Photo: Berghof, Montage 3S-Smart Software Solutions

Integrated safety – trend or hype?
The advantages of integrated safety project engineering under the roof of standard tools in automation technology

The realization of safety functions with software is nothing new. Successful safety systems from noted safety specialists are widespread in all sectors of industry. Most applications were written either in classic programming languages (e.g. C) or using configuration tools for compact safety controllers. Currently many larger manufacturers of control technology are striving to offer integrated products for standard and safety controllers. On the basis of the advantages that result from the integration of the safety technology in standard automation solutions, it can be shown that this trend is no hype.

One tool for different requirements
The project engineering and certification of proprietary safety systems with standard software tools is reserved for safety specialists. For the automation company it is comparatively simple to achieve acceptance of their machines and plants, e.g. in accordance with the obligations of the machinery directive, if they use control systems that are already certified in accordance with safety standards. The software tools for compact safety controllers are very easy to use. However, there are special software tools that have to be installed, learned and maintained by the user. What could be more obvious, therefore, than to promote the IEC 61131-3 convenience of the user interface for safety-relevant circuits? As is familiar and valued for the project engineering of the operating functions? The manufacturers are taking precisely this route with integrated tools that are suitable for safety applications.

Every machine or plant has a software application part for the operating functions. The risk analysis of this machine or plant determines the need for safety functions and their necessary Safety Integrity Levels (SIL 2 or 3 according to IEC 61508) or Performance Levels

(PL d or PL e according to EN 13849) and Categories (2, 3 or 4). Depending on the classification the degree of integration of the safety software in the automation tool can assume different dimensions.

The application development of SIL2 safety functions can take place using the same editors that are also used for the operating functions. Hence, the user can program both within an overall application using the CODESYS Development System according to IEC 61131-3. In addition the standard FBD, LD and ST editors are available, whose suitability has been certified by the TÜV. The user can also access certified function libraries. The tool is extended only by an additional plug-in component, which can be installed seamlessly into the existing setup. Naturally the controller itself must also be certified for SIL2 or PL d and equipped with a suitable runtime system.

If the risk analysis requires the coverage of safety functions in accordance with SIL3, then suitable safety editors are employed, e.g. function block diagrams, which can be used like the familiar standard editors. The functional range of the editor is reduced for easier certification of the SIL3 program. Standardized function blocks according to PLCopen for typical safety devices such as emergency stop button, two-hand operation, safety door, etc. permit simple familiarization with, and implementation of the application. The freezing of applications (pinning) guarantees the re-use of the certified safety application in case of changes to the configuration or the standard project without the need for re-acceptance.

Apart from these safety functions, the operating functions are created within the same CODESYS project and configured for the mutual exchange of data. Even if two physical controllers are programmed, the entire project engineering expenditure is reduced due to the integration of both tasks within one project. The safety application thereby abstracts the devices tree of the I/O configuration of the standard controller and thus initially examines it only logically. This means that a certified safety application can be used for different operating functions and I/O configurations without modification, without download and thus without re-acceptance: if, for example, the user replaces physical inputs or outputs by those of another type or manufacturer or if he modifies the default application, then the safety application is entirely unaffected by this. The total expenditure for acceptance and commissioning is thus significantly reduced.

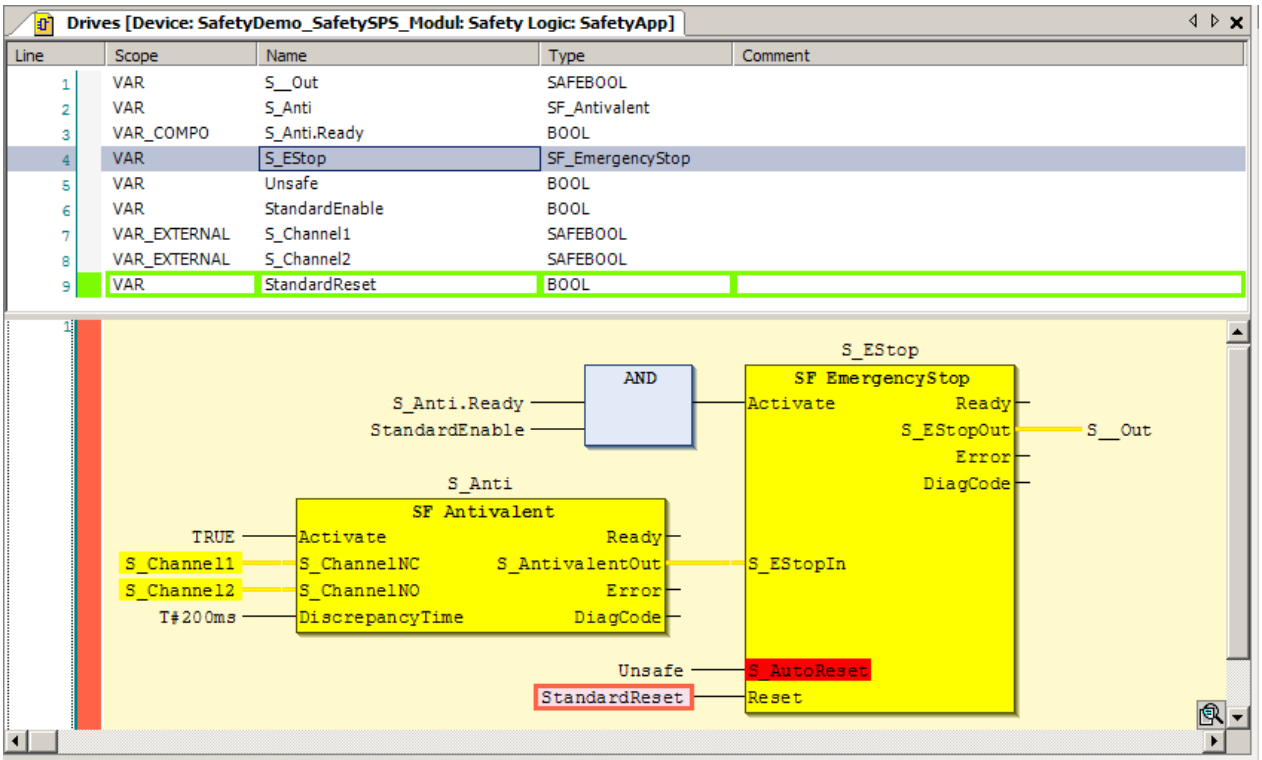

Fig. 1: SIL3-certified FBD editor completely integrated in the CODESYS Development System

More space in the control cabinet

If safety functions within a machine or plant are realized in software, then an additional safety controller is normally used. In the long run this means that at least two controllers must be placed in the control cabinet for safety and operational functions. A separate safety controller immediately brings with it the necessity for a separate safety fieldbus system and the associated wiring.

If the main controller is certified according to SIL2, then both functions can be implemented in this device for SIL2 applications – without an additional controller or fieldbus. No additional space is taken up in the control cabinet. Operating and safety functions access the same database and can thus exchange data very simply.

For SIL3 applications it is possible to reduce the use of space in the control cabinet by implementing the safety controller as a child module of an existing standard controller. This means:

- The safety controller is inserted, for example, in the extension bus or fieldbus of the main controller.
  The advantage for the user: the wiring of the safety controller to the power supply and for data exchange is unnecessary. That means: additional hardware in the form of I/O channels and their wiring is not required!
- The safe fieldbus terminals are managed by the standard controller and their data is exchanged with the safety controller via a safe protocol layer.
  The advantage for the user: there is only one fieldbus for both functions!

The total expenditure is thus reduced quite significantly by the integration of the operating and safety functions in one project.

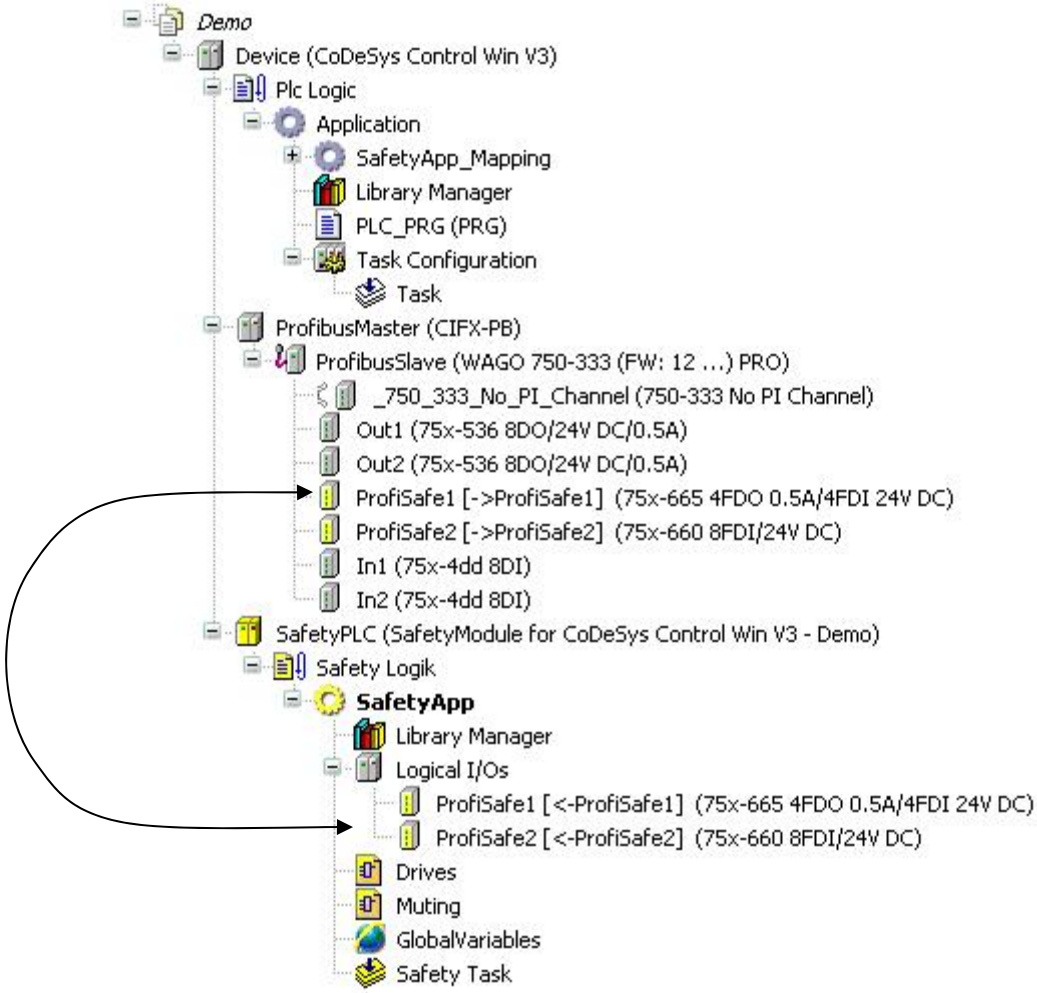

Fig. 2: The I/O configuration is configured in the standard PLC and is used abstractedly by the safety controller.

Integration extends proven fieldbus technologies
Fieldbus technologies that can be used further for safety systems already exist due to the integration in standard controllers: PROFIBUS/PROFINET or EtherCAT are extended by an additional certified fieldbus layer to PROFIsafe and EtherCAT FSoE (Fail Safe over EtherCAT).

For the manufacturer of integrated safety controllers this naturally means first of all reduced expenditure in the implementation: a Hilscher netX chip with integrated protocol stack is sufficient for PROFIBUS/PROFINET, while a commercially available Ethernet chip such as Intel Pro1000/Gigabit or Realtek 8169 is sufficient for EtherCAT. A master protocol stack is available for CODESYS in the form of a portable library. With the integrated configurators, CODESYS already contains everything required to realize the standard fieldbus connection. If the device manufacturer extends this implementation by the SIL3-certified PROFIsafe master or FSoE master layer on its safety controller, then the fieldbus aspect is fully covered for certification of the device at a later date.

The procedure is comparable for SIL2 systems: due to the proliferation on the market for typical SIL2 applications, however, the use of CANopen or CANopen Safety lends itself here, since these are also supported in CODESYS with their own protocol stack and configurator.

Users benefit in turn from the uniform project engineering of the fieldbus connection as well as the integrated I/O information on the basis of standard configuration files in the formats GSD/GSDML, EtherCAT-XML or EDS.

Fig. 3: Comparison: Architecture of a control system subsequently extended by safety functions vs architecture with integrated safety

Integrated safety connection with decentralized safety terminal
With the system described, an SIL3 application can also be project engineered with a decentral safety terminal, such as the Beckhoff EL6900 on the EtherCAT fieldbus.

The application:
A standard PLC with implemented CODESYS EtherCAT master that is programmable with CODESYS controls a machine. On the basis of the risk analysis, measures are to be taken in order to accept this machine to SIL3 in accordance with IEC 61508. In addition a compact safety controller is to be used, such as the EL6900 EtherCAT safety terminal. Instead of now project engineering this device using proprietary software, the user makes use of the solution integrated in CODESYS. That is to say, he parameterizes the EtherCAT network with the configurator integrated in the programming system and in addition inserts the safety terminal as a child module of the main controller as well as safety I/O modules. With the certified FBD editor he creates the safety application and loads it into the EL6900 via the FSoE layer. This executes the safety application. The point where the terminal or the safety I/O module is accommodated in the EtherCAT network does not matter – the safety extension in the fieldbus connection makes it possible. The user thus has an economical possibility to project engineer safety and operating functions commonly in one user interface and also to evaluate their data in the main controller.

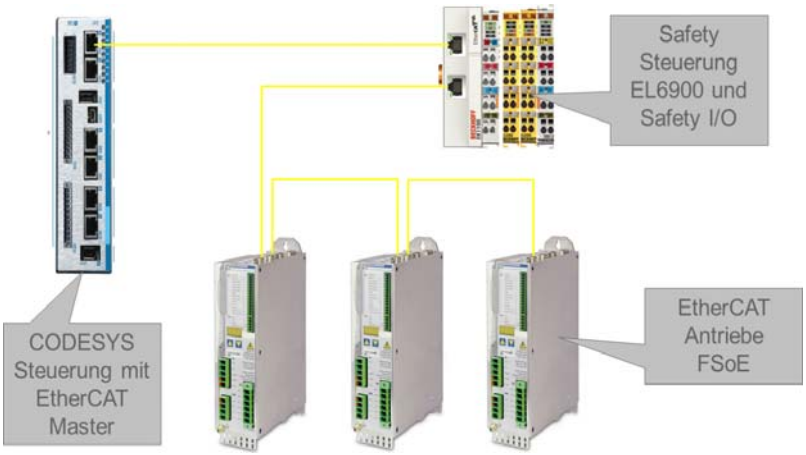

Fig. 4: Decentral safety controller in the EtherCAT network with FSoE

Although this solution is initially only available for the EtherCAT terminal described, the procedure can be transferred to comparable FSoE or PROFIsafe systems.

Conclusion

The trend toward integrated safety solutions under the roof of common automation solutions is easy to comprehend. Device manufacturers and users benefit, in particular through savings in project engineering and wiring. With the CODESYS Development System according to IEC 61131-3, device manufacturers and users have a system at their disposal that integrates suitable safety products for different applications. Thus integrated safety is no hype, but reality in an increasing number of automation applications.