information monitoring system for an industrial control device network according to the present disclosure further includes:

- a comprehensive processing module, configured to perform comprehensive processing and analysis on the device information to generate comprehensive information; where
- the UI module is further configured to display the comprehensive information to the user.

The network device of the information monitoring system for an industrial control device network according to the present disclosure includes at least one of the following:

- a programmable logic controller (PLC), a remote terminal unit (RTU), a distributed control system (DCS) controller, an industrial control device, a workstation, a historical data station, an industrial application software product, and a security protection product.

The device information of the information monitoring system for an industrial control device network according to the present disclosure includes at least one of the following:

- device asset information, device performance information, device-related event information, device-related security vulnerability information, device-related security threat information, device-related traffic information, and network topology information.

According to a second aspect of the present disclosure, an information monitoring method for an industrial control device network is provided includes:

- obtaining, by a data acquisition module, device information of a network device in the industrial control device network;
- receiving, by an information scheduling engine module, the device information and storing the device information into a database; and
- using the database to store the device information.

The information monitoring method according to the present disclosure further includes:

- providing, by a web service provision module, a web service for monitoring the device information for a user.

The information monitoring method according to the present disclosure further includes:

receiving, by an acquisition scheduling model module, the device information; and
storing, by a database module, the device information into the database.

The information monitoring method according to the present disclosure further includes:

providing, by a UI module, the user with a UI for inputting a monitoring operation instruction and displaying monitored device information; and

forwarding, by a backend module, the monitoring operation instruction to the database, and forwarding the monitored device information to the UI module.

The information monitoring method according to the present disclosure further includes:

performing, by a comprehensive processing module, comprehensive processing and analysis on the device information to generate comprehensive information; and

displaying, by the UI module, the comprehensive information to the user.

In the information monitoring method according to the present disclosure, the network device includes at least one of the following:

a PLC, an RTU, a DCS controller, an industrial control device, a workstation, a historical data station, an industrial application software product, and a security protection product.

In the information monitoring method according to the present disclosure, the device information includes at least one of the following:

device asset information, device performance information, device-related event information, device-related security vulnerability information, device-related security threat information, device-related traffic information, and network topology information.

According to a third aspect of the present disclosure, a computer-readable storage medium is provided, where the storage medium stores a computer program, and when the computer program is executed by a processor, steps of the foregoing method are implemented.

According to a fourth aspect of the present disclosure, a computer device is provided, including a memory, a processor, and a computer program stored in the memory and capable of running on the processor, where when the computer program is executed by the processor, at least one of the following steps is implemented:

obtaining, by a data acquisition module, device information of a network device in the industrial control device network;

storing, by an information scheduling engine module, the device information into a database;

using the database to store the device information;

providing, by a web service provision module, a web service for monitoring the device information for a user;

receiving, by an acquisition scheduling model module, the device information;

storing, by a database module, the device information into the database;

providing, by a UI module, the user with a UI for inputting a monitoring operation instruction and displaying monitored device information; and

forwarding, by a backend module, the monitoring operation instruction to the database, and forwarding the monitored device information to the UI module.

The present disclosure provides an information monitoring system and method for an industrial control device network, a computer-readable storage medium, and a computer device, which implement effective information monitoring for the industrial control device network.

By reading the following description of the example embodiments with reference to the accompanying drawings, those skilled in the art will be clear about other characteristics, features and advantages of the embodiments of the present disclosure.

BRIEF DESCRIPTION OF DRAWINGS

The drawings incorporated into the specification and constituting a part of the specification illustrate the embodiments of the present disclosure, and are used together with the description to explain the principles of the embodiments of the present disclosure. In these drawings, similar reference signs are used to represent similar elements. The drawings in the following description are a part rather than all of the embodiments of the present disclosure. Persons of ordinary skill in the art can obtain other drawings based on these drawings without creative efforts.

FIG. 1 is a schematic diagram of an information monitoring system for an industrial control device network according to a first aspect of the present disclosure.

FIG. 2 is a schematic flowchart of an information monitoring method for an industrial control device network according to a second aspect of the present disclosure.

DETAILED DESCRIPTION

In order to make the objectives, technical solutions and advantages of the embodiments of the present disclosure clearer, the following clearly and completely describes the technical solutions in the embodiments of the present disclosure with reference to accompanying drawings in the embodiments of the present disclosure. Apparently, the described embodiments are some rather than all of the embodiments. All other embodiments obtained by persons of ordinary skill in the art based on the embodiments of the present disclosure without creative efforts shall fall within the scope of the present embodiments. It should be noted that the embodiments in the application and features in the embodiments of the present disclosure may be combined with each other in a non-conflicting situation.

FIG. 1 is a schematic diagram of an information monitoring system for an industrial control device network according to a first aspect of the present disclosure.

As shown in FIG. 1, the information monitoring system for an industrial control device network according to the first aspect of the present disclosure includes:

a data acquisition module, configured to obtain device information of a network device (not shown in FIG. 1) in the industrial control device network;

an information scheduling engine (module), configured to receive the device information and store the device information into a database; and

a database, configured to store the device information.

For example, as shown in FIG. 1, the data acquisition module can be deployed in a distributed manner in a complex network, with minimal or no impact on network performance.

For example, the acquired device information may be preprocessed, converted into a predetermined unified format, and submitted to another module or component (for example, a comprehensive processing module described below or a component related to it) for comprehensive processing and analysis.

The data acquisition module can also acquire information from all protected objects (that is, network devices) together.

Optionally, the information monitoring system for an industrial control device network according to the first aspect of the present disclosure further includes:

a web service (provision module), configured to provide a web service for monitoring the device information for a user.

Optionally, the information scheduling engine module of the information monitoring system for an industrial control device network according to the first aspect of the present disclosure includes:

an acquisition scheduling model (module), configured to receive the device information; and

a database module, configured to store the device information into the database.

Optionally, the web service provision module of the information monitoring system for an industrial control device network according to the first aspect of the present disclosure includes:

a UI (module), configured to provide the user with a UI for inputting a monitoring operation instruction and displaying monitored device information; and

a backend (module), configured to forward the monitoring operation instruction to the database, and forward the monitored device information to the UI module.

Optionally, the information monitoring system for an industrial control device network according to the first aspect of the present disclosure further includes:

a comprehensive processing module, configured to perform comprehensive processing and analysis on the device information to generate comprehensive information; where

the UI module is further configured to display the comprehensive information to the user.

For example, the comprehensive processing module may include four modules: a device monitoring module, a security information management module, an industrial control threat management module, and a unified interface module.

The device monitoring module can identify and sort monitored objects and provide basic information support, which may include device management, industrial control topology building, device and link performance status monitoring, and industrial control device identification and monitoring. The security information management module can comprehensively manage security event information and vulnerability information in the industrial control network, which may include centralized management and query services of security events, centralized management of vulnerability information, security information management of protection products, and management of security knowledge bases. The industrial control threat management module can integrate link and device monitoring with various security information to form threat discovery-oriented presentation and analysis capabilities, and can provide risk management, industrial control business health analysis, correlation analysis, and KPI-based threat analysis. The unified interface module can integrate external interfaces, and provide an alarm interface for centralized monitoring output for enterprises, an interface for information acquisition of third-party protection products, and an interface for probe management and information exchange of national-level monitoring systems.

Optionally, the network device of the information monitoring system for an industrial control device network according to the first aspect of the present disclosure includes at least one of the following:

a programmable logic controller (PLC), a remote terminal unit (RTU), a distributed control system (DCS) controller, an industrial control device, a workstation, a historical data (storage) station, an industrial application software product, and a security protection product.

Optionally, the device information of the information monitoring system for an industrial control device network according to the first aspect of the present disclosure includes at least one of the following:

device asset information, device performance information, device-related event information, device-related security vulnerability information, device-related security threat information, device-related traffic information, and network topology information.

For example, the device information may include information of various (security) devices deployed in the industrial control device network, such as events, alarms, assets, topology, performance, events, vulnerabilities, traffic, and industrial control instructions.

FIG. 2 is a schematic flowchart of an information monitoring method for an industrial control device network according to a second aspect of the present disclosure.

As shown in solid boxes in FIG. 2, the information monitoring method for an industrial control device network according to the second aspect of the present disclosure includes the following steps:

Step S202: A data acquisition module obtains device information of a network device in the

industrial control device network.

Step S204: An information scheduling engine module receives the device information, and stores the device information into a database.

Step S206: Use the database to store the device information.

Optionally, as shown in dashed boxes in FIG. 2, the information monitoring method according to the second aspect of the present disclosure further includes the following step.

Step S208: A web service provision module provides a web service for monitoring the device information for a user.

Optionally, as shown in dashed boxes in FIG. 2, the information monitoring method according to the second aspect of the present disclosure further includes the following steps.

Step S210: An acquisition scheduling model module receives the device information.

Step S212: A database module stores the device information into the database.

Optionally, as shown in dashed boxes in FIG. 2, the information monitoring method according to the second aspect of the present disclosure further includes the following steps.

Step S214: A UI module provides the user with a UI for inputting a monitoring operation instruction and displaying monitored device information.

Step S216: A backend module forwards the monitoring operation instruction to the database, and forwards the monitored device information to the UI module.

Optionally, as shown in dashed boxes in FIG. 2, the information monitoring method according to the second aspect of the present disclosure further includes the following steps.

Step S218: A comprehensive processing module performs comprehensive processing and analysis on the device information to generate comprehensive information.

Step S220: The UI module displays the comprehensive information to the user.

Optionally, in the information monitoring method according to the second aspect of the present disclosure, the network device includes at least one of the following:

a PLC, an RTU, a DCS controller, an industrial control device, a workstation, a historical data station, an industrial application software product, and a security protection product.

Optionally, in the information monitoring method according to the second aspect of the present disclosure, the device information includes at least one of the following:

device asset information, device performance information, device-related event information, device-related security vulnerability information, device-related security threat information, device-related traffic information, and network topology information.

According to a third aspect of the present disclosure, a computer-readable storage medium is provided, where the storage medium stores a computer program, and when the computer program is executed by a processor, steps of the foregoing method are implemented.

According to a fourth aspect of the present disclosure, a computer device is provided, including a memory, a processor, and a computer program stored in the memory and capable of running on the processor, where when the computer program is executed by the processor, at least one of steps S202 to S220 is implemented.

The present disclosure provides an information monitoring system and method for an industrial control device network, a computer-readable storage medium, and a computer device, which implement effective information monitoring for the industrial control device network.

The content described above can be implemented individually or in various combinations, and these modifications are all within the protection scope of the embodiments of the present disclosure.

Finally, it should be noted that the foregoing embodiments are only used to explain the technical solutions of the present disclosure, and are not intended to limit the same. Although the present disclosure is described in detail with reference to the foregoing embodiments, those of ordinary skill in the art should understand that they can still modify the technical solutions described in the foregoing embodiments, or make equivalent substitutions on some technical features therein. These modifications or substitutions do not make the essence of the corresponding technical solutions deviate from the spirit and scope of the technical solutions of the embodiments of the present disclosure.

INDUSTRIAL APPLICABILITY

The present disclosure provides an information monitoring system and method for an industrial control device network, a computer-readable storage medium, and a computer device, which implement effective information monitoring for the industrial control device network.

What is claimed is:

1. An information monitoring system for an industrial control device network, comprising:
a data acquisition module, configured to obtain device information of a network device in the industrial control device network;
an information scheduling engine module, configured to receive the device information and store the device information into a database; and
a database, configured to store the device information.
2. The information monitoring system according to claim 1, further comprising:
a web service provision module, configured to provide a web service for monitoring the device information for a user.
3. The information monitoring system according to claim 1, wherein the information scheduling engine module comprises:
an acquisition scheduling model module, configured to receive the device information; and
a database module, configured to store the device information into the database.
4. The information monitoring system according to claim 2, wherein the web service module comprises:
a user interface (UI) module, configured to provide the user with a UI for inputting a monitoring operation instruction and displaying monitored device information; and
a backend module, configured to forward the monitoring operation instruction to the database, and forward the monitored device information to the UI module.
5. The information monitoring system according to claim 4, further comprising:
a comprehensive processing module, configured to perform comprehensive processing and analysis on the device information to generate comprehensive information; wherein
the UI module is further configured to display the comprehensive information to the user.
6. The information monitoring system according to claim 1, wherein the network device comprises at least one of the following:
a programmable logic controller (PLC), a remote terminal unit (RTU), a distributed control system (DCS) controller, an industrial control device, a workstation, a historical data station, an industrial application software product, and a security protection product.
7. The information monitoring system according to claim 1, wherein the device information comprises at least one of the following:
device asset information, device performance information, device-related event information, device-related security vulnerability information, device-related security threat information, device-related traffic information, and network topology information.
8. An information monitoring method for an industrial control device network, comprising:

obtaining, by a data acquisition module, device information of a network device in the industrial control device network;

receiving, by an information scheduling engine module, the device information and storing the device information into a database; and

using the database to store the device information.

9. The information monitoring method according to claim 8, further comprising:

providing, by a web service provision module, a web service for monitoring the device information for a user.

10. The information monitoring method according to claim 8, further comprising:

receiving, by an acquisition scheduling model module, the device information; and

storing, by a database module, the device information into the database.

11. The information monitoring method according to claim 9, further comprising:

providing, by a UI module, the user with a UI for inputting a monitoring operation instruction and displaying monitored device information; and

forwarding, by a backend module, the monitoring operation instruction to the database, and forwarding the monitored device information to the UI module.

12. The information monitoring system according to claim 11, further comprising:

performing, by a comprehensive processing module, comprehensive processing and analysis on the device information to generate comprehensive information; and

displaying, by the UI module, the comprehensive information to the user.

13. The information monitoring method according to claim 8, wherein the network device comprises at least one of the following:

a PLC, an RTU, a DCS controller, an industrial control device, a workstation, a historical data station, an industrial application software product, and a security protection product.

14. The information monitoring method according to claim 8, wherein the device information comprises at least one of the following:

device asset information, device performance information, device-related event information, device-related security vulnerability information, device-related security threat information, device-related traffic information, and network topology information.

15. A computer-readable storage medium, wherein the storage medium stores a computer program, and when the computer program is executed by a processor, steps of the method according to any one of claims 8 to 14 are implemented.

16. A computer device, comprising a memory, a processor, and a computer program stored in the memory and capable of running on the processor, wherein when the computer program is executed by the processor, at least one of the following steps is implemented:

obtaining, by a data acquisition module, device information of a network device in an industrial control device network;

receiving, by an information scheduling engine module, the device information and storing the device information into a database;

using the database to store the device information;

providing, by a web service provision module, a web service for monitoring the device information for a user;

receiving, by an acquisition scheduling model module, the device information;

storing, by a database module, the device information into the database;

providing, by a UI module, the user with a UI for inputting a monitoring operation instruction and displaying monitored device information; and

forwarding, by a backend module, the monitoring operation instruction to the database, and forwarding the monitored device information to the UI module.