SIEMENS

How to become a **Safety Hero**

Guidelines for optimal machine safety
siemens.com/safety-hero

Time for heroes

Machine safety is of primary importance to manufacturing companies. It protects people and the environment, contributing to reliable production. Ensuring this requires compliance with multiple standards and specifications.

It is an important issue. But is it also a complicated one? In the videos, Paul showed you examples that point the way and offer possible steps that you can take to achieve optimal machine safety. He guided you through the process step-by-step with his magic word, “structure”, as well as introducing several tools that can help you.

This iPDF summarizes the most important points from the videos and provides additional links to related information.

We hope you will find this document to be an informative and entertaining read.

Contents

1 The goal

Safety is essential if you want to market or commission a machine in the European Economic Area. A structured approach helps you prove that your machine meets fundamental health and safety requirements. In this way, you minimize the risk of anything happening in connection with your machine. You also ensure that you will be legally protected if anything does happen.

These guidelines provide a structured procedure for achieving a safe machine. The topics are risk assessment, risk reduction, and the proof that risks have been reduced according to requirements. These are followed by a practical implementation based on a real machine.

Paul's tip:

The magic word is structure!
It ensures clarity and oversight, both of which are needed for optimal machine safety. The more structured your approach, the more easily you will reach your goal.

2 The challenges

Machines must operate in order to produce. Such operation must be absolutely safe. Guaranteeing and documenting this safety is essential. Increasingly complex technology and ever more stringent standards are only two of the challenges on the rocky road to machine safety. If you diligently tackle these challenges and seek out expert support at the right moment, you'll be very close to achieving safety hero status.

By following the right steps, using the right tools, and choosing the right partners, you will overcome all the challenges of machine safety.

3 Theoretical background

3.1 The foundation: risk assessment

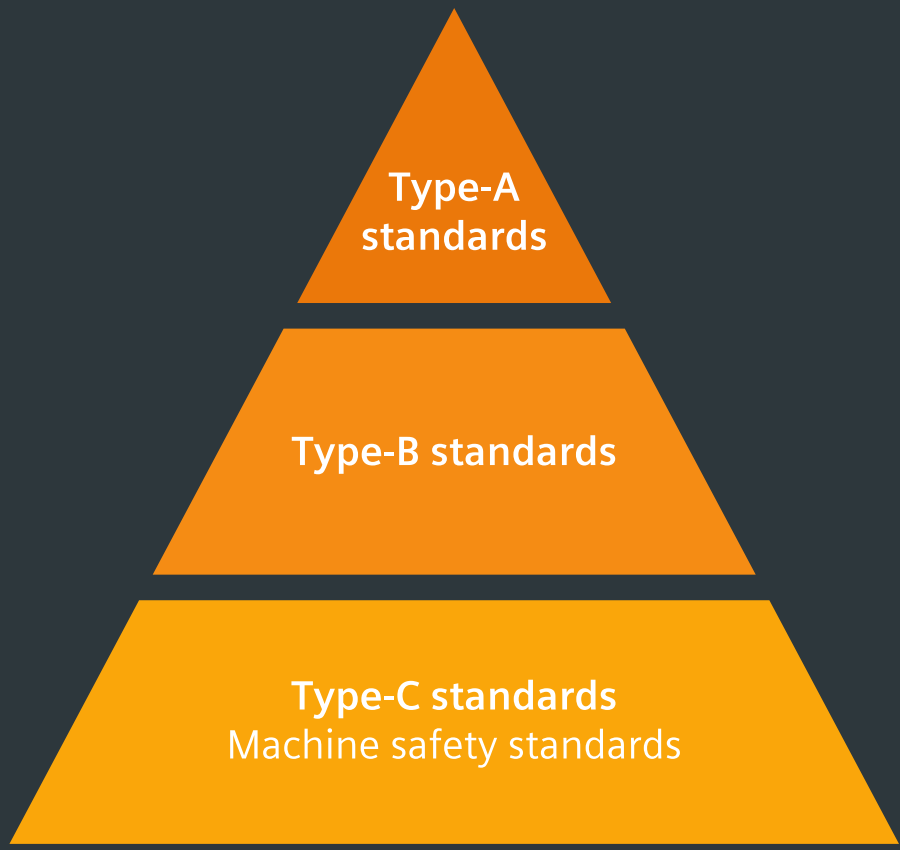
The foundation of machine safety is the risk assessment. This is where you record and assess all the potential risks. Everything is built on this in later stages. If any risks are left out of the assessment, even the best equipment cannot achieve the necessary safety level.

First, you need to identify the standards that apply to your machine. There are A, B, and C standards. For more information on these standards, refer to Section 4, Practical implementation.

You determine the extent to which your machine is covered by a particular standard. The amount of effort required for the individual assessment depends on the degree to which the standard covers your machine. If there is a C standard for your machine, it already specifies a great deal, but you still must check whether there are any other hazards that might occur with your machine.

In any case, the next thing you need is ISO 12100. This standard provides general principles for risk assessment and risk reduction and helps you manufacture a safe machine. ISO 12100 guides you through the risk assessment in three steps:

1. Identification of hazards
2. Risk estimation
3. Risk evaluation and reduction



3 Theoretical background

3.1.1 Identification of hazards

To identify hazards, you need to take a detailed look at your machine, including its use, areas of application, users, zone of movement, workstations, and intervals and period of use – for each phase of its life cycle and for each mode of operation. This is the only way to uncover all potential hazards. The devil is often in the detail.

3 Theoretical background

3.1.2 Risk estimation

Once you have identified all the potential hazards, you need to examine and assess the risks. Risk is a combination of the extent of the potential damage and the probability of the occurrence of damage. In other words: what is the worst-case scenario and how likely is it to occur?

A highly probable papercut, for example, is not as serious as a highly unlikely crushed arm. Naturally, you want to avoid both, which is why you perform a risk assessment.

3 Theoretical background

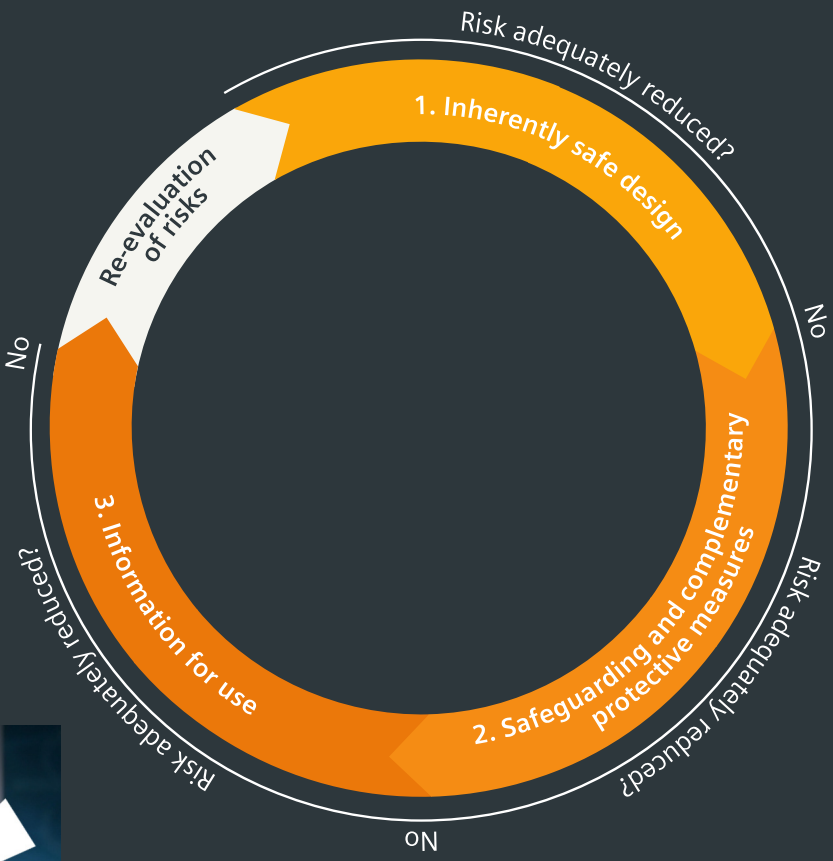
3.1.3 Risk evaluation/risk reduction

Once you have evaluated all the risks, the next step is to reduce or mitigate those risks if necessary. ISO 12100 offers three options.

- Inherently safe design
- Technical measures
- User information

The goal is to reduce the residual risk to a tolerable level.

If you have completed these steps and the risk has not been sufficiently reduced, you need to restart the process from the beginning. You must repeat these loops until the residual risk has been reduced to an acceptable level.



Paul's tip:

Always play it safe! It goes like this: evaluate the risk, initiate measures, evaluate the risk. If necessary, initiate measures, evaluate the risk, and so on and so forth.

3 Theoretical background

3.1.3.1 Inherently safe design
(elimination of hazard due to design modification)

Inherently safe design is achieved by avoiding hazards or reducing risks through a suitable choice of design features for the machine itself and/or interactions between the exposed persons and the machine.

These characteristics include, for example, the machine's geometry/design and the arrangement of the machine's components. It is important to avoid sharp corners and edges as well as protruding parts. Physical aspects also play an important role, as does limiting the actuating force, mass, and velocity.

3 Theoretical background

3.1.3.2 Technical measures
(use of safety components or protective devices)

Technical protective measures are necessary when hazards cannot be avoided by means of design measures alone or when the resulting risks can't be sufficiently reduced.

Technical protective measures are divided into two categories: protective devices such as light curtains or light barriers and guards such as protective doors. The level of risk determines the specific safety level and, by extension, the quality of technical protective measures necessary.

There are two standards for determining risk and the resulting safety levels: ISO13849-1, in which classification is by Performance Level (PL a to PL e), and IEC62061, in which classification is by Safety Integrity Level (SIL 1 to 3).

Regardless of which standard you choose, the result will be the necessary safety level for each protective measure.

Theoretical background

3.1.3.3 User information about residual risks

User information is the last option for risk reduction but is not a substitute for the correct use of the first two options. It is to be used only when, despite an inherently safe design and technical protective measures, risks still remain. In this case, user information must indicate all possible residual risks. It must include the following:

- The procedures to be followed when operating the machine and the capabilities required of operators and other people who might be exposed to hazards originating from the machine
- A description of the recommended procedures for working safely with the machine and the corresponding training requirements, provided in a suitable format
- Sufficient information and warnings regarding residual risks in the different phases of the machine life cycle
- Description of each recommended item of personal protective equipment, including details on its use and the training necessary for its use

For more information, see our reference work Introduction and Terminology for Functional Safety of Machines and Systems.

4 Practical implementation

4.1 Our demonstration machine

To make things a little easier, we have developed a demonstration machine that makes it possible to clearly apply theoretical knowledge in the real world. We can start with a brief functional description.

The tray handler in the rear section of the demonstration machine makes small parts available. The robot arm grips these parts and places them in the frames on the conveyer belt. This machine already has a safe design, but you can still see where there might be a potential hazard: at the robot arm, conveyor belt, and tray handler.

4 Practical implementation

4.2 Risk assessment: DIY or using software tools?

If you want to perform the risk assessment yourself, you can use ISO 12100 as a guideline for the steps you need to perform.

To find the standard, visit these websites, for example:

www.beuth.de/en*

www.kan.de/en/kan-praxis/kan-praxis-overview/*

You then must think about how best to structure the knowledge you've acquired and "put it down on paper" in a way that is comprehensible and can be stored in document form.

Or if you want to make things a little easier, several vendors offer tools specifically for this purpose that can greatly facilitate the process. We use the Safexpert tool (www.ibf-solutions.com/en/).*

Paul's tip:

You do not have to know everything yourself, but you do need to know where to find the things that will help you.

4 Practical implementation

4.3 Becoming a safety hero through Safexpert

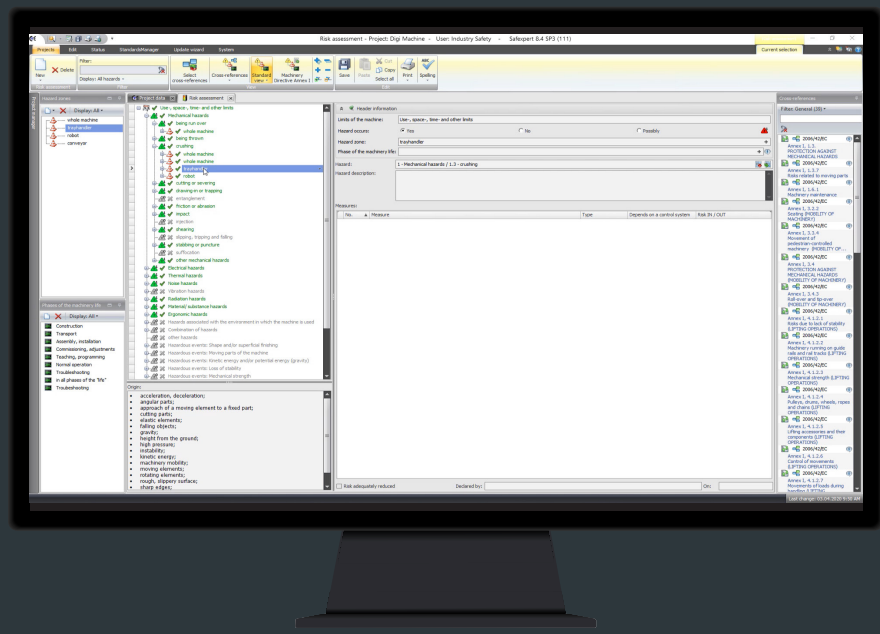
In Safexpert, you start by defining the hazardous zones and hazards. You can then define risk avoidance measures one step at a time for each phase of the machine's life cycle. The result is an acceptable residual risk.

Safexpert is divided into several areas.

- The sources, from which the potential hazards originate
- The phases of the machinery life, for which several suggestions are already given but which can also be extended
- The potential hazards mentioned in ISO 12100 and regarding which you must decide whether they apply to your machine

These items are combined in such a way that you decide for each hazard, at each hazard location, and in each lifecycle phase whether a hazard can actually occur. Finally, you describe the measures with which you are attempting to reduce the risk of each hazard.

For an example of using Safexpert to generate a risk assessment, watch the Module 2 video or visit the vendor's website: (www.ibf-solutions.com/en/).*



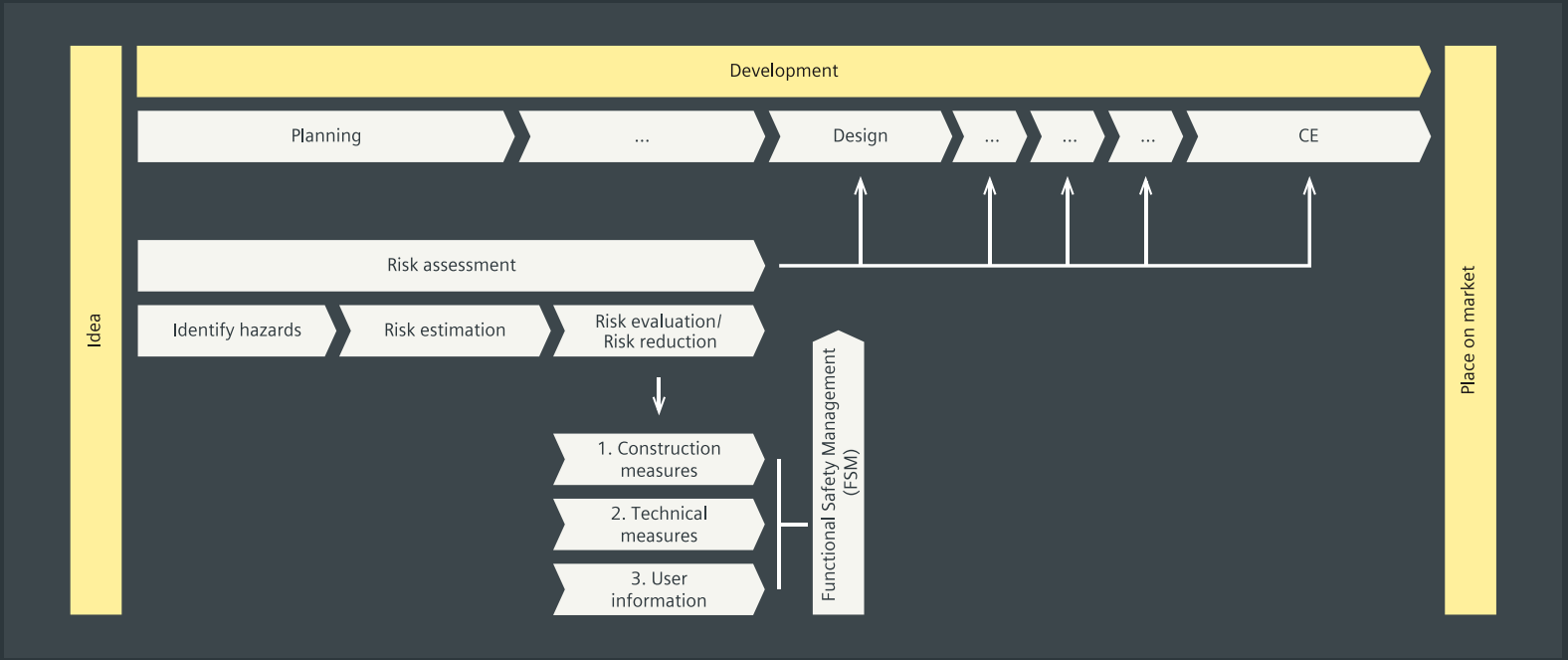
4 Practical implementation

4.4 Functional Safety Management process

In the risk assessment, safety functions were defined in the technical measures. Now it is time for their implementation.

To ensure high quality during the implementation and design phase, you must establish a suitable process. For the description, several steps are necessary to meet the requirements. With these steps, the specification, implementation, verification, and validation phases can be properly completed. The entire process is called Functional Safety Management (FSM).

To make this process as simple as possible, we've summarized the most important information here.



4 Practical implementation

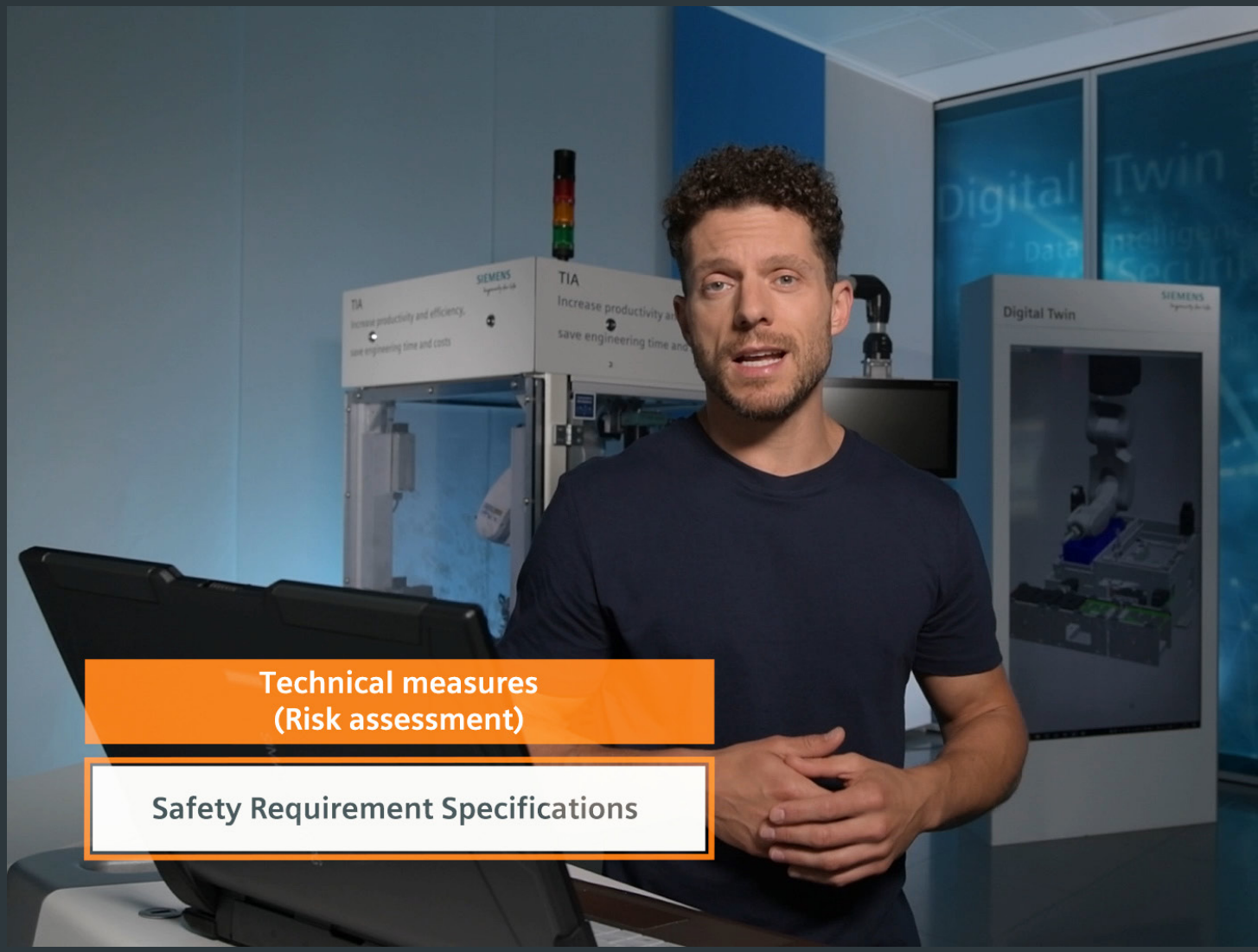
4.5 Safety Requirements Specification

The first step in the Functional Safety Management process is the Safety Requirements Specification (SRS). In this document, you specify the requirements for each safety function. You can take the necessary information from the risk assessment.

For an example of how to structure an SRS, refer to our document on the Functional Safety Management process (see page 16).

The next step in implementing the requirements is selecting and describing the hardware and defining the desired software functions.

We will start with the hardware.



4 Practical implementation

4.6 Technical measures

4.6.1 Check suitability of hardware

Safety-relevant parts must be monitored by a fail-safe system. This system can either be separate or implemented by means of SIMATIC S7-1500. It can take charge of the general automation part as well as processing and monitoring the safety functions.

Regardless of which components you choose, you should always test and document whether they enable you to achieve the required safety level.

The following components were used for our demonstration machine:

- Position switch for monitoring. It is connected to a fail-safe input module.
- Input module. It forwards the signal status to the fail-safe CPU.
- Finally, the CPU evaluates the signal and forwards it to SINAMICS S210 via PROFINET/ PROFISAFE. This then triggers the safety function.

4 Practical implementation

4.6.2 Find values and formulae

Similarly to the risk assessment, there are two options for testing whether your selection is suitable. Either you yourself can calculate whether the selected components and the structure conform to the required safety level or you can again use tools that do it for you.

To calculate it yourself, you need the appropriate formulas and the necessary characteristic values of the products used. The formulae are provided in the standards. You will find the characteristic values from Siemens and other vendors in the relevant VDMA library* or in the corresponding component manuals.

4 Practical implementation

4.6.3 Example using the TIA Selection Tool

In our opinion, it is best to use a tool. Ours is the TIA Selection Tool, which makes it possible to evaluate configurations using the “Safety Evaluation” function.

The TIA Selection Tool comprises the following four steps.

1. Select the desired products and configure if applicable. You can integrate components from additional manufacturers by importing a VDMA library.
2. Create a safety area.
3. In this safety area, create a safety function and the desired safety level (e.g. Performance Level).
4. Assign the safety function to the selected products.

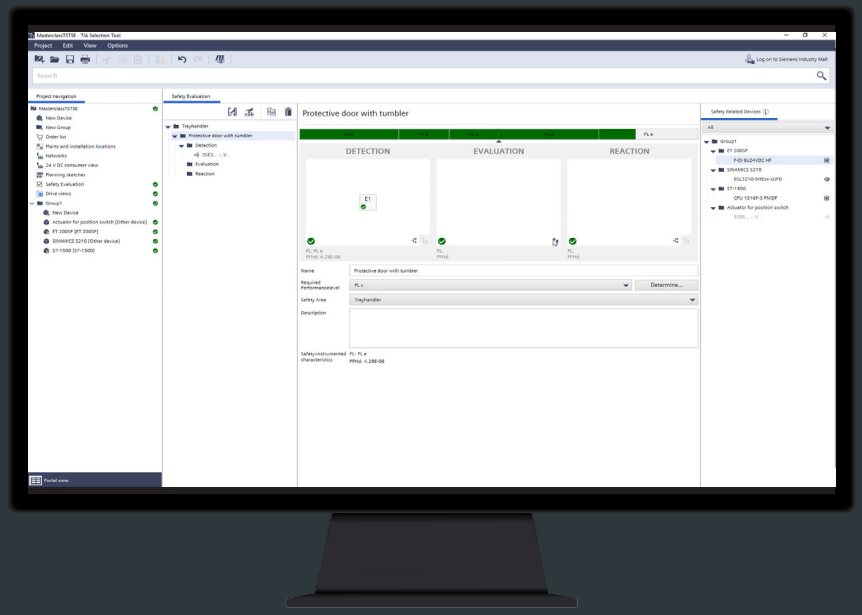
You can now see at a glance whether your selected components and the structure meet the requirements.

Once you have done that, you can save or print out this project as proof of the suitability of the selected components. To see exactly how this is done, watch the Module 2 video.

You will find the TIA Selection Tool and additional information at www.siemens.com/safety-evaluation.

Paul’s tip:

Have someone help you! Everything is much simpler with the right tool. After all, you do not use your fingers to pull a cork out of a bottle.



Practical implementation

4.6.4 Solution using SIMATIC S7

In Section 4.6.1 (page 18), we presented the hardware solution for our demonstration machine. We use SIMATIC S7-1500 as a fail-safe CPU. This step now involves programming or creating a program – for example, for monitoring the protective door. This is done in the TIA Portal.

Before we get to the actual subject of what makes a well-structured program, here is a brief overview of the TIA Portal.

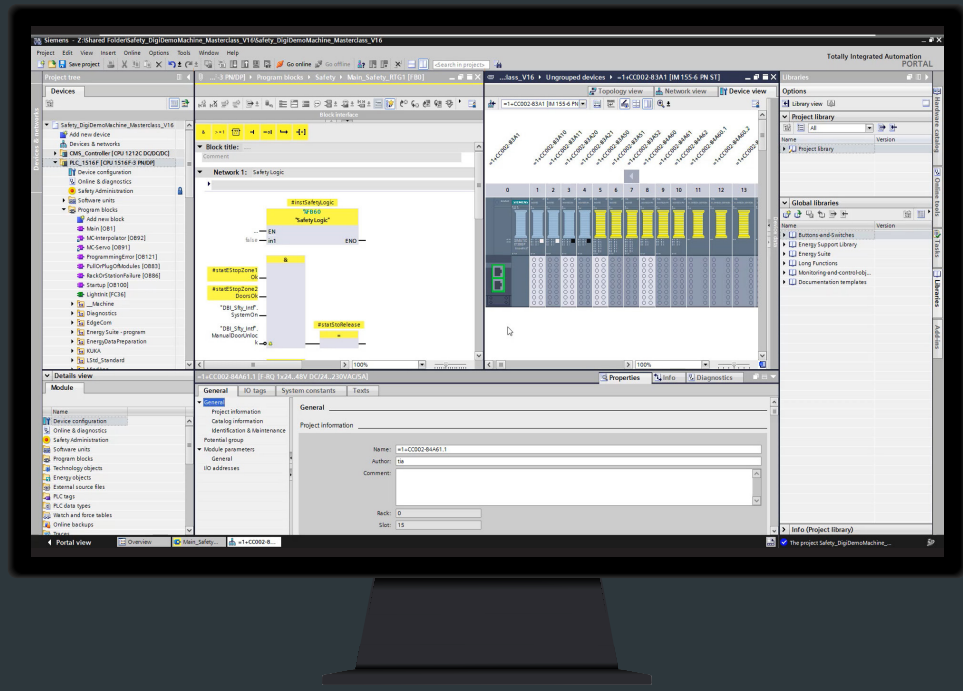
The large window in the center is the work area. This is where the objects that are open for processing are displayed.

At the bottom, you will find the Inspector window. It contains additional information on the selected object:

- The “Properties” tab shows the information that you can edit, and the “Info” tab displays additional information on the object.
- The “Diagnostics” tab provides information on system diagnostics as well as alarms and connection information.

The right-hand column contains various task cards. For example, you can select objects from a library or the hardware catalog or you can search and replace objects in the project.

You can find much more information on the TIA Portal here.



4 Practical implementation

4.6.5 Programming guidelines

We also recommend that when you are programming the safety functions, you make structure and organization a priority. In the Module 3 video, Paul highlights some important points that we will deal with here. Naturally, it is only a partial list. You will have to decide what's important and what really helps you for your particular project.

The program structure

Our demonstration machine has a separate block for each machine area or each function. These blocks are called in the Main Safety block. This makes the program easy to read and easier to test. But we will get to that later.

Create your own blocks

Commands and application blocks are available for this purpose (e.g. for monitoring the position switch or protective door). You can easily transfer them to your block using drag and drop. You must then interconnect the block's inputs and outputs.

Paul's tip:

It is recommended that you access all the signals in your block via variables and not directly (for example, the signals of the position switch). This allows you to reuse the block in other projects. And do not forget to add comments and block information! That will help you or a colleague understand what is happening in the block even after some time has passed.

4 Practical implementation

Use blocks from a library

If you use your own blocks or a block from another library, you can verify the block's checksum under Safety Administration. Then you can be sure that you are also using the desired function.

The safety program's unique fingerprint

When you have finished creating everything and the program's complete, you then have to compile it. This generates a single fingerprint for the program – the unique checksum for the entire safety program. If anything in the program is changed, the checksum also changes. That is why the checksum should be included in the documentation for your machine and can be read out or displayed on the controller.

You will find lots of useful information and practical tips relating to the Safety Programming Guideline here. You may also be interested in SIMATIC Safety Integrated.

Paul's tip:

Store the data that is exchanged between a standard and a safety program in a separate data block, once for reading and once for writing. This is the clearest way to organize it.

4 Practical implementation

4.7 Validate, verify, test

You are almost done! These final sections are about testing and inspection. Two terms that often arise in this context are validate and verify.

With validation, you prove the effectiveness of the safety functions. In other words, you check whether the measures you implemented have resulted in the required risk reduction. If not, you need to correct the technical implementation. The final option is to document the residual risk and attach warning notices.

Verification involves proving correctness, meaning you test whether the hardware and software meet the relevant requirements.

4 Practical implementation

4.7.1 Testing block functionality using the TIA Portal Test Suite

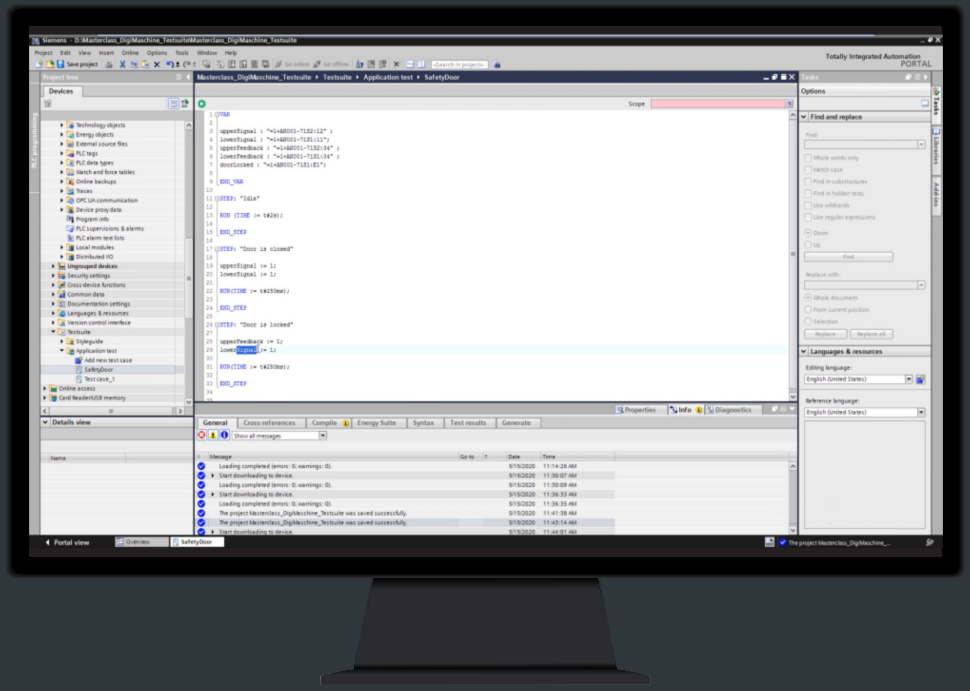
To test whether the software and individual blocks function as specified, you need to perform a function test. If applicable, you can also test functioning in a simulation.

The TIA Portal contains the TIA Portal Test Suite, which makes this process somewhat easier. For example, you can use the Test Suite for a block test to:

- Specify the input values and the expected results
- Execute the block
- Compare the results of the block with what was expected

If the test is successful, you then add it to the documentation. In the Module 4 video, Paul shows you how this is done, based on the example of protective door and tumbler mechanism monitoring in our demonstration machine.

For related information, watch this video* on the TIA Portal Test Suite and visit this webpage on software in the TIA Portal.



4 Practical implementation

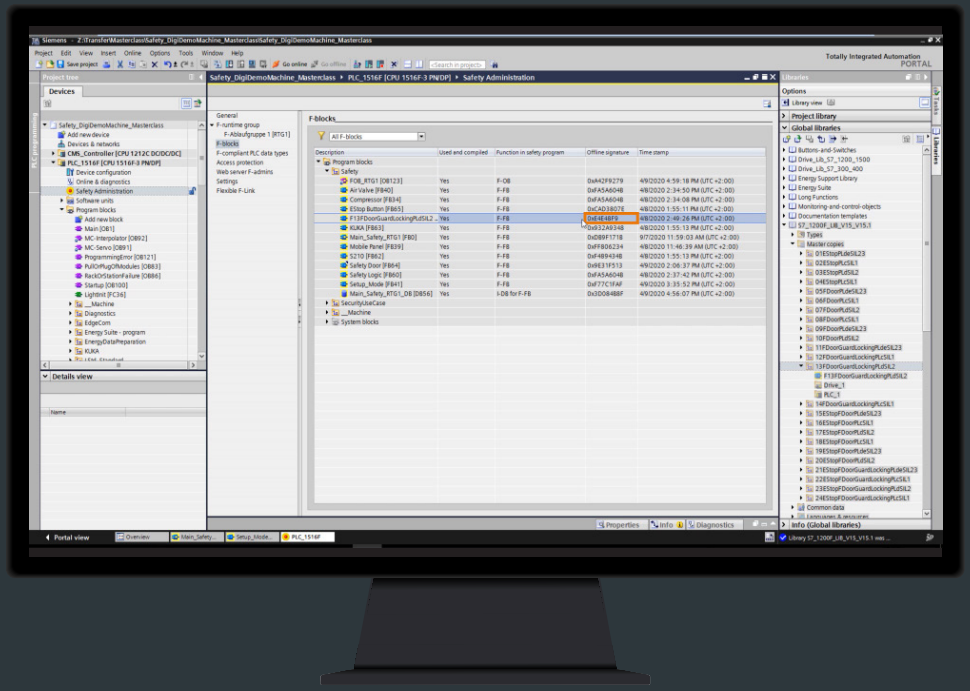
4.7.2 Simplifying by using pretested blocks

Verification is much easier if you are using a block that may have already been used in another project or has already been tested.

Each block has a unique checksum that changes as soon as changes are made to the block.

This means that if you want to reuse a block without changing it, you simply have to verify the block's checksum under Safety Administration. Then all you need to do is check whether the block call uses the right parameters or variables.

So, you see, creating reusable (meaning standardized) blocks can save you a lot of time.



4 Practical implementation

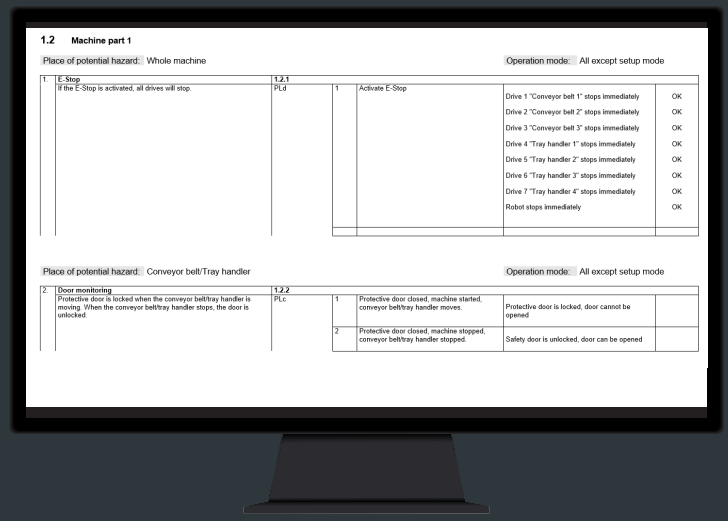
4.7.3 Acceptance test

We have saved the Factory Acceptance Test (FAT) for last. It is also a function test – in this case, a test of everything together, meaning hardware and software.

Once again, we recommend that you document the test cases as well as possible ahead of time. We have provided a sample template that we have also used as part of the FAT for our demonstration machine.

If a test yields the expected results, you can check off the associated item.

Once all tests have been successfully passed, you simply have to sign your name and add the test protocol to the other documents.



1.2 Machine part 1

Place of potential hazard: Whole machine — Operation mode: All except setup mode

1	E-Stop If the E-Stop is activated, all drives will stop.	1.2.1 PLd	1	Activate E-Stop	Drive 1 "Conveyor belt 1" stops immediately	OK
					Drive 2 "Conveyor belt 2" stops immediately	OK
					Drive 3 "Conveyor belt 3" stops immediately	OK
					Drive 4 "Tray handler 1" stops immediately	OK
					Drive 5 "Tray handler 2" stops immediately	OK
					Drive 6 "Tray handler 3" stops immediately	OK
					Drive 7 "Tray handler 4" stops immediately	OK
					Robot stops immediately	OK

Place of potential hazard: Conveyor belt/Tray handler — Operation mode: All except setup mode

2	Door monitoring Protective door is locked when the conveyor belt/tray handler is moving. When the conveyor belt/tray handler stops, the door is unlocked.	1.2.2 PLc	1	Protective door closed, machine started, conveyor belt/tray handler moves.	Protective door is locked, door cannot be opened	
			2	Protective door closed, machine stopped, conveyor belt/tray handler stopped.	Safety door is unlocked, door can be opened	

Paul's tip:

You will have accumulated quite a few completed documents, test protocols, and other paperwork. Once again, STRUCTURE is the key. Apart from an organized folder structure, we recommend that you create an additional document about all the other documents. This will make it clear what documents exist and where they are stored.

5 Summary

Can you feel it? You now have what it takes to become a safety hero. Functional, effective safety is not rocket science! Structured procedures – as well as useful tools and documents – assist you on your way to a safe machine.

Good luck for the future!
The Siemens Safety Integrated team

Published by
Siemens AG

Digital Industries
Factory Automation
P.O. Box 4848
90026 Nuremberg
Germany

* Disclaimer

The hyperlink above refers to other websites or sources (in the following called "sites"). Siemens has no control over these sites and therefore cannot be held responsible for the availability, completeness or faultiness of such sites. Further on, Siemens does not endorse and is not responsible or liable for any content, goods and products or other materials on or available from such sites. Any contract has to be made exclusively between the consumer and the provider of these sites on the provider's specific business conditions.