How Next-Gen Systems of Action Can Improve Your Operational Technology Management

In this era of increasingly connected manufacturing processes, it’s difficult to generate a complete picture of the operational technology (OT) environment — let alone efficiently secure, monitor and manage it. Compounding this issue is the need to maximize productivity across personnel and systems, as well as the rise in cybersecurity threats against industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. Proper OT management is a critical aspect of minimizing unplanned downtime, managing operational costs and detecting and responding to cyber threats.

The solution to these OT challenges is to deploy a single digital platform that offers a complete, contextual view of all assets, allowing manufacturers to secure their equipment and keep everything up and running. Once these assets are integrated into a single system of action, they can connect equipment to production processes and digital workflows. This ability to “see” all assets in one place lets manufacturers easily assess, prioritize and respond to OT events and threats, driving success across the entire operation.

The Drawbacks of Traditional OT Management

Traditional OT management, which is still spreadsheet based in many organizations, doesn’t scale to the demands of modern digital manufacturing. These legacy management processes expose production processes to potential downtime, preventing plants from reaching their full potential. Manufacturers can experience strain on their OT management in several ways. For one, having to manually track, manage and update various operational technologies is labor-intensive, preventing information technology (IT) managers from focusing on more important tasks. In addition:

• Manufacturers face difficulties in maintaining and retiring OT systems.
• Legacy systems are a challenge to monitor and manage.
• There is an increasing need to secure assets from threats.
• Managing and updating various OT systems manually is labor-intensive, preventing valuable resources from focusing on more critical tasks.

The lack of a full picture of the OT landscape has increased the need to secure assets from cybersecurity threats, putting both people and production processes at risk. From 2019 to 2020 alone, there has been a 25 percent increase in ICS vulnerabilities, with 60 percent of heavy industries reporting a breach in ICS or SCADA systems.1 Another 28 percent of manufacturers reported a loss of revenue due to cyberattacks.2 While IT teams have made some progress in securing and managing their assets across the enterprise, it’s time to extend these improvements to OT system management.

Common OT Needs

• Connecting new sensors or edge devices
• Connecting a SCADA system to the historian
• Connecting data to the Cloud
• Applying a systems upgrade
• Requesting a robotics program update
• Reporting a system incident or data quality problem
• Changing a name tag or updating tag configurations
• Retrieving archived data
• Viewing asset inventories
• Managing reported incidents
• Responding to cybersecurity vulnerabilities

1. X-Force Threat Intelligence Index, IBM, 2020
2. Critical Infrastructure Companies and the Global Cybersecurity Threat, McKinsey, April 2019
Monitoring Infrastructure with Sophisticated CMDB Applications

To avoid unplanned downtime, keep costs low and secure assets, manufacturers need a new approach to managing their OT environment — one that creates a single, integrated view of the IT and OT estate in one unified place. When it comes to OT assets in particular, manufacturers’ needs fall into three general categories:

• **Visibility.** Having a single view of all assets, including the location, configuration and health data, can significantly improve OT asset availability.

• **Service management.** To improve their response to OT service requests, manufacturers require proper incident, request, problem and change management.

• **Security and governance.** Better vulnerability detection and response efforts can reduce risk and increase compliance in OT environments.

Sophisticated Configuration Management Database (CMDB) applications can provide the necessary visibility, security and availability that are missing from traditional OT management processes. These systems allow manufacturers to build logical representations of their assets and the relationships between them that comprise their organization’s infrastructure. Compared to traditional CMDBs, which were limited in scope and capabilities, these next-generation systems are broader — guided by a common service data model (CSDM) that supports multiple configuration strategies and includes guidelines for using base system tables and relationships. Using this framework, the CMDB application connects all functions that are necessary to manage OT assets and combines data from third-party sources, from data management software to cybersecurity platforms, into one single source of truth.

Asset Discovery and the OT Class Model

To align OT assets within the database, these sophisticated applications utilize an OT class model that reflects the Purdue Model for enterprise architecture. The levels are as follows:

• **Level 0:** The field-level devices like sensors, actuators and robotics.

• **Level 1:** The programmable logic controllers (PLC) and remote terminal unit (RTU).

• **Level 2:** The human–machine interface that connects distributed control systems, SCADA servers, and HMI.

• **Level 3:** The manufacturing execution systems and operations management systems, historians EWS, and SCADA clients.

• **The demilitarized zone (DMZ):** The security systems, firewalls and proxies that separate the IT and OT worlds.

Using these classes, the CMDB leverages advanced identification and reconciliation tools to discover and tag OT and IT assets on OT network, as well as automatically reconcile any data integrity issues, integrating with third-party security vendors for asset discovery. Any OT configuration items (CI) that are discovered on the OT network – Levels 0 to DMZ via OT security vendors – are designated as operational technology. IT assets on OT network can be discovered by ServiceNow’s discovery engine, while the same assets can be discovered as an OT asset by third party security vendor, and it merges the records as a single record. For example, it may recognize an industrial PC running on a Windows server on the IT side. It will also identify the PC as a SCADA system on the OT side, then merge both discoveries under a single IP address within the system. Using this class model, the CMDB can then build visual representations of the assets, along with the relationships between them.

The Benefits of Extending Digital Workflows to the OT World

• Increased system availability through improved response and recovery

• Less reliance on institutional knowledge and industry practices

• Lower operating costs due to the elimination of redundant processes

• Increased control over distributed operations

• Better security through an integrated cybersecurity approach across IT/OT

• More consistent risk management across technology domains

• Improved governance and management of OT systems

• Better overall plant safety
To improve OT management and visibility, the ServiceNow® CMDB provides visual representations of asset relationships. Generate asset maps — from the field level up to the advanced control systems.

Effective Vulnerability Solutions Management

In addition to automating the asset discovery process and improving OT visibility via visualizations, sophisticated CMDB applications use the data to enhance the vulnerability solutions management process. Once it brings all asset information into the database, the CMDB “triares” the data using artificial intelligence (AI) to process and prioritize the information. In other words, the software automatically factors in the assets’ contextual information — including their hardware, criticality and other attributes — and organizes the information so manufacturers can easily see which assets require immediate attention. Manufacturers can then trigger digital workflows — to correct a security vulnerability, for example. This process brings several benefits, enabling manufacturers to:

• Easily view the highest-priority vulnerability options.
• Identify the highest-impact solutions for active vulnerabilities.
• Monitor the progress of deployed solutions.
• Identify earlier “hot-fix” solutions when the latest solutions are too broad to test and deploy quickly.

A vulnerability solutions management dashboard.
It All Starts With OT Management

At ServiceNow, we’re already building the future of IT with digital workflows on a single, unified platform. We’re now extending these benefits to the OT world. Our ServiceNow® CMDB application, which introduces a new OT class model, sheds light on the various network relationships with OT assets and also maps out the dependent relationships, providing manufacturers with a fuller, more complete view of their assets.

By unlocking OT visibility in this way, our single system of action empowers manufacturers to lower operating costs, quickly resolve security issues — and act with confidence. To learn more about how ServiceNow can help you improve your OT management, please visit www.servicenow.com/otmanagement