EmSA Product Catalog 2018

We provide products and services for

- **CANopen / CANopen FD configuration, analysis, simulation and test**
- **Embedding CAN and CAN-FD based protocols CANopen and J1939**
- **Secure software updates and bootloading of embedded systems**
- **Training and consulting on many aspects of embedded systems**

Catalog Contents

Expertise

Our expertise covers many microcontroller architectures and their development tools. We focus on time-to-market, quality improvement, security and embedded networking applications using Controller Area Network (CAN bus), CAN-FD, CANopen and Embedded Internetworking.

Application fields include consumer, industrial, medical, sub-sea and after-market automotive. We participate in CiA (CAN in Automation user's group) standardization committees such as CiA 301, CiA 305, CiA 447 and many others. We work with other CAN-bus protocols such as J1939 and ISO-TP (ISO 15765-2).

Contact

European Union

Embedded Systems Academy, GmbH
Bahnhof Str. 17
D-30890 Barsinghausen
Deutschland

Phone: +49 (5105) 582-7897
Fax: +49 (5105) 584-0735
Email: info@esacademy.de

North America

Embedded Systems Academy, Inc.
1250 Oakmead Parkway, Suite 210
Sunnyvale, CA 94085
United States

Phone: +1 (877) 812-6393
Fax: +1 (877) 812-6382
Email: info@em-sa.com

www.em-sa.com ▪ www.canopenstore.com ▪ www.canopenstore.eu

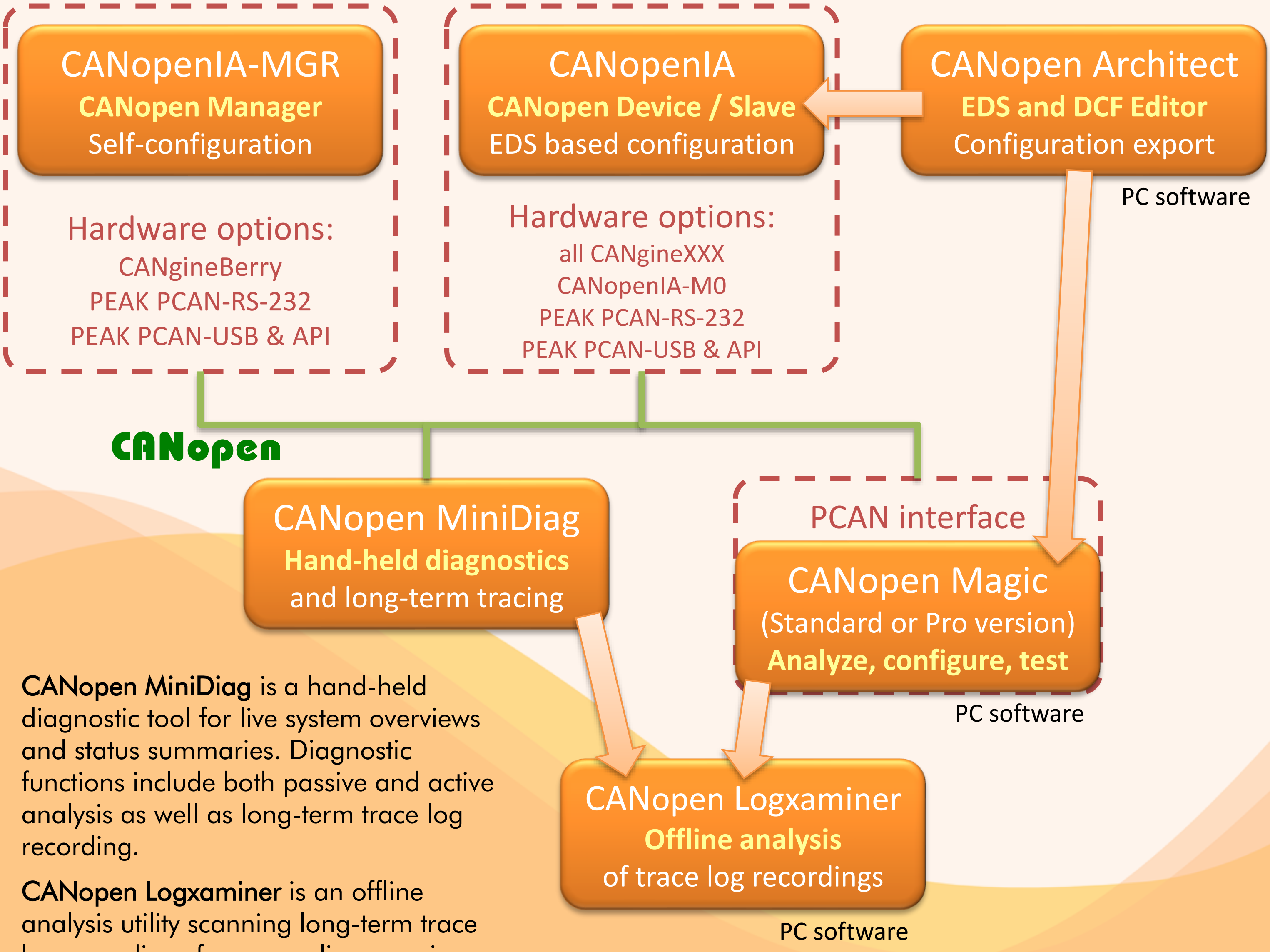
EmSA CANopen Simplified

Product overview of our entry-level CANopen solutions: Self-configuring Manager, CANopenIA based devices and tools for configuration, diagnostics and analysis

CANopenIA-MGR Minimal Manager solutions provide quick and easy access to the CANopen or CANopen FD devices connected. The manager scans the devices and offers all PDO (Process Data Object) I/O data to the connected host system. The host accesses CANopenIA-MGR through a simple UART protocol or an API. In any case, the host system can directly refer to the CANopen data objects by node ID, Index and Subindex.

CANopenIA coprocessors or stand-alone solutions implement CANopen devices (slaves). They communicate to their host (if any) through a simple UART protocol and are configured by custom setup tools provided or the **CANopen Architect** EDS (Electronic Data Sheet) editor.

The CANopen EDS configurations can also be imported by the **CANopen Magic** tools for monitoring and analyzing CANopen networks.



CANopen MiniDiag is a hand-held diagnostic tool for live system overviews and status summaries. Diagnostic functions include both passive and active analysis as well as long-term trace log recording.

CANopen Logxaminer is an offline analysis utility scanning long-term trace log recordings for anomalies, warnings and errors. Findings can be exported as a PDF report.

www.em-sa.com ▪ www.canopenstore.com ▪ www.canopenstore.eu

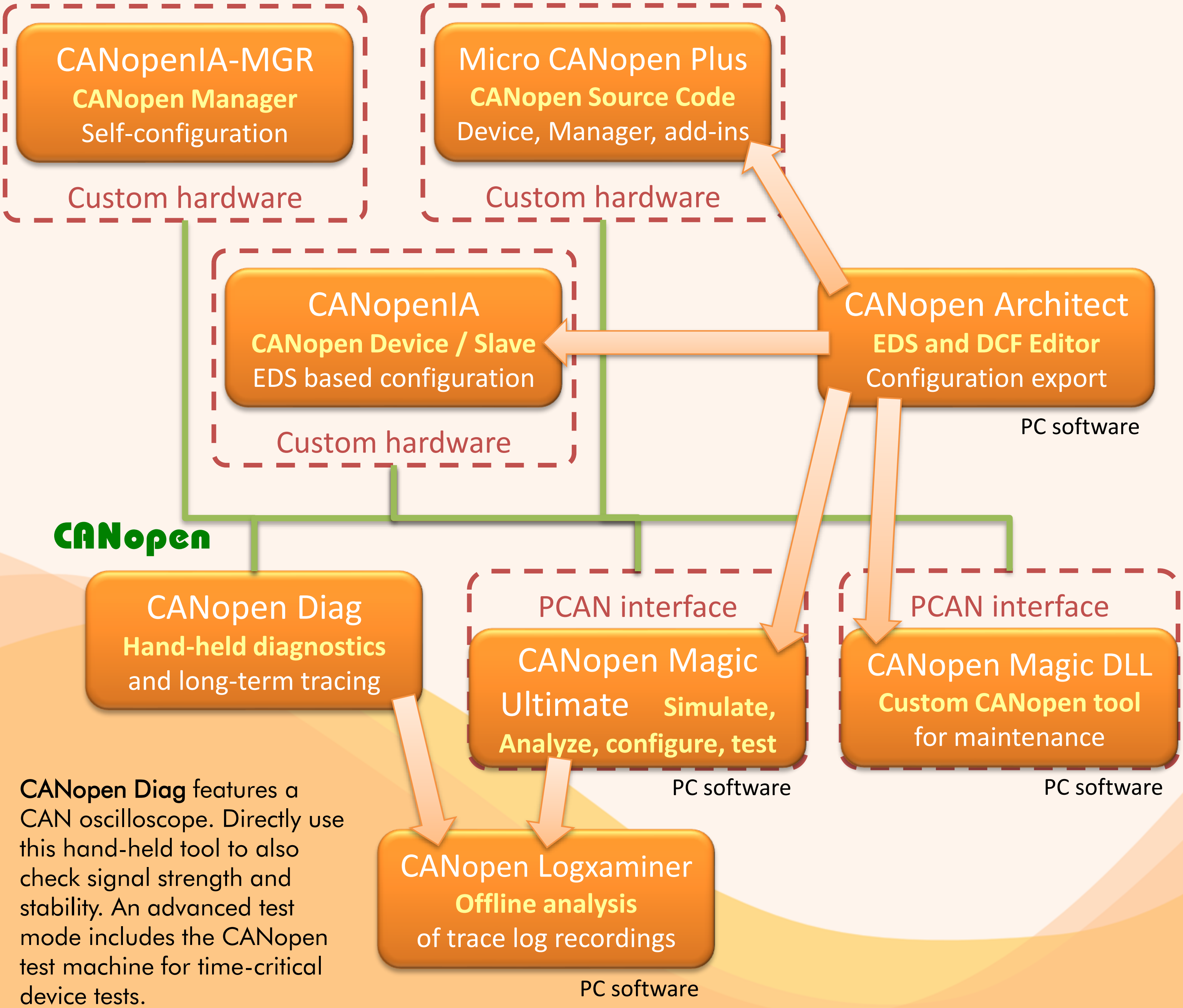
EmSA

CANopen Complete

Product overview of our full-featured CANopen solutions: Source code for devices and manager, custom maintenance tools, hardware support, advanced diagnostics

CANopenIA solutions can be customized for your own hardware.

Micro CANopen Plus is a complete source code solution including advanced CANopen functionality such as LSS (Layer Setting Services) or advanced, dynamic configurations of objects and PDOs. Device and application profile examples are available for many profiles.



CANopen Diag features a CAN oscilloscope. Directly use this hand-held tool to also check signal strength and stability. An advanced test mode includes the CANopen test machine for time-critical device tests.

www.em-sa.com ▪ www.canopenstore.com ▪ www.canopenstore.eu

EmSA

CANopen Book

Embedded Networking with CAN and CANopen
THE CANopen book for beginners and advanced users

CANopen is an open communication standard based on CAN – Controller Area Network. It is maintained by the CiA (CAN in Automation) user's group and features a high number of device and application profiles. Uses include industrial, transportation, maritime, medical, sub-sea, after market automotive and many more.

The book contains three parts:

Part 1: Using CANopen, by Olaf Pfeiffer

This part focuses on CANopen up to the system integrator level. Any technician or engineer who needs to be able to configure and/or maintain a CANopen network will find the required knowledge to do so in this part. The last chapter in this part contains a step-by-step example of a network configuration and test cycle.

- ✓ Understanding Embedded Networking Requirements
- ✓ The CANopen Standard
- ✓ CANopen Beyond DS301
- ✓ CANopen Configuration Example

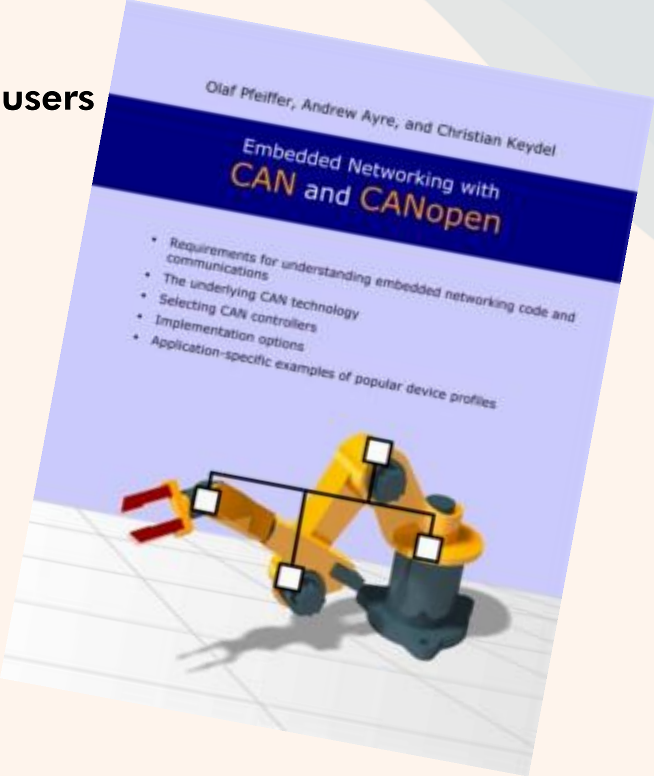
Part 2: CANopen Engineering, by Christian Keydel

This is the part for engineers who need to have a detailed knowledge of how CAN and CANopen work, especially for those developing their own CANopen devices. It describes and compares various implementation methods in detail.

- ✓ Underlying Technology: CAN
- ✓ Implementing CANopen

Embedded Networking with CAN and CANopen

ISBN 978-0-692-74087-3: Paperback edition. Demo software matching the examples in the book is available for download.



Olaf Pfeiffer, Andrew Ayre, and Christian Keydel

Embedded Networking with
CAN and CANopen

- Requirements for understanding embedded networking code and communications
- The underlying CAN technology
- Selecting CAN controllers
- Implementation options
- Application-specific examples of popular device profiles

Part 3: CANopen Reference, by Andrew Ayre

A pure reference section for all CANopen users. Key elements of CANopen are summarized in a way that allows a quick look-up. The core of this part is an Object Dictionary reference listing all Object Dictionary entries specified by the CiA CANopen standards DS301 and DS302.

- ✓ Frequently Asked Questions
- ✓ Physical Layer
- ✓ Data Types
- ✓ The Object Dictionary
- ✓ Minimal Object Dictionaries
- ✓ Communication Object Identifiers (COB IDs)
- ✓ Emergency Objects
- ✓ SDO Abort Messages
- ✓ Node States
- ✓ CANopen Glossary (provided by CiA)

www.canopenbook.com

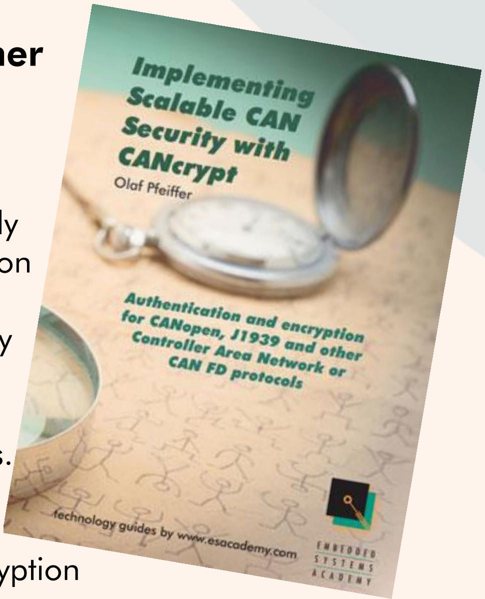
EmSA

CANcrypt Book

Security solutions for CAN, CAN-FD, CANopen, J1939 or other CAN based protocols and secure bootloading solutions

Any new development using embedded networks such as CAN, CAN-FD or any of the higher layer protocols like CANopen or J1939 should also focus on security aspects. Even if the network is considered closed at the time of development and has no "obvious" gateways to other networks: You cannot always rule out that at some point in the future a service technician installs remote access or diagnostics device to make his job easier. Or that a new device is officially developed and added to the network that offers similar access options due to market pressure.

The required system resources are not only minimal in comparison to traditional cryptography methods, they can also be scaled towards the system's security requirements. On the higher end, CANcrypt supports AES-128 based encryption and authentication.

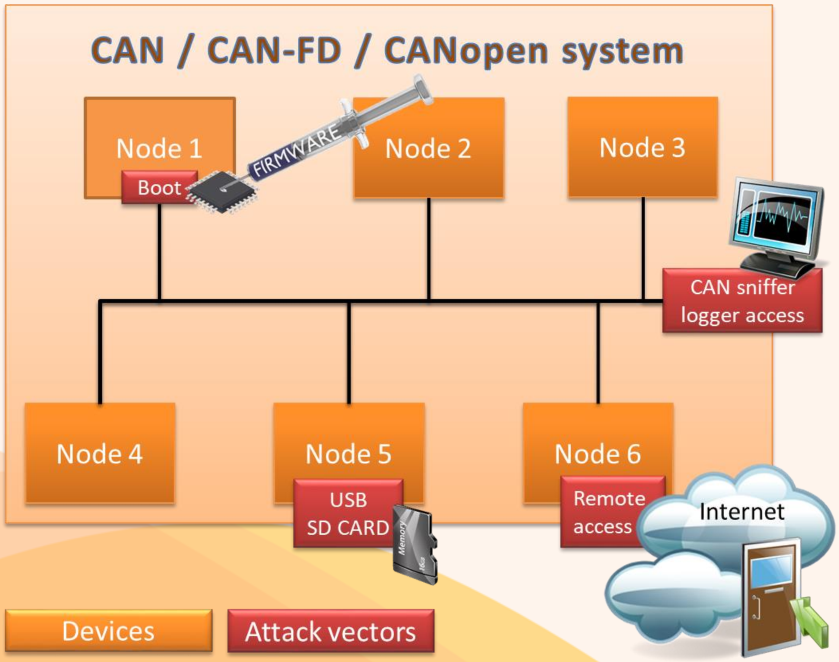

Implementing Scalable CAN Security with CANcrypt

Olaf Pfeiffer

Authentication and encryption for CANopen, J1939 and other Controller Area Network or CAN FD protocols

technology guides by www.esacademy.com

EMBEDDED SYSTEMS ACADEMY


CAN / CAN-FD / CANopen system

Node 1

Boot

FIRMWARE

Node 2

Node 3

CAN sniffer logger access

Node 4

Node 5

USB SD CARD

Node 6

Remote access

Internet

Devices

Attack vectors

Especially if firmware update support through a bootloader is somewhere on the horizon, ensure right from the start that only authorized parties can activate it in the first place.

The CANcrypt system adds different levels of security features to CAN. The basic functionality provided supports the grouping of multiple devices and authenticated communication between them based on a secure heartbeat.

The CANcrypt pairing mode is used to securely connect a configurator or active diagnostic tool to a single device. This ensures that only authorized parties can modify configurations or initiate software updates.

A key hierarchy allows the implementation of a smart, simplified key management supporting manufacturers, system builders/integrators and owners. The CANcrypt system is protocol independent and can be used with CANopen or other higher-layer CAN protocols. Up to 15 devices can participate in the secure communication. A manager / configurator is only required for the generation and exchange of keys, but not during regular operation.

Implementing Scalable CAN Security with CANcrypt

ISBN 978-0-9987454-0-4: Black and white paperback edition. Demo software matching the examples in the book is available for download.

ISBN 978-0-9987454-1-1: Full color hardcover edition including a commercial CANcrypt software version. The software license covers prototyping and an initial pilot production run of up to 500 devices.

www.cancrypt.eu

Flash Magic

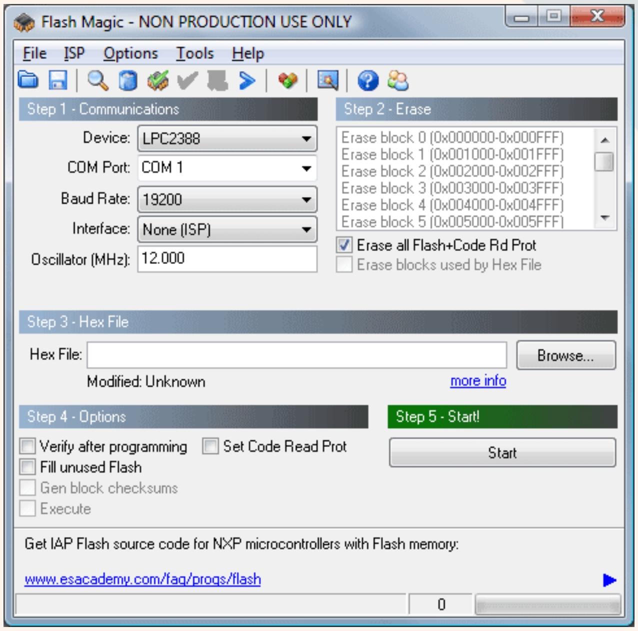
15+ years of Flashing

Flash programming tool for NXP's LPCxxx microcontroller families

Flash Magic is a PC tool for programming flash based microcontrollers from NXP using a serial or Ethernet protocol while in the target hardware.

Features

- Straightforward and intuitive user interface
- Five simple steps to erasing and programming a device and setting key options
- Programs Intel Hex Files
- Automatic verifying after programming
- Fills unused Flash to increase firmware security
- Automatically program checksums. Using the supplied checksum calculation routine your firmware can easily verify the integrity of a Flash block, ensuring no unauthorized or corrupted code can ever be executed
- Program security bits
- Check which Flash blocks are blank or in use with the ability to easily erase all blocks in use
- Read any section of Flash and save as an Intel Hex File
- Reprogram the Boot Vector and Status Byte with the help of confirmation features that prevent accidentally programming incorrect values
- Display the contents of Flash in ASCII and Hexadecimal formats
- Single-click access to the manual, Flash Magic home page and NXP Microcontrollers home page
- Use high-speed serial communications on devices that support it.
- Command Line interface allowing use in IDEs and Batch Files
- Manual in PDF format



Step 1 - Communications

Device: LPC2388

COM Port: COM 1

Baud Rate: 19200

Interface: None (ISP)

Oscillator (MHz): 12.000

Step 2 - Erase

Erase block 0 (0x000000-0x000FFF)
Erase block 1 (0x001000-0x001FFF)
Erase block 2 (0x002000-0x002FFF)
Erase block 3 (0x003000-0x003FFF)
Erase block 4 (0x004000-0x004FFF)
Erase block 5 (0x005000-0x005FFF)

☑ Erase all Flash+Code Rd Prot
□ Erase blocks used by Hex File

Step 3 - Hex File

Hex File:

Modified: Unknown

Step 4 - Options

□ Verify after programming
□ Set Code Read Prot
□ Fill unused Flash
□ Gen block checksums
□ Execute

Step 5 - Start!

Get IAP Flash source code for NXP microcontrollers with Flash memory:

www.esacademy.com/faq/progs/flash

0

- Supports half-duplex communications for many devices
- Verify Hex Files previously programmed
- Save and open settings
- Control the DTR and RTS RS232 signals to place the device into BootROM and Execute modes automatically (requires hardware support)
- Send commands to place the device in Bootloader mode
- Play any Wave file when finished programming
- Powerful, flexible Just In Time Code feature. Write your own JIT Modules to generate last minute code for programming, for example serial number generation.
- Displays information about the selected Hex File, including the creation and modification dates, flash memory used, percentage of the current device used

Order codes

ES-SFT-FMPS: Flash Magic Commercial

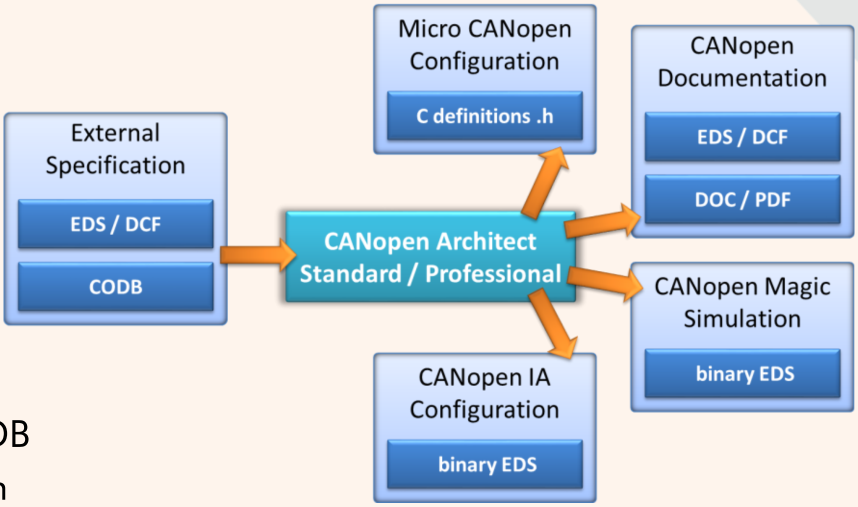
ES-SFT-FMPSN: Flash Magic Commercial .NET

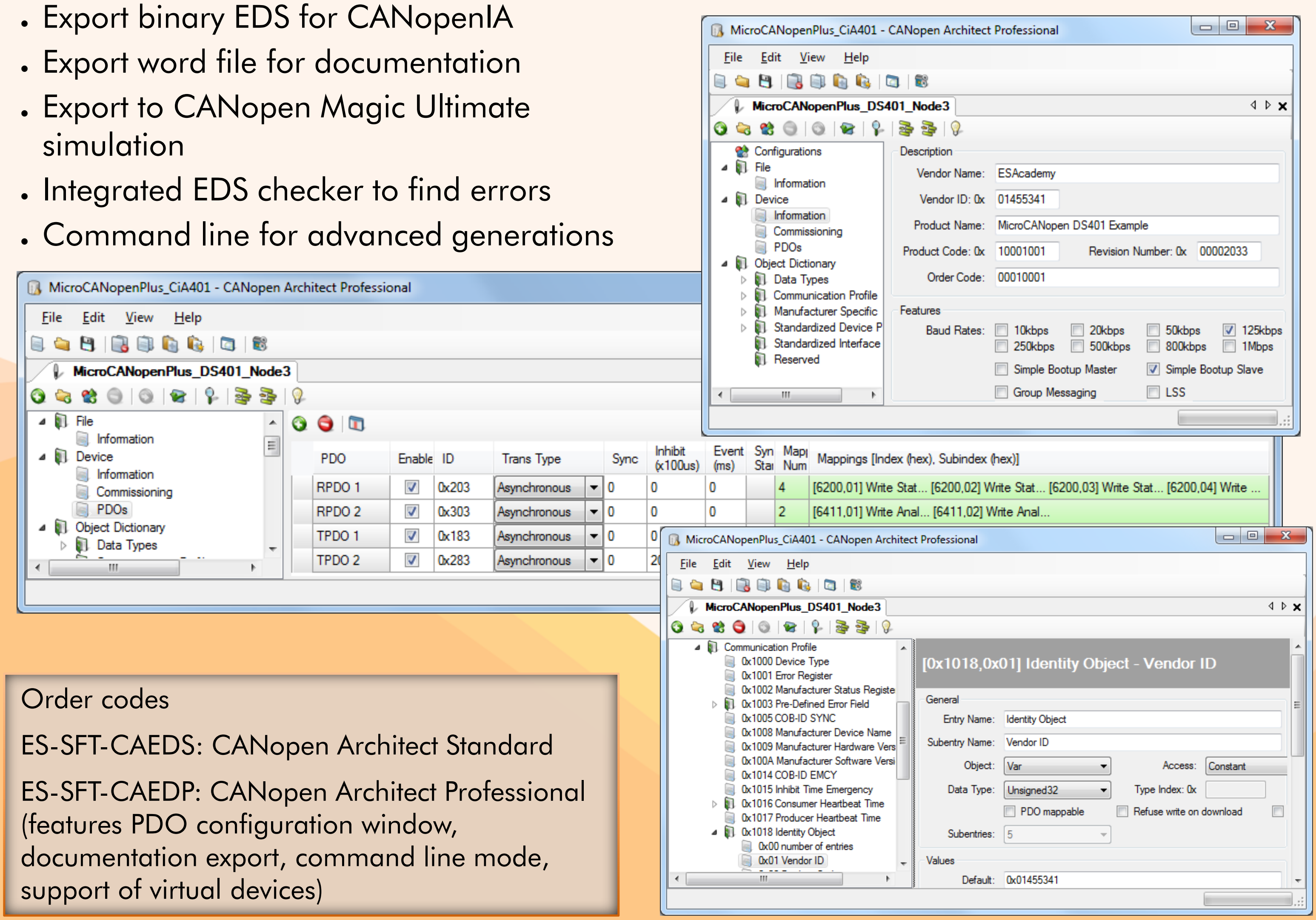
www.flashmagictool.com

EmSA CANopen Architect

CANopen EDS (Electronic Datasheet) and DCF (Device Configuration File) creation and editing tool. Supports various imports and exports.

- Add, edit and delete entries
- Cut, copy and paste to clipboard and between EDS/DCF files
- Specify device configuration, file info and commissioning details
- Autocorrection for obvious faults
- Support of Virtual Devices (Pro)
- Simplified PDO configuration (Pro)
- Import from existing EDS, DCF or CODB
- Export source code for Micro CANopen
- Export binary EDS for CANopenIA
- Export word file for documentation
- Export to CANopen Magic Ultimate simulation
- Integrated EDS checker to find errors
- Command line for advanced generations





Description

Vendor Name: ESAcademy

Vendor ID: 0x 01455341

Product Name: MicroCANopen DS401 Example

Product Code: 0x 10001001 Revision Number: 0x 00002033

Order Code: 00010001

Features

Baud Rates: □ 10kbps □ 20kbps □ 50kbps ☑ 125kbps □ 250kbps □ 500kbps □ 800kbps □ 1Mbps

□ Simple Bootup Master ☑ Simple Bootup Slave

□ Group Messaging □ LSS

PDO	Enable	ID	Trans Type	Sync	Inhibit (x100us)	Event (ms)	Syn Star	Mapp Num	Mappings [Index (hex), Subindex (hex)]
RPDO 1	☑	0x203	Asynchronous	0	0	0		4	[6200,01] Write Stat... [6200,02] Write Stat... [6200,03] Write Stat... [6200,04] Write ...
RPDO 2	☑	0x303	Asynchronous	0	0	0		2	[6411,01] Write Anal... [6411,02] Write Anal...
TPDO 1	☑	0x183	Asynchronous	0	0				
TPDO 2	☑	0x283	Asynchronous	0	20				

MicroCANopenPlus_CiA401 - CANopen Architect Professional
File
Edit
View
Help
MicroCANopenPlus_DS401_Node3
Communication Profile
0x1000 Device Type
0x1001 Error Register
0x1002 Manufacturer Status Registe
0x1003 Pre-Defined Error Field
0x1005 COB-ID SYNC
0x1008 Manufacturer Device Name
0x1009 Manufacturer Hardware Vers
0x100A Manufacturer Software Versi
0x1014 COB-ID EMCY
0x1015 Inhibit Time Emergency
0x1016 Consumer Heartbeat Time
0x1017 Producer Heartbeat Time
0x1018 Identity Object
0x00 number of entries
0x01 Vendor ID

[0x1018,0x01] Identity Object - Vendor ID

General

Entry Name: Identity Object

Subentry Name: Vendor ID

Object: Var Access: Constant

Data Type: Unsigned32 Type Index: 0x

□ PDO mappable □ Refuse write on download □

Subentries: 5

Values

Default: 0x01455341

Order codes

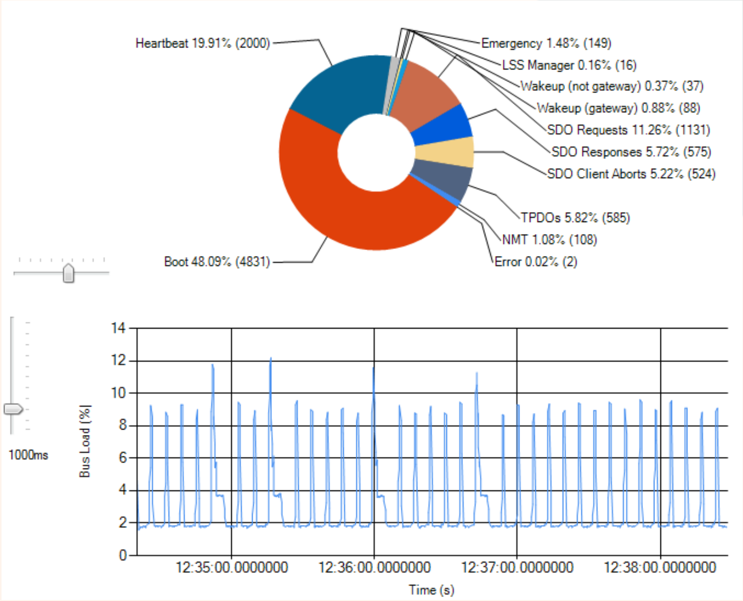
ES-SFT-CAEDS: CANopen Architect Standard

ES-SFT-CAEDP: CANopen Architect Professional (features PDO configuration window, documentation export, command line mode, support of virtual devices)

www.canopenarchitect.com

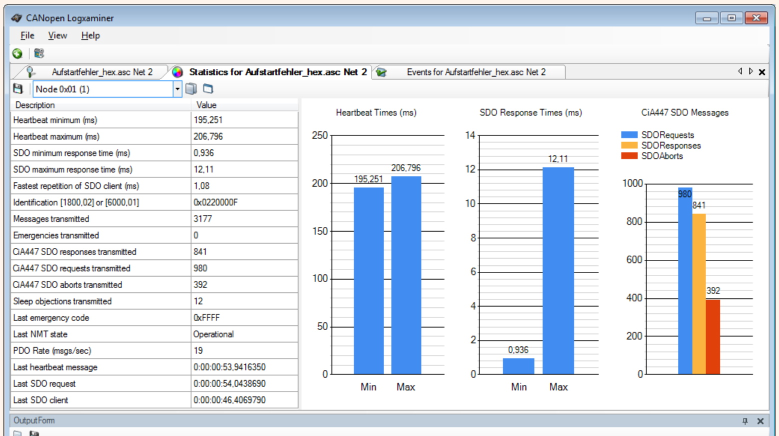
CANopen Logxaminer
Automated trace analysis

CANopen Logxaminer is a sophisticated log file analysis tool for CANopen networks



When it comes to long-time system monitoring or testing, a typical approach is to generate long-term logs containing CANopen traffic data covering multiple hours or sometimes even days. However, the often unsolved question is: how do I efficiently examine a log file with possibly 100s of thousands of CANopen messages? A typical approach is to load the log file into a spread sheet program and do manual searches, color highlighting and sometimes run custom scripts or macros to help locating issues.

EmSA's Logxaminer helps with the post analysis of such recordings. It creates statistics and event lists on a configurable level of detail. This drastically shortens the time to get "real results" out of a CANopen log recording made. Statistics are not only produced globally, there are dedicated statistic views for each node present on the network during the recording.

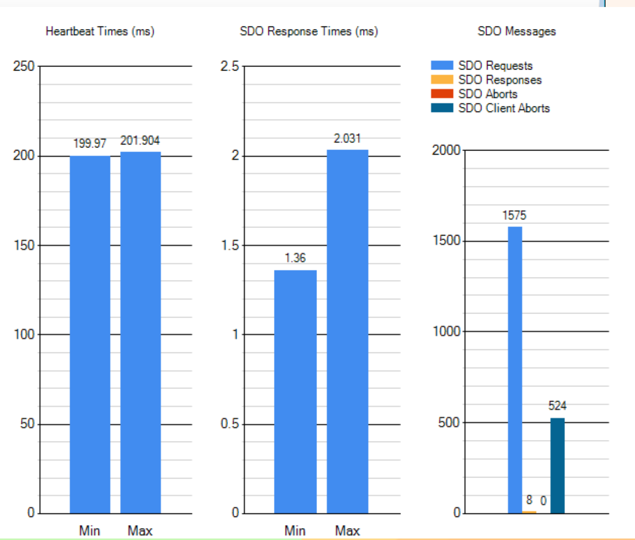


Description	Value
Heartbeat minimum (ms)	195,251
Heartbeat maximum (ms)	206,796
SDO minimum response time (ms)	0,936
SDO maximum response time (ms)	12,11
Fastest repetition of SDO client (ms)	1,08
Identification [1800,02] or [6000,01]	0x0220000F
Messages transmitted	3177
Emergencies transmitted	0
CiA447 SDO responses transmitted	841
CiA447 SDO requests transmitted	980
CiA447 SDO aborts transmitted	392
Sleep objections transmitted	12
Last emergency code	0xFFFF
Last NMT state	Operational
PDO Rate (msgs/sec)	19
Last heartbeat message	0:00:00:53,9416350
Last SDO request	0:00:00:54,0438690
Last SDO client	0:00:00:46,4069790

```
Finished parsing
Unknown log line 'internal events logged'
Found 7613 CAN messages
Started analysis of C:\Users\Olaf\Desktop\Tr
Finished analysis of C:\Users\Olaf\Desktop\T
Analysis took 0:00:06,3613639
```

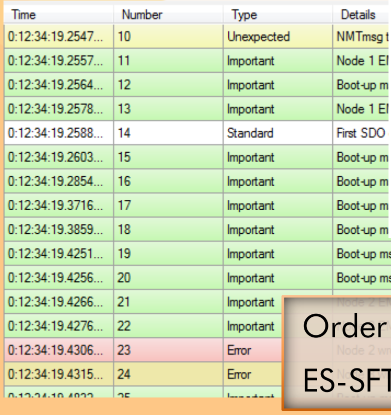
Per node statistics include:

- Minimum/maximum heartbeat time
- Minimum/maximum SDO response time
- Number of bootups
- Number of emergencies transmitted
- PDO message rate



The **Logxaminer** not only produces statistics, it also generates an event listing with all important system events. The event listing filters information from the log including:

- Node ID assignment (by LSS)
- Bootups (expected/unexpected)
- Emergencies
- SDO Aborts
- Unexpected messages
- Errors in LSS or SDO sequences



Time	Number	Type	Details
0:12:34:19.2547...	10	Unexpected	NMTmsg t
0:12:34:19.2557...	11	Important	Node 1 EI
0:12:34:19.2564...	12	Important	Boot-up m
0:12:34:19.2578...	13	Important	Node 1 EI
0:12:34:19.2588...	14	Standard	First SDO
0:12:34:19.2603...	15	Important	Boot-up m
0:12:34:19.2854...	16	Important	Boot-up m
0:12:34:19.3716...	17	Important	Boot-up m
0:12:34:19.3859...	18	Important	Boot-up m
0:12:34:19.4251...	19	Important	Boot-up msg node 2 : Time since reset: 170ms
0:12:34:19.4256...	20	Important	Boot-up msg node 8 : Time since reset: 171ms
0:12:34:19.4266...	21	Important	Node 2 EMCY reset 00h : EMCY 0000h-00h-00h 00h 00h 00h 00h
0:12:34:19.4276...	22	Important	: EMCY 0000h-00h-00h 00h 00h 00h 00h
0:12:34:19.4306...	23	Error	Node 2 wrong data : [1000h,0] invalid combination
0:12:34:19.4315...	24	Error	wrong data : [1000h,0] invalid combination
0:12:34:19.4822	25	Important	Boot-up msg node 32

Order code

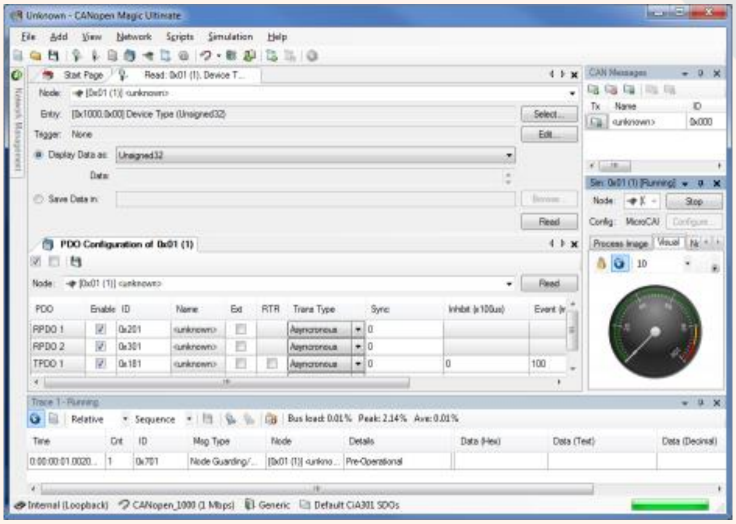
ES-SFT-COXM: CANopen Logxaminer

www.em-sa.com

CANopen Magic
Configuration and test tool

Professional CANopen configurator, monitor, analyzer, test tool and simulator available in three versions and as DLL for the creation of own service tools

CANopen Magic is a versatile software tool to monitor, analyze, trace, configure, simulate and test CANopen and CANopen FD networks and devices. It contains functions for the entire lifetime of a CANopen network: from development and test to system integration and performance analysis. Use sophisticated trace filtering and node access to monitor, analyze and test all aspects of your network. Simulate nodes that are still under development.



Node: [0x01 (1)] <unknown>
Entry: [0x1000.0x00] Device Type (Unsigned32)
Trigger: None
● Display Data as: Unsigned32
Data:
○ Save Data in:

Tx	Name	ID
	<unknown>	0x000

Sim: 0x01 (1) [Running]
Node:
Config: MicroCAI

PDO Configuration of 0x01 (1)
Node: [0x01 (1)] <unknown>

PDO	Enable	ID	Name	Ext	RTR	Trans Type	Sync	Inhibit (x100us)	Event (r
RPDO 1	☑	0x201	<unknown>	□		Asynchronous	0		
RPDO 2	☑	0x301	<unknown>	□		Asynchronous	0		
TPDO 1	☑	0x181	<unknown>	□	□	Asynchronous	0	0	100

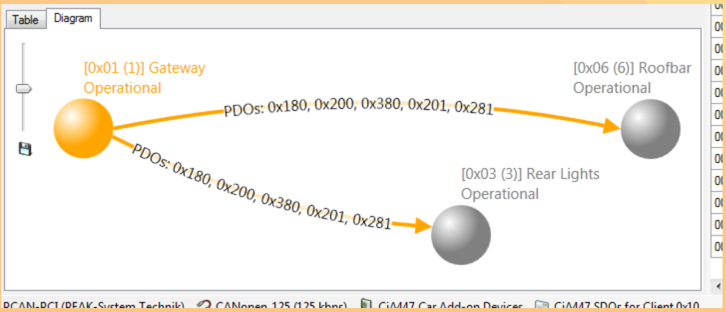
Trace 1 - Running
Relative Sequence Bus load: 0.01% Peak: 2.14% Ave: 0.01%

Time	Cnt	ID	Msg Type	Node	Details	Data (Hex)	Data (Text)	Data (Decimal)
0:00:00:01.0020...	1	0x701	Node Guarding/...	[0x01 (1)] <unkno...	Pre-Operational			

Internal (Loopback) CANopen_1000 (1 Mbps) Generic Default CiA301 SDOs

Features (Version depending):

- Read and write to nodes using SDOs
- SDO expedited, segmented and block modes
- Transmit CAN messages
- Display network overview
- Network management (NMT)
- Trace windows
- Display and configure PDOs
- Read/write device configuration files (DCF)
- Custom SDO channels
- Custom vendor names
- Custom device types
- Custom error codes
- Custom abort codes
- Can describe nodes (name, EDS)
- Trace filter scripts
- CANopen manager configuration
- Layer Setting Services (LSS) support
- Display process data meters, graphs, LEDs, etc.
- Replay log files
- Trace window filtering
- Trace window continuous (long term) recording
- CiA 447 Car Add-on Devices support
- Multiple node setup windows
- Multiple PDO configuration windows
- Multiple node read windows
- Multiple node write windows
- Node Object Dictionary Overview and Access
- Python Script API, Editors and Interpreters
- Simulated nodes
- Automatic object dictionary simulation from an EDS or DCF
- Automatic generation of network diagrams
- Trace analysis graphs and charts
- Supports real CAN interfaces
- PEAK CAN interface support
- Kvaser CAN interface support
- VSCOM NET-CAN 110 interface support
- Command line interface



PCAN-PCI (PEAK-System Technik) CANopen 125 (125 kbps) CiA447 Car Add-on Devices CiA447 SDOs for Client 0x10

Order codes

ES-SFT-COMS: CANopen Magic Standard
ES-SFT-COMP: CANopen Magic Professional
ES-SFT-COMU: CANopen Magic Ultimate
ES-SFT-PCDEV: CANopen Magic DLL

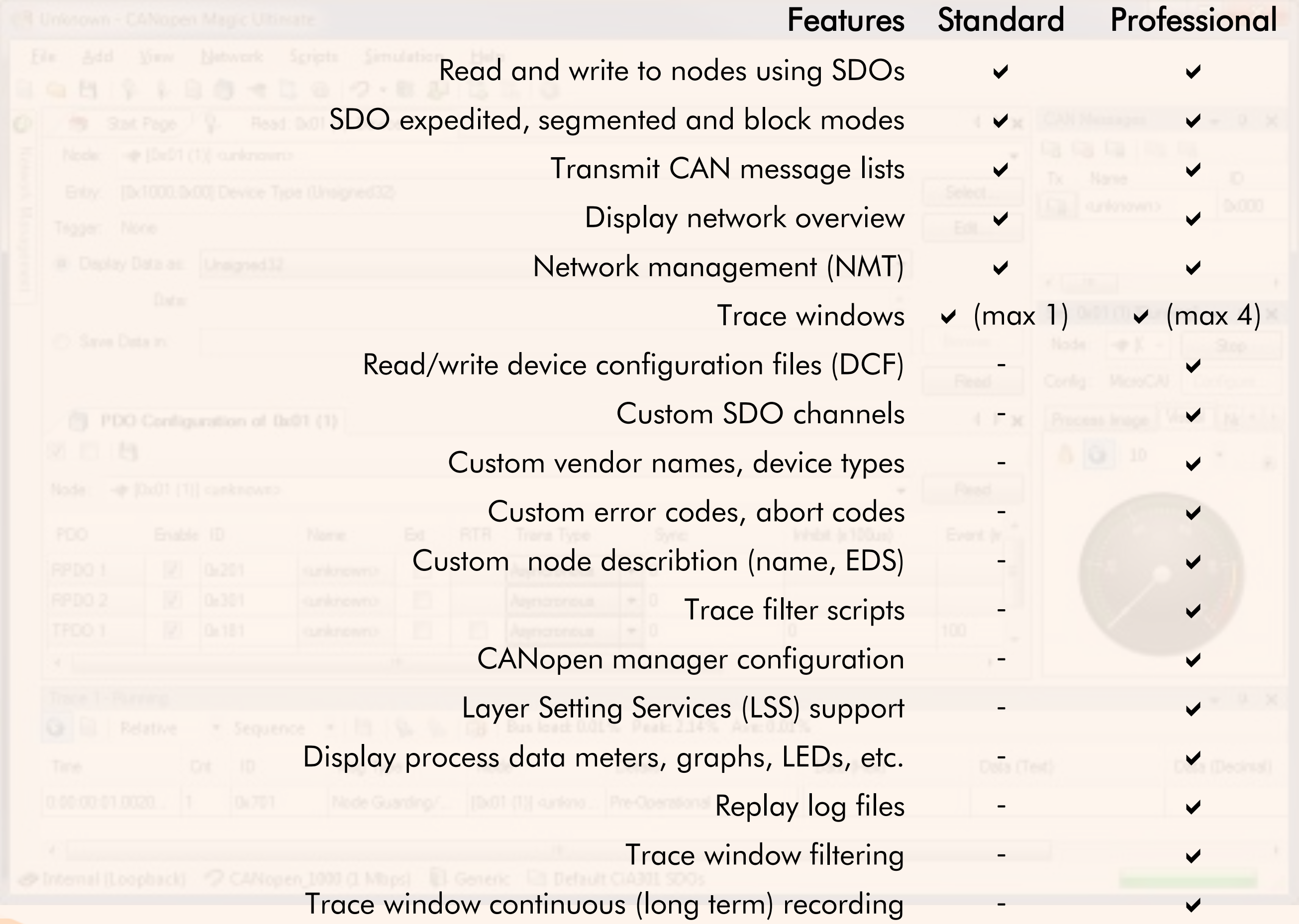
Version comparison

www.canopenmagic.com

CANopen Magic
Versions

CANopen Magic is available in the versions Standard, Professional and Ultimate. The optional DLL version allows the implementation of custom service tools.

All versions support both CANopen and CANopen FD.



Features	Standard	Professional	Ultimate
Read and write to nodes using SDOs	✓	✓	✓
SDO expedited, segmented and block modes	✓	✓	✓
Transmit CAN message lists	✓	✓	✓
Display network overview	✓	✓	✓
Network management (NMT)	✓	✓	✓
Trace windows	✓ (max 1)	✓ (max 4)	✓ (max 4)
Read/write device configuration files (DCF)	-	✓	✓
Custom SDO channels	-	✓	✓
Custom vendor names, device types	-	✓	✓
Custom error codes, abort codes	-	✓	✓
Custom node describtion (name, EDS)	-	✓	✓
Trace filter scripts	-	✓	✓
CANopen manager configuration	-	✓	✓
Layer Setting Services (LSS) support	-	✓	✓
Display process data meters, graphs, LEDs, etc.	-	✓	✓
Replay log files	-	✓	✓
Trace window filtering	-	✓	✓
Trace window continuous (long term) recording	-	✓	✓
CiA 447 Car Add-on Devices support	-	✓	✓
Multiple node setup windows	-	✓ (max 10)	✓ (max 10)
Multiple PDO configuration wizard windows	-	✓ (max 10)	✓ (max 10)
Multiple node read and write windows	-	✓ (max 10)	✓ (max 10)
Node Object Dictionary Overview and Access	-	✓ (max 1)	✓ (max 10)
Python Script API, Editors and Interpreters	-	-	✓ (max 10)
Simulated nodes	-	-	✓ (max 127)
Automatic object dictionary simulation from an EDS or DCF	-	-	✓
Automatic generation of network diagrams	-	-	✓
Trace analysis graphs and charts	-	-	✓
CAN Interfaces supported: PEAK, Kvaser, VSCOM NET-CAN 110	✓	✓	✓
Command line interface	✓	✓	✓

Micro CANopen Plus
CANopen C source code

Powerful and flexible CANopen compliant source code supporting a wide range of microcontrollers, compilers, CANopen device and application profiles

Micro CANopen Plus is a small-footprint, commercial-grade CANopen implementation with advanced features. Ideal for situations requiring medium configurability during run-time and great performance on any type of platform, and for building networks that include manager nodes, Micro CANopen Plus provides the most flexible solution. Auto-generated configuration from the EDS/DCF file makes its setup a quick and painless one-step process.

Portable. Micro CANopen Plus is written in 100% standard ANSI C code allowing for straightforward porting.

Compact. ROM specifications: 7K - 14K bytes.

Feature Highlights

- Code configured from EDS or DCF file with our CANopen Architect software
- CANopen NMT State Machine
- Object Dictionary with Process Image
- Expedited, segmented and block-transfer SDO
- Multiple SDO servers
- Optional fully-meshed (matrix) SDO
- PDO with runtime-configurable event time, inhibit timer, transmission type and SYNC
- Heartbeat and EMCY producer and consumer
- Non-volatile save/restore of parameters
- Extensive call-back API interface
- Access hooks for RTOS-based applications

Order codes

ES-LIC-MCOP	Micro CANopen Plus source code
ES-LIC-MCOP-XX	Various drivers available
ES-LIC-MCOP-PC	PEAK PCAN driver support
ES-LIC-MCODYN	Extended OD / PDO functions
ES-LIC-MCOMGR	Manager functions

Micro CANopen Plus is delivered with an example CiA401 (Generic I/O) implementation and drivers for NXP ARM and CANopen Magic Ultimate simulation. Customized examples for other device profiles are available under our consulting services.

Our stack example application passes the official CANopen Conformance Test!

Full documentation is supplied. All software products include a one-year maintenance and priority support agreement that can be extended anytime.

Also included is a single license for our CANopen Architect, an EDS/DCF editor with code generation for quick stack configuration.

Currently Available Ports

The following list has some of the microcontroller and compiler combinations that Micro CANopen Plus is currently available for as (optional) add-ons. More combinations are available, please contact us with your requirements. For currently unsupported combinations you can either perform the port yourself or we can perform it for you.

- PC Simulation (with CANopen Magic Ultimate, always included)
- NXP LPC ARM7, Cortex-Mx families w/ Realview, LPCXpresso, IAR, GCC (some always included)
- ST STM32 family w/ Realview, IAR, GCC
- Microchip PIC18 family w/ MPLABX and XC8
- Microchip/Atmel AVR w/ WinAVR, ImageCraft
- NXP/Freescale S08/S12 family w/ CodeWarrior
- TI TM4C12x family w/ Realview
- TI TMS470 family w/ Realview
- Peak System PCAN interfaces w/ MS Visual C++

www.microcanopen.com

EmSA

CANopenIA

CANopen coprocessor

Devices, modules and chips that provide a host microcontroller system with instant access to CANopen using a simple serial interface.

CANopenIA is a concept developed by ESAcademy that helps you to easily build CANopen devices. Access, test or control the devices/nodes connected to a CANopen network. Build sensors, actuators or other devices with a CANopen interface. The main benefits of CANopenIA are:

Decreased complexity level

- Simple setup through CANopen Architect or dedicated setup software
- Only minimal CANopen knowledge required
- Simplified software development

Increased security level

- Fewer attack points for intruders
- In coprocessor mode, CANopenIA acts as a firewall between CANopen and host

Faster time-to-market

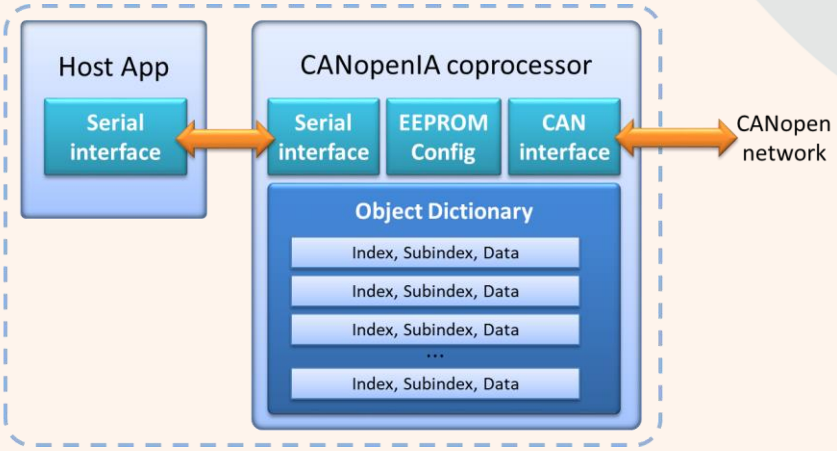
- Minimized software development
- Faster test cycles

Available Devices

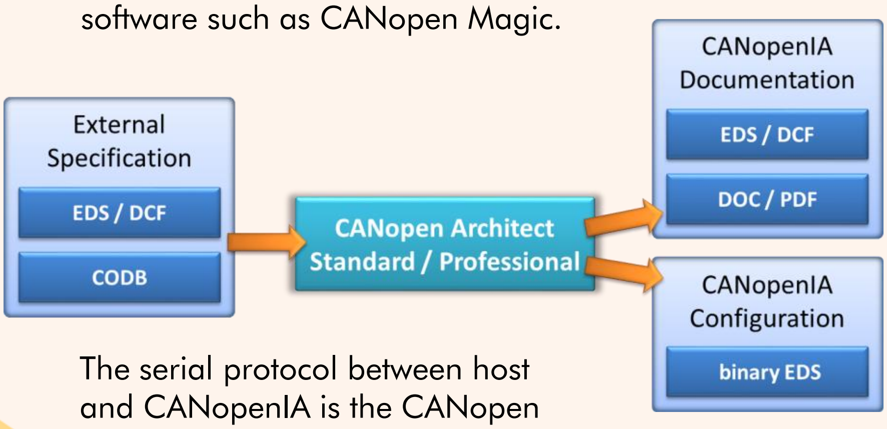
- CANgineLight (CANopen – RS232)
- PCAN-RS232 (CANopen – RS232)
- CANgineII-BT (CANopen – Bluetooth)

Supported Chips

NXP:	LPC11C24
ST:	STM32F042
	STM32F091



Use ESAcademy's CANopen Architect software to start a new configuration or import an existing one, for example an EDS (Electronic Data Sheet) or CODB (CANopen data base) file. Once the desired configuration is finished, save it as EDS or binary EDS. Then, transfer the binary EDS configuration to a CANopenIA implementation using any CANopen configuration software such as CANopen Magic.



The serial protocol between host and CANopenIA is the CANopen remote access protocol by ESAcademy. It supports reporting events (new data arrived on CANopen side) as well as reading and writing data of the local Object Dictionary.

CANopen Manager or CiA 447 implementations also support read and write accesses to Object Dictionary entries of any node connected to the CANopen network. For more information visit our dedicated web page www.canopenia.com.

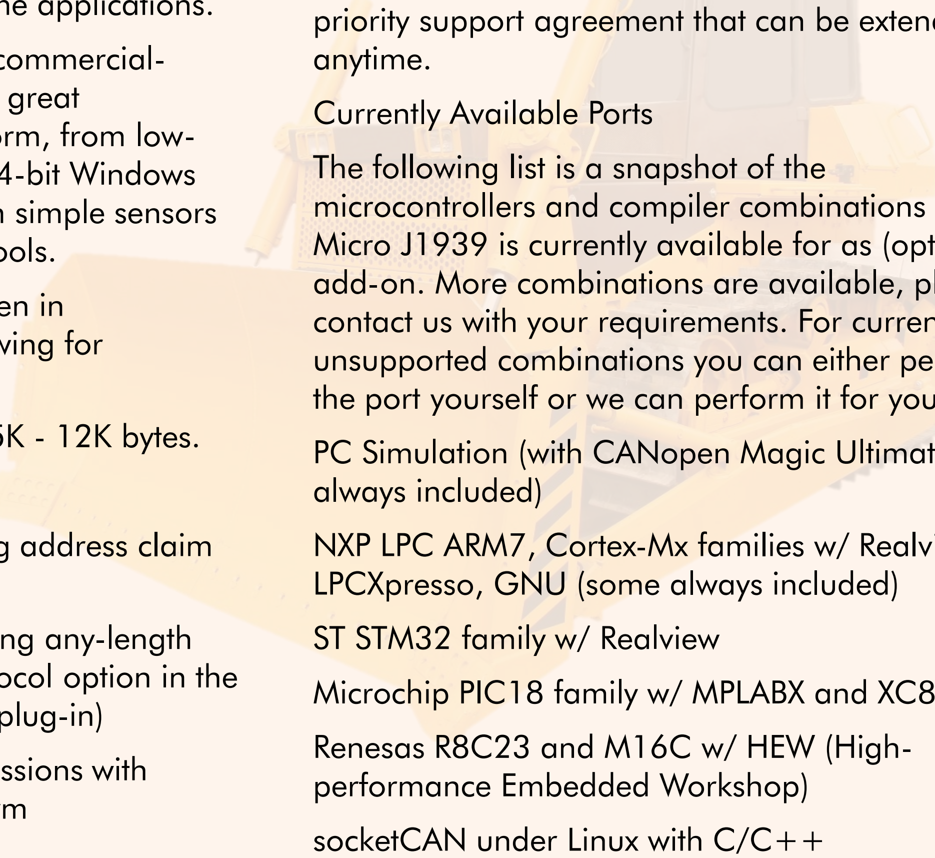
www.canopenia.com

Micro J1939

SAE J1939 C source code

Compact and flexible SAE J1939 compliant source code supporting a wide range of microcontrollers, compilers and SAE J1939 protocol variations

The J1939 communication standard was developed by the Society of Automotive Engineers (SAE). It is based on CAN high-speed communications and primarily used in heavy-truck and off-road vehicle applications. The NMEA 2000 variant is primarily used in maritime applications.



Micro J1939 is a small-footprint, commercial-grade J1939 implementation with great performance on any type of platform, from low-end 8-bit microcontrollers up to 64-bit Windows PCs, ideal for building nodes from simple sensors up to SAE J1939-73 diagnostics tools.

Portable. Micro J1939 Plus is written in 100% standard ANSI C code allowing for straightforward porting.

Compact. ROM specifications: 3.5K - 12K bytes.

Feature Highlights

- Network management including address claim and commanded address.
- Sending, receiving and requesting any-length PGNs, using any transport protocol option in the standard (with the appropriate plug-in)
- Persistent periodic PGN transmissions with highest precision on any platform
- Extensive call-back API interface

Micro J1939 is delivered with full source code and an example implementation with drivers for NXP ARM and CANopen Magic Ultimate simulation.

Full documentation is supplied. All software products include a one-year maintenance and priority support agreement that can be extended anytime.

Currently Available Ports

The following list is a snapshot of the microcontrollers and compiler combinations that Micro J1939 is currently available for as (optional) add-on. More combinations are available, please contact us with your requirements. For currently unsupported combinations you can either perform the port yourself or we can perform it for you.

PC Simulation (with CANopen Magic Ultimate, always included)

NXP LPC ARM7, Cortex-Mx families w/ Realview, LPCXpresso, GNU (some always included)

ST STM32 family w/ Realview

Microchip PIC18 family w/ MPLABX and XC8

Renesas R8C23 and M16C w/ HEW (High-performance Embedded Workshop)

socketCAN under Linux with C/C++

Peak System PCAN interfaces w/ MS Visual C++

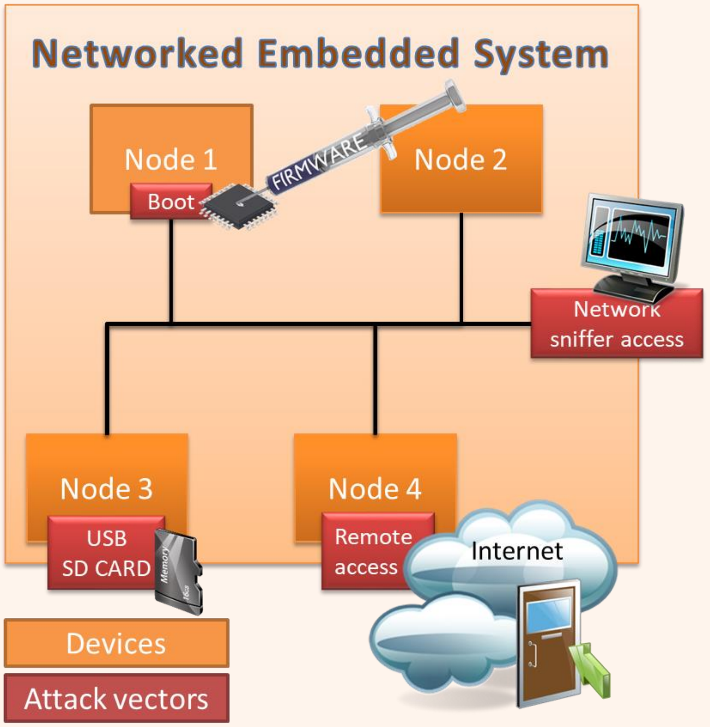
Order codes

ES-LIC-MJ1939	Micro J1939 source code
ES-LIC-MJ1939-XX	Micro J1939 driver
ES-LIC-MJ1939-BAM	plug-in broadcast announce message mode
ES-LIC-MJ1939-CMDT	plug-in peer-to-peer transport protocol
ES-LIC-MJ1939-FP	plug-in fast-packet transport protocol for NMEA 2000
ES-SFT-J1939-PCDEV	Micro J1939 as native and .NET DLL with examples

Bootloading

Secure update solutions

Securely updating firmware and software of embedded systems through embedded networks like CAN, CANopen, RS-232, I2C, SPI or Ethernet



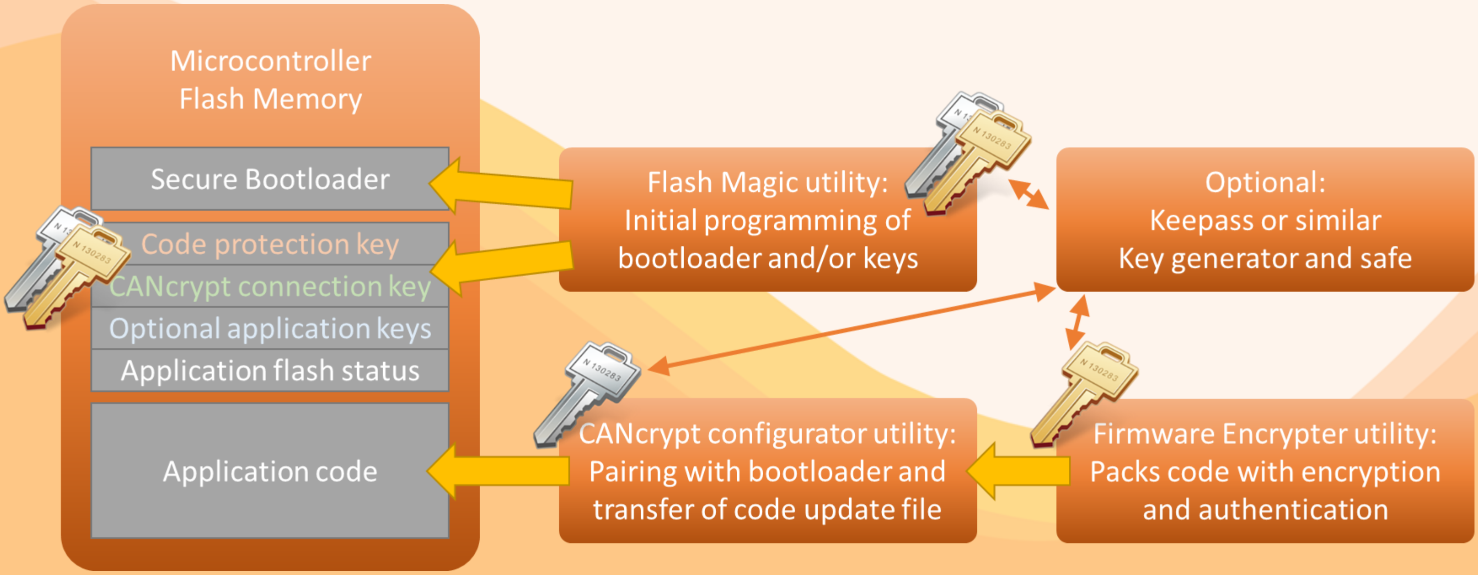
Many embedded systems feature a variety of communication channels. Even if these channels primarily connect to internal, closed networks only, there is always a security risk that networks get compromised.

Being able to update the firmware of embedded systems allows applying security updates. However, the update process must be secured to prohibit intruders to install malicious software.

Our secure bootloader solutions are framework based and support multiple security and key methods based on symmetric or private/public key systems. Multiple security layers allow security updates based on different keys to individually authenticate manufacturers and service technicians or system integrators. Only the manufacturer can produce authenticated code and only the service technician or system integrator can activate the bootloader of an embedded system.

Our engineers have been working on embedded security solutions since 2014. They are regular participants in the SIG (Special Interest Group) CAN/CANopen Security and have published several articles about Embedded Ransomware and other embedded security aspects.

We provide software security solutions for lightweight communication channels and bootloading scenarios. Contact us to find out how we can help.


Microcontroller Flash Memory
Secure Bootloader
Code protection key
CANcrypt connection key
Optional application keys
Application flash status
Application code
Flash Magic utility: Initial programming of bootloader and/or keys
Optional: Keepass or similar Key generator and safe
CANcrypt configurator utility: Pairing with bootloader and transfer of code update file
Firmware Encrypter utility: Packs code with encryption and authentication

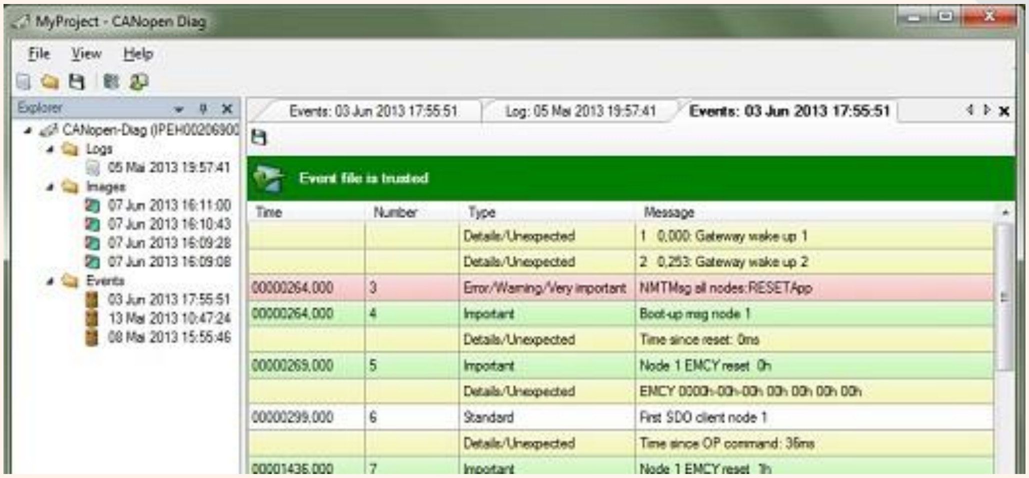
www.em-sa.com/security

EmSA

CANopen MiniDiag
Hand-held Diagnostics

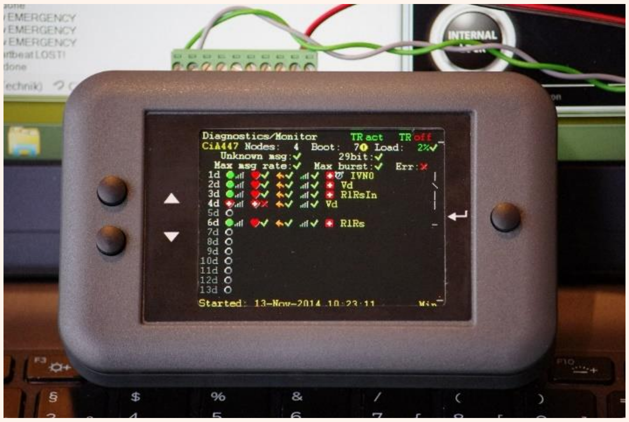
The CANopen MiniDiag hand-held unit provides flexible and sophisticated CANopen testing. Ideal for in application testing or workshop environments.

The CANopen MinDiag devices are compact, hand-held diagnostic and test devices for CANopen networks. Being a dedicated hand-held device the CANopen MiniDiag is especially suited for in-the-field use to perform diagnostic functions directly at machinery or vehicles. A continuous logging mode collects data for later analysis, for example with our optional Logxaminer software.


MyProject - CANopen Diag
File
View
Help
Explorer
Events: 03 Jun 2013 17:55:51
Log: 05 Mai 2013 19:57:41
Events: 03 Jun 2013 17:55:51
Event file is trusted

CANopen-Diag (PEH00206900
- Logs
  - 05 Mai 2013 19:57:41
- Images
  - 07 Jun 2013 16:11:00
  - 07 Jun 2013 16:10:43
  - 07 Jun 2013 16:09:28
  - 07 Jun 2013 16:09:08
- Events
  - 03 Jun 2013 17:55:51
  - 13 Mai 2013 10:47:24
  - 08 Mai 2013 15:55:46

Time	Number	Type	Message
		Details/Unexpected	1 0,000: Gateway wake up 1
		Details/Unexpected	2 0,253: Gateway wake up 2
00000264,000	3	Error/Warning/Very important	NMTMsg all nodes:RESETApp
00000264,000	4	Important	Boot-up msg node 1
		Details/Unexpected	Time since reset: 0ms
00000269,000	5	Important	Node 1 EMCY reset 0h
		Details/Unexpected	EMCY 0000h-00h-00h 00h 00h 00h 00h
00000299,000	6	Standard	First SDO client node 1
		Details/Unexpected	Time since OP command: 36ms
00001436,000	7	Important	Node 1 EMCY reset 1h


INTERNAL
Diagnostics/Monitor TR act TR off
CiA447 Nodes: 4 Boot: 7 Load: 2%
Unknown msg: 29bit:
Max msg rate: Max burst: Err:
1d IVNO
2d Vd
3d R1RsIn
4d Vd
5d
6d R1Rs
7d
8d
9d
10d
11d
12d
13d
Started: 13-Nov-2014 10:23:11 Min

CANopen Network Status Overview

The status overview provides a summary of the most important information: the number of nodes found, number of boot-up messages, current bus load, longest message burst, SDO usage and LSS usage.

For each node found: its NMT status, its min/max heartbeat, its current message rate generated and node info where available (e.g. names of Virtual Devices implemented by a device)

Important Events History

The events history is a trace of the most important network events including LSS node ID assignments, NMT commands, boot-ups, emergencies, SDO aborts, first PDO use and time since reset.

Further functions and features include

- Power: extern 7-30V (not included)
- CiA447 Application Profile support
- Active network scan
- Single device control (NMT commands, LSS Master commands, generic SDO access)
- Executing write/configuration sequences
- Executing bootloader sequences to load firmware into devices
- Recognizing Virtual Devices where supported
- Execute CDCF (Concise Device Configuration File)

CiA 447 Tester or Gateway Simulation

The CANopen MiniDiag hand held module can be set into a CiA 447 tester mode as specified by the CiA 447 documents. It becomes an active node and can produce specified background traffic.

The optional gateway simulation turns the Diag into a CiA 447 gateway.

Order code

ES-DIAG-MINI: CANopen Mini Diag
ES-DIAG-SIM447: Mini Diag with 447 gateway SW

CANopen Diag
Hand-held CANopen Tester

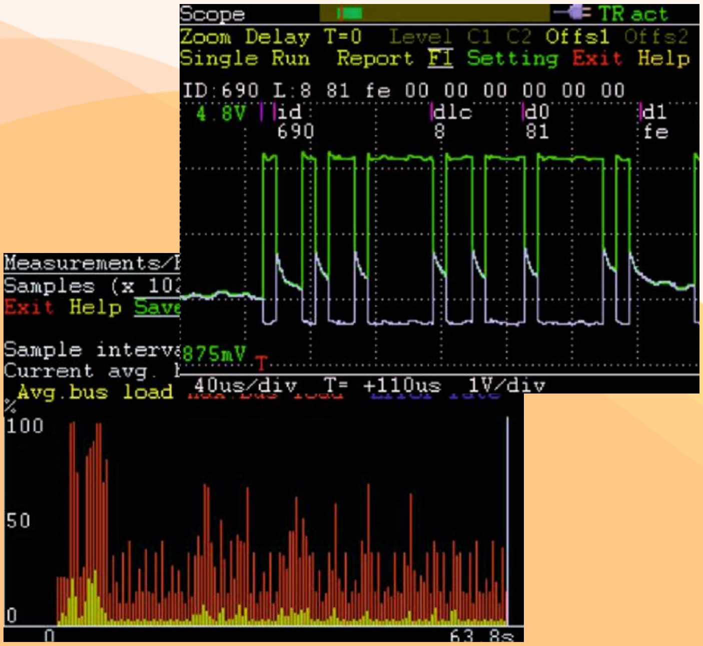
The CANopen Diag unit provides all functions of the MiniDiag plus hardware measurements like a CAN oscilloscope and the optional CANopen Test Machine

The CANopen Diag devicess are compact, hand-held diagnostic and test devices for entire CANopen networks as well as for single Devices Under Test (DUT). It operates on batteries (4 x AA) or external power supply.

The diagnostic functions includes physical layer measurements:

Physical Layer and Generic CAN

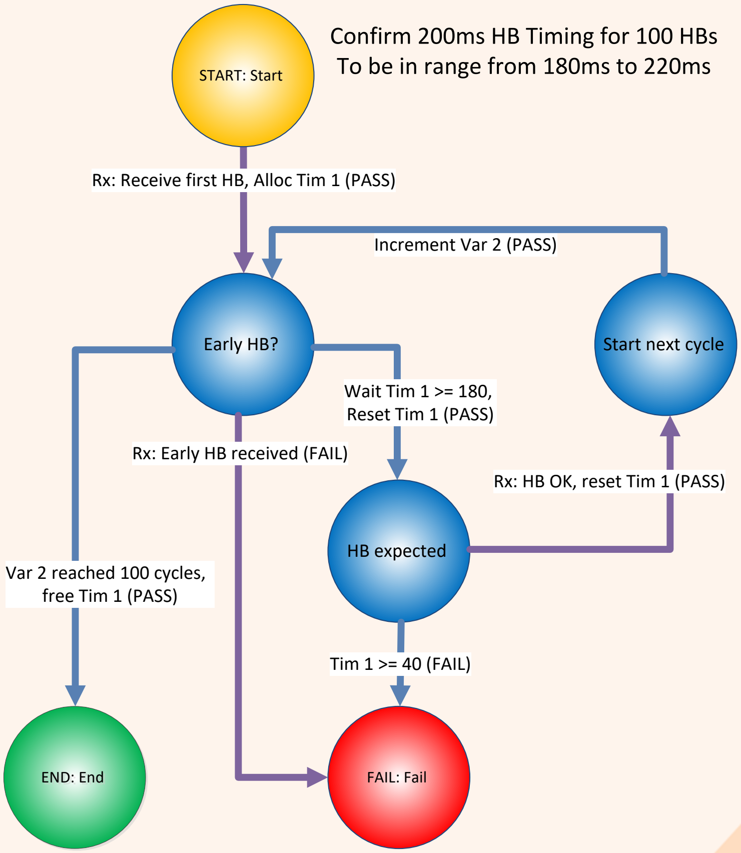
- Termination resistor measurement
- Voltage at pins measurements
- Bus load measurements and statistics
- CAN oscilloscope



ID:690 L:8 81 fe 00 00 00 00 00 00

CANopen Test Machine

The tests are based on a state machine with transition rules triggered by the transmission or reception of a CAN message and conditions that include timers and counters. Each individual transition rule can contribute towards a test result by specifying if this transition should add to the fail counter. The test graphs can be drawn with Microsoft Visio®, provided macros auto-generate the test script from the graph.


START: Start
Confirm 200ms HB Timing for 100 HBs
To be in range from 180ms to 220ms
Rx: Receive first HB, Alloc Tim 1 (PASS)
Increment Var 2 (PASS)
Early HB?
Start next cycle
Wait Tim 1 >= 180,
Reset Tim 1 (PASS)
Rx: Early HB received (FAIL)
Rx: HB OK, reset Tim 1 (PASS)
HB expected
Var 2 reached 100 cycles,
free Tim 1 (PASS)
Tim 1 >= 40 (FAIL)
END: End
FAIL: Fail

Order codes

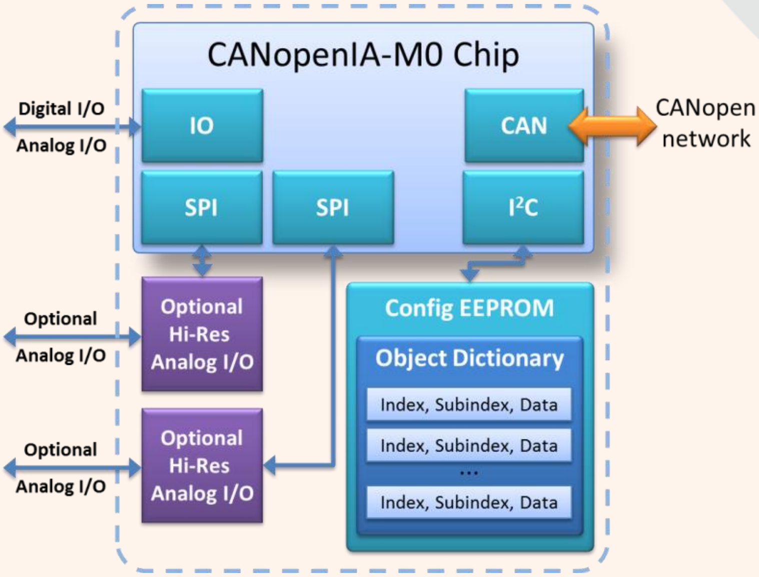
ES-DIAG-BAS: CANopen Diag
ES-DIAG-COP: CANopen Diag with test machine
ES-DIAG-443: CiA 443 add-on for CANopen Diag
ES-DIAG-447: CiA 447 add-on for CANopen Diag

www.canopendiag.de

CANopenIA-M0
Stand-alone CANopen I/O

Modules and chips by Embedded Systems Solutions that provide instant access to digital and analog CANopen input or output signals.

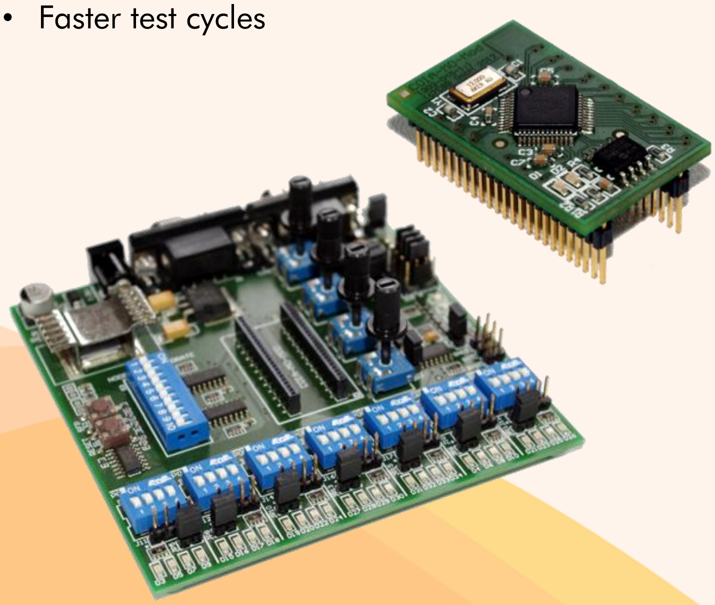
CANopenIA is a concept developed by ESAcademy that helps you to easily build CANopen devices. Quickly develop devices or nodes connected to a CANopen network. Build sensors, actuators or other devices with access to CANopen systems. The main benefits of CANopenIA are:



Decreased complexity level
- Simple setup through CANopen Architect or dedicated setup software
- Only minimal CANopen knowledge required
- No software development

Increased security level
- Fewer attack points for intruders

Faster time-to-market
- No software development
- Faster test cycles



Configurations can be generated and loaded using the provided CANopenIA-M0 setup utility. The chip's configuration gets stored in an EEPROM. Configurable parameters include:
- Port configurations for a total of 28 signals
  - 4 signals per port
  - any port can be digital input ot output
  - one port can be analog output (10bit ADC)
  - one port can be SPI ananlog input (12bit ADC)
  - one port can be SPI analog output (12bit DAC)
- Port to Object Dictionary assignment
  - which signal is where in Object Dicitonary
- CANopen PDO (Process Data Object) configuration
  - communication and mapping parameters

The CANopen standards implemented by CANopenIA-M0 include
- CiA301 version 4.2 CANopen Application layer and communication profile
- CiA305 version 2.2.14 LSS, node ID assignment using Layer Setting Services and protocols
- CiA401 version 3.0 Device Profile for generic I/O modules

Available Products from Embedded Systems Solutions GmbH
- CANopenIA-M0 Chip
48-pin LQFP (9x9mm)
- CANopenIA-M0 Module
48-pin 1.27mm grid
- CANopenIA-M0 Starter Kit

www.canopenia.com

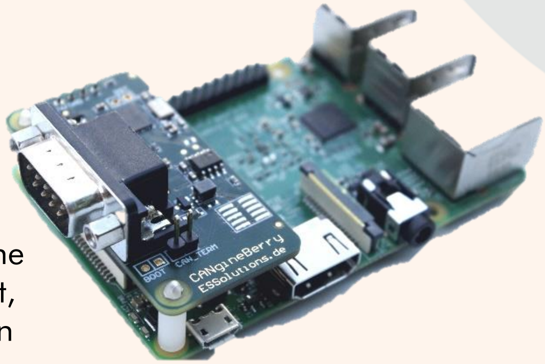
EmSA CANgineBerry

Active CANcrypt and CANopen module for Raspberry Pi and other embedded computing platforms

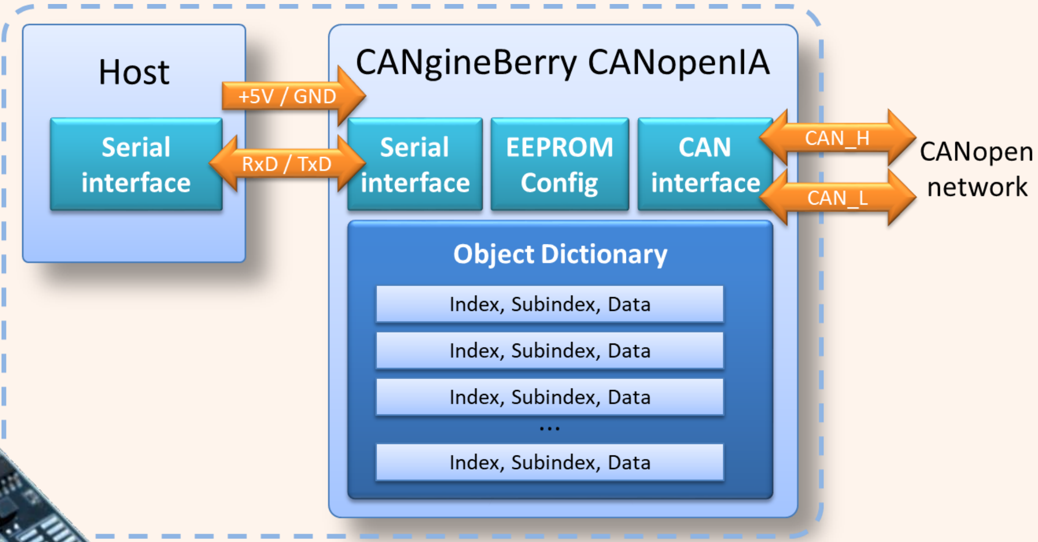
The CANgineBerry CANopen is an active CAN co-processor module that uses a regular UART communication channel towards the host system. With its independent 32-bit microcontroller, the CANgineBerry can easily execute CAN protocols with tough timing demands such as CANcrypt or CANopen with response times of under 10 ms.

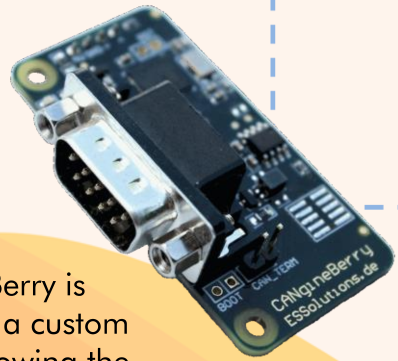
Depending on the configuration, the CAN communication can be up and running within 50 ms after power-on, even if the host system takes significantly longer to boot.

Available firmware options at launch include a generic minimal CANopen Manager based on the CANopenIA implementation and a secure CANcrypt version of the popular Lawicel protocol (SLCAN).



The connection to the host system uses only four pins: Two for power (5V) and two for the UART. The four-pin header row directly matches the Raspberry Pi pin layout, but also other common connectors, such as the popular PL2303 USB-to-UART converter modules.





Technical data

- The CANgineBerry is equipped with a custom bootloader allowing the installation of one of the firmware packages provided by Embedded Systems Academy. Check our web page for available firmware packages.
- Two LEDs (green and red) indicate the network connection status.
- EEPROM to store configuration data.
- CAN termination configuration by jumper.
- Based on a Cortex-M0 microcontroller.

The serial protocol between host and CANopenIA is the CANopen remote access protocol by Embedded Systems Academy. It supports reporting events (new data arrived on CANopen side) as well as reading and writing data of the local Object Dictionary.

The CANopen Manager performs automatic network scans, simplifying application code as it can directly access the data scanned.

CANopen Manager implementations also support read and write accesses to Object Dictionary entries of any node connected to the CANopen network.

www.cangineberry.com