The serious risk to life from asphyxiating or poisonous smoke in buildings has become well-known to the general public, particularly since the fire at Düsseldorf Airport (Germany) with 17 fatalities. The causes are rooted in a variety of human and technological details, and this does not make it any easier to assign liability. The situation can be summarised as follows: Smoke in buildings is a serious and life-threatening danger that must be countered with suitable technical and organisational actions.

The increasing direct and indirect influence of DIN EN 61508 on building automation is increasing the pressure on building automation suppliers, operators and safety officers to deal with the implementation of automated safety functions that comply with the state of the art. This is described for
In projects such as the "Berlin Olympic Stadium" and the "Pharmaceutical Plant" at Boehringer Ingelheim, Germany, the smoke and fire dampers are already controlled by HIMA safety technology.

The advantages are obvious. The high reliability is proven to increase system availability and thus operating safety. The high degree of integration that can be achieved allows interfaces between the systems to be minimised. The distribution of the controller intelligence increases availability in emergencies. The primary goal is to process all programmable sequences over all systems and check for plausibility. This significantly increases the degree of functional safety. The PLC technology allows on- and off-line simulations of the complex logic to verify functional sequences. This saves time and money during a function check and during commissioning on site.

The application of this competence and the available technology depends greatly on the sensitivity with which responsible authorities and persons deal with this subject. For the first time safety can be quantified independently on the basis of the basic standard DIN (IEC) EN 61508. This establishes a unified procedure for an objective assessment of safety. The technology is available and now the responsible parties can act!

Typical systems integrated in the smoke protection design are
Smoke detection, alarming, smoke damping, pressurised ventilation, lift control, Venetian blinds/smoke curtains, dynamic evacuation route controls, dynamic extinguishing.....

Typical applications are
High-rise buildings, industrial and commercial buildings, traffic tunnels, underground rail systems, airports, special constructions .......

Figure 5 shows the HiMatrix network and the application of distributed controller and I/O modules with additional significant advantages arising from the HIMA technology. Virtually any desired network architectures are possible based on standard Ethernet in accordance with IEEE 802.3. The use of standard Ethernet technology for the secure HIMA protocol enables data transmission over copper, fibre optics or radio. The HIMA safe ethernet safety protocol links all HiMatrix modules on a safe controller level.

Although many involved in building automation find this subject new and strange, it is not really new. HIMA has been developing safety technologies that are implemented in thousands of applications all over the world for over 30 years. HIMA as a manufacturer and e.g. TÜV as approval authority offer a variety of experience and competence.

Figure 5: HiMatrix safety network

Advantages of HiMatrix
Reliability confirmed by SIL3 certificate
Availability by:
1) decentralised network architecture
2) high failure safety of the entire controller network
Design flexibility by controller and I/O modules distributed as desired
Open integration in BAS / DCS (Ethernet, Modbus/TCP, Profibus, OPC)
Reduction of bus systems and interfaces
High degree of integration of the systems involved in the safety design
Integrated control function of dynamic processes
SIL3 ring bus
ATEX certification
EN 54-2 certification and NFPA 72 conformity as fire alarm panel
Remote maintenance by telephone, leased line, ISDN
Data transmission – secure and independent of medium (copper, fibre optic, wireless)
HIMA references
- Olympic Stadium, Berlin
- Pharma plant
Boehringer Ingelheim
While the device manufacturer is responsible for all safety aspects of the device from the design phase to decommissioning, the operator is responsible for all technical system and organisational aspects of safety through all phases of the life of the system (design to general operation and maintenance).

This supports the basic idea that overall safety is "generated" at a central point and gaps in safety caused by the uncoordinated interplay of different safety systems are prevented. Interdisciplinary action is required to implement the resulting system safety.

This not only affects the system manufacturer but also others responsible for safety such as consultants, engineering associations, building inspection authorities, insurers and of course the operator.

**Functional Safety**

From a technical point of view the automated protection function must operate reliably when required, i.e. the probability of hazardous failure of the safety system must be reduced to a tolerable minimum. Therefore, the task is to allow as few undetected hazardous faults as possible on the controller level - see fault type classification in Figure 3. If detected hazardous faults occur, the system is reset to the safe status.

Safety controllers are characterised by the high quality of their components (hardware) and intelligent methods for failure analysis (software) in the overall system. This is the only way to reach the high reliability and the resulting low probability of failure of the controller. All design and development stages are monitored by an independent consultant and a TÜV certificate is issued to confirm that all the requirements of the standard have been met. This certifies the functional safety of the product. This is "Part of the overall-safety that depends on the correct function of the safety-relevant, software-supported system".

Advantages for the user

The resulting safety requirement can be implemented by the application of decentralised SIL-PLC technology, which enables a high degree of integration of the system into the overall safety design. A seamless safety controller level is established, which receives any safety-relevant signals anywhere in the building, processes them logically as required and forwards them to the relevant actuators or systems at any other location within less than a second. This has not been possible in the past.

The economic advantages of the new solutions are already known and accepted, and the technology is coming into more common use.

---

### Non-availability of the safety function

<table>
<thead>
<tr>
<th>SAFETY INTEGRITY LEVEL (SIL)</th>
<th>LOW DEMAND MODE OF OPERATION (Probability of failure to perform its designed function on demand)</th>
<th>Statistical time per year in which the safety system (undetected) is not available</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$10^{-5}$ up to $10^{-4}$</td>
<td>52.6 min bis 5.3 min</td>
</tr>
<tr>
<td>3</td>
<td>$10^{-4}$ up to $10^{-2}$</td>
<td>8.76 h bis 52.6 min</td>
</tr>
<tr>
<td>2</td>
<td>$10^{-3}$ up to $10^{-2}$</td>
<td>87.6 h bis 87.6 h</td>
</tr>
<tr>
<td>1</td>
<td>$10^{-2}$ up to $10^{-1}$</td>
<td>876.6 h bis 87.6 h</td>
</tr>
</tbody>
</table>

Figure 3: What failures do exist? ($\lambda = failure probability$)

This means that effective action for prevention of faults, detection of faults and management of faults has been confirmed.

Analysis of the fault probability and the resulting quantification of safety that was possible for the first time allows different levels of safety and risk to be defined - SIL1 to SIL4. (SIL = Safety Integrity Level)

A probability interval for a hazardous failure is assigned to an SIL. The statistical failure probability from SIL1 to SIL4 systems is illustrated in Figure 4.

The risk assessment and the resulting determination of the required SIL is the result of a hazard assessment conducted by an interdisciplinary team.

**Figure 4**: Interconnection of SIL and hazardous probability of failure
software-supported systems by the new DIN EN 61508 standard or VDE 0803 (Germany). It provides a framework for the application of PLC technology in safety-relevant systems – here: smoke protection in buildings. Smoke protection systems with complex dependencies can now be integrated into a decentralised PLC network. This eliminates a number of unnecessary interface problems (see concept figure 1).

**DIN (IEC) EN 61508 and national legislation (in Germany)**

IEC 61508 is an international standard, which describes the relevant safety requirements for electrical, electronic and programmable electronic systems (E/E/PES). It is the first internationally harmonised basic set of regulations that is applicable for all E/E/PES in any application. The EN 61508 series of standards on functional safety, which has been accepted by CENELEC, the European standards organisation, as IEC 61508 was ratified as long ago as July 2001. It was implemented as a German standard under DIN EN 61508 (VDE 0803) on 1 August 2002 and defines the state of the art for E/E/PES, which is applied for safety functions in safety-critical applications. Prior standards such as DIN V VDE 0801 and DIN V 19250 do not conform to the new standard and will be withdrawn on 1 August 2004. Under this system DIN EN 61508 operates as a basic standard for the development of application-oriented standards or product standards. Drafts for application-specific safety standards are available for the process industries and the wide field of factory automation. They are referred to as application standards. Building automation is currently not in a position to apply such application standards, because safety-oriented technology in accordance with DIN EN 61508 or the prior standards has had little or no consideration. This has been possible because DIN V VDE 0801 and DIN V 19250 were always draft standards only and were therefore not binding. DIN EN 61508 is now available as a white paper, making it a valid basic standard.

Normative references to DIN EN 61508 in sector-specific standards such as EN 81 (lift), DIN VDE 0108 (power supply) and other national standards indicate the pressure that is being built up by the new standard. In addition, there are drafts of completely new regulations that include safety requirements in accordance with DIN EN 61508. An example is the VDMA standard publication 24100-1 "Automated fire protection and smoke damping systems - ABE" (German version available only).

The application of DIN EN 61508 receives further support from legislative requirements, which require implementation of technology in appropriate regulations in accordance with the state of the art. This includes transferring responsibility for safety in plants, processes and also buildings to the operator (German regulations governing safe working conditions). Under this system the implementation of system technology in accordance with the "new state of the art", i.e. in conformity with DIN EN 61508, gives the operator a relatively high degree of legal security.

The transfer of responsibility for safety to the operator also supports the general safety-life cycle philosophy of DIN EN 61508. (Figure 2)