CANopen Safety in Mobile Machines

Roland Wagner (Ingo Hornberger, Stefan Blasi)

Control applications for ECUs in mobile machines are nowadays realized either with proprietary software or IEC 61131-3 tools. A significant number of machines needs certifying according to Safety standards, e.g. the EN/ISO 13849. Both device manufacturers and machine builders profit from a validation of the IDE (Integrated Development Environment) for Safety critical applications. In order to access sensors and actors of the machine, it is necessary, to have a Safety certified fieldbus system. CANopen Safety provides the ideal solution: an on-hand and certified system.

Each product launch in the Mobile Machines area nowadays requires not only the availability of functional properties, but also a risk analysis. According to the risk analysis results, potential dangers may be localized and limited by means of technical safety activities. If ECUs (**E**lectronic **C**ontrol **U**nits) are used to cover these activities, there are (at least) two aspects that must be considered: Firstly, the data exchange between the devices, sensors and actors. Secondly, the functional application running on the ECU.

Means of choice: CANopen Safety

The CANopen Safety protocol (CiA 304) developed by the international users' and manufacturers' group CAN in Automation (CiA), was published in 2010 as a European standard EN 50325-5. The protocol allows the transmission of safety-relevant data via CAN networks according to the IEC 61508 standard. TÜV Rheinland, one of the German Technical Supervisory Associations, has approved the protocol for use in systems requiring up to Safety Integrity Level 3 (SIL3).

If the CANopen Safety protocol is used on CAN networks within mobile machines, the safety aspect of data transfer is already covered. The standard way to implement the CiA 304 protocol on ECUs is to purchase an available protocol stack and to embed it into the firmware of the ECU. Once implemented in the device, the necessary memory for the stack is no longer available for other software parts like the ECU application - no matter if the application accesses the stack or not. The stack has to be adapted to the hardware and operating system environment in a way that the freedom of interferences against the other software in the system can be proved. Such an implementation usually might take several months. In case the manufacturer of the ECUs decides to offer other devices with different CPU or OS platforms, the adaptation effort has to be provided for each new platform. As soon as the stack is available on the ECU, a configurator is needed in order to configure the connected CANopen Safety devices. The Safety qualification of the configurator must of course be validated and certified as well.

Safety certification according to IEC 61508 SIL2

But the implementation of CANopen Safety is only half of the battle. Usually the mobile machine manufacturer will have to perform functional and safety tests which are often carried out by external institutes or companies such as several TÜV institutes or Exida. In order to receive a certification according to EN/ISO 13849 performance level D, all integrated software needs to conform to IEC 61508. Thus, mobile machine manufacturers will have to present the Safety reliability of the whole tool chain and of the application software on the ECU. Furthermore the

access of the ECU to the CANopen Safety protocol has to be proved safe.

The use of pre-certified tool chains will considerably speed up the certification process.

A combination of the aspects of data transfer and Safety application development within one surface will be helpful both for ECU manufacturers and mobile machine builders.

Integration of all Safety aspects in an IEC 61131-3 IDE

In application programming, standard programming environments typically for the language C have been the common standard for a long time. Meanwhile, more and more machine builders have discovered the advantages of IEC 61131-3 development environments, such as specific editors for different parts of the application software which can be mixed within a single project. Sophisticated IEC 61131-3 systems offer integrated compilers for different CPU platforms, which means that the application code can easily be reused in different ECUs.

Furthermore IEC 61131-3 systems are designed for industrial automation applications and thus come along with a lot of powerful features that standard environments usually miss: integrated support for common fieldbus systems such as CAN, Profibus/Profinet or EtherCAT, integrated visualization for the generation of user interfaces for commissioning, diagnostics and machine operation. These tools can only be used with a pre-installed special runtime system. The benefit: this runtime system comes along with many integrated debugging features which for their part make additional software tools needless.

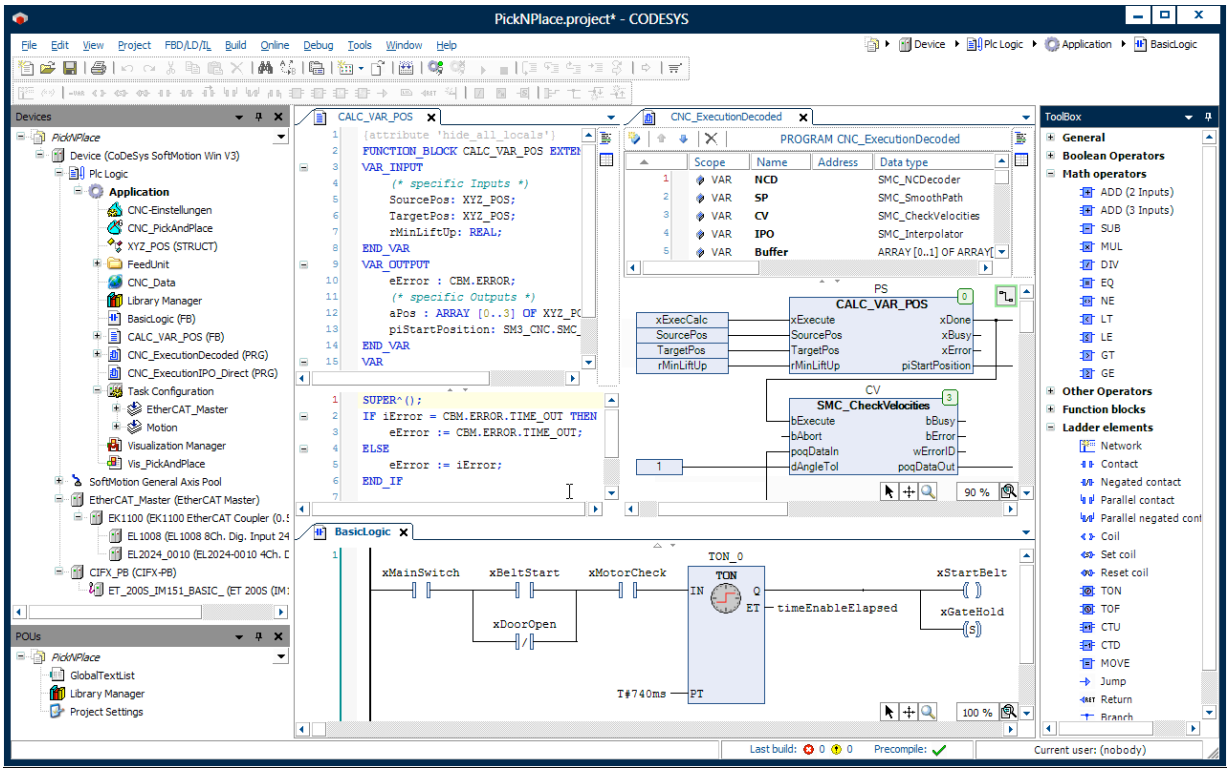

Figure 1: Different textual and graphical IEC 61131-3 programming languages under one surface

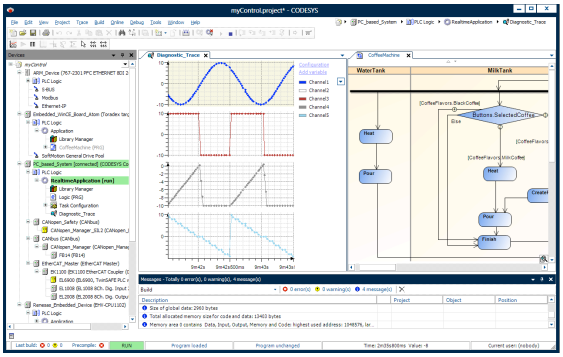

Figure 2: Debugging features such as data monitoring, breakpoints/single step execution of the application or data tracing, completely integrated in an IEC 61131-3 platform.

Some IEC 61131-3 tools, such as Codesys from 3S-Smart Software Solutions are certified for Safety applications. Codesys Safety SIL2 offers the standard set of the IEC 61131-3 functions, and has been validated and certified as suitable for the development of Safety relevant software for controllers according to EN/ISO 13849 to PL d, category 2 or 3 by TÜV Süd. The certification covers the Development System including the programming languages ST (Structured Text), FBD (Function Block Diagram) and LD (Ladder Diagram), the Runtime System as well as the compilers for different CPU platforms, such as ARM and TriCore. The Safety user manual is also part of the Safety product.

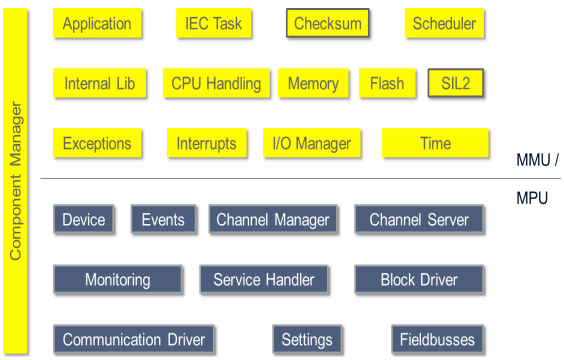

Figure 3: Safe and standard components of the certified Runtime System Codesys Control

The Safety extension of the standard Development System allows users to toggle between debug and safe operation mode. Certified SIL2 libraries for IEC 61131-3 standard functions and some additional user libraries are part of the delivery.

The certified Safety Runtime System is based on standard Codesys runtime components. Safety relevant parts have been replaced by certified components according to IEC 61508-3. Thus the components are strictly divided into the categories "safe" and "standard". Safe parts are protected against interference from standard parts with MMU or MPU.

Integration of CANopen Safety

Additionally, the tool is equipped with a comprehensive CAN support: Integrated configurators allow the user to configure standard (non-safe) CANopen, J1939 and DeviceNet networks directly in the development systems. Furthermore, native CAN commands can be transmitted by means of simple library function calls. The protocol stacks are implemented as Codesys libraries written in ST, one of the IEC 61131-3 programming languages. Thus the stack may be used on all supported platforms without adaptation effort, as they are compiled together with the application code by means of internal compilers.

The implementation of CANopen Safety is based on Codesys Safety SIL2. Thus a series of existing, already certified I/O nodes from multiple manufacturers may now be integrated in the configuration of the machine's Safety application.

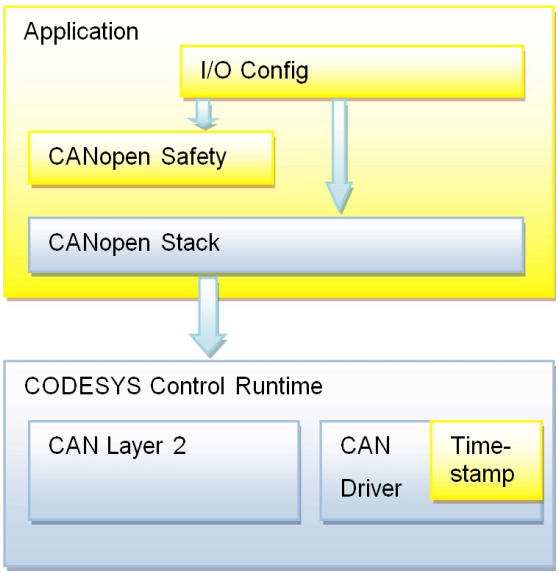

Figure 4: Architecture of the Codesys CANopen Safety stack

The CANopen Safety stack was developed conformal to the EN50325-5 standard. It is based on the standard Codesys CANopen stack developed by 3S-Smart Software Solutions. It offers the complete functionality of the non-safe CANopen stack for communication with other standard CANopen nodes. As to the architecture, the CANopen Safety stack is attached on top of the standard CANopen stack and uses the latter to receive and to transmit PDOs (process data objects).

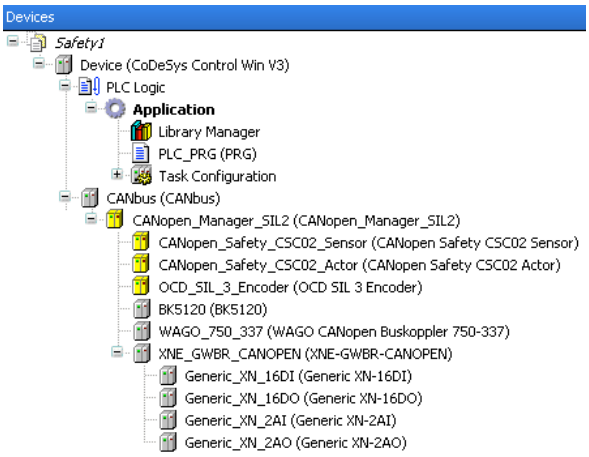

Figure 5: Mixed usage of standard and Safety-relevant CANopen slaves in one Codesys project

The implementation of the CANopen Safety stack is hardware independent which means that it can be used with any available CAN chip. For connection, a miniature CAN driver is required, which is already available for most of the CAN chips. When developing a Safety- relevant solution, the complete CAN communication channel is regarded as not safe. The CANopen Safety stack handles all possible failure scenarios. The only safe software parts are the CANopen Safety stack and a small part of the CAN driver. By means of this TÜV certified solution it is possible to use Safety-relevant CANopen devices and standard CANopen NMT slaves in the same network. Compliance with both kinds of CANopen devices was considered in the development phase.

Sensor-Technik Wiedemann and Inter Control (Germany) were the first companies porting the Codesys Safety SIL2 to one of its mobile controllers.

Conclusion

The combination of a modern IEC 61131-3 development system certified for SIL2 applications with the support of CANopen / CANopen Safety is an ideal solution both for ECU manufacturers and mobile machine builders. The effort device manufacturers have to make in order to implement all necessary and Safety relevant functions is reduced considerably. At the same time, the application programmer at the mobile machine builders' site can use the full Codesys functionality to program the functional and Safety part of the application. On top of that the certification effort for single machines or derivatives is significantly reduced by using the certified software.

Roland Wagner
3S-Smart Software Solutions GmbH
Memminger Straße 151
D-87439 Kempten/Germany
Phone +49-831-54031-0
Fax +49-831-54031-50
E-mail r.wagner@codesys.com
Website www.codesys.com

Ingo Hornberger
3S-Smart Software Solutions GmbH
Memminger Straße 151
D-87439 Kempten/Germany
Phone +49-831-54031-0
Fax +49-831-54031-50
E-mail: i.hornberger@codesys.com
Website: www.codesys.com

Stefan Blasi
3S-Smart Software Solutions GmbH
Memminger Straße 151
D-87439 Kempten/Germany
Phone +49-831-54031-0
Fax +49-831-54031-50
E-mail: s.blasi@codesys.com
Website: www.codesys.com

References

CiA DS 301, CANopen application layer and communication profile
EN 50325-5, Standardized CANopen Safety protocol (CiA 304)