Industry analysts are bullish in their assessment of the IoT opportunity within the industrial manufacturing sector. For example, the Boston Consulting Group expects spending to have quadrupled to $40 billion in the five years to 2020. And McKinsey and Co. estimates that IoT applications in factories have the potential to create value of up to $3.7 trillion by 2025.

The bulk of this value will likely be delivered through operational optimization. But IoT has the power to radically reshape every aspect of product development and delivery, from the plant floor to every aspect value chain. For example, machinery sensors can allow energy and water wastage to be measured and reduced, realizing cost and environmental benefits. Information from other systems and devices can be fed directly back into the production line, potentially enabling changes to be implemented in hours or days. The inventory replenishment process can be completely automated based on improved asset tracking and sensor-based alerts that trigger orders when stock runs low. Potential equipment failures can be identified automatically before they happen, protecting employees and minimizing unplanned downtime – and so on. The exciting reality is that the possible applications of IoT in manufacturing are almost limitless, once the right infrastructure is in the place. And therein lies the challenge.

In the past, Operational Technology (OT) and Information Technology (IT) within manufacturing concerns were separate entities, staffed by experts with limited knowledge and understanding of each other’s worlds or requirements. However, the successful implementation of IoT demands that this siloed approach is dismantled for good, and replaced with a unified infrastructure that treats the different elements of OT and IT as complementary cogs within the same process wheel. In addition, the arrival of IoT means security suddenly becomes a far more important issue for both OT and IT. By adding a broader range and number of devices to networks, IoT can create more potential entry points for hackers, hostile governments and competitors to gain access to sensitive information, or disrupt operations, if they are not secured properly. As a result, manufacturers need to build an infrastructure that closes the gap between OT and IT, while ensuring security risks are minimized.

With its new Pulse IoT Center solution, VMware is extending its leadership in optimizing the management and security of data centers into the IoT space. The solution enables the integrated management of all the gateways required to enable the efficient and secure operation of manufacturing processes and the supply chain that feeds them. Moreover, VMware’s relationships with other leading technology vendors create the ability to deliver a complete end-to-end IoT solution for manufacturers, from device selection to business analytics. The benefits will be measurable in reduced downtime, increased efficiency and profitability, enhanced safety, higher product quality, and the potential to reduce the environmental footprint of each production site. In short, VMware is making the factory of the future real, today.
MAKING UNPLANNED DOWNTIME HISTORY

From an operational perspective, downtime has always been ‘enemy No. 1’ for manufacturers. IoT offers them a future in which they will be able to minimize it with complete real-time visibility over the status of every machine in the factory. But that’s just where the benefits begin.

Once connected to single management platform, machine failure parameters can be continuously measured and analyzed. Based on these parameters, normal and abnormal states can be tracked much more accurately, enabling preventative action to be taken before problems occur, saving time and money by minimizing damage and disruption.

Once enough data has been collected and analyzed, patterns can be established that can be fed back into the manufacturing process quickly. This will help improve the efficiency and effectiveness of future manufacturing and maintenance processes. It will also provide insight into how to change or optimize machine and component purchases in the future. In addition, manufacturers could even decide to monetize the information and process changes they make by selling them to their peers in other sectors.

The sophisticated operations rules engine and granular data assignment capabilities of the VMware Pulse IoT Center solution enable the management effectiveness and efficiency required to deliver all of the above, and empower manufacturers to realize bottom line benefits from their IoT investments.

SIMPLIFYING THE SMART FACTORY

Within the context of IoT, the complexity and interdependencies of modern manufacturing are simultaneously an opportunity and a challenge. On the one hand, a more connected factory can enable improvements across the board, from proactive maintenance to higher production quality and a more efficient supply chain. But on the other, heterogeneous OT and IT within modern factories creates a communications gap that prevents connected devices from sharing information.

For example, even within a single production line, there can be machines from multiple vendors, all with different control systems, that cannot communicate effectively or quickly with one another. A truly connected factory also requires the integration of a wide range of device types, from sensors on robots to conveyor belts, cameras, vehicles and so on. Onsite factory IT can also feature thousands of proprietary protocols and gateways that operate in different ways, e.g. with or without operating systems, with or without Web interfaces, etc. And the lack of interoperability between all these different elements makes it difficult to collate and analyze IoT data quickly.

VMware Pulse IoT Center provides an end-to-end solution for onboarding, managing, monitoring and securing all the connected devices in a smart factory or industrial facility, from equipment sensor and IoT edge systems to the data center. Data from every relevant device is collected and delivered to the VMware’s Pulse IoT Control Center, which can also distribute commands back to devices as required. The solution closes the gap between OT and IT, allowing these two previously disparate worlds to become part of the same integrated, efficient and secure system. By leveraging this technology and strategic alliances with other leading providers, VMware will enable millions of heterogeneous ‘things’ to be managed via a single pane of glass. As a result, manufacturers can implement their IoT strategies in a more streamlined and consistent way.
SECURITY IN THE INDUSTRY 4.0 ERA

Prior to the IoT era, factories were primarily closed systems, so securing them against Internet-based attacks was not a significant priority. And to minimize any operational disruption from potential vulnerabilities, many OT systems were walled off from IT. Today, this siloed approach presents a significant barrier to the implementation of IoT in the factory. That’s because effective IoT implementations require greater OT and IT integration, and more connections to external or third-party data sources, systems and analytics platforms.

To create smarter factories, a thoroughly connected, integrated infrastructure is required. But connecting machines directly or indirectly to the Internet, or even to a private cloud environment, enlarges the potential attack surface area significantly, increasing the number of access points that criminals could exploit for espionage, vandalism, or terrorism. The risks range from machine damage to factory worker injury, intellectual property theft, and the economic impact of production or supply chain disruption.

VMware’s Pulse IoT Center solution provides a reliable platform for the secure, integrated management of IoT within factories. Leveraging VMware’s extensive experience in securing data centers, it can distribute software upgrades and security patches to devices and edge systems at scale, and rapidly quarantine rogue devices if a breach or other anomaly is detected. In other words, it delivers the peace of mind that manufacturers are looking for as they start to embrace the opportunities of Industry 4.0.

ENABLING THE CONNECTED SUPPLY CHAIN

Connecting the factory production process directly with supplier-, logistics-, product lifecycle- and ordering systems will deliver a range of benefits to manufacturers including, the ability to accommodate rapidly changing and increasingly individual customer requirements.

When ordering a new kitchen for example, in the pre-IoT world, a consumer must manually select the specifications and components in advance, and is unable to make changes once the order has entered the vendor’s system. A truly connected manufacturing process will allow the same consumer to make specification changes during production. So, a customer could decide to change the color of the units or the specification of the oven, and the relevant production line would be informed immediately. The processes required to execute the changes would be adjusted, and the relevant systems for managing stock levels and invoicing the customer would also be updated as part of an automated, IoT-enabled process.

Increased integration will deliver similar automation and streamlining benefits across the supply chain. These could include: the ability to utilize better asset tracking and inventory management to optimize costs by reducing asset loss and ‘empty shelf’ incidences; or allowing an IoT-enabled vehicle fleet to adjust employee transport and product delivery routes according to weather conditions, traffic congestion or other variables.

The VMware Pulse IoT Center provides a centralized, integrated platform for controlling the entire supply chain in the IoT era, enabling every ‘thing’, whether a component shipment, product or a warehouse vehicle, to be managed securely and accurately from a single console.
IoT BUSINESS BRIEF SERIES

The VMware IoT Business Brief Series explains how VMware helps organizations across manufacturing, public service, healthcare and energy sectors build the secure infrastructure for they need to maximize the IoT opportunity:

01 Industrial Manufacturing Business: How IoT will help close the gap between OT and IT in smart factories, and enable secure management of the connected value chain.

02 Healthcare Business: How the right IoT solution can enhance patient care and reduce the cost of lost equipment, without compromising on data privacy and security.

03 Public Sector Business: How smart cities that automate everything from parking space allocation to interactive tourist information can be enabled through the right IoT management solution.

04 Energy & Oil Business: How integrated IoT gateway management delivers efficiency benefits across energy and fossil fuel infrastructures, as well as vehicle fleets, realizing financial and sustainability advantages for their owners and customers.
Your Contact

**Matthias Schorer**  
Lead Business Development Manager – IoT, EMEA

Since 2017 Matthias Schorer leads the Business Development for IoT in EMEA. Before he was Head of Strategy Consulting and responsible for the VMware Accelerate Advisory Services Team in Central and Eastern Europe. He has extensive expertise in IT architecture, legacy system migration, cloud computing and virtualization across multiple industries, with a focus on the automotive sector and connected car innovations.

mschorer@vmware.com  
Tel. +49 89 / 3706 17108

---

**Mimi Spier**  
VP Business Development, Marketing & GTM Strategy for IoT

Mimi leads since 2016 a team responsible for defining and launching the marketing, product and business strategy for IoT at VMware, and developing the strategic partners necessary to deliver the most complete solution to the market. Before, she was responsible for ISV Business Development and Marketing for VMware’s Mobility solution and helped shape the growth and GTM strategy for VMware’s $1.5 billion acquisition of AirWatch.

mspier@vmware.com  
Tel. +1 (650) 561-2489