CANopen Maritime – A New Standard for Highly Dependable Communication Systems

Prof. Dr. K. Etschberger, IXXAT Automation
Dipl.-Ing. C. Schlegel, IXXAT Automation
Dr. O. Schnelle, MTU Friedrichshafen
Bjørnar Wiulsrød, Kongsberg Maritime Ship Systems

Although the intention of the new CIA-standard DSP 307 - "A framework for maritime electronics" - was to facilitate the interoperability of electronic equipment in maritime systems and to support the features required by these systems, the developed standard is also of great interest for any application where highly reliable communication is required.

In the paper, the required extensions of the CANopen standard such as redundant communication, flying master capability and maritime multiplexed PDOs will be explained.

Due to its many advantages, there are already a large number of CAN-based communication systems in use in marine automation today. Although these systems meet the requirements made of them, they are mainly company-specific solutions, so that the integration of sub-systems and external devices of various manufacturers is generally difficult or very expensive.

This was the starting point for an initiative of the companies MTU Friedrichshafen, KMSS Horten (Kongsberg Maritime Ship Systems) and other companies for the development of an open communication standard for control and monitoring tasks in the area of maritime electronic systems. The work of the Special Interest Group (SIG) CANopen Maritime of CiA was begun in 1999 and completed for the time being in 2002 with the adoption of the standardization proposal CiA-DSP307 [1]. The aim of the work was to create a standard framework that meets the special requirements of marine automation, such as redundant communication, high availability of central network management functions, multi-master capability and the support of a large number of process data and configuration parameters. Here the SIG CANopen Maritime was able to fall back on tried and tested concepts and experience from already implemented CAN- or CANopen-based marine automation systems of the companies involved [2, 3].

With the adoption of the DSP 307 standard, the requirements of marine automation systems regarding reliability, safety and cost-effective engineering are met.

CANopen as a basis for an extended standard

Of the various CAN-based higher protocol standards, CANopen [5, 6] in particular has established itself as the worldwide recognized standard for the various applications in embedded systems, in industrial automation and in the various applications of mobile systems. The reasons for this are, among others, the powerful mechanisms provided by CANopen, the high reliability of the CAN protocol and the cost-effective implementability of CAN-based systems. It is therefore not surprising that in the meantime numerous standardized profiles are available for specific devices and applications based on CANopen. With regard to the special requirements of marine automation, however, it was necessary to extend CANopen by additional performance features, such as redundant communication and the flying master principle and to define further aspects.

Based on the so-called electronic data sheets defined for CANopen devices, in which the manufacturers describe the functionality, operating parameters and

specifications of their devices in standardized form, the simple engineering of customized automation systems is possible with the standard configuration tools available on the market [8]. As a result of the system configuration, so-called device configuration files are available that describe the actual settings of the devices in a specific system configuration and therefore fulfill the corresponding requirements of system integrators.

Redundant communication

The redundant concept defined for CANopen Maritime is defined on the "hot standby" principle and meets the requirements of the various classification organizations. This principle ensures that not only the failure of a transmission channel is detected and the telegrams are then evaluated on the redundant channel but also that no messages are lost during the transition of the evaluation from one CAN channel to the other.

As the extended standard should also cover applications where event-oriented status messages and process data are transmitted, temporary faults on a transmission channel, for example, must not lead to incorrect interpretations of a delayed message. The transmission mechanism must therefore take precautions against "obsolete" messages.

Fig. 1 shows the system configuration for devices with redundant data transmission on which CANopen Maritime is based. Such a device is connected to the two bus line pairs via two CAN controllers and two CAN drivers. Here the normally active bus lines are referred to as "default CAN lines" and the bus lines active in the event of a fault as "redundant CAN lines". In fault-free operation, transmission occurs on both transmission channels. One "transmission channel" is therefore defined by the transmit part of the transmitting CAN controller, the transmitting CAN bus driver, the transmission line, the receive part of the receiving CAN bus driver and the receive part of the receiving CAN controller.

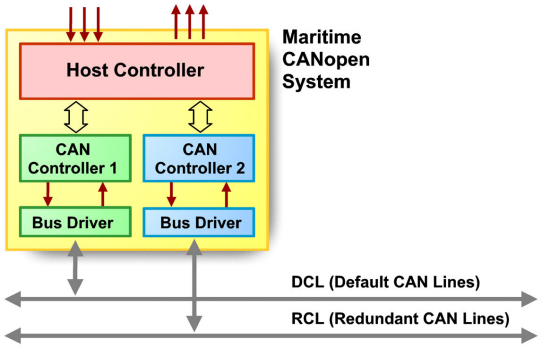

Fig. 1: System Configuration of a CANopen Device with Redundant Communication Channel

Fig. 2 shows the basic principle of the redundant message transmission for so-called PDOs ("Process Data Objects"). PDOs are CAN messages via which process data are transmitted according to the "producer-consumer" principle. Generally, every PDO is transmitted via both transmission channels. Due to different states of the transmission channels (for example different bus loads or a temporary fault on one channel), it may happen that transmission takes place at a different time ("Tx delay time") despite of an almost simultaneous transmit request (entry of a transmit request in the relevant CAN controller).

This assumes that with a correctly dimensioned system it is always possible for a message to be transmitted within a defined maximum time interval ("Max Tx delay time"). This time interval must be smaller than the so-called "PDO inhibit

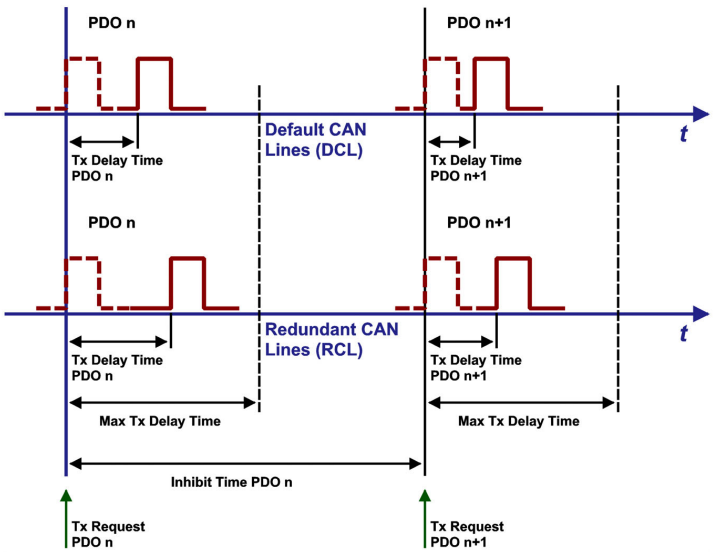

Fig. 2: Basic Principle of Redundant Data Communication

time" defined in CANopen. This time defines the minimum time interval for each message (PDO) in which the message can be transmitted again. If the delay of a CAN message is to great, a fault in the relevant channel can be assumed. If transmission of a CAN message is delayed compared to the transmit request by more than the "Max Tx delay time", this message may no longer be transmitted.

Every time the transmission of a CAN message on the default channel is aborted due to the maximum Tx delay time being exceeded, the so-called "channel error counter" is incremented by a certain value. If in the meantime successful transmission occurs again on the faulty channel, the error counter is decremented by the value one. In this way, temporary faults of the channel do not lead to immediate switching over to the redundant channel. However, in the event that the error counter reaches a maximum value, all other devices are informed by the transmission of an "indicate active line" message via the redundant channel that from now on the redundant channel is to be regarded as the "active line". In addition, the concerned device does not transmit any more heartbeat messages on the default channel. The "indicate active line" message via the redundant channel is also transmitted if a device has detected the failure of the heartbeat message of another device on the default channel.

Application-specific measures can be triggered via the "indicate active line" message with regard to signaling or rectification of errors.

If the error counter has reached the value zero again, for example after the recovery from a temporary fault, the device indicates its readiness for operation by transmitting its heartbeat message. After receiving at least 3 heartbeat messages from all other devices, it indicates this by transmitting an "indicate active line" message on the default channel.

The CAN messages transmitted are accepted on the receive side on both channels. The application decides on their further use. Typically, for example, the message previously received on one channel can be overwritten by the same message received on the other channel. Overwriting of a newer message by an older one is prevented by the previously described mechanism of delay time monitoring on the transmit side.

The described principle of simultaneous transmission of CAN messages via both CAN buses applies apart from PDOs (process data objects) also to the transmission of so-called "emergency" messages (standardized device error messages), timestamp- and synchronization messages. Only the timestamp and synchronization messages transmitted via the "active CAN lines" are processed on the receive side.

As it must be possible to control the communication state of a node by means of network management messages independently of one another via both CAN channels, a separate NMT state machine is implemented for each channel, although only one unambiguous state of the node is passed on to the application. The NMT state of a node that is valid for the application is determined via defined priority rules.

In contrast to the transmission of process data with PDO messages, the transmission of data between two devices happens according to the "client-server" principle via so-called SDOs (Service Data Objects). Via SDOs an acknowledged transmission of large quantities of data between two nodes is possible, for example for loading configuration data, subsequent loading of application software or reading out device diagnosis data. Request-SDOs (client-SDOs) are only transmitted via one CAN channel, response-SDOs (server-SDOs) are transmitted via the channel on which the transmit request was made.

Table 1 lists the various methods of transmission and processing of the various message types.

CANopen Message Type	Method of Transmission and Processing
PDO, Emergency Message	Simultaneous transmission on both CAN lines
Time Stamp Message, Synchronization Message	Simultaneous transmission on both CAN lines. Only messages received on active CAN line are processed.
SDO	SDO-Request: Transmitted on CAN line which provides a connection to the addressed SDO server SDO-Response: Transmitted on CAN line on which the request was received.
NMT Management Messages	Independent transmission and processing on both CAN lines

Table 1: Transmission and Processing of CANopen Messages in a CANopen Maritime System

Error-tolerant network management functions according to Flying Master principle

CANopen supports a series of functions that are allocated to a superior network instance. Such functions are, for example, network management tasks (NMT) such as the initialization of the network ("system start-up") or the control of the communication state of nodes by the so-called "NMT master", the allocation of SDO channels by the so-called "SDO manager" or the management of device configuration data by the so-called "configuration manager". As in particular the functions of the so-called "NMT master" are absolutely necessary for operating a distributed system, a failure-tolerant implementation of these functions is required. The solution developed for CANopen Maritime is based on the so-called "Flying Master principle". In the event of a failure of the active NMT master, for example, another "master-capable" device takes on the role of the active NMT master. The solution defined by the Maritime working group has since been adopted as the general standard for programmable CANopen devices [4].

For every master-capable device, a specific initialization process is required. This ensures that a new device appearing in a network becomes the active master by determining the currently active master (Fig. 3) if it has the highest master priority (Figs. 4 and 5) or does not carry out the master function, i.e. becomes a slave device if a master device of higher priority is already active.

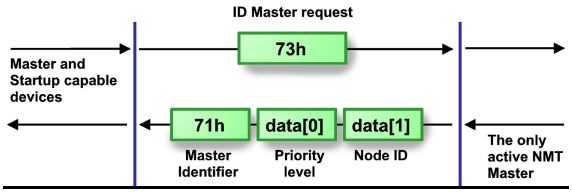

Fig. 3: Determination of the Active NMT Master

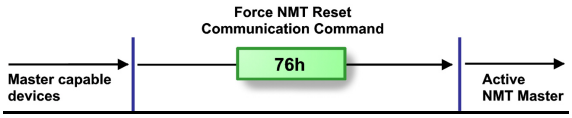

Fig. 4: Triggering of a New Master Determination Process

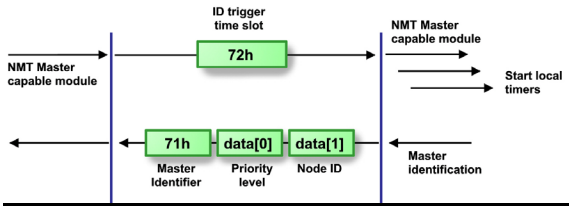

Fig. 5: Determination of the NMT Master

On the other hand it is necessary to constantly monitor the correct functioning of the currently active master in order to detect a failure of this device quickly enough. This is achieved by monitoring the heartbeat message cyclically transmitted by the active master by all devices. If a master-capable device detects the failure of the previously active master, it initiates a reset of the whole network of the relevant CAN line and initiates a new master determination process. As a result of this process, the device with the highest master priority assumes control. Due to the independence of the network management functions of both CAN channels and the redundant process data communication, the temporary unavailability of the channel concerned has no influence on the continual availability of the process data.

Monitoring of the communication-capability of devices via cyclic heartbeat messages

An important factor for the reliable operation of a distributed system is the communication-capability of all devices in the system. This is achieved by the so-called heartbeat protocol defined in CANopen (Fig. 6). Every device cyclically transmits a

message indicating its communication state. If a node defined for the monitoring of the device does not receive a heartbeat message of the device within the “heartbeat consumer time”, it is assumed that the device is no longer capable of communication. If a device that supports redundant communication detects the absence of heartbeat messages of another device on the default CAN line, it indicates this to all other devices by transmitting the so-called “indicate active CAN line” message on the redundant CAN line.

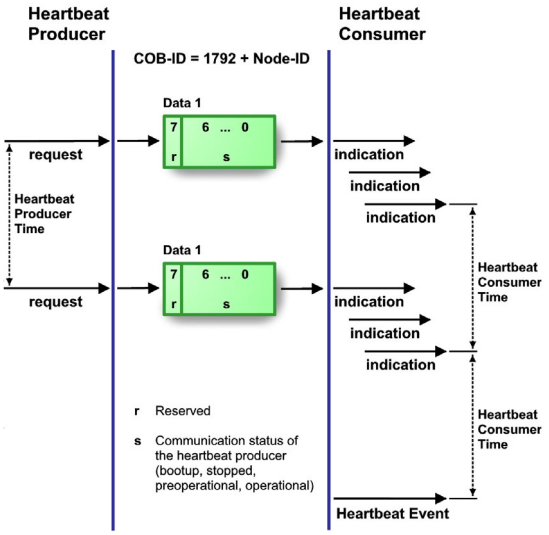

Fig. 6: Heartbeat Protocol

Extended Addressing of Parameters and Process Variables using Multiplexed PDOs

Applications of marine automation are characterized by a very large number of process variables and parameters. Up to now, manufacturer-specific data identifiers (tags) were often used to identify process variables and parameters. In order to get round the restricted number of CAN messages based on 11-bit message identifiers (2048 messages), CANopen offers an extended addressing of variables and parameters based on the so-called multiplexed PDOs (MPDOs). CANopen Maritime favors the multiplexed PDOs that are generally transmitted event-oriented (for example, when a certain alarm level is exceeded). With multiplexed PDOs, 4 bytes of the data part are used for the specification of a source or destination address of the variable or parameter transmitted in the form of index and subindex of the object dictionary of the transmitting or receiving node. Thus 4 bytes remain for the transmission of the actual data (fig. 7). MPDOs can be implemented in two addressing modes:

In the “producer addressing mode” the first data byte of the CAN data field contains the node-ID of the transmitting node and data bytes two to four the specification of the transmitted process variable in the form of object dictionary index and subindex.

In the “consumer addressing mode” the first data byte contains the node-ID of the destination node and data bytes two to four the index and subindex of the destination node object dictionary. Via node-ID zero it is possible to write to the object dictionary of several or of all nodes simultaneously.

In marine automation, producer-addressed MPDOs are used for the transmission of process data and consumer-addressed MPDOs for the transmission of parameter values for system configuration and commands.

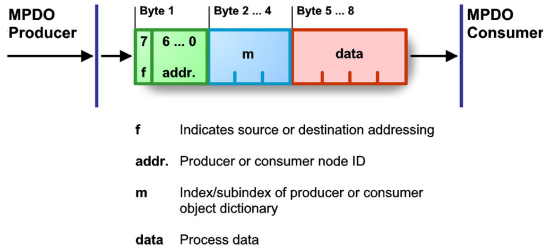

Fig. 7: Multiplexed PDO Protocol

Available Protocol Software and First Reference Implementations

The standard CANopen protocol stack extended to the special requirements of maritime applications has since been implemented by IXXAT [7] on various microcontrollers and subjected to comprehensive tests. The extensive development and implementation work for the extended functionality has been successfully completed. The protocol stack is now used in the solutions of various manufacturers.

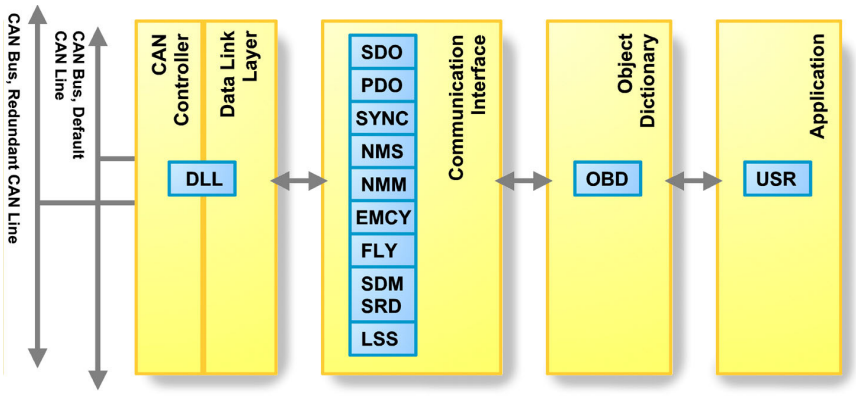

Fig. 8: Basic Architecture of the CANopen Maritime Protocol Stack

Fig. 8 shows the basic architecture of the CANopen Maritime Protocol software. The software package is structured in the form of separate modules for services such as Network Management (NMT), Process Data Objects (PDOs), Service Data Objects (SDOs), Emergency (EMCY), Flying Master (FLY), Synchronization (SYNC), SDO Manager (SDM/SDR), Layer Setting Services (LSS) and the Object Dictionary (OBD). The CAN controller (e.g. transmission and reception of CAN messages) is accessed by the Data Link Layer interface, which is also integrated in a separate module (DLL module). This allows simple adaptation of the CANopen Maritime Protocol software to different CAN controllers as well as to the available resources of various microcontroller systems. All modules have access to the object dictionary, which represents the central instance in the software package.

As a CANopen Maritime device supports redundant communication via two CAN buses (CAN lines) that are independent of each other, the communication-specific software components (Data Link Layer, NMT slave) must also be available in duplicate. The device-specific components (application, node-ID, object dictionary), on the other hand, are only provided once.

Summary

With the extension of the standard CANopen protocol to redundant communication and Flying Master principle, a standard is now available that meets the increased requirements of marine automation. Based on this standard it is possible to operate devices of different manufacturers in the same system without additional expense and to easily integrate subsystems of different manufacturers. This greatly reduces expenses for system engineering and integration. By using already available protocol software, test and configuration tools, personnel and material costs required for the development of devices and systems are considerably reduced. The solutions developed for maritime automation can naturally also be used for all applications requiring failure tolerance of the communication system.

Bibliography

1 CiA DSP 307: CANopen Framework for Maritime Electronics. CAN-in-Automation; 2002

2 Etschberger et al: A Failure-Tolerant CANopen System for Marine Automation Systems. Proceedings 7th international CAN Conference, Oct. 2000, Amsterdam

3 O. Schnelle: CANopen – The Fieldbus solution for system builders. Proceedings CIMAC Congress, 2001, Hamburg

4 CiA DSP 302: CANopen, Framework for Programmable Devices, V3.2.1. CAN-in-Automation, 2003

5 CiA DS 301 CANopen Communication Profile for Industrial Systems, V 4.02; CAN-in-Automation; 2002

6 K. Etschberger, Controller Area Network: Basics, Protocols, Chips and Applications. IXXAT, First edition 2001. ISBN 3-00-007376-0

7 www.ixxat.de

Prof. Dr. K. Etschberger
IXXAT Automation GmbH
Leibnizstr. 15, 88250 Weingarten
Germany
Phone: +49-(0)7 51/ 5 61 46-0
Fax: +49-(0)7 51/ 5 61 46-29
E-mail: etschberger@ixxat.de
Website: www.ixxat.de

Dipl.-Ing. Christian Schlegel
IXXAT Automation GmbH
Leibnizstr. 15, 88250 Weingarten
Germany
Phone: +49-(0)7 51/ 5 61 46-0
Fax: +49-(0)7 51/ 5 61 46-29
E-mail: schlegel@ixxat.de
Website: www.ixxat.de

Dr. Olaf Schnelle
MTU Friedrichshafen GmbH
Kapellenstraße 29, 88048 Friedrichshafen
Germany
Phone: +49-(0) 75 41 / 90-62 20
Fax: +49-(0) 75 41 / 90-61 34
E-mail: olaf.schnelle@mtu-online.com
Website: www.mtu-friedrichshafen.com

Bjørnar Wiulsrød
Kongsberg Maritime Ship Systems
P.O. Box 1009, 3194 Horten
Norway
Phone: +47-33 03 22 36
Fax: +47-33 04 22 50
E-mail: bjornar.wiulsrod@km-ss.com
Website: www.kongsberg.com