September 2020

CAN Newsletter

Hardware + Software + Tools + Engineering

Selecting a connector system for harsh environments

Integrated security mechanisms

Why encrypt logged CAN data?

Engineering

www.can-newsletter.org

Digital I/O Module for CANopen® & CANopen FD®

PCAN-MicroMod FD DR CANopen Digital 1

The PCAN-MicroMod FD DR CANopen Digital 1 is an I/O module for operation in CANopen® and CANopen FD® networks. The modern standard CANopen FD® makes it possible to handle the ever-increasing demand for data transmission from sensors, machines, and complex production plants. The module has a CAN FD interface as well as 8 digital inputs and 8 digital outputs. The node ID and bit rates are set via rotary switches. Thus, no configuration software is required for putting the device in operation.

Specifications:

- I/O module for CANopen® and CANopen FD®
  - Communication profiles according to CiA® 301 version 4.2.0 and CiA® 1301 version 1.0.0
  - Device profile according to CiA® 401 version 3.0.0
- High-speed CAN connection (ISO 11898-2)
  - Selectable CANopen bit rates: Nominal: 20, 50, 125, 250, 500, 800, and 1000 kbit/s
  - Selectable CANopen FD bit rates: Nominal: 250, 500, 800, and 1000 kbit/s Data: 1, 2, 4, 5, 8, and 10 Mbit/s
  - Galvanic isolation against the power supply up to 500 V
- Configuration of the CAN and CAN FD bit rates as well as the node ID with rotary switches on the casing
- 2 LEDs „RUN“ and „ERROR“ for status indication according to CiA® DR 303-3
- 8 digital inputs
  - Comply with the IEC 61131-2 standard
  - Input characteristics: Type 3
  - 2 groups of 4 inputs to be used either as sourcing or sinking inputs
  - Galvanic isolation of the digital inputs 0 to 3 and 4 to 7 each up to 100 V against the module supply
- 8 digital outputs
  - 500 mA load per High-side output
  - Thermal protection per output
  - Short circuit detection per output
  - Open load detection in on-state and off-state per output
- LEDs for status indication of the digital inputs and outputs
- Connections for CAN, I/O, and power supply via 5-pole screw-terminal strips (Phoenix)
- Plastic casing (width: 22.5 mm) for mounting on a DIN rail
- Voltage supply from 8 to 36 V
- Extended operating temperature range from -40 to 85 °C

Note: CANopen® conformity has been tested and certified by the CAN in Automation (CiA) association. The device conformity test and certification for CANopen FD® is pending.

www.peak-system.com

Take a look at our website for the international sales partners. Scan the QR code on the left to open that page.

PEAK-System Technik GmbH

Otto-Roehm-Str. 69, 64293 Darmstadt, Germany
Phone: +49 6151 8173-20 - Fax: +49 6151 8173-29
E-mail: info@peak-system.com

PEAK System

Engineering

Devices

Semiconductors

Imprint

Publisher
CAN in Automation GmbH
Kontumazgarten 3
DE-90429 Nuremberg

publications@can-cia.org
www.can-cia.org

Tel.: +49-911-928819-0
Fax: +49-911-928819-79

CEO
Reiner Zitzmann

AG Nürnberg 24338

Downloads June issue:
(retrieved August 17, 2020)
3009 full magazine

Editors
Olga Fischer (of)
Cindy Weissmueller (cw)
Holger Zeltwanger (hz) *
pr@can-cia.org

Layout
Nickel Plankermann

Media consultant
Tobias Kammerer
Rosanna Rybin
Meng Xie-Buchert *

Distribution manager
Rosanna Rybin

* responsible according to the press law

New CiA specifications under development

In the last months, CiA members requested some new standardization activities. Already established is the Special Interest Group (SIG) CAN FD light. Intended is the development of a "master/slave"[1] communication system based on CAN FD for price-sensitive applications such as smart LED headlights for road vehicles. The "slave" nodes transmit only on request of the CAN FD "master". Therefore no bus arbitration is needed. Consequently, the "slave" does not support error and overload frames. They are synchronized by the FD data frames sent by the "master", which avoids the use of expensive external components.

Other CiA members desired the standardization regarding bus-line redundancy for Classical CAN and CAN FD networks. This is needed for example for maritime applications. CiA will develop a generic bus-line redundancy specification and its mapping to classic CANopen and CANopen FD.

Of course, the work on the CAN XL specification is continued. Most of the technical decisions have been taken for the CAN XL data link layer and the CAN XL physical layer. This includes also the new MICI (medium-independent CAN interface) interface between CAN XL controller and CAN XL transceiver. Technical details will be reported in the next CAN Newsletter issues.

hz

[1] This term is politically not correct; but it has been used for decades. Until the international standardization bodies agree on a harmonized substituting term, CiA writes it in quotation marks.

Table of contents

Integrated security mechanisms

Increasing networking of devices with the Internet makes the devices vulnerable and poses a risk to operational reliability. Analog Devices explains how to achieve data security at the edge of the IIoT network.

IoT (Internet of Things) system attacks are making headlines and continue to showcase the security vulnerabilities of networks, edge nodes, and gateways. A recent Mirai botnet infected over 2,5 million IoT nodes by logging into devices running telnet servers in which the default password had not been changed. [1] Mirai later was able to invoke a denial of service for servers that disrupted Internet access for a large portion of the world. The Reaper Botnet attacked over a million IoT devices by exploiting software vulnerabilities and infecting them. An Internet-connected fish tank provided the entry point into a casino's network, leading to the theft of 10 GiB of data. Smart televisions have been exploited and used for espionage and surveillance.

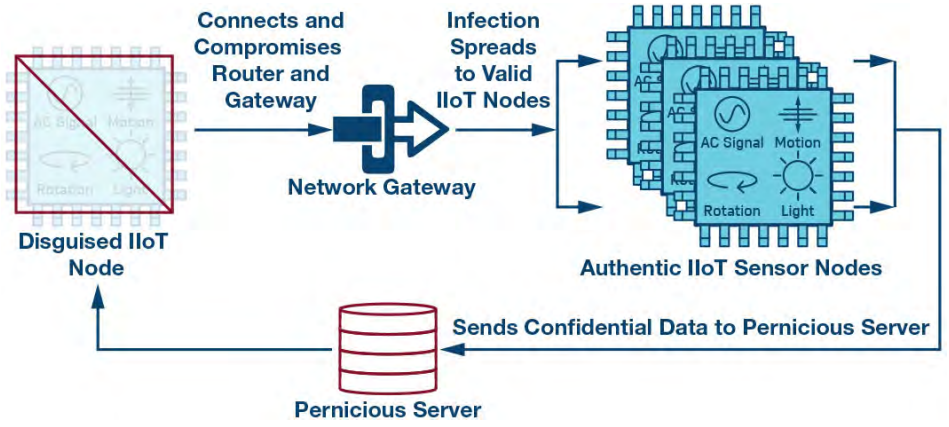


Figure 1: A spoof masquerades as a known node to a gateway (Source: Analog Devices)

Embedded sensor systems are just starting to be connected and exposed to the Internet. As part of the Industrial Internet of Things (IIoT), these sensors lack the past two decades of evolution that web servers have had in this hostile environment. Hence, the industry is witnessing many of the attacks commonly seen in the 1990s and earlier in these systems. The lifecycle of an IIoT system is often much longer than one in traditional computing. Some devices may continue operating for decades after they are deployed, and with unknown maintenance schedules.

While servers and PCs are complex enough to allow for security provisions, IIoT nodes are usually low in power consumption and processing power. This leaves a small power budget for intentional security measures. Security is largely a tradeoff, as there are development costs involved. Although IIoT may have higher costs than consumer IoT, it will still face challenges in cost for scalability. If security is ignored there are hidden impacts that will arise after products are deployed, and these costs will eventually need to be addressed.

Sensors and actuators allow IIoT devices to interact with the physical world. Cyber attacks have been mostly limited to the loss of data, although an IIoT hack allows potential entry into the physical world easier than it has in the past. Attacks now have the potential to cause physical harm. This is even more significant in IIoT, where a failure could potentially shut down or destroy a multimillion-dollar industrial process or lead to a life-threatening situation.

A connected world

IIoT devices are generally connected to some network and often the Internet. This connectivity is what exposes them the most to an attack. Similar to the realm of epidemiology, infection is spread by contact with other machines. Attack vectors exist where systems interact with the outside world. Attackers are able to interact with systems strictly due to their connected access. The first system design security question to be asked is: "Does the device really need to be connected to a network?" Connecting it to a network dramatically increases the security risk.

The best way to secure a system is to prevent it from connecting to a network or limiting it to a closed network. Many IIoT devices are connected to networks solely because they can be without much reason. Does the benefit of having the device connected to a network outweigh the security risks associated with it? In addition, any other legacy systems that interact with the Internet facing system can also be put at risk.

In many cases, an otherwise secure network and secure nodes must also interoperate with a legacy incumbent network that could be far inferior in its own security. This poses a new problem in that the weakest security risk could be outside the influence of the IIoT system. In that case, the IIoT system also needs to protect itself from within the network.

Security considerations at the node [2]:

- Confidentiality—protection from data disclosure to unauthorized people, such as from a spoof attack
- Authentication—use of digital certificates to validate the identity between two machines
- Secure boot—ROM bootloader storage validates authenticity of second-stage bootloader
- Secure firmware updates—only authorized code from the manufacturer is permitted
- Authorization—only authentic nodes should be able to gain network access
- Integrity—protecting data from being altered
- Accounting—proper accounting of data, node counts, and timestamps can help prevent unwanted access to IIoT networks
- Secure communication—encrypted protocols that can reside on a low power node
- Availability—ensuring users have access when they need it
- Nonrepudiation—assurance that authentic communication requests cannot be denied
- Reliability—even in harsh electrical environments, access needs to be reliable

Isolation

Isolating systems from each other can reduce the attack surface and limit the spread of malware. Isolate systems that do not require network connectivity from systems that are exposed to networks. Consider setting up a separate air-gapped or tightly monitored network that is separated from other networks for high risk systems. Ideally, critical systems should be completely isolated from the outside world [3].

The infotainment system of a connected car can expose the vehicle to many new attack vectors not previously seen before. The main engine control unit (ECU) has nothing to do with the infotainment system and there should be no way to interact with it through the infotainment system. Though there are typically two separate CAN networks in vehicles separating the most critical systems from the rest, they are still connected together in some way. It is still possible to compromise one and gain control of the other. If there is total isolation between these networks, the risk of compromise would be reduced from potentially life threatening to something far less serious.

Many IIoT systems connect to a cloud server that collects and processes information sent to it by the device and also manages the device. As the number of devices scales to large numbers, the cloud can have difficulty keeping up with all of them. Many systems are moving processing out to the edge on the IIoT devices to reduce the amount of traffic to the cloud.

We often think of data as an asset. Data is mined and sold to find hidden patterns in large data sets. However, the bulk of collected data is usually not very useful, though it may be useful to an attacker. Sensitive data creates a target for attackers and creates a liability. Collected data should be filtered down to only what is needed, and the rest should be deleted as soon as possible. This not only improves security, but also the utility of the collected data. ▷

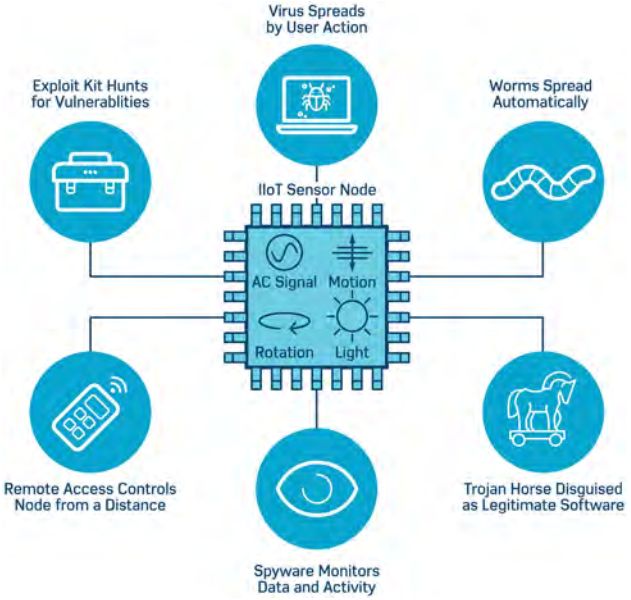


Figure 2: Various types of malware that can potentially infect an IIoT system (Source: Analog Devices)

It is important to identify potentially sensitive information and eliminate or limit its collection.

Processing data at the edge can reduce the amount of data sent and exposed to the cloud. The more locations data is sent, the more difficult it is to keep it confidential. Each new node is another potential compromise where data can be leaked. The attack surface can grow exponentially.

Keeping sensitive data contained at the edge can limit the attack surface specifically on confidential data. If it is confined to one edge node, it is less likely to be stolen. A parking occupancy sensor that detects and only reports the presence of a vehicle through a binary signal after image processing will not stream video. It eliminates the large amount of unnecessary data contained in an image. This reduces the burden on the receiving server so that it cannot be reused maliciously for surveillance.

Similar to consumer IoT systems, industrial IoT systems also have proprietary and confidential information that must be maintained:

- Proprietary algorithms
- Embedded firmware
- Customer information
- Financial information
- Asset location
- Equipment usage patterns
- Competitive intelligence
- Access to a larger network

Some IIoT devices still lack the power and performance to be edge-based. Another topology emerging, the fog model, is a hybrid between cloud- and edge-based systems. In the fog model, the edge nodes first connect to a gateway that receives data and does some processing before sending it to the cloud. There may be one gateway for many IIoT devices. The gateway does not need to operate on battery power, can afford a much higher budget in processing power, and costs more than constrained IIoT devices.

The fog has risen more from scalability issues, but could also come to play a role in security. The gateway device could help protect vulnerable edge nodes that may be too constrained to provide security on their own, but it may be better to provide some level of protection instead of none. The gateway can be used to help manage all the nodes underneath it instead of managing each individual node directly. The fog model can also allow for incident response in IIoT while avoiding disruption of service. For example, security may respond by interacting with the gateway instead of shutting down a mission critical manufacturing line.

Among the greatest challenges in IIoT is the deployment and management of large numbers of devices. Wide reaching IIoT systems are notoriously difficult to set up and configure. With the long lifecycle of IIoT, systems may be deployed by one team and still be operational years later when yet a different team supports it.

IIoT systems are often insecure with weak authentication mechanisms by default. As seen with the Mirai botnet, most users never log into IIoT devices to configure them. They may even be unaware that they are supposed to be configured. Most IIoT users assume things just work out of the box. Systems must be made secure by default. A system expectation should be set that the user may never configure the device other than the default. Weak default passwords are a common mistake.

Network security

While the edge receives most of the focus in IIoT, it is important to not neglect the cloud or the server side of a system. Test for common server side vulnerabilities such as cross-site scripting, SQL injection, and cross-site request forgeries, and review APIs for vulnerabilities ensure that software running on the server is patched promptly.

Data in transit across the network needs to be secured, or it could be intercepted and modified maliciously. Secure cryptographic protocols such as TLS or SSH are used to protect data in transit. Data should ideally be end-to-end protected.

The perimeter boundary of an IIoT network can often be blurry. IIoT sensor nodes often spatially reside on the periphery of their network. However, they also provide an easy portal into a larger industrial network through a fixed gateway [4]. Proper authentication of these devices to the

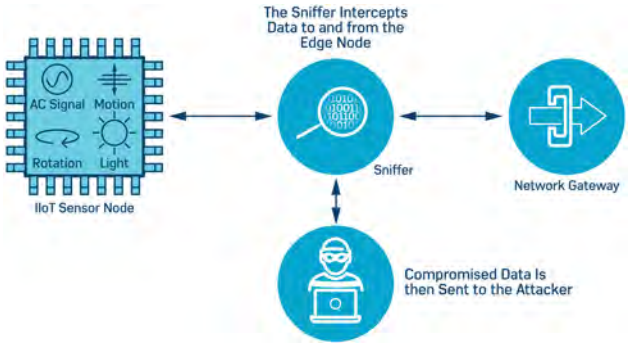


Figure 3: A Man-in-the-middle attack inserts a malicious access point between a node and a gateway (Source: Analog Devices)

help prevent traffic from being tampered by a malicious third party.

Securing network data traffic involves the use of a secure communications protocol. The best practices should be to use standard protocols that are known to be secure. Security on an Ethernet LAN can be provided using IEEE 802.1AE Macsec. Wireless LANs tend to be a higher risk since they are more accessible and ubiquitous. WPA2 provides security for IEEE 802.11 wireless networks. The low power IEEE 802.15.4 standard, often used within wireless IIoT solutions, offers its own suite of security protocols. However, these are layer-2 protocols used on the data link layer and only secure traffic on the LAN.

Securing traffic that needs to be routed outside the LAN, for example over the Internet, requires higher layer protocols that provide end-to-end security. TLS (transport layer security) is commonly used to secure Internet traffic and provides end-to-end security. While TLS uses TCP (transmission control protocol) and many IoT devices communicate using UDP (user datagram protocol), there is DTLS (datagram transport layer security), which works over UDP. While IoT devices are constrained in power and memory, it is possible to implement TLS for most constrained applications with minimal effort. For even more tightly constrained devices, there is currently a new protocol, constrained application protocol (CoAP) in development by the IETF.

Endpoint security

While securing data in transit is important and necessary, attacks are more often targeted at the endpoints. Network facing interfaces need to be hardened against vulnerabilities. One approach to IIoT security is to build protection directly into the sensor node device. This provides a first critical security layer, as the devices are no longer dependent on the corporate firewall for their sole protection. This can be especially critical for mobile corporate devices and IIoT sensors that are deployed in remote locations.

A security solution for IIoT devices must provide protection against a wide range of cyber attacks. It must ensure that the device firmware has not been tampered with. Additionally, it hast to be able to secure the data stored within the device, be able to secure inbound and outbound communications, and it must be able to detect and report any attempted cyber attacks [5]. This can only be achieved by including security in the early stages of design.

There can never be a one-size-fits-all security solution for embedded devices. Solutions are available that provide a general framework for OEMs (original equipment manufacturers). However, a complete security framework must consider the core capabilities required to protect specific devices, networks, and entire systems. There must be also the flexibility to customize a solution to any specific requirements, while also ensuring that critical security capabilities are included.

In medicine, sterilization of surgical tools is essential to allow their reuse while preventing the spread of disease. The autoclave is the gold standard for sterilization. It quickly sterilizes instruments with superheated steam at high pressure. It obliterates all bacteria and returns the instruments to a known good state. This allows a surgeon to use a scalpel for surgery and safely reuse the scalpel after sterilizing it.

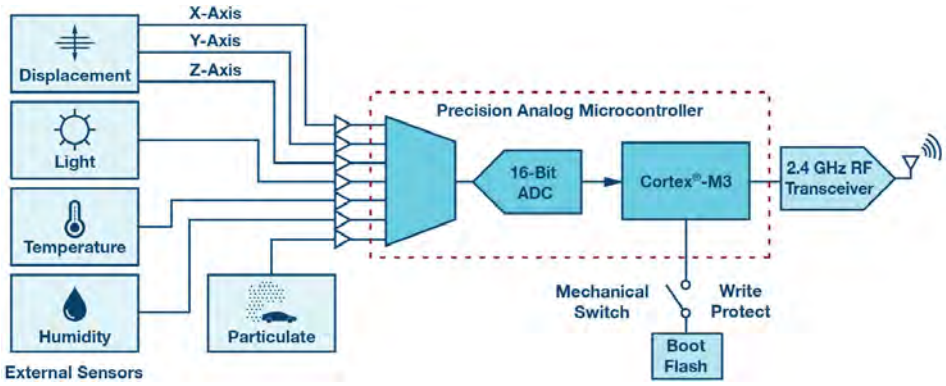


Figure 4: Physically write protecting firmware, except when performing an update, is an effective way to protect the integrity of a device (Source: Analog Devices)

The ability to return the system to a known good state after compromise is more important than making it bullet-proof to all attacks. A resilient system can quickly recover and resume operation with confidence.

Once a system is infected, how can it be disinfected? When a system is infected, it alters the state of the system in some unknown way. Remote exploits take control of the processor and inject new malicious code into the system. Typically, the firmware is modified or replaced in some way with malware so the system now behaves in a different way. Once this occurs, the processor can no longer be trusted.

Embedded systems are often designed in a way that make it too difficult to reliably recover from a compromize. Often, the only way to sanitize a system and verify that a system is clean is to physically dump all nonvolatile memory directly to an external reader. Then it can be verified against the original firmware and replaced with the original if it is not intact. Most systems are not designed in a way to make this possible.

One method to protect the integrity of a system is to physically write-protect nonvolatile memory with a mechanical switch. When the switch is set to write-protect, the memory is physically protected in hardware. Moving the control over memory outside the domain of the processor makes it physically impossible to remotely install permanent malware into this memory without physical access to the device. This reduces the list of potential attackers from anyone in the world with an Internet connection to only those that have physical access to the device for an extended period of time. Firmware updates are usually a very rare event. When a firmware update is required, the user can set the switch to write enable the memory to authorize the update and then write-protect the device once the update is complete. Many devices also use their nonvolatile memory to store data needed for write access. In a high security system, a separate nonvolatile memory chip may be used to store data but not the software. An attacker may still compromise some systems by writing malicious data to this memory and exploiting software bugs, so the system should be thoroughly analyzed and tested. Thus no matter which data is stored in this memory, the system will not be compromized. The addition of an extra memory chip increases cost, however, some flash memory allows certain sectors to be write protected, while allowing others to be writable.

Secure boot

A secure boot prevents unauthorized software from being loaded onto the device during the boot process. It is the beginning of the chain of trust. A secure boot starts with a first-stage bootloader programmed into a read-only, nonvolatile memory located on the node. This bootloader only validates the authenticity of the second-stage bootloader. The second-stage bootloader, which very often is more complex and can be stored in a reprogrammable flash memory, repeats the process [6]. It verifies that the operating system and loaded applications are indeed valid from a trusted source.

An IIoT node with secure boot and secure firmware update capabilities ensures that the device is running authorized code and not altered or malicious code, as this prevents the permanent installation of malware or code. The device will either only run unmodified code or will fail to boot.

The secure boot process usually relies on digital signatures to protect the authenticity of the code. The code images are signed by the device's OEM using the OEM's private key at the time of manufacturing assembly. The OEM's corresponding public key is then used by the node to validate the signature for the firmware image.

The code can also be protected with a message authentication code (MAC) using symmetric cryptography, but this requires the private key to be stored on the device, which puts it at risk. However, it is computationally easier to use a MAC.

While a secure boot can enhance security, it can sometimes be too restrictive to end users since it can prevent them from changing the software running on their devices or running their own software. Depending on the application, users may need more flexibility and the ability to configure a secure boot, which allows it to trust their own code.

Secure firmware updates, similar to a secure boot, validate that new code images have been signed by the OEM during the upgrade process. If the downloaded images are not valid, then they are discarded and the upgrade is halted. Only valid images are acceptable and subsequently saved to the device memory.

Assume that a vulnerability will be discovered sometime. There should be a plan in place for how vulnerabilities will be addressed when they are found or exploited. There usually needs to be a way to allow software updates and patches to be installed on the device to fix vulnerabilities. The update process also needs to be properly implemented so that it is not used as an attack vector that allows anyone to install malware on the device. Making a device accessible through a network, merely to provide patching capability, can introduce more risk than it mitigates.

Secure communication

Most engineers think of security as communications protocol, such as SSL/TLS, SSH, and Ipsec, as secure communications have been added to many embedded devices. However, while this is a portion of the security threat, other attack vectors provide new avenues. Many IIoT sensor nodes operate in a low power configuration with lower power processors that are not capable of supporting some of the best options, such as TLS or Ipsec. Security protocols provide a good starting point for building secure devices [7]. They are designed to protect against packet sniffing, man-in-the-middle attacks, replay attacks, and unauthorized attempts to communicate with the node.

Small IIoT edge sensor devices are often adopted with wireless protocols such as Zigbee, Bluetooth low energy (BLE), and other wireless and mesh networking protocols. These protocols have some amount of built-in security. However, it is relatively weak. Many exploits have already been published and are well known by sophisticated hackers. Small form factor IIoT devices typically run on very low cost, lower power processors that do not support TLS or Ipsec. For small edge devices, DTLS, which is TLS over UDP, can be used for secure communication.

Physical security

Physical attacks target the actual edge hardware nodes or gateways of an IIoT system and can include breaches at the front-end sensor. These attacks often require physical access to the system, but may also simply involve actions that merely limit the efficacy of the IIoT hardware. Attackers can tamper with nodes to gain control over sensors or other devices within an IIoT environment. They can then extract confidential data and embedded firmware code from the source. Using a malicious node injection strategy, attackers can physically deploy malicious nodes between legitimate nodes into an IIoT network [8].

To help mitigate these attacks, several hardware forethoughts can be implemented during the design phase. Easy physical probing of signals through leaded devices, exposed copper vias, or unused connectors should be minimized or even abandoned from the design. A silk screen that details components and offers potential hackers additional information should be removed, unless it is deemed absolutely necessary for the design. Although it can increase system complexity, an industrial conformal coating not only buffers the hardware from the elements, but can also add an additional step to prevent direct probing of the electronics on the PCB (printed circuit board).

Any embedded nonvolatile memory contents should be encrypted and write-protected within the component. The interface between the micro-controller and DSP device should be within buried trace layers on the PCB. Even if the contents of the embedded memory could be retrieved, the encryption and validity of that data should render it meaningless.

Manufacturers often include debug or test ports. These are usually serial or JTAG and can be used to gain access and control most of the system. Ensure that these ports are functionally disabled or protected in production, because it is insufficient to not populate debug headers, as a determined individual can just populate them or solder their own connections to pins. Authentication before these interfaces are allowed to be used is required if they need to remain enabled in production devices. They can be password protected, but be sure to allow the user the ability to set strong passwords.

Cryptographic functions usually require some sort of random number generator (RNG). Random numbers may need to be unpredictable for key generation or they may need to never repeat. Generating random numbers in constrained embedded systems usually presents a significant challenge, due to the lack of resources and entropy.

Many embedded systems have suffered from too little entropy. This can lead to catastrophic breaks, such as in Taiwan's national ID smart cards. Researchers found that many ID cards generated related keys from the same numbers due to a lack of entropy. As a result, they were able to be broken, despite using a strong RNG [9]. Similarly, in 2012, researchers found that 0,38 % of RSA keys on public key servers shared weak, random number generation and were able to break them [10].

It is difficult or nearly impossible to validate the strength of an RNG. RNG design in the past has been fairly ad hoc and poorly understood. However, in recent years, significant progress has been made toward the design and formal analysis of robust cryptographic random number generators.

Modern, robust RNG designs now tend to have three stages [8]. There is an entropy source that provides the raw entropy, an entropy extractor to give the entropy a uniform distribution, and an expand stage to expand the small amount of entropy available.

The first stage is the entropy source. This may be some physical noise source, such as clock jitter or thermal noise. Some processors, such at the ADI Blackfin DSP, provide hardware with random number generators that can be used for entropy generation.

Random numbers for crypto need to have a uniform statistical distribution. All entropy sources have some amount of bias, and this bias needs to be eliminated before using it for a cryptographic application. This is done using an entropy extractor, which takes non-uniformly distributed input with high entropy and generates a uniformly distributed output with high entropy. This comes at the cost of some entropy loss, as the entropy extractor requires more entropy input into it than it can output. As a result, many more bits need to be collected from the entropy source and distilled into a small, high entropy number that can be used to seed a cryptographically secure pseudo-random number generator [11], [12].

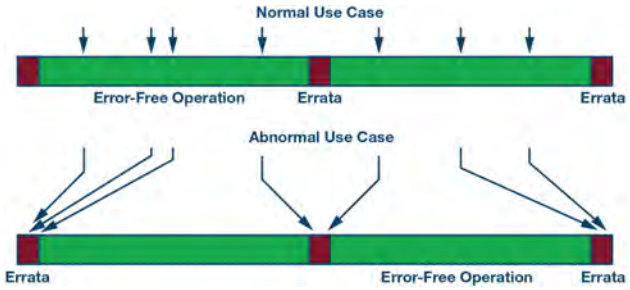


Figure 5: Exploiting small errata to force a failure 100 % of the time (Source: Analog Devices)

Exploiting errata

Nearly all IIoT nodes are operated with some form of embedded firmware or algorithms. Functionally, this firmware may operate just fine with no apparent issue in its capability to perform its requirements. However, all software has some level of bug or erratum that permits a small percentage of abnormal operation that may cause security problems. For instance, a 99,99 % erratum-free firmware will rarely, if ever, cause any operational problems. But this small, 0,01 % erratum may be able to be exploited by an intruder to force the operation of the node to fail 100 % of the time for that particular mode of operation. Software bugs arise from complexity, which is necessary for any system to do anything useful. Software bugs and vulnerabilities exist in essentially all systems.

Security must be a consideration of the system design from the beginning. It should be a part of the design process, not something that is bolted on at the end of the project. Security is not about adding security features; it is about ▷

The missing security aspects

There is a lot of discussion about cybersecurity in automobiles. The automotive industry wants that we are afraid of bad boys attacking our cars. This means, the vehicles should be secured against unauthorized access. But this is just one viewpoint.

Another one is that data produced by me and my car needs to be secured and protected, too. I do not want to give this data for free to OEMs and Tier1s, because they may make money with them. But it is my data and I want to have the freedom to sell them or not. This means, I agree to secure my car against third party access, but this also includes the access by OEMs and Tier1s. Of course, I will allow access in case of maintenance and repair.

Additionally, I would also appreciate secured ECUs and other electronic equipment, which makes it impossible for owners to manipulate or to tamper their vehicles. I give you some examples: Truck owners should be not able to change tachograph data and load measurements. Also the integration of Adblue simulators should be not possible. In general, the vehicles should be secured against any illegal "improvements".

Unfortunately, this kind of security is not in the focus of OEMs and Tier1s. I think we should talk about this.

Holger Zeltwanger

References

[1] Mirai botnet leaked source code.
[2] Ross Yu. “Security and Reliability Are Key in Wireless Networks for Industrial IoT.” Analog Devices, Inc., 2017.
[3] Patrick Nelson. “Organizations Must Isolate IoT from Regular IT, Says Telco.” Network World, March 2016.
[4] Brian Girardi “Endpoint Security and the Internet of Things.” CSO, 2017.
[5] Tristan O’Gorman. “A Primer on IoT Security Risks.” Security Intelligence, February 2017.
[6] Abhijeet Rane. “IoT Security Starts with Secure Boot.” Embedded Computing Design, January 2017.
[7] Amitrajan Gantait, Ayan Mukherjee, and Joy Parta. “Securing IoT Devices and Gateways.” IBM, May 2016.
[8] Boaz Barak and Shai Halevi. “A Model and Architecture for Pseudo- Random Generation with Applications to /dev/random.” Proceedings of the 12th ACM conference on Computer and communications security, November 2005.
[9] Chen-Mou Chang, Daniel J. Bernstein, Chang, Li-Ping Chou, Nadia Heninger, Nicko van Sormersen, Tanja Lange, and Yun-An Chang. “Factoring RSA Keys from Certified Smart Cards: Coppersmith in the Wild.” Springer, 2013.
[10] Arjen K. Lenstra, Christopher Wachter, James P. Hughes, Joppe W. Bos, Maxine Augier, and Thorsten Kliengun. “Ron Was Wrong. Whit Is Right.” Cryptology ePrint Archive, Report 2012/064, 2012.
[11] Boaz Barak, Eran Tromer, and Ronen Shaltiel. “True Random Number Generators Secure in a Changing Environment.” Springer, 2003.
[12] Boaz Barak, François-Xavier Standaert, Hugo Krawczyk, Krzysztof Pietrzak, Olivier Pereira, Yevgeniy Dodis, and Yu Yu. “Leftover Hash Lemma, Revisited.” 31st Annual Conference on Advances in Cryptology, August 2011.

managing risk. Secure design methodologies are essential for any IIoT system development.

Existing secure design practices still apply. Use threat modeling to identify risks and to choose appropriate risk mitigation strategies. Identify the entry points to a system in order to identify the highest risk areas in a system. Most attack vectors are through external interfaces, so review the design implementation for security vulnerabilities. Handle unknown data carefully and validate all input—validation and security should not just be limited to the entry points. Defense in depth is important, meaning layers of security are needed in case the outer layer is breached.

Many processors provide different levels of privilege. ARM has Trustzone and the ADI Blackfin DSP provides both user-level execution mode and privileged execution mode. Execute as much code as possible in the lowest level of privilege possible to keep the most important code within a privileged mode. Security requirements for IIoT devices must take into consideration the cost of a security failure, the likelihood of an attack, primary attack vectors, and the cost of implementing a security solution.

Conclusion

Many of these recommendations conflict with each other and with the other design goals of the system. Providing security usually involves some sort of trade-off, often with cost, functionality, or usability. Some trade-offs are very effective and inexpensive, while others have high cost and little impact. Security needs to be balanced against the other needs of the design and should be determined in an application specific basis through a secure design process.

To assist with securing the IIoT, Analog Devices offers several processors that provide hardware-based security enhancements that can help push the boundary of what is possible in edge nodes. The ADF7023 RF, low power transceiver offers internal AES encryption by using an ISM band with many different available modulation schemes.

The embedded transceiver within the ADuCM3029 provides AES and SHA-256 hardware acceleration and a true random number generator, along with multiparity protected SRAM. The ADSP-BF70X Blackfin family of digital signal processors provide embedded, one-time programmable memory for secure key storage and fast secure boot, providing a strong guarantee that the system will return to a known good state after compromize.

Rollback protection in the Blackfin DSP with a hardware-based, increment-only counter allows firmware to be updated to fix vulnerabilities when they arise. This, coupled with the immutability of the key storage, provide the capability to create a robust and resilient edge node. In addition, the Blackfin DSP provides crypto hardware accelerators, a hardware-based true random number generator, separation of privileged and unprivileged code execution, an memory management unit, and the ability to restrict access for many direct memory access channels to allow for parallel and power efficient secure DSP at low cost. ◀


Author

Erik MacLean, Ian Beavers
Analog Devices
adi-germany@analog.com
www.analog.com

Why encrypt logged CAN data?

A common method for collecting raw CAN data is to log it on an SD card or to upload it to a server. In many cases, the collected CAN data is unencrypted. This article highlights three reasons why the lack of encryption may lead to problems.

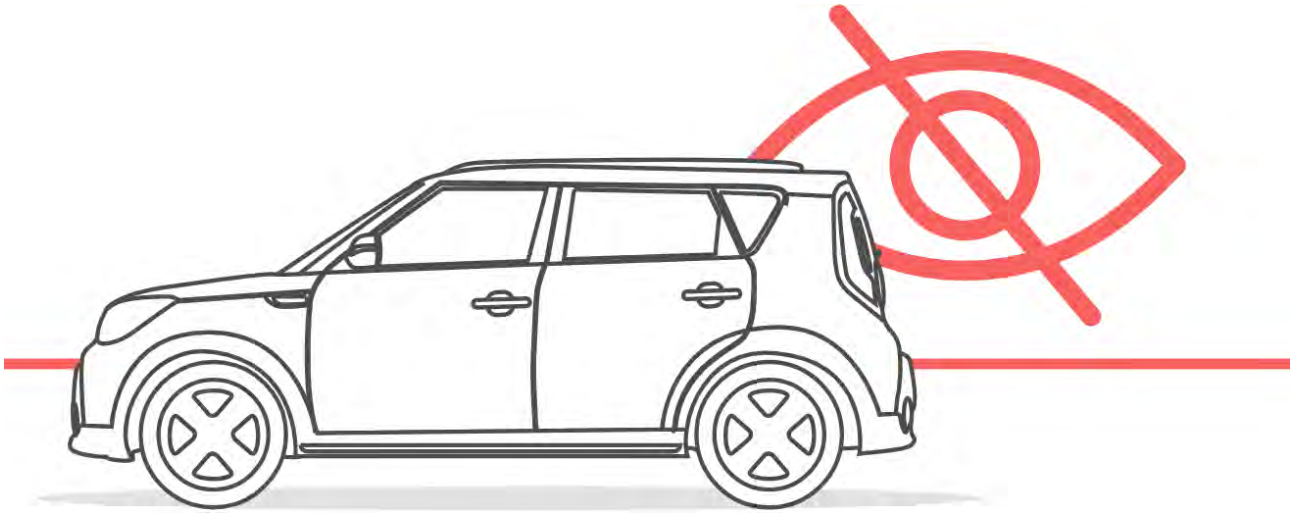


Figure 1: Privacy regulations like GDPR and CCPA are key reasons for encrypting recorded CAN data at rest on SD cards (Source: CSS Electronics)

Privacy regulations

Recent years have shown a drastic increase in privacy regulations, including GDPR (general data protection regulation) in EU and CCPA (California consumer privacy act) in California. If a breach occurs, companies may face substantial fines. However, if the data is encrypted "at rest" (e.g. on an SD card) and "in transit" (e.g. during upload), fines may be waived or reduced.

CAN data is often linked to e.g. a driver of a vehicle and may contain information on VIN (vehicle identification number), speed, fuel consumption, DTCs (diagnostic trouble codes), and GPS (global positioning system) data. It is generally considered in scope of the privacy regulations. In short, not encrypted CAN data can have large financial consequences in case of data breaches.

Remote cyber-attacks of connected assets

Vehicles and machinery are increasingly connected, which exposes these assets to cyber-attacks. For example, a compromised CAN dongle can be used to remotely control asset functionality (e.g. turning a steering wheel) or to deny service of low-priority CAN messages by broadcasting high-priority CAN messages at high frequency.

CAN FD may solve this problem via such solutions as Secure Onboard Communication (SecOC), effectively encrypting the CAN data and making it difficult to spoof the system. However, CAN FD is still in the early stages of roll-out and Classical CAN assets remain exposed.

If a dongle uploads unencrypted CAN data, an attacker may use this to reverse engineer the CAN frames required to control specific asset behavior. Such attacks can be harder to defend as the denial of service attacks. In short, not encrypting CAN data used in e.g. telematics may expose assets to critical cyber-attacks.

Business-critical data

CAN data is increasingly used by OEMs (original equipment manufacturers) e.g. in prototype fleet testing or as part of 'black box' systems used for legal compliance, insurance or warranty dispute handling. This type of CAN data is often sensitive in its nature. The validity of such data can be critical.

For example, a dispute may arise if a CAN-based asset breaks down in the field. This could lead to large financial consequences. Here, an OEM might use CAN log files to prove that the asset failure was due to the incorrect usage. However, before the OEM can collect the unencrypted CAN data from the SD card, it is possible for the end user to modify the log files e.g. to remove the traces ▷

Figure 2: Remote cyber-attacks via Classical CAN is an increasingly critical security risk (Source: CSS Electronics)

Figure 3: Data integrity is essential for use cases where data is used as a legal proof (e.g. warranty dispute handling) (Source: CSS Electronics)

of the incorrect usage. Conversely, the end user may claim that the OEM has injected false data into the log files. In short, unencrypted CAN data logs may be stolen or falsified - with big consequences.

Is raw CAN data not already encrypted?

Someone may argue that "raw" CAN data is already encrypted as the data must be decoded to be interpretable (e.g. via DBC files). There are fallacies to this view. A large share of data logging use cases relates to J1939 data (heavy duty vehicles) or OBD2 data (cars). In both cases, data can be easily decoded via DBC files available for purchase or free online. Secondly, even if the data is 100 % proprietary with a carefully protected DBC file, the data can still be decrypted via reverse engineering. In the view from CSS Electronics, raw CAN data is equivalent to a plain text.

Things to consider when encrypting CAN data

To encrypt the CAN data, companies should consider various aspects of their data logging setup:

- If data is stored on an SD card, the data logger should be real-time encryptable. This means that the files should not be temporarily exposed e.g. while the batch-processing process.

Figure 4: A modern telematics solution needs to address multiple security risks (Source: CSS Electronics)

Figure 5: The CANedge2 is designed for end-to-end security (Source: CSS Electronics)

- The data encryption must ensure data integrity to prove that the data contents were not changed. The risk of data falsification can be removed e.g. by deploying an AES-GCM (advanced encryption standard, Galois-counter mode) algorithm.
- If CAN data is uploaded via a WiFi connection or 3G/4G cellular networks, the device should support HTTPS (hypertext transfer protocol secure) for secure data transfer.
- All involved passwords must be encrypted if these are stored on a device or an SD card.

A key challenge considering the above requirements is that real-time data encryption is a computationally intensive task. As such, proper encryption requires dedicated hardware components, which are not available in most CAN data loggers deployed in the field today.

Data encryption implementation

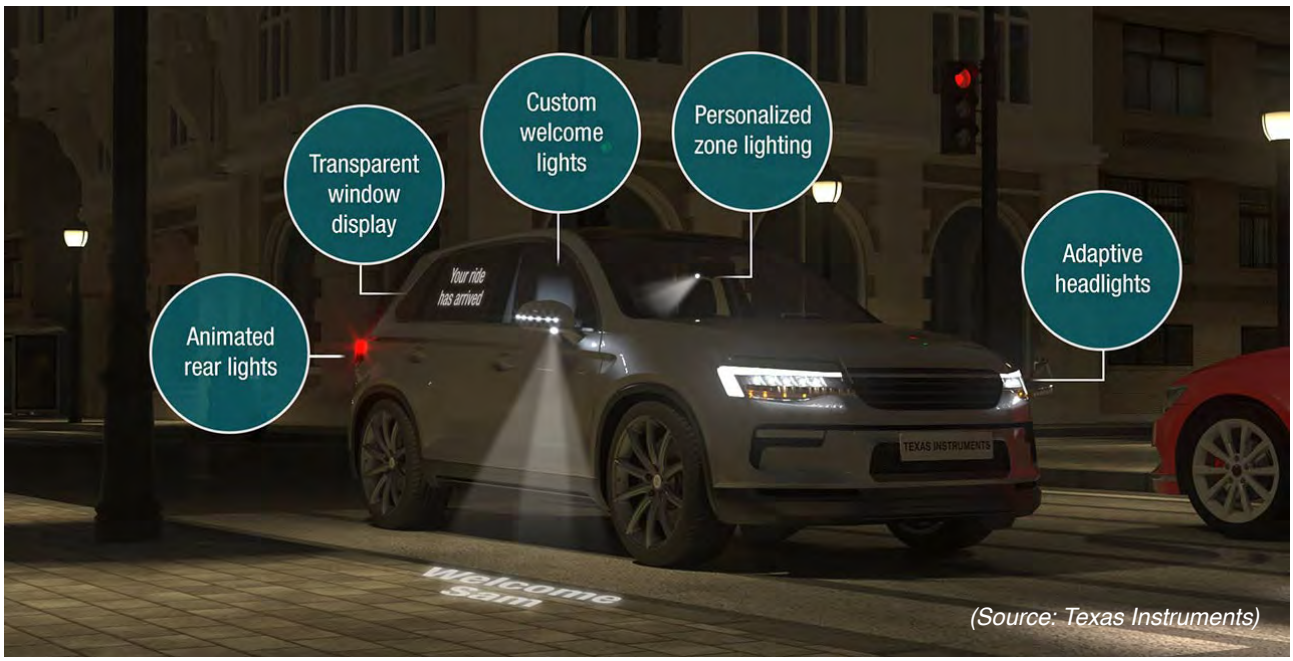
At CSS Electronics, encryption was a key design criterion for the CANedge data logger. CSS faced increasing demand from customers for encryption, in particular after the roll-out of the CCPA. Many OEMs see this as make-or-break for their use cases. To meet the demand for encryption, the CANedge1 and CANedge2 data loggers support data encryption.

Author

Martin Falch
CSS Electronics
contact@csselectronics.com
www.csselectronics.com

Semiconductors for automotive lighting solutions

Original equipment manufacturers are implementing modern automotive lighting use cases. This article introduces semiconductor technologies from Texas Instruments (TI) impacting headlight, rear light, and other lighting systems.



(Source: Texas Instruments)

Automotive lighting applications include dynamic and static headlights (low beam, high beam, turn indicators, etc.), rear lights, as well as interior light systems. Adaptive headlight systems (see Figure 1) adjusting the beam shape are available on cars in Europe, but yet forbidden in the USA. The systems use high-powered LEDs (light-emitting diodes) as a light source. The LEDs require high-powered drivers to regulate current and to achieve the required brightness. Switching LED drivers must be implemented as dual-stage power-processing topologies.

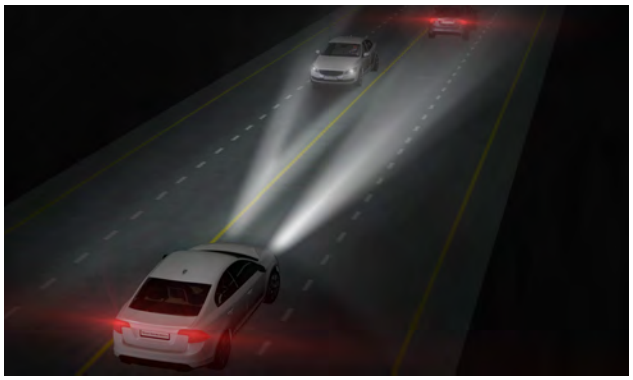


Figure 1: Adaptive headlights adjust the beam shape and illuminate the entire field of view while avoiding glare from oncoming traffic. (Source: Texas Instruments)

Headlight ECU reference design

The headlight ECU implements a two-stage boost controller of multiple buck LED drivers that support four channels to an LED matrix manager. The system overview is shown in Figure 2. The TPS92682-Q1 boost controller is set in voltage regulation mode capable of 130-W output power. The boost output drives two TPS92520-Q1 dual-channel synchronous buck LED drivers. This makes a total of four buck channels with a 120-W total output. The synchronous buck channels manage pixel-controlled loads using the TPS92662 LED matrix manager devices. The LED matrix-manager ICs (integrated circuits) are responsible for adjusting the headlight beam shape (see Figure 1). They control the intensity of each pixel to generate different beam patterns and to illuminate the entire field of view while avoiding glare from oncoming traffic.

The MSP432E401Y micro-controller enables the headlight ECU with two CAN interfaces. The micro-controller communicates with the in-vehicle CAN networks. It controls the TPS92682-Q1 and the two TPS92520-Q1 devices via SPI (serial peripheral interface). It also communicates with the lighting matrix module using UART (universal asynchronous receiver transmitter) communications via the TCAN1042 CAN transceiver.

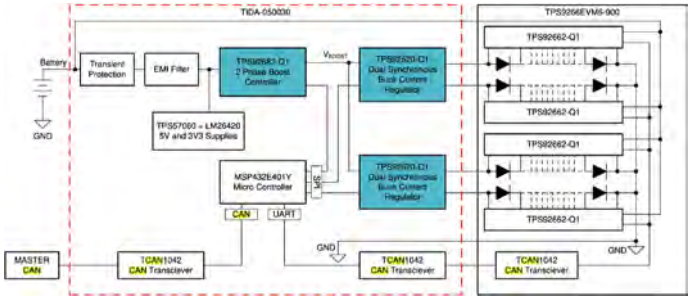


Figure 2: Automotive headlight ECU reference design (Source: Texas Instruments)

The system can operate at voltages from 9 V_{DC} to 24 V_{DC} with a derate down to 6 V_{DC}. It also operates during cold crank and load dump conditions when the battery voltage varies. A two-stage ECU is needed due to the dynamic nature of a matrix load. Here, the LED current regulation is done by a low-output capacitor topology such as a buck at the second stage. The wide input voltage variability of an automotive battery system requires to boost the first stage to ensure a consistent input voltage for the buck second stage.

Further headlight options

Headlights based on TI's DLP technology enable beam shape adjustment as well as symbol projection. Symbols can be made visible to the drivers as well as to other road participants. For example, the lane marking uses headlights to draw the planned driving path on the road. This can help drivers to navigate within hazardous driving conditions. This marking helps also the others to see where the vehicle will be traveling. Company's DLP5531-Q1 chipset for headlight such applications is already used on the road.

CAN FD light protocol

CAN in Automation (CiA) members started to develop the CAN FD light master/slave protocol based on CAN FD. It is intended for simple sensor and actuator communication. A typical example are the modern LED lamps in passenger cars.

The CAN FD master node synchronizes the slave nodes with hundreds of LEDs. The slave nodes transmit CAN-FD data frames only on request of the master. This avoids the implementation of high-performance and costly oscillators. The implementation of the CAN FD slave nodes is also simplified, because there is no arbitration needed. It is intended to run such networks with one bit-rate. Therefore, the bit-rate is limited to 1 Mbit/s, which is fast enough for such applications. Only the CAN FD data frames with 11-bit CAN-identifier are used for the communication. Error and overload frames are not supported at all. Nevertheless, data fields of up to 64 byte are possible.

The CiA Special Interest Group (SIG) named "CAN FD light" works on the intended specification. Fred Rennig from ST Microelectronics chairs the group, which comprises about 20 experts from different companies.

Figure 3: Rear lighting that spans across the length of a vehicle (Source: Texas Instruments)

Using the headlight leveling technology, the beam lights the road regardless of the road inclination or vehicle's acceleration (deceleration). Pointing the headlight to the road enhances visibility while driving in the night. Bipolar stepper motors are typically used to control headlight leveling. The DRV8889-Q1 stepper motor driver integrates a power stage to drive the motor, as well as a stall detection capability.

TI's CAN transceivers (e.g. TCAN1044-Q1), and CAN-capable system-basis chips (e.g. TCAN4550-Q1) are the provided options for automotive lighting applications.

Animated rear lights

LED-based rear lights (e.g. brake lights, turn indicators) can also include animation or personalized lighting messages. A static LED driver module enables lights operation at low battery voltages and lowers the high battery voltages to optimize the thermal management of the second-stage LED drivers. TI's TPS929120-Q1 12-channel LED driver for animated lighting uses company's Flexwire (UART) interface to enable individual pixel control. Thus, high-LED-count systems can dim independently. The unit can also provide a CAN interface. A diagnostic and a fail-safe mode ensure LED lamps reliability. The chip offers off-board support, which is suitable for rear lighting implementations spanning across the entire vehicle length. (see Figure 3).

Another example is the swiping turn, where the turn indicator LEDs light up in sequence instead of all at once. Rear lights can also be used to display welcome messages for drivers or message alerts for drivers behind the car.

Additional lighting functions

Inside the cabin an array of LEDs can be adopted to display personal messages (e.g. welcome messages) or to adapt the light beam to shine at a specific location. The TLC6C5724-Q1 is a 24-channel red-green-blue LED driver that independently controls each channel, which is critical for zoning applications.

The original intention of ground projection (puddle lights) was to illuminate the vicinity of the vehicle to help drivers to navigate entering. The next generation of puddle lights will enable dynamic ground projection. This feature can communicate information to drivers before they enter their cars, alert those around the car, or provide a branding opportunity for automakers. Cars with static puddle lights that project a static symbol such as a logo are already available.

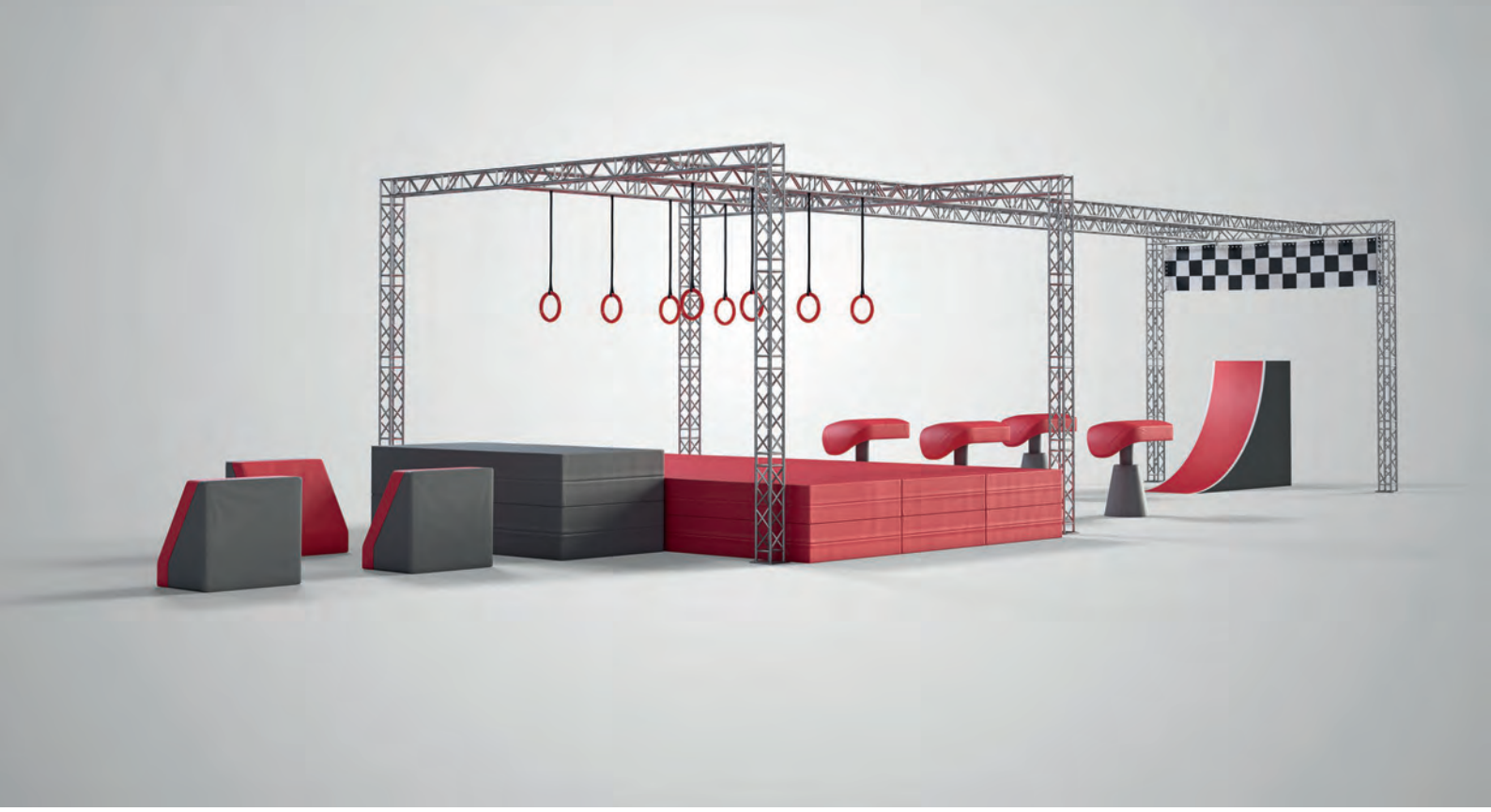
There is a need to develop systems displaying ride-sharing-related messages. Additionally, the trend toward autonomous vehicles demands methods for cars to communicate with other vehicles and pedestrians. For example, such messages can be displayed on a car window. TI's DLP technology can project information on windows when the car is stopped and keep the windows clear when the car is being driven. The technology can also display billboard advertisements on the window. ◀

Author

Olga Fischer
CAN Newsletter
pr@can-cia.org
www.can-newsletter.org

Vector Testing Solution

It's Good If Your Software Runs. And Even Better If It Tackles Every Challenge.



Outstanding Software Quality Demands Rigorous Testing.

For embedded software to be successful, it must meet the highest demands. Our comprehensive test solution enables your software project to effortlessly pass every performance test. From the design and implementation of the test to its execution, along with the centralized administration and analysis of your test data – we cover the whole gamut, whether for unit or system tests, SIL or HIL. This allows you to always be on the safe side and identify potential improvements for your software at an early stage. And to tackle every challenge with ease.

Vector brings your software development a giant leap forward.

vector.com/testing-solution

VECTOR

Selecting a connector system for harsh environments


(Source: Adobe Stock)

This article gives a deep insight into the aspects to be considered when selecting a connector for use e.g. in mobile working machines. These include connector's CAN connection, IP protection, wire sealing, contacts, mounting, flammability, etc.

The world is full of different connectors. Connectors are available in many different shapes, sizes, materials and colors. It might seem that selecting a connector system to suit perfectly in the intended application is a trivial task. But there is a lot more to it.

Most connectors are located in such environments that do not pose too strict requirements for the connector system in terms of size, shape, current throughput, ingress protection levels, vibration performance and so on. But when you start to list the requirements of a mobile working machine environment, the options to choose from narrow down drastically. Connector systems should support the design of a high-quality system built on top of a machine and therefore there is a lot more to a high-quality connector than just high ingress protection level. From system architecture and harness design point of view, the right amount of contacts is important so that the harness stays simple and easy to assemble and service. The ability to withstand vibration and high acceleration mechanical shocks is vital. Also, extreme temperatures are often to be found in mobile ECU (electronic control unit) operating environments.

Connectors are obviously not the only components in the control system that must withstand harsh environments, so the connector design must support high quality ECU and wire harness design. Manufacturability of wire harness or ECU is crucial when electronic systems get more complex and the price must be kept in control.

This article has been written to help a mobile working machine builder, electronic control system integrator, system architect or an ECU design engineer in their job by providing important points that should be taken into consideration when selecting a connector system for demanding applications.

System architecture

To begin with, a simple question is how many wire connections per connector is suitable for the application. If you have a single unit that controls several small auxiliaries all over the machine, you probably want to have a lot of connectors with small amount of contacts in order to keep the harness simple. On the other hand, you might want to keep the assembly and unit change simple and go with one connector with the cost of more complex wire harness design. A common way to build machines is to dedicate one medium to high I/O (input/output) unit for one section of a machine. This often provides room for some auxiliary device expansions.

Equally important is to determine if the communication buses are routed through the same connectors as sensor inputs and control outputs or if they have their own connectors. Traditional communication protocols such as CAN and serial protocols such as EIA-232 and EIA-485 can be routed through almost any kind of connector with no need ▷

Figure 1: Typical operation environment for an ECU (Source: Epec)

for uninterrupted external shielding or only short untwisted section of a twisted pair cable. High-speed communication protocols such as Ethernet or USB (universal serial bus) are widely used in mobile machinery today. These kind of communication protocols need external shielding for cables and are quite sensitive to untwisted and unshielded sections. So, in order to use such protocols, a separate high-speed connector or a hybrid connector needs to be used. Since these signals not only require specialized connectors but also the cables need to fulfill certain requirements, often off-the-shelf cables are preferred. When using a hybrid connector, it should be noted that these cables are routed within the power and IO-cabling.

CAN design considerations

Electronic control units in mobile machinery communicate with each other with almost no exceptions via a field bus. CAN has established its place as the industry standard for more than 20 years now. As the amount of data increases, Classical CAN is also evolving from maximum bit-rate of 1 Mbit/s to CAN FD (Flexible data rate), which can reach up to 5 Mbit/s. Also, next evolution versions of CAN are in sight, CAN XL will someday reach the bit-rates up to 10 Mbit/s.

What kind of requirements does CAN set to the connector system? CAN is a robust and fault-tolerant field bus, and especially at bit-rates below 500 kbit/s it is not too picky on the cable nor the connector. But when the bit-rate increases from 500 kbit/s up to 1 Mbit/s or even higher, the significance of a proper signal path provided by the cable and the connector system becomes more relevant. Even more so, when the environment is critical in terms of EMC (electromagnetic compatibility) and the CAN emissions must be kept low and the tolerance against external electromagnetic fields high. For most demanding applications, a tight twisted pair with 360-degree shielding is the way to go. The connector system must support this with short untwisted length of the signal pair and secure the cable shield connection.

CAN bus uses a differential, single twisted pair signal that has a characteristic impedance of 120 Ohm. The ▷

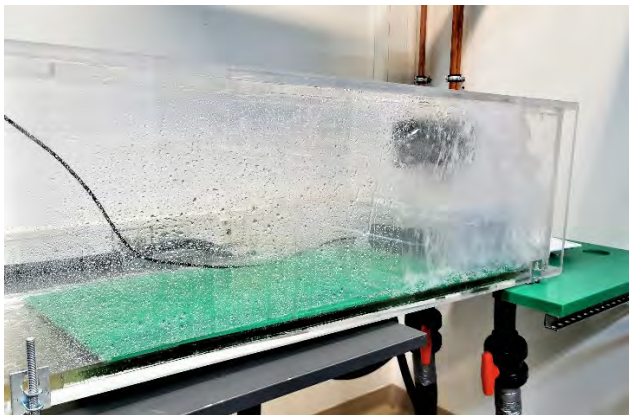


Figure 2: IP65 test performed inside acrylic tube (Source: Epec)

bus must be terminated with 120-Ohm resistors from each end of the bus. Also, a ground return path shall be provided between nodes, and, if cabling incorporates shielding, this should be able to connect to the connector also. To connect CAN sensors to the system, a supply voltage to the sensor is needed too. So, to take all scenarios into account, it is required to have five connector pins for a single CAN interface. For sensors, a 5-pin A-coded M12-connector is the choice of most manufacturers, since it serves almost all features a properly cabled CAN would need. The only downsides are bulky (and costly) cables and cable branching. For a more common ECU connector (rectangular plastic connector) a perfect design would incorporate the following features:

- CAN bus cables separated from I/O cabling,
- inbuilt selectable bus termination resistor, and
- the possibility to branch the bus to the next ECU or sensor.

Designated ground and shield pins for each CAN bus are very useful as well. Sometimes the service technician will want to connect a diagnostics tool to the CAN bus. A perfect connector design would make this both easy and simple.

Protection against environment

Anyone who has been dealing with harsh environment systems is usually familiar with most common IP (ingress protection) classes. But what distinguishes these different protection classes from each other? Here we focus only on dust tight IP6x classifications since these are the most common ones to appear in waterproof connectors. Both, IP65-rated and IP66-rated devices have to withstand 3-minute water spray tests from 2,5 m to 3 m distance, with different nozzles and water flow. In IP65, the nozzle diameter is 6,3 mm and water flow 12,5 l/min. These figures add up to approximately 0,3 bar pressure. For comparison, IP66 water flow is significantly higher, 100 l/min from a 12,5-mm nozzle. That is almost two times the diameter of an IP65-nozzle, and the pressure for IP66 is around 1 bar, more than three times higher as the pressure of IP65. Both tests are normally made with roughly room-temperature water, the deviation between EUT (equipment under test) temperature and water should be kept smaller than 5 °C.

IP67 is probably one of the most recognized tests, a static immersion test in 1-m deep water for half an hour. IP68 is also a static immersion test, but in this test the depth and the immersion time is specified by the manufacturer. So, if one sees the IP68 classification, it should always be accompanied with specification for immersion depth and time. Currently the highest classification IP69/IP69K represents equipment that is protected against high-power steam washers. In practice, there is quite minimal difference in the testing procedure between IP69 and IP69K. IP69 is specified in the IEC 60529 and IP69k in the ISO 20653 standard. Both are generally used, but ISO 20653 is more often used in the automotive industry. When one looks at a sealed connector, there is one big difference between IP69-/IP69K-rated connectors compared with the lower classifications. In IP69/IP69K the sealing material (silicone in most cases) is usually protected by harder material (plastic/metal) since the water spray is so intensive that the seal would easily fail if a direct water spray hits it. To give a rough idea of the IP69 tests compared to lower classification spray tests, here are the important figures: 15 l/min, 100 bar pressure with water temperature of 80 °C.

Also, one important note is that IP classes are only cumulative up to IP66. This means that if a device fulfills IP67 it does not automatically gain IP66 classification, if it is not tested separately. A device designer or system designer should also take into consideration that most of the weatherproof connectors fulfill their ingress protection classification only mated with a corresponding connector. Some connectors can have different ratings for mated/unmated connectors, but if the manufacturer does not specify this accordingly, the assumption should be that the rating is for a mated pair only. So, if some connectors are left unconnected in a system, cap/sealed empty connector must be used to provide for the proper protection of the whole system.

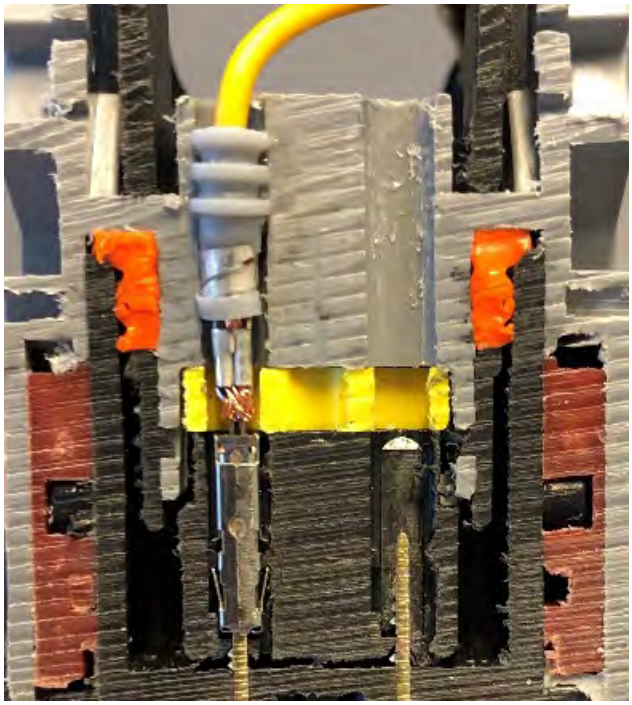


Figure 3: Single wire sealing (SWS) example featuring TE Connectivity's Leavyseal connector (Source: Epec)

Wire-sealing systems

How a wire or a cable seals when it enters the connector is probably the most important sealing interface in a watertight connector. A good practice to mount a control unit is to consider water running along the cables into the connector. Often the placement of the control unit is not optimal, so the connector must be able to withstand water running along the cables.

Multi-pin I/O connectors traditionally have two different approaches for wire sealing: a connector-integrated family seal and SWS (single wire sealing) system. Let us take a closer look at these two connector structures. The name "family seal" evidently comes from the fact that this single seal takes care of sealing all the wires going into the connector. Family seal design incorporates few mm thick sealing part inside the connector. This part is often made of silicone or a similar, very flexible material. There are through holes in this part for each conductor, and sometimes a very thin membrane in each hole (e.g. TE Connectivity's Ampseal connector). The function of this membrane is to plug unused holes (connector contacts). Once a wire with a crimp in the end is inserted into the connector, this membrane will be punctured. Holes in this sealing part are dimensioned smaller in diameter than the conductors to be able to form a seal around the conductor. This type of sealing system is easy to use, since wire seals and blind plugs are all incorporated in the connector. No external wire seals and blind plugs are required. The ease of course comes with some compromises: if different sizes of wires are routed to the connector, a seal hole can be too big for smaller wire gauges and water can flow into the connector through it. Also, if wires are pulled in a 90° angle from the

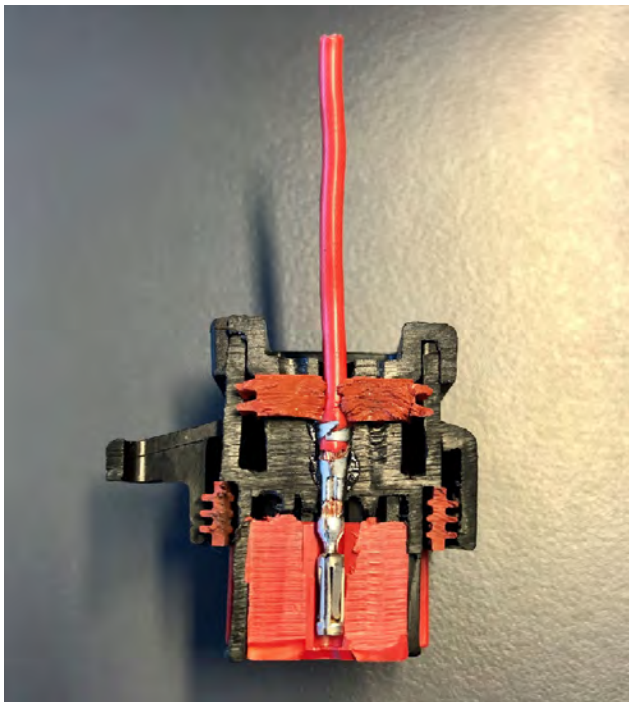


Figure 4: Family seal system example featuring TE Connectivity's Ampseal connector (Source: Epec)

Figure 5: Diesel engine ECU with in-built cable clamps. Source: TE Connectivity

connector it is possible that the hole in this sealing part is stretched to the side and is not able to perform a full 360° seal any longer. Another consideration to keep in mind is that if the wire crimp is not made according to specifications, it could rip the edges of the sealing hole especially if the wire is inserted and retracted multiple times through it. Also, if a wire is removed and a contact is left empty an additional blind plug must be inserted since the membrane is punctured at this point and cannot act as a blind plug anymore.

Single wire sealing system (SWS) is a different approach to this conductor sealing challenge. In a SWS connector (e.g. TE Connectivity's Leavyseal connector) there are no seals in the connector for the wires. Silicone SWS seals are inserted into the wires before the crimp and once crimped, the back part of the crimp holds the SWS seal in place. In the connector, each contact has own cylinder-shaped cavity. As each wire is now sealed with a barrel-like silicone seal crimped into the wire, a 360° sealing surface to the connector body and wire insulation of several mm length is given. This kind of seal can be inserted and retracted from the connector body with no degradation or risk to the sealing performance. Contacts left unconnected must be sealed with blind plugs. Different sized SWS seals are available for different wire sizes, so it is possible to have numerous different size wires going into the same connector without compromising the sealing performance. The downsides of this wire sealing system are: one further assembly step is required in the crimping procedure, and the need of multiple sealing parts and plugs. Fortunately for the machine builder, wire harnesses are mostly manufactured by dedicated harness manufacturers who have automatic application machines for the SWS seals.

Contact system performance

Contact system performance is easily overlooked when a suitable connector in terms of pin count, operation and form-factor has been found. However, contact system is the part of a connector system that has the biggest research and development work put in. Let us take a brief insight into the different properties of any contact system and how these properties relate to each other.

Current carrying capability is dependent on many different parameters, contact size being the most obvious of them. When two flat metal surfaces are placed against each other the current is conducted through the microscopic peaks in the flat metal. In electrical connector contacts, these peaks are exaggerated to mountains and current flow path is directed to these "contact points". The amount and size of these contact points significantly determine the current carrying capability of a contact pair. The size of the contact point is determined by contact normal force, e.g. how much spring force there is to clamp a female contact against the male contact. The greater the force, the larger the contact point and therefore also the higher the current carrying capability.

Connector contacts are usually plated with tin, while higher performance/harsh environment connector contact outer plating is done with silver or gold due to their higher resistance against corrosion. All of the mentioned metals are quite soft. When a contact with high normal force is mated, it always results in deformation of the plating metal. This helps with contact point formation, but it has downsides as well. High normal force and contact metal deformation means very limited amount of mating cycles and high contact retention force. High contact retention force sets challenges for connector cavity blocks and headers. Generally speaking, gold plated contacts can withstand the highest amount of mating cycles. Gold and silver plating are quite equal in terms of current carrying capability, in some applications silver might even be slightly better. All contacts have resistance and resistance creates heat as a function of current. When environment temperature increases, the maximum current of contact pair decreases so that the overall temperature of the connector is kept in the safe zone. This is called connector de-rating.

Connector mounting (ECU design considerations)

A connector defines the ECU design from many different angles: mechanical enclosure is of course defined greatly by the connector(s). PCB (printed circuit board) layout architecture and electro-mechanical design of an ECU is full of compromises, and the application defines which of them can be made and which not.

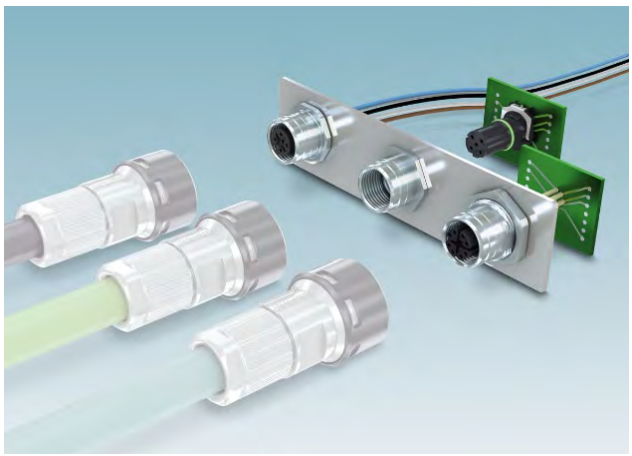


Figure 6: Push-pull connectors with different device interfaces: panel-mount connector with wires, a 2-piece SMD, and thru-hole one-piece connector (from left to right). (Source: Phoenix Contact)

Here are a few points that should be taken into consideration when designing a connector interface to a product:

- Mechanical stress to PCB: Is the connector subjected to high forces caused by thick cables, big and heavy mating connector, high number of mating cycles, etc.? What is taking up this force?
- Sealing system between connector and enclosure: What are the sealing requirements for this interface, and which requirements does the connector set for the enclosure? Of course, this interface can also be deleted completely from the equation by using enclosure-integrated connector body together with a PCB header, or an over-molded solution where the connector pins are molded inside a plastic enclosure with an integrated connector body. These solutions often require close co-creation with the connector manufacturer and might not be the most economical solution for low-volume and medium-volume products. For high-volume products, these solutions can enhance the manufacturability and lower the cost of the connector system at the ECU side.
- Connector space requirements regarding PCB and enclosure. Some connectors use relatively large space on a PCB. Is it possible to sacrifice PCB space for connector support? Is it required to place components near to the connector pins?
- Manufacturability is always a very important part of any design. Two main points in manufacturing related to connectors are the mounting and the electrical connection to the PCB. Often sealed device connectors require both, but in some cases just a solder-joint or a press-fit connection is required for a connector to stay sufficiently attached. Additional mounting methods include (but are not limited to) screws, rivets, snap-in clips, gluing.

Device connectors can be roughly divided into PCB-mounted and panel-mounted with wires. A panel-mounted wire connector is mounted to the enclosure, and short wires from the connector are then connected to the PCB. These wires are often connected to the PCB with a wire-to-PCB connector, but also soldering can be used. The benefit of this type of connector is a full mechanical isolation between the connector and the PCB. This is useful in applications where the connector is subjected to high mechanical forces. This kind of solution is serviceable especially if a wire-to-board connector is being used in the PCB end. Also, the PCB does not determine the placement of the connector, which creates a lot of flexibility for the mechanical design. Downsides of the panel-mount wire connectors are, without limitation, labor intensive manual assembly in production, poor signal integrity for fast signals as well as multiple connection points (connector-to-wire and wire-to-PCB).

In some high-vibration/shock environments it is vital to provide very effective support for the cable to protect the connector from excess forces caused by the cable. Incorporating a cable clamp to the unit design would prolong the connector lifetime. Cable-clamping would also ▷

Figure 7: Ampseal snap-in latch type connector from TE Connectivity (Source: TE Connectivity)

make sure that no water ingress happens in the connector caused by excess pull of the cable. The latter is often a family-sealed connector problem as it was described earlier in this article.

Receptacle

A receptacle or wire-side connector is equally important in achieving the desired performance for a connector system. In most cases a connector can meet the certified IP level only mated with a receptacle, which is assembled with suitable wire seals for the used cables. A receptacle is also the human interface of a connector system. Usability preferences of connector operators must be taken into consideration.

Most ingress protected connectors have a heavy-duty locking mechanism, whereas some device internal connectors rely on friction locking or plastic tabs. Since water and dust will greatly affect the friction of a connector, these kinds of locking mechanisms are not reliable enough in connectors dedicated for harsh environments. For circular connectors, the most common are threads, twisting and push-pull locking. Push-pull locking has become more popular over the last years, and connectors that have traditionally been thread or twist-locked have now push-pull locked siblings.

Rectangular connectors are often locked with a simple snap-in latch, which is a simple and cost-effective solution. But, sometimes it is difficult to open them without special tools.

Also, for high contact number connectors a single snap-in latch is not sufficient to keep the connector straight and locked. Over the last years, lever-locked receptacles have become more common. The benefits of a lever-locked receptacle include the following: visual indication if the connector is fully mated and locked or not. Controlled mating of the connector; leverage to the insertion for the lever, this is especially helpful with high-current connectors where required insertion force is quite high. Additionally, a lever-lockable connector usually provides a possibility to use the safety wire locking to prevent unwanted, unintended, or unsupervised unmating of the connector. The connector is also simple to unmate. It is also highly unlikely that the locking interface becomes destroyed during the unmating.

As the amount of connections in a single connector increases, the wire harness weight also increases and creates stress for the receptacle and the contacts. Especially in environments with constant vibration or high G shocks, the wire-harness supporting clamps are essential. Even if the receptacle can withstand high G and rough vibration environments, a freely hanging wire harness can destroy the plating of wire contacts. Connector manufacturers usually also perform vibration and shock tests for a connector system with cables supported from recommended distance. Clamping the cables to the mounting base is an efficient way to protect the connector from excess forces generated by a heavy cable harness.

Electrical contacts inside the receptacle body must be secured in place. Often these locking mechanisms are plastic tabs or clips, and the releasing procedure can either require a specific contact-release tool or not. If the contact is almost impossible to remove without a designated tool, it is more likely that a removal tool is being used and less damage happens to the connector housing during this servicing procedure.

Connector flammability

Some mounting locations require the materials to be self-extinguishing or flame retardant. These kinds of requirements could be found for example in trucks that have extended sleep-in cabins. For human safety, materials inside the cabin must be self-extinguishing to protect sleeping humans.

The most commonly used flammability classification among mobile machinery connectors is the UL-94 burning test. Most common classifications for plastic connectors are HB (horizontal burning) and V-0 (vertical zero). These tests describe how a material performs when subjected to a burner flame. Basically, HB burns and does not go off by itself and V-0 burns slowly and fades by itself.

PBT (Polybutylene terephthalate) plastic mixed with glass fiber (PBT+GF) is the material most commonly used in sealed mobile machinery connectors. This material's flammability rating is normally UL94 HB but can be modified with additives to the self-extinguishing UL94 V-0 classification. This may sound simple, but there is more to it. Additives make this PBT+GF plastic less elastic and more sensitive to low temperatures and vibration. For this reason, it has proven to be quite difficult to convert existing HB-headers to V-0 without sacrificing vibration performance and operating-temperature range. Therefore, a V-0 requirement for a connector should always be thoroughly grounded.

Figure 8: Leavyseal rectangular lever-locked connector from TE Connectivity (Source: Epec)

What if the header (device side) and the receptacle (wire harness side) are made of different materials? Let us take an ▷

example of a situation where the header is made of HB material and the receptacle has the higher class (self-extinguishing V-0). When mated, the receptacle covers the header almost completely.

Some manufacturers would specify this kind of combination as HB and some as V-0. The UL-94 test is performed with a blow torch separately for both, but this is hardly considered as a real-life scenario. What would then be the real-life scenarios where flammability ratings could be evaluated? In the normal operation, a fault in the electric circuit and a faulty or missing fuse could cause excess heat in the contact pair inside the connector system. This could lead to a fire inside the connector, but the contact pair would probably be almost completely encapsulated by self-extinguishing V-0 receptacle. How about a fire from an external source? The V-0 material is designed to be self-extinguishing and therefore keep the fire from spreading and lessen the total mass of the burning material on a machine. In our example case, the receptacle covers the header, so it protects the lover-flammability-rated header from catching the fire.

Conclusion

Many aspects must be taken into consideration when selecting a connector system for any application. It becomes especially challenging when connectors are subjected to tough environmental conditions and are mounted in machines that have a long lifetime. Such requirements are the standard for mobile working machines. These conditions are challenging for the connectors, and, eventually, it is up to the user to utilize the connector in a specified way.

Besides electronics, connectors are the most important component in any ECU and can even have a significant effect on the performance of the device. A good connector system enables trouble-free operation for many years to come, and a poor one can cause unexplained trouble from the beginning and even restrict the performance specifications of an ECU. ◀

Author

Tuomo Yli-Taipalus
Epec Oy
techsupport@epec.fi
www.epec.fi

CAN Newsletter Online: IP69K-rated

Outdoor applications such as mobile machines are challenging. Often, they require devices in special housing classified by the Ingress Protection (IP) Code standardized in IEC 60529. The first digit indicates the level of protection against parts: 6 means, it is effective against dust. The second digit describes the protection against liquids: 9K means, it is effective against high-pressure and high-temperature spray downs. The CAN Newsletter Online sister publication has reported about the following IP69K-rated CAN-connectable products.

Mobile machine I/Os

Coming in IP69K-rated housings

Data Panel (Germany) offers the XtremeDB family of CANopen I/O devices. They are intended for off-highway and off-road mobile machines.

Read on

IP67 or IP69K rated

J1939 actuator for harsh environments

Thomson (US) introduced the Electrak MD electromechanical linear actuators with embedded J1939 interface. It is suited for mobile off-highway, material handling, and factory automation applications.

Read on

J1939

6D inertial sensor unit for demanding transport tasks

The 6D inertial sensor unit of Honeywell's Tars (transportation attitude reference system) series enables simultaneous acquisition of rotation rate, acceleration, and tilt data for heavy-duty, off-highway, or other special vehicles.

Read on

Up to 14-bit resolution

Rotary encoders approved for SIL 2 applications

The CANopen-connectible TBN/TRN-S4 magnetic encoder series by TWK Elektronik (Germany) received the SIL 2 (safety integrity level) certification by TÜV (German Technical Inspection Association).

Read on

Moving detection

Mining safety kit for working in dangerous environments

To reduce the risk of accidents and equipment damage in quarries, mines, and construction sites, VIA is showcased the VIA Mobile360 AI Mining Safety Kit at the Conexpo-CON/AGG. Dynamic moving object detection is realized via CAN.

Read on

Mobile automation

Encoders, draw-wire encoders, and inclinometers with J1939

For years, Kuebler has been offering a portfolio of rotary encoders, draw-wire encoders, inclinometers, and slip rings suitable for transmitting loads, signals, and data. The company now also offers its sensors with the SAE J1939 interface.

Read on

Limiting local pressure in post-compensated valves

(Source: Bucher Hydraulics)

Bucher Hydraulics has found a way to combine the advantages of pre-compensated load sensing (LS) valves with those of post-compensated flow-sharing valves. CAN and J1939 are also part of this.

The HDS24 flow-sharing valve combines the post-compensated function (can continue to work in undersaturation, or under-supply mode) with the LS local pressure limitation, and enables precision movement in a range of applications. Load sensing valves are well known and popular because they are the best way to control actuators independently of the load pressure. The technology behind this kind of directional valve developed over time, creating two families, the pre-compensated and the post-compensated valves.

The pre-compensated valves are the more common load sensing valves, where the compensator works between the pump pressure and the local section pressure. To do this, the compensator is forced to work with a fixed delta P determined by the compensator spring, and the highest section LS pressure feeds the load sensing pump. The main advantage of this solution is, thanks to a small LS relief valve, of independently limiting the maximum pressure on each section, closing the local compensator and preventing the discharge of the full section flow to tank through port relief valves. Post-compensated valves, or flow-sharing valves, are also load sensing valves, but the local compensator works with the pressure signal from the local section and from the highest LS pressure of the whole valve. In this case the compensator works without spring (or with a very weak spring in some cases).

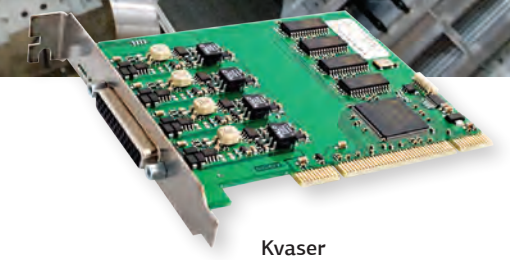
Flow-sharing valves are used in a very large number of applications because the section compensator also can work when the pump cannot supply enough oil (undersaturation). An example is a system with a maximum pump flow of 150 l/min and two simultaneous movements, where the first function needs 80 l/min and the second function 120 l/min (total 200 l/min). In this case, the post-compensated valve is able to work with a smaller delta P on the compensator, and it shares the 150 l/min from the pump to both cylinders in accordance with the following formula:

$$\frac{150}{(120+80)} \times 80 = 60\ l/min$$

to the first cylinder, and 90 l/min to the second.

The proportionality of the two movements (the ratio between the two cylinder speeds) is maintained under all conditions. In the case of a pre-compensated valve, as soon as the system goes into undersaturation the delta P on each compensator drops below the spring force and the compensators open fully, losing any function. In this case, the oil goes to the actuator needing the lowest pressure, just as in a normal open-center directional valve.

CERN's Large Hadron Collider relies on Kvaser PCIcanx boards to connect it's CANopen network.



Kvaser
PCIcanx 4xHS

Communicate with and configure your CANopen application securely using Kvaser's CAN interfaces and software from our Technical Associates.

- Swedish-made hardware, with high performance features and exacting production, ensure long-time reliability. A true fit-and-forget solution.
- Enclosed interfaces or PCI-based boards for embedded networking – the choice is yours.
- A free, universal and forward-compatible API simplifies software integration.
- A global network of technical associates offering CANopen and CANopen FD expertise, software and system-design.

Find out more about how Kvaser can help you create a powerful, tailored solution for your CANopen application here: www.kvaser.com/canopen

KVASER

copley controls · port · Olympus CONTROLS · tke · emotas · Elmo · ADVANCED MOTION CONTROLS · SK2L · Actronic SOLUTIONS

The biggest challenge for a post-compensated solution has been how to limit the maximum pressure on each section. The only way to limit the pressure was by using a secondary port relief valve able to discharge the full section flow to tank with a large waste of flow and energy. What Bucher Hydraulics has achieved with the HDS24 flow-sharing valve is the ability to combine the post-compensated function (also able to work in undersaturation) with the LS local pressure limitation. Up to now, this LS local pressure limitation has only been possible with pre-compensated valves. The HDS24 flow-sharing directional valve is available with mechanical, hydraulic, and electro-hydraulic operators as well as the innovative electro-mechanical CAN network pilot system, to give incomparable flexibility, accurate movements, and the new patented solution for the LS section pressure limitation.

Precise movements

The HDS24 flow-sharing directional valve, with spool stroke of 7,5 mm and spool diameter of 16 mm, gives performances in terms of controllability, stability, and responsiveness of the flow control. In combination with the electro-mechanical actuator, the spool hysteresis is reduced to zero. The very fine positioning of loading devices that need slow and parallel movements is therefore no longer a problem when using the device.

The large number of options and variations does not always result in special, customized parts. The sections, end plates, relief, and secondary valves are already used in other Bucher Hydraulics directional valves, thus optimizing the series production, which makes use of assembly solutions and fully automated test benches. The HDS24 is available for LS and fixed-displacement gear pumps, with or without priority valve for steering, main and LS relief valve, and integrated anti-dumping valve used to stabilize the LS signal between the valve and the variable pump. The secondary-port relief valves are available in versions with fixed or adjustable pressure settings. The spools can be piloted by the mechanical joystick, hydraulic, or electro-hydraulic devices.

Figure 1: The HDS34 with electromechanical pilot system (Source: Bucher Hydraulics)

Furthermore, the company is now able to offer electro-mechanical operation with stepper motor, without need of any pilot pressure. This solution, after many years of development, is in series production on HDS24 and other Bucher valves.

The main advantages of this solution are the speed of spool movement and accuracy of the spool position. The high spool-movement speed leads to a fast response time, so the end user can see the machine responding as quickly as they are moving the joystick. The stepper motor, responsible for the spool-position accuracy, counts every motor step and thus 'knows' the position of the spool throughout the whole spool stroke. The spool and the electric stepper motor are mechanically connected together, so that the hysteresis is zero. Moreover, by means of a proper interface, it is possible to combine the HDS24 with other Bucher Hydraulics flow-sharing valves for higher flows such as the HDS34, LVS12, and LVS18 up ▷

Table 1: Main characteristics

Technical Data:		
Max inlet flow		130 l/min
Max work port A/B flow (13 bar /190 PSI margin)		100 l/min
Supply port P max continuous operating pressure		280 bar
Work port A/B max peak pressure		320 bar
Max internal leakage A/B -> T (at 100 bar / 1430 PSI, 50° C, 23 mm2/s) Lower values on demand	Without port valves With port valves	16 cc/min 20 cc/min
Max contamination level		20 / 18 / 15 - ISO 4406:1999 (NAS 1638 class 9)
Fluid temperature (NBR seals)		-20°C / +80°C
Viscosity operating range	recommended admissible	from 15 to 75 mm^2/s from 12 to 400 mm^2/s
Max number of elements		10
Ambient temperature in operating conditions	With mechanical/hydraulic/ pneumatic controls With electric/ electro-hydraulic devices	from -30 to 60 °C from -30 to 50 °C
Port threads size (A/B):		1/2" BSP, SAE10, M22x1.5 or equivalent
Port threads size (P/T):		3/4" BSP, SAE12, M27x2 or equivalent

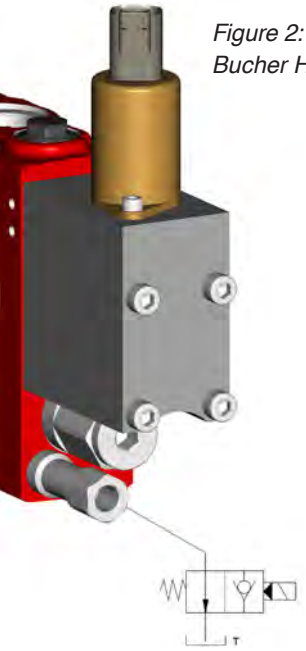


Figure 2: The HDS24 with remote flow cut off (Source: Bucher Hydraulics)

to 250 l/min per section or, by dedicated inlet plate that sets a fixed flow from the variable pump, with open-center valves such as the HDS11 or HDS16.

LS local pressure limitation

The announced option of closing the section compensator through the LS pressure limitation function is now available on the HDS24 flow-sharing valve. The two LS relief valves can be integrated in the section just as on a standard LS pre-compensated valve.

This LS local relief function enables the compensator to close the oil passage to the A or B port when a defined pressure is reached, and independently of the spool position. Compared with a standard port relief valve, this solution has the advantage of closing the oil passage to the outlet ports. The energy losses are less because, with the local compensator in the closed position, the flow through the section is almost zero. With secondary-port relief valves, the full section flow goes to tank at the valve setting, with high heat generation and waste of energy. A further advantage with this solution is that the oil, which is not going to the tank, is then available for other sections, giving faster parallel movements. When the LS relief valve is replaced by an on/off solenoid valve, we can close the compensator with an electrical signal. By connecting the LS port to tank, the local compensator is pushed to the closed position and flow cannot pass to port A or B even if the spool is piloted. This is a feature used in applications where an extra safety function, integrated in the main valve to stop actuator movements, is needed.

CAN network and stepper motor

The Tier IV engines and the forthcoming newer engine generations are forcing all OEMs (original equipment manufacturers) to use more and more electronics on their machines. As a result, the CAN system has been used not just on large construction machines but also more and more on medium and small-sized machines. For this reason and in order to have an easy "plug and play" solution, the CAN-based J1939 higher-layer protocol, is already available on the HDS24 stepper motor version. The stepper motor itself, through the CAN network, can receive and send data such as error information and spool position (from the number of the motor steps) from/to the other electrical devices. The on-board electronics also have the advantage of being able to process information internally and to work in closed loop, sending only the main important information to the other electronic devices, without exceeding the CAN information capacity.

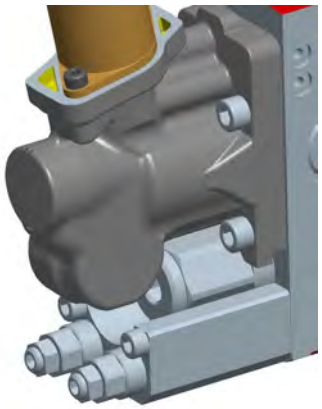


Figure 3: The HDS24 with integrated LS local pressure limitation (Source: Bucher Hydraulics)

On a standard system where the main valve is piloted with PWM (pulse-width modulation), an interface module to translate data from the CAN network to an electrical power signal is needed. Thus, the host controller has to manage the pilot signal to the valve, read the feedback information from sensors, and make the comparison between the two signals, and check if the target position has been reached. All these information exchanges and calculations require CPU (central processing unit) and CAN time, with a risk of overloading the system.

Using the CAN-connectible on-board electronics of the HDS24, many of the necessary items of information are managed internally on the electronic card mounted on each section, and the data items transmitted to the CAN are the only information needed by the system. In this configuration, the data exchanged is brought down to the minimum, and the risk of overloading the CAN network is very limited. ◀

Author

Bucher Hydraulics
info@bucherhydraulics.com
www.bucherhydraulics.com

CAN transceiver choice for improved signal integrity

This article gives an introduction into the signal theory of the energy transmission via a CAN network. Then, some hints for achieving of an improved signal integrity and recommendations for further readings are given.

Impedance analysis of a CAN network

Figure 1 shows a CAN network with a 9,6-m CAN-line (from point 16 to point 17) and possible stub-lines (points 1 to 15). The stub-lines can be selectively connected in order to execute diverse tests.

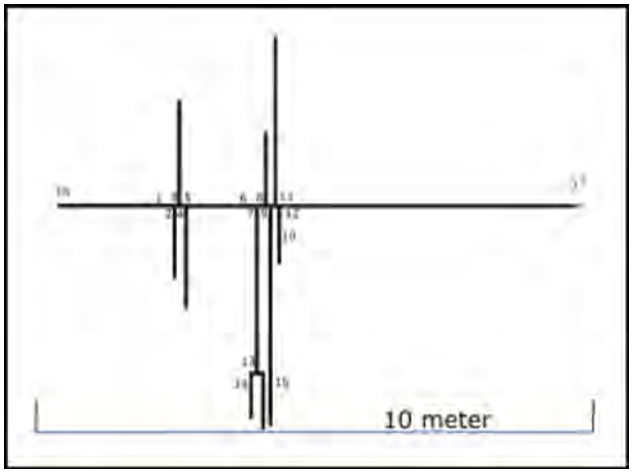


Figure 1: Network topology with all possible stub-lines (see for lengths in Table 1) (Source: Kvaser)

The impedance check is done with the TDR (time domain reflectometer) tool connected at point 16. In the first test the impedance of a point-to-point connection (16 to 17) without stub-lines is analyzed.

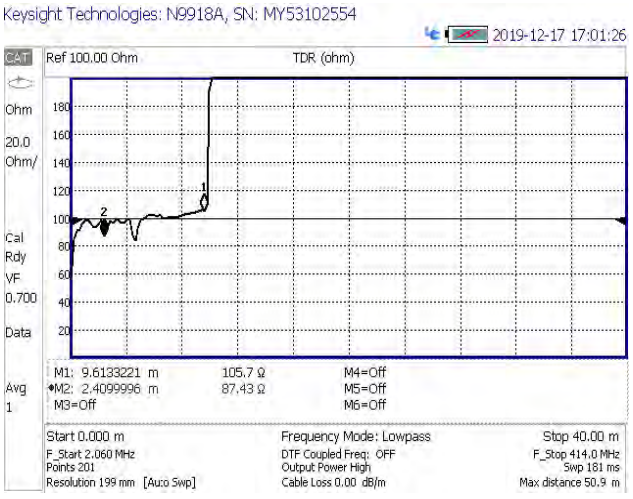


Figure 2: Impedance of a point-to-point connection (16 to 17) (Source: Kvaser)

Figure 2 shows that the impedance value starts at 50 Ohm (standard impedance of most analyzing tools). The tool is connected with a 0,2-m, 50-Ohm coax cable via a 9-pin Dsub connector to the end of the CAT5 cable (point 16) with a characteristic impedance of 100 Ohm. Figure 2 also shows two impedance drops at the locations of possible connection points. These are caused by the small T-connectors without connected stub-lines. The cable ends at point 17 without a termination. Here, the impedance jumps to infinity. The signal delay from point 16 to point 17 lies in the range from 45 ns to 50 ns. The distance is calculated with an assumed wave speed of 4,7 ns/m (70 % of the light speed). With well-designed CAN-transceivers installed directly at the T-connector devices, it would be possible to achieve communication with bit-rates higher than 20 Mbit/s.

By adding of stub-lines to the T-connectors it is possible to see the changes in the impedance characteristics. Table 1 lists the lengths of the cable segments and the stub-lines, which can be connected.

Table 1: Lengths of the cable segments and the stub-lines, which can be connected (Source: Kvaser)

Segment	Length in meters
16 - 1	2.1
2	1.3
3	1.9
4	1.85
5 - 6	1.6
7 - 13	3.0
8	1.4
9	3.9
10	1.0
11 - 17	3.0
12	5.2
14	0.8
15	1.0

In the next test, only the short stub-lines at points 2, 8, 10, 14, and 15 are connected. The impedance characteristic for this case is shown in Figure 3.

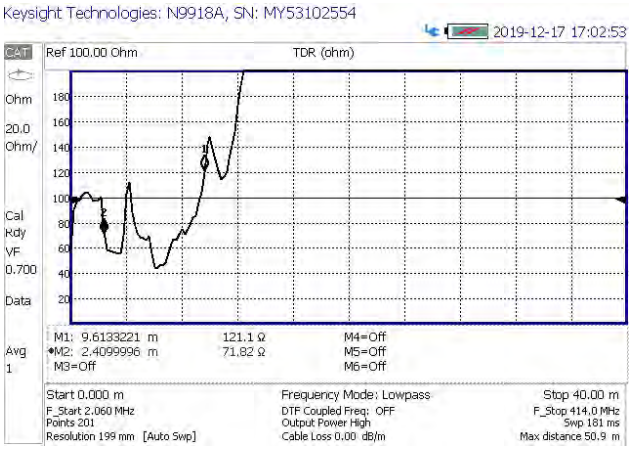


Figure 3: Impedance of the CAN-line with short stub-lines at points 2,8,10,14, and 15. (Source: Kvaser)

The impedance remains at 100 Ohm in the first cable segment (from point 16 to 1). At point 2 (1,3-m stub-line connected) the impedance drops to 60 Ohm. The measurement shows an impedance increase until the next section of the stub-lines connections, where the impedance drops to 40 Ohm. It should also be observed that at the cable end, the TDR measures a sloped (instead of a vertical) line to infinity. This means, that the star-topology prevents the TDR from measuring the correct impedance at the cable end. The impedance measurement using the TDR tool with all connected stub-lines delivers no meaningful results. A TDR tool is designed to find small impedance variations in a point-to-point connection. In a complex network topology it is necessary to use other tools to understand the limitations.

Scattering parameter analysis

If the impedance variation is too large, the high-speed data communication will be prevented. To understand the bit-rate limitation, it is necessary to check the frequency response and to estimate the possible analog bandwidth from that. This is achieved by measuring of the S12 parameters from the energy sender to the receiver. It is required to measure the parameters at several points in order to find out the worst-case frequency limits.

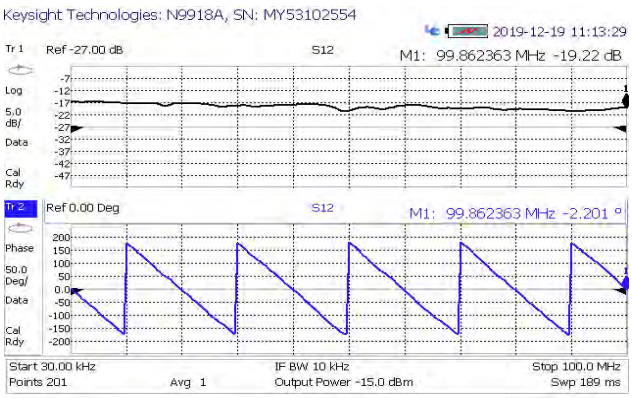


Figure 4: S12 tool measurement at frequencies 0 MHz to 100 MHz in a point-to-point connection (Source: Kvaser)

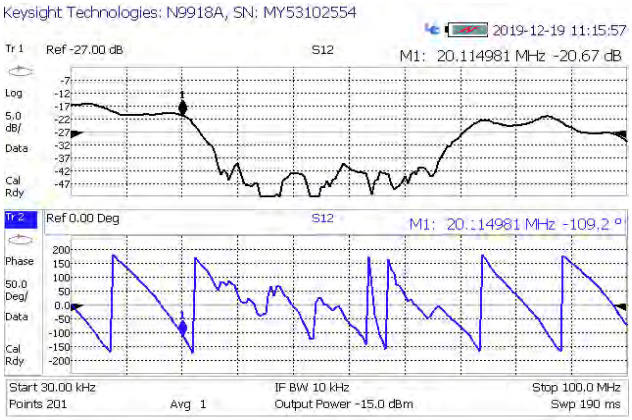


Figure 5: S12 parameters measured at frequencies from 0 MHz to 100 MHz in a CAN network with stub-lines at points 2, 8, 10, 14, and 15. (Source: Kvaser)

The first measurement is done on the 9,6-m point-to-point line. The S12 tool (energy source) connected at point 16 sends a signal with different frequencies, and the same tool measures how much of this energy reaches point 17.

The upper graph in Figure 4 shows the energy loss. The energy drop is 1dB to 2 dB for frequencies up to 45 MHz. From 45 MHz to 95 MHz, energy drops of up to 4 dB are measured. A 3-dB loss equates to a half of the input voltage. In this topology, a 2-V input would result in a 1-V output at 50 MHz.

The lower graph in Figure 4 shows the phase shift between points 16 and 17. At low frequency, the phase shift is zero and at 20 MHz it is 360°, which equates to one whole wavelength. The cycle time at 20 MHz is the inverse of this value, which is 50 ns. If 50 ns is divided by the length of the cable (ca. 10 m), one gets ca. 5 ns/m. At 100 MHz five full cycles between points 16 and 17 are elapsed.

In the next step the short stub-lines at points 2, 8, 10, 14, and 15 are connected.

The upper graph in Figure 5 shows the energy loss in dB. At 20 MHz (cursor) the 3-dB level is achieved at which the signal voltage drops to 50 % of the transmitted level. This particular CAN network blocks all frequencies from 20 MHz to 75 MHz. The frequencies from 75 MHz to 100 MHz are 10 dB lower than the input level, but are not completely blocked. The phase diagram (lower graph)

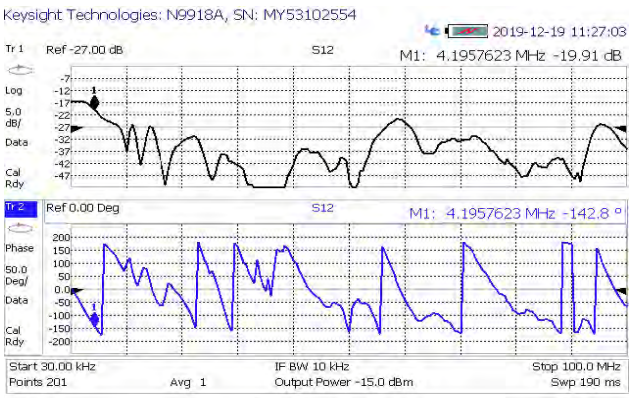


Figure 6: The S12 parameters measured at frequencies from 0 to 100 MHz in a CAN network with all possible stub-lines connected. (Source: Kvaser)

should not change very much, but when the signal level is low, there are increased measurement uncertainties.

The next step is to install all possible stub-lines as shown in Figure 1 with the lengths given in Table 1.

Figure 6 shows the possible analog bandwidth between points 16 and 17. The 3-dB limit is reached at 4,2 MHz (see cursor 1). For frequencies above 4,2 MHz it is not possible to transfer energy from point 16 to point 17. If one repeats this measurement from point 16 to all other stub-line ends there will be similar but differing results. The connection from point 16 to 17 has the highest analog bandwidth of 4,2 MHz. The lowest analog bandwidth of 2,8 MHz was measured between point 16 and the end of the stub-line at point 2.

Relation between analog bandwidth and bit-rate

Data communication depends on the energy transfer over a transmission line. The analog bandwidth defines the highest sinus signal within a certain frequency that can transfer energy over the transmission line. A digital signal is similar to a square wave. A CAN-frame transmitted at 500 kbit/s is similar to a square signal with a frequency of 250 kHz. A cyclic signal can be transformed into the frequency spectrum by a Fourier transformation.

$$Squarewave\ (t) = \frac{4}{\pi} * \sum_{n=1,3,5..}^{\infty} \frac{Amp}{n} * \sin\ (n * \pi * t)$$

Using this information, it is possible to make a list of frequencies and their amplitudes, which, if combined, will shape a square wave signal. Table 2 lists the first six elements for the 250-kHz square wave.

Table 2: The first six elements in the Fourier transformation for a 250-kHz square wave (Source: Kvaser)

Peak	n	Freq kHz	Amp	Amp =1	Power
1	1	250	$\frac{4 * Amp}{(\pi * 1)}$	1.27	1.61
2	3	750	$\frac{4 * Amp}{(\pi * 3)}$	0.42	0.18
3	5	1250	$\frac{4 * Amp}{(\pi * 5)}$	0.25	0.06
4	7	1750	$\frac{4 * Amp}{(\pi * 7)}$	0.18	0.03
5	9	2250	$\frac{4 * Amp}{(\pi * 9)}$	0.14	0.02
6	11	2750	$\frac{4 * Amp}{(\pi * 11)}$	0.11	0.01

Figure 7 shows the frequency spectrum measured at point 17, if a square wave generator (here a 250-kHz square wave) is connected at point 16. The first peak is at 250 kHz (-12 dB) and the second peak is at 750 kHz (-21,6 dB). Taking the power values from the first two peaks in Table 2, it is possible to calculate the power difference between the two peaks in dB. The 10log(0,18/1,61) results in an expected -9,6 dB lower value for the 750-kHz peak.

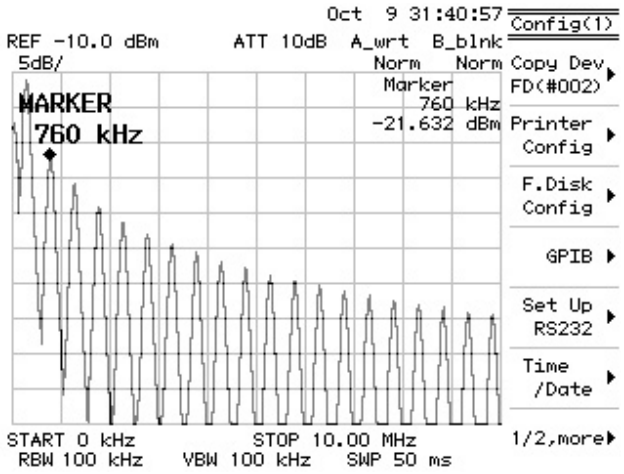


Figure 7: Spectrum for a 250-kHz square wave with a signal-change in 5 ns. (Source: Kvaser)

By taking the measured dB-value (see Figure 7) for the first peak (-12 dB) and subtracting from it the calculated value (-9,6 dB) the expected level of -21,6 dB for the 750-kHz peak is confirmed in Figure 7.

Figure 7 shows that the energy is spread from 250 kHz up to 10 MHz and beyond. The simple solution to reduce energy at higher frequencies is to reduce the slew-rate. The slew-rate is defined as the change of voltage (or other electrical quantity) per unit of time. In Figure 7 the signal-level change is performed in 5 ns. Figure 8 shows the spectrum with the same square wave but with a signal-level change in 200 ns instead of 5 ns.

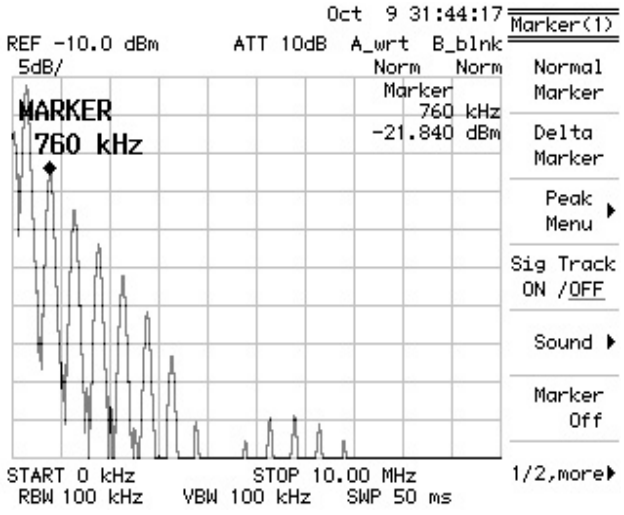


Figure 8: Spectrum for a 250-kHz square wave with a signal-change in 200 ns. (Source: Kvaser)

As shown in Figure 8, the dB-level on the first two peaks is identical for the signal-change in 5 ns and in 200 ns. All the other peaks are lowered. There is almost no energy transmitted at frequencies above 3 MHz.

Figure 9 and Figure 10 show the analog signal with the two different slew-rates on a point-to-point connection (16 to 17) without stub-lines. The top signal is generated at point 16 and the lower signal is measured at point 17.

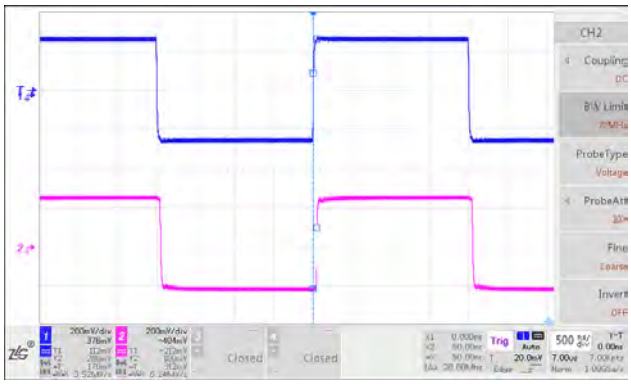


Figure 9: 250-kHz square wave signal with a signal-change in 5 ns on a point-to-point connection without stub-lines. (Source: Kvaser)

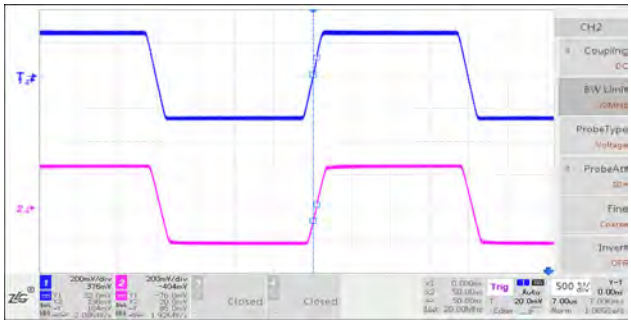


Figure 10: 250-kHz square wave signal with a signal-change in 200 ns on a point-to-point connection without stub-lines. (Source: Kvaser)

It can be concluded that there is no problem to have a high slew-rate (signal-change in 5 ns) and bit-rates up to 25 Mbit/s in a point-to-point connection. As shown in the TDR and S12 measurements, much lower possible bandwidth has to be expected in complex CAN topologies. Figure 11 and Figure 12 show the analog signal with the two different slew-rates on a CAN network with all possible stub-lines connected. The top signal is generated at point 16 and the lower signal is measured at point 17.

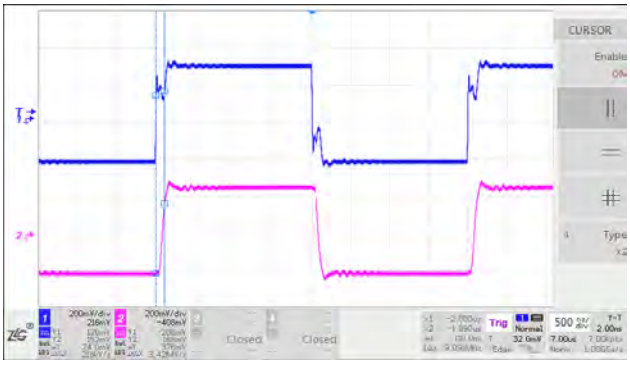


Figure 11: 250-kHz square wave signal with a signal-change in 5 ns on a CAN network with all possible stub-lines connected. (Source: Kvaser)

As seen in Figure 11, there is an LP-filter (low-pass), which prevents the higher frequencies from reaching the point 17. The expected signal delay of 50 ns (Figure 15) is now 110 ns. There is also a lot of high-frequency ripple in the signal.

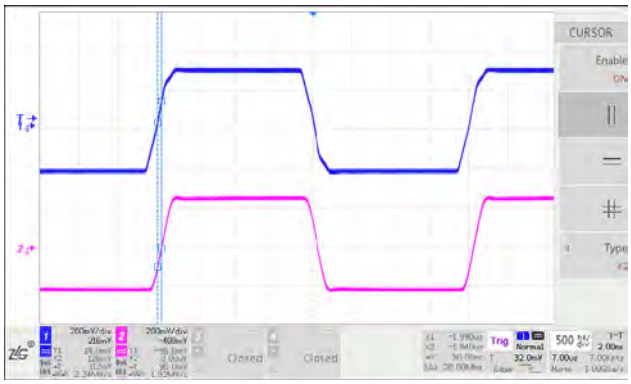


Figure 12: 250-kHz square wave signal with a signal-change in 200 ns on a CAN network with all possible stub-lines connected. (Source: Kvaser)

The simple solution to remove the high-frequency energy is to reduce the slew-rate (i.e. to increase the time of the signal-change).

Figure 12 (signal-change in 200 ns) shows almost identical characteristics as Figure 10 (point-to-point connection). The edge delay is also 50 ns as no high-frequency energy has to be absorbed.

CAN-bus signaling

Previously the signal theory for transmission of the energy via a CAN network with different numbers and lengths of the stub-lines was described. These measurements are carried out with a signal source and a receiver, which is impedance-matched to the transmission line. A standard CAN-transceiver is not impedance-matched to the transmission line. As a transmitter, it behaves as a low-impedance voltage source, and as a receiver, it behaves as a high-impedance connection point, requiring that the energy is absorbed in the termination resistors. This means that the signal shape varies depending of the signal transmission direction when standard CAN-transceivers are used.

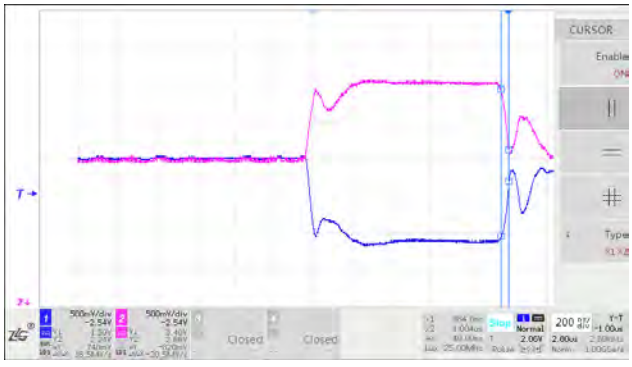


Figure 13: Dominant signal at point 17 in a CAN network with all connected stub-lines. Bit-rate is 1 Mbit/s. (Source: Kvaser)

Figure 13 shows a dominant bit measured at point 17 in the CAN network with all connected stub-lines. There is a negative reflection at the recessive-to-dominant edge causing a signal drop after 100 ns, but the signal becomes stable after 250 ns.

At the dominant-to-recessive edge a relatively large positive reflection can be seen. Figure 14 shows a dominant bit at the same topology but with a bit-rate of 500 kbit/s. The bit length is increased, but the edge shapes do not change because the edge shapes depend on the slew-rate and not on the bit-rate. The cable delay is 50 ns and all reflections back to the point 17 are returned after 100 ns. After another 100 ns the system is almost on a stable level.

At low bit-rates such as 1 Mbit/s, the bit-time is sufficiently long to consider the signal as a DC-signal (direct current). If the bits become shorter than 250 ns, the energy would oscillate from one edge to the next edge. Thus, a bit-rate above 4 Mbit/s would modify the shape of the edges and the signal has to be treated as an AC-signal.

The cursors in Figure 14 show that the signal-change at the dominant-to-recessive edge is performed in 40 ns. At 500 kbit/s the bit-length is 2000 ns. It would cause no problem to increase the signal-change time from 40 ns to 200 ns. This would result in the fact that all oscillations at the edges would disappear. The ringing at the dominant-to-recessive edge is not a problem for the CAN-related communication because any extra dominant-to-recessive edges are ignored by the CAN-controller.

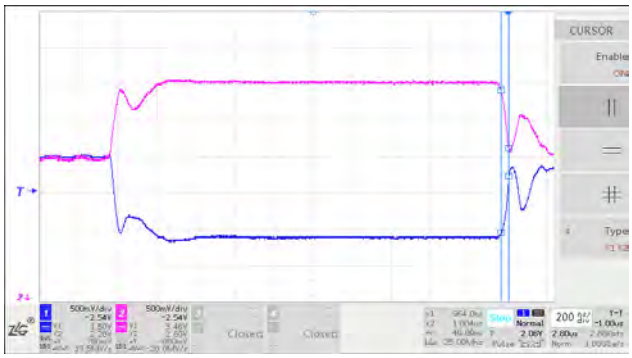


Figure 14: Dominant signal at point 17 in the CAN network with all connected stub-lines. Bit-rate is 500 kbit/s. (Source: Kvaser)

Figure 15 and 16 show the same measurements over multiple bits by setting the oscilloscope in persist mode. Figure 15 shows the signal at 1 Mbit/s. The most clearly seen signal is the most common signal shape. There is also a signal with a higher amplitude that begins earlier and starts with a spread in time. This is the ACK-bit (acknowledge), which has a higher amplitude because it is sent by all CAN-frame receivers simultaneously. The spread in the recessive-to-dominant edge of the ACK-bit is caused by the fact that the receivers start the bit-transmission relative to the internal re-synchronization on a received CAN-frame. The individual re-synchronization of each CAN device is delayed by the CAN-transceiver and the appropriate cable distance. The ACK-bit has a large over-shoot because the energy is sent from several sources, adding up to a high voltage at the edge.

Figure 16 shows almost the same signal shape as seen in Figure 15. The difference is that there are two levels between the normal bit level and the ACK-bit level. This is the arbitration level where two (or more) devices are sending the arbitration bits simultaneously.

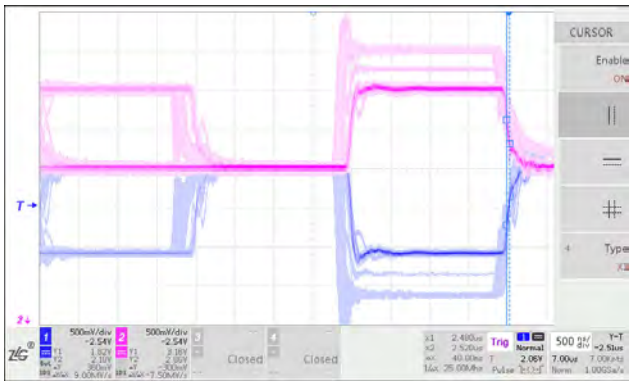


Figure 15: Dominant signal at point 17 with oscilloscope in persist mode. Bit-rate is 1 Mbit/s. (Source: Kvaser)

This arbitration level also exists at 1 Mbit/s. This level is somewhat higher than the normal bit level, but not that high as the ACK-bit sent by all devices. There is also a slightly larger spread at the start of the ACK-bit. This is caused by using a twofold TQ-length (time quanta) at 500 kbit/s than at 1 Mbit/s. Using the same TQ-length at 500 kbit/s would provide an edge shape that is similar to the shape at 1Mbit/s.

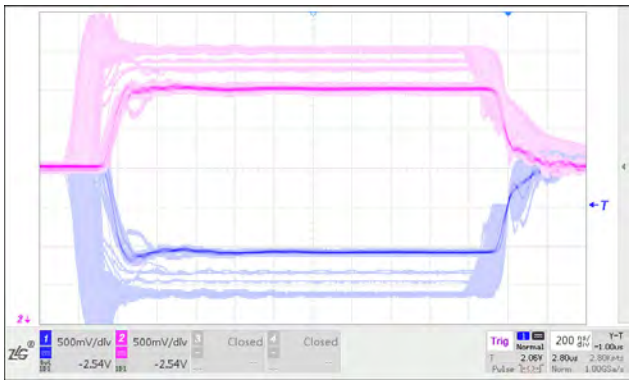


Figure 16: Dominant signal at point 17 with oscilloscope in persist mode. Bit-rate is 500 kbit/s. (Source: Kvaser)

Conclusion

The best way to improve the CAN signaling is to use a network topology with the shortest possible stub-lines. If this is not possible, it is necessary to get knowledge for the problem understanding and to find out the limitations set by a given network topology.

The most important issue to achieve a good signal quality is to optimize the slew-rate for the actual network topology. Slew-rate adjustment is supported by the most CAN-transceivers, but it requires the use an adjustable resistor (current). This is a suitable solution for a mass-produced vehicle with a fixed number of ECUs (electronic control units) and a fixed network topology.

The ideal solution would be to use CAN-transceivers that allow adjustment of the slew-rate to the bit-rate and to the actual network topology.

Usage of capacitors and inductors between the CAN-transceivers and the CAN wires should be avoided. Chokes are useful to avoid the influence of the unbalanced current and the high frequencies on the CAN-transceiver. A better solution is to prevent this problem by selecting a CAN-transceiver with a slew-rate adjustment and the ability to match the current between the CAN-High and CAN-Low lines.

High frequency handling and theory requires a complex knowledge. The following books explain the physics and math for the transmission lines. For an engineer, the book “Signal Integrity Simplified” is highly recommended. It contains a lot of examples to gain an intuitive understanding of the high-speed signal. The author, Eric Bogatin, made also a lot of educational videos. The other book that I recommend is “High Speed Signal Propagation: Advanced Black Magic” by Drs. Howard Johnson and Martin Graham. This is more theoretical and a little harder to read, but covers material that is not described in Bogatin’s book. ◀

Author

Kent Lennartsson
Kvaser
kent@kvaser.com
www.kvaser.com

Implementing a CANopen injector FSA

An injector compliant with the CiA 425-2 implements a CANopen NMT (network management) slave FSA (finite state automaton) and an injector FSA. The coupling possibilities of the both FSA are analyzed in this article.

The CiA 425 specification available from CAN in Automation (CiA) is a CANopen application profile for medical diagnostic add-on modules. The part 2 (CiA 425-2 [3]) specifies the CANopen interface of an injector. The document does not explicitly specify the relationship between the injector's CANopen NMT slave FSA and the injector FSA. It states that the both automata are only loosely coupled, as an injector provides local control functions (local safety requirements) even if communication between the injector and its communication partner (scanner) breaks down. The latter is commonly known as a communication loss. CiA 425-2, nevertheless, specifies for the injector FSA selectable safety-behavior options in case of a communication loss. Similarly, the CiA 301 ([1], base CANopen specification) specifies options for the CANopen NMT slave FSA.

This article tries to establish a relationship between the two state machines, if a communication loss occurs. Achievable and realistic relationship with currently available options (see CiA 425-2 and CiA 301) is analyzed regardless of injector's local safety requirements.

CANopen NMT slave FSA and injector FSA

The CANopen NMT slave FSA (see CiA 301) models the behavior of the communication function unit on a CANopen device. The injector FSA (see CiA 425-2) models the application behavior of the injector device. The latter utilizes its underlying CANopen communication function unit to communicate with its counterpart CANopen communication function unit on a scanner device. In a CANopen network consisting of an injector and a scanner, the injector is the NMT slave, and the scanner is the NMT master (specified in CiA 425-1 [2]). Thus, the injector implements an NMT slave FSA, which is controlled by the scanner. This is valid regardless of the injector's operation mode.

Which injector functions can be controlled by the scanner depends on the currently active operation mode (see CiA 425-2), namely monitor, tracking, or control mode. The scanner can choose in which operation mode the injector shall operate. In other words, the scanner decides how much control it has over the injector FSA.

In the monitor mode, the scanner has no control over the injector FSA. The injector and the scanner start and operate independently. But the injector notifies the scanner about its current state (therefore the monitoring).

Compared with the monitor mode, the tracking mode is different in the following two points:

- The injector cannot enter the system ready state until the scanner informs the injector that it is also ready.
- If the injector starts locally, the scanner is triggered to start itself (therefore the tracking).

Consequently, the only difference between the monitor mode and the tracking mode is the way in which the injector and scanner start. In the monitor mode, the injector and scanner start separately. In the tracking mode, the injector starts locally, which then triggers the scanner to start automatically. But, the scanner prevents the injector from entering the system ready state when it is not ready itself. This guarantees that the scanner and the injector can start at the same time. This is the only control function, which the scanner has over the injector FSA in the tracking mode.

In the control mode, the scanner takes full control over the injector FSA. For example, when the scanner starts, it sends a command to start the injector as well. However, due to the different safety control requirements in the injectors implemented by the OEMs, the scanner's control over the injector FSA is more restricted than it is allowed in the CiA 425-2. For example, scanner's request to arm the injector (i.e. remote arming by transitioning state from idle to injector ready) may be denied by the injector, even though the state transition is remotely allowed per CiA 425-2.

As described above, in the tracking mode, the scanner is triggered by the injector to start. In the control mode (in addition to being triggered by the injector) the scanner started by the operator, can also command the injector to start at the same time. As far as the starting (entering into the procedure-executing state) is concerned, it is a one-way issue in the tracking mode, but a both-way issue in the control mode.

The scanner command (i.e. the control word, including selection of injector's operation mode and controlling the injector FSA) is received by the injector through RPDO 1 (receive process data object). The injector state

Table 1: Value definition for object 1029_h (Source: CiA 301)

Value	Meaning
0x00	Change state to NMT pre-operational if the current state is NMT operational
0x01	Stay in the current NMT state.
0x02	Change state to NMT stopped regardless of the current NMT state

Table 2: Injector FSA reaction to a communication loss (Source: Bayer)

Case	Injector State	Mode		
		Monitor	Tracking	Control
1	Idle configuration Ready configuration Injector ready System ready	No effect	• Transition automatically to idle state, • Change mode immediately to monitor, and • Set global bit-10 to 1 (scanner not ready)	
2	Procedure executing Hold Hold configuration Injection completed	No effect	• Remain in current state or transition to procedure interrupted state (see Table 3), • Change mode immediately to monitor, and • Set global bit-10 to 1 (scanner not ready)	

notification (i.e. the status word, sent either as a response to the scanner control word, or due to a state transition on the injector) is sent to the scanner through TPDO 1 (transmit PDO). This implies that the injector NMT state must be NMT operational, as it is the only NMT state in which a PDO communication is possible. In other words, the injector FSA "lives" in the NMT operational state, regardless of its operation mode. This is the case until the communication breaks down between the injector and the scanner (commonly known as a communication loss).

Communication breakdown

Communication loss happens in two situations: loss of the heartbeat from either side (or both sides), and CAN bus-off on either side, which is eventually detected from the other side as a loss of the heartbeat. So, in the context of the injector FSA, communication loss comes down to two scenarios: loss of the scanner heartbeat and CAN bus-off on the injector.

According to ISO 11898-1 [4], a CAN node is always in one of the three bus error states, namely error-active, error-passive, or bus-off. The error state transitions are controlled by the FCE (fault confinement entity) within the node. A node is said to be in the bus-off state when it is switched off from the CAN bus by the physical layer upon request from the node's FCE. In the bus-off state, the node can neither send nor receive any frames (messages), and can only recover from the bus-off state upon request from the user. The user request here usually means hard- or soft-reboot of the node.

According to CiA 301, loss of the heartbeat is a heartbeat event. Here the heartbeat consumer declares a heartbeat error if no heartbeat messages are received from the heartbeat producer within the pre-determined consumer time (defined in object 1016_h). What has happened to the heartbeat producer is unknown to the heartbeat consumer. The heartbeat producer could have simply failed to send heartbeats in time (but otherwise have been functioning properly) or it could have gone bus-off.

In the injector's object dictionary, object 1029_h (error behavior) informs the scanner what happens with the injector's NMT slave FSA when communication loss occurs. CiA 301 defines three possible options for this object (see Table 1).

If the communication loss is caused by the loss of heartbeat, all three options are possible. But if the communication loss is caused by the injector going bus-off, the first option (0x00) seems to be the only achievable one. The reason is that the NMT pre-operational will be the resulting state after injector's recovery from the bus-off state. It is the only NMT state to which an NMT slave (injector) can be rebooted to.

When the communication loss occurs, CiA 425-2 specifies for the injector FSA the transitions as shown in Table 2. These depend on the current operation mode and the injector state.

The object 6006_h (communication lost) is defined in CiA 425-2 with four possible options (see Table 3).

In the monitor mode, the injector FSA will not be affected by a communication loss regardless of what state it is in. In the tracking or control mode, the injector (regardless of its current state) can choose to change to the monitor mode immediately or to remain in the current mode. But the injector FSA will be impacted by its current state. If the current state is one of the pre-procedure-active states

Table 3: Value definition for object 6006_h (Source: CiA 425-2)

Value	Meaning
0x00	Current injection shall abort immediately, but the injector shall remain in current mode
0x01	Current injection shall complete, and the injector shall remain in current mode
0x02	Current injection shall abort immediately, and the injector shall change to monitor mode immediately
0x03	Current injection shall complete, but the injector shall change to monitor mode immediately

Table 4: NMT slave FSA and injector FSA relationship while normal operation (reliable communication) (Source: Bayer)

Scanner Control Over FSA		
Injector FSA		NMT FSA
Monitor	No control	Full control
Tracking	No control other than: • Able to prevent injector from entering system ready state • Scanner's start triggered by injector's local start	
Control	Full control including: • Able to prevent injector from entering system ready state • Scanner's start triggered by injector's local start • Able to start injector at same time as scanner starts	
Relationship between Injector FSA and NMT FSA		
Injector FSA exists and lives in NMT operational state		

Table 5: NMT slave FSA and injector FSA relationship during a communication loss (Source: Bayer)

Injector FSA			NMT FSA
Monitor	No effect		Injector moves to NMT pre-operational state
Tracking Control	If current state is:	Injector reacts by:	
	Idle configuration, Ready configuration, Injector ready, or System ready	• Changing mode to monitor, and • Moving state to idle	
	Procedure executing, Hold, Hold configuration, or Injection completed	• Changing mode to monitor, and • Aborting or completing injection	
Relationship between Injector FSA and NMT FSA			
Injector FSA exists and lives in NMT pre-operational state			

(case 1 in Table 2), the injector will disarm (by transitioning to the idle state). But if the injector is in one of the procedure-active states (case 2 in Table 2), the injector will either stay in the procedure-executing state to complete the injection, or transit to the procedure interrupted state to abort the injection.

The objects 1029_h and 6006_h make it clear to the scanner that, during a communication loss, the injector FSA may live in the NMT pre-operational, NMT stopped state or in the NMT operational state. However, injector's staying in the NMT operational state (if communication loss occurs) means that TPDO 2 and TPDO 3 will still be transmitted by the injector at the rate set by the scanner. But, these TPDOs are most likely to fail, eventually resulting in the error of CAN Tx buffer overrun on the injector. This will force the injector to change its NMT state anyway (i.e. to stop the TPDOs), in violation of the 0x01 option (stay in the current NMT state) set in the object 1029_h sub-index 01_h. Therefore, remaining in the NMT operational state in case of a communication loss is not a realistic option.

The state and mode transitions make more sense if the communication loss is caused by the heartbeat loss. If the injector goes bus-off, it will go to the idle state and the monitor mode after a reboot (recovering from the bus-off). But the CiA 425-2 does not differentiate between the heartbeat loss and the bus-off as far as the objects 1029_h and 6006_h are concerned.

Therefore, in order to satisfy both cases (heartbeat loss and bus-off), the most realistic options for object 1029_h sub-index 01_h seems to be 0x00 or 0x02. For the object 6006_h it seems to be 0x02 or 0x03 (if the injector has a separate sub-system that can go bus-off without interrupting the injector). This means that during a communication loss, the injector FSA, with the mode changing to monitor, most likely lives in the NMT pre-operational state.

When the communication loss recovers, the scanner reconnects with the injector, and switches the injector back to the NMT operational state, so that the injector FSA will be living in the NMT operational state again. But the injector may deny the connection until the current injection has completed (if 6006_h has the option 0x01 or 0x03) and the injector state has moved to idle (either automatically or by a user interaction).

Summary

The relationship between the injector's NMT slave FSA and the injector FSA is summarized in the Table 4 (normal operation) and Table 5 (communication loss). ◀

References

[1] CiA 301: CANopen application layer and communication profile, v. 4.02

[2] CiA 425-1: CANopen application profile for medical diagnostic add-on modules, Part 1: General definitions, v. 2.1

[3] CiA 425-2: CANopen application profile for medical diagnostic add-on modules, Part 2: Injector, v. 2.3

[4] ISO 11898-1: Road vehicles – Controller area network (CAN) – Part 1: Data link layer and physical signaling, 2015

Author

Ron Kong
Bayer US LLC
ron.kong@bayer.com
www.bayer.us

Control device platform for small batch development

In the initial phase of development, companies must tailor control units specifically to the respective test bench or prototype. These units can often only be used once. Due to a customizable controller, soon they will be variable enough for further projects.

During the concept development and testing phase, prototypes and test systems typically require electronic components, which have to be developed and manufactured especially for this single use. This generates high costs and the extensive amount of the required time delaying product launch. The costly initial phase rules out a rapid response to changes at short notice. This is a serious disadvantage, particularly for the fast-paced automotive industry. In order to accelerate this step in the process while simultaneously creating space for the flexibility required, the development service provider Arrk Engineering has chosen a different path: Numerous use cases were used to identify frequently requested functions and to develop the relevant components for a modular control device concept, the Build Rapid System (BuildRS). Thanks to this, it is now possible to create measuring and control systems for a wide variety of applications faster and more affordably than before: The components with the functionality required must only be taken from and combined with a pool of existing hardware and software components.

"For many years, we have supported automobile manufacturers and suppliers as their strategic development partner," explained Zarko Tomic, team leader for software development at Arrk Engineering. "Throughout the course of predevelopment projects, component tests and test series, certain applications emerge time and again. These include the transfer of data and signals via bus systems or wireless networks, the evaluation of sensors and control of motors." Generally, control devices are developed specifically for these cases – leading to high time and cost requirements due to the low quantity required. Alternatively, teams may resort to universal control devices which are usually oversized for the specific application. Both extend development times and costs, which is a disadvantage in view of the fast pace of the automotive industry. "We began from this starting point: Instead of repeatedly developing new control units for test devices and prototypes which can only be used for single projects, we wanted to specify components – like Lego bricks – which can be assembled in a few, easy steps to create a unique and freely adaptable control device for the relevant application," continued Tomic.

In-house development

Arrk Engineering developed the underlying hardware kit and software in-house. "This was necessary because comparable systems on the market were either too large and cost-intensive for our purposes or were targeted

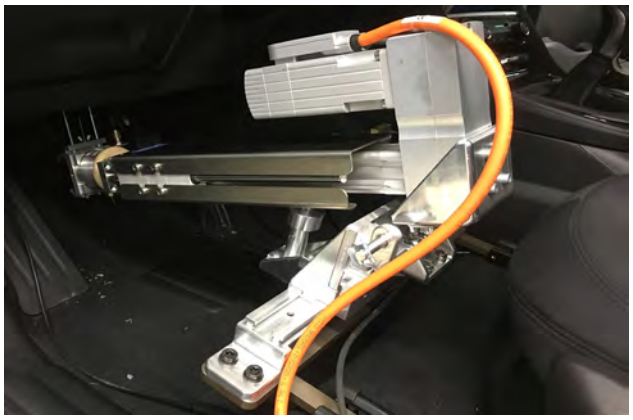
Figure 1: BuildRS comprises two circuit boards; The controller board connects to other devices via CAN and forms the starting point for the unit; the peripheral unit specifies the actual function of the control device (Source: Arrk Engineering)

at electronics hobbyists. As a consequence, they were inefficient and unstable," noted Tomic. Another problem often arose when it was not possible to directly integrate these models into the software, leaving Arrk Engineering unable to perform any comprehensive changes. This prevents the system from being adapted and extended flexibly, which is of great importance in a wide range of projects.

While developing the new control device concept, Arrk Engineering chose an approach as systematic as it was pragmatic: "After the platform concept was established, a new component for our modular control device platform was developed for all subsequent projects requiring a function, which had not previously been necessary," Tomic recalled. Thus, in the course of the past year, the idea has given rise to a comprehensive modular system – which has continued to grow, much like the customer requirements conveyed throughout the course of numerous projects. Meanwhile, Arrk Engineering can refer to a pool of functions for different possible applications, such as digital or analog inputs and outputs, engine control, and Bluetooth or wireless transmission, and numerous supported bus systems. The portfolio is consistently developed further.

Modules with adaptable software

The system, which Arrk Engineering has named BuildRS, comprises two circuit boards: The controller board connects to other devices via CAN and forms the starting point for the unit; the peripheral unit specifies the actual function ▷



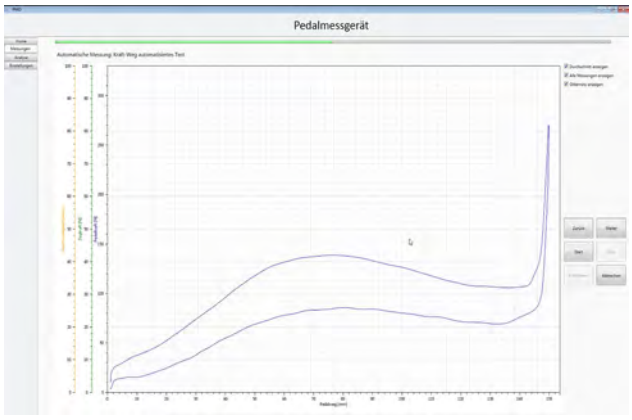


Figure 2: Control units for measuring instruments and test systems are created. One example is a treadle measuring device for determining treadle stroke and force (Source: Arrk Engineering)

of the control device. "If, for example, it is necessary to switch from digital to analog inputs or from one sensor to another due to a change in customer requirements, we only have to change the peripheral board," explained the team leader. "The customer benefits from the quick response time, lower costs, and increased system stability." There are two options for fitting the boards together: They can be arranged next to each other for easier access to all components, or stacked neatly on top of one another to make the system less vulnerable to external influences. Depending on customer requirements, other connections are possible in addition to CAN by means of an additional module, such as LIN, Bluetooth, or wireless network.

The software architecture for the BuildRS platform is also modular: "The software and hardware have a constantly growing portfolio of possible functions which correspond to the functionality of the peripheral board," explained Tomic. The system can be configured or reprogrammed via the CAN interface. This implies that, in the event of a function change, often only software reconfiguration is required and there is no need for complete reprogramming. As this is a matter of in-house development by Arrk Engineering, the company has full access to the source code. In this way, it is possible for both hardware and software to be adapted to customer requirements quickly and effectively at any time, ensuring that hardware is utilized to its full potential.

Figure 3: „Our development service for the treadle measuring device's controls comprised a selection of suitable BuildRS boards, software setup, and function configuration – the time taken amounted to a few hours," explained Zarko Tomic (Source: Arrk Engineering)

Possible applications for concept development and testing

BuildRS offers a wide range of possible applications relating to concept development and testing. In this way, the modules can, for example, support the electrification of individual prototypes. "For instance, BuildRS was used in a seat box for seat adjustment – as a motor driver and for digital signal transmission," explained Tomic.

The durability of the modules is a great advantage here: They can be stacked or built into a housing and used for years to come. This also makes them suitable as long-term test subjects or demonstration samples, such as for fairs.

They can also be used for small batches or test devices. "One example of this is a treadle measuring device which we developed for the automotive industry," explained Tomic. The aim of this testing device is to both measure and analyze treadle stroke and force, such as for brake pedals, clutch pedals, and gas pedals. One module assumes the task of managing the values of both sensors, translating these into digital signals and transmitting them for further processing. A second module is part of the remote control which allows the system to be controlled from a distance. The customer benefits from the system's modularity: "Our development service for controls comprised, in this case, a selection of suitable BuildRS boards, software setup, and function configuration – the time taken amounted to a few hours and costs were low," said Tomic.

But the BuildRS also offers advantages for budget and time-planning as part of workstations during concept testing because, unlike in other cases, it is not necessary to develop a new control device. At the same time, it can be more freely adjusted by the customer, unlike standard units, giving them the option of using the BuildRS multiple times. Since the individual peripheral boards are replaceable and can be switched easily, it is quick and comparably affordable to purchase new functions. The new board can be started up via the CAN connection using the modular basic software which is installed in the controller board. In this way, the user is able to independently adjust the function of the control unit and integrate it into the workstation. "BuildRS can be used for all types of prototypes and small batches. This allows development costs to be drastically reduced per terminal," concluded Tomic. ◀

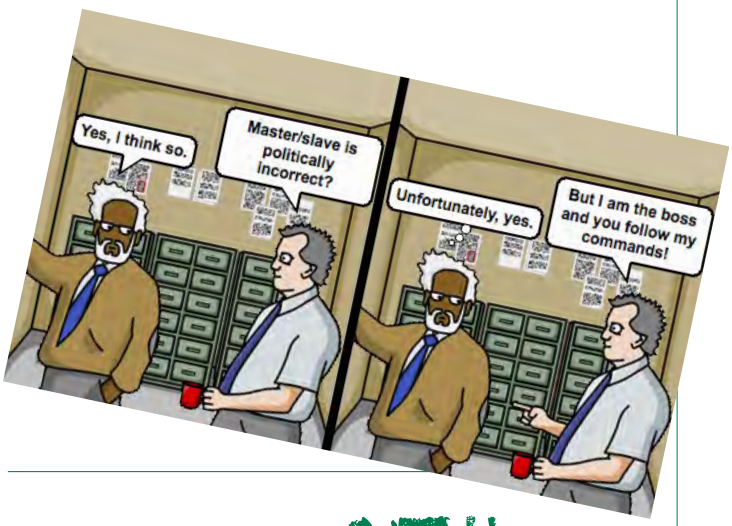
Author

Annika Mahl
Arrk Engineering
info@arrk-engineering.com
www.arrk-engineering.com

Facts & Figures

700th CiA member

Rhode & Schwarz is the 700th member of the nonprofit CAN in Automation (CiA) international users' and manufacturers' group. More than 85 years ago, Dr. Lothar Rohde and Dr. Hermann Schwarz founded the Munich-based company. The company has more than 12 000 employees worldwide and offers oscilloscopes, which diagnose Classical CAN and CAN FD networks.



Emotas' CANopen protocol stack has been assessed and endorsed by ST Microelectronics to become the first MadeForSTM32 approved CANopen software for STM32 microcontrollers.

17th iCC

Due to the novel coronavirus, the international CAN Conference 2020 has been postponed. The new date is June 15 and 16, 2021. Location is still Baden-Baden in Germany.

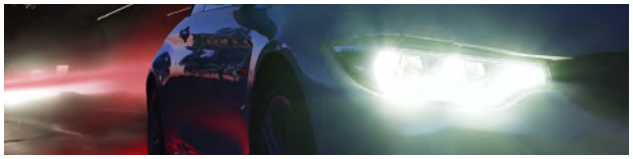
Of course, the authors will update their presentations. The iCC 2020 proceedings are already available for purchase.

Transceiver naming

CiA has agreed on names for two transceiver approaches: CAN SIC transceiver (CiA 601-4) and CAN SIC XL transceiver (CiA 610-3). Recommended are the terms CAN high-speed (up to 1 Mbit/s) and CAN FD transceivers (up to 5 Mbit/s) for ISO 11898-2:2016 compliant components.

CAN FD light

CiA has established a Special Interest Group specifying the CAN FD light protocol, which is intended for price-sensitive networks. Typical examples include the communication within sophisticated vehicle headlights. CAN FD light nodes do not need an oscillator and transmits only on request by a CAN FD node.



Density of CiA members

Switzerland's area is 41 285 km² and there are 39 CiA members headquartered. This results in 1 058 km² per member and is the highest CiA member density worldwide. Germany follows closely with 1 195 km² per member (area 357 582 km² and 299 members). Regarding the CiA member density per population also Switzerland is ahead: 219 747 citizens per member. Germany counts 278 149 citizens per member.

CAN in Automation

The non-profit CiA organization promotes CAN and CAN FD, develops CAN FD recommendations and CANopen specifications, and supports other CAN-based higher-layer protocols such as J1939-based approaches.

Join the community!

- Initiate and influence CiA specifications
- Get credits on CiA training and education events
- Download CiA specifications, already in work draft status
- Get credits on CiA publications
- Receive the exclusive, monthly CiA Member News (CMN) email service
- Get CANopen vendor-IDs free-of-charge
- Participate in plugfests and workshops
- Get the classic CANopen conformance test tool
- Participate in joint marketing activities
- Develop partnerships with other CiA members
- Get credits on CiA testing services

For more details please contact CiA office at headquarters@can-cia.org

www.can-cia.org