



becomes



3DEXPERIENCE™

THE ULTIMATE IIoT GLOSSARY

A GUIDE TO 100 OF THE MOST COMMON
INDUSTRIAL INTERNET OF THINGS (IIOT)
TERMS AND ACRONYMS

Whitepaper

THE ULTIMATE IIOT GLOSSARY

A GUIDE TO 101 OF THE MOST COMMON INDUSTRIAL INTERNET OF THINGS (IIOT) TERMS AND ACRONYMS

Since it was dubbed Industry 4.0 in 2011, the Industrial Internet of Things (IIoT) has been transforming business processes across the board, from manufacturing and production to inventory management and procurement.

IIoT led to the dawn of the smart factory and predictive technologies that have moved manufacturing into a new era, with cloud-based technologies built into machinery and advanced software platforms designed to manage all that data floating around.

But getting a handle on IIoT doesn't have to be daunting.

Whether you're just starting to shift to networked systems, in the process of incorporating IIoT into your operations, or just trying to keep your systems current with the latest technologies, this guide provides you with a basis of knowledge for any level of implementation.

Inside you'll find:

- A solid set of terms to help you understand IIoT
- Technology tools to incorporate into an IIoT strategy
- Further research opportunities to learn more about IIoT



1. 3G

A mobile communications standard that allows mobile phones, computers and other portable electronic devices to access the Internet wirelessly. With minimum consistent Internet speeds of 144 Kbps, 3G was created to bring 'mobile broadband'.

2. 4G

A mobile communications standard intended to replace 3G, allowing wireless Internet access at a much higher speed. It is the 4th generation data speed and faster than 3G. 4G is considered 4.7 Mbps and up.

3. 5G

Short for 5th generation, 5G is a commonly used term for certain advanced wireless systems. Industry association 3GPP defines any system using 5G New Radio software as 5G.

4. 6LoWPAN

An acronym of IPv6 over Low-Power Wireless Personal Area Networks. 6LoWPAN is also the name of a working group in the Internet area of the IETF.

5. Access Point

Connects users to other users within the network and can also serve as a point of interconnection between the WLAN and a fixed wire network.

6. Action

Used to describe an event that takes place when an associated process data changes; a critical function of RTPM that enables up-to-date calculations and detailed analysis of your data.

7. Additive Manufacturing

A manufacturing process where materials are selectively accumulated to build, grow or increase an object by adding layers versus traditional processes that remove material (cutting, drilling). Also known as 3D printing and is the official industry term for ASTM F2792.

8. Analytics

Applying data analysis tools and procedures to gain value from the enormous volume of data generated by connected IoT devices.

9. Application Programming Interface (API)

A set of routines, protocols, and tools for building software applications. It ties together the connected 'things' of the 'Internet of Things'. It specifies how software components should interact, and is the point of interaction between an IoT device and the Internet and/or other elements within a network.

10. Artificial Intelligence (AI)

The ability of computer systems to utilize data and perform tasks that normally require human intelligence. Examples include visual perception, speech recognition, decision-making and language translation.

11. Asset Tracking

The method used for tracking physical assets, either by scanning barcode labels attached to the assets, or by using tags that use GPS, BLE (Bluetooth low power), WiFi, etc.

12. Attestation

A legal acknowledgement of the authenticity of a document or decision made and a verification that proper processes were followed.

13. Augmented Reality

Overlays information and digital content onto a real-world scenario that a user can interact with, versus virtual reality that creates a fully fabricated viewing environment. Used in training, safety and maintenance applications in manufacturing.

14. Authenticated Identity

The process of a system to determine whether someone or something is who or what they say they are. Users are usually identified through a user ID, and authentication is accomplished when the user provides a credential, like a password, that matches with that user ID.

15. Big Data

Extremely large data sets that are analyzed computationally to reveal patterns, trends and associations.

16. Big Data Analytics

A complex process of examining large and varied data sets (big data) to help discover information, like hidden patterns, unknown correlations, market trends and customer preferences, that can help organizations make informed business decisions.

17. Block Chain

Stores networked information in chunks (blocks) along a connected path (chain) that makes the manufacturing process more secure by improves data mobility, component traceability and communication across the supply chain.

18. Bring Your Own Device (BYOD)

The increasingly common practice of bringing personally owned devices (phones, laptops, etc.) to work and using them to access privileged company information.

19. Brownfields

Problem spaces that need the development and deployment of new software systems in the immediate presence of existing (legacy) software applications/systems.

20. Business Impact Analysis (BIA)

A systematic process to determine and evaluate the potential effects of an interruption to critical business operations, often resulting from disaster, accident or emergency.

21. Business Intelligence (BI)

Software tools that transform raw data into useful reports, email alerts, analytics, dashboards and more to help you evaluate your business data.

22. Capital Expense (CAPEX)

The money a company spends to buy, maintain or improve its fixed assets, like buildings, vehicles, equipment or land.

23. Cloud Computing

The delivery of computing services via a network to provide on-demand resources, such as storage, software applications, file sharing and communications. A cloud can be public, private or a combination of both.

24. Constrained Application Protocol (CoAP)

A specialized Internet application protocol for constrained devices, as defined in RFC 7252. It enables those constrained devices, called "nodes", to communicate with the wider Internet using similar protocols. CoAP is also being used via other mechanisms, such as SMS on mobile communication networks.

25. Control Domain

A functional domain for implementing industrial control systems.

26. Cyber-physical System (CPS)

A mechanism that is controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users.

27. Cybersecurity

Also known as computer security or information technology security, cybersecurity is the protection of a computer system from the theft of, or damage to, its hardware, software or electronic data, as well as from the disruption or misdirection of the services it provides.

28. Data at Rest

Inactive data that is stored physically in any digital form.

29. Data Communications Infrastructure

An infrastructure that uses computing and communication technologies to transfer data from one place to another. It enables the movement of electronic or digital data between two or more nodes, regardless of geographical location, technological medium or data contents.

30. Data in Motion

A stream of data moving through any kind of network.

31. Data Lake

A large collection of raw, unstructured data stored in a repository that can be quickly accessed for analysis and reporting, versus a data warehouse that has an existing, and sometimes limiting, hierarchical structure to the data.

32. Databus

A system within a computer or device, consisting of a connector or set of wires, that provides transportation for data.

33. Demand-driven Production

A method of production based on actual customer orders (demand) rather than on a forecast.

34. Digital Twin

Digital twin refers to the creation of a series of digital replicas of actual, functioning physical assets. Digital twin strategies that are the most effective can simulate processes and systems in a digital environment prior to being placed in production.

35. Distributed Control System

A specially designed automated control system that consists of geographically distributed control elements over a plant or control area.

36. Edge Computing

A distributed computing pattern that brings computation and data storage closer to the location where it is needed. It improves system response times and saves bandwidth.

37. Edge Device

A device that provides an entry point into a service provider's core networks. These types of devices include routers, routing switches, integrated access devices, multiplexers and a variety of access devices.

38. Enterprise Resource Planning (ERP)

Business management software that helps run your company through an integrated view of your core enterprise operations.

39. Functional Domain

A set of interlinked requirements or functionalities for any software program, constructed to solve a problem within a computer system. Often determined by the number of built-in functions or knowledge the system has available.

40. Functional Framework

A series of systems that have proven successful in production use and are operational.

41. Gateway

A hardware unit that brokers data and machine learning models between IoT devices and the cloud.

42. Greenfield

Software that is created from scratch in a totally new environment. No constraints are imposed by legacy code, and there are no requirements to integrate with other systems.

43. Horizontal and Vertical Corporate Networking

Networking that allows for an efficient exchange of data between internal and external agents, machines and workpieces. It enables all business processes to be outsourced.

44. Human Machine Interface (HMI)

A graphics-based user interface or display of a manufacturing or process control system that enables personnel to interact with the system.

45. Implementation Viewpoint

Defines the programs and projects within a computing architecture, and where they will be implemented.

46. Industrial Cloud

A cloud system that has been heavily customized to fit a specific industry. It accommodates the business, operatory, legal, regulatory, security and other considerations for that business.

47. Industrial Control Systems

A general term that encompasses several types of control systems and associated instrumentation used for industrial process control.

48. Industrial Internet

The integration and linking of big data, analytical tools and wireless networks with physical and industrial equipment to distributed systems.

49. Industrial Internet of Things (IIoT)

Interconnected sensors, instruments and other devices networked with a computer's industrial applications, including manufacturing and energy management. This connectivity allows for data collection, exchange and analysis, while helping to facilitate improvements in productivity and efficiency, as well as other economic benefits.

50. Industry 4.0

The trend towards automation and data exchange in manufacturing technologies and processes, including CPS, IoT, IIOT, cloud computing, cognitive computing and AI. Often used as an alternate term for IIoT.

51. Infrastructure as a Service (IaaS)

The lowest service level in cloud computing. With IaaS, a third party manages the basic components of a functioning computer environment, such as virtualization technologies, raw storage, firewall options and other network connectivity infrastructure. The manufacturer is responsible for managing the platform and applications.

52. Intelligent Asset

Transmits information directly to the data communications infrastructure, where it is converted into actionable information. This information can then be used for predictive maintenance as well as to optimize business processes.

53. Internet of Things (IoT)

The concept of connecting everything imaginable to a network, so that information from one device can be quickly and easily shared through network connections with everything else.

54. Interoperability

The ability of computer systems or software to exchange and make use of information.

55. IoT Actuator

A mechanism for turning energy into motion, generating a change in the physical system through producing force, heat, motion, etc.

56. IoT Cloud Platform

A platform designed to store and process massive volumes of IoT data generated by devices, sensors, websites, applications, customers and partners, then initiate actions for real-time responses.

57. IoT Device

Non-standard computing device that connects wirelessly to a network and is able to transmit data.

58. IoT Protocol

Connectivity of traditional equipment, like desktop computers, laptops, tablets, printers, and phones as well as embedded technologies, such as security systems, thermostats, and home lighting systems – all via the Internet. Because of the wide variety of technologies that fall in IoT, there are several protocols. Some of the most well-known are Bluetooth, Zigbee, Z-Wave and 6LowPAN.

59. IoT Sensor

Sensors that collect data from the surrounding environment. Also known as ‘things’ of an IoT system, sensors form the front end.

60. IT/OT Convergence

The integration of IT systems, used for data-centric computing, with OT systems, used to monitor events, processes and devices and make adjustments in enterprise and industrial operations.

61. Least Privilege

Sometimes called the principle of least privilege (POLP); enforces a minimal level of user rights, or lowest clearance level, that allows the user to perform his/her role.

62. Lights Out Factory

A manufacturing methodology (or philosophy), rather than a specific process. Factories that run lights out are fully automated and require no human presence on-site. These factories can be considered to run ‘with the lights off’.

63. Machine-to-machine (M2M) Communication

Technology that allows wired and wireless devices to exchange information and perform actions with each other. M2M is an integral component to IoT. The remote monitoring of work centers is an example of M2M in a manufacturing environment.

64. Machine Learning

An application of AI that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. It focuses on the development of computer programs that can access data and use it to learn for themselves.

65. Man-in-the-middle Attack (MitM)

An attack where the perpetrator secretly relays, and possibly alters, the communications between two parties, who believe they are directly communicating with each other.

66. Manufacturing Execution System (MES)

A software package that monitors and manages production on the shop floor. Originally a self-contained solution, MES software is now increasingly integrated with ERP systems.

67. Manufacturing Intelligence

Tools that gather large amounts of manufacturing data from a variety of sources into once central structure (ERP) for reporting, analysis and performance review.

68. Material Resource Planning (MRP)

The predecessor to ERP, MRP now refers to a set of features inside ERP software that manage production planning, scheduling and inventory control.

69. Mesh Network

A communications network made up of radio nodes organized in a mesh topology. It is also a form of wireless ad hoc network. A mesh refers to the rich interconnection among devices or nodes. Wireless mesh networks often consist of mesh clients, mesh routers and gateways.

70. Message Queuing Telemetry Transport (MQTT)

An ISO standard that follows a publish/subscribe model to organize information into a hierarchy and transmit to only those that subscribe to a specific topic. It works on top of the TCP/IP protocol and used in remote locations and limited bandwidth applications.

71. Mobile IoT

Low power wide area (LPWA) network that offers long-range connectivity for devices requiring limited bandwidth and that aren’t transmitting data continuously. Also known as Cellular LPWA or c-LPWA.

72. Multi-tenancy

A software structural design where a single instance of software runs on a server and supplies multiple tenants. Such systems are considered ‘shared’.

73. Node

A basic unit of data structure that contains data and are often linked with other nodes.

74. Open Platform Communication, Unified Architecture (OPC UA)

A series of standards and specifications designed for secure, reliable and platform independent interoperability. It defines data and information transport from first-tier factory and process control devices through to the enterprise information system.

75. Operational Technology (OT)

The hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices.

76. Personal Identifiable Information (PII)

Any data that could potentially be used to identify a particular person, like a social security number, driver's license number, bank account number, passport number or email address.

77. Platform as a Service (PaaS)

PaaS builds upon the IaaS level in Cloud Computing where a third party provides not only the necessary IaaS components, but also operating environments such as fully ready database systems, web servers, rendering farms, software development environments and more. The manufacturer is still responsible for managing the applications.

78. Predictive Analytics

A variety of statistical techniques, including data mining, predictive modeling and machine learning, that analyze current and historical facts to make predictions about future events.

79. Predictive Maintenance

Helps determine the condition of in-service equipment in order to estimate when maintenance should be performed and avoid unexpected halts in production.

80. Programmable Logic Controller (PLC)

A digital computer used for automation and control of machines in manufacturing work centers. PLCs can collect detailed process data and relay it back to an ERP system.

81. Proportional–integral–derivative (PID) Controller

Provides a continuous variation of output within a control loop to calculate the appropriate corrective action of a control function within an industrial control system.

82. Provisioning

Assigning a physical device to a virtual identity. Providing or making something available. For example, in grid computing, to provision is to activate a grid component, like a server, array or switch, so that it is available for use.

83. Public Key Infrastructure (PKI)

A set of roles, policies and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public key encryption.

84. Quality of Service (QoS)

Manages network capabilities and resources to provide a reliable backbone to IoT connectivity. QoS manages delays, delay variation, bandwidth and packet loss by classifying traffic and registering channel limits.

85. Real Time Process Monitoring (RTPM)

Process data parameters are captured, viewed and analyzed in real time, enabling automatic updates across the enterprise.

86. Remote Maintenance

Support tools and software that enable an IT technician or a support representative to connect remotely to a computer from their consoles via the Internet and work directly on the system without being on-site.

87. Semantic Interoperability

The ability of computer systems to exchange data with unambiguous, shared meaning. It is required to enable machine computable logic, inferencing, knowledge discovery and data virtualization between information systems.

88. Sensor Data

The output of a device that detects and responds to some type of input from the physical environment. The output can be used to provide information or input to another system. It can also be used to guide a process.

89. Smart Factory

Highly digitized and connected production facility that relies on smart manufacturing. Thought to be the 'factory of the future.'

90. Smart Grid

An electricity supply network that uses digital communications technology to detect and react to local changes in usage.

91. Smart Machines

A device embedded with M2M and/or cognitive computing technologies, like AI, machine learning or deep learning. These machines can reason, problem-solve, make decisions and take action.

92. Smart Manufacturing

Manufacturing that incorporates big data and computer-integrated processes into a networked environment designed to improve operational efficiency and data processing capabilities as well as incorporate advanced robotics and rapid design changes.

93. Smart Metering

An electronic device that tracks energy consumption data and transmits wirelessly within a network, helping monitor consumption and costs. Smart meters typically record energy hourly or more frequently, and report at least daily.

94. Smart Robotics

Extending beyond pre-programmed instruction and tasks, these machines incorporate artificial intelligence (AI) and advanced sensor networks to learn from the environment or application and refine or adapt actions accordingly.

95. Software as a Service (SaaS)

SaaS is the topmost service level in Cloud Computing with a third party that provides all IaaS and PaaS services, plus all required maintenance, configuration and updates to your ERP system. With a SaaS contract, you do not own any part of your ERP system, but rather rent the program from a service provider on a monthly basis.

96. Supervisory Control and Data Acquisition (SCADA) System

A control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management, as well as peripheral devices such as PLC and discrete PID controllers to interface with the process plant or machinery.

97. Syntactic Interoperability

A prerequisite for semantic interoperability. Syntactic interoperability refers to the packaging and transmission mechanisms for data.

98. Telematics

An interdisciplinary field that encompasses telecommunications and vehicle technologies.

99. Transport Layer Security (TLS) protocol

A cryptographic protocol that provides end-to-end communications security over networks and is widely used for Internet communications and online transactions.

100. Zero Trust Security (ZTS)

As traditional network perimeters dissolve, organizations must discard the old model of “trust but verify” which relied on well-defined boundaries. Zero Trust mandates a “never trust, always verify, enforce least privilege” approach to privileged access, from inside or outside the network. ZTS is used to help prevent data breaches. No one is trusted by default from inside or outside the network. Verification is required from everyone trying to gain access to resources on the network.

For more information, please visit www.iqms.com or call 1.866.367.3772

Our **3DEXPERIENCE**® platform powers our brand applications, serving 11 industries, and provides a rich portfolio of industry solution experiences.

Dassault Systèmes, the **3DEXPERIENCE**® Company, provides business and people with virtual universes to imagine sustainable innovations. Its world-leading solutions transform the way products are designed, produced, and supported. Dassault Systèmes' collaborative solutions foster social innovation, expanding possibilities for the virtual world to improve the real world. The group brings value to over 210,000 customers of all sizes in all industries in more than 140 countries. For more information, visit www.3ds.com.



3DEXPERIENCE