SafeFlex
FUNCTIONAL SAFETY DEVELOPMENT KIT

Creating safety.
With passion.

NewTec
System-Entwicklung und Beratung

Safety Reference Application Note

Safety over Ethernet
Reference Design for Altera FPGAs

Revision Sheet

Revision	Change History
Rev:: 126	Initial Revision
$Rev:: 131 $	First Issue

1 Introduction to Industrial Ethernet Solutions

While classical field automation was based on PLCs with discrete wired sensors and actors, modern automation technologies require fast communication field busses. Current market trends for autonomous and fully automated machinery involve a huge number of sensors, actors and decentralized controls. These applications often have high demands for real time capability and require intelligent communication networks. In this context, Ethernet based communication field buses have gained importance and replace classical fieldbuses.

Basically industrial communication networks are standardized by ICE 61158, ICE 61784-1 and -2. These standards define about 26 communication protocols and classify them into 19 communication profile families (CPF). The most important and widely spread Industrial Ethernet protocols are shown in Figure 1. More than 85% of the worldwide newly installed nodes are based on one of these six technologies.

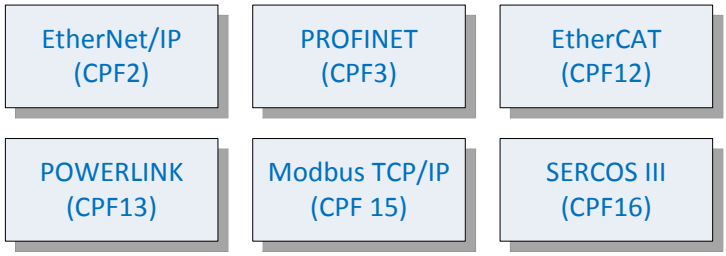

Figure 1: Common Industrial Ethernet Protocols

Those Industrial Ethernet protocols are based on different principles and have different characteristics. Some use standard TCP/IP mechanisms, others are suitable for hard real-time requirements of highly dynamic Motion Control systems with short cycle times and use modified Ethernet frames. Each technology has its benefits and so the decision on which protocol shall be used often depends on the application itself.

On the one hand, performance is a decisive parameter of Industrial Ethernet protocols to meet the needs of modern field automation. On the other hand, functional safety of machinery is an increasingly important point and so safe communication channels are demanded. The standard DIN EN IEC 61508 is the major standard for functional safety and serves as the basic standard for functional safety across all kinds of industry. It defines functional safety as the *"part of the overall safety that depends on a system or equipment operating correctly in response to its inputs".* In order to cope with the growing safety challenges and to guarantee a high level of safety in industries, regulatory bodies have introduced the safety standard DIN EN ISO 13849 which especially applies to machinery safety. It provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems, including the design of software.

Standard Industrial Ethernet fieldbuses (shown in Figure 1) are not sufficient to transmit data safely. Since functionally safe machinery require safe communication networks, the Black Channel

principle can be used to enable a failsafe communication via a standard bus network. The Black Channel is an approach that sends safety-related and none-safe data using the same communication protocol and network – the physical connections as well as the transport mechanisms are identical. To allow a safe communication, a safety protocol is added above the standard protocol. This safety protocol implements for example safety mechanisms on the application layer and uses the payload data of the none-safe protocol to tunnel safety-related data through the network (see Figure 2). The failsafe communication is not ensured by the lower communication layers, but by the safety mechanisms of the application layer that ensure that the transmitted data is correct.

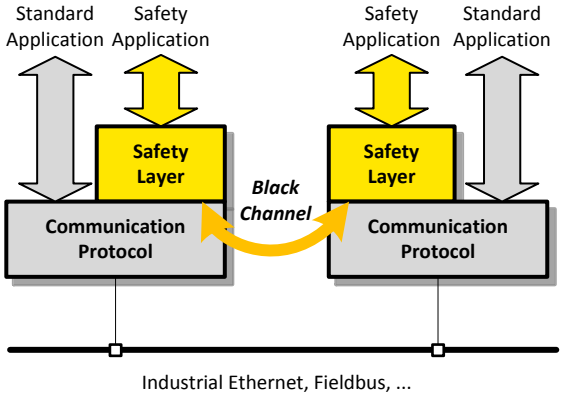

Figure 2: Black Channel Principle

Functional safe fieldbuses for industrial communication networks are specified by the IEC 61784-3. This standard describes basic principles and requirements for safe communication fieldbuses and defines safety communication profiles of fieldbuses. There are different safety communication profiles for different basic Industrial Ethernet protocols applicable (see Figure 3).

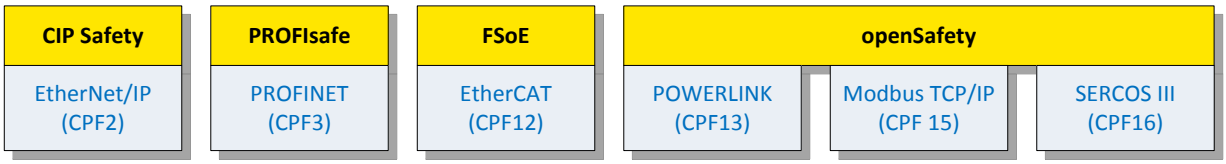

Figure 3: Safety over Industrial Ethernet Protocols

In the following, this application note describes a reference design including a POWERLINK field device with an openSAFETY implementation representative for any other Industrial Ethernet protocol.

POWERLINK

POWERLINK was originally developed by the Austrian company B&R as an Industrial Ethernet solution that covers almost every application of automation technology and especially those where hard real time performance with cycle times of less than 100µs is required. The further development

of the POWERLINK technology is advanced by the EPSG, an independent association consisting of users, manufactures and research institutes.

POWERLINK is based on a standard Ethernet frame according to IEEE 802.3 and implements all protocol features like cross-traffic, hot-plugging and transport protocols like TCP/IP, UDP and HTTP. Furthermore, POWERLINK includes the complete CANopen mechanisms (PDO, SDO, OD, etc.) on the application layer and so all CANopen device profiles are applicable for POWERLINK.

Within the Ethernet payload of the standard Ethernet frame, the POWERLINK protocol embeds a POWERLINK frame which consists of a header and a payload area (see Figure 4). The POWERLINK header indicates the purpose of the message by the message type and provides information about the node addressing by source and destination IDs.

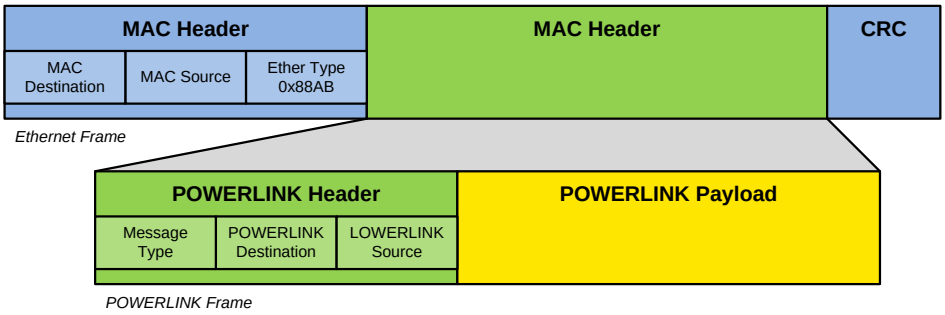

Figure 4: POWERLINK Frame

The POWERLINK protocol is based on a polling-procedure shown in Figure 5 that guarantees that each network device sends its data at a specific time-slot within a specific communication cycle. By this time-slot management it is ensured that no data collision occurs and so data delays are suspended. Therefore, each POWERLINK network has one Managing Node (MN) that coordinates the communication. The MN can either be a PLC or an industrial PC. All other devices within the POWERLINK network are called Controlled Nodes (CN).

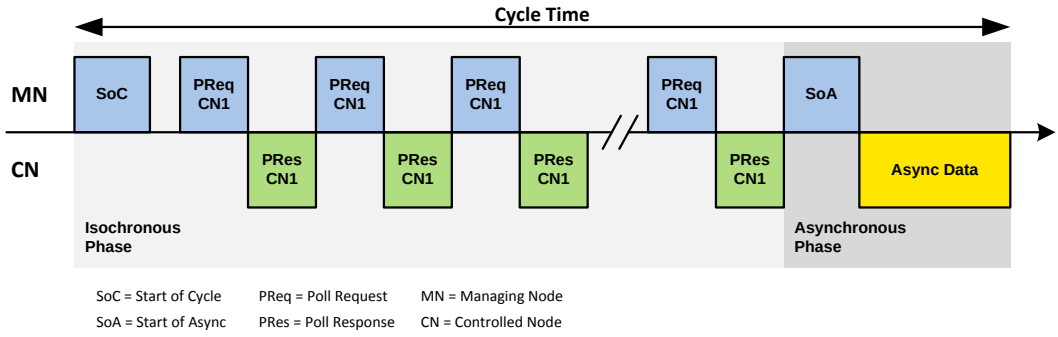

Figure 5: POWERLINK Polling-Procedure

Each communication cycle begins with the Start of Cycle (SoC) which is send by the MN to all CNs. By this initial message good time synchronization between the networking nodes is achieved with a low jitter.

In the subsequent isochronous phase the MN sends Poll Requests (PReq) to the CNs. Each request addresses a specific CN within a specific time-slot. The addressed CN replies to the request with a Poll Response (PRes) which includes isochronous data (like process data) of the CN. By this time-slot polling procedure hard real-time performance is established.

The third phase of the communication cycle includes asynchronous data transfer. This phase can be used to transfer large or non-time-critical data like TCP/IP frames or configuration data.

openSAFETY

openSAFETY is defined and internationally standardized as FSCP13 within the IEC661784-3 and was established by the openSAFETY Working Group within the EPSG in 2004. It is a bus-independent safety protocol based on the Black Channel principle and it is independent of the transport media. It is applicable for about 91% of the worlds Industrial Ethernet fieldbuses.

openSAFETY allows standard and safety related devices to use in the same network and guarantees real-time Ethernet communication with data transfer time below 100 µs. It supports various network architectures and is capable of cross-traffic. It fulfills the error probability rate up to SIL3 according to IEC 61508 and implements different measures like time stamp, ID, CRC, etc. to detect the possible faults regarding the IEC61784-3 (Figure 6).

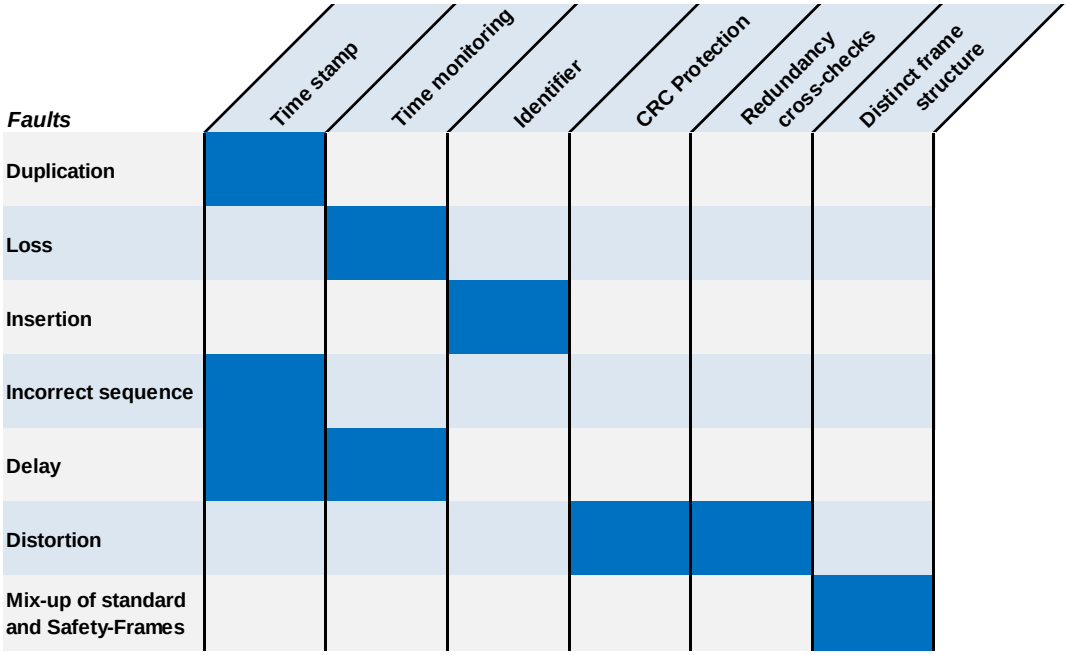

Figure 6: openSAFETY Measures

2 Reference Design

Industrial Ethernet networks often consist of various safety-related and non-safe communication devices like PLCs, robots, sensors, drives, I/O cards, light curtains, etc. These decentralized networks benefit from their flexibility and the low wiring effort.

The scope of this application note is to illustrate the implementation of a functional safe field device with a POWERLINK interface. This device has several safe inputs to observe the digital signals of safety-related sensors like light curtains and emergency stop buttons. These sensors could, for example, monitor a hazardous working zone of an industrial robot. However, the robot is controlled by a separate safe PLC and so the safety-related monitoring data has to be transmitted by the safe field device via the openSAFETY protocol through the POWERLINK interface.

This application requires a SIL2 or SIL3 architecture dependent on the estimated potential risk of the robot. A typical approach to reach the required SIL3 level is a redundant 1oo2 system architecture with two independent microcontrollers. However, this approach is quite expensive, since it is not enough just to implement diagnostic measures. It must also be proven that these measures are sufficient enough to gain the safety certification. Furthermore, these measures have to be implemented in software whereby the performance of the system is limited and the system safety time is increased. Other issues that have to be considered are the flexibility of the system and the consequences of changes. Any change in a functional safe design might result in a huge effort for documentation and a recertification process. Manufactures of field devices often plan to provide the same device with different Industrial Ethernet interfaces. If the system is implemented on a FPGA device like Altera's Cyclone® V, developers can benefit from the great flexibility and the pre-certified SoC ("System on Chip") components to reduce development and certification costs with a simultaneous improvement of the system's performance.

Single Chip Design

Figure 7 shows a recommended structure of functional safe field devices based on Model A - annex A of the IEC61784-3. The openSAFETY protocol stack needs to be implemented redundantly, because it is a functional-safety-related part of the device. The Ethernet communication network itself is an unsafe medium and so there is no redundancy required regarding the communication layers of the POWERLINK protocol since the Black Channel principle applies. Failures caused by the communication medium must be detected safely by the superior Safety Layer in every possible case. Failures of the communication device itself need to be eliminated by hardware or software diversity of the Safety Layer.

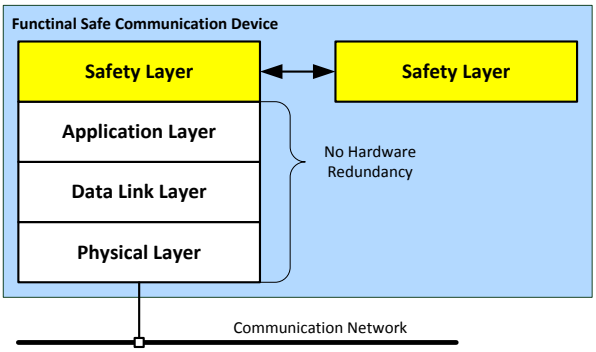

Figure 7: IEC61784-3 Model A

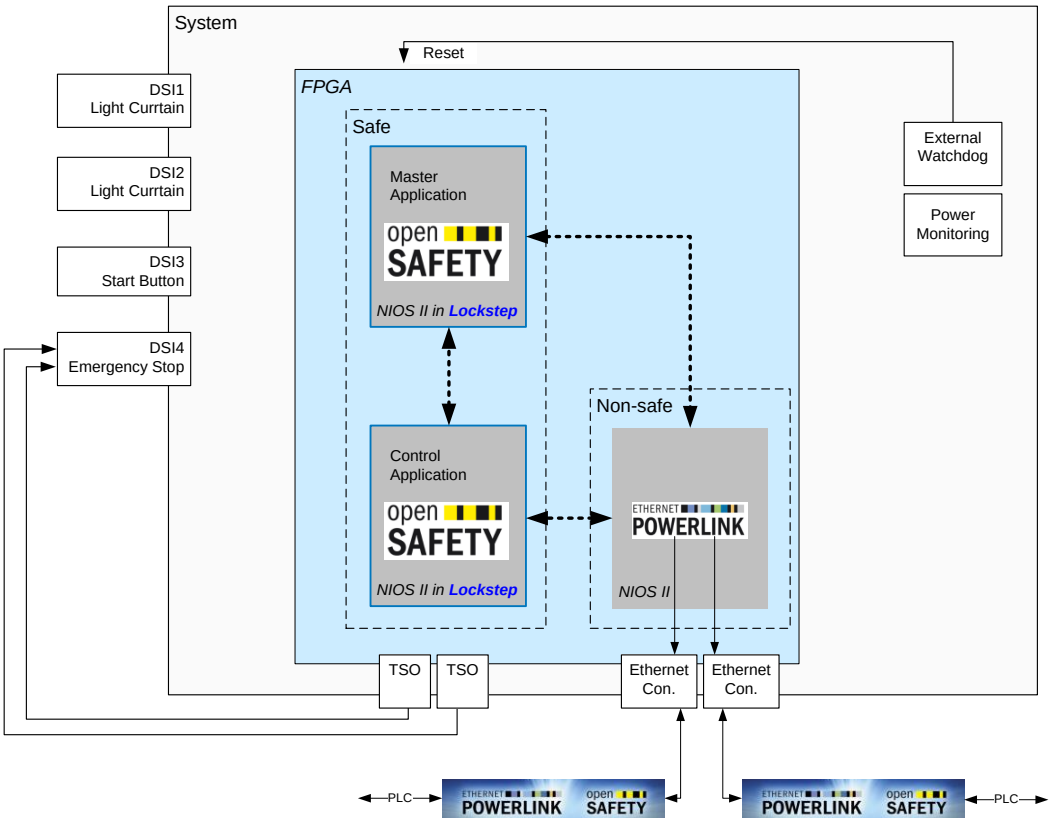

Figure 8: SIL2 Field Device Architecture (SIL3 possible with DC>99%)

Figure 8 shows the architecture of the safe reference design field device. The system is implemented on a single Cyclone® V FPGA. To fulfil the requirements of the IEC61508, the whole system need to meet the safety requirements and so safety measures have to be implemented on all parts of the system. Figure 9 gives an overview of which diagnostic coverage is required to reach a specific SIL level with certain architectures.

Diagnostic Coverage (DC)	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Figure 9: Maximum SIL Level Depending on DC and HFT

To capture the input of safety-related digital signals, the system has four Digital Safe Inputs (DSI). DSI 1 and 2 are used for a redundant connection of a light curtain. DSI 3 is connected with a start button which is not safety-related. DSI 4 is connected to an emergency stop button. The DSI's are protected from overvoltage and have self-test circuits to monitor the correct function of the inputs (see Figure 10).

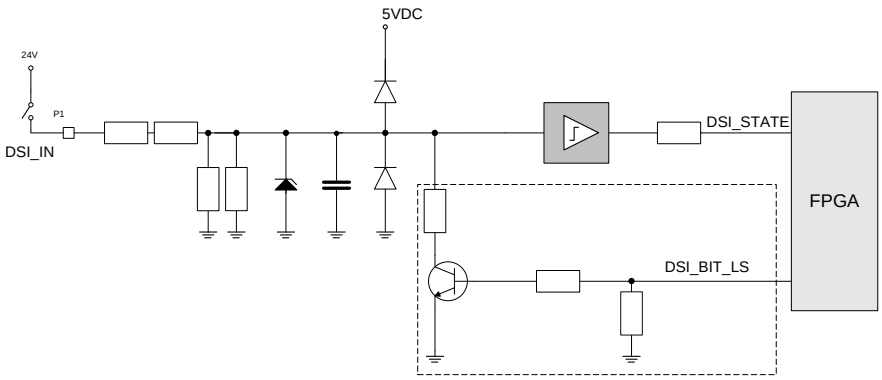

Figure 10: DSI Structure

A test output (TSO) is added to the emergency stop which enables the FPGA to turn off the power of the emergency stop to test whether the signal wire is stuck high. The different internal supply voltages are monitored for overvoltage and undervoltage as additional safety features. If one of these voltages is beyond the specified range, the FPGA is kept in reset. When all voltages return into the specified range, a FPGA reconfiguration is started.

The IEC61508 demands a separate watchdog as an external monitoring element to accomplish the required SFF and DC. For this purpose an external window watchdog is used which applies for multiple safety measures like program sequence monitoring, clock monitoring and further diagnostic functions.

The FPGA includes a redundant implementation of the safety layer on two Nios® II soft CPU cores. The two Nios® II are setup in a lockstep architecture which is enabled by the “fRSmartComp_nios2” component. The function of the “fRSmartComp_nios2” is based on the comparison of two standard Altera Nios® II CPU cores. It compares the outputs of both CPUs cycle-by-cycle and detects any discrepancy. Furthermore, different timers and watchdogs are used to detect time-outs, faults and endless loops at the system. For that purpose the identical software, including the openSAFETY stack, is embedded on both CPUs. If any fault or discrepancy is detected, the system is set to the safe state.

The “fRSmartComp_nios2” component is a Verilog RTL soft IP developed and distributed by YOGITECH, an Italian provider of IP solutions for functional safety. The IP is verified following the quality standard defined by the norms. Any further verification of the IP by the user is not requested since it guarantees a SFF >99% and is pre-certified up to SIL3 in accordance with IEC61508. It is fully documented including a Safety Manual which is essential for the certification process. Due to the guaranteed SFF >99% there is no need for additional measures regarding the CPU functional safety.

The none-safe POWERLINK stack is implemented on another Nios® II on a spate partition. The only interface between the non-safe and the safe CPUs is an internal SPI interface to transfer payload data between the CPUs. Partitions are generally advantageously whenever one has to prove that there is no influence of the none-safe on any functionally safe parts. For this purpose Altera offers certified tools in the Quartus II development environment to verify that non-safe partition changes do not impact safe partitions. Hence, a redesign does not lead to high recertification efforts. Detailed reliability data, FMEDA tools and different implementation and design guidelines help to reduce the time to market.

To support the functionally safe development, Altera provides an IEC61508 certified Functional Safety Data Package to save development time and to reduce costs. It includes not only diagnostic IP components, but also documentation, guidelines and tools. Those tools and IP are validated to be sufficiently free of systematic errors and Cyclone® V FPGAs are qualified for SIL3 applications by TÜV Rheinland.

Altera’s Functional Safety Data Package includes the following diagnostic IP:

- clock check: Monitors a clock under test and compares it to a reference clock,
- CRC calculation: Implements a CRC calculation over user-specified data,
- SEU check: Ensures that the FPGA’s SEU CRC test works correctly.

All diagnostic IP components are hardware-implemented so that the performance of the CPU is not reduced by the self-test functions. All these tools can help to reach the desirable DC of >99%.

The openSAFETY protocol stack that has been implemented on the reference design is based on the openSAFETY 1.4 stack, which is available as an open-source software from SourceForge. It has been pre-certified by TÜV Rheinland up to SIL3 in accordance with IEC 61508:2010. Besides the basic measures of the openSAFETY stack, the lockstep capability of the Nios® II architecture is utilized in a special way (see Figure 11). Instead of comparing the CRC results of the subframes in a separate operation, the CRC results just need to be written to a separate memory block inside the FPGA. The comparison will be done automatically by the lockstep since writing data to a separate memory is an output operation and so it is monitored by the lockstep.

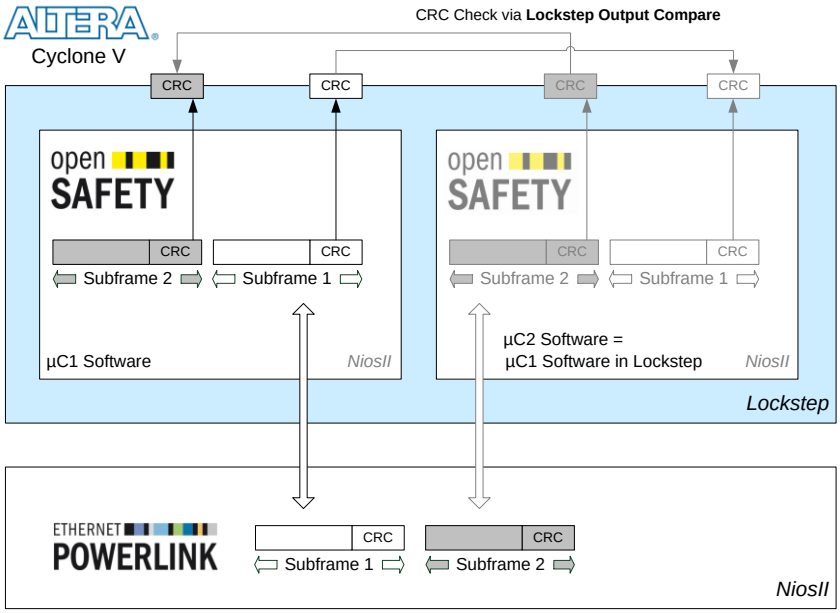

Figure 11: openSAFTY CRC and Subframes

Even though the stack software and the external hardware are SIL3-capable, the DC of the whole system has to be considered (see Figure 9). Although the reference design has a redundant lockstep architecture with a SFF >99%, the system still has a HFT = 0, because the lockstep is embedded in a single FPGA. A common cause error of the power supply could lead to a stimulations failure of both Nios® II cores. So to reach a SIL3 capability a DC > 99% is required for the whole system including buses and memories. This might be difficult to implement and moreover hard to prove for the certification.

Design with two FPGAs

A SIL2 implementation with a diagnostic coverage of >90% is a state of the art architecture and can be easily reached with a lockstep architecture on a single chip. So a simple way to make the system fulfill SIL3 is to implement the device with a hardware redundant system with two FPGAs (see Figure 12 and Figure 13). For this case, each of the FPGAs reaches a SIL2 rating. However, it is desirable to implement the system on a single chip to keep production costs low.

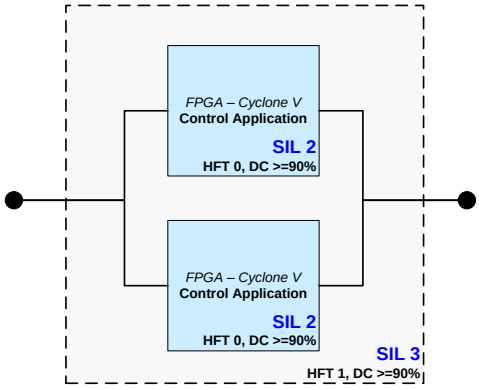

Figure 12: Hardware Redundant SIL3 Architecture

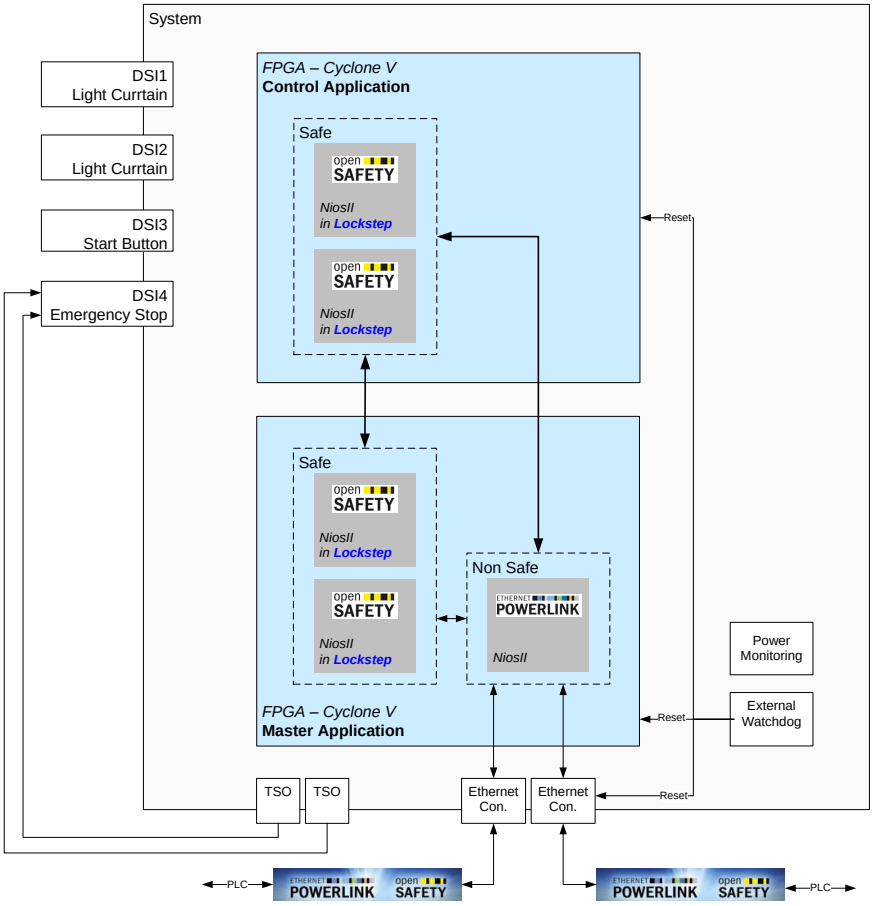

Figure 13: SIL3 Architecture with two FPGAs

Alternative Single Chip Approach

An alternative approach to accomplish SIL3 with a single chip solution is shown in Figure 14. Its special feature is that it is possible - under certain conditions - to enable a HFT1 by partitioning a single FPGA. Therefore, it must be proven that the partitions are separated clearly and that there is no common cause failure apart from the possible failure of the common power rails. So the shown SoC architecture is SIL3-sufficient with just about a DC of >90%. The implementation of each partition can easily be done with the lockstep IP of YOGITECH as shown previously in Figure 13.

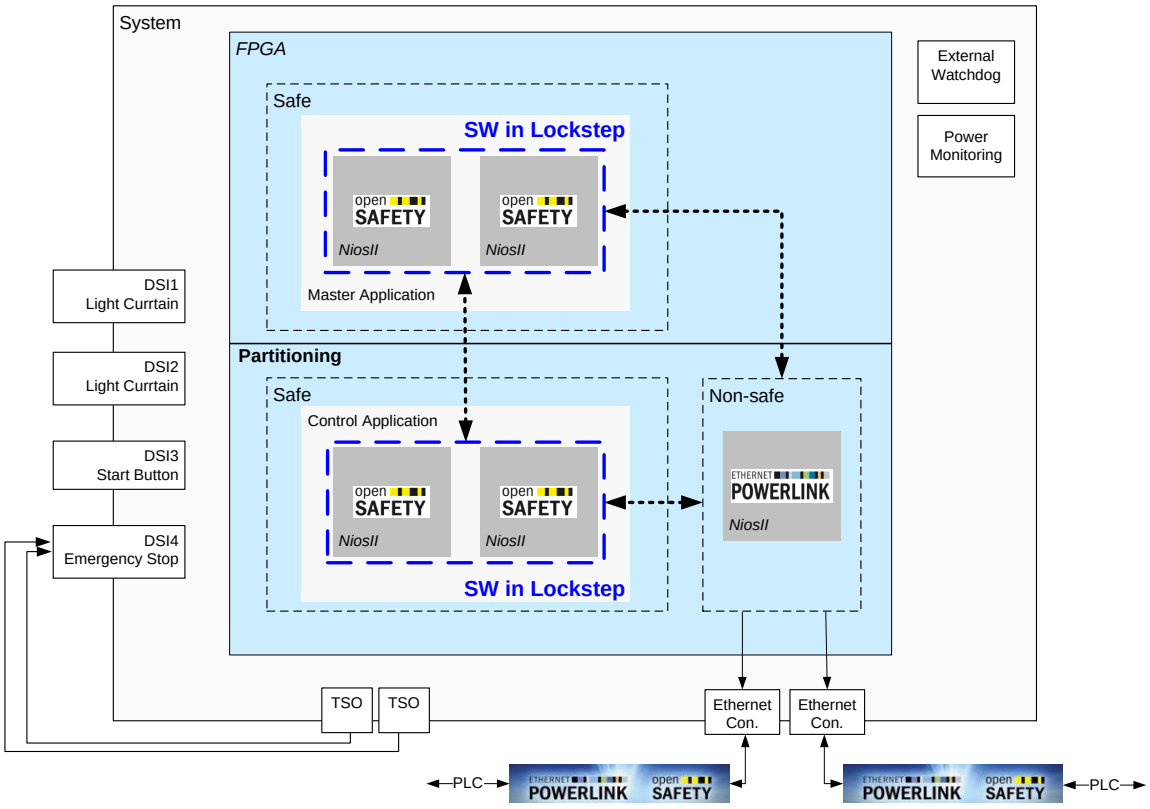

Figure 14: Single Chip SIL3 Architecture

3 Prospect

The 1oo2 design as shown in Figure 13 has been implemented on NewTec's SafeFlex FSDK (see Figure 15) which supports various industrial fieldbus communications and safety protocols. The SafeFlex – Functional Safety Development Kit (FSDK) is a FPGA based evaluation board which has been developed in cooperation with Altera. It meets the standards IEC 61508 standard up to SIL3 and ISO 13849 standard up to Pl e Cat. 4.

Additional demonstration examples of typical safety applications in industries and the gapless documentation including a standard-compliant instruction manual for the whole safety development shows which steps are needed to fulfill all the requirements of the safety standards. The SafeFlex FSDK is the ideal development platform to get stated with a safety-related Industrial Ethernet development and to reduce risks, costs, time and process overhead of new designs.

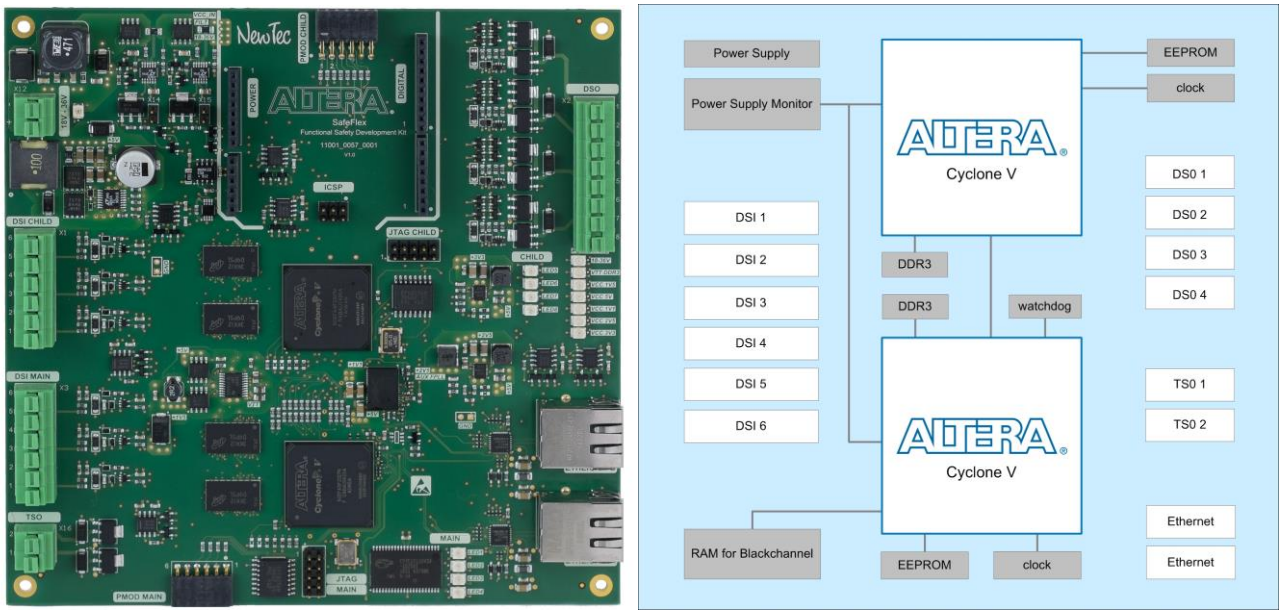

Figure 15: SafeFlex FSDK and Block Diagram

The SafeFlex FSDK offers:

- a 1oo2 Architecture (HFT = 1) with two Cyclone® V FPGAs,
- an external watchdog,
- 6 Safety Digital Signal Inputs (DSI),
- 4 Safety Digital Signal Outputs (DSO) and 2 Test Outputs (TSO),
- 2 Ethernet interfaces (for daisy chain connection in industrial networks),
- DDR3 SDRAMs, EEPROMs,
- connectors for expansion shields (PMOD, Arduino),
- a monitored power supply.

For more information go to www.newtec.de or www.altera.com.