SIMATIC S7-400F/FH:
Safety-Related Programmable Logic Controller

Andreas Schenk
Siemens AG, Automation and Drives, Advanced Group Technologies, A&D GT 4,
P.O.Box 4848, D-90327 Nuremberg, Germany
andreas.schenk@nbgm.siemens.de

Abstract. SIMATIC S7-400F/FH is a fail-safe and fault-tolerant programmable logic controller which achieves safety integrity level 3 (SIL 3) with one standard SIMATIC CPU module and distributed fail-safe input and output (I/O) modules. This paper shows the underlying safety principles.

1 Introduction

Safety-related programmable logic controllers are used for risk reduction when a process or a machine endangers persons, environment or equipment. Generally they are fail-safe - in process industry even fault-tolerant.

The safety-related programmable logic controller SIMATIC S7-400F/FH deals with the following challenges:

1. Standard SIMATIC modules should be used where possible – especially in case of complex modules like CPU modules and the programming environment. The reasons for this are cost savings, profit from improvements of the standard modules and better integration into the automation system.
2. Mixing of safety-related and not safety-related functions and modules in the same automation system should be allowed.
3. One CPU module should already achieve safety integrity level 3 according to IEC 61508 [1]. SIMATIC S7-400FH uses a second CPU module for fault-tolerance.

The answer to this was concentrating safety functions in few hardware and software modules, the so called ‘safety islands’. These safety islands contain measures to detect and control faults at the hardware level as well as at the safety function level. By the latter interference of standard modules on the safety function is controlled.
Architecture of Safety Islands

Safety is achieved by few safety-related modules:

1. Fail-safe I/O modules (F-SMs)
2. Option package ‘S7 F Systems’
3. Safety-related application program, built of safety-related function blocks (F-FBs)

Fig. 1. Architecture of safety islands

2.1 Safety-Related Distributed I/O

Safety-related input from and output to the process are done with special fail-safe I/O modules that are inserted in distributed ET200M-cabinets at the PROFIBUS. The fail-safe I/O modules provide an internal 1oo2 structure with comparison, self-tests and external fault diagnostics.

2.2 Safety-Related Communication

For safety-related communication standard busses and protocols can be used together with a safety layer. Guidelines are given in prEN 50159 [2][3].

Safety-related communication between the safety-related application program and the fail-safe I/O modules via the PROFIBUS is done with the safety protocol ProfiSafe [4]. This safety protocol is transparent to the programmer as it is implemented in the fail-safe I/O modules and special safety-related function blocks.

Safety-related communication between safety-related application programs in different CPUs, e.g. via PROFIBUS or Industrial Ethernet, is done with special safety-related function blocks implementing a similar safety protocol.