The new path forward to maximize OT uptime

Three critical skills for managing OT in the era of hyperconnected manufacturing

Start
Digitize to maximize uptime

As manufacturing technology advances, any innovation could be judged by one question: Does it improve uptime?

Today’s era of hyperconnected manufacturing creates both new opportunities and risks to OT availability. Connecting OT assets to the network may support more preventative or even predictive maintenance—but it could also create new security vulnerabilities in a world where “security by obscurity” once ruled.

Still, there are significant opportunities for manufacturers to digitize in ways that maximize uptime, by making smart investments in:

- Visibility
- Security
- Maintenance
The ability to gain true visibility of OT assets is arguably the most important smart factory advancement in recent years. In a large manufacturing operation, hundreds of thousands of individual components need to work together for efficient, high-quality production.

But until recently, manufacturers had to orchestrate all of this without the ability to fully visualize all of those assets or their relationships. They were reliant on multiple systems, manual processes, and legacy knowledge to know what assets they have and how they work together.

This approach doesn’t scale to the demands of a modern smart factory—and it puts uptime at risk. All it takes is a lack of understanding of how taking one machine offline impacts the rest of the production line, and work halts. With the extreme expense of even an hour of downtime, visibility is a core competency that must improve.

The traditional method of achieving visibility of OT assets is heavily dependent on experienced subject matter experts (SMEs) who often maintain information in disparate, disconnected systems, in spreadsheets, or even on paper.

As the amount of assets increases, it becomes increasingly difficult to maintain this information and understand the relationships and dependencies between assets as they are replaced, or the production process evolves.

In this environment, improvements to business and production processes are mostly reactive; the result of learning from costly mistakes and system failures. Proactive changes can typically only pick off the low hanging fruit, as you aren’t able to collect and analyze enough data to glean less obvious yet actionable insights.
ServiceNow and Fujitsu offer a new path towards OT visibility.

With our Fujitsu OT Digital Transformation solution, based on ServiceNow Operational Technology Management, we offer one complete view of the OT environment.

The OT Discovery feature of this solution identifies all the OT assets on your industrial network. Unconnected devices are tagged with a QR code and scanned, and our software is able to discover your industrial control system (ICS) architecture in the background. Once validated, these assets are loaded into ServiceNow, providing you with a dynamic, always up-to-date view of your OT assets and allowing you to master your IT/OT environments in a single configuration management database (CMDB).

This solution unlocks a tremendous amount of valuable features, such as:

- A full view of all OT assets and IT assets in one place
- The creation of an always up to date ServiceNow CMDB
- The ability to create and visualize relationships between IT and OT assets that enable the adoption/strengthening of key process improvement methods, such as Information Technology Infrastructure Library (ITIL) and Lean Six Sigma
- Customizable OT asset dashboards and reporting functionality to gain even more visibility and insight into your critical infrastructure
- Additionally, this level of visibility creates a solid foundation to support two other critical competencies for managing OT in the Industry 4.0 era: security and maintenance
Security

The modern smart factory also needs a modern approach to security. Historically, manufacturers had no need to connect their ICS to the internet, and plants were less susceptible to cyberattacks due to this lack of connectivity. While the convergence of IT and OT environments has created tremendous business value, it has also made the manufacturing industry a top target of cybercriminals. "Security through obscurity" is no longer an option, and top manufacturing executives agree that a comprehensive cybersecurity strategy is critically important.

While the threats that plague enterprise businesses are still a top concern for manufacturers, there are also serious concerns related to safety (both for plant workers and the products being produced), quality (imagine a hacked sensor that can no longer accurately detect a potential issue), and, of course, uptime.

Cybersecurity threats create new downtime risks that must be actively managed. OT leaders need to trust that as they connect more devices to the network, they’re not putting people or production at risk.

What’s worse—many legacy OT assets were never designed with security in mind, and even modern-day internet of things (IoT) devices are subject to zero-day vulnerabilities that require continued vigilance to stay protected.

There have been tremendous advancements in ICS and SCADA security endpoints to meet these needs. However, toggling between different systems to assess threats and prioritize remediation activities can take significant time. It’s difficult to gain a unified view of threat levels across the OT estate.

Though many OT components are able to be scanned and patches are available, OT risk assessments via spreadsheets and manual patching cycles are impractical as the smart factory grows and it is difficult to assess threat levels and prioritize threat remediation across the OT estate.
ServiceNow and Fujitsu offer a new path forward for security.

Our joint solution offers manufacturers a holistic approach to implement their security strategy. Combining Fujitsu tools and processes with the power of the Now Platform®, we’re able to provide a unified view across your ICS and SCADA security endpoints, enabling you to identify, prioritize, and respond to cyber threats faster.

To help manufacturers improve their OT security posture, Fujitsu offers an on-site security review and analyzes the data from the SecOps environment to produce a Security Assessment Report, helping you craft your initial strategy and showing you how to automate your security processes. And, your SecOps Dashboard highlights vulnerabilities and ongoing incidents, and features, like proactive outage avoidance and workflow and automation tools, allow you to fix or isolate incidents automatically while minimizing the impact to production.
As manufacturing operations scale to include more and more highly complex assets, properly maintaining your OT assets becomes not only increasingly important, but also increasingly complex. Improperly maintained equipment erodes availability, performance, and quality, which when taken together are the three contributors to overall equipment effectiveness (OEE), the gold standard for measuring productivity.

Originally, maintenance was a mostly reactive task. Machines broke, and manufacturers depended on SMEs to assess the problem and fix the issue. Of course, waiting until something breaks means unplanned downtime—which is unacceptable in today’s world.

This has evolved into a more proactive approach to maintenance, with operators performing proactive tasks at scheduled intervals, based on their previous experience or known life expectancy of OT assets and their components.

While this has improved OEE, the process is still largely manual and leads to inflated labor and material costs. And, the risk of unplanned downtime still looms, with unanticipated maintenance issues halting production at times.
The advent of smart sensors has made truly predictive maintenance possible—by detecting potential issues before they cause downtime and scheduling maintenance based on real machine data, not static maintenance schedules. With our solution, we create a solid foundation to drive progress toward this approach.

We make it easy to see when sensor readings get out of the desired range and can provide an early warning system to automatically deploy maintenance teams to inspect and maintain key assets before downtime ever happens.

This automated approach, supported by centralized knowledge management, helps avoid downtime and reduces the cost to attain high OEE levels.

ServiceNow and Fujitsu support a **new path forward for maintenance**.
Conclusion

With all the advancements in smart manufacturing, a world with no unplanned downtime may truly be on the horizon. The path will come through improvements in critical competencies, like visibility, security, and maintenance, to control the most common causes of that downtime.

Fujitsu and ServiceNow’s solution provides a foundation to support this objective. Fujitsu’s Smart Factory solutions integrate with ServiceNow Operational Technology Management to provide enhanced visibility, security, and predictive maintenance to your manufacturing operation, actually connecting your connected devices and helping to drive improvements to maximize uptime while keeping your factory secure from the constant threat of cyberattacks.

Unlock OT visibility: Discover and map all OT assets and their relationships. Gain one complete view of your OT environment across different production lines and facilities.

Protect OT assets: Detect and remediate security vulnerabilities in your OT environment—before they cause unplanned downtime.

Achieve proactive maintenance: Use digital workflows and artificial intelligence to predict and avoid outages—maximizing uptime and profit.