# How can modern control systems help to overcome limitations in mobile machines?

Alexander Holler, Inter Control Hermann Köhler Elektrik GmbH & Co.KG

**Today's mobile machines provide an enormous functionality – they reach further, move smoother, lift higher, react quicker and safer.**

**But still there are limitations that prevent mobile machines from being even better and -once these were overcome- there are limitations to implement these improvements fast. New safety standards like the EN ISO 13849 and their integration in C-level standards impose further restrictions to designers.**

**This paper will describe means that modern electronic control systems provide to further improve the performance of mobile machines, reduce their downtime and increase their flexibility – with consideration of the safety requirements set forth in EN ISO 13849.**

## Safety meets performance

With the increasing functionality of mobile machines the requirements in regards of processing power and available memory growth constantly. On the one hand side processors utilized in mobile controllers running at e. g. 200 MHz provide sufficient speed to assure the timely processing of the machine functionality. On the other hand safety standards enforce a high level of controller internal diagnosis which could significantly reduce the available processor resources and thus affect the functionality itself. The internal architecture of the controller helps to overcome this limitation.

To address the safety requirements in controller architectures two principles are usual. The first architecture is realized as a category 2 system acc. to IEC 13849, the logic unit (main processor) is supervised by a test unit (companion).

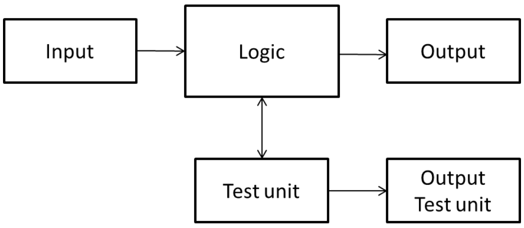

**Figure 1: Category 2 architecture**

The second architecture is realized as a category 3 system. In this case two individual logic units (processors) process the function and check their results in a cross comparison.

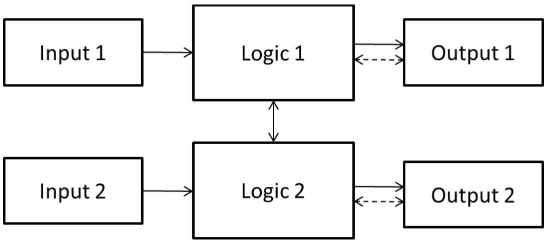

**Figure 2: Category 3 architecture / discrete**

The category 2 architecture demands significant processor resources for self-test and thus limits the capacity available for the functionality itself.

Furthermore specific C-level standards like the EN 280 do not permit dedicated safety functions in category 2.

Common category 3 systems with discrete main processors offer higher performance but at higher costs than category 2 systems. Beside that two application programs, one for each logic (main processor), are required which imposes a higher work load on the programmer.

To overcome the disadvantages of both concepts and to achieve the initial goal – providing more calculation power for the different and constantly increasing machine functions - a new approach is necessary.

To avoid the inconvenient handling of two application programs as well as the costs of a discrete category 3 system on the one hand side and to take advantage of the higher performance of the two main processors the utilization of a safety dual core processor as shown in figure 3 is helpful.

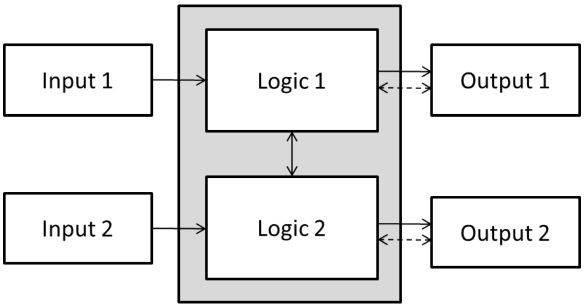

**Figure 3: Category 3 architecture / integrated**

Dual core safety processors integrate the two logics and therefore are able to manage the distribution of the application program on the two cores internally. The processing of the application program is done on both processors in parallel step by step. A step in this regards is the smallest possible processor operation, consisting of reading, processing and writing results. Finally the results of both cores are compared. As the operation of both cores is locked together this procedure is called lock step mode.

For demanding applications it might be necessary to perform complex operations like trigonometric calculations. In this case FPU's (floating point units) are the appropriate processing platform to assure reasonable calculation time. While the supervision of FPU operations in category 2 architectures is not feasible, dual core processors provide the means to meet safety requirements without overload of internal self-tests.

### Safety meets flexibility

Many manufactures of mobile machines are providing a wide spectrum of vehicles and variances with relatively small number of machines per type. As safety standards are strongly recommending the utilization of per tested software modules it makes for economic as well as for quality and safety reasons much sense to structure the application software in a modular way. Similar functions in different machines are realized with the same software function block. To take full advantage of this modular software approach a common safety controller for the complete range of vehicles is necessary. But to meet the different requirements of the different machines this controller must be adaptable in different ways.

Multifunctional IO's which are software configurable help to configure one controller to various machine IO-requirements. As this feature is common and well accepted for standard controllers it becomes necessary for safety controllers as well to not reduce the flexibility of the machine builder. To provide this functionality safety controller have to assure sufficient internal diagnosis to cover all optional settings of an IO point.

Different sizes of machines typically require different number of IO points. To economically meet this requirement mobile controllers have to offer modularity which allows the configuration of the required numbers of IO points. While this concept is common in the industrial automation it provides some challenges in mobile machinery due to the tougher environmental conditions.

Beside that the modularity and thus the opportunity to extend IO's should not be limited to standard IO's but must especially meet the increasing demand of safe IO points. As sensors dedicated to safety functions are often redundant, the number of required inputs doubles.

It becomes obvious that to achieve the flexibility to cover a complete range of different mobile machines with one controller basis it is important that this controller has to be adaptable in terms of the function of the individual IO and the number of IO's – still considering the harsh environment and the safety requirements.

Safe automation systems require beside appropriate controllers sensors which provide the machine status in a safe way. The communication between controller and sensor could be set up principally in two ways – via safe fieldbus like CANopenSafety or direct connection via inputs. When connecting the safety sensor directly there are two solutions feasible, redundant or single channel connection, depending on the required safety level and the design of the sensor. Due to the still limited number of safety sensors available on the market it is useful to have the opportunity to choose between both options – provided that required safety level could be achieve in both ways. Controllers do not naturally provide the option to connect safety sensors with just one channel. To support this single channel connection the input of the controller needs to have internal diagnosis to assure the demanded diagnostic coverage. If this is available safety sensors could be connected with a single channel connection as shown in figure 4.

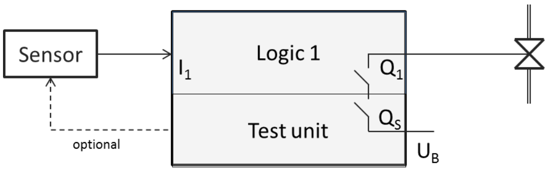

**Figure 4: Single channel connection, typical for category 2 architectures**

Alternatively redundant sensors or two sensors providing redundant signals could be connected to the same safety controller as shown in figure 5.

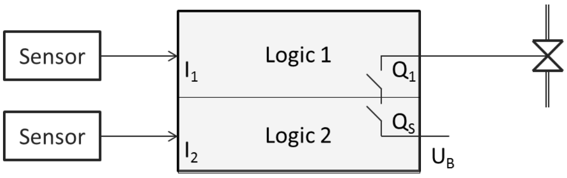

**Figure 5: Redundant connection, typical for category 3 architectures**

This solution is typically implemented when the relevant safety standards demand it or if category 2 sensors are not available. Safety controllers supporting the connection of category 2 and category 3 sensors provide the flexibility to select the sensor by its performance and not by its interface.

### Securing the investment

The implementation of a controller in a machine series is major step which should last for a long time. Therefore it is of importance to be able to integrate functionalities during the life time of the machine. The above described flexibility of safety controllers is not only key to allow the utilization of one controller for different types and variants of mobile machines. It furthermore allows modifying or adding new functionalities on machines which have already started their live cycle. When it comes to safety the ability of modifying existing machines is not only a question of hardware modularity and flexibility.

As additional functions typically require a change of the application software the programming environment needs to be considered as well. Later changes of the application software have to be done in a way that they do not affect the machines safety. The related validation and verification effort can be significantly reduced if the safety controller provides means to separate the safe and the standard functionality in a way, that changes of standard/comfort functions do not interfere with safety functions. When programming in the IEC 61131 environment the separation of safe and standard/comfort functions could be arranged by setting up a safe project and a standard project. Both projects have access to the set of variables they need while it is assured, that the standard project cannot interfere with the safety project. A software structure which dedicates all non-safety related functions to the standard project and the safety related functions to the safe project increases the flexibility and reduces the time to market, if standard functions are changed or added.

Hardware modularity and software flexibility especially in safety applications is important to extend the life cycle of a machine. The consequent usage of accepted industry standards for field communication like CANopen and CANopenSafety, service interfaces like USB and Ethernet and programming languages like the IEC 61131 helps to later seamlessly integrate components in existing automation systems – another major aspect in machine life time considerations.

## Increasing uptime

Safety controllers have the task to monitor the automation system and, if safety critical failures occur, to initiate the fail safe state. The fail safe state in mobile machines is the de-energized state at the outputs, corresponding to a logic zero.

Safety critical failures could occur in the controller itself, at the communication system, on sensors or actuators. Depending on which component fails and which function this component is related to it might be necessary to de-energize the complete system by switching all outputs to zero by initiating the second switch-off path. But not all failures require a complete shut-off of the machine. A safety analysis might come to the result that a failure on one function must not automatically cause other functions to stop as well. If this is the case, it could be very useful to keep the other functions alive and allow the machine operator to finish his job or to recover the vehicle, even if a safety critical error has happen.

To allow this, the safety controller must provide not just a single second switch off path. If the safety related outputs are combined in groups and each of these groups have their own second shut of path different machine functions could be allocated to different output groups. This allows the machine builder to structure their control system in a way that different functions could be shut off individually while the other functions stay alive.

Once a failure –safety critical or non-safety critical- has occurred time is pressing to keep the downtime of the machine as short as possible. With the constantly increasing complexity of mobile machines it gets more and more difficult to have the right expert on site to fix the problem fast. Cellular phone/data networks allow to directly get connected to the machines control system at nearly any place in the world. The gathered data's about the actual machine state as well as failure descriptions help to get the problem analyzed by the appropriate expert. Thus it is possible to provide professional guidance to the on-site service technician and help him to get the machine up and running. Furthermore the problem could be fixed remotely by sending new parameters or even software updates to the machine.

On the machine the connection to the cellular phone/data networks is established by a modem or router which is connected to the controller. Typical interfaces between modem/routers and controller are RS232/485, providing a data transfer rate of typically 115 kbit/s, Ethernet with a data transfer rate of up to 10 Mbit/s or Fast Ethernet with 100 Mbit/s. As the interfaces on modems/routers have developed so have the maximum transfer-rates of the mobile communication. While EDGE networks support up to 260 kbit/s communications via LTE supports up to 100 Mbit/s.

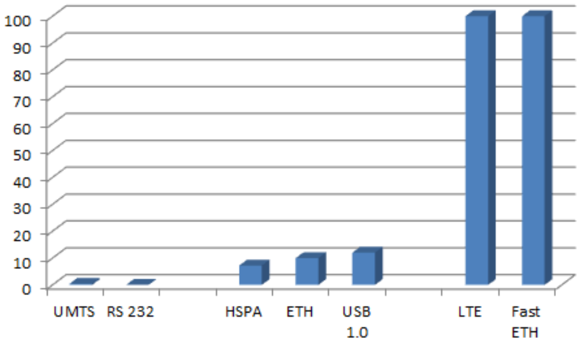

**Figure 5: Maximum data transfer rates in Mbit/s**

When laying out new machines which shall be sold for 5 to 10 years and stay in operation for much longer, it is important that the control system provides interfaces which are not only meeting todays needs but also the requirements of telematic solutions in 10 to 15 years. Figure 5 shows that the maximum data rate is today already at 100 Mbit/s for LTE. To avoid bottlenecks on the machine Fast Ethernet interface on mobile controllers for remote-service and other solutions like for instance fleet management are necessary.

To ensure proper update of machine software remote service is not the only approach. To enable service technicians with a non-electronic background to update software the USB interface with Host functionality can be used. When plugging a USB-stick in the controllers USB connector the complete set of software available on the stick will be updated at the controller. The update process is completely automated and therefore reliable.

## Summary

It is certainly a challenge to set up the electronic control system for mobile machines due to their relative high mix and a comparatively low volume per type and variant and the increasing safety requirements. But the selection of the appropriate mobile suitable safety controller providing scalability, flexibility and connectivity establishes an adaptable and long-lasting foundation for the machine automation.

Alexander Holler
Inter Control
Hermann Köhler Elektrik GmbH & Co.KG
Schafhofstraße 30
D-90411 Nürnberg
Phone +49-911-9522-850
Fax +49-911-9522-857
Holler.Alexander@intercontrol.de
www.intercontrol.de

## References

[1] DIN EN ISO 13849, DIN Deutsches Institut für Normung e.V.

[2] CiA DSP 302, Framework for CANopen managers and programmable CANopen devices