Whitepaper

Risk Assessment: Safety vs. Security

Learn more about how to

- Distinguish between the terms safety and security
- Carry out a risk assessment in accordance with the Machinery Directive
- Analyze risks in the context of industrial security

PHOENIX CONTACT

Introduction

In the fields of manufacturing and machine operation, the terms safety and security are increasingly used in connection with one another. Both terms involve protection of people and machines as their ultimate goal.

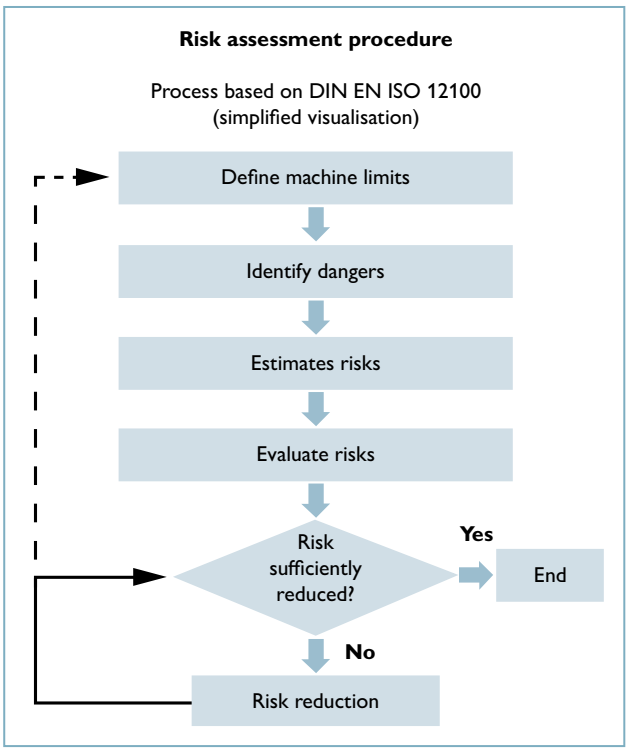
The term safety is to be understood to be the protection of people from the dangers posed by the machine. The term security is used when people are talking about the protection of machines from unauthorized access by people. Examples of this could involve data hacking or destruction of the system.

Below, we will demonstrate the extent to which risk assessment (safety) and risk analysis (security) are similar to one another in their approaches and implementation.

Content

1 Machine safety risk assessment

The requirements for creating the risk assessment for machines can be found in the EC Machinery Directive. It states that the machine manufacturer must start the risk assessment during the design phase. Findings gained during manufacturing and field information from past projects must be included. The risk assessment ends when the machine is implemented; in other words, when it is built.



Overview of the risk assessment process in accordance with EN ISO 12100

The first step is defining the limits of the machine. It's not just the obvious aspects such as weight, dimensions, materials used, or the type of workpieces to be processed that fall under the limits of the machine. In particular, the personnel that will be working on and around the machine must be thoroughly analyzed. This involves distinct differences with regard to training, experience, and abilities. In this context, hazards for an operator can and must be estimated differently than those for a repair worker, since both people work on the machine at different times (as an example). The activities in the individual life stages and the operating modes of the machine provide the necessary information to recognize the different hazards. EN ISO 12100 also provides useful information.

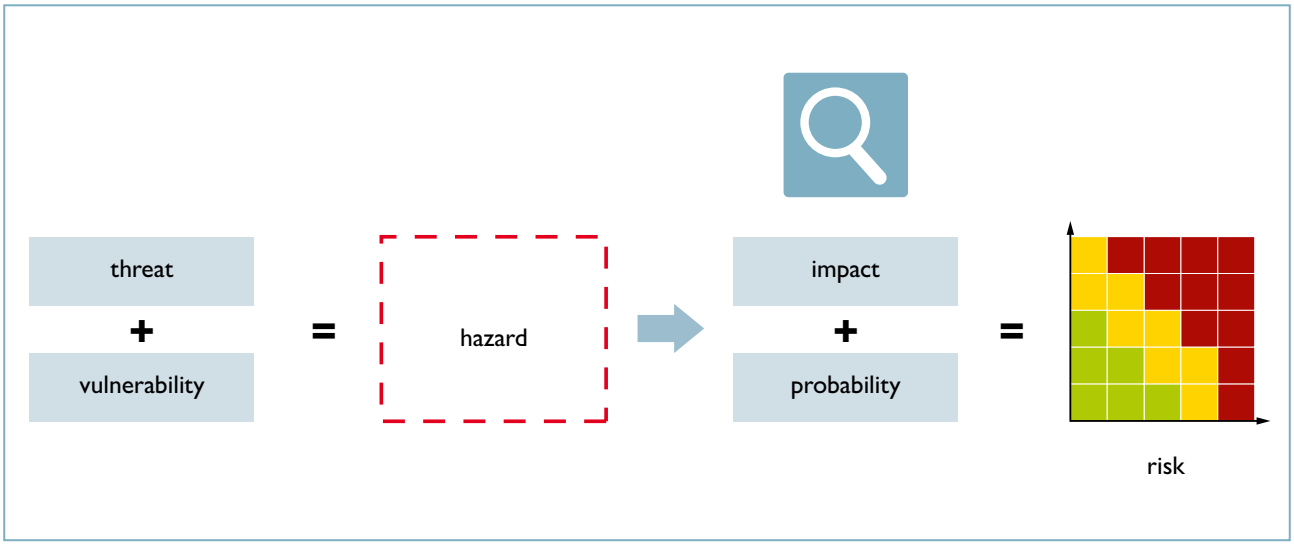
Afterward, all dangers that are caused by the machine must be identified. The dangers are then evaluated based on factors, such as the severity of the possible injury. With this assessment, the user can evaluate whether they need to take action to reduce the risk. To achieve sufficient risk reduction, protective measures must then be defined. The user can find the process for determining potential dangers in EN ISO 12100. There, possible hazards are listed which could arise during different life phases, among other things.

It is recommended to conduct the hazard identification and the risk estimation, risk assessment, and risk reduction based on a list or table. Listing them in table form allows a structured approach. Furthermore, this provides proof that all possible hazards have been checked. The risk assessment consists of many individual parts. Only after all elements have been examined and documented is it certain that the machine will meet the basic health and safety requirements. The risk assessment is used as legal proof that the machine manufacturer has adhered to that the requirements of the Machinery Directive.

2 Risk analysis for industrial security

Machine manufacturers are not (yet) under any legal obligation to carry out a risk analysis. Protecting a machine against attacks by third parties is the result of a voluntary decision by the manufacturer or happens upon the request of the operator (contract law).

The risk analysis begins with the development of the automation concept, and must be checked on an ongoing basis. It can never be considered complete, because the threat conditions are constantly changing and the implemented measures must be reviewed regularly in terms of their effectiveness.



Explanation of the terms in the context of industrial security

IEC 62443 can be applied to perform a risk analysis. First, the persons carrying out the analysis must determine which security threats are relevant for an automation system. Frequently, this is discussed as part of a threat analysis.

The regularly-published document from BSI, "Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen", can be analyzed as a template for threats present in the industrial environment, for example. This document is also published in English with the title "Top 10 Threats and Countermeasures" on the German Federal Office for Information Security website. One example of a threat are interfaces to which the system in question can be connected. These interfaces can serve as weak points that allow for the introduction of malware via removable media and external hardware. The threat must be considered relevant and analyzed in a risk analysis.

According to the common definition of the term risk, an estimate with regard to the possible effects and the possible damage and the probability of occurrence is made. It is helpful to establish how many stages will be considered in the assessment and how these are defined in advance. For example, the monetary definition of serious damage will be different for each company.

The estimate for the potential damage posed by a threat is still comparatively easy. It is much more

difficult to assess the probability of occurrence, which must be calculated based on various individual parameters and contextual information. One possible approach for calculating the probability of occurrence is based on two parameters. First, you determine how complex the possible attack is and which access rights the potential attacker needs. From this, you can arrive at a statement on the probability of occurrence instead of simply expressing it all as a single value.

Measures must be developed for risks that are unacceptable to the company. These measures must be checked prior to implementation for their potential influence on the damage and the probability of occurrence. Usually, a differentiation is made between four options for dealing with risk:

- Risk prevention
- Risk reduction
- Risk shifting
- Risk acceptance

3 Conclusion

Conclusion: Differences between safety and security

Even if there are different goals, the approach for determining the risk is very similar. Common terms can be found in EN ISO 12100 and IEC 62443. Certainly a single person cannot perform both a risk assessment or a risk analysis for both safety and security. These require comprehensive knowledge of the respective field. But anyone can follow and understand the basic procedure.

Contact

Book your consultation now!

Are you looking for a powerful partner for the subject of functional safety?

Functional safety is an important subject. Phoenix Contact provides the products, training courses, and TÜV-certified experts to help you meet the safety requirements of the Machinery Directive and the process industry. We'll get you fit for the safety of people and machines.

Let´s get **#FitForSafety**

Visit us at phoenixcontact.com/fitforsafety

Carsten Gregorius
Product Marketing for Safety
at Phoenix Contact

cgregorius@phoenixcontact.com

Torsten Gast
Director Competence Center
Services at Phoenix Contact,
Author of the whitepaper

torsten.gast@phoenixcontact.com

AI 04-21.001.L3