	Marwadi University **Faculty of Technology** **Department of Information and Communication Technology**	
Subject: Microcontroller and Interfacing (01CT0403)	**Aim:** Controller Area Network (CAN)	
Case Study :- 03	**Date:-** 27-03-2024	**Enrollment No:-** 92200133030

CAN basics and their importance

❖ Introduction

- The Controller Area Network (CAN) protocol is a robust and reliable communication protocol designed for use in harsh industrial environments. It is widely employed in automotive applications, as well as in industrial and medical equipment.

❖ CAN Protocol Overview

- CAN is a message-based protocol that uses bit-wise arbitration to ensure reliable data transmission. Each message consists of an identifier, data field, and error-checking mechanisms. Nodes on the network compete for access to the bus using arbitration, with higher-priority messages taking precedence.

❖ CAN Physical Layer

- The CAN physical layer specifies the electrical signaling and bus topology. It uses a differential signal transmission method over a twisted-pair cable to achieve high noise immunity. The CAN bus is terminated at both ends with resistors to prevent signal reflections.

❖ CAN Message Format

- **Start of Frame (SOF) bit:** This is the first bit of a CAN frame, indicating the start of a message transmission. It serves as a synchronization signal for the receiving nodes to correctly interpret the incoming message.
- **Identifier (11 or 29 bits):** The identifier is a unique identifier assigned to each CAN message. In CAN 2.0A, the identifier is 11 bits long, allowing for up to 2^11 (2048) different message identifiers. In CAN 2.0B, the extended identifier is 29 bits long, allowing for a much larger number of unique identifiers.
- **Remote Transmission Request (RTR) bit:** This bit is used to indicate whether the message is a data frame (RTR = 0) or a remote frame (RTR = 1). In a remote frame, the transmitting node is requesting data from other nodes rather than transmitting actual data.
- **Data Length Code (DLC):** This field indicates the number of bytes of data being transmitted in the CAN frame. It ranges from 0 to 8 bytes, allowing for variable-length data payloads.
- **Data field (0-8 bytes):** This is the actual data being transmitted within the CAN frame. The size of the data field is determined by the DLC field mentioned above, and it can contain up to 8 bytes of information.
- **Cyclic Redundancy Check (CRC):** The CRC is a mechanism used for error detection in the CAN frame. It is computed based on the contents of the frame and appended to the end of the data field. Upon receiving a frame, the receiving node recalculates the CRC and compares it to the received CRC to check for any transmission errors.

- **Acknowledgment (ACK) bit:** This bit is sent by the receiving node to acknowledge the correct reception of a CAN frame. It indicates to the transmitting node that the frame was successfully received without any errors.
- **End of Frame (EOF) bit:** This bit signals the end of the CAN frame transmission. It follows the CRC field and precedes the interframe space before the next CAN frame transmission can begin.

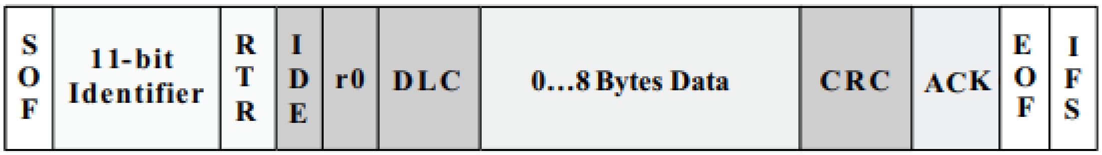

Figure 2. Standard CAN: 11-Bit Identifier

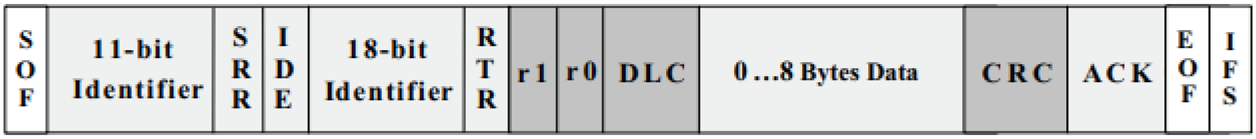

Figure 3. Extended CAN: 29-Bit Identifier

❖ **CAN Error Handling:-**

- **Cyclic Redundancy Check (CRC):**

○ CRC is a method used to detect errors in transmitted data. It involves performing a mathematical calculation on the transmitted data to generate a checksum, which is then compared with a checksum received by the recipient. If the two checksums do not match, it indicates that the data has been corrupted during transmission.

- **Acknowledgment (ACK) bit:**

○ In CAN, each message sent by a node requires acknowledgment from at least one other node to confirm successful transmission. This acknowledgment bit indicates whether the message was received correctly. If a node doesn't receive an acknowledgment, it can attempt to retransmit the message.

- **Error Frames:**

○ Error frames are special CAN messages used to indicate various types of errors that may occur on the bus. There are several types of error frames, such as:
  - Active Error Frame: Indicates errors that are currently occurring on the bus.

- Passive Error Frame: Indicates errors that have occurred but have not yet caused the node to go into an error state.
- Overload Frame: Used to postpone transmission during heavy bus traffic.

Error Counters:

- CAN nodes maintain error counters to keep track of the number of errors that occur during communication. These counters help in identifying faulty nodes or segments of the CAN bus network. There are two main types of error counters:

  - Transmit Error Counter (TEC): Counts errors that occur during message transmission.
  - Receive Error Counter (REC): Counts errors detected during message reception.

Bus Guardians:

- Bus guardians are mechanisms implemented in CAN nodes to monitor the integrity of the CAN bus. They ensure that the bus remains in a consistent state and take corrective actions if errors are detected. Bus guardians may include features such as:
  - Bus-off Recovery: Automatically recovering from a bus-off state where a node has been disabled due to excessive errors.
  - Error Recovery Mechanisms: Implementing strategies to recover from errors and maintain communication integrity.

❖ **CAN Transceivers:-**

CAN transceivers are devices that interface between the CAN controller and the physical bus. They provide electrical isolation and signal conversion. Key features of CAN transceivers include:

- **Differential Signal Transmission:** CAN transceivers utilize a differential signaling scheme, where data is transmitted as the voltage difference between two signal lines (CAN_H and CAN_L). This method offers noise immunity and robust communication, especially in noisy industrial environments.

- **Common-Mode Noise Rejection:** Differential signaling inherently provides common-mode noise rejection, which means that noise present on both signal lines is effectively canceled out. This feature helps ensure reliable communication in the presence of electromagnetic interference (EMI) and other noise sources.

- **Controlled Driver Output Transition Times:** CAN transceivers regulate the timing of signal transitions to meet the requirements of the CAN protocol. This controlled transition helps maintain signal integrity and minimize the risk of errors during data transmission.

- **Low-Current Bus Monitor:** Some CAN transceivers include a low-current bus monitoring mode, which allows them to passively monitor the bus without actively transmitting data. This feature is useful for diagnostic purposes and for detecting errors or anomalies on the bus without disrupting normal operation.

- **Standby and Sleep Modes:** Transceivers often include power-saving modes such as standby or sleep modes, which reduce power consumption when the device is not actively transmitting or receiving data. These modes help improve energy efficiency in battery-powered or low-power applications.

- **Bus Pin Short-Circuit Protection:** CAN transceivers typically incorporate protection mechanisms to safeguard against faults such as bus pin short circuits. This protection helps prevent damage to the transceiver and ensures the integrity of the overall CAN network.

❖ Importance of CAN

CAN is an important communication protocol for several reasons:

- **Reliability:** CAN is renowned for its high reliability, particularly in demanding environments like automotive, industrial automation, and aerospace. It achieves this through built-in error detection and error handling mechanisms. CAN uses a cyclic redundancy check (CRC) to verify the integrity of transmitted data packets. Additionally, it employs message acknowledgment and retransmission strategies to ensure that data is reliably delivered even in the presence of errors or faults on the bus.
- **Real-time Performance:** CAN's deterministic behavior makes it well-suited for real-time applications where timely and predictable communication is essential. CAN utilizes a priority-based arbitration mechanism, where messages with lower identifier values have higher priority. This ensures that critical messages can be transmitted without delay, enabling timely responses and coordination among network nodes. As a result, CAN is widely used in applications such as automotive control systems, where precise timing is crucial for safety and performance.
- **Noise Immunity:** CAN's differential signaling scheme and robust error detection mechanisms make it highly immune to electrical noise and interference. By transmitting data as the voltage difference between two signal lines (CAN_H and CAN_L), CAN effectively cancels out common-mode noise, ensuring reliable communication even in noisy industrial environments. This noise immunity is essential for maintaining communication integrity and preventing data corruption, especially in applications where electromagnetic interference (EMI) is prevalent.
- **Scalability:** CAN networks offer scalability in terms of the number of nodes they can support on a single bus. While the CAN specification allows for up to 128 nodes on a single bus, practical limitations such as cable length, baud rate, and network topology may impose constraints on network size. Nonetheless, CAN's ability to support multiple nodes on a single bus makes it suitable for a wide range of applications, from small-scale embedded systems to large-scale industrial networks.
- **Cost-effectiveness:** One of the key advantages of CAN technology is its cost-effectiveness. CAN transceivers and controllers are relatively inexpensive compared to other communication protocols, making CAN an attractive choice for cost-sensitive applications. Additionally, the widespread adoption of CAN in automotive and industrial sectors has led to economies of scale, further driving

down the cost of CAN components. This affordability, combined with its reliability and versatility, makes CAN a popular choice for various applications where cost is a significant consideration.

❖ Attacks, Faults, and Challenges

- **Attacks**

CAN systems are vulnerable to various attacks, including:

1) **Message Spoofing:** Attackers can send false messages onto the CAN bus, pretending to be legitimate nodes. This can lead to erroneous behavior in the system, potentially causing safety hazards or data corruption.
2) **Message Replay:** Attackers intercept and retransmit previously captured messages onto the bus, potentially causing confusion or disruption in the system's operation.
3) **Bus Flooding:** Attackers flood the bus with a high volume of messages, overwhelming the network bandwidth and causing communication delays or denial of service to legitimate nodes.
4) **Denial of Service (DoS):** Attackers intentionally disrupt the normal operation of the CAN network by flooding it with invalid messages, causing legitimate messages to be delayed or lost, thereby disrupting the functionality of the system.

- **Faults**

Common CAN faults include:

- **Bus Shorts:** Short circuits on the CAN bus can cause communication failures between nodes or even damage to the transceivers and other components connected to the bus.
- **Ground Faults:** Faulty ground connections can disrupt the electrical continuity of the CAN network, leading to communication errors or complete system failure.
- **Open Circuits:** Breaks in the wiring or connectors can create open circuits, preventing data transmission between nodes and resulting in communication failures.
- **Noise Interference:** External electromagnetic interference or electromagnetic compatibility (EMC) issues can introduce noise into the CAN bus, potentially corrupting data transmission and causing errors.
- **ESD Damage:** Electrostatic discharge (ESD) events can damage CAN transceivers or other electronic components connected to the bus, leading to malfunctions or permanent failures.

❖ Challenges

- Network Management: Proper configuration, monitoring, and maintenance of CAN networks are essential to ensure reliable operation. This includes addressing issues such as node addressing, message prioritization, and network topology management.
- Security: Protecting CAN systems from unauthorized access and malicious attacks is crucial, especially in applications where safety and security are critical, such as automotive and industrial control systems.
- Scalability: CAN networks have inherent limitations in terms of scalability due to the distributed nature of the arbitration mechanism and the finite bandwidth of the bus. As the number of nodes or the complexity of

the network increases, managing arbitration and ensuring timely message delivery becomes more challenging.

❖ CAN Applications

In addition to automotive applications, CAN is also used in a wide range of industrial and medical equipment, including:

- **Industrial Automation:** CAN is extensively used in industrial automation for communication between various components such as sensors, actuators, controllers, and human-machine interfaces (HMIs). It enables real-time monitoring and control of industrial processes, facilitating efficient operation and automation of manufacturing plants, assembly lines, and industrial machinery.

- **Building Automation:** In building automation systems, CAN is employed to interconnect devices like temperature sensors, lighting controls, HVAC (heating, ventilation, and air conditioning) systems, security systems, and energy management systems. CAN enables seamless communication and integration of these devices, allowing for centralized control, energy efficiency, and enhanced occupant comfort and safety in buildings.

- **Medical Devices:** CAN is used in various medical devices and equipment, including patient monitoring systems, infusion pumps, diagnostic instruments, and imaging devices. It provides reliable communication between different subsystems within medical equipment, ensuring accurate data transfer, synchronization of operations, and real-time feedback for healthcare professionals.

- **Aerospace Systems:** In aerospace applications, CAN is utilized for communication between avionics systems, including flight control systems, engine control units, navigation systems, and cockpit displays. CAN enables robust and fault-tolerant communication in harsh aerospace environments, contributing to the safety, reliability, and performance of aircraft and spacecraft systems.

- **Marine Electronics:** CAN is employed in marine electronics for communication between navigation systems, propulsion controls, monitoring systems, and other onboard equipment. It facilitates data exchange and integration of various marine subsystems, supporting navigation, propulsion, monitoring, and control functions in ships, boats, and marine vessels.

- **Robotics:** CAN technology plays a crucial role in robotic systems for communication between sensors, actuators, motor controllers, and central processing units (CPUs). It enables precise control, coordination, and synchronization of robotic movements and operations, enhancing the performance, efficiency, and versatility of industrial robots, autonomous vehicles, robotic arms, and other robotic platforms.

❖ CAN Features and Benefits

- **Reliability**: CAN's error-checking mechanisms, such as CRC (Cyclic Redundancy Check), ensure reliable data transmission even in noisy environments.
- **Real-time Performance:** CAN's deterministic arbitration mechanism allows for timely message delivery, enabling real-time control and monitoring.
- **Noise Immunity:** CAN's differential signaling and balanced line topology provide robust noise immunity, making it suitable for use in electromagnetically noisy environments.
- **Scalability:** CAN networks can support multiple nodes (up to 128 in theory), allowing for the expansion of networks as needed.
- **Cost-effectiveness:** CAN transceivers and controllers are relatively inexpensive compared to other communication protocols, making CAN a cost-effective solution for various applications.

❖ CAN Network Design Considerations

When designing a CAN network, several factors should be considered:

- **Bus Topology:** CAN networks commonly use a linear or star topology, although hybrid topologies are also possible.
- **Cable Type:** Twisted-pair cables with a characteristic impedance of 120 ohms are recommended to minimize signal degradation and reflections.
- **Termination:** Proper termination of the CAN bus with 120-ohm resistors at both ends is essential to prevent signal reflections and ensure signal integrity.
- **Node Configuration:** Each node on the CAN network must have a unique identifier (CAN ID) to facilitate message filtering and routing.
- **Message Prioritization:** Messages with higher priority should be assigned lower CAN IDs to ensure they are transmitted with minimal delay.

❖ CAN Security

CAN systems can be vulnerable to various security attacks. Common security measures for CAN networks include:

- **Authentication:** Verifying the identity of nodes before allowing them to communicate helps prevent unauthorized access and spoofing attacks.
- **Encryption:** Encrypting CAN messages can protect sensitive data from eavesdropping and tampering.
- **Message Integrity Checks:** Using checksums or cryptographic hashing to verify the integrity of CAN messages helps detect tampering or data corruption.
- **Intrusion Detection:** Monitoring the CAN network for abnormal behavior or unauthorized access can help detect and mitigate security threats in real-time.

❖ CAN Standards

The CAN protocol is defined by several international standards, including:

- ISO 11898-1: Physical layer
- ISO 11898-2: Data link layer
- ISO 11898-3: Network layer
- ISO 11898-4: Transport layer
- ISO 11898-5: Application layer

❖ Applications of CAN

CAN is used in a wide range of applications, including:

- **Automotive:** Used for engine control, transmission control, airbag deployment, anti-lock braking systems (ABS), and more.
- **Industrial Automation:** Employed in programmable logic controllers (PLCs), distributed control systems (DCSs), supervisory control and data acquisition (SCADA) systems, and other industrial automation applications.
- **Medical Devices:** Utilized in patient monitoring equipment, infusion pumps, medical imaging devices, and other medical devices requiring reliable communication and control.
- **Aerospace Systems:** Found in flight control systems, navigation systems, engine control units (ECUs), and avionics systems for aircraft and spacecraft.
- **Marine Electronics:** Used for engine control, navigation systems, monitoring systems, and communication systems in marine vessels.
- **Robotics:** Employed in motion control systems, sensor data acquisition, robotic arms, autonomous vehicles, and other robotic applications requiring real-time communication and control.

❖ Conclusion

- CAN is a highly reliable and robust communication protocol that is widely used in automotive and industrial applications. Its features, such as bit-wise arbitration, error handling, and differential signal transmission, make it suitable for harsh environments. However, CAN systems are not immune to attacks and faults, and proper security and network management practices are essential to ensure their integrity and availability.