Ethernet links CANopen domain controllers

Structuring the vehicle network architecture into separate domains becomes highly meaningful. A powerful unit can be used to perform all domain-related tasks.

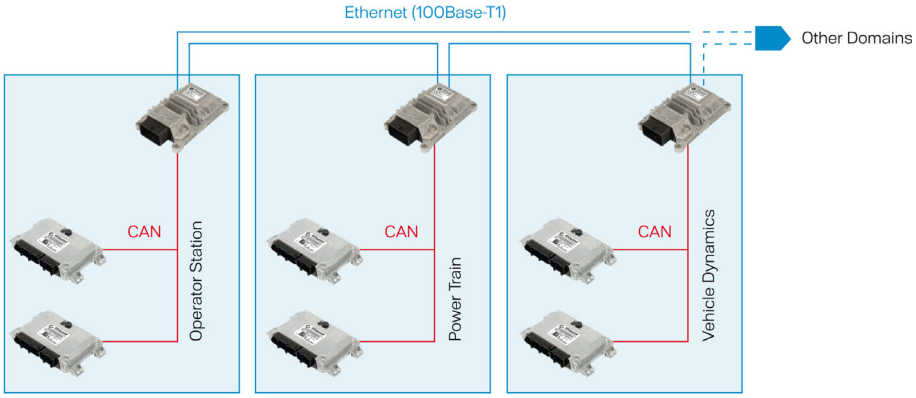

Figure 1: Domains separated by Ethernet interfaces using a ring topology (Source: TTControl)

The agricultural machinery market is advancing as fast as many other high-tech sectors, and we see more and more start-ups and large companies moving into the market.

Major trends such as connectivity and automation, as well as the growing ecosystem of software and hardware that needs to coexist and interoperate, bring new challenges that must be addressed in the very first stages of the development of a mobile machinery – right at the drawing board. Above all, a machine will no longer be an independent entity, but will likely exist as part of a group of machines that form a higher entity.

All of these trends and technologies bring about three direct consequences for the electronic architecture of a vehicle:

- Higher bandwidth requirements are imposed on the vehicle´s communication channels.
- The machine's electronics are becoming increasingly complex.
- Security must be improved.

Bandwidth requirements

In general, and across all verticals of mobile machinery markets, there is an increase in the amount of data being transmitted. Newer, more complex sensors and cameras produce more data that needs to be processed by the control units and displays. Furthermore, the connectivity between different control units in different areas of the machine requires reliable data distribution over the electronic network.

Modern agricultural machines, such as tractors or highly automated harvesters, employ numerous CAN networks to enable communication within the control system, for example engine CAN or vehicle CAN.

For this purpose – depending on the application – the CAN-based Isobus (ISO 11783) is used in addition to allow communication with implements such as trailers. SAE J1939 is often used as a basic protocol for these CAN networks, which specifies a bit rate of 250 kbit/s. In the case of Isobus, an implement that offers virtual terminal client functionality must transmit the associated object pool to the Isobus universal terminal in the machine. Depending on the specific features and functionality of the implement, this object pool can take up to a few megabytes. At 250 kbit/s the transfer of data that occurs at start-up can take a significant amount of time, especially considering protocol overheads and the fact that the communication protocol is contention based and that the CAN network must be shared with other devices.

The bandwidth requirements of new technologies, such as the continuously increasing resolution of displays, IP cameras (in some cases with surround view functionality), sophisticated fleet management systems using technologies from the IoT/Industry 4.0 world, as well as increasing automation of machine functions all exceed the currently available bandwidth by orders of magnitude. A single IP camera creates a data throughput in the range of 10 Mbit/s. A modern CAN-based system which includes complex gateways often has an overall bandwidth of approximately 1 Mbit/s to 2 Mbit/s, whilst future technologies will create a data volume that is up to three orders of magnitude higher than currently available.

Several of these functions, especially the automation functions in the area of drive, steering, and working functions also set strict requirements on functional safety, security, and real-time capability. These requirements come to the fore when automation functions have to share the physical communication medium with other services, for example in a steer-by-wire system that shares a network with the diagnosis system that has cloud access. In this case, it must be ensured that in the event of problems in the diagnosis system, the automation function continues to have guaranteed bandwidth and latencies, so that the steering continues to work reliably and safely, despite any unwanted network load created by the diagnosis system. ▷

At this point the need for different paths and routes for data arises in order to transverse vehicles without compromising intended functionalities of each particular block. This can be achieved by utilizing alternative transport technologies which operate side by side to create multiple network domains within the same architecture. Traditional control protocols can be implemented using CAN-based protocols, whereas bandwidth intensive applications and components can utilize the added capacity of Ethernet technology. Data then flows from one interface to the other as needed by the application. At the intersection of the different interfaces a central communication node ensures that the data is properly and efficiently transmitted from source to destination. This communication node, or gateway, allows for the separation of different “zones” and enables the implementation of very complex systems using a segmented and scalable approach.

It is worth noting that in the automotive market, which has very similar requirements to the agricultural market, the use of Ethernet is now pervasive, and standards based. Suppliers of Automotive Ethernet (100Base-T1, 1000Base-T1) Socs are now in full production and the adoption rate is increasing. Adoption of the technology in the mobile machine market is slower but will grow in the coming years as the applications demand it. Standard Ethernet (100Base-TX, 100Base-TX) is also present in many devices in the off-highway market, such as displays or telematics nodes, as it provides a way to connect to the machine with service computers and diagnostics tools.

Many industry players are already working on solutions to address the increasing needs of bandwidth and capacity of machine architectures. Most notably the AEF and the group of companies that contribute to the Isobus standard have been working on the High Speed Isobus standard, which provides gigabit grade connections over unshielded twisted pairs and is based on existing Ethernet technology.

Increase in complexity

New demands for advanced features are increasing the complexity of the electrical network within the vehicles, becoming a burden on the traditional levels of bandwidth and computing power. Until very recently, electronic control units were used almost exclusively for the control of electrohydraulic systems, such as valves, actuators, etc. The code needed to implement said functionality was often simple enough to run on low-cost MCUs (micro-control unit). Today, controllers are morphing into sophisticated platforms with high computational power that not only control other elements in the vehicle but also process enormous amounts of data at very high speeds. Increase of performance no longer translates into an increase in the number of electronic units needed. The exponential increase of system complexity can only be met with very powerful electronic control units, with high performing CPUs (central processing unit), often with multiple cores running in parallel, and external interfaces to match.

As complexity increases, a domain-based architecture may prove useful in keeping complexity levels manageable and provides a more modular approach to ▷

Ixxat®
BY HMS NETWORKS

USB-to-CAN FD
for CAN and CAN FD

PC/CAN Interfaces

Easy CAN and CAN FD connection for your application

- Interface for your control or monitoring application as well as for the Ixxat tool suite
- All PC interface standards supported with one uniform driver interface – easy exchange without programming!
- Drivers (32/64 bit) for Windows7/8/10, Linux, QNX, INtime, VxWorks and RTX
- APIs for CANopen and SAE J1939

Discover more:
www.all4CAN.com

CAN-IB 200/600/PCIe
1-4 x CAN, CAN FD

CAN@net NT 420
Ethernet PC Interface, Bridge, Gateway
4 x CAN, 2 x CAN FD

CAN-IB 120/520/PCIe Mini 1-2 x CAN, CAN FD

CAN-IB 230/630/PCIe 104
2-4 x CAN, CAN FD

CANblue II - Bluetooth
PC Interface, Bridge, Gateway
1 x CAN

HMS Industrial Networks GmbH
Emmy-Noether-Str. 17 · 76131 Karlsruhe
+49 721 989777-000 · info@hms-networks.de
www.anybus.com · www.ixxat.com · www.ewon.biz

software development. Moreover, significant amounts of data can be kept within the domain itself, avoiding an overload of the existing networks. Only data that needs to be shared by the different domains would cross a communication gateway.

The different domains could be connected using Ethernet technology if available on the domain controller unit, so that the CAN networks are not overloaded and remain reserved for the control applications. This segmenting into different domains might not be suitable for smaller machines that only require a very low number of control functions but as we connect machines to the cloud and to other vehicles in the field, even rather simple devices begin to need some concept of domains. Figure 1 depicts an example of a machine with several domains separated by (automotive) Ethernet interfaces using a ring topology.

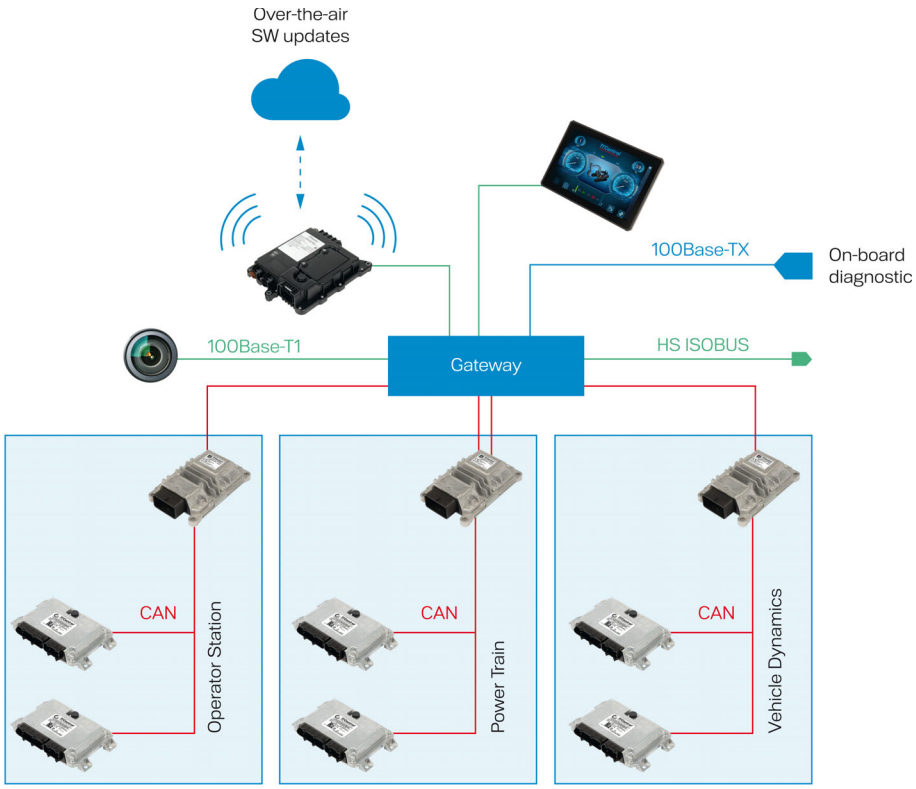

Figure 2: Illustration of vehicle architecture with a central communication node (Source: TTControl)

Need for improving security

Security will likely become one of the most, if not the most important topic in future designs of machines. As most machines today include both wired and wireless ports to connect to the outside world, it is already of the utmost importance to implement some type of security mechanism for diagnostics ports, cloud platforms, or construction, and farm site infrastructures. Connectivity to cloud platforms for machine monitoring or farm management software products are now almost a firm requirement among all players, as unprecedented demands of efficiency in the field require detailed analysis of processes and parameters related to the farm. These wireless interfaces are not the only potential point of entry for attackers; diagnostic or maintenance ports could also be used for entry to the electrical network of the machine. In essence, any physical port could be used for malicious or fraudulent purposes – the potential for such susceptibility only continues to increase.

Smart farming and its associated technologies offer farmers the potential for reaping huge benefits by reducing cost and increasing crop yield, however it can also pose a threat to farmers and even machine manufacturers. Hackers could target the farming sector for any number of reasons, as we have seen in some other industries in the past. Potential threats could be ransom-demands for blocked machines, but also a breach of data collected by the farmer which could potentially provide significant value to criminal organizations. Machine manufacturers may also be at risk of losing money to tech-savvy owners who hack their machines in order to tweak performance levels or manipulate machine data for fraudulent purposes.

As we transition to higher levels of autonomy in the field, security becomes increasingly important, as machines will independently make decisions that could affect yield performance or even human life. If a machine is to operate on its own or be able to detect and react to obstacles, including humans, it is of the utmost importance that the machine and its associated functionalities have not been tampered with.

It is therefore a hard requirement on machines to have a strong security concept that ensures that any kind of attack or unwanted modification can be avoided. Such a security concept is implemented at machine level. It not only affects telematics units or diagnostics ports, but rather it should provide an end-to-end concept that safeguards each of the key elements of the machine. To this end, a specific unit is required within the vehicle that is in charge of "policing" data traffic coming in and out of the machine, and within the machine itself. This gateway should be involved in security sensitive procedures, such as firmware updates (over-the-air or local), diagnostics, and M2M communications for machine control.

For example, the gateway could provide (amongst other measures) isolation between an "outside network" based on wireless connectivity and Ethernet and the "in vehicle network" based on CAN and potentially also Ethernet. Telematics, diagnostics, and a WLAN connection could be connected to the gateway, and not directly to the devices on the CAN networks, such as the ECUs.

A firmware update process triggered from the telematics unit (OTA FW update) or from the diagnostics port would then be authenticated by the security gateway before being executed. Encrypted communication could be enforced between the gateway and an outside device (PC, diagnostics device, etc.) by using protocols such as TLS in order to prevent "man in the middle" attacks or other unauthorized access attempts. Furthermore, TLS could be ▷

used between the gateway and the ECUs connected to it to increase the level of security of the whole vehicle.

A secure boot mechanism could then be implemented where a check of the firmware images loaded in each of the control units would ensure that the machine is safe to operate. Any anomaly in the machine software could be detected and appropriate actions executed.

Another vehicle architecture is shown in Figure 2 in which a central communications node, or gateway is utilized. This device provides data routing through the different domains and interfaces (CAN to CAN, CAN to Ethernet, Ethernet to Ethernet, HS-Isobus to display and/or cloud, and so forth), as well as security mechanisms to avoid fraudulent use or malicious attacks.

Future and even present developments in the agricultural sector only highlight and reinforce the importance of the three aforementioned consequences regarding vehicle architectures (increase of complexity, bandwidth requirements and necessary security efforts). For instance, the “Tractor Implement Management” (TIM) being implemented as an Isobus functionality will allow the implement to automate some operations of the tractor. Implements from various manufacturers will work together with tractors from several different providers. At the same time the tractor and the implement will also receive commands from other vehicles in the field and even real-time command and analytics information from cloud platforms. This combination of wired and wireless automation will require a very high degree of security and performance in order to ensure safe operations.

New devices, like the ones offered by TTControl, will be integrated in the vehicle architecture as centralized communications and control nodes or high-performance computing platforms. Displays will also experience significant increases in performance and complexity as operator assistance functionalities are integrated. New powerful CPUs with support for multiple cores operating in parallel, as well as real-time operating systems are key in addressing these new trends. Functional safety of the systems will also pose a major challenge in the new era of automation and digitalization of machines, especially if some machines are also to share the road with vehicles that are not part of the farm. This vision is being realized today – the introduction of new, scalable, and flexile architectures will play a critical role for the development speed of the farms of the future.

Author

Jose Ogara
TTControl
products@ttcontrol.com
www.ttcontrol.com

Ixxat®
BY HMS NETWORKS

CAN@net NT
CAN-to-Ethernet Gateway/Bridge
with 4 x CAN and 2 x CAN FD

CAN and CAN FD

Repeater, Bridges and Gateways

- Save costs due to simple wiring
- Increase your system reliability and protect devices by galvanic isolation (up to 4 kV)
- Filter/conversion functionality as well as coupling of CAN and CAN FD
- Bridging of large distances and easy system access via Bluetooth or Ethernet
- **NEW:** Cloud connection via MQTT and easy execution of tasks using “Action Rules“ – no programming!

All you need for CAN

Discover more:
www.all4CAN.com


CANblue II
Bluetooth PC Interface, Bridge, Gateway


CANbridge NT
(up to 4 x CAN / 2 x CAN-FD)


CAN-CR120/HV
CAN / CAN FD Repeater
(3 kV galv. iso.)


CAN-CR300
CAN / CAN FD Repeater
(4 channels)


CAN-CR 110/FO
CAN / CAN FD
to fiber optic

HMS Industrial Networks GmbH
Emmy-Noether-Str. 17 · 76131 Karlsruhe
+49 721 989777-000 · info@hms-networks.de
www.anybus.com · www.ixxat.com · www.ewon.biz