

# Advantages of CAN topology components in building automation systems

Thomas Waggerhauser

CAN was originally developed for use in vehicles, but is also extremely successful in the field of industrial automation due to very good network stability, flexibility in terms of inter-communication of the devices (producer/consumer principle) and the low costs. Further advantages of CAN are the possible line length of up to several kilometers, the good electromagnetic compatibility (EMC) and the availability of CAN interfaces on most industrial microcontrollers. In addition, there is a wide range of development and test tools as well as communication software.

On the other hand, CAN is a bus with line topology and limited stub line length, the use of topology components is particularly advantageous in building automation systems to flexibly adapt the CAN bus to the requirements of line routing in the building. Depending on the requirements due to local circumstances, gateways, CAN bridges or CAN repeaters can be used.

## CAN repeater

A frequent requirement of the building management network is stub lines to be able to integrate remote sensors or actuators into the network. In CAN networks stub lines can be implemented by CAN repeaters. Through the use of CAN repeaters, a network is physically separated. The length of the stub lines enabled by the use of CAN repeaters are only limited by the CAN baud rate used: Only the line length between the two most distant devices in the complete network restrict the used CAN baudrate. It is thus also possible to set up CAN systems in tree or star structures. As a repeater only physically separates the network, arbitration of the messages is carried out over the whole network and only network segments with the same baud rate can be connected.

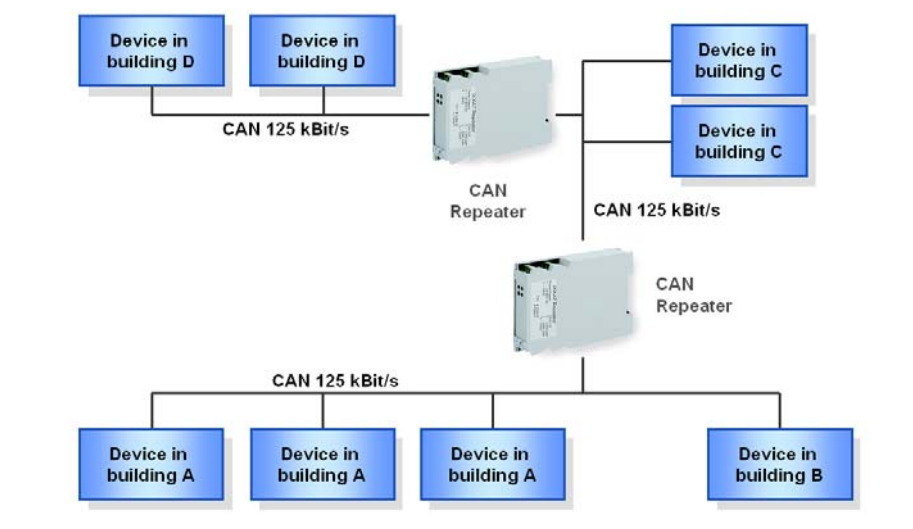


Fig. 1: Cascaded CAN network using CAN repeaters

CAN repeaters also improve the EMC and the radiation behavior of CAN systems. The integrated galvanic isolation of the IXXAT CAN repeater (up to 4 kV) prevents the propagation of interferences

on the CAN network. In addition, faults caused by electromagnetic interference or the quality of the cables used, are filtered by the signal repetition of the CAN repeater.

Alternatively, optical fibres can be used as the transmission medium with IXXAT FO repeaters (fiber-optic repeater). Thus a complete galvanic isolation of segments can be carried out, and the radiation and irradiation behavior is also considerably improved. This is especially useful in parts of the building with a heavily EM-contaminated environment or also in parts of the building that are to be completely shielded from EM effects, as the optical CAN data line does not act as an antenna and faults are not passed on.

Due to the integrated fault detection of the IXXAT CAN repeaters, faulty network segments are detected and isolated, which ensures that in the event of faults the remaining network continues working. As soon as the fault is eliminated, the faulty network segment is connected to the rest of the network again without interruption.

Repeaters are therefore the solution for various topologies and offer additional protection against faults from the outside or due to defective units.

### CAN bridges

In contrast to the repeaters discussed so far, CAN bridges divide a CAN system into independent CAN networks. In this way CAN networks with different baud rates can be connected to each other. Due to the integrated filter function, the messages can be filtered out before transmission from one network to another in order to minimize the bus load on the individual networks. The CAN bridges from IXXAT also make it possible to change the identifiers of the CAN messages. This is necessary if the CAN-ID used is already assigned to another message or function in a network.

In contrast to repeaters, with CAN bridges the network can be effectively extended – a network can be divided into several CAN networks to increase the extension or the bus speed of the CAN system: The effective line length of a CAN system can be increased at will by separating and interposing CAN bridges.

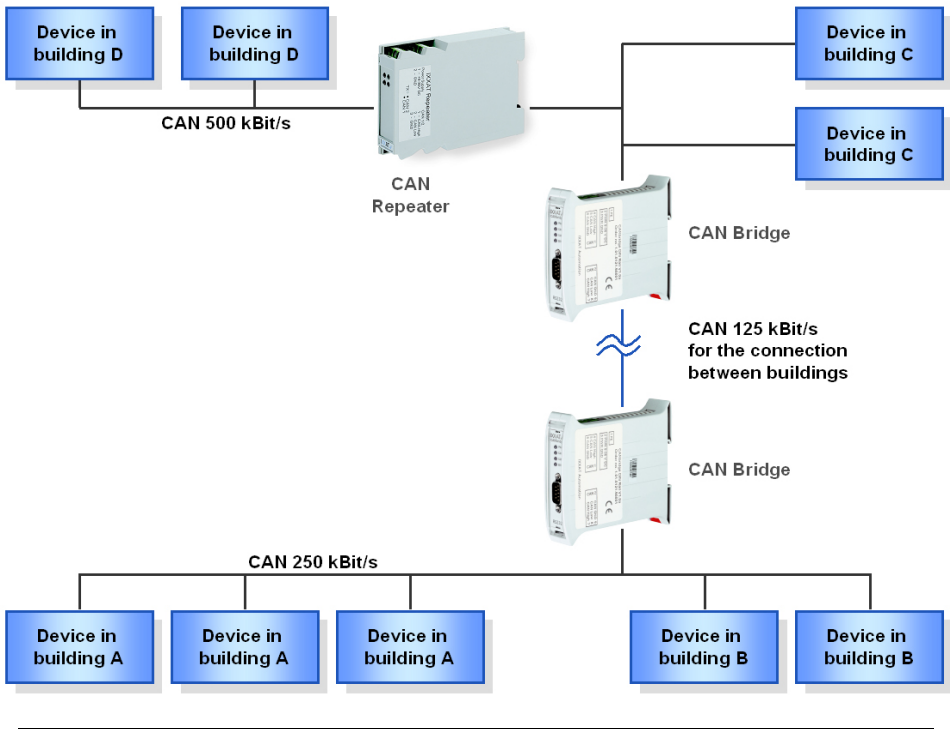


Fig. 2: Extension of the network structure with CAN bridges

## Gateways

Gateways such as the IXXAT CAN@net II connect CAN networks to other network types, mainly Ethernet. By using gateways it is possible to benefit from the high transmission rate of the Ethernet network available in buildings, as Ethernet is usually already available for networking of the management level (PCs). CAN can be used as a lower order bus to exploit the advantages of high fail-safety and high availability at fieldbus level.

Gateways are often used to connect management and service computers to CAN networks: a management or service computer can thus access CAN networks directly via Ethernet with the CAN@net II.

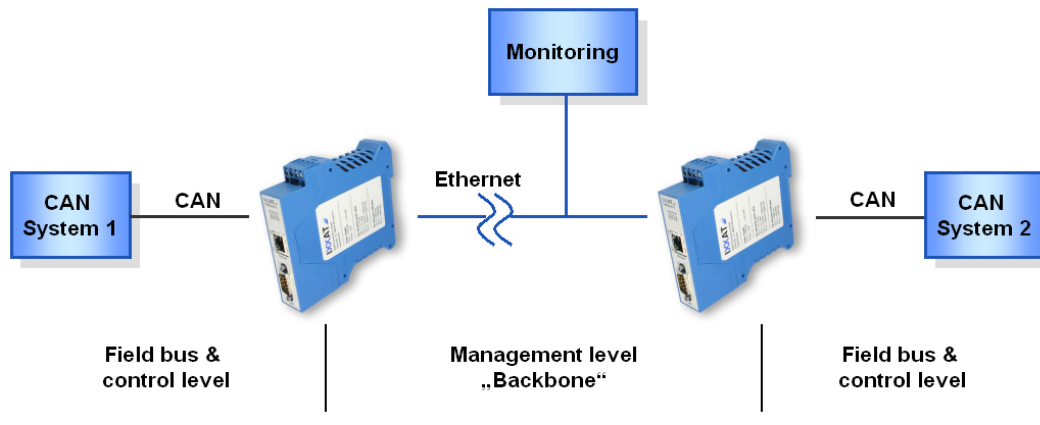


Fig. 3: Use of Ethernet as a "backbone" and for connection to the management level

Another important application is the connection of local CAN networks via existing WAN/LAN connections with high transmission rates even with large extensions. It is thus possible to connect CAN networks via Ethernet over large distances with high data transmission rates using the CAN@net II.

Another interesting application for gateways is remote maintenance of building systems: the CANmodem from IXXAT enables worldwide remote access to CAN networks via the public telephone network. The CANmodem is mainly used for service and monitoring purposes, as the transmission rate via the telephone network is limited. The CANmodem is therefore used as an access point for regular monitoring and maintenance services. As the CANmodem monitors the CAN network without interruption, it can actively make a connection to the monitoring and service center in the event of a fault and thus helps to prevent system failures. The early fault messages and the fault memory of the CANmodem also help to detect and eliminate the cause of the fault.

By using topology components, CAN can be ideally adapted to the requirements of the building. Unnecessary cable looms are also avoided, planning, installation operating costs are reduced, influences on the network due to faults from the outside are minimized and thus greater security is achieved.