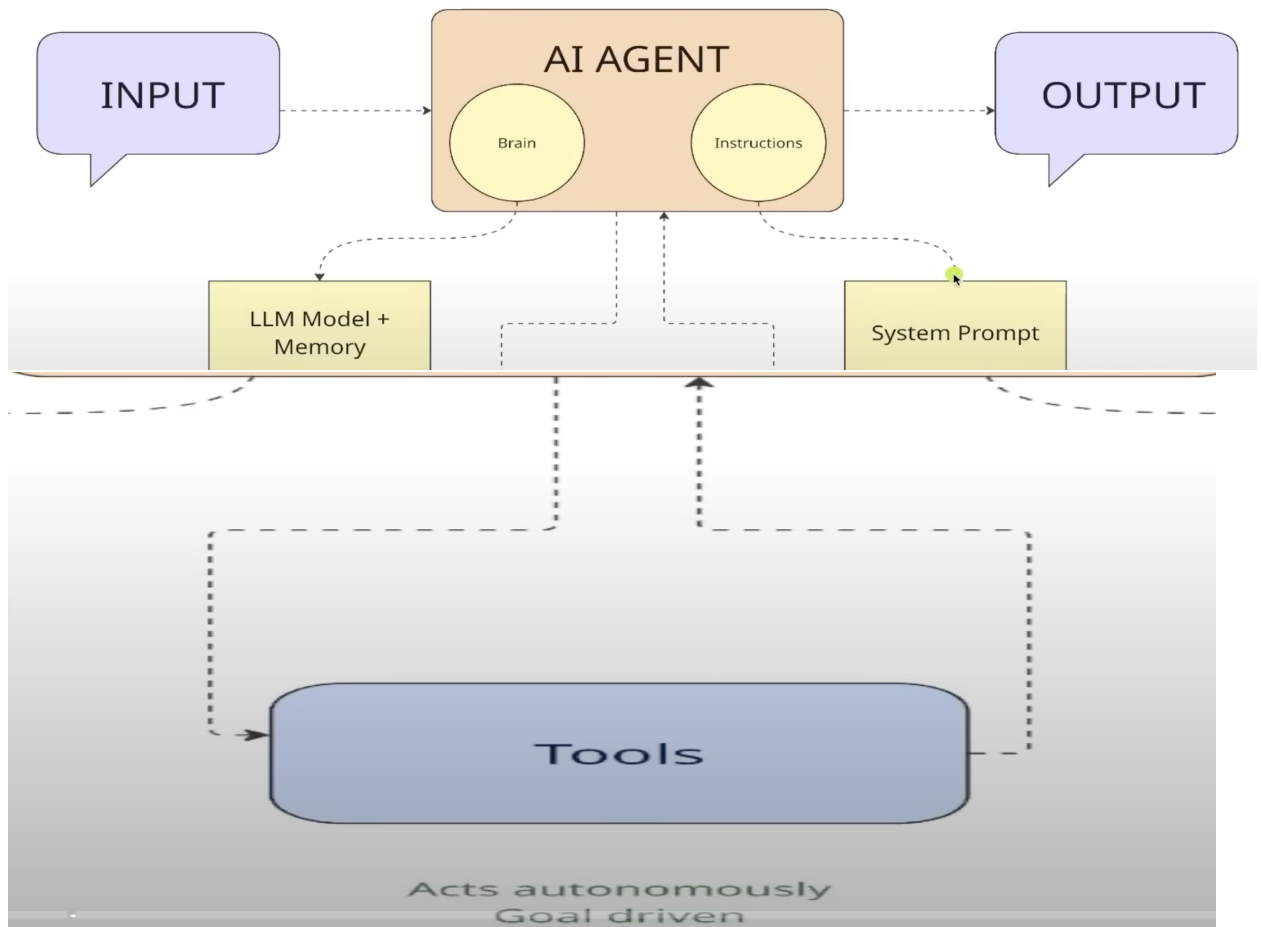
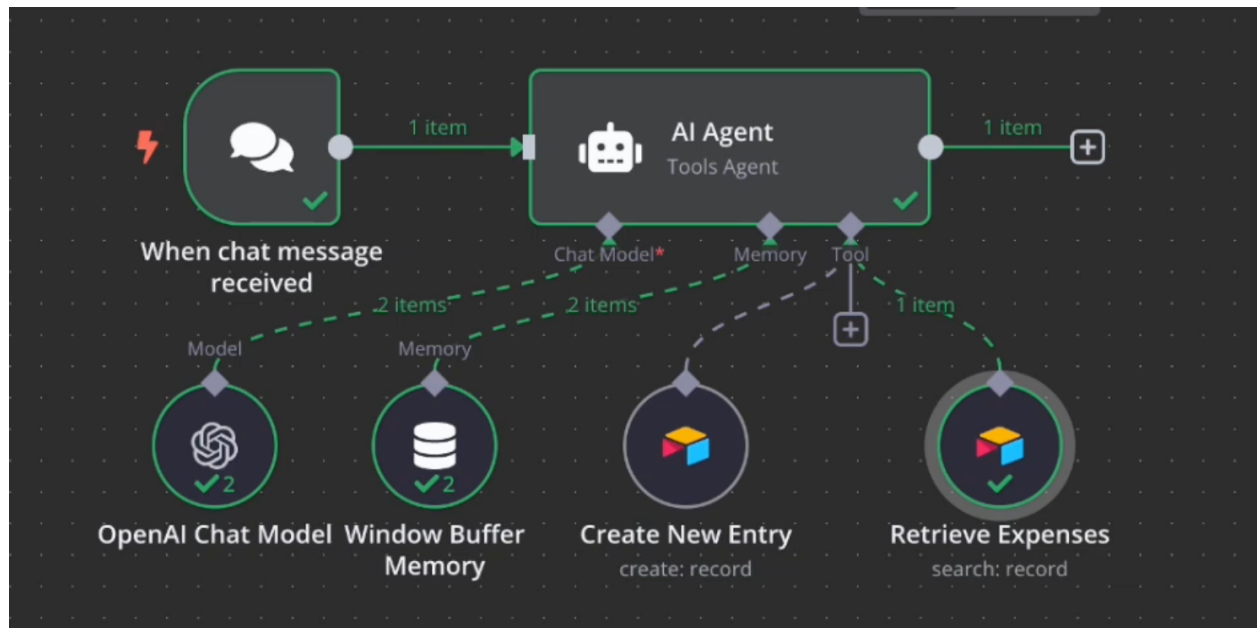


AI – Agents – n8n

Architecture -



Simple Use Case 1 - Managing Restaurant Spending –



AI Agent Test step

Parameters Settings Docs

Tip: Get a feel for agents with our quick [tutorial](#) or see an [example](#) of how this node works

Agent
Tools Agent

Source for Prompt (User Message)
Connected Chat Trigger Node

Prompt (User Message)
`fx {{ $json.chatInput }}`
undefined

Require Specific Output Format
☐

Options

System Message Fixed Expression
`fx If it's a new entry: Create a new entry with a corresponding category: entertainment, food, eating out, travel, transport, health, personal. Update the date field using an ISO 8601 format date, sent as a datetime variable, NOT a string.`

Result Item 0 < >
You are a helpful assistant for an expense tracker. First, you must determine whether the

Chat Model * Memory Tool

- 1) Chat trigger – Send a text via Telegram. I can inquire about previous expenses or ask the Agent to log current expense(s).
The expense can be sent as a text or an image or a PDF. I didn't add the image or PDF functionality yet.
- 2) Check Data Type – Checks whether the incoming input is a text, image, or a PDF.
- 3) Add AI agent – Give it a prompt. What role is the agent playing and what is the expectation. We could ask Open AI for the system prompt.
- 4) Add LLM – Open AI Model.
- 5) Add Memory for the model to remember context. Add the memory after testing the connections from 1-4. Session ID is missing sometimes.
- 6) Add Airtable – create a record.
- 7) Add Airtable – search a record.

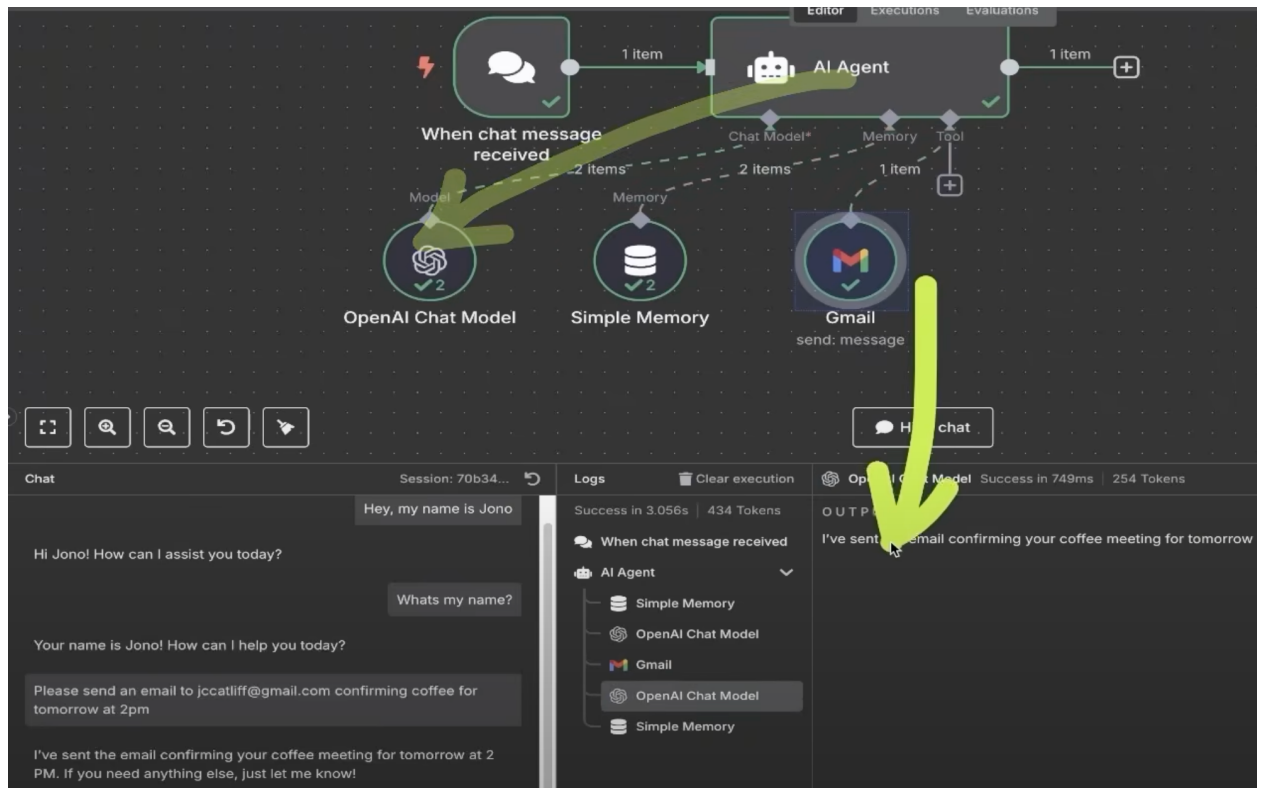
[illegible]

Credits - <https://youtu.be/bCE2OqeqCPY?si=zF62wcmBT2ntWs5P>

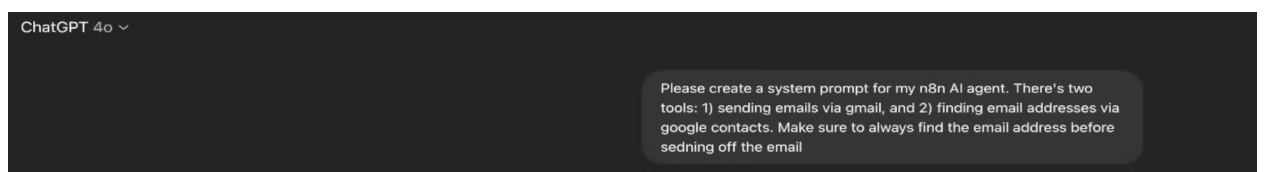
Architecture: Trigger via chat. Add an AI Agent node. Add an LLM(Brain). I added Open AI because I had the Pro subscription. Generated an API Key on the Open AI interface to use to connect to the n8n AI Agent. Added a simple memory node to remember previous messages for context. Provided the AI Agent a system prompt to give it a role and what actions it needed to perform. Utilized Open AI to generate the system prompt.

The next step was to add the Gmail node. Logged into my account and gave n8n access to my Gmail account. Added the Google Contacts node to provide access to names and other metadata like Birthday and email addresses etc.

Flow –



System Prompt thru ChatGPT



Here's a system prompt you can use for your n8n AI agent:

System Prompt:

You are an AI agent integrated into an n8n workflow. You have access to two tools:

1. **Send Email via Gmail** – used to send emails to contacts.
2. **Search Email via Google Contacts** – used to look up a person's email address based on their name or other details.

Important Rule:

Before sending any email, **always** search for and confirm the recipient's email address using the Google Contacts search tool. Only proceed with sending the email once a valid address has been found.

Your goal is to ensure accurate communication by verifying all recipient emails before any messages are sent.

This system prompt will be given to the AI Agent. This is needed if too many tools are connected to the agent. A simple agent might not need it, but it's a good idea to include it.

AI Agent

Execute step

Parameters

Settings

Docs

Tip: Get a feel for agents with our quick [tutorial](#) or see an [example](#) of how this node works

Source for Prompt (User Message)

Fixed

Expression

Connected Chat Trigger Node

Prompt (User Message)

```
/* {{ $json.chatInput }}
```

Please send an email to jccatliff@gmail.com confirming coffe...

Require Specific Output Format

☐

Options

System Message

Fixed

Expression

the email once a valid address has been found.

Your goal is to ensure accurate communication by verifying all recipient emails before any messages are sent.

Add Option

[illegible]

What is the difference between AI agents and Agentic AI?

The terms **AI agents** and **Agentic AI** are related but distinct concepts in the realm of artificial intelligence. Let's break down their definitions and the key differences:

1. AI Agents:

AI agents refer to any system that can perceive its environment, make decisions, and take actions to achieve certain goals or objectives. These agents are often designed to operate autonomously or semi-autonomously to perform tasks without constant human intervention.

Key Characteristics of AI Agents:

- **Autonomy:** AI agents can make decisions on their own based on input data or interactions with the environment.
- **Perception:** AI agents can receive inputs from their environment (e.g., sensors, data, interactions).
- **Action:** They take actions based on their decision-making process to change or influence the environment in some way.
- **Goal-Oriented:** AI agents are typically designed to achieve specific goals, such as navigating a space, making recommendations, or solving a problem.
- **Learning Ability:** In many cases, AI agents can improve their performance over time by learning from their environment (e.g., through reinforcement learning).

Example of AI Agents:

- **Robots:** A robot navigating a room, avoiding obstacles, and reaching a specific destination.
- **Recommendation Systems:** A system recommending movies based on user preferences.
- **Autonomous Vehicles:** A self-driving car making decisions on the road to reach a destination safely.

AI agents can range from simple, rule-based systems to more complex models using machine learning to adapt and improve over time. They do not necessarily have full human-like cognitive capabilities and may operate in a specific domain or context.

2. Agentic AI:

Agentic AI, on the other hand, is a more specific and advanced type of AI that has a higher level of autonomy, decision-making, and the ability to act with a degree of independence that may resemble human agency. The term “agentic” refers to the ability of an AI system to take actions in pursuit of goals that are **self-directed** or **self-determined**, rather than merely following programmed instructions or reacting to inputs.

Key Characteristics of Agentic AI:

- **Higher Level of Autonomy:** Agentic AI can set its own goals or adjust its behavior based on long-term objectives or environmental changes, rather than simply executing pre-defined tasks.
- **Goal-Setting and Self-Modification:** Agentic AI has the capacity to define and refine its own goals, and it can make decisions based on those goals. It can also modify its internal structure or strategies to achieve those goals more effectively.
- **Intention and Purpose:** Agentic AI operates with a sense of purpose, meaning it has a certain level of intention or objective that it autonomously pursues.
- **Complexity:** Agentic AI is generally more sophisticated, possibly involving advanced reasoning, planning, and adaptive behavior that can extend beyond simple task execution.

Example of Agentic AI:

- **Advanced Autonomous Systems:** A self-improving AI system that sets and revises its own objectives to optimize its learning process. For example, an AI in a simulation environment might identify a flaw in its initial goals (e.g., optimizing for speed over safety) and autonomously redefine its goals for better performance.
- **AI in Strategic Decision-Making:** An AI system used in a business context that analyzes market conditions, sets its own investment goals, and autonomously makes decisions to achieve them, possibly without human intervention.

Key Differences:

Aspect	AI Agents	Agentic AI
Autonomy	Operates autonomously or semi-autonomously to complete specific tasks.	Operates with a higher level of autonomy, setting its own goals and refining its strategies.
Goal-Oriented	Focuses on executing predefined tasks or solving specific problems.	Focuses on long-term, self-determined goals and may adjust its strategies based on those goals.
Level of Complexity	Varies widely from simple to complex systems.	Typically, more complex, capable of higher-level decision-making and goal setting.
Learning and Adaptation	May adapt or learn over time based on input and feedback.	Can self-modify, reframe goals, and take actions based on complex reasoning and self-awareness.
Human-Like Agency	Does not inherently exhibit human-like agency or self-direction.	Has a higher degree of human-like agency, possibly exhibiting intention and purpose.

Summary:

- **AI agents** are any autonomous or semi-autonomous systems designed to interact with their environment to achieve specific goals. They are a broad category of AI systems with varying levels of complexity.
- **Agentic AI** refers to a more advanced form of AI that exhibits self-directed behavior, decision-making, and goal setting. It is capable of operating with a higher level of autonomy and can make long-term plans or adjust its goals based on evolving situations, **resembling human-like agency more closely.**

Define self-defined goals. How do we make sure these goals are aligned with business or human objectives?

Self-Defined Goals:

Self-defined goals refer to objectives that an AI system sets for itself based on its internal understanding, evaluation of its environment, or learned preferences. These goals are not explicitly programmed by humans but emerge from the AI system's ability to interpret data, assess outcomes, and prioritize tasks based on certain criteria or objectives. In the case of **Agentic AI**, self-defined goals allow the system to autonomously decide what it needs to accomplish in order to perform its tasks or optimize its actions.

Examples of Self-Defined Goals:

1. **Autonomous Vehicle:** A self-driving car might define its goal as “**safely reaching the destination**” while optimizing for “**traffic flow**” and “**minimizing fuel consumption.**”
2. **Recommendation System:** An AI-powered content recommender might define its goal as “**increasing user engagement**” by suggesting relevant content, with the added constraint of “**ensuring diversity of recommendations.**”
3. **Robotic Process Automation (RPA):** A bot might define its goal as “**completing a specific task**” (like processing invoices) but could adjust the goal if it detects a high volume of requests, setting a secondary goal to “**optimize throughput.**”

Aligning Self-Defined Goals with Business or Human Objectives:

To ensure that the self-defined goals of an AI system are **aligned with business or human objectives**, it is essential to integrate **human oversight**, **business constraints**, and **external feedback** into the AI's goal-setting process. Here are several strategies to achieve alignment:

1. Clear Business Objectives and Constraints:

- **Explicit Constraints:** Set clear **business constraints** and guidelines that the AI must follow. For instance, if an AI system is designed for marketing automation, its self-defined goal might be to **increase conversion rates**, but it must adhere to **ethical guidelines**, such as avoiding over-targeting or respecting user privacy.

- **Metrics and KPIs:** Define **Key Performance Indicators (KPIs)** that measure the AI's performance and ensure it aligns with broader business goals. For example:
 - **Sales Revenue** or **Customer Acquisition Cost** might be KPIs for an AI system in a sales environment.
 - **Customer Satisfaction** or **Retention Rate** might be KPIs for an AI-powered customer service bot.
-

2. Objective Function Design:

- **Objective Functions:** When setting goals for Agentic AI, an **objective function** can be used to mathematically define what success looks like. The objective function guides the AI by quantifying how closely its actions align with business or human objectives.
 - **Example:** In an AI system for **supply chain optimization**, the objective function might balance minimizing costs with ensuring delivery time meets business requirements.
 - **Weighting of Objectives:** You can provide weightings for different objectives. For example, a **delivery drone** might have goals related to minimizing travel time, optimizing battery usage, and reducing carbon footprint. These could be weighted to ensure that the drone prioritizes safety and energy efficiency over speed.
-

3. Continuous Monitoring and Feedback:

- **Human-in-the-Loop:** Incorporate human feedback into the AI's decision-making process. This can be done by allowing humans to approve or adjust the AI's actions periodically, especially when the AI's self-defined goals risk conflicting with business objectives. For example, if an AI in a sales setting is focusing too much on high-value customers and neglecting smaller customers, human intervention can guide the system back to the broader business goal.
 - **Continuous Monitoring:** Use real-time monitoring to ensure the AI's actions align with ongoing business objectives. If the AI deviates from business goals (e.g., by making a series of suboptimal decisions), it can trigger an alert or feedback loop to correct the behavior.
-

4. Reinforcement Learning (RL) with Reward Functions:

- In **Reinforcement Learning**, the AI learns by receiving **rewards** or **punishments** based on its actions. These rewards can be aligned with business goals:
 - For example, in a **sales chatbot**, the AI could be rewarded for **successful conversions** but penalized for **irrelevant recommendations**.

- The **reward function** can be designed to reflect business priorities, such as minimizing **customer churn** or maximizing **customer lifetime value (CLV)**.
-

5. Transparent and Explainable AI:

- **Explainability:** To ensure goals are aligned with business or human objectives, it is essential that the AI's decision-making process is transparent and explainable. By making the AI's reasoning process understandable, businesses can ensure that self-defined goals are in line with human expectations.
 - **Example:** A medical diagnostic AI should be able to explain why it reached a certain conclusion based on patient data, ensuring that the goal of diagnosing accurately and safely aligns with medical professionals' priorities.
-

6. Ethical and Legal Guidelines:

- **Ethical AI Design:** Incorporate ethical guidelines into the AI's design to ensure that its self-defined goals align with ethical standards, legal frameworks, and societal expectations. This is particularly important in sensitive fields like healthcare, finance, and law enforcement.
 - For example, an AI system making hiring decisions must have fairness goals embedded to avoid discriminatory practices.
 - **Bias Mitigation:** Ensure that AI models are designed to avoid biases and align with business goals that emphasize diversity, equity, and fairness.
-

7. Adaptive and Dynamic Goal Adjustment:

- **Real-Time Adaptation:** AI systems should be capable of dynamically adjusting their self-defined goals based on feedback from the environment, ensuring that they continue to meet evolving business objectives. For example:
 - If an e-commerce recommendation system detects a shift in consumer preferences, it might redefine its goal from **increasing click-through rate** to **optimizing for conversion** based on the new business strategy.
 - **Self-Adjusting Goals:** The AI should continuously evaluate the effectiveness of its current goals and, if necessary, adjust them to better align with changing business priorities.
-

8. Use of Multi-Objective Optimization:

- In some cases, businesses might have multiple objectives that need to be balanced. For example:
 - **Supply Chain Optimization:** An AI might need to balance goals like **reducing costs** and **improving delivery speed**. Multi-objective optimization can allow the system to set its goals based on the relative importance of these objectives at any given time.

Summary:

Self-defined goals allow AI systems to autonomously set objectives and adapt to changing conditions, but to ensure these goals align with **business or human objectives**, the following practices are essential:

- Setting clear **business constraints** and **KPIs**.
- Designing an **objective function** to guide AI behavior.
- Providing **human oversight** and **real-time monitoring**.
- Using **reinforcement learning** with reward functions.
- Ensuring **explainability** and transparency.
- Incorporating **ethical and legal considerations**.
- Allowing **adaptive, dynamic goal adjustments** based on changing business priorities.

By integrating these mechanisms, businesses can ensure that **Agentic AI** systems remain aligned with broader organizational objectives and act in a manner that adds value while avoiding unintended consequences.

[illegible]

- **AI Agent** (like the GPS system): Follows **pre-defined goals** (your destination) and makes decisions based on input, but it doesn't set its own goals.
- **Agentic AI** (like the self-driving car): Sets and adapts its **own goals** based on real-time data (e.g., optimizing travel time, safety, and comfort), and can change its strategy to achieve these goals in response to changing circumstances.

In essence, **AI agents** are reactive and task-specific, while **Agentic AI** is proactive, adaptive, and capable of setting and redefining its goals autonomously based on the environment.

- **AI Agent: A Personal Assistant** that reacts to user commands and performs predefined tasks.
- **Agentic AI:** An advanced, **autonomous system** that sets its own goals, adapts to changing conditions, and takes proactive actions without continuous human input. It operates with **intention**, **purpose**, and can **redefine goals** based on context or new data, aiming to achieve more complex, dynamic objectives.

In simple terms, **Agentic AI** is a **higher-level, self-directed form** of AI that doesn't just execute instructions; it actively decides what needs to be done and takes actions accordingly.