2nd generation safety controller for mobile applications

Alexander Holler, Hans-Dieter Kaiser

Figure 2: Safety controller digsy fusion S

Introduction

The safety requirements defined in EN ISO 13849 are getting more and more relevant in the mobile machinery market. When comparing the requirements in dedicated C-level standards for different mobile machines, it appears that Performance Level d (PL-d) is mainly demanded for controllers to achieve sufficient functional safety. Not all C-level standards demand to meet the safety requirements set forth in the EN ISO 13849 today. But when developing a new machine with a life cycle of 5 to 10 years, the consideration of functional safety is inevitable. Beyond the performance level, additional features of a safety controller help increase the sustainability and flexibility of the machine's control system.

The processing power of a safety PLC is not only defined by its processor's speed but also by its architecture. To address the safety requirements in controller architectures two principles are usual:

Firstly, the architecture could be realized as a category 2 system according to IEC 13849; the logic unit (main processor) in that case is supervised by a test unit (companion). This 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.

Secondly, category 3 architectures are built with two discrete main processors. This offers higher performance but at higher costs than category 2 systems. In addition, two application programs, one for each logic (main processor), are required, which imposes a higher work load on the programmer.

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 safety controller digsy fusion S is based on a dual core safety processor as shown in Figure 1. The dual core safety processor integrates the two logics and is therefore 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 connection is the smallest possible processor operation, consisting of reading and processing data 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.

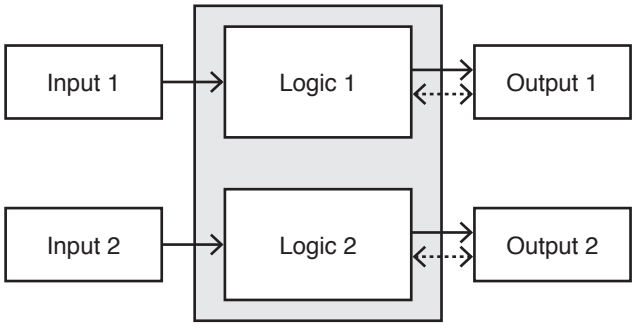

Figure 1: Category 3 architecture / integrated

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.

CAT.3 or CAT.2 control systems

Even if a safety controller has an internal category 3 architecture, it may also be integrated in category 2 machine control systems. The digsy fusion S safety controller for example is able to communicate with safety sensors in two ways: either as a redundant or as a 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 the required safety level can be achieved in both ways. Controllers do not inherently 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 2. Alternatively, redundant sensors or two sensors providing redundant signals could be connected to the same safety controller as shown in Figure 3.

This solution is typically implemented when the ▷

relevant safety standards demand it or if category 2 sensors are not available. As the safety controller supports connecting category 2 and category 3 sensors, it provides the flexibility to select the sensor by its performance and not by its interface.

Standard and safe communication

In terms of field busses CAN is the standard protocol in mobile machinery. The digsy fusion S offers four CAN interfaces. Each provides different protocols, as they are CANopen and J1939. Layer 2 programming serves as a way to achieve any other desired protocol. CANopen is widely used in mobile automation. Many components, i. e. sensors and actors, are available on the market, using this standard and meeting the requirements for industrial and mobile applications. CANopen offers all basic protocol functionalities as a defined system start up, network management, system data exchange, process data exchange, synchronization and emergency messaging. The required configuration of CANopen communication is performed using the standard programming tool of the safety controller. If functional safe communication via CAN is required, CANopen Safety standard (EN 50325-5) is recommended. It is a protocol extension of CANopen and provides a safe communication between two or more CAN network members.

Safe communication is achieved through Safety Related Data Objects (SRDO). SRDOs have to be transmitted periodically within a Safeguard Cycle Time (SCT). A SRDO consists of two CAN communication objects (COB) CAN1 and CAN2 that have to be transmitted within the Safety Related Validation Time (SRVT). The two COBs differ in COB-Identifier (COB-ID) – min. 2 bit – and in normal (CAN1), respectively bitwise inverted (CAN2) payload. If a receiving node detects expired SCT or SRVT cycles or differences after comparing the payloads of CAN1 and CAN2, it will enter safe state. Thus, a safe communication is guaranteed that meets the requirements of the EN 61784-3 standard regarding message corruption, unintended repetition, incorrect sequence, message loss, message insertion, masquerade and addressing.

Flexible changes of the application program

The long life cycle of mobile machines often requires adapting their functionality to changing market requirements. Digsy fusion S supports this through the ability of running two projects in parallel. The first project (safe project) is responsible for safe machine functions, while the second project (standard project) takes care of all non-safety related functions like comfort functions. As the standard project can not interfere with the safe project, it is possible to change the standard project without an additional safety analysis. The safety controller utilizes Codesys 3.5 SIL2 for running the safe and the standard project, thus it is ensured that just one consistent programming environment is necessary.

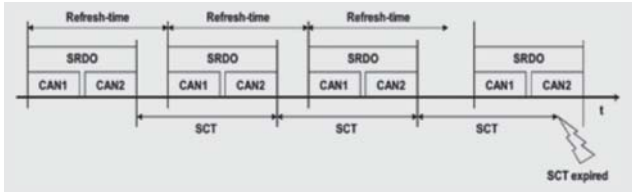

Figure 5: CANopen Safety – Safeguard Cycle Time

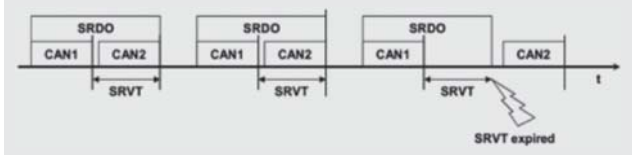

Figure 6: CANopen Safety – Safety Related Validation Time

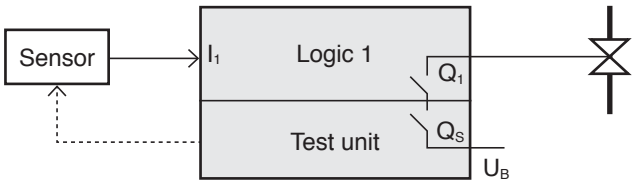

Figure 3: Single channel connection, typical for category 2 architectures

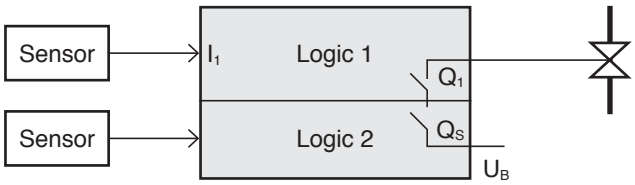

Figure 4: Redundant connection, typical for category 3 architectures

Increased uptime

Monitoring the machines functionality regarding dangerous conditions is one of the core tasks of a safety controller. Once a dangerous condition is detected the machine is set in failsafe state by the safety controller. This is done by activating a second cut off path which de-energizes the outputs. Depending on the kind of failure causing the dangerous condition it may be necessary to shut down the complete machine. But not all failures must cause a complete shutdown. A safety analysis may lead to the result that a failure in one function does not have to automatically result in a shutdown of other machine functions. In this case it is useful to keep the functions unrelated to the failure alive to allow e.g. the recovering of the machine or complete the last maneuver. For this reason the safety controller provides four groups of second cut off paths. This enables the user to just shut down the outputs that are related to the dangerous condition. Other functions can be kept alive even in case of a failsafe. ◀

Authors

Alexander Holler

Hans-Dieter Kaiser

Inter Control
Hermann Köhler Elektrik
GmbH & Co.KG
Schafhofstraße 30
DE-90411 Nürnberg
Tel.: +49-911-9522-851
Fax: +49-911-9522-857

Link
www.intercontrol.de

Resumee
Performance, functionality and conformity with the relevant safety standards do not exclude each other. 2nd generation safety controllers that achieve PL-d according to EN ISO 13849 provide the necessary features.