Wireless replacement for cables in CAN Network

Derek Sum, Kvaser AB

Cable harnessing is always a headache in any system design. Although CAN Bus implementation is a cable friendly solution compared to other communication protocols used in the industrial space, in some applications - especially demanding areas such as Robotic Systems and Heavy Duty Machinery - cable wearing is a well-known un-resolved issue.

Another complicating factor is that electronically controlled features are becoming more advanced and their quantity increases year on year. As a result, more nodes and network gateways appear in the system and complex cable harnessing and routing mechanisms are required.

The idea of replacing CAN cabling with a wireless solution is not new. Indeed, many similar CAN-Wireless gateway products with a variety of wireless solutions can be found in the market. Such a solution results in the problem of merging two different types of communication protocol (CAN and Wireless). From a system design point of view, how to implement wireless communication into CAN is a challenge. Issues such as data throughput, latency and data security need to be addressed.

About wireless communication in general

In wireless communication, the license free ISM (Industrial, Scientific and Medical) Bands such as 2.4 Ghz, 915 Mhz, and 868 MHz are widely chosen for industrial applications in a point to point master and slave (or multi-slave) configuration. In most cases, frequency hopping spread spectrum is being used to provide communication quality and minimize the chance of interference by another device using the same channel. Most of the technology providers of such radio communication have their own proprietary radio protocol. A typical example for such a solution is a Truck and a Trailer where an expensive cable is used to link the two vehicles.

Wireless cable replacement over a CAN Network.

At the physical layer level, the whole implementation should be as simple as making a cut through the CAN bus and connecting a radio transceiver module at each end so that the transceiver modules form a wireless gateway.

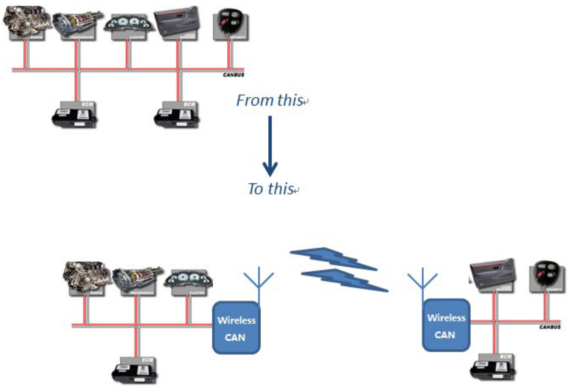

Figure 1: Idea of CAN Network with wireless implementation as cable replacement.

With a wireless implementation, the system is turned into a dual physical network. However, this means that CAN's arbitration feature is lost, as well as an important part of the error checking. There might be arbitration at the transmitting side before the messages are accepted by the radio gateway and the message may be involved in arbitration when the receiving gateway is transmitting the message. The best way to avoid unexpected delays due to arbitration is to schedule the messages at both sides so arbitration does not take place during normal conditions. The error checking also takes place independently on both sides, so it is necessary to understand that a message can be accepted on the transmitting side but not on the receiving side. This error case has to be handled by the Higher Layer Protocol. Therefore, we are expecting the concept of original system design to be changed or adapted.

Wireless CAN cable hardware

The basic hardware implementation should consist of both a CAN Transceiver and Radio Transceiver in which the CAN Message will be buffered and carried in the payload of a Radio Frame. Filtering is required to optimize Radio Bandwidth/Data throughput.

The MCU should able to handle the compression and extraction of CAN data from the radio packet with a good size of FIFO buffering any burst of data.

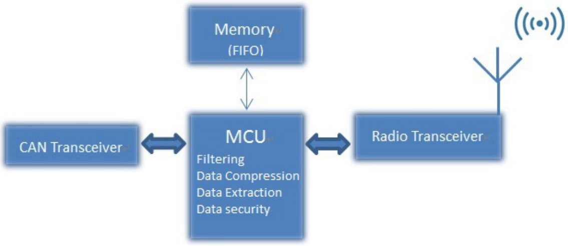

Figure 2: Concept of wireless CAN cable hardware.

Why not Wi-Fi or Bluetooth?

There are many radio protocol standards in the industrial space such as Wi-Fi and Bluetooth.

Wi-Fi and Bluetooth are dominant within the consumer market. However, when dealing with control systems, a propriety radio protocol is always preferred.

One issue for Bluetooth is range as it is typically less than 10 meters in most applications. As a cable replacement, this may not be enough for a short physical length CAN network requiring a 125K baud rate.

Initially, it seems that Wi-Fi's data throughput and range is far better than Bluetooth. However, the latency is not controllable and can be as much as 100ms. That might not be suitable for cable replacement in a real-time CAN-based control system.

It is necessary to point out that both Bluetooth and Wi-Fi, plus their related security encryption mechanisms, are well-known radio protocols in the control system market. For this reason, they could be far easier to hack than a propriety radio protocol.

Data throughput and bandwidth between Radio and CAN protocol

Data throughput is a major consideration for any Wireless implementation within a CAN System. In the radio frequency range between 2.4 GHz and 2.480 GHz, 1 to 2Mhz bandwidths is widely used by industrial applications for Frequency Hopping.

Although the Radio Bandwidth seems to suit the CAN Bus Protocol, the possible data throughput for the application (in this case CAN Messages as Radio packet's payload) may not be enough. This is because of the overhead from the radio mechanism. The actual application throughput will be roughly from 20kbps to as high as 128kbps according to similar products currently on the market. Actual Data Throughput is dependent on how their proprietary radio protocol has been implemented.

With such proprietary protocols, the handshaking method over TX and RX, as well as the radio packet overhead, can be limited in order to support higher CAN data throughput. Such overhead also contains important information to aid the system designer of a CAN System.

Taking the example of a well-designed 30 % - 40 % busload CAN system, 128 kbps is enough for a lower speed CAN network such as a 125K to 250K CAN Baud rate.

With a medium to high CAN Baud rate such as 500 K to 1M, proper filtering has to be in place in order to optimize the CAN data throughput over the radio link.

The data throughput for CAN over Radio Protocol will be independent of CAN Baud rate. Indeed, a CAN System Designer has to understand the capacity of the radio protocol should a wireless solution be chosen.

Real time performance and latency

In the wireless environment, latency is inevitable due to factors such as hand shaking of the TX message and Acknowledgement, as well as external interference causing re-transmission.

In regular practice, most radio protocols quietly handle error detection and retransmit at the expense of throughput and variable latency.

Indeed, there are couples of factors that affect latency:

1. The time a radio packet waits before being transmitted depends upon the internal buffer size as well as cross traffic (if the protocol is working as half duplex)
2. If there is any error causing re-transmission of the packet?
3. The time to receive an acknowledgment after successful transmission depends on the performance of the radio device from other side

CAN is well-known as a protocol for real time prioritized communication systems. In most cases, it would be hard for a CAN control system to tolerate delays caused by wireless cable replacement without knowing the possible latency over radio link.

A good wireless solution should have a known maximum latency within a successful radio packet transmission. A controllable/known latency is a key for scheduling the CAN message within a system. Hence, any unknown latency could possibly affect the actual outcome of the CAN System behavior.

Some wireless products currently on the market could add up to 30ms of latency over the radio packet. However, with a well-designed proprietary radio protocol, the latency could be minimized down to the region of 2ms for a successfully transmitted radio packet.

An additional factor to bear in mind is that a known maximum latency and data throughput have a critical influence over how the buffer stack should be setup for incoming CAN Messages. The reason for this will be explained later in the article.

Diagnostic over wireless link

There are two philosophies to consider when employing Diagnostic services over a wireless link when it is used as a cable replacement:

- Higher Layer Protocol – i.e. Diagnostic Services Protocol for the CAN System.
- Self-Diagnostic information on the Wireless link.

Diagnostic Protocol service is widely used in CAN applications such as J1939 and ISO 14229.
Very complex Transport Protocols such as ISO 15765 require precise timing control over multiple consecutive CAN Message transmissions. Therefore, as mentioned in previously, a known/controllable latency as well as good buffering are important.

A controllable latency over the radio packet allows the application layer to manage the timing according to the actual capability of the physical layer.

Good buffering will ensure the correct handling of any burst message, especially in multi-frame transmission of the Transport Protocol. There is only a thin line between the maximum latency and data loss.

The rule of thumb is that if the message burst exceeds the capacity of the buffer times latency, there will be message loss.

For self-diagnostic information, the Wireless link should provide the ability to self-check information such as:

- Radio packet information
- Radio signal quality
- Any history of error occurrence
- Any re-transmission of the packet

One way of looking at this is as a cable replacement using Wireless technology. On the other hand, this is also an individual

ECU within a system. Therefore, instead of viewing it purely as a data carrier, the wireless link's self-information and status should be considered as part of the system design.

Possible wireless range for CAN communication

The possible range is limited by four elements: radio frequency power, receiver sensitivity, antenna type and the environment surrounding the wireless implementation.

The effective possible range is determined is often anticipated to be determined by the actual radio frequency power. This is measured in Watt on a logarithmic scale i.e. in, decibels (dB). The power density is proportional to the inverse square of the distance.

Table 1: Milli watt and decibels scale

Milli watt (mW)	Decibels (dBm)
1 mW	0 dBm
2 mW	3 dBm
4 mW	6 dBm
10 mW	10 dBm
100 mW	20 dBm
1 mW	30 dBm

It should be pointed out that range can never be guaranteed for a radio connection. Range is dependent not only on the output power but also on the antenna diagram, the quality of the antennas, physical objects in the wave path causing radio shadows, reflections and absorptions, plus weather conditions. Sensitivity to these reducing factors depends on the actual wavelength. Only output power can be specified with accuracy. Thus any wireless connection should better be verified by practical tests on site.

There are some ways to enhance the radio range:

1. Use of different frequency bands
   The simple rule is that frequency band is proportional to the available bandwidth but inversely to the effective distance and propagation through obstacles.

2. Use of a power amplifier to increase the dBm level of the transmitter. A half watt of power increase will result in a 10dBm gain on the transmitter.

3. Use of advanced receiving antennas. By including a directional antenna on the receiver side, n such a case, the receiver sensitivity will be boosted. There are several other alternatives, e.g. Diversity antennas, array antennas, rake antennas, etc.

In regular practice, the ISM band is widely used for 2 solution types:

1. 900 MHz for longer range, lower bandwidth
2. 2.4 GHz for higher bandwidth, lower range

From an application point of view, in most cases, 2.4 GHz is still the preferred choice for wireless cable replacement in a CAN Bus system. This is because it offers:

- more bandwidth (i.e. data throughput)
- a worldwide frequency band for use in multiple countries
- smaller antenna implementation.

The 900 MHz range is chosen because:

- System implementation requires a larger range e.g. mining.
- Remote movable device/system in large area.
- Government restriction of the use of a higher frequency band in certain heavy duty industrial areas.

Although the 2.4 GHz frequency band has a shorter range, with the correct antenna approach, it could still be effective at a 300-400m distance.

For most CAN physical layer implementations, there is a recommended cable length due to propagation delays i.e. a 500K network recommends 100 meters of cable and 250 meters on a 250K network. So, in most cases the range of the radio link will not be an issue as the implementation is a cable replacement but the system integrator may face problems with data throughput and real-time performance.

Error handling of CAN over wireless

The CAN Bus protocol has a state of the art complete error handling mechanism.

However, in a wireless implementation, the physical network that connects all the nodes together will be split into two networks, with each network having its own error handling mechanism.

This means that some original communication behavior will be hidden. For example, figure 3 shows that the original network has been split into Network 1a and Network 1b. While the node in network 1a is broadcasting Message A for the node in network 1b, the acknowledgement in network 1b will not been seen back in network 1a.

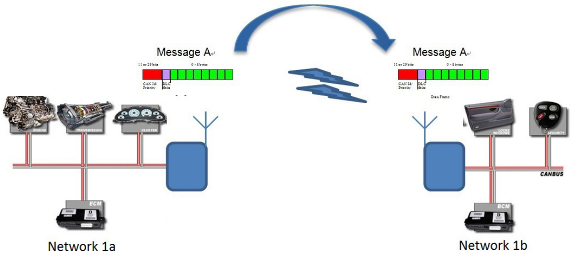

Figure 3: Concept of wireless CAN cable hardware.

As the Wireless Radio Protocol has its own error handling mechanisms such as re-transmission, acknowledgement, CRC checks … etc., it effectively divides the whole system into three sets of active communication protocol i.e. Network 1a, Wireless Cable replacement and Network 1b as Figure 3 shows.

However, the status as well as any error appearance on a wireless network could be useful to the CAN Network itself i.e. the Wireless Cable replacement also acts as an individual CAN node and reports its status.

Such a mechanism could be a huge benefit for the safety of a control system. For example, if the Wireless cable replacement is able to broadcast its re-transmission rate and RSSI (received signal strength indication) to the CAN Network, the whole system could enter into safe mode when the re-transmission rate is too high and RSSI is lower than an accepted level.

Vice versa, a pair of wireless cable replacements could also monitor the CAN Network and thus report abnormal CAN activities to the other side over the radio link.

Such an implementation is totally feasible with current technology and should improve the safety and reliability of the combined communication protocols.

Data consistency and security

The advantage of a traditional wired CAN network is that any kind of intrusion has to be made by physical appearance. Thus taking CAN applications in Automotive as an example, the security of the CAN network is ensured by seed and key access through the transport protocol. Only a valid security key code is allowed to access the proprietary memory of the ECU.

A wireless network requires a different approach, as it exposes the system to greater access through the air.

Common radio packet practice includes identification methods such as pairing Radio ID, identification of a transmitter or receiver, packet sequence/serial number, Data Payload as well as CRC checksum.

With that information available in the air, there are some potential risks with a wireless network:

1. Denial of Service:
   The control system's wireless communication link is intruded and services are terminated.
2. Manipulation and replay.
   Intruder attacks the system acting as the control signal and manipulates the system in an abnormal way.
3. Information leakage:
   Hacker is able to sniff the information.

In general, many type of security methods can be added to those scenarios to protect the system from being intruded such as:

- Additional Authentication Key
- Encrypting the payload data
- Additional Addressing on top of Radio Pairing ID

However, as mentioned previously, the real time performance as well as data throughput are a major concern when sending CAN data over a wireless link. During the implementation, some of the security methods could possibly:

- Reduce the payload capacity
- Prolong the latency

Conclusion

In conclusion, a wireless CAN cable replacement will bring advantages over cable harnessing.
However, we believe that such technology demands more than just a cable replacement, especially as the system design will turn from a single CAN network into a system with two CAN networks connected via a wireless gateway. Proper attention needs to be paid in order to fully utilize the properties of a Wireless CAN cable:

- A propriety radio protocol with Controllable/Measurable latency over the radio packet
- A good size of internal buffer that takes account of the latency
- Wireless link self-information/status need to be available for CAN System use (or system designer)
- Error handling information available between CAN protocol and Radio Protocol.
- A certain level of data security that does not affect the actual throughput or cause delay over the communication.

Derek Sum
Kvaser AB
Aminogatan 25 A
SE-43153 Mölndal
Tel.: +46-31-886344
Fax: +46-31-886343
ds@kvaser.com
www.kvaser.com

References

[1] ISO-11898-1
[2] Ten Commandments of Wireless Communications I WP-33-R2-1112-1/6 © 2009
[3] Andreas Johnsson: Bandwidth Measurements in Wired and Wireless Networks, 2005