Controller Area Network Protocol For Vehicle System

1st Sheikh Muhammad Adib Bin Sh Abu Bakar
Hochshule Hamm-Lippstadt
B.Eng. Electronic Engineering
Lippstadt, Germany
sheikh-muhammad-adib.bin-sh-abu-bakar@stud.hshl.de

2nd Zafirul Izzat Bin Mohamad Zaidi
Hochshule Hamm-Lippstadt
B.Eng. Electronic Engineering
Lippstadt, Germany
zafirul-izzat-bin.mohamad-zaidi@stud.hshl.de

3rd Muhammad Farid Izwan Bin Mohamad Shabri
Hochshule Hamm-Lippstadt
B.Eng. Electronic Engineering
Lippstadt, Germany
muhammad-farid-izwan.bin-mohamad-shabri@stud.hshl.de

***Abstract*—**

***Index Terms*—real time system, resource, protocol**

I. Introduction

The rising power and cost effectiveness of electronic devices has affected all aspects of human endeavour during the last several decades. This also not exceptional to industrial control systems which are always improvise progressively. Control of industrial and process facilities was first done mechanically in the early 20th century, either manually with analogue devices or through the use of hydraulic controllers. Mechanical control systems were superseded by electronic control loops that used transducers, relays, and hard-wired control circuits as discrete electronics became more prevalent now a days. These systems were enormous and took up a lot of area, frequently necessitating many kilometres of wire, starting from one point to another point, as example the connection from the field itself to the control circuits. The functionality of many analogue control loops may be reproduced by a single digital controller thanks to the introduction of integrated circuits and microprocessors.

We know that at the beginning phase, a digital computer was for the first time being applied as a digital controller. As time goes by, Digital controllers gradually replaced analogue control, however connection with the field was still done using analogue signals. The transition to digital systems necessitated the development of new communication protocols for the field as well as between controllers. Fieldbus protocols are the most frequent name for these communication protocols. Recently, digital control systems began to include networking at all levels of industrial control, as well as the interconnection of commercial and industrial equipment utilizing Ethernet standards. This has resulted in a networking environment that, on the surface, looks to be comparable to traditional networks but has fundamentally different requirements.

An industrial communication network is the foundation of any automation system design since it provides a strong method of data interchange, data controllability, and the flexibility to link numerous devices. Over the last decade, the deployment of proprietary digital communication networks in industries has resulted in improved end-to-end digital signal correctness and integrity. With the help of real-time communication among machines and control centers, industrial communication networks power smart manufacturing scenarios. They guarantee that supply chain abnormalities may be evaluated and avoided by monitoring procedures and operations. Predictive maintenance is an excellent illustration of how the Industrial Internet of Things may improve efficiency and cost optimization through connection and data analytics. For example, any machine with sensors may collect vital information about its state and interactions with other equipment and operators. The network transmits this data to processing centers, where it is compared to historical and statistical data to find trends, recurrences, and exceptions. They can also build links between certain inputs and any breakdowns or inefficiencies. Intelligent gateways provide smooth interaction between several communication protocols that are structured in separate subnetworks.

This paper serves as an introduction to industrial communication networks. Industrial networking concerns itself with the implementation of communications protocols between field equipment, digital controllers, various software suites and also to external systems. To assist the reader, the communication network that is widely used specially in industrial field will be explain generally so that the reader can have humongous imagination and deep understanding regarding this topic. The chosen communication network which is CAN will be thoroughly discussed and contrast with those other networks. Many aspects of the operation and philosophy of industrial

Identify applicable funding agency here. If none, delete this.

networks has evolved over a significant period of time and as such a history of the field is provided. The operation of modern control networks is examined and some popular protocols are described

II. Type of communication

A. wireless network

1) bluetooth:

2) near field communication:

3) wifi:

B. wired network

1) ethernet:

2) I2C:

3) UART:

III. Problem

Wired communication protocol always being used in many application because of its reliability in term of the connection and it efficiency especially in transferring long sequence of data.

Today, there is many protocol that support weird communication such as UART, SPI and I2C as written in the previous subtopic. each protocol have their on advantage to solve many problem in a curtain application domain. For instance, SPI support many salve to be controlled by one master that almost impossible to be implemented using UART. This kind of protocol use atleast 4 wire to connect between one master and one slave. By using this protocol, increasing number of slave means that the used number of wire for the communication also will be increased. This is a huge problem for a system that use a lot of distinct sensors and actuators smartphone, computer and machine in production line. Here is where the I2C play a big role because with the I2C, only two wire are need for the communication between a master and their slaves regardless of the number of the salve.

Another problem that arrive when using I2C in a more rugged application is their reliability and efficiency. Imagine a main controller for a car system that is located at the front of ther car want to communicate withe the brake lamp at the back of the car, where the length of the used wire could be 5 meter.. Since the I2C protocol only support for low voltage application, with that long, it is possible that output from the controller will not be well received by the brake lamp system. If the output is well receive it cloud be very slow becouse with that long, we only allowed to use very low frequency to make the communication works. But to make it work is not only the purpose. In case on emergency brake, it is important for the car behind to that this car a breaking through the brake lamp. If the signal is to slow this can cause a catastrophic event.

To solve this problem which is to reduce the number of used wire, reliable and efficient communication protocol for rugged application, Controller Area Network protocol or CAN protocol should be used.

We will explain more bout this protocol in the next subtopic followed by the application to make user more understand and able to implement this kind of protocol.

IV. CAN Communication Protocol

The controller area network (CAN) is a highly integrated system using serial bus and communications protocol to connect intelligent devices for real-time control applications. Control Area Network use a vehicle bus standard that allows communication such as, sending message, data or information between microcontrollers and other devices to happen. CAN is able to operate at data rates of up to 1 megabits per second over a possible line length of up to several kilometres, and has excellent error detection and confinement capabilities. Control Area Network which is also well-known as CAN Communication was introduced by Robert Bosch GmbH in 1983. CAN is purposely created to make automobile industry system more reliable and efficient but it is also widely used in industrial automation and other areas.

A. The CAN Standard

CAN is a serial communications bus established by the International Organization for Standardization (ISO) that was developed for the automotive industry to replace the complex wiring harness with a two-wire bus. High immunity to electrical interference is required, as well as the ability to self-diagnose and rectify data mistakes, according to the specification. Because of these characteristics, CAN is widely used in a range of industries, including building automation, medical, and manufacturing.

The CAN communications protocol, ISO-11898: 2003, specifies how data is transmitted between devices on a network and follows the Open Systems Interconnection (OSI) paradigm, which is divided into layers. The physical layer of the model defines the actual communication between devices connected by the physical medium.

B. Standard CAN

The CAN communication protocol is a carrier-sense, multiple-access protocol (CSMA/CD+AMP) that includes collision detection and message priority arbitration. Each node on a bus must wait for a certain duration of idleness before attempting to send a message, according to CSMA. CD+AMP denotes that collisions are resolved using bit-wise arbitration, with each message's priority preprogrammed in the identification field. Bus access is always granted to the identification with the highest priority. That example, because the last logichigh in the identification has the highest priority, it continues to transmit. An arbitrating node knows if it placed the logic-high bit on the bus because every node on the bus participates in writing every bit "as it is written."

1) The Bit Fields of Standard CAN: The standard CAN frame consists of the following bits:

SOF- Start of Frame. The message starts from this point. Identifier: It decides the priority of the message. Lower the binary value, higher is the priority. It is 11 bit. RTR– Remote Transmission Request. It is dominant when information is required from another node. Each node receives the request, but only that node whose identifier matches that of the message is the required node. Each node receives the response as well.z

IDE– Single Identification Extension. If it is dominant, it means a standard CAN identifier with no extension is being transmitted. R0– reserved bit. DLC– Data Length Code. It defines the length of the data being sent. It is 4 bit Data– Up to 64 bit of data can be transmitted. CRC– Cyclic Redundancy Check. It contains the checksum (number of bits transmitted) of the preceding application data for error detection. ACK– Acknowledge. It is for 2 bit. It is dominant if an accurate message is received. EOF– end of the frame. It marks the end of can frame and disables bit stuffing. IFS– Inter Frame Space. It contains the time required by the controller to move a correctly received frame to its proper position.

C. A CAN Message

1) Arbitration: The opposing logic state between the bus and the driver input and receiver output is a basic CAN property, as shown in Figure 4. A logic high is normally linked with a one, and a logic low with a zero, however this is not the case on a CAN bus. This is why the driver input and receiver output pins of TI CAN transceivers are internally passively pushed high, such that the device defaults to a recessive bus state on all input and output pins in the absence of any input.

Bus access is based on events and occurs at random. If two nodes try to occupy the bus at the same time, nondestructive bit-wise arbitration is used to provide access. Nondestructive means that the node that wins arbitration keeps sending the message without it being deleted or corrupted by another node.

A feature of CAN that makes it particularly appealing for application in a real-time control environment is the allocation of priority to messages in the identification. The higher the priority, the smaller the binary message identifying number. Because it keeps the bus dominant the longest, a message with an identification made entirely of zeros is the highest priority message on a network. As a result, if two nodes start transmitting at the same time, the node that sends a zero (dominant) as the last identifying bit while the others send a one (recessive) holds control of the CAN bus and continues to complete its message. On a CAN bus, a dominant bit always overwrites a recessive bit.

2) Message Types: There are four different message types (or frames) that can be transmitted on a CAN system as below:

1) The Data Frame 2) The Remote Frame 3) The Error Frame 4) The Overload Frame

3) A Valid Frame: When the last bit of a message's terminating EOF field is received in the error-free recessive state, the message is considered error-free. The transmitter repeats a broadcast if a dominating bit in the EOF field is present.

4) Error Checking and Fault Confinement: The abundance of error-checking mechanisms in CAN contributes to its robustness. The CAN protocol has five error-checking methods: three at the message level and two at the bit level. If a message fails to pass any of these error detection mechanisms, it is not accepted, and the receiving node generates an error frame. This compels the transmitting node to relay the message several times until it is appropriately received. If a malfunctioning node hangs up a bus by repeatedly repeating an error, its controller disables its transmit capacity if an error limit is reached.

1) Message Level

A form check is performed at the message level. This check examines the message for fields that must always be recessive bits. An error is generated if a dominating bit is discovered. The SOF, EOF, ACK delimiter, and CRC delimiter bits are all examined.

2) Bit Level

Each bit transferred is monitored at the bit level by the message's transmitter. An error is caused if a data bit (not an arbitration bit) is written onto the bus and its opposite is read. The message identity field, which is used for arbitration, and the acknowledge slot, which requires a recessive bit to be replaced by a dominant bit, are the only exceptions.

D. The CAN Bus

The CAN standard establishes a communication network that connects all bus nodes and allows them to communicate with one another. A central control node may or may not exist, and nodes may be added at any moment, even while the network is operational (hot-plugging)

1) CAN Transceiver Features: 1) 3.3V Supply Voltage
2) ESD Protection
3)Common- Mode Voltage Operating Range
4) Common-Mode Noise Rejection
5) Controlled Driver Output Transistion Times
6) Low-Current Bus Monitor, Standby and Sleep Modes
7) Low-Current Bus Monitor, Standby and Sleep Modes
8) Thermal Shutdown Protection
9) Bus Input Impedance
10) Glitch-Free Power Up and Power Down
11) Unpowered Node Protection
12) Reference Voltage
13) V-Split
14) Loopback
15) Autobaud Loopback

2) CAN Transceiver Selection Guide :

V. Application of CAN Protocol

A. Scenario

B. Application Model

C. Implementation

1) Hardware:

2) Software:

VI. State Of The Art

VII. Discussion

VIII. Conclusion

Acknowledgment

We, Sheikh Muhammad Adib and .. and ... thanks..

References

[1] G. C. Buttazzo, "Hard real-time computing systems: Predictable scheduling algorithms and applications". New York: Springer, 2011.