iCC 1995

2nd international CAN Conference

in London (United Kingdom)

Sponsored by

Motorola Semiconductor
National Semiconductor
Philips Semiconductors

Organized by

CAN in Automation (CiA)
international users and manufacturers group
Am Weichselgarten 26
D-91058 Erlangen
Phone +49-9131-69086-0
Fax +49-9131-69086-79
Email:headquarters@can-cia.de
URL: http://www.can-cia.de

ir. M.W. Nelisse
TNO Institute of Applied Physics, Delft, The Netherlands

M3S

A general-purpose integrated and modular architecture for the rehabilitation environment.

M3S stands for Multiple Master Multiple Slave and is a system concept designed to improve access to assistive technical devices by disabled people. It is a proposed standard architecture for general-purpose integrated and modular systems, which specification is available as an open standard. It is based on an industry-standard digital communication bus, the Controller Area Network (CAN), and includes additional signal lines to increase system safety and integrity. M3S provides a standard interface between input devices and end-effectors, allowing devices from different manufacturers to be linked in the same system. During revalidation phases this facilitates the process of evaluating different input devices and making the decision what input devices are optimal for a specific user. Furthermore the M3S architecture enables the user to operate more end-effectors, from categories like mobility, manipulation, environmental control and communication, using a single input-device.

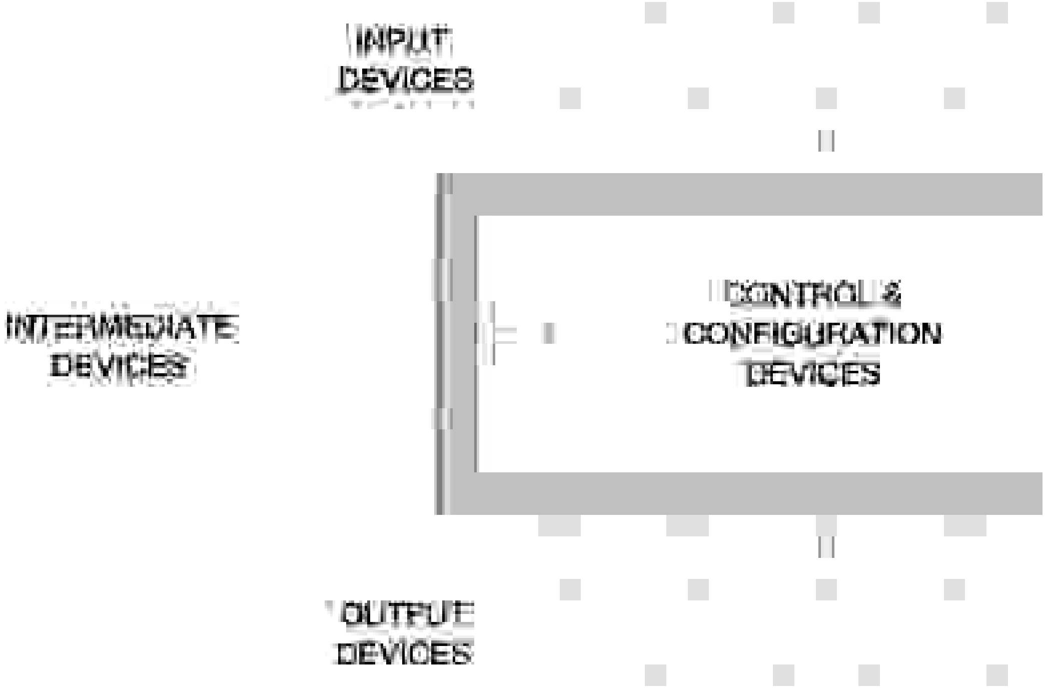
M3S **Fehler! Schalterargument nicht angegeben.**

Many technical aids are available for the purpose of increasing the independence of disabled and elderly people. An increased independence of this group would have a positive effect on nearly every aspect of the lives of the disabled people, both on personal and vocational activities. Technical aids for these purposes are employed to an ever increasing extent. But until now these technical aids are developed in a rather uncoordinated way, which results in many products not compatible with each other and rather poor system safety characteristics. Furthermore the level of customisation and flexibility is very limited and involves considerable additional costs. Long time support is also not guaranteed and this leads to extra costs for maintenance.

The next step is to integrate these technical aids to form an integral aid which offers disabled people better opportunities to function as independently as possible. Integral systems will comprise many different technical aids and (sub-)systems. One of the most important points of attention is integration of all systems employed. This is a pre-requisite for simple and optimal use of the integral system. Therefore it is essential that the integral system has a modular construction. This modular construction also allows users to compile a specific package of technical aids to a complete integral system, while still permitting them to extend or modify the system later on, because of changing wishes, needs and user environments. The basic M3S concept will connect different devices in a safe and easy to use way.

System architecture

A M3S system is based on a bus and devices. The bus is based on the three parts: 2 lines for digital communication (CAN bus), 2 lines for power distribution (POW bus) and 2 lines for safety features (SAF bus). Devices are connected to this bus. A single device may also consists of more physical entities on the bus, these are called *modules*. Some devices on the bus can link the local bus to one or more remote bus parts in the M3S system using a (wireless) link. The M3S system architecture is depicted in the next figure.



Fehler! Schalterargument nicht angegeben.

Four types of devices can be distinguished in a M3S system:

control & configuration
output
intermediate
input

Control and configuration devices deal with configuration functions, control functions and safeguarding functions. *Output devices* or *end-effectors* have primarily an actuator function. *Input devices* have primarily an input or sensor function. *Intermediate devices* have both input and output features.

M3S is basically a distributed system which needs a central control and configuration method. The configuration method is based on a generalisation of devices. This ensures that new devices can be added to the system at a later stage without any further adaptions, therefore it must be assumed that an input device knows nothing about an output device and vice-versa. All devices on the bus have internally stored *device configuration* information, which describes the specific behaviour of a device in a uniform way. The CCM is able to retrieve this distributed configuration information from the devices and based on this data a *system configuration* can be build. This system configuration describes the setup of the complete system and all possible actions for the special needs of a user.

When later on a device is malfunctioning, it can simply be replaced by an identical device. The CCM will detect this device replacement and checks if the new device is fully compatible (identical device from the same company) with the old device. If they match no reconfiguration of the system is necessary.

Safety

Within reasonable levels of cost, complexity and ease of use, systems cannot be 100% safe. The M3S bus concept aims at the highest levels of safety within a usable system. Nevertheless, manufacturers, configurers, facilitators and users should always be aware that for complex systems, circumstances can arise where safety is at risk. Appropriate measures must then be taken to inform all concerned of the safety implications, and to minimise the risks wherever possible. It is therefore assumed that individual devices brought to the M3S system are intrinsically safe as independent devices. Nevertheless, using the devices in combination with other equipment can result in situations where the combined system could be at risk and appropriate restrictions should be placed upon use.

Impaired users with high levels of disability will often benefit most from using complex systems. However, they will also tend to have the greatest limitations in controlling the system. Input systems will often be serial in nature, slow to operate, with consequent control problems. Configurers and facilitators should be aware of this, restrict the capability of the system where necessary, and inform the users of the safety implications. When the M3S system is to be configured for use in a particular environment, the manufacturers, configurers, facilitators and impaired users should be aware of the limitations of use.

CAN communication

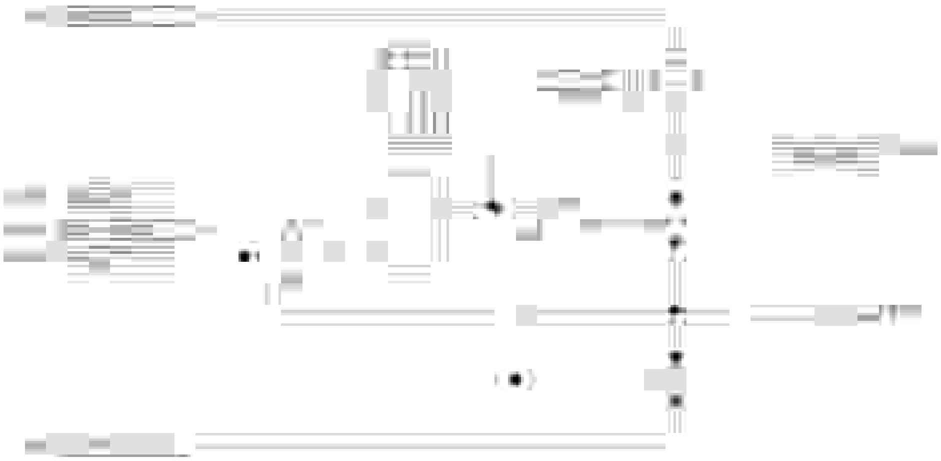
The digital communication between the devices in a M3S system is based on CAN. This communication standard originally developed for automotive applications has extensive error detection and automatic retransmissions facilities while still allowing a deterministic method of exchanging information based on priorities.

Information on the CAN bus is exchanged in messages and a message transmitted on the bus is received by all other devices connected to the bus. Each message starts with an arbitration field which is used to determine the message with the highest priority which can take control of the bus. The arbitration field contains an eleven bit identifier an a single bit indication if the message contains data or is used to request data. After the arbitration field, the winning message continues with a length indication of the number of data bytes, the data bytes itself (up to a maximum of eight bytes) and a fifteen bit cyclic redundancy check (CRC) number used for error detection. All devices which have successfully received the message will simultaneously transmit an acknowledgement at the end of the message. Devices which noticed an error on the bus, will immediately transmit a special sequence of bits after the error was detected. This will automatically force retransmissions of the message.

Key switch function

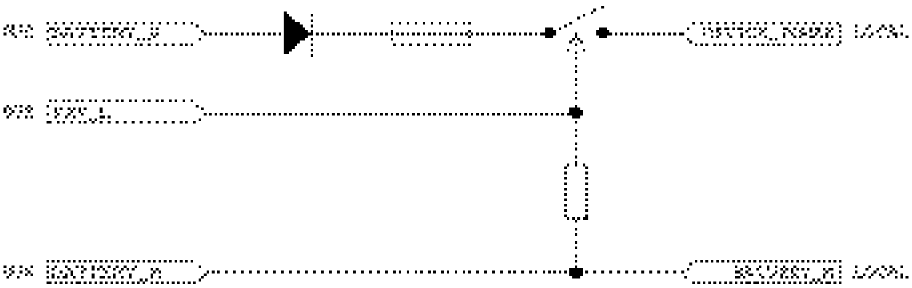
The key switch function can be operated by the user or a helper and is meant to turn on or off the complete system. It also allows the system to be stopped immediately in case of an emergency.

The key switch functionality consists of one or more key on and off switches, a hardwired KEY line as part of the M3S bus and some circuitry on all devices to interrupt the power supply to the device. The key on switch is a non-latching physical switch meant to turn on the complete system. The key on switch is associated with a key off switch which can be integral or independent. The key off switch is a physically operated switch, but the key off switch can also be operated by the CCM on request of the user or when major faults occur. The KEY line provides an enable signal to the local power supply circuitry on the devices. No device should be able to operate unless the KEY line is active. The KEY line is connected to the battery plus via the key on switches in the input systems. Pulling the KEY line to battery minus should turn off the local power supply circuitry and hence turn off the system. Where appropriate, a limited time delay may be incorporated in the power supply interruption circuitry of the devices.



Fehler! Schalterargument nicht angegeben.

Key switch latch circuitry



Fehler! Schalterargument nicht angegeben.

Device power circuitry

Although the key on switch is a non-latching physical switch, the key switch circuitry should provide a latching function. A key switch status signal at the input systems is used to check the latch status. Where duplicate key on switches are provided, only one should be active at any one time, which means only one key switch is latched. The CCM can monitor the key switch status and ensure that only one is active. This guarantees that the system can be turned off with any key off switch in the system, independently of the actual key on switch used to turn on the system.

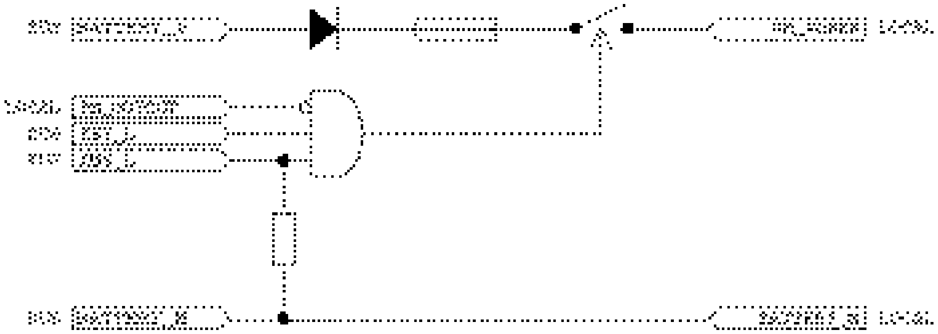
Dead man switch function

The dead man switch (DMS) is a function, which requires a continuous positive action from the user to allow the operation of devices which are capable of powered motion and which can affect the safety of the user: safety critical prime movers. It allows the user to halt these devices safely and quickly by releasing the DMS.

The dead man switch functionality consists of one or more dead man switches, a hardwired dead man switch line as part of the M3S bus and some circuitry on the output devices to interrupt normal power supply to the prime moving parts. In case duplicate dead man switches are provided, only one should be active at any time (to be ensured by the CCM).

Fehler! Schalterargument nicht angegeben.

Dead man switch circuitry



Fehler! Schalterargument nicht angegeben.

Prime mover power circuitry

The addition of the DMS line to the CAN bus, provides an additional safety backup to turn off the safety critical prime movers independent of the CAN bus and the control function of the CCM. This means that even if a non-trapped fault were to develop in the CCM, the user can still shut down the safety critical prime movers safely by releasing the dead man switch.

Safety monitoring

The purpose of the safety monitor is to regularly check the safety of the system at all levels and when appropriate to shut down or restrict functions for specific parts of the system. The safety monitor mechanism is based upon a global safety monitor in the CCM: the *system safety monitor*, a local safety monitor in each device: the *device safety monitor* and additional safety monitors in the transceivers of a link when a system contains local and remote busses: the *link safety monitor*s.

In order for the system to remain active, the system safety monitor should monitor the overall system safety and should receive confirmation from all device safety monitors that the devices are in a safe operating condition. This is achieved via periodic status requests and responses. No device should be enabled without a prior safety check. This requires a response from the device safety monitor indicating a safe state. The system safety monitor also monitors the status and connections of the DMS and KEY lines and of the dead man switches and key switch latches.

Each device safety monitor ensures the safe operation of its own device. The device safety monitor of the active output device should monitor input device DOF signals into the output device which should be refreshed at an appropriate rate. If the DOF's are interrupted or not received at all, a time out will occur and the output device safety monitor should then execute an immediate stop. Device safety monitors on prime movers should be able to shut down the motor power circuitry directly and so give a rapid response to serious errors. The device safety monitor should then immediately report these situations to the system safety monitor.

The safety monitoring procedures of the M3S system can only be specified in general. It is not possible for the system to have knowledge of the detailed functionality of device hardware and software. It is therefore the responsibility of device manufacturers and suppliers to define fatal and non-fatal errors, to ensure that the device is safe and is provided with adequate monitoring and shut down facilities. M3S will only provide generic mechanisms to signal, detect, and handle these kinds of situations.

Safety equations

A device which can put the system or parts of it in a potentially dangerous position, should signal safety events to the CCM in the system. Together with safety equations defined in the system configuration, the CCM will respond on these events by signalling safety restrictions to other devices in the system. These devices will now be limited in their usage.

Both the safety events and safety restrictions are boolean type of signals and can therefore only indicate a TRUE or FALSE situation. The relationship between the safety events and safety restrictions is specified in safety equations. These safety equations are defined in what is called 'a sum of products' form. This form describes the formula, how to calculate the equations using the boolean operators AND, OR and NOT. All devices can signal changes in the their safety events, but the CCM will only signal changes in the safety restrictions defined for the safety equations in the current task.

Initialisation

The initialisation phase begins when the key line is activated and the system is powered on. Each device is allowed a fixed amount of time to perform some power-up actions, which are necessary to take part in a mechanism called the *Serial Number Arbitration Protocol* (SNAP). After this mechanism each device finishes remaining initialisation actions before it is ready to participate in normal operations.

The purpose of the SNAP mechanism is two fold. First it is used to identify all devices in a system, and secondly it is used to give each device a unique handle, called a device number. The SNAP mechanism completely eliminates the need for hardware jumpers, DIP switches or harness resistors and therefore making it easier to install devices in a system. Together with an auto configuration mechanism it can offer true *Plug and Play* (PnP) possibilities.

Every device has a unique 64 bit SNAP ID number that differentiates one device from another. This ID number contains a manufacturer ID, a serial number and an additional category number. On power up all devices are placed in an inactive state. They arbitrate for the bus and the device with the smallest ID number wins. Because all ID numbers are world-wide unique it is guaranteed that only a single device is *isolated* on the bus at a time. The arbitration is done in a byte oriented sequence, so a single arbitration cycle takes 8 steps. After a device has won arbitration, all other devices drop off. The first arbitration cycle is used to find a master to control the SNAP mechanism, this device is called the arbiter. The arbiter will assign itself the first free handle, it gets device number 0. In following cycles the arbiter will repeatedly assign the next free device number to the devices which won arbitration cycles. Once a device has been assigned a device number, it no longer participates in the arbitration mechanism and arbitration of devices with higher ID numbers can proceed.

The power-up actions and the SNAP mechanism take place after activation of the key line. However three kinds of activation are possible, the normal activation of the key on switch, *hot insertion* of a device or a when a remote bus link becomes active. Depending on these condition a device has to differentiate between a system without or with an already existing arbiter. Therefore each device starts the SNAP mechanism by issuing a request for an arbiter. If an arbiter is available it should respond within a certain time-span and start a new arbitration cycle, otherwise the device can start an initial arbitration cycle by himself.

An arbiter can assign 64 device numbers, but when it has run out of available device numbers, the arbiter assigns a void device number to all remaining devices. This limit of 64 device numbers, restricts the number of concurrently active devices in a M3S system to 64. However by using a *warm system reset* procedure it is possible to assign device numbers to a new set of devices in a M3S system. To speed up the SNAP mechanism in M3S systems, the arbiter can also directly assign device numbers to devices based on information stored in an existing system configuration.

Configuration

Configuration is basically changing the contents of the system by adjusting the system setup and replacing or adding devices to the M3S bus. As a result of the fact that the M3S system is a modular and open bus system, the system contents can be changed easily to adapt to the wishes of the impaired user in case of a changing illness.

In order to secure a safe system, the configurer has to adjust or create the right relationships between the different devices. The facilitator, in co-operation with the impaired user, has to personalise the system. The impaired user has to be able to adjust basic settings that influence the interaction with the system. Alterations on the system setup will be limited for each user group.

Selection

Selection is the way which allows the user to start a new kind of operation, called a task. In order to do selection, the system and in particular the CCM, should have some knowledge about what can be chosen. The man-machine interface is strongly involved in this topic.

After start up of the system, the user will enter the system in an environment with the possibility to directly access several tasks. Only important and frequently used tasks will be a part of this environment. Other tasks might require more access actions. These tasks are less frequently used. Especially the more sophisticated systems will have a multi level accessibility.

As a result of the fact that the M3S system is a modular and open bus system, the way of selecting several tasks can be changed from a impaired user's point of view during operation (short timescale) or more likely because of a changing illness (longer timescale).

For this purpose M3S defines a hierarchical and logical organisation of the different tasks the system can provide based on a tree structure. This tree structure has the possibility to group related and frequently used tasks is so called nodes. Besides the relation of a node to a set of tasks, a node can also refer to other nodes, so called sub-nodes.

The user must have a possibility to navigate in the tree, from a node to a sub-node, to other levels in the hierarchy or between different tasks and finally to select the task he wants to start. However the ideal selection mechanism will be direct switching between tasks instead of a selection - operation - selection sequence through the tree. The switching between the tasks will require some changing of modes on the devices, but it is important that the user should not be aware of this.

Operation

The prime actions during operation are related to the execution of a task. A task is a system wide mode in which one or more devices in the system perform actions initiated by the user. Both configuration and the explicit task selection are in fact specific appearances of such tasks. Like in configuration and selection the man-machine interface is very important here and can be freely configured to suit the needs of the impaired user.

Evolution

The first specification of M3S was released in October 1992 as version 1.0. This preliminary specification was meant as a document for comments and discussions. Version 1.1 was released in April 1993 and this document was accepted as a Working Draft by ISO/TC173/SC1/WG7. In March 1994 an enhanced specification of M3S was released as version 1.1 revision B. This specification included extensions for a separate display device, extra safety monitoring features, naming conventions and less restrictive timing specifications.

Based on evaluations and comments from the ISO working group ISO/TC173/SC1/WG7, a rewritten specification of M3S including extensions for fully automatic system identification, plug and play possibilities, enhanced global safety handling and wireless links was released in July 1995 as version 2.0. The annotated M3S reference manual version 2.0 is now available as a draft specification and will be used as a base document for the formal standardisation of M3S by ISO/TC-173/SC-1/WG-7.

Getting started

A number of packages from different companies are available to make a quick start with M3S. These M3S starter-kits include items like protocol specification, frequently asked questions (FAQ), personal computer based plug-in or add-on cards, micro-controller based prototype boards, software development kits (SDK) for PC's and application programming interfaces (API) for both PC and microcontroller environments (currently 80x86, 8x592, 68331). Furthermore a program, called M3sWizard, is available which can create a full-featured (C code) skeleton for your M3S API based application program ready to compile within a single minute. In the near future also an M3S chipset will become available.

Further information

The central place for information on M3S is the M3S dissemination office. You can refer to this office for all kinds of general information, questions or comments on M3S. General information on M3S is also available in electronic form. Currently e-mail, ftp and world wide web services are available.

M3S dissemination office
TNO Institute of Applied Physics
PO Box 155
2600 AD Delft
the Netherlands

telephone: +31 152 692004
telefax: +31 152 692111
e-mail: m3s@tpd.tno.nl
ftp: ftp.tpd.tno.nl pub/m3s
www: http://147.252.133.152/m3s