Cognishen Focus

Smart Factory: Forefront Technologies

Volume 2 Issue 2, February 2023

Our January 2023 newsletter described Industry 4.0 components and the growth of smart factories. To recall, a smart factory may be visualized as one equipped to collect data, analyze the collected data, and use the data to make intelligent operations decisions. We will continue to discuss the components of Industry 4.0 in simple terms in this newsletter.

Smart factories must fend off cyber invaders to gain and retain competitive advantage. These firms must use their resources wisely and deploy well-integrated systems to achieve their strategic goals. Such actions involve forefront technologies. The components of forefront technology include cloud computing, cyber security, and system integration. Computer and telecommunication technology have helped industrial revolutions in the past and that is no exception to Industry 4.0. Let us take a look at the figure. The forefront technologies are used by the smart systems, which in turn drive the intelligent automation that is required of smart factories.

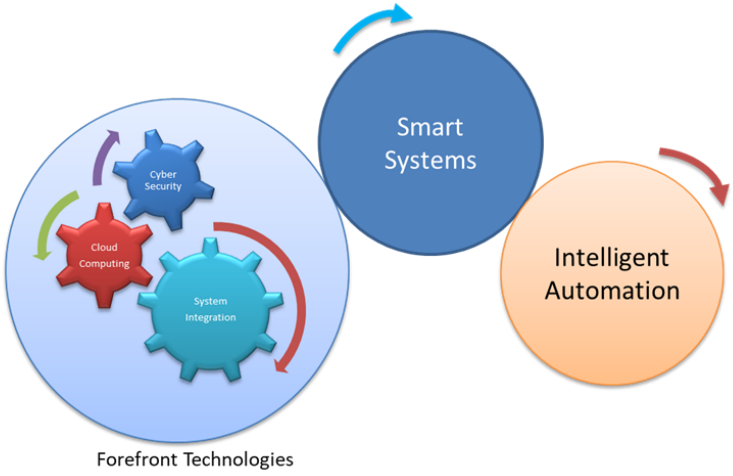


Figure 1. Digital Transformation Components of Industry 4.0

Cloud Computing

We are used to storing documents and files in our computer's hard drive. When such information is stored in a remote location and can be accessed virtually, we use the term "cloud computing." Cloud computing service providers such as Amazon Web Services (AWS), Google Cloud Platform, and Microsoft's Azure provide services that enable users to store files and applications on remote servers and then access all the data via the Internet.

The cloud computing providers are equipped with necessary hardware (like your computer), software (like Microsoft Excel), and the means to access them from anywhere in the world using the Internet. With unlimited storage space, businesses need not invest capital to buy the necessary computers and software—they can just use the cloud computing provider's resources at a fraction of the cost of buying the same software or storage space. Firms can take advantage of the flexible resources and the economies of scale by using cloud computing. For example, Facebook uses AWS to store information in addition to its own hyperscale datacenter facilities. Using cloud services, smart factories can integrate various systems to provide high-quality, inexpensive, custom manufacturing services.

Research Insight

"Deloitte's survey on cloud technology found that 90% of respondents agree, or completely agree, that cloud combined with other technologies such as AI, IoT, and analytics serve as "force multipliers" for their digital strategy. Overall, respondents think that cloud drives positive outcomes for businesses across a range of key measures including: 83% for mitigating business and regulatory risk, 80% for building net new product/service revenue, 74% for expanding into new markets, and 72% for providing better sustainability in support of environmental issues—to name a few."

Click for More Details

"What drives IT executives to initiate cloud migration? Deloitte's survey of more than 500 IT leaders and executives reveals that security and data protection is the top driver. With 58 percent of respondents ranking it No. 1 or 2, security is top-of-mind for everyone, from C-suite IT executives and senior leaders to IT managers and developers.

Some IT executives are turning to third-party cloud and managed security services, with cloud providers delivering sophisticated cyber capabilities and solutions and cloud offering the potential of helping to mitigate security incidents. These factors suggest that IT executives may be increasingly relying on the expertise of third-party cloud-based security and infrastructure providers to protect their data."

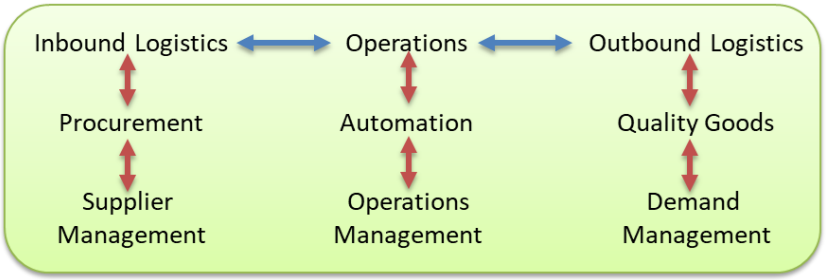
Click for More Details

System Integration

In a smart factory, the different systems, applications, and databases must work together seamlessly and efficiently. This is called system integration in simple terms. For example, a smart factory that produces high-end electronic components may require a clean room integrated with the heating, ventilation, and air conditioning (HVAC) system and the enterprise resource planning (ERP) system. System integration enables various disparate systems to "talk to each other," which enables the flow of information between those systems.

System integration works in two dimensions—the horizontal and the vertical integration of all operational systems and processes in an organization as shown in the below figure. For example, horizontal integration may involve all supply chain systems while vertical integration may involve all related processes and data.

Figure 2. Horizontal and Vertical System Integration



Cyber Security

Smart factories not only must implement cloud services for flexibility and agility and systems integration for seamless and efficient operations, but they must also protect their systems, processes, and data. Smart factories have computer systems that are highly interconnected and integrated. Security risks, both inherent risk and residual risk, increase when processes and flow of data are connected through the Internet. Inherent risk usually occurs due to a lack of protective and preventative measures. Residual risk is the risk remains after internal controls and mitigation efforts have been implemented.

Firms face the threat of malicious attacks by unauthorized users in the form of cyber-attacks, which are aimed at retrieving, modifying, or destroying sensitive information, extorting money from companies, or disrupting their business process. The cybersecurity process involves the protection of computer systems and networks from theft or damage to data, hardware, or software as well as from the misuse of information stored in those systems. Cybersecurity is an important technology in smart factories and smart operations. The increase in data, the reliance of Internet to store and access data, and the sophistication of cyber attackers have increased the importance of cybersecurity.

The International Information System Security Certification Consortium or $(ISC)^2$, the non-profit organization which specializes in training and certifications for cybersecurity professionals defines cyber security in eight domains including security risk management, security of assets, security models, secure networks, authentication management, security audits, software security, and security operations.

Practical Insight

"The Small Medium Enterprises (SME) sector is quickly becoming more reliant on technology, and the problem of integration has started to filter down to them. Many SME's are using a few incompatible applications to automate their processes; and have no idea how much integration could benefit them."
- Thom Leggett
Software Integration for SMEs
Streetdirectory.com

Click for More Details

"SMEs have been increasingly receptive to adopting cloud-based security solutions, and cloud-based security service providers can capitalize on this trend by offering organizations customized security services. As SMEs change their focus to cloud-based solutions, cloud-based data protection solutions and service providers are anticipated to encounter substantial growth prospects, such as protecting SMEs' data from security breaches and vulnerabilities. Hence with the broader adoption of cloud data security by SMEs due to the increasing cyber-attacks, the market's growth is expected to surge. "

Click for More Details

Published by cognishen.com
Email: info@cognishen.com

Cognishen
Innovate...Grow...Inspire
https://www. cognishen.com