

IoT IN ROBOTICS AND AUTOMATION.

MEANING OF IoT

IoT stands for Internet of Things.

It refers to the network of physical objects ("things") that are embedded with sensors, software, processing ability, and other technologies, allowing them to connect to the internet (or other networks) and exchange data with each other and with central systems – often with little or no direct human intervention.

In simple terms: Everyday objects become "smart" because they can collect data about their environment, send it over the internet, receive instructions, and sometimes take actions automatically.

Core elements usually present in IoT

- Physical object; e.g. thermostat, car, fridge, wearable, industrial machine, street light.
- Sensors or actuators ; to detect (temperature, motion, light, pressure...) and sometimes act (turn on or off, open or close)
- Connectivity ; Wi-Fi, Bluetooth, cellular, LoRa, Zigbee, etc.
- Data processing ; either on the device itself or in the cloud
- Unique identification – so each device can be individually addressed

MEANING OF ROBOTICS.

Robotics is the interdisciplinary field of science, engineering, and technology focused on the design, construction, operation, programming, and use of robots such as machines that can sense their environment, process information, and perform actions (often with some degree of autonomy) to carry out tasks that are typically dangerous, repetitive, precise, or otherwise difficult for humans.

In simple terms: Robotics is about creating intelligent machines that can perceive, think (or compute), and act in the physical world, usually to assist, replace, or extend human capabilities.

Core components of a robot (common to almost all definitions)

- Mechanical structure ; the physical body (arms, wheels, legs, grippers)



- Sensors ; to detect the environment (cameras, lidar, touch, temperature, force)
- Actuators ; motors or systems that enable movement
- Control system / software ; the "brain" (microcontrollers, AI algorithms, programming) that processes data and decides actions
- Power source ; batteries, electricity, etc.

MEANING OF AUTOMATION

Automation refers to the use of technology, machines, computers, software, or systems to perform tasks, processes, or operations with minimal or no human intervention.

In simple terms: Instead of a person doing repetitive, predictable, or rule-based work manually , a machine/system does it automatically.

Core Meaning (from major sources)

- 1) Merriam-Webster: The technique of making an apparatus, process, or system operate automatically; the state of being operated automatically (often by mechanical/electronic devices replacing human labor).
- 2) Cambridge Dictionary: The use of machines or computers instead of people to do a job (especially in factories or offices).
- 3) Wikipedia or general technical view: A wide range of technologies that reduce human intervention in processes by predetermining decision criteria, rules, and actions, then embodying them in machines.
- 4) IBM / modern business view: The application of technology, programs, robotics, or processes to achieve outcomes with minimal human input.
- 5) ISA (International Society of Automation): The creation and application of technology to monitor and control the production and delivery of products and services.

Main Types of Automation (2025–2026 perspective)

- 1) Basic / Task Automation ; Simple repetitive tasks (e.g., data entry bots, macro in Excel).
- 2) Process Automation ; Multi-step business workflows (e.g., RPA = Robotic Process Automation tools like UiPath, Automation Anywhere).
- 3) Industrial Automation ; Factory robotics, PLCs (programmable logic controllers),



SCADA systems.

- 4) IT & Infrastructure Automation ; DevOps tools, Ansible, Terraform, auto-healing systems.
- 5) Hyperautomation ; Combining RPA + AI + ML + low-code tools to automate complex end-to-end processes.

Relationships between IoT , robotics and automation.

IoT (Internet of Things) robotics, often referred to as the Internet of Robotic Things (IoRT), represents the integration of IoT technologies such as sensors, connectivity, and data exchange—into robotic systems to make them smarter, more interconnected, and capable of operating with greater autonomy. This fusion essentially elevates traditional robotics by enabling robots to communicate with other devices, networks, and environments in real-time, turning them into "connected machines."

Automation, on the other hand, is the broader use of technology to perform tasks with minimal human intervention, often through machines, software, or systems that follow predefined rules or processes. The relationship between IoT robotics and automation is one of enhancement and synergy: IoT robotics is a specialized subset or advanced evolution of automation, where IoT adds layers of intelligence, data-driven decision-making, and interconnectivity to robotic automation. In essence, while automation can exist without IoT , for example, simple mechanical assembly lines), integrating IoT into robotics supercharges automation by allowing systems to adapt dynamically, predict issues, and optimize operations across ecosystems.

Key Aspects of the Relationship

- 1) Enhanced Autonomy and Efficiency: IoT enables robots to collect vast amounts of sensor data from their surroundings, process it via cloud or edge computing, and make autonomous decisions without constant human oversight. This leads to "hyper-automation" in fields like manufacturing, where robots can self-adjust for predictive maintenance or real-time process tweaks.
- 2) Interconnectivity and Collaboration: In IoT robotics, robots don't operate in isolation; they form part of a larger network. Such includes, in smart factories under Industry 4.0), sharing data with other IoT devices for coordinated actions. This multi-robot collaboration boosts overall automation by enabling complex, synchronized tasks that traditional automation couldn't handle as fluidly.
- 3) Data-Driven Intelligence: Both IoT devices and robots rely on sensors to perceive



and respond to environments, but their combination amplifies automation through AI integration, allowing for learning from data patterns, anomaly detection, and adaptive behaviors.

- 4) Applications Across Industries: In manufacturing, IoT-enabled robotic arms automate assembly while monitoring equipment health. In agriculture, drones and robots use IoT for precision farming automation like crop monitoring. Healthcare sees robotic assistants automating patient care routines with real-time data from wearables. Even in smart homes, IoT robotics automates tasks like vacuuming or security patrols.

Overall, IoT robotics doesn't replace automation but transforms it into a more intelligent, scalable, and responsive framework, driving innovations in efficiency, cost reduction, and safety as of 2026. This convergence is key to emerging technologies like AI-powered smart factories, where the lines between IoT, robotics, and automation increasingly blur for seamless operations.

IMPORTANCE OF IoT IN MODERN ROBOTICS AND AUTOMATION.

- 1) **Real-Time Data Collection and Visibility** : IoT sensors on robots and machinery continuously gather data on performance, environment, vibrations, temperature, energy use, and more. This provides unprecedented visibility into operations, allowing instant monitoring and feedback loops that traditional automation lacks.
- 2) **Predictive Maintenance and Reduced Downtime**: By analyzing IoT data streams (often with AI/ML), systems detect anomalies early . Such includes, unusual wear in a robotic arm—predicting failures before they occur. This minimizes costly unplanned stops, extends equipment life, and is a core driver of efficiency in modern factories.
- 3) **Enhanced Autonomy and Intelligent Decision-Making**: IoT enables robots to "sense" their surroundings dynamically and make autonomous adjustments. Combined with edge computing (processing data locally for low latency), robots respond instantly without constant cloud reliance which is essential for fast-moving tasks like autonomous mobile robots (AMRs) in warehouses or adaptive assembly lines.
- 4) **Interconnectivity and Ecosystem Collaboration**: IoT turns individual robots into part of a larger network: robots share data with other machines, conveyors, inventory systems, or even supply chain platforms. This creates coordinated fleets (e.g., swarms of AMRs or collaborative cobots), breaking down silos and

enabling versatile, scalable automation under IT/OT convergence.

- 5) Optimization, Efficiency, and Cost Savings: Real-time insights from IoT optimize energy use, resource allocation, production quality, and workflows. In manufacturing, this means higher throughput, fewer errors, better traceability, and safer operations such as robots handling hazardous tasks while humans oversee via data dashboards).
- 6) Support for Emerging Trends like Physical AI and Humanoids: In 2026, advanced robotics (including humanoids and AI-driven agents) rely on IoT for perception, real-time environmental data, and integration into digital twins or "digital nervous systems." This convergence of IoT, AI, robotics, and edge tech is accelerating "Physical AI," where robots act intelligently in unstructured settings.

HOW IoT WORKS IN ROBOTICS AND AUTOMATION.

IoT works in robotics and automation by turning isolated machines and robots into connected, data-aware, and systems through a network of sensors, connectivity, processing, and communication layers. This integration, often called the Internet of Robotic Things (IoRT) enables real-time data collection, sharing, analysis, and action, making automation smarter, more adaptive, and scalable.

At its core, IoT adds connectivity and intelligence to traditional robotics (which focus on physical manipulation) and automation (rule-based task execution), allowing systems to perceive environments dynamically, collaborate, predict issues, and optimize operations autonomously.

Core Components and How IoT Works Step-by-Step

IoT in robotics and automation typically follows a layered architecture (inspired by common IoRT models as of 2026):

- 1) Physical / Perception Layer (The "Senses" and "Muscles"); Robots and automated machines are equipped with IoT sensors (cameras, LiDAR, ultrasonic, temperature, pressure, vibration, force/torque, microphones, IMUs) and actuators (motors, grippers, valves). These collect raw real-time data from the environment, the robot's own state, and nearby objects/machines. For example: A robotic arm in a factory senses part misalignment via vision sensors.
- 2) Connectivity / Network Layer (The "Nervous System"): Data is transmitted securely via wireless protocols (Wi-Fi, 5G, Bluetooth, Zigbee, LoRaWAN, or wired Ethernet for industrial reliability). Edge gateways or local networks handle low-

latency communication between robots, other IoT devices, and central systems. Robots share data with each other (fleet coordination) or with external platforms such as MES, ERP, cloud). This enables remote monitoring, control, and multi-robot collaboration.

3) Processing / Intelligence Layer (The "Brain")

Data is processed at multiple levels:

- Edge computing (on-device or nearby gateways) for fast, low-latency decisions (e.g., obstacle avoidance in an autonomous mobile robot).
- Fog/Cloud computing for heavier analysis using AI/ML (e.g., pattern recognition, predictive models).
- Fusion of multi-sensor data creates a comprehensive "understanding" of the scene.

AI algorithms analyze streams to detect anomalies, optimize paths, or learn from experience.

- 4) Application / Service Layer (The "Decision and Action"); Processed insights trigger actions: adjust robot behavior, send alerts, update digital twins, or feed enterprise systems. Humans can monitor dashboards or intervene remotely if needed. Over time, systems self-optimize (e.g., predictive maintenance schedules robot downtime).

CHALLENGES OF IoT IN ROBOTICS AND AUTOMATION.

- Cybersecurity Vulnerabilities and Threats: Connectivity dramatically expands the attack surface: robots, sensors, edge devices, and cloud links become prime targets for hackers. Risks include AI-driven attacks, malware, ransomware, unauthorized control of robots (potentially causing physical harm), data breaches, botnets, and manipulation of autonomous systems. In 2026, experts highlight rising AI-assisted threats, deep learning "black box" opacity (hard-to-explain decisions), and the need for zero-trust security as integral (not add-on) to IoT/automation strategies.

Consequences: production halts, intellectual property theft, safety incidents, or even physical damage from tampered robots.

- High Implementation and Upfront Cost: Deploying IoT in robotics involves expensive hardware (sensors, 5G/edge gateways), software, integration, and network upgrades Full system setup (e.g., for smart factories or robot fleets)

often adds 10–30% beyond robot costs, plus ongoing expenses for maintenance, updates, and security tools.

Smaller manufacturers or SMEs struggle with ROI justification, especially amid economic pressures and supply chain issues.

- Integration and Interoperability Issues: Legacy systems (old PLCs, SCADA, MES) often don't easily connect to modern IoT platforms, leading to compatibility problems, data silos, and complex retrofits.
- Lack of universal standards for protocols, data formats, and device communication creates "vertical silos," slows adoption, and increases deployment time/risk.

In robotics, this hinders seamless multi-robot collaboration or fleet coordination.

- Reliability, Latency, and Real-Time Performance Challenges: Dependence on networks (even 5G) introduces risks of downtime, packet loss, or latency in critical applications (e.g., autonomous mobile robots or collaborative cobots). Edge computing helps, but resource-limited robotic hardware struggles with heavy AI processing, energy demands, or adapting to dynamic environments.

Wireless sensors can face slow transmission or hacking vulnerabilities in industrial settings.

- Scalability and Complexity Management: Scaling IoT-robotics across large facilities or fleets becomes difficult: managing thousands of connected devices, data volumes, and orchestration grows exponentially complex.

Issues include energy efficiency (battery-powered robots drain faster with constant connectivity), over-reliance on cloud (vs. edge), and maintaining performance in unstable networks.

- Workforce and Skills Gaps: Requires specialized expertise in IoT, cybersecurity, AI, robotics programming, and data analytics—skills that remain scarce. Organizations face training demands, hiring challenges, or reskilling needs.

Workforce acceptance can be an issue if automation is perceived as job-threatening (though it often augments roles).

- Ethical, Privacy, and Regulatory Concerns: IoT robots collect sensitive data (e.g., video/audio from workplaces, health info in care settings), raising privacy risks and ethical dilemmas (e.g., surveillance vs. rights). Liability questions arise for autonomous decisions causing harm, plus regulatory hurdles for safety certification and large-scale deployment.



In human-robot collaboration, safety remains a key barrier.

Other Operational Drawbacks

- Maintenance and Downtime: Connected systems need frequent updates and monitoring to avoid failures.
- Overheating/Malfunctions: Poorly integrated IoT can cause physical issues in devices or products.
- Adaptability Limits: Robots may struggle in highly unstructured or rapidly changing environments despite IoT enhancements.