ENABLING SIL2 SAFETY CERTIFIED APPLICATIONS FOR MOBILE MACHINE OEMS

Dr. Peter Lauer

Eaton Cooperation, Industrial Sector COE, Hydraulics, 7945 Wallace Road, Eden Prairie, MN 55344 USA
Tel.: +1 952 937 7119; E-mail address: petermlauer@eaton.com

ABSTRACT
Eaton created a new safety controller architecture to allow our customers to design implement, verify and maintain a SIL-2 safety certified application for compliance with IEC 61508:2010 and ISO 13849 Functional Safety Standards. The new architecture has been implemented in a line of safety controllers SFX12 and SFX20 that extend the line of existing mobile controllers HFX12 to HFX48. The new controllers are targeted for controlling mobile and stationary machine applications with focus on steer by wire and propel by wire. Keywords: functional safety, IEC 61508, Safety Integrity Level

1. INTRODUCTION
Functional Safety for mobile machinery is a new challenge for machine OEMs that are integrating hydraulics with electronic control systems. Several standards have emerged that can be used to prove compliance to the machinery directive by the European Union.

In this document we will outline a path to certify a mobile machine for functional safety using one of Eaton’s safety controllers.

2. THE PROCESS TO A CERTIFIED SIL2 SAFETY APPLICATION
2.1. Overview over safety standards
By signing the Machinery Directive into law, the European union mandated that products must be assessed for safety. The overarching standard for functional safety is IEC 61508 for electric, electronic and programmable electronic systems. It defines in detail how to design verify and validate an E/E/EP system and defines four SIL, safety integrity levels. ISO 13849 focuses on machinery safety and includes guidance for the
mechanical part of the machinery in addition to the electronic control. IEC 62061 and ISO 26262 apply the safety aspects to industrial application and automotive applications (Figure 1).

ISO 19014 Earth moving machines, ISO 5010 Wheel loaders, ISO 25119 Tractors, ISO 3691 Industrial trucks and others are application standards for specific groups of machines. If you are creating a safety application for a machine where an application standard exists, that standard will contain the most detailed information, since the operating conditions of the machines are known.

2.2. Steps to functional safety compliance

Select a safety standard

The machine builder/ OEM is responsible for selecting the safety standard to apply. Each standard has named their safety levels differently and associates different requirements to these levels. Once selected, the Hazard and Risk analysis will determine which safety level needs to be achieved in that standard.

Create a Hazard and Risk analysis (HARA)

The HARA is a formal process to list, classify, assess and rank the risks and hazard in the system. The standard ISO 12100 gives guidance and a basic framework to conduct the HARA.

Define the safety function AND SAFE STATE

The risk in the safety related part of the control system that needs to be reduced according to the HARA will be supervised by the Safety Function. Creating a FMEA (failure mode and effect analysis) will create the necessary input for the requirements and creates data for the diagnostic coverage. The safety function will be able to detect a hazardous state and put the system into the safe state.

The standards have design criteria that specify safety functions and safe states that must be met. An important part of the verification and validation process is to prove the correct execution of these functions.

Define and verify safety requirements

Safety standards require a formalized process to manage requirements through out the life cycle of the product.

The V model (Figure 2) is always referenced when higher level system requirements are decomposed in to lower level software and hardware requirements. Part of the planning process is to create test procedures that will be executed during the verification and validation phase.

Figure 2: V Model for System Verification and Validation
**Design and implement functional safety**

In the development process, the individual requirement elements will be realized. Hardware will be designed or purchased, software will be written, and the system will be built.

**Verify and Validate functional safety**

Verification and validation will prove that the system requirements are implemented and perform as expected. It is important that each requirement is covered with an appropriate test case, and no requirements will be missed. Testing needs to be well documented and serves as proof to the certification agency.

**Operation and Support**

The functional safety standard requires the machine builder to have processes in place for operation, production and long-term support. The product needs to have a complete life cycle support.

---

### 3. THE EATON SFX CONTROLLER

The SFX product is certified for functional safety and is a version of the Eaton HFX mobile controller family. The HFX product line is a mobile controller with typical inputs and outputs that are needed in mobile machinery. They are designed to drive hydraulic proportional valves and interface with a variety of sensors, digital and analog.

Connectivity is provided via CANbus ports using the SAE J1939 or CANopen standards.
Two sizes with four versions of programmable IO configurations, from 6 inputs and 6 outputs to 24 inputs and 24 outputs allow fitting the controller perfectly to the machine application.

Software programming in the application domain can be done in C with an extensive C-API library, MATLAB / Simulink or any of the IEC 61113-3 languages.

In addition to the standard HFX application controller with the I/O functions, the SFX version contains a separate safety CPU (Figure 3). The safety CPU monitors all inputs and outputs independent of the application CPU to allow for the implementation of application-specific safety functions that are physically isolated in the safety domain (Figure 3). The safety domain provides greater than 90% fault detection coverage.

This includes supervision of all internal voltages and servicing a hardware watchdog timer. The lockstep core ensures very low FIT numbers for the processor chip.

3.1. Channel Structure

The safety CPU is connected to the sensor input. (Figure 5). It will read the voltage directly from the pin and has its own sensor conditioning. If there is a fault in the sensor input conditioning of the Main CPU in the application channel, it does not affect the reading of the safety CPU. With the knowledge of the connected sensor in the application it can decide if the application is safe. The safety CPU queries the application CPU about the type of sensor connected, to interpret

Figure 5: 1001 Channel architecture according to IEC61508

Figure 6: SFX software architecture block diagram
the pin voltage correctly. In case the safety CPU detects a faulty sensor, it can open the safety relay that will then disable the output driver of the main CPU. That way it can prevent the application to operate with a faulty sensor and put the system into a dangerous state.

3.2. Safety function

The safety CPU will execute the user written application specific safety functions that will supervise the machine operation. In a fault condition the safety function will deactivate a safety relay that will remove power to all outputs. This will remove power from all actuators and valves that will then move into their fail-safe position.

3.3. Software architecture

The software architecture block diagram is shown in Figure 6, illustrating the software modules.

In the application domain, the core software contains all low-level drivers to service the hardware, general real time operating system functions (RTOS) and the communication interfaces. These elements are provided by Eaton. The main domain application software is created by the machine builder / OEM and contains the functions that the machine will execute. Since the main domain application is separated from the safety domain, this software does not have to meet the requirements from the safety standard. For example, once the product is released and the safety software is certified, changes in the application software will not affect the safety certificate.

In the safety domain, the core software provided by Eaton is SIL 2 compliant. The RTOS is a commercial of the shelf operating system (SAFERTOS) that is pre-certified by the vendor. All the code development is done with a SIL certified compiler (Greenhills C). A verification and validation model is executed (Figure 2), and the code quality was assessed with static and dynamic verification tools such as MISRA, Polyspace bug finder and other code analysis methods for timing, complexity and memory utilisation.

4. THE PRODUCT DESIGN PROCESS

This chapter will layout the process to design a system that requires functional safety. From the overall functionality of the machine, the safety critical functions need to be isolated. ISO 18349 calls them SRP/CS, Safety Related Part of the Control System. The hazard analysis of the system will guide through that process and identity if a SIL2 system is necessary.

For example, if the system is a truck mounted crane with a hydraulic actuator and an electronic control, then the SRP/CS is the cylinder actuation of the boom of the crane.

The next step is to identify the safe state the system needs go into in case of a failure. On a hydraulic system the safe state can be zero output flow from the hydraulic valve and no movement of the boom cylinder. In the example the hazard analysis determined a SIL2 system to be necessary. The function is a type B, high demand. Since the system has no fault tolerance, the safety failure fraction of the system needs to be 90% to 99%, the PFD below 10e-6 hours.

The safety function will be able to ensure that the SRP/CS executes correctly, that there are no faults and the actuator response is in accordance with the command input. The safety controller supervises the hydraulic system and will detect unintended cylinder motion. The safety controller will shut down the hydraulic valve via a mechanism (electronic power off or external hydraulic shut down) within a specified time, for example 0.2 seconds. It is verified by the user of the machine that when the safety function brings the system into the safe state within that specified time that the hazard has been avoided. In the verification and validation process test cases will be created that verify that the specified time can be achieved by the functionally safe system.

Creating of safety software

Application-specific safety functions monitor commands, cylinder motion and decide if unintended motion is occurring and activates the safety function. Since the main application and safety software on the SFX controller run in different domains on different processors, the safety software does not need to include application code. This simplifies the creation and verification of the software and reduces the design cycle time and effort. The safety software
will be more robust and will require no changes when the application software is modified.

**verify the metrics**

With the system completed, the actual SFF (safe failure fraction), MTBFd (mean time to dangerous failure), DC (diagnostic coverage) for the system can be calculated. The results for the SFX controller are provided by Eaton.

Verification and validation tools shall be applied to the safety software to satisfy the requirements of IEC61508. Test cases on the complete system that verify safety function, shall be executed.

**Document results**

An important part of safety system design is to create good and detailed documentation from requirements to test results. Good requirements management tools ensure valid documentation through the product life cycle. The documentation is critical for the approval process from the certification agency.

**Creating safety manual**

The documentation created during the design process are internal documents. Customer facing documents are catalogs, operation and instruction manual and most importantly the safety manual.

The safety manual gives the OEM detailed instructions under what conditions the safety integrity level is achieved.

5. CONCLUSION AND OUTLOOK

The newly designed SFX controllers will help more easily to introduce functional safety compliant machinery into the market with their unique safety architecture. This architecture is important because it allows changes to the application to be made later without having to re-certify the entire system.

**NOMENCLATURE**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>SFF</td>
<td>Safe Failure Fraction</td>
</tr>
<tr>
<td>MTBFd</td>
<td>Mean Time to dangerous Failure</td>
</tr>
<tr>
<td>DC</td>
<td>Diagnostic Coverage</td>
</tr>
<tr>
<td>SRP/CS</td>
<td>Safety Related Part of the Control System</td>
</tr>
<tr>
<td>PFD</td>
<td>Probability of dangerous failure per hour</td>
</tr>
<tr>
<td>RTOS</td>
<td>Real Time Operating System</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>HARA</td>
<td>Hazard and Risk Analysis</td>
</tr>
<tr>
<td>FMEA</td>
<td>Failure Mode and Effect Analysis</td>
</tr>
<tr>
<td>HFX</td>
<td>Eaton Hydraulics Controller</td>
</tr>
<tr>
<td>SFX</td>
<td>Eaton Safety Controller</td>
</tr>
</tbody>
</table>

**REFERENCES**

[4] IEC 61113-3 PLC languages