SOLUTION BRIEF

ABB Ability™ Cyber Security Asset Inventory

Automatic inventory for OT systems

Executive summary

Challenge
Industrial control systems consist of a diverse group of technologies of different ages. Typically, the inventory of these systems are maintained manually, which is time-consuming, expensive and inefficient.

Solution
ABB Cyber Security Asset Inventory uses technology that automatically and inherently identifies cyber assets, and captures inventory information such as ports, services and software. Cyber Asset Inventory provides up-to-date information on control networks and can help in decision-making on issues of cyber security, asset lifecycle and asset management.

Benefits
- Significant cost savings
- Shorter incident response
- Simplified compliance and regulatory reporting
- Better IT/OT collaboration
- Ability to troubleshoot network issues
- Automatic inventory monitoring

—
01 Cyber Security Asset Inventory automatically identifies cyber assets and provides up-to-date information on control systems.

An accurate cyber asset inventory is critical for maintaining any cyber security program. In most global industrial cyber security standards and frameworks, requirements exist for operators of critical infrastructure to be able to define cyber security risks and show that they can monitor them. In addition to these requirements, security professionals managing incident response must understand a control system's authorized cyber asset inventory in order to mitigate risks and make decisions. This information facilitates effective defense against cyber-attacks.

Operational information such as asset owner, relationships to other assets, service agreements, support numbers, external access requirements and application criticality can be used to determine whether a device or application is authorized, and may accelerate efforts to recover from a cyber incident. An automated, inherent, centralized asset inventory solution reduces time required to address cyber risks, cuts costs associated with risk management, improves incident response and provides an accurate inventory to mitigate cyber risks.

Challenge
Finding and documenting all cyber assets requires significant effort. Most industrial control systems consist of a diverse group of technologies of different ages, which generally have an operating life of 10 to 30 years. Over time, components are added, removed and changed on the control network.

Typically, cyber asset inventory upkeep is done manually. This is time-consuming, expensive, and results in an incomplete inventory that is outdated as soon as the upkeep is completed.

Often, changes to the network are not documented in a way that supports operational needs (such as troubleshooting) or enterprise cyber needs (such as preparing cyber inventory documentation for audits or assessments). Asset inventory audits require different metrics and report formats, often on short notice.

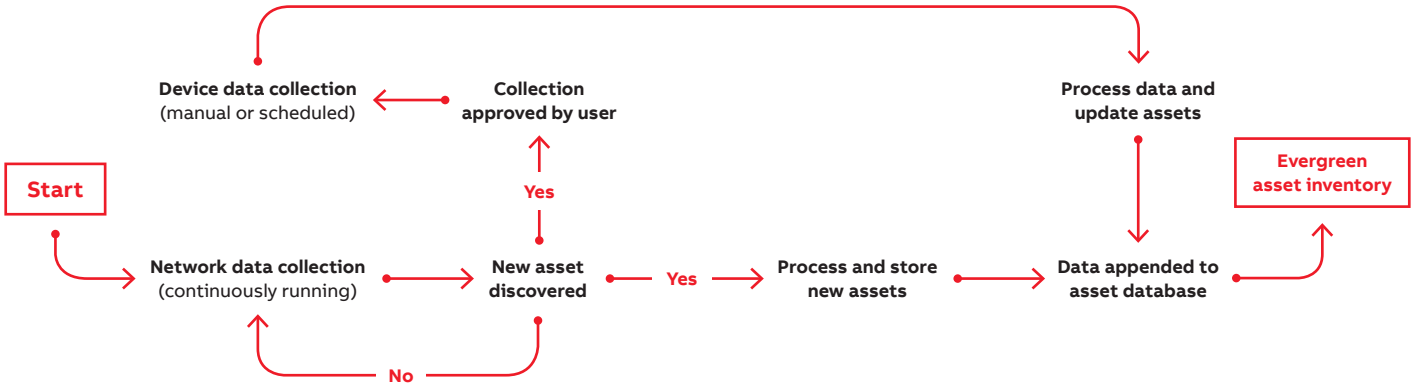
Generally, the cyber asset inventory is identified by third-party cyber security consultants, which usually require production units to be off-line for active scanning. This adversely impacts control system operational integrity, introduces production risks, and adds significant operational costs, all of which negatively affect a business.

ABB's solution
ABB Cyber Security Asset Inventory automatically identifies cyber assets and captures updated inventory information on ports, services and software connected to the control networks. The solution enables users to make better operational, compliance and risk decisions related to cyber security controls, asset lifecycle and asset management.

Overview
Network data collection: Cyber Security Asset Inventory continuously monitors network traffic and detects new and changed assets. This data is automatically stored in the asset database.

Device data collection: Users can manually trigger a device data collection to gather more information on a specific asset. Data from the device collection are appended to the database record. Users can configure the device collection to automatically collect and update the data from known and detected assets. By combining data from both the network and device collectors, users will know assets that are present in the system, software packages that are installed and devices that are communicating with each other.

—
02 How does Cyber Asset Inventory work?



—
02

—
03 Example information, AC800M

—
04 Fleet wide inventory data collected by ABB Ability Cyber Security Asset Inventory

Information collected by ABB Cyber Security Asset Inventory

All network-enabled devices reveal valuable information about themselves when connected to a network. This data can be collected by monitoring network traffic. Data is parsed and stored in the asset database. Changes are detected and the database is updated. Figure 3 is an example of what can be gathered from an AC800M controller through automatic network data collection.

Figure 4 shows the fleet-wide inventory data matrix that ABB Cyber Security Asset Inventory can automatically collect. The inventory includes device details such as operating system version, open ports, device vendor model, firmware version, serial number, I/O modules and vulnerabilities for all major industrial control systems and 35+ industrial protocols.

This level of detailed data collection expedites response to vulnerabilities and incidents. This information can be sorted by application, by operating system, or any other available data point, making identifying exposures to vulnerabilities less daunting.

Data	Information
IP address	192.16.80.151 (Private IP)
Host name	controller_1
Other host names	
MAC addresses	00:0C:29:2E:A4:E2 (Vmware) 00:00:23:0A:10:12 (AbbAutom)
Networks	800XA (172.16.0.0/16)
Role	PLC
Other roles	Slave, File server, Web server
Vendor/model	ABB (AC 800 M PM861)
Other vendors/models	ABB, ABB(AC 800 M/PEC)
OS version	
Client protocol(s)	ABB_CNCP (UDP), ABB_RNRP (UDP), NoData (TCP)
Server protocol(s)	FailedConnection (TCP), HTTP (TCP), MMS (TCP), NFS (TCP), NoData (TCP), NotAKnownOne (TCP)

Labels	firmware_version=5.0.2004.52
	module_identity=CI867A;
	rev:5.0.2002.10
	module_identity=PM861 C;
	rev:5.0.2004.52
	project=Boiler

Purdue level	1 – Process control

—
03

	ABB			Siemens	Rockwell Automation		Emerson		GE	SEL	Honeywell	Yokogawa		Phoenix Contact
	800xA	Symphony Plus	Freelance	S7	Logix	PLC5/SLC500	Ovation	DeltaV	Mark V/Vie RX31		Experion	Schneider Modicon	Centum	PROFINET
IP address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
MAC address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Vendor	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Client protocols	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Server protocols	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Role	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Host name	✓			✓	✓			✓		✓		✓	✓	3)
Device model	✓			✓	✓		✓	✓	✓	1)		✓	✓	✓
Firmware version	✓			✓	✓			✓	✓	1)	✓	✓		N/A
Serial number	N/A			✓	✓				✓	1)		✓		N/A
Device ID			N/A	N/A	N/A	N/A	✓	N/A		1)		✓	✓	N/A
Module(s) identity	✓			2)				2)	✓	N/A		2)		N/A
Project name	✓									N/A		✓		N/A

—
04

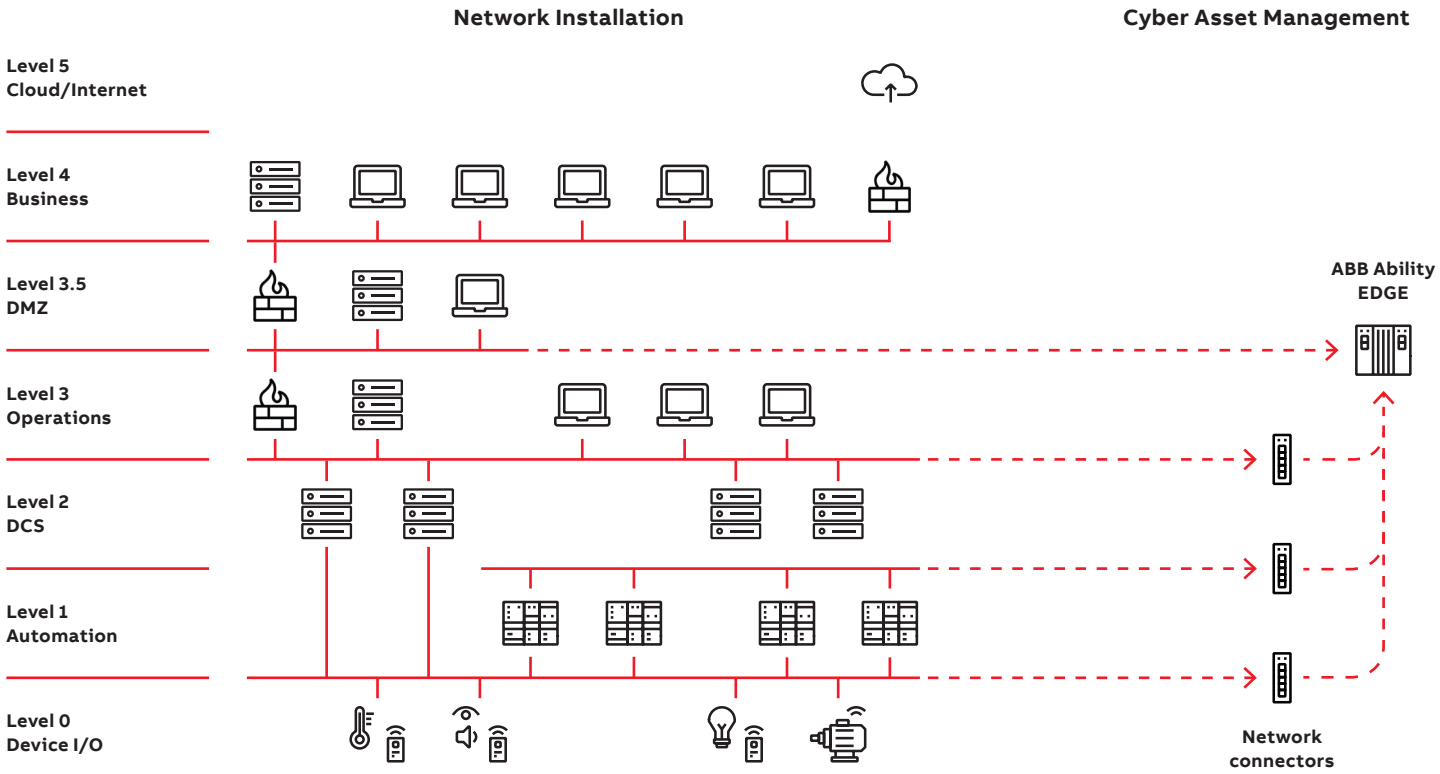
—
05 Typical network installation

How is data collected?
The mirror ports, or TAPs, are used to automatically monitor network traffic and analyze industrial protocol communications to automatically generate a full cyber asset inventory and complete communications analysis of devices on monitored networks (Figure 5).

Automatic information collection allows continuous monitoring of changes in the control network without impacting network availability. If something has been added to the control network, or if something stops communicating, an alert is created to provide an updated view of the inventory.

ABB Cyber Security Asset Inventory allows manual input of assets that are not online, or are not connected to an ethernet network, such as a USB printer. In addition to manual input, Cyber Security Asset Inventory provides an interface that allows administrative rights access to execute a device scan by selecting a single device and acquiring more detailed cyber inventory information. The collection is done with simple native MS Windows commands activated through the user interface.

Because all networks are different, and availability is top priority, ABB recommends that this tool be used when control networks are in a scheduled outage . Data collected through the interface completes the cyber asset inventory so it can be printed or exported in various formats, including PDF and .csv.



—
05

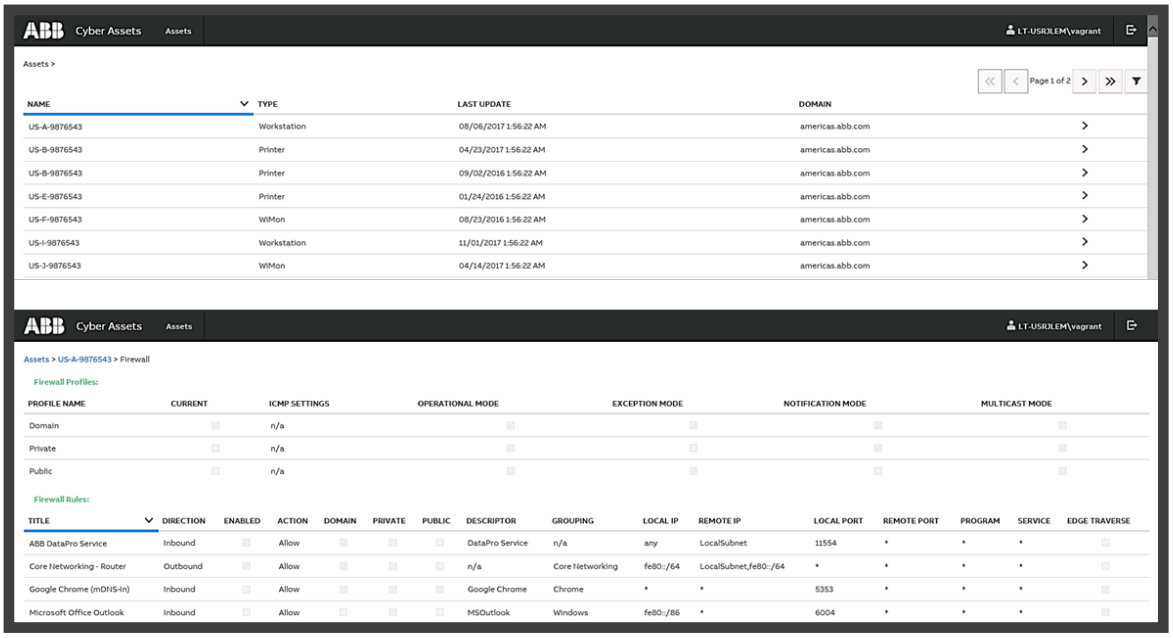
Scope

- **Implementation**
  - Review of the control network to define ability to use existing network switches and optimal configuration of mirroring and in some cases placement of TAPs to monitor network.
  - Due to potential interactions with the network, specifically changing configuration to implement mirror ports, or unplugging trunk ports to install TAPs, it is recommended that the process not be online during the networking phase.
  - Once network switches are configured or TAPs are installed, plugging in ABB Cyber Security Asset Inventory will not affect the system network. It only monitors traffic; it does not modify traffic in any way.
  - Installation service, system tuning and support to ensure appropriate logging is sent to corporate security users

- **Easy-to-use interface**
  - Web-based user interface
  - Automatic detection of new, missing, removed and changed assets
  - Device scan for more detailed asset data
  - Manual input of asset functionality to add additional asset details
  - Comment field to make notes related to an asset

- **Review and Reporting**
  - Data from passive network and device data collections are seamlessly displayed (Figure 6)
  - Only authenticated users get access
  - Digital record of cyber assets: computers, network devices, controllers, instruments, etc.
  - User can navigate the data and transition from high-level overviews to precise details
  - Views can be filtered and sorted
  - Search for anything among all assets
  - Export data
  - Event list shows added, removed, missing and updated assets
  - Connect to company email server to send notifications to users

—
06 Cyber Security Asset Inventory web-based user interface provides easy access to data.



—
06

—
07 ABB Ability Cyber Asset Inventory provides many benefits to users and organizations

Benefits

- **Time and cost reduction**

An automated asset inventory solution saves time, which saves money. Because the asset information is aggregated into a single pane of glass, the asset owner has immediate access to their asset inventory. Automating asset inventory also reduces the costs associated with physical inspections, including paying personnel to perform frequent site visits and vehicle maintenance expenses.

- **Improved incident responses**

An accurate asset inventory helps reduce the amount of time required to effectively manage vulnerabilities and incident responses. The first step in vulnerability management or incident response is to understand the organization's exposure and impact in the event of a cyber incident. If control system owners know the assets they have in their environment (the baseline), users can conduct thorough vulnerability and risk analyses to prioritize assets and spending, and prepare contingency plans to mitigate risk from unexpected incidents. It also keeps a historical record of this information, so that if an incident occurs, organizations have the data to continuously improve response strategies to ensure employee safety and minimize financial damage from unexpected downtime.

- **Simplified compliance and regulatory reporting**

Automatic network monitoring makes complying with standards such as the NIST Cybersecurity Framework, NERC CIP and IEC 62443 easier by automatically collecting and presenting asset inventory information necessary for compliance reporting. ABB Ability Cyber Security Asset Inventory provides comprehensive details on each asset including IP address, host name, vendor, model of the asset, operating system version, firmware version of industrial control system devices, and device module information. Assets and their communications are also visualized in an interactive network map and grouped by device type and network. This provides a clear understanding of which devices sit in which part of the network and how they are connected with each other. The information can easily be exported and included in compliance documentation, resulting in an audit-proof asset inventory with minimal effort.

- **Better IT/OT Collaboration**

Information Technology (IT) and Operational Technology (OT) have different objectives: IT's top priority is to protect data; OT's top priority is to protect the availability and integrity of industrial production processes. However, because of the widespread adoption of IT protocols in OT networks, today's IT and OT departments must cooperate to protect the industrial control system network. Chief Information Officers and Chief Information Security Officers now find themselves with a degree of responsibility for unexpected downtime, equipment damage or safety risks in their companies caused by cyber incidents affecting industrial control systems. ABB Ability Cyber Security Asset Inventory improves the strategic alignment between IT and OT by providing real-time visibility behind the OT firewall and establishing a baseline from which a mutual defense of the network can be built.

—
07

—
08 ABB Cyber Security Asset Inventory saves labor hours for companies

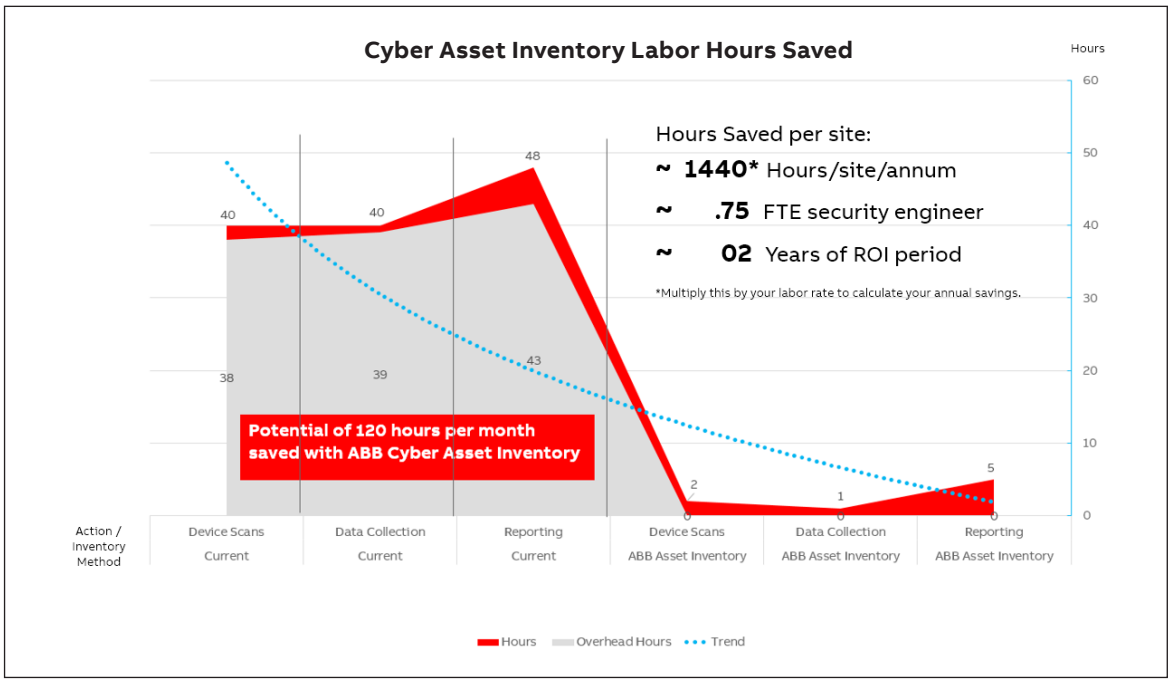
Summary

ABB Cyber Security Asset Inventory works across most major control systems in the power generation space. With easy-to-use reporting features supporting compliance activities such as regulatory audit of software, ports and services, and ongoing risk assessments, it reduces time required for operations teams to maintain this information.

In addition to reducing time and costs associated with cyber data collection activities, ABB Cyber Security Asset Inventory also provides improved visibility into plant control networks and anomalies related to the authorized baseline for corporate security professionals to use for incident response and recovery.

With the simple web-based user interface, ABB Cyber Security Asset Inventory offers flexible data collection and the capability to quickly add new devices throughout the lifecycle of the control network.

ABB Cyber Security Asset Inventory improves the strategic alignment between IT and OT by providing real-time visibility behind the OT firewall and establishing a baseline for defending the network.



	Time required with manual cyber asset inventory methods (hours/month)	Time required with ABB Cyber Asset Inventory (hours/month)
Device scans	40	2 (for new devices discovered)
Data collection and analysis	40	1
Reporting	48	5
Total	128	8

- **Total estimated labor hours saved per month = 120**
- **Total estimated labor hours saved per year = 1440***

—
08 *Multiply this by your labor rate to calculate your annual savings.

—

ABB
Operating in more than 100 countries.

www.abb.com/cybersecurity

8VZZ001190T00001