advertorial

Advertorial: Witteveen+Bos

Within the Netherlands, there are hundreds of movable bridges located throughout the entire country. These bridges are owned be several instances, like Rijkswaterstaat, ProRail, provinces, municipalities, but also water boards. These bridges should be considered as a machine with large, moving parts and therefore they can be assessed by means of the Machinery Directive (2006/42/EG). The main goal of this directive is to establish that these machines comply with the so-called essential health and safety requirements. In other words, the movable bridges in our country need to be safe.

Risk assessment

In order to determine what 'safe' actually means, it is required by the Machinery Directive to perform a risk assessment movable bridges. By following a structured analysis the present risks are to be identified, quantified and then reduced or mitigated by taking adequate measures. A well-known method for performing risk assessment on machinery is described by ISO 12100. In the end, one will find a list of risks which need to be reduced.

Figure 1. Example of a movable bridge (Schinkelbruggen, Amsterdam).

author: dr.ir. H. Droogendijk

The first step in reducing risks is to alter the design, in order that either the hazard is removed or the risk has vanished. However, in many cases this step cannot be executed due to e.g. design specifications. The second step is to look for mechanical solutions, which prevent a person from entering hazardous areas, such as physical barriers and guards. Though, there are numerous situations in which these types of solutions do not suffice. For example, if maintenance is required, one will actually need to enter hazardous areas. Then, the solution for risk reduction can be yield by functional safety.

Functional safety

Functional safety in machinery usually means systems that safely monitor and, when necessary, override the machine applications to ensure safe operation. This means that a safety-related system implements the required safety functions by detecting hazardous conditions and bringing operation to a safe state, by ensuring that a desired action, e.g. safe stopping, takes place.

Generally, safety chains are designed in order to obtain the input ('sensor'), process this input by a control system ('logic') and perform an action on the machine ('actuator').

The way safe stopping actually needs to be realized is a matter of choice and standards. The standards for electronic safety systems are formally designated by both ISO 13849- 1 for Performance Level (PL) and IEC 62061 for Safety Integrity Level (SIL).

In this article, the standard for SIL and its application on designing movable bridges is discussed, since the method of SIL is commonly used by Witteveen+Bos in projects on movable bridges.

Safety Integrity Level (SIL)

IEC 62061 is the standard for designing electrical safety systems. It includes recommendations for the design, integration and validation of safety-related electrical, electronic and programmable electronic control systems for machinery. This standard also covers the entire safety chain, e.g. sensor-logic-actuator. As long as the entire safety function fulfils the defined requirements, individual sub-systems need not be certified.

The standard defines how to determine both the required and achieved Safety Integrity Level (SIL). SIL represents the reliability of safety functions. Four SIL levels are possible: 1, 2, 3, and 4. 'SIL 4' is the highest level of safety integrity and 'SIL 1' the lowest. In the field of machinery (and thus movable bridges), only levels 1-3 are used.

Safety integrity level	Probability of a dangerous Failure per Hour (PFH_D)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Table 1. Overview of safety integrity levels

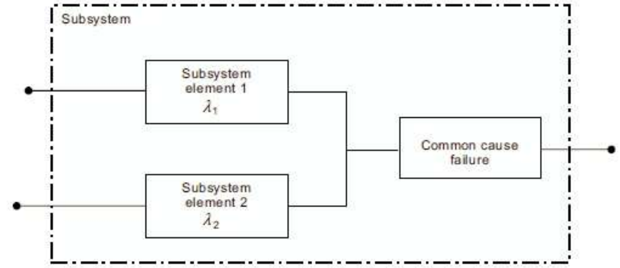

Figure 2. Example of a subsystem for a safety chain

Dangerous failure

In IEC 62061, a safety integrity requirement is expressed as a target failure value for the probability of dangerous failure per hour, PFH_D, as shown in table 1. A dangerous failure is to be considered as a situation where a malfunction of the system will lead to a dangerous situation (like unexpected movements of the machine).

Additionally, there exist threshold values (per hour) for systems that do not contain sufficient diagnostic coverage (e.g. automatic diagnostic tests on proper component operation). This coverage DC can be expressed as the ratio between detected dangerous hardware

$$DC = \frac{\Sigma\lambda_{DD}}{\Sigma\lambda_{D,total}}$$

failures, $\sum\lambda_{DD}$, and the total of dangerous hardware failures $\sum\lambda_{D,total}$:

Determination of the value of PFH_D depends of the design of the safety chain and choice of components and can be quite complicated. An example is given below, where a system is considered with single fault tolerance (i.e. redundant architecture) and without a diagnostic function. Note the presence of the common cause failure (CCF), for which a single fault will lead to a failure by both channels.

For such an architecture, the probability of dangerous failure of the subsystem is:

$PFH_D = \lambda \times 1h$,
$\lambda = (1-\beta^2)\lambda_1\lambda_2 T_1 + \beta/2\,(\lambda_1+\lambda_2)$

where T_1 is the proof test interval or lifetime (smallest), β is the susceptibility to common cause failures and λ is the failure rate.

Architectural constraints

To realize a system which yields a sufficient integrity on safety, there are generally two approaches. The first approach is to consider hardware fault tolerance, by designing a system using a redundant architecture (e.g. the previously mentioned subsystem). Though, there are limits on what can be achieved on SIL, by considering table 2, due to the lack of diagnosis.

Diagnosis

As can be derived from the analysis on architectural constraints, the other approach for achieving safety integrity is to design a 'smart' system. Such a system contains several diagnostic functions in which dangerous failures are either early detected or will lead directly lead to a

Safe failure fraction	Hardware fault tolerance (see Note 1)		
	0	1	2
< 60 %	Not allowed	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL3 (see Note 2)
≥ 99 %	SIL3	SIL3 (see Note 2)	SIL3 (see Note 2)

NOTE 1 A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety-related control function.

NOTE 2 A SIL 4 claim limit is not considered in this standard. For SIL 4 see IEC 61508-1.

Table 2. Architectural constraints for SIL

safe condition of the system.

From this table, the so-called safe failure fraction SFF determines which SIL can be achieved by implementing a specifically chosen hardware fault tolerance. The expression for SFF is:
where $\sum\lambda_S$ is the rate of safe failure (when a fault leads to a safe state/stop), $\sum\lambda_{DD}$ is the rate of dangerous failure which is detected by the diagnostic functions and $\sum \lambda_D$ is the rate of dangerous failure.

$$SFF = \frac{\Sigma\lambda_S + \Sigma\lambda_{DD}}{\Sigma\lambda_S + \Sigma\lambda_D}$$

Safety chain example

To illustrate how such a safety chain can look in practice, consider the example below. Here, two emergency stop buttons in series are considered, that are connected to a safety-PLC (i.e. redundant processors, I/O, communications etc.). From this PLC, two actuators (contactors) in series are controlled, that can switch the main current to the driving motor. Diagnostics are implemented by proper configuration of the safety PLC: the input is monitored by e.g. cross-monitoring contacts of the emergency buttons, whereas the output is monitored by exploiting feedback on the contactors. By using a redundant architecture (hardware fault tolerance equal to one), safety components and diagnostics, this safety chain is suitable up to SIL3.

Conclusion

Safety for movable bridges can be achieved in several ways. Today, the majority of risks for these type of bridges are reduced or mitigated by means of functional safety, wherein a safety chain will bring the bridge control system in a safe state (e.g. stop). Key aspects of designing these safety chains are failure rate, choice in architectural constraints and diagnosis.

Further reading

See standard IEC 62061.

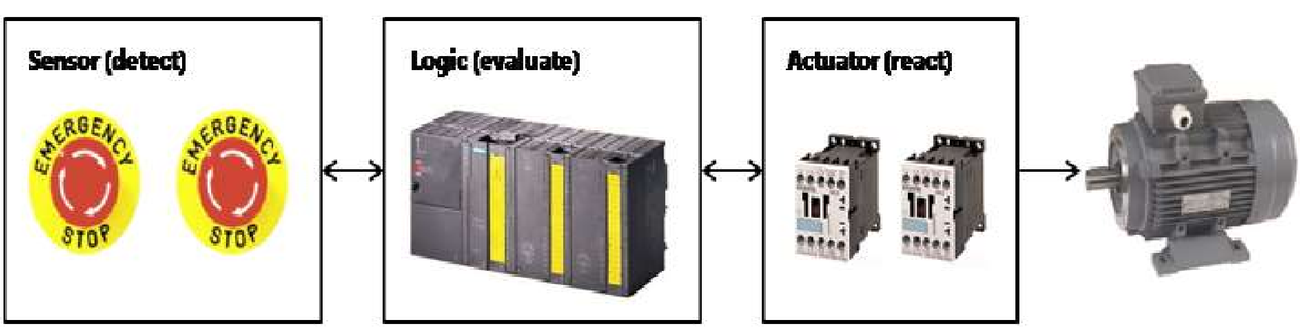

Figure 3. Example of a safety chain with redundant architecture and diagnostics.