

Digital Workflows Take Machine and Worker Safety to a New Level

One of the areas the Internet of Things (IoT) is revolutionizing is safety. Thanks to the rise of smart, connected devices, manufacturers have unprecedented levels of visibility into the operating conditions of machines, the wellbeing of workers and the state of their plants. From wearable devices that capture a worker’s biometric data, to sensors that detect a facility’s carbon monoxide levels, more data is streaming from IoT-enabled safety devices and systems than ever before.

But to truly reap the benefits of the IoT, bear in mind that scraping as much data as you can from your safety assets isn’t enough. You need an intelligent platform that can turn this information into action. Addressing this challenge, a new stream-processing IoT Bridge evaluates safety device data against user-defined rules—transforming this information into action in the form of digital workflows. From proactively scheduling maintenance to shutting down power to a machine, these workflows have profound implications for the ways you handle machine safety and incident response.

Let’s take a closer look at how this IoT technology can help you take machine and worker safety to new levels.

A Scalable IoT Engine for Managing Safety Devices

Currently, there’s no shortage of IoT devices that fall under the umbrella of safety—especially in oil and gas, manufacturing and other industrial environments. Temperature and other environmental sensors record information about safe or hazardous working conditions. Wearables capture workers’ physical metrics, including heart rate, movement and location. Safety devices continuously monitor the operating conditions of machines in real time—ensuring equipment continues to operate safely with no signs of wear or breakdown.

But while the IoT has undoubtedly created new opportunities for understanding our processes, it’s also created new challenges in making that data actionable—especially where safety is concerned.

This is where the ServiceNow® IoT Bridge comes in. This horizontally scalable, stream-processing platform connects various safety devices to digital workflows—making it possible to collect, view and act upon the large volumes of available data from safety devices. Using standard protocols, it authenticates and communicates with devices and then uses a rules-processing engine to evaluate the data against user-defined rules—all in near-real time.

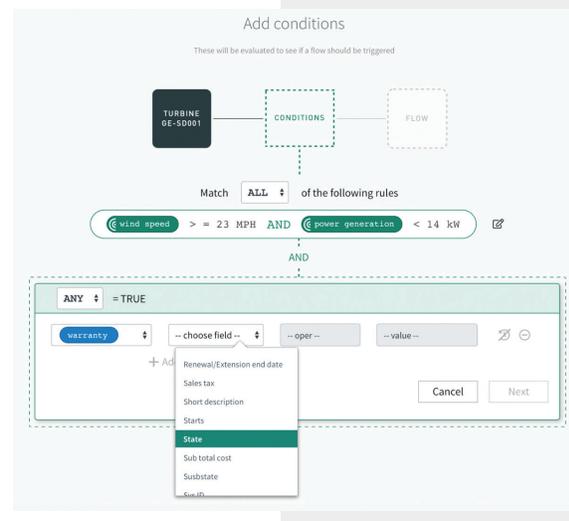
These rules automatically trigger digital workflows that bridge the incoming data streams with existing ServiceNow capabilities, enabling you to quickly prioritize and respond to safety-related incidents.

The IoT Bridge applies condition-based, equation-based or model-based rules against streaming device events.

Safety as a Service

Digital workflow platforms like the ServiceNow IoT Bridge monitor the health of your safety devices using secure, real-time data and intelligence software. By leveraging the IoT, it automates multi-step processes between various people and systems—improving the efficiency of your operation and the quality of your customer service.

Thanks to these features, the IoT Bridge can help you make a seamless switch to a servitized business model, which focuses on selling an entire service support system around a product. By making it easier than ever to embed safety into your machines, you can begin to offer safety as a service—enhancing your competitive edge.



Transforming Workplace Safety

By turning valuable safety device data into action, digital workflows bring a number of benefits to your operation, enabling you to:

Enhance the functional safety of your equipment. While the benefits of the IoT are clear, the abundance of interconnected devices—each with increasingly more complex electronics and software—can make implementing system safety functions all the more difficult.

Improve worker health, safety and wellness. Digital workflows can help you more efficiently manage data from environmental sensors—providing better visibility into working environments and reducing worker exposure to harsh conditions like radiation, heat or humidity. For these reasons, digital workflows can help you reduce the rate of worker injuries, accidents and absences—in turn minimizing your downtime and improving productivity.

Accelerate and improve incident response. If a worker reports a critical event or accident, predetermined, automated workflows initiate and

accelerate safety protocols, such as dispatching a medical team. Vice versa, if an environmental sensor detects a dangerous working condition—high levels of a gas, for example—workflows will automatically notify personnel to evacuate the area.

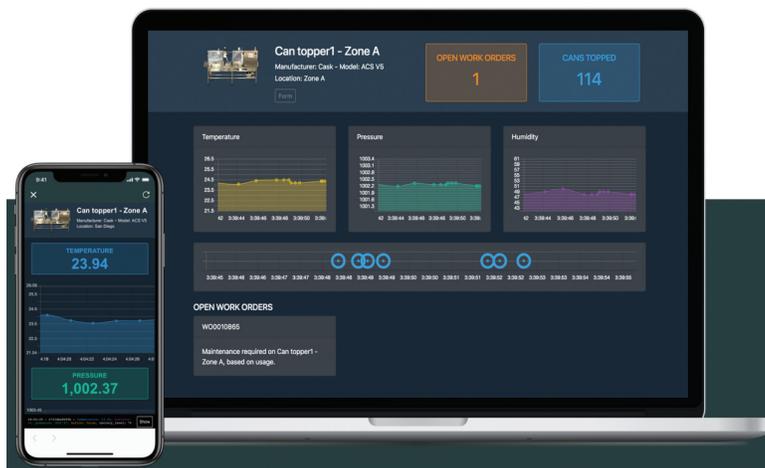
Achieve true predictive maintenance. Beyond just providing reactive responses, digital workflows can help you anticipate and prevent hazardous machine failures before they happen. By aggregating data from field safety devices and then making the information available to machine learning and predictive algorithms, the IoT Bridge can proactively trigger workflows that avoid potentially dangerous equipment failures.

Using constant condition monitoring and predictive analytics, the IoT Bridge detects potentially dangerous conditions and automatically triggers corrective workflows—preventing hazards before they happen and improving the overall functional safety of your equipment. For these reasons, the IoT Bridge can help you maintain safety integrity levels (SIL) and other standards.

Digital Workflows and Cybersecurity

Despite the many benefits of the IoT, the explosion of smart, connected devices has given rise to an increasing number of cyberattacks—which pose a growing threat to worker safety. Fortunately, ServiceNow provides safety solutions to help you address these cybersecurity threats.

A security orchestration, automation and response engine, the ServiceNow Security Operations leverages intelligent workflows, along with security incident response, vulnerability response and threat intelligence capabilities. When Security Operations receives an alert from your existing security products, it deduplicates the event, creates a security incident and then matches the affected asset against the Configuration Management Database to determine its priority. At the same time, Security Operations uses orchestration tools to perform additional malware scans or pull processes from affected endpoints—condensing up to an hour of research into seconds.



Remote monitoring of IoT-enabled safety devices provides proactive alerting and real-time visibility into working conditions.

servicenow

© 2019 ServiceNow, Inc. ServiceNow, the ServiceNow logo, Now, Now Platform, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc. in the United States and/or other countries. Other company and product names may be trademarks of the respective companies with which they are associated.
SN-SolutionBrief-Name-062019