SAFETY INTEGRATED. HOW MUCH SAFETY LIES WITHIN TUNNEL AUTOMATION?

R. Raffeiner, T. Pfeiffer
Siemens AG Österreich

ABSTRACT

In automation technology, fail-safe control components have been long enforced. Ensuring the safety of human, machine and equipment has led to a wide product range of safety components at any considerable manufacturer of control components. Thereby, functional safety is able to cover a further aspect in addition to the availability of control systems. Compliance with the applicable standards is a prerequisite to realize a secure machine or facility.

In tunnel automation, consideration of the availability of the control system has been proven and led to a high standard for automation solutions. Fail-safe control components are able to add to the automation solution, besides availability, also the component of functional safety, and even in the case of error to increase the quality of execution of the control task and, thus, contribute significantly to risk reduction.

This paper seeks to provide insight into safety engineering from the perspective of automation and to highlight possibilities of tunnel automation applications.

Keywords: tunnel automation, high-available, safety integrated, safety

1. INTRODUCTION

„Ensuring safety in automated processes is not only a question of human obligation, but also of economic reason.” - Werner von Siemens 1880

An old quote that, even in today’s time, hasn’t lost of its topicality. Especially in tunnels, safety is top priority.

Through risk analysis of tunnel systems, measures can be defined that help increase the safety in the tunnel concerning each particular application. These measures determine the way of ventilation systems, possibilities of hazardous transportation, etc. The inclusion of the automation system, which implies the components allowing a safe operation of the tunnel, is usually not considered.

A robust automation system with a high-availability configuration is a prerequisite to ensure safe operation and to offer, in case of fire, the highest possible protection for human beings and the tunnel itself. However, it is vital to note that “zero risk” is not feasible. As shown in Figure 1, risk can be reduced to an acceptable level by applying appropriate measures and, in the final step, also via a safety system (Failsafe Control).

Within the first step, structural measures should be a priority. These are adequately described in various standards and guidelines. Nevertheless, it should not be forgotten that control technology contributes significantly to the operation and safety of the tunnel.
Modern control technology regulates complex ventilation programs, manages the flow of information within the tunnel, takes control of traffic programs and guidance systems and, thus, forms the backbone of all technical equipment in the tunnel.

2. SAFETY FROM THE PERSPECTIVE OF AUTOMATION TECHNOLOGY – THE BASICS AND DEFINITIONS

Particularly in tunnels, special attention needs to be paid to availability, functional safety and functional integrity. Availability and functional safety can be guaranteed through the system design and the selection of suitable control components. Functional integrity of the control system should be given when the automation system could be directly exposed to the effects of fire within the tunnel (mostly not the case when spatial separation).

2.1. Availiability

Availability is the probability of a system being operable at a predetermined time. It can be increased by the use of high-availability modules, which extend the MTBF (Mean Time Between Failure) of a system by a large factor. [1]

2.2. Functional Safety

Functional safety describes the part of the system’s safety, which is challenged by a 100% function of the safety-related system and the external devices for risk reduction. Once the system detects an error, it leads to a safe-defined state of the application or the machine / facility. [2]

2.3. Functional Integrity

The functional integrity (fire resistance) of a component is part of a substance’s reaction to fire. It is measured by the duration for which a component keeps its function in the case of fire. Depending on the prescribed duration of function maintenance, E30 / E90 (integrity at least 30 / 90 minutes) is required for the wiring systems (cables and ducts). [3]
2.4. Norms and Guidelines

For control systems to meet the safety requirements and thus offer functional safety (Safety Integrated), they must principally be designed accordingly to the basic standard IEC 61508.

- **IEC 61508**
  Regarded as a fundamental standard and the basis for safety standardization. It covers all areas in which safety-related protection is realized by electrical, electronic, or (memory-) programmable systems. [4]

The way in which systems need to be safety-related designed, is treated in the standard IEC 61511 and IEC 62061.

- **IEC 61511**
  Functional safety for processes, sector-specific standard for the process industry [5]

- **IEC 62061**
  Safety of machinery – functional safety of electrical, electronic and programmable controllers of machines and equipment [2]

Regarding the minimum requirements for safety in tunnels of the road network one must consider for Europe the directive 2004/54/EC and for respective member states corresponding guidelines for implementation. Exemplary, Germany RABT (guidelines for the equipment and operation of road tunnels) and Austria RVS (directives and regulations for highways) are being considered in terms of availability and functional safety of automation.

- **RVS**: The RVS prescribes explicitly the consideration of the system redundancy within the control system depending on the risk level. Functional safety of the automation system is not being covered by this directive. [6]

- **RABT**: The RABT also describes the redundancy of control systems and bus systems. Regarding functional safety of the control system, no description is being provided. [7]

Therefore, control manufacturers and installers of the equipment need to obey the directives in order to fulfill the safety requirements.

In the above guidelines for tunnel equipment inclusion of the availability is given, however a consideration in terms of functional safety is not yet explicitly stated.

3. TECHNICAL SOLUTIONS

What are the possibilities for designing a fail-safe control system and which advantages can the system provide?

3.1. Design variations for Failsafe Controllers

Considering a purely fail-safe system, four construction alternatives arise as shown in Figure 2. Looking at the cost analysis, flexibility, ease of programming, maintenance and commissioning, the structure would prevail with only one SPS and mixed I/O system (Figure 2, variant 4).
For the bus system, it is recommended to use a standardized and possibly widespread system, which is also able to allow fail-safe communication. Since its introduction in 1989, PROFINET has become the world’s leading field bus system for the automation of machines and plants.

In addition to PROFIBUS, the Ethernet based PROFINET also counts to the world’s most widespread bus systems. Both bus systems are supported by the PI organization (PROFIBUS und PROFINET International), which is the world’s largest automation community.

Relevant guidelines mentioned in chapter 2.4 define primarily a high-available system. Logically, in the case of an additional fail-safe structure, a system can be chosen, which supports a high-available configuration where components can run fail-safe as needed. A basic requirement is that the PLC (programmable logic controller) runs high-available and fail-safe. Thus selected system architecture, as shown in Figure 3, can be designed as a fail-safe high-available system via a skillful selection of additional fail-safe modules, inexpensively and without changing the system architecture.

Figure 2: Fail-safe design variations (yellow components are fail-safe modules)

Figure 3: Construction types of high available fail-safe controls
3.2. Availability and functional safety of high-available fail-safe systems

The MTBF (Meantime between Failure) value is relevant for the availability of a module. The MTBF represents a statistical mean for the average time between two random failures during the normal period of use [8]. Table 1 displays the effect of a high-availability setup on the MTBF value. Concerning the control system, a Siemens S7-CPU417-5H was used for this calculation. This type of control is already applied in tunnels worldwide and due to its hardware-based PLC architecture (no PC based control) it comes with high robustness (MTBF 23 years). Hence, in case of a high-availability configuration, the MTBF value can be increased by the factor 38. Involving the control system periphery into the system’s observation, an additional significant increase of the overall system can be achieved.

### Table 1: Characteristics of high-availability automation systems [9]

<table>
<thead>
<tr>
<th>PLC Layout</th>
<th>MTBF Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault-tolerant PLC in stand-alone mode (e.g. CPU 417–5H)</td>
<td>1</td>
</tr>
<tr>
<td>Redundant PLC 417–5H in divided rack, CCF = 2%</td>
<td>approx. 20</td>
</tr>
<tr>
<td>Redundant PLC 417–5H in two separate racks, CCF = 1%</td>
<td>approx. 38</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Layout</th>
<th>MTBF Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-sided distributed I/Os</td>
<td>1</td>
</tr>
<tr>
<td>Switched distributed I/O, PROFIBUS DP, CCF = 2 %</td>
<td>approx. 15</td>
</tr>
<tr>
<td>Switched distributed I/O, PROFINET, CCF = 2 %</td>
<td>approx. 10</td>
</tr>
</tbody>
</table>

Once the system is being expanded by including the aspect of functional safety, it is recommended to consider the SIL (Safety Integrity Level) for the control system.

The Safety Integrity Level is, among others, a performance criterion, which describes the probability of failure of the SIS (Safety Instrumented System) in case of an incident. A higher SIL should therefore lead to a higher functional safety.
Consequently, the MTBF time can be increased significantly by a high-available system. Additionally, if the automation system is fail-safe the risk of a “wrong” executed switching action, in case of failure, can be reduced (Table 2). If an error occurs, the system is able to switch over into the safe mode where, in our case of a tunnel, ventilation, lighting or fire dampers can be controlled so that a safe operation is still possible. In order to guarantee this service, control components must be approved for the determined SIL level.

**Table 2: Safety Integrity Level: Probability of failure on demand [5]**

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Probability of failure on demand (PFD) per year</th>
<th>Risk Reduction Factor = 1/PFD</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 4</td>
<td>&gt;=10^{-5} to &lt; 10^{-4}</td>
<td>100000 to 10000</td>
</tr>
<tr>
<td>SIL 3</td>
<td>&gt;=10^{-4} to &lt; 10^{-3}</td>
<td>10000 to 1000</td>
</tr>
<tr>
<td>SIL 2</td>
<td>&gt;=10^{-3} to &lt; 10^{-2}</td>
<td>1000 to 100</td>
</tr>
<tr>
<td>SIL 1</td>
<td>&gt;=10^{-2} to &lt; 10^{-1}</td>
<td>100 to 10</td>
</tr>
</tbody>
</table>

When considering fail-safe control modules, emphasis is not only placed on the system being able to switch off „safely“, but a major feature is the safe operation in case of an error. And this safe operation plays an important role when looking at structures, such as tunnels, where the safety of a great amount of people is mandatory.

**4. Risk Assessment Process**

In order to perform risk assessment, a risk analysis must be carried out first (determination of limits of the machine / system and identification of hazards). Then in the next step, the Safety Integrity Level can be defined via risk assessment. [10]

**4.1. Risk Assessment**

In order to elicit the required level of functional safety in a plant, it is vital to act according to the norms IEC 61511 or IEC 62061. Figure 4 shows a decision matrix executed based on the norm IEC 61511, which leads to the executed SIL level.

![Figure 4: Determination SIL regarding IEC 61511 [5]](image-url)
For an exemplary determination, following assumptions are made:

- Failure of a safety device may lead to the death of several or many people.
- The frequency and duration of stay in the danger zone is often to permanently.
- Risk aversion is possible under certain conditions.
- Probability of occurrence is very low.

Cc ➔ FB ➔ PA ➔ W1 ➔ SIL1 (Death of several people possible)
Cd ➔ FB ➔ PA ➔ W1 ➔ SIL2 (Death of many people possible)

The above mentioned assumptions are chosen to apply particularly for a tunnel. Consequently, consideration of the SIL Level arises as an additional safety criterion for a control system in the tunnel.

5. EXAMPLES

Examples for already running tunnel systems with highly available, fail-safe systems:

**France - Tunnel Croix Rousse**
 Highly available and fail-safe control system (SIL3) / in operation

**Germany - Tunnel München Mittlerer Ring Ost**
 Highly available and fail-safe control system (SIL3) / in operation

**Belgium - Liefkenshoektunnel**
 Highly available and fail-safe control system (SIL2) / currently commissioned

**United Kingdom - Dartford Road Tunnel and Bridge**
 Highly available and fail-safe control system (SIL2) / in operation

The provided examples show the determination of the SIL level for subsystems such as ventilation, lighting, control, etc. via a safety-related evaluation where the control hardware was designed accordingly.

6. CONCLUSION

First and foremost, it is important to distinguish between availability and functional safety. Availability is, as shown in many directives, a major topic. Functional safety is, however, often not taken into account, but should find its way to tunnel automation due to its proliferation and state of technology.

Posing the question of how much safety lies within tunnel automation, one needs to answer that emphasis is put on availability, but the idea of safety controllers and functional safety has only, so far, prevailed in some countries.

7. REFERENCES


