ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

IoT DEFINITIONS

Term	Definition
General	
Internet of Things (IoT)	The concept to allow Internet-based communications to happen between physical objects, sensors, and controllers. The network of physical objects—devices, vehicles, buildings, and other items that are embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.
Machine-to-Machine (M2M)	Was initially a one-to-one connection, linking one machine to another. This has evolved to mean a much wider range of devices with data easily transmitted via a system of IP networks. Communicate and exchange information with another connected device, without the assistance of a human.
Thing	Device being measured and connected. Also known as Internet "appliances," smart devices, netcentric computing devices, network computers, and ubiquitous or pervasive computing devices, or even information appliances.
Internet of Everything (IoE)	Broader term describing the highest level of IoT, including people, things, machines, and subsystems.
Web of Things	Solely focuses on software architecture (narrow focus).
Smart Product	The intelligent product plays an active role within the production system. It communicates with machines, humans, and other system components to control its own processing, as well as its processing time in an independent manner.
Cyber Physical System (CPS)	Cyber physical systems are intelligent objects based on embedded systems, connected to an Internet of data and services (also IoT) as interacting elements with physical input and output. They are characterized through a combination of real (physical) objects and processes with information processing (virtual) objects and processes by using open, partially global, and always connected information networks. Autonomous systems that merge the physical and the virtual world, connected to each other and to the Internet by wire or wireless.
Application Programming Interface (API)	A set of routines, protocols, and tools for building software applications. The API specifies how software components should interact and APIs are used when programming graphical user interface (GUI) components. Third parties use other company's API platforms as a point of integration.
Gateway	A point on a network that receives information from many other points on the network and transmits information to another network. It can be physical (for example, the router for your home Internet) or embedded.
Node	A connection point, either a redistribution point or an endpoint for data transmissions (a communication endpoint).
Intelligent Node	Gives ability to make a decision locally.
Mote	"Endpoint" in IoT.
Wireless Sensor Network (WSN)	A group of spatially distributed, independent devices that collect data by measuring physical or environmental conditions with minimal power consumption.
IP Address	Method or protocol by which data is sent on the Internet. Each thing with an IP address uniquely identifies it from all others.
Ubiquitous (Pervasive) Computing	Trend of embedding microprocessors in everyday objects so they can communicate information. Pervasive computing devices are completely connected and constantly available.
Ambient Intelligence (AmI)	Electronic environments that are sensitive and responsive to the presence of people.
Situated Computing	Suchman's theory of situated cognition emphasizes the importance of the environment as an integral part of the cognitive process.
Embedded Software	Instruction code that runs on hardware microcontrollers. Usually it is performing specific low level functions, often without using an operating system.
Media Access Control (MAC)	The "layer 2" in a network that allows the physical medium (radio waves or wire signals) to be organized to pass data back and forth.
Transmission Control Protocol/ Internet Protocol (TCP/IP)	The core standard protocol for Internet-based communications.
Software-Defined Network (SDN)	An approach to networking. SDN architectures decouple network control and forwarding functions, enabling network control to become directly programmable.
Spime	Neologism for a futuristic object, characteristic to IoT, that can be tracked through space and time throughout its lifetime.
Edge Node	The interface between the outside network. Sometimes referred to as gateway nodes. Most commonly, edge nodes are used to run client applications and cluster administration tools.
Edge Computing/ Edge Node Analytics	Pushes applications, data, and computing power (services) away from centralized points to the logical extremes of a network. Edge computing replicates fragments of information across distributed networks of Web servers, which may be vast and include many networks. Edge analytics can reduce the need to store and process all data at a central location.
Security	
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.

Public Key Certificate (Digital Certificate or Identity Certificate)	An electronic document used to prove ownership of a public key.
Hardware Roots of Trust	Highly reliable components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. Roots of trust are implemented in hardware so that malware cannot tamper with the functions they provide.
Mutual Authentication (Two-Way Authentication)	Refers to two parties authenticating each other at the same time, and it is a default mode of authentication in some protocols (IKE, SSH) and optional in others (TLS).
Security as a Service (SECaaS)	A business model in which a large service provider integrates its security services into a corporate infrastructure on a subscription basis more cost effectively than most individuals or corporations can provide on their own, when the total cost of ownership is considered.
Entropy (Information Theory)	Systems are modeled by a transmitter, channel, and receiver. The transmitter produces messages that are sent through the channel. The channel modifies the message in some way. The receiver attempts to infer which message was sent. In this context, entropy (more specifically, Shannon entropy) is the expected value (average) of the information contained in each message. Messages can be modeled by any flow of information.
Cryptography (Cryptology)	The practice and study of techniques for secure communication in the presence of third parties called adversaries.
Layered Security (Layered Defense)	Describes the practice of combining multiple mitigating security controls to protect resources and data.
Direct Anonymous Attestation (DAA)	A cryptographic primitive that enables remote authentication of a trusted computer while preserving privacy of the platform's user.
Message Authentication Code (MAC)	A short piece of information used to authenticate a message—in other words, to confirm that the message came from the stated sender (its authenticity) and has not been changed in transit (its integrity).
Wireless Physical Layer Security	The enhancement of privacy at the radio interface of wireless networks, as it is critical to ensure that confidential data are accessible only to the intended users rather than intruders. Jamming and eavesdropping are two primary attacks at the physical layer of a wireless network. The prevalent methods to enhance security are generally classified into five major categories: theoretical secure capacity, and the power, code, channel, and signal detection approaches.
Advanced Encryption Standard (AES)	A symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.
OWASP (Open Web Application Security Project)	A worldwide not-for-profit charitable organization focused on improving the security of software.
Web Application Firewalls (WAF)	An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection.
Wireless	
Wi-Fi	IEEE 802.11x (2.4 GHz) wireless standard. Wi-Fi works with no physical wired connection between sender and receiver by using radio frequency (RF) technology.
802.11ah	Wi-Fi protocol that utilizes sub-1 GHz license-exempt bands as opposed to conventional Wi-Fi that operates in the 2.4 GHz and 5 GHz bands.
Bluetooth®	A standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.
Bluetooth Low Energy (BLE)	Next-generation Bluetooth. Personal area network with short range and low power consumption that allows for objects to transmit data.
6LoWPAN	A low power wireless mesh network where every node has its own IPv6 address, allowing it to connect directly to the Internet using open standards. Combines the Internet protocol (IPv6) and low power wireless personal area networks (LoWPAN). An enhancement to the 802.15.4 (ZigBee).
Sigfox	Proprietary ultranarrow-band (UNB) technology for low power wide area network (LPWAN).
LoRa	Proprietary LoRaWAN (long range wide area network) is a low power of sub-GHz ISM bands wireless networking protocol.
Thread	Proprietary IPv6-based mesh networking protocol, developed on low cost, low power 802.15.4 chipsets (home applications).
ZigBee	Typically used for personal or home area networks or as a mesh network specification for low power wireless local area networks (WLANs) that cover a larger area (ZigBee, ZigBee IP, and ZigBee RF4CE).
General Packet Radio Service (GPRS)	A wireless communications standard on 2G and 3G cellular networks which supports a number of bandwidths and provides data rates of 56 kbps to 114 kbps.
Long-Term Evolution (LTE)	4G wireless broadband technology developed by the Third Generation Partnership Project (3GPP), an industry trade group.
Near-Field Communication (NFC)	Low power, low speed, short range radio communication standard that allows two-way communication between endpoints within very close proximity.
Industrial, Scientific, and Medical (ISM) Band	An unlicensed part of the RF spectrum used for general-purpose data communications. In the U.S., the ISM bands are 915 MHz, 2.4 GHz, and 5.5 GHz, whereas 2.4 GHz is the global unlicensed frequency, and has increasing amounts of interference.
Low Power Wide Area (LPWA)	Built for M2M communications and offer long range, low power consumption. They solve cost and battery life issues that cellular technology cannot, and solve range issues that technologies like Bluetooth or BLE struggle with.
Radio Frequency (RF)/Radio Frequency Identification (RFID)	"Wireless communication" when referred to in IoT discussions. Radio waves to "excite" enough current in a small tag to send a radio transmission back. It works over short range, and only for small amounts of data.
Ultrawideband	A "spark gap" transmitter that emits a very weak, very wide (in frequency) pulse of RF energy. This signal is used mostly for localizing signals. Wide signal bandwidths are short range, high bandwidth communications over a large portion of the radio spectrum.

Wired	
Ethernet	The most widely used local area network (LAN) technology. The Ethernet access method is a system for connecting a number of computer systems over a wired connection to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems.
4 mA to 20 mA	A point-to-point or multidrop circuit mainly used in the process automation field to transmit signals from instruments and sensors in the field to a controller. It sends an analog signal from 4 mA to 20 mA that represents 0% to 100% of some process variable.
HART (highway addressable remote transducer)	A widely used extension to the 4 mA to 20 mA analog signal used in sensor networks, the HART protocol superimposes a 1200 bits per second digital signal onto the line that provides bidirectional communications with intelligent devices.
Services	
Cloud Computing	A network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.
SaaS	Software as a service is now considered as a key offering within cloud computing.
IaaS	Infrastructure as a service.
PaaS	Platform as a service.
DaaS	Desktop as a service.
BaaS	Mobile back end as a service.
ITMaaS	Information technology management as a service.
Analytics	
Real-Time Analytics	Dynamic analysis and reporting, based on data entered into a system less than one minute before the actual time of use.
Historical Analytics	The study of past historical data to research potential trends, to analyze the effects of certain decisions or events, or to evaluate performance.
Predictive Analytics	The practice of extracting information from existing data sets in order to determine patterns and predict future outcomes and trends. Using predictive analytics, we can predict future events like when a machine might fail. It does not however change a machine's operating conditions to extend remaining useful life. That would be the domain of prescriptive analytics.
Prescriptive Analytics	Automatically synthesizes big data, multiple disciplines of mathematical sciences and computational sciences, and business rules to make predictions and suggest decision options to take advantage of the predictions.
Industry	
Industrial IoT	M2M communication for machinery and other industrial applications (wired and wireless). Machinery and equipment can send back real-time information to an application to better understand how efficiently that equipment is running.
Industry 4.0	The fourth industrial revolution is a collective term embracing a number of contemporary automation, data exchange, and manufacturing technologies. Industry 4.0 facilitates the vision and execution of a "smart factory." Within the modular structured smart factories of industry 4.0, cyber physical systems (CPS) monitor physical processes, create a virtual copy of the physical world and make decentralized decisions. Over the Internet of Things, cyber physical systems communicate and cooperate with each other and with humans in real time, and via the Internet of Services, both internal and cross-organizational services are offered and utilized by participants of the value chain. Industry 4.0 involves the technical integration of CPS into manufacturing and logistics, and it describes the convergence of cybernetics and informatics, which get through all production areas and thereby creates intelligent self-configuring, self-controlling products and production systems. From a technical point of view, Industry 4.0 is the convergence of IoT with the Internet of Things and Services.
Health	
VSM	Vital signs monitoring. Portable devices that continuously monitor multiple indicators.
Energy	
Smart Meter	An electronic device that collects data about consumption of energy (gas, electric) and communicates it back to the energy company and/or consumer.

Analog Devices, Inc.
Worldwide Headquarters

Analog Devices, Inc.
One Technology Way
P.O. Box 9106
Norwood, MA 02062-9106
U.S.A.
Tel: 781.329.4700
(800.262.5643, U.S.A. only)
Fax: 781.461.3113

Analog Devices, Inc.
Europe Headquarters

Analog Devices, Inc.
Otl-Aicher-Str. 60-64
80807 München
Germany
Tel: 49.89.76903.0
Fax: 49.89.76903.157

Analog Devices, Inc.
Japan Headquarters

Analog Devices, KK
New Pier Takeshiba
South Tower Building
1-16-1 Kaigan, Minato-ku,
Tokyo, 105-6891
Japan
Tel: 813.5402.8200
Fax: 813.5402.1064

Analog Devices, Inc.
Asia Pacific Headquarters

Analog Devices
5F, Sandhill Plaza
2290 Zuchongzhi Road
Zhangjiang Hi-Tech Park
Pudong New District
Shanghai, China 201203
Tel: 86.21.2320.8000
Fax: 86.21.2320.8222

analog.com

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™