



OPERATIONAL TECHNOLOGY: DIGITIZING AND SECURING FACTORIES OF THE FUTURE

Abstract

The footprint of operational technology assets in the manufacturing industry is growing rapidly as the cloud, 5G and Industrial Internet of Things (IIoT) become ubiquitous. These solutions connect the shopfloor to boost productivity, efficiency and business growth. However, a digital factory with smart devices requires an enterprise view of the infrastructure to achieve business goals. As a result, Operational Technology Management (OTM) is transforming into the backbone of smart manufacturing systems.



Introduction

OTM frameworks provide a unified view of OT assets, enabling superior management and effective support for plant and machinery. In addition, they offer real-time insights about the performance of connected devices. However, interconnected OT infrastructure is a source of risk. According to a joint survey by the Manufacturers Alliance for Productivity and Innovation (MAPI), manufacturers

report that operational risks, including cybersecurity, are an impediment to smart factory initiatives. It is a concern, as data does not reside within the enterprise in IIoT deployments, which combine cloud services, networked assets and edge computing devices. Further, a centralized view of the IT-OT environment is often obstructed by the diversity of OT assets operating with varied IIoT software.

The Cybersecurity and Infrastructure Security Agency (CISA) identified 1,200+ OT system-related security issues that affect production facilities. The consequences of a major security issue: plant shutdown, supply chain disruption, cost of resolution, and reputational risks.

IT safeguards OT

Building cyber resilience is imperative to safeguard people, OT assets, and information in a smart factory. This can be achieved with effective cybersecurity measures spanning IT and OT.

First and foremost, OT investment decisions should be made by plant managers in consultation with IT operations and security teams. This partnership ensures compatibility of new IoT devices, IIoT use cases and OT solutions with the existing IT infrastructure and network security capabilities. Besides, it drives adoption of OT systems with pre-built security, and integration of cybersecurity workflows with industrial control operations.

Second, manufacturers should undertake regular cybersecurity maturity assessment and establish a cybersecurity governance program focused on the OT footprint. It ensures compliance with the latest cybersecurity standards while enabling detection of threats and cyber events. Proven IT security management tools evaluate the OT landscape and safeguard the digital operating environment with credible intelligence for proactive response. Moreover, digital tools enhance preparedness for risk mitigation, incident management and recovery from cyberattacks.

Third, IT teams should create a catalog of OT assets and identify siloed systems to be decommissioned. The interdependence of components in industrial automation and control systems should be mapped for effective risk management. The Purdue enterprise reference architecture establishes interrelationships between assets in the OT network of a manufacturing enterprise.

Finally, industrial enterprises should automate cybersecurity systems and implement rule-based processes. It enables rapid response to incidents and faster issue resolution. Automated monitoring and alert mechanisms reduce IT issues and tickets through real-time diagnostics and prioritization of action based on the risk profile. In addition, automated systems detect anomalies in the OT environment, which helps manage phishing, ransomware attacks and other vulnerabilities.




OTM security powered by Infosys and ServiceNow

[Infosys and ServiceNow](#) have collaborated to jointly offer solutions to safeguard the OT environment of industrial facilities.

ServiceNow Operational Technology Management (OTM) integrates the manufacturing landscape, providing visibility into engineering and IT assets, disparate industrial control systems, equipment from different suppliers, and aging machinery retrofitted with IIoT protocols. It supports OT hardware and software – control systems (process controllers, sensors, DCS, PLC, and SCADA), automation systems (HVAC, materials handling, energy management, and remote monitoring), tracking solutions (asset, vehicle, inventory, and people), office equipment (scanners, computers and printers), and personal devices (wearable safety devices and badge readers). It also supports communication network equipment as well as embedded applications. Significantly, it protects data processed at the edge and stored on the cloud.

ServiceNow Operational Technology Management, with integrated workflows enhanced by [Infosys Cobalt](#) cloud blueprints, transforms the operations infrastructure by providing a single pane view of the configuration and health of OT devices. The OTM platform enhances discovery of IT and OT assets, networked systems and intelligent devices across and beyond the shopfloor, be it using standard or bespoke network communication and connectivity protocols. It provides a single source of truth for hardware and software assets across the IT-OT estate, enabling ICT teams to understand vulnerabilities of each connected component and accurately assess risk exposure of devices.

Knowledge tools and security workflows in ServiceNow OTM enable security professionals to establish correlations between OT assets by leveraging the Purdue model and topology diagrams. Visibility into interconnected OT assets in manufacturing units helps identify security gaps and address them with appropriate security tools. The insights also help security teams ensure compatibility of security control systems across IT and OT ecosystems. Moreover, visibility into vulnerabilities is useful to prevent cybersecurity breaches, mitigate risks and protect the infrastructure by implementing advanced threat detection and continuous traffic monitoring.

A man with dark hair tied back, wearing a dark polo shirt, is leaning over a large white industrial robot arm in a factory setting. The robot arm is positioned in the foreground, and the man is looking down at it. In the background, there are various pieces of industrial machinery, including a computer monitor displaying data. The overall scene is dimly lit with a greenish tint.

Real-time security threat intelligence, gathered through third-party OT security monitoring tools, is imperative to protect the IT-OT network from vulnerabilities, cyberattacks and security breaches. In-built data governance, threat management tools, and a risk management framework in **ServiceNow OTM** offer a comprehensive cybersecurity mechanism for smart factories. The platform safeguards connected assets and autonomous systems by identifying security gaps, remediating issues promptly, and isolating infected devices / assets instantaneously. In addition, it assesses the IT-OT landscape periodically for proactive risk mitigation.

ServiceNow OTM enables prompt response to OT service requests and accelerates OT issue resolution across a connected manufacturing unit by automating OT asset lifecycle management. An automated system for alert and incident management rationalizes the cost of proactive risk mitigation on a digitized production floor. Notably, the automated OTM platform ensures compliance with cybersecurity standards while expediting response and recovery in the event of a security breach in a converged IT-OT environment.

ServiceNow OTM enhances shopfloors

Digitized factory floors require superior OT service management to prevent bottlenecks and address production issues in real time.

ServiceNow OTM unifies OT data residing in silos across systems to offer a single pane view of the configuration, performance and health of OT assets. It collects, processes and analyzes a huge volume of data in different formats from the OT estate, providing manufacturing units with the ability to realize business value through actionable insights and informed decision making.

ServiceNow OTM boosts responsiveness and adaptability of manufacturing enterprises via an ecosystem integration on the cloud. The seamless integration of physical OT infrastructure, virtual IT assets, network devices, people, processes, and databases transforms global operations as well as support services. At the same time, a cloud ecosystem maximizes both the availability and scalability of OT infrastructure.

Scalable infrastructure as well as pervasive connectivity enable manufacturers to capitalize on emerging technologies for lean production, supply chain optimization, quality improvement, and cost rationalization. **ServiceNow OTM** transforms an industrial facility into a data-driven agile enterprise. Such a transformation supports Artificial Intelligence (AI), Machine Learning (ML), robotic, and IIoT systems across the extended manufacturing value chain. Cognitive production systems and streamlined processes maximize resource utilization and significantly reduce unplanned downtime, while safeguarding the interests of constituents, including the environment.

ServiceNow OTM enables planning, production, maintenance, and supply chain operations teams to combine real-time OT data and AI/ML output for informed decisions related to increasing production, optimizing daily shift schedule, or avoiding excess inventory. Further, the platform automates discovery and normalization of OT systems as well as upgrade of OT databases. This minimizes the time and effort for reporting while improving the accuracy of alert systems and risk management solutions.

ServiceNow OTM powers smart manufacturing with enhanced efficiency and security. A digital industrial environment operating on a cloud ecosystem can better manage physical and virtual assets. OT reinforces manufacturing systems to maximize production. Simultaneously, digital security tools safeguard assets and production systems to maximize return on OT investment.



About the authors



Rajiv Puri, Vice President – Manufacturing Strategy, Solutions and Partnerships, Infosys

Rajiv Puri is a part of Infosys manufacturing leadership team focused on helping manufacturers capitalize on opportunities in smart manufacturing, B2B2C transformation, and servitization. He is an industry veteran with a career spanning functional, consulting, and client relationships roles in the manufacturing industry.



Aniesh Myneni, Principal Consultant - Practice Lead for ServiceNow Industry Vertical Solutions and NowPlatform AppEngine

Aniesh Myneni has been part of the IT Industry for over 14 years and has spent over eight years of these leading large-scale ServiceNow transformation programs for global organizations. He is currently the Practice Lead for ServiceNow Industry Vertical solutions and NowPlatform AppEngine.

Infosys Cobalt is a set of services, solutions and platforms for enterprises to accelerate their cloud journey. It offers 35,000 cloud assets, over 300 industry cloud solution blueprints and a thriving community of cloud business and technology practitioners to drive increased business value. With Infosys Cobalt, regulatory and security compliance, along with technical and financial governance comes baked into every solution delivered.

For more information, contact askus@infosys.com



© 2021 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.

[Infosys.com](https://www.infosys.com) | NYSE: INFY

Stay Connected   