Control and protective systems on industrial thermoprocessing installations

by **Klaus Kroner**

A control system for industrial thermoprocessing equipment must meet stringent requirements in terms of plant and operational safety, functionality, availability and cost-effectiveness. The electrical and electronic equipment for these installations must comply with a number of relevant EC Directives and Standards. This article explains the context. It also explains the requirements on the design of protective systems and describes the necessary steps of risk assessment. In addition, the determination of so-called "SIL/PL levels" for safety functions is described.

Owing to the new Machinery Directive 2006/42/EC having come into force on 29 December 2009, requirements as regards functional safety are imposed on thermoprocessing installations as well. International standards define requirements in relation to reliability of safety functions (Safety Integrity Levels SIL and Performance Levels PL) with the aim of minimizing the risk to persons, the environment, products and processes in the case of a malfunction. Manufacturers of thermoprocessing installations and, in particular, constructors of control systems must now deal with these topics.

The electrical and electronic equipment of a thermoprocessing installation consists of the higher-level process control system (**Fig. 1**) and the electrically actuated devices (sensors/actuators) which are arranged in distributed fashion on a thermoprocessing installation.

Fig. 2 schematically shows an industrial furnace for high temperature operation as an example of a thermoprocessing installation. The process control system is functionally linked to a large number of components which are arranged in the gas inlet section 1, the air inlet section 2, the burner control unit 3 and in the combustion chamber, the flue gas system and the power section (actuators as blower / drives) of the thermoprocessing installation. The required signal exchange between the control components involved and the field level is, in this case, classified into safety-related and non-safety-related signals.

The process control system itself consists on the one hand of the control system/operating level. This accommodates the operating equipment required for visualization and operation of the installation. Control sequences and control loops for the process are implemented and visualized (non-fail-safe part of the process control system).

Fig. 1: Process control system

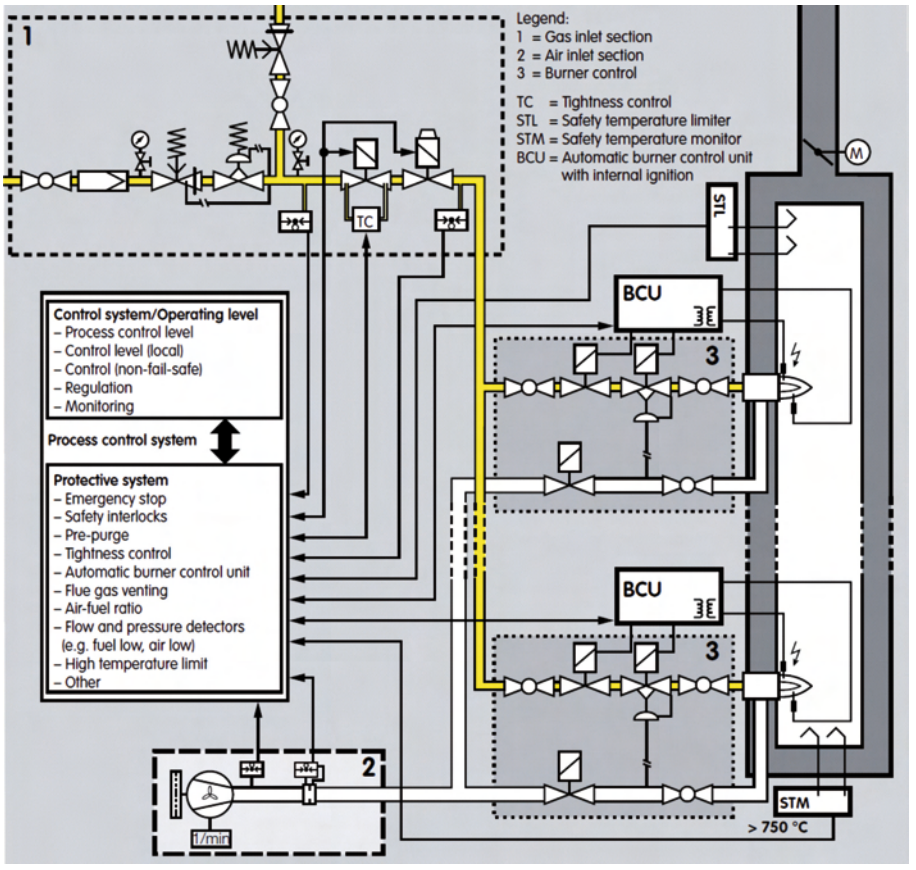

Fig. 2: High temperature industrial furnace

Moreover, the process control system comprises the so-called protective system which includes all facilities, devices and control units for safety functions whose main purpose is to protect persons, the installation and the environment.

"The protective system is a collection of equipment, units and safety related circuits whose main purpose is the protection of personnel, property and the environment. The protective system includes all the components required to carry out the safety function, such as sensors which monitor safety related parameters (e.g. flame monitoring), interruption device for the flow of fuel, ventilation of the body of the furnace and protection of the heated system (e.g. monitoring the temperature level). Typically a protective system consists of sensors, logic solving protective equipment and actuating elements. If this is achieved by multi-channel systems, then all channels and monitoring devices used for safety purposes are included within the protective system", (source: EN 746-2:2010).

DESIGN REQUIREMENTS ON THE PROCESS CONTROL SYSTEM

Stringent requirements as regards safety, availability and economy are made of the control system of a thermoprocessing installation. The control-engineering task consists of implementing the essential requirements made of plant and operational safety in accordance with the corresponding EC Directives and Standards in the design of circuit engineering, hardware and control programs (software), in addition to the functionality.

EC DIRECTIVES, HORIZONTAL APPLICATION

EC Directives must be applied horizontally, i.e. all the Directives applicable to a product represent the legal requirements and must be used in the design (**Fig. 3**). The requirements specified by the EC Directives are implemented in national law by corresponding acts. The essential requirements of the Directives must be allowed for and implemented by the machine manufacturer and also by the control system manufacturer.

However, the essential requirements stipulated in the EC Directives represent only minimum requirements on the electrical equipment of a thermoprocessing installation. What are crucial for specific implementation of all requirements in respect of the design of the electrical equipment of a thermoprocessing installation are the contractual agreements between the contracting parties, manufacturer and owner, of a thermoprocessing installation. Owner-specific requirements, extending beyond the essential requirements of the EC Directives, may, for example, be specified in Factory Standards, reference to which is then made in the contract.

The Machinery Directive 2006/42/EC stipulates essential health and safety requirements for designing and constructing machinery. In Germany, implementation in national law takes the form of the 9th Ordinance relating to the German Product Safety Act (ProdSG).

The Low Voltage Directive 2006/95/EC stipulates essential requirements in respect of the safety objectives for electrical equipment. Implementation in national law, in Germany, takes the form of the 1st Ordinance relating to the German Product Safety Act. Most of the safety objectives described here deal with compliance with the safety measures for protecting persons and installations in respect of the use of electrical equipment and dimensioning thereof.

The EMC Directive 2004/108/EC stipulates essential requirements in respect of faultless functioning of electrical/electronic equipment relating to electromagnetic fields. In Germany, implementation in national law takes the form of the German EMC Act (EMVG). In accordance with this, devices and systems should, themselves, not

emit interference wherever possible, but be as resistant as possible to interference pickup or line-borne interference.

The Gas Appliances Directive 2009/142/EC stipulates essential requirements made of appliances, safety, controlling and regulating devices as well as sub-assemblies. Implementation in national law, in Germany, takes the form of the 7th Ordinance relating to the German Product Safety Act. Appliances, safety, controlling and regulating devices as well as sub-assemblies for gas appliances must be designed, manufactured and used in such a way that failure thereof cannot result in hazardous situations.

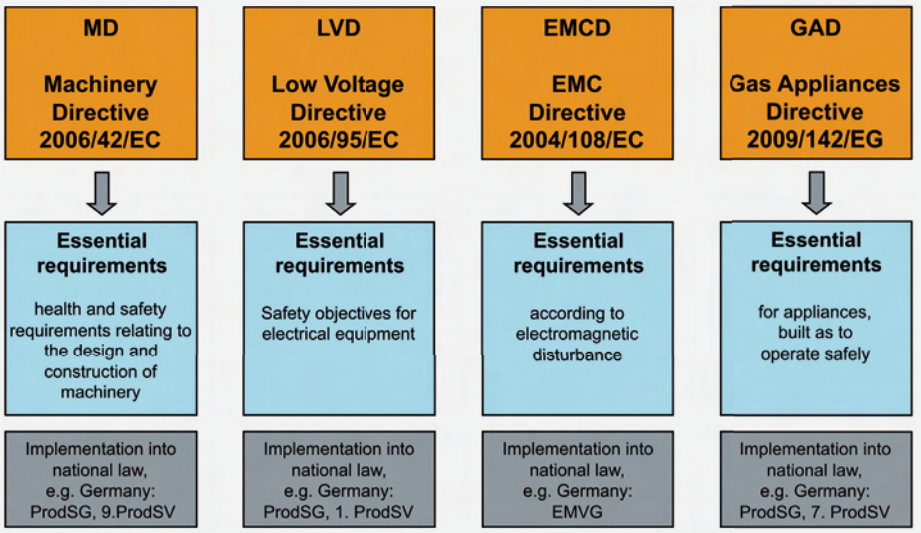

Fig. 3: EC Directives, legal requirements

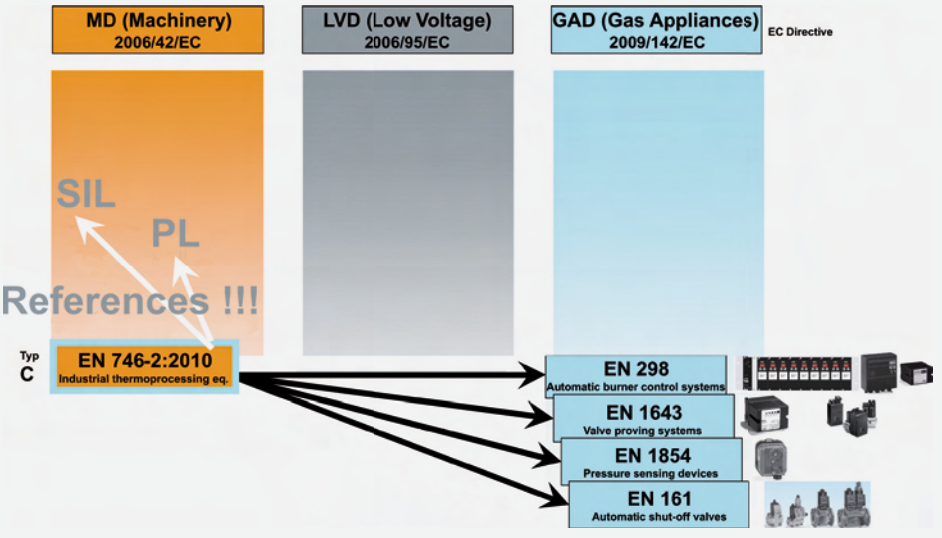

Fig. 4: Machine-safety product standards

REQUIREMENTS ON MANUFACTURERS

Manufacturers of thermoprocessing equipment (IThE) apply the Machinery Directive 2006/42/EC and must certify installation conformity with the Directive and, thus, the legal conformity (in accordance with the ProdSG) by issuing a Declaration of Conformity for the thermoprocessing installation.

Device manufacturers primarily apply the Gas Appliances Directive 2009/142/EC. The Low Voltage Directive 2006/95/EC and the EMC Directive 2004/108/EC must also be applied in the case of electrically operated devices.

Control system manufacturers apply the Low Voltage Directive 2006/95/EC and the EMC Directive 2004/108/EC. In addition, the control system must also comply with the relevant health and safety requirements of the Machinery Directive 2006/42/EC since, after all, it assumes the control tasks for precisely this machine. However, the control system, considered alone, is subject solely to the Low Voltage Directive 2006/95/EC and the EMC Directive 2004/108/EC.

EC DIRECTIVES, ESSENTIAL REQUIREMENTS

An excerpt (Section 1.2 "Control systems") of Annex 1 of the Machinery Directive 2006/42/EC (applicable since 29 January 2009) is shown here:

1.2. CONTROL SYSTEMS

1.2.1. Safety and reliability of control systems

Control systems must be designed and constructed in such a way as to prevent hazardous situations from arising. Above all, they must be designed and constructed in such a way that:

- they can withstand the intended operating stresses and external influences,
- a fault in the hardware or the software of the control system does not lead to hazardous situations,
- errors in the control system logic do not lead to hazardous situations,
- reasonably foreseeable human error during operation does not lead to hazardous situations. (Source: Machinery Directive 2006/42/EC)

This excerpt clearly shows that the safety objectives (essential requirements) which must be implemented by

the designer are described in the Directive. The designer of the control system then finds specific assistance for practically orientated implementation of these safety objectives in the relevant standards where design details are described.

European Standards, after publication in the Official Journal of the European Union, receive the status of "Harmonized Standard". Harmonized Standards must then be transposed unchanged into national standards. Harmonized Standards specify how the essential requirements of the EC Directives can be complied with in accordance with the current state of the art. Compliance of products with Harmonized Standards gives rise to the assumption of compliance with the essential requirements of the EU Directives.

Standards do not have the force of law. Application thereof is voluntary but, nevertheless, recommended. The manufacturer is free to opt whether he takes recourse to Harmonized Standards when manufacturing his products or complies with the stipulated, essential requirements of the EC Directives in another way.

NORMATIVE INTERRELATIONSHIPS, MACHINE-SAFETY PRODUCT STANDARDS

In order to illustrate important interrelationships, **Fig. 4** uses a form of representation which clearly shows the relationships between the Harmonized Standards among each other and to the related Directives.

The relevant EC Directives are shown horizontally and, beneath them, the corresponding Harmonized Standards are assigned in each case.

EN 746-2:2010 (Industrial thermoprocessing equipment – Part 2: Safety requirements for combustion and fuel handling systems) is a Harmonized Type C Standard further to the Machinery Directive.

"This part of EN 746 together with EN 746-1 specifies safety requirements for single and multiple burners that are part of Industrial Thermoprocessing Equipment. (In this standard referred to as IThE).

This document deals with significant hazards, hazardous situations and events relevant to combustion and fuel handling systems that are part of IThE, when used as intended and under the conditions foreseen by the manufacturer.

This European Standard covers fuel pipework downstream of and including the manual isolating valve; burner(s), burner system and ignition device; safety related control system (protective system).

This European Standard is not applicable to electricity cabling and power cabling upstream of the IThE control panel/protective system". (Source: EN 746-2:2010)

The Product Standards EN 298, EN 1643, EN 1854 and EN 161 are Harmonized Product Standards further to the Gas Appliances Directive. These Product Standards obtain the reference to the Machinery Directive under which they are not harmonized by cross-references in EN 746-2.

For instance, when using flame supervision devices and automatic burner control units, EN 746-2 makes reference to EN 298 which describes the technical-safety and design requirements made of these devices in great detail.

Automatic burner control units are developed and manufactured in accordance with the Product Standard EN 298 (Automatic gas burner control systems for gas burners and gas burning appliances with or without fans). Valve proving systems such as leak tightness devices are developed and designed in accordance with the Product Standard EN 1643 (Valve proving systems for automatic shut-off valves for gas burners and gas appliances). Pressure switches are developed and designed in accordance with the Product Standard EN 1854 (Pressure sensing devices for gas burners and gas burning appliances) and automatic shut-off valves are developed and designed in accordance with the Product Standard EN 161 (Automatic shut-off valves for gas burners and gas appliances).

Furthermore, reference is also made to standards for functional safety in which the requirements in respect of SIL or PL levels are described.

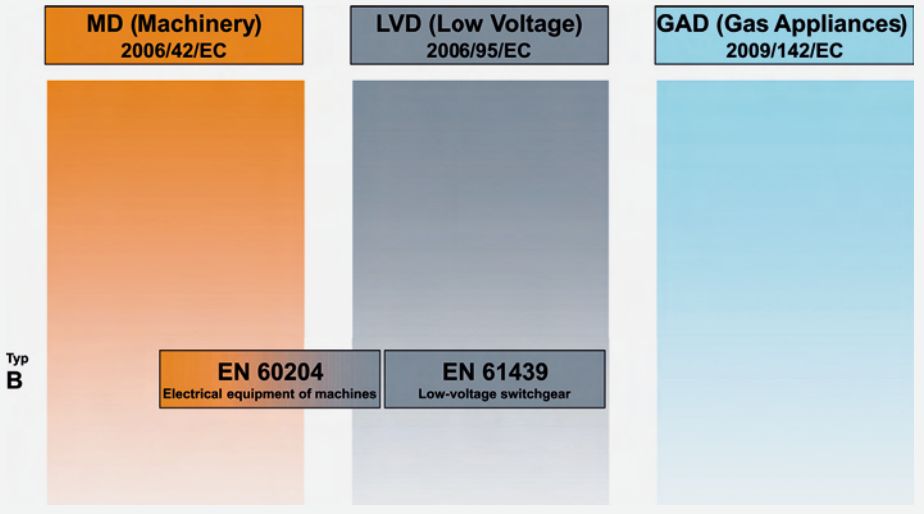

Fig. 5: Electrical safety standards

NORMATIVE INTERRELATIONSHIPS, ELECTRICAL SAFETY STANDARDS

Electrical safety is described in the Standards EN 60204 (Safety of machinery – Electrical equipment of machines), harmonized under the Machinery Directive and under the Low Voltage Directive, and EN 61439 (Low-voltage switchgear and controlgear assemblies), harmonized under the Low Voltage Directive (**Fig. 5**).

These Standards stipulate agreements and recommendations for the safety, operability and maintenance of electrical equipment and describe safety measures such as protection against electric shock, dimensioning and design of switchgear, lines and overcurrent devices, in addition to equipotential bonding, etc.

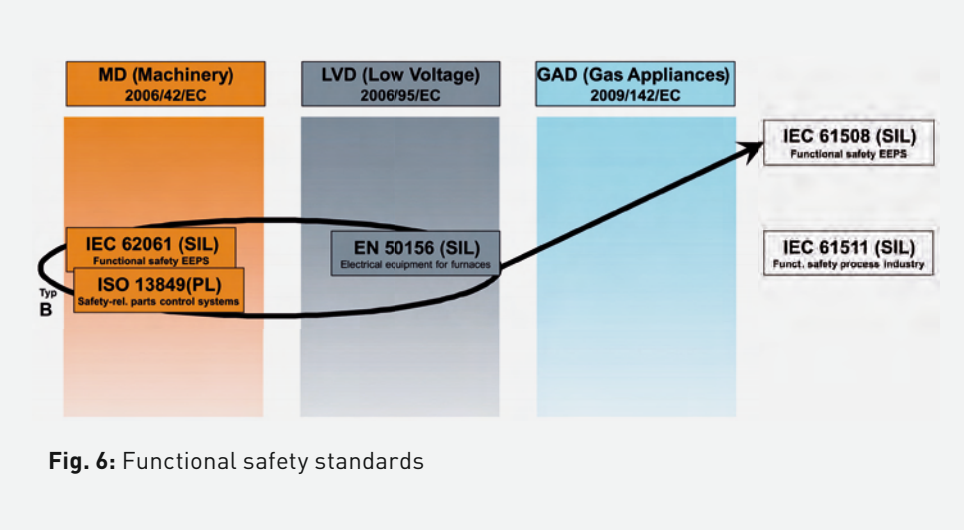

Fig. 6: Functional safety standards

The electrical equipment of thermoprocessing installations must comply with the requirements set out in EN 60204-1. Furthermore hazards which were identified in the risk assessment (required by the Machinery Directive during the design phase) must be considered.

NORMATIVE INTERRELATIONSHIPS, FUNCTIONAL-SAFETY STANDARDS

Standard IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems) defines requirements in respect of safety-related systems (**Fig. 6**). The scope of this Standard comprises the entire lifecycle of safety-related systems and covers the concept, planning, development, implementation and operation of the system through to decommissioning of an installation. IEC 61508 is a generic standard which is not restricted to a specific field of application. The following, industry-specific Sector Standards were derived by other standardization committees from this Standard:

- IEC 61511 – Functional safety - Safety instrumented systems for the process industry sector
- EN 50156 – Electrical equipment for furnaces and ancillary equipment
- IEC 62061 – Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
- ISO 13849 – Safety of machinery - Safety-related parts of control systems.

IEC 61508 and the Sector Standard IEC 61511 are applied to process-engineering systems in the chemical industry. Both of the IEC Standards are not harmonized under an EC Directive.

Now that the SIL assessment of safety functions has been used for some years in the chemical industry, this assessment has now been extended to cover machinery and plant installations in accordance with the Machinery Directive. Since this topic is still a relatively new one, particularly for manufacturers of thermoprocessing installations and for manufacturers of safety devices for thermoprocessing installations, the knowledge and experience required for this frequently still needs to be acquired in order to adapt new installations to the additional functional safety requirements.

Standards EN IEC 62061 and EN ISO 13849 are Harmonized Standards further to the Machinery Directive and are applied to machinery such as thermoprocessing installations. EN 50156 is a Harmonized Standard further to the Low Voltage Directive and is applied, for instance, to steam boiler installations.

All three Sector Standards deal with the requirements made of the functional safety of systems and describe how to ascertain and calculate the required SIL or PL levels. In turn, reference is made at various points in these Sector Standards to the generic IEC 61508.

Fail-safe PLCs, safety relays and also more recent automatic burner control units and protective system electronics comply with the requirements of IEC 61508 and IEC 62061 or ISO 13849. SIL certificates or PL certificates are available for these devices.

NORMATIVE INTERRELATIONSHIPS, DETERMINISTIC AND PROBABILISTIC APPROACH

The relevant Product Standards for safety devices such as EN 298 for automatic burner control systems or EN 161 for automatic shut-off valves were developed on the basis of the deterministic approach for assessment of faults and failures (**Fig. 7**). This means that, when developing a device, defined and reproducible dangerous failures are considered, which the aim is to avoid.

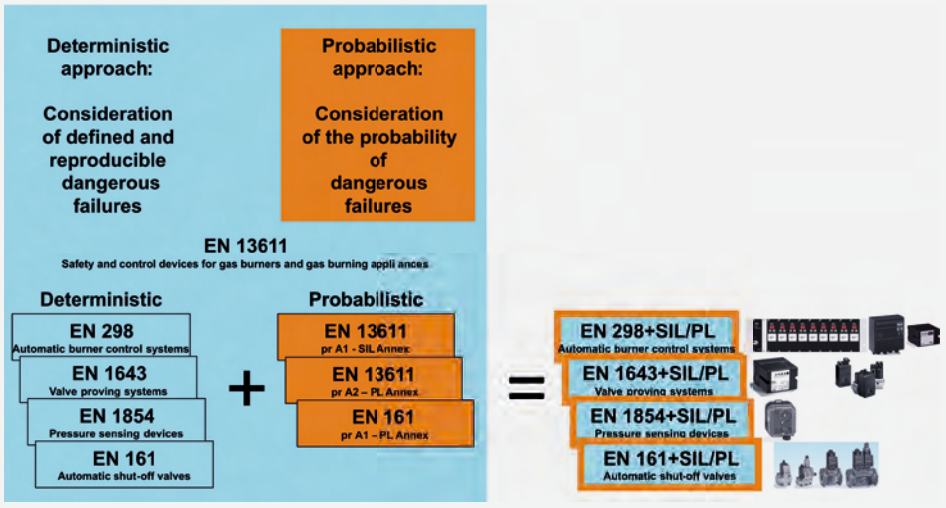

Fig. 7: Normative interrelationships, deterministic + probabilistic approach

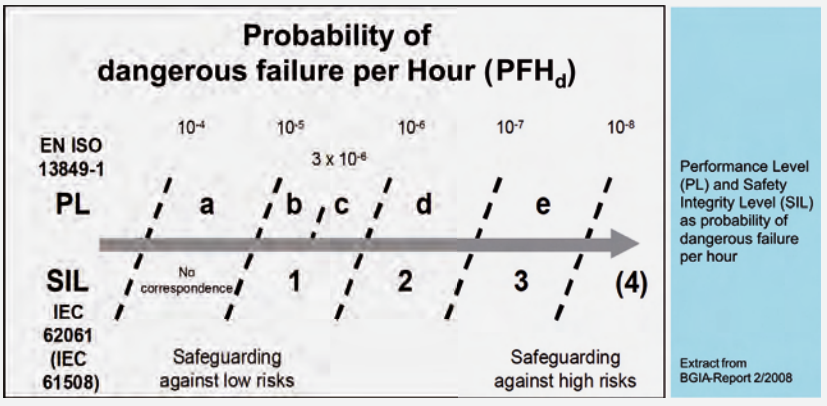

Fig. 8: Comparative assessment of PL/SIL, source: IFA (BGIA report 2/2008

The probabilistic approach merely represents another point of view for assessment of faults and failures. In this case, the statistical probability of dangerous failures is determined, and this must be proven by the safety device manufacturer during the device development by calculations and endurance tests in a complex process.

In the case of development of safety devices, the new standards for functional safety in accordance with the probabilistic approach are also applied, in addition to the deterministic Product Standards where essential requirements (essential functional requirements such as requirements as regards the leak tightness of devices and safety times, etc.) are described. By additional application of these new Standards, which are published as an SIL Annex or PL Annex further to existing Product Standards, the device manufacturers can supply type-tested safety devices also with an SIL/PL certificate in accordance with the Gas Appliances Directive.

The device manufacturers will only gradually be able to make available safety devices with additional SIL/PL certificates to manufacturers of thermoprocessing equipment since creation of SIL/PL certificates for safety devices is an extensive, time-consuming and very complex process which is normally and practically done in parallel with device development and since the required standards are partially still being processed by the standardization committees or these are currently only available as a Preliminary Standard (prEN).

SIL/PL CERTIFICATES FOR SAFETY DEVICES OF ELSTER GMBH

Automatic burner control unit:

An SIL 3/PL e certificate is available for Elster Kromschröder automatic burner control units of Series PFU 700. The certificate was elaborated in cooperation with TÜV Süd (German technical inspection authority for Southern Germany). The standards complied with, SIL and PL values and all relevant values are specified in the certificate.

Automatic shut-off valves:

An SIL/PL certificate (which can be used up to SIL 3/PL e) is available for Elster Kromschröder automatic shut-off valves of Series VAS 1. The SIL/PL level of this product depends on the quantity (1 or 2 valves) and the number of operating cycles of the relevant application. The actual SIL/PL value is determined from various characteristic values of the product and the number of operating cycles of the application. The calculation formula is printed in the certificate. The certificate was elaborated in cooperation with TÜV Rheinland (German technical inspection authority for the Rhineland). Calculation of the relevant values as a function of the number of operating cycles can be determined interactively in the Technical Information Bulletin (TI).

Pressure switches:

An SIL/PL certificate (which can be used up to SIL 3/PL e) is available for Elster Kromschröder pressure switches of Series DG. For this product as well, the SIL/PL level depends on the quantity (1 or 2 pressure switches) and on the number of operating cycles of the relevant application. The actual SIL/PL value is determined from various characteristic values of the product and the number of operating

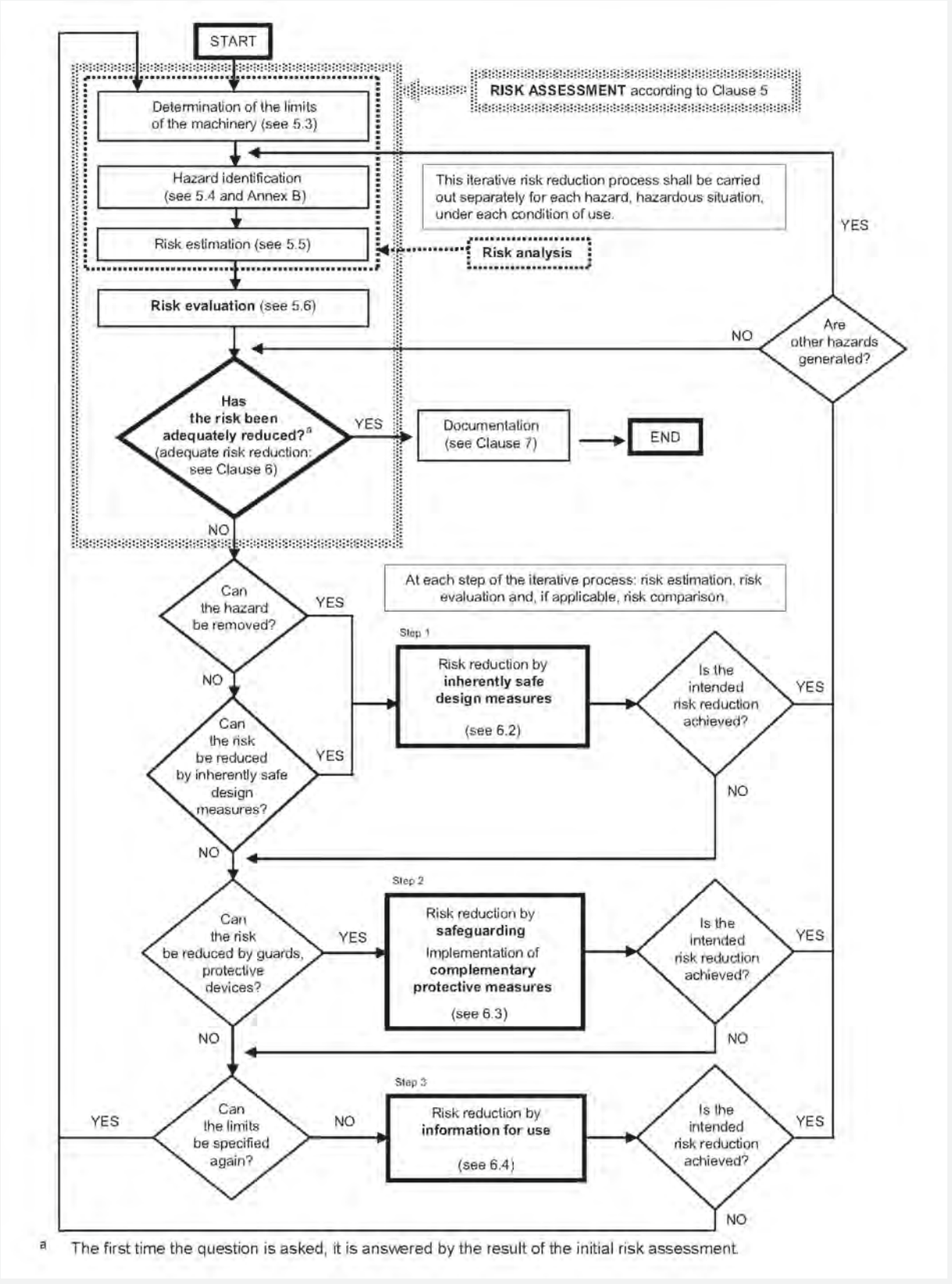

Fig. 9: Risk assessment/Risk reduction in accordance with EN ISO 12100, source: EN ISO 12100:2011-03

cycles of the application. The calculation formula is printed in the certificate. The certificate was elaborated in cooperation with TÜV Rheinland (German technical inspection authority for the Rhineland).

Calculation of the relevant values as a function of the number of operating cycles can be determined interactively in the Technical Information Bulletin (TI).

All certificates and further information on the safety devices of Elster GmbH are provided online in the "Dokuthek" **www.docuthek.com**. Further information and calculation tools are offered on the KST website at **www.system-technik.info**.

SAFETY INTEGRITY LEVELS (SIL LEVELS)

Safety Integrity Levels (SIL) are defined in the Safety Standards IEC 61508 and IEC 62061 (Functional safety of safety-related electrical, electronic and programmable electronic control systems). The probability of a dangerous failure of electrical devices/systems is considered.

We distinguish between three levels, SIL 1 – SIL 3 (4):

- SIL 1 = lowest level
- SIL 3 = highest level
- Level SIL 4 is not considered in the Harmonized Standards further to the Machinery Directive. See IEC 61508-1 for SIL 4.

PERFORMANCE LEVELS (PL)

Performance Levels (PL) are defined in the Safety Standard ISO 13849 (Safety-related parts of control systems). The probability of a dangerous failure of electrical, hydraulic, pneumatic and mechanical devices/systems is considered. We distinguish between five levels, PL a – PL e:

- PL a = lowest level
- PL e = highest level

COMPARISON BETWEEN PL AND SIL

Fig. 8 shows the Performance Level (PL) and Safety Integrity Level (SIL) as a probability of a dangerous failure per hour (PFHD). High risks are safeguarded with SIL 3 or PL e. In both cases, the probability of a dangerous failure per hour lies between 10^{-8} and 10^{-7}. Low risks are safeguarded, for instance, with SIL 1 or PL b/c. In both cases, the probability of a dangerous failure per hour lies between 10^{-6} and 10^{-5}. The higher the risk, the lower the failure probability of the safety devices used must be.

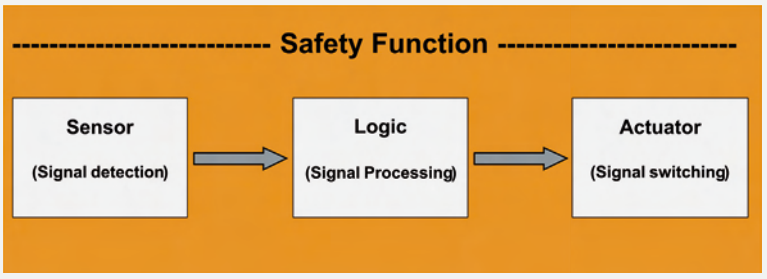

Fig. 10: PL/SIL level of a safety function

NORMATIVE INTERRELATIONSHIPS, HAZARD ANALYSIS AND RISK ASSESSMENT

In the sector of machine safety, DIN EN ISO 12100:2011-03 (Safety of machinery - General principles for design - Risk assessment and risk reduction) specifies an overall framework for systematic risk reduction. In this case, the risks are assessed in accordance with the principles shown here. Standard DIN EN ISO 12100 is a Harmonized Standard further to the Machinery Directive.

Within the framework of DIN EN ISO 12100, the Standard IEC 62061 stipulates safety requirements for electrical/electronic and programmable, electronic (E/E/PE) control systems. Moreover, it provides a methodology and requirements for integrating safety-related subsystems, designed in compliance with ISO 13849. This also allows consideration of the risks of hydraulic, pneumatic and mechanical devices/systems.

"The manufacturer of machinery or his authorised representative must ensure that a risk assessment is carried out in order to determine the health and safety requirements which apply to the machinery. The machinery must then be designed and constructed taking into account the results of the risk assessment", (Source: DIRECTIVE 2006/42/EC - ANNEX I).

The manufacturer of a machine carries out the risk assessment prescribed in the Machinery Directive and then constructs the machine allowing for the risk assessment and applying Harmonized Standards. The manufacturer elaborates a Declaration of Conformity for the safe machine constructed in this way. A CE mark is attached to this machine.

In accordance with the Work Equipment Directive, the German Labour Protection Act and the German Ordinance on Industrial Safety and Health, the owner of a machine analyzes the hazards at his employees' workplaces. He assumes the owner's responsibility by providing safe working equipment, training and instruction of the staff, and ensures safe workplaces and safe operation of the machine. Safe operation of a thermoprocessing installation also comprises regular maintenance of the installation.

Risk assessment in accordance with EN ISO 12100, iterative process

The individual steps in risk assessment are described in EN ISO 12100 (**Fig. 9**). The risk analysis includes a stipula-

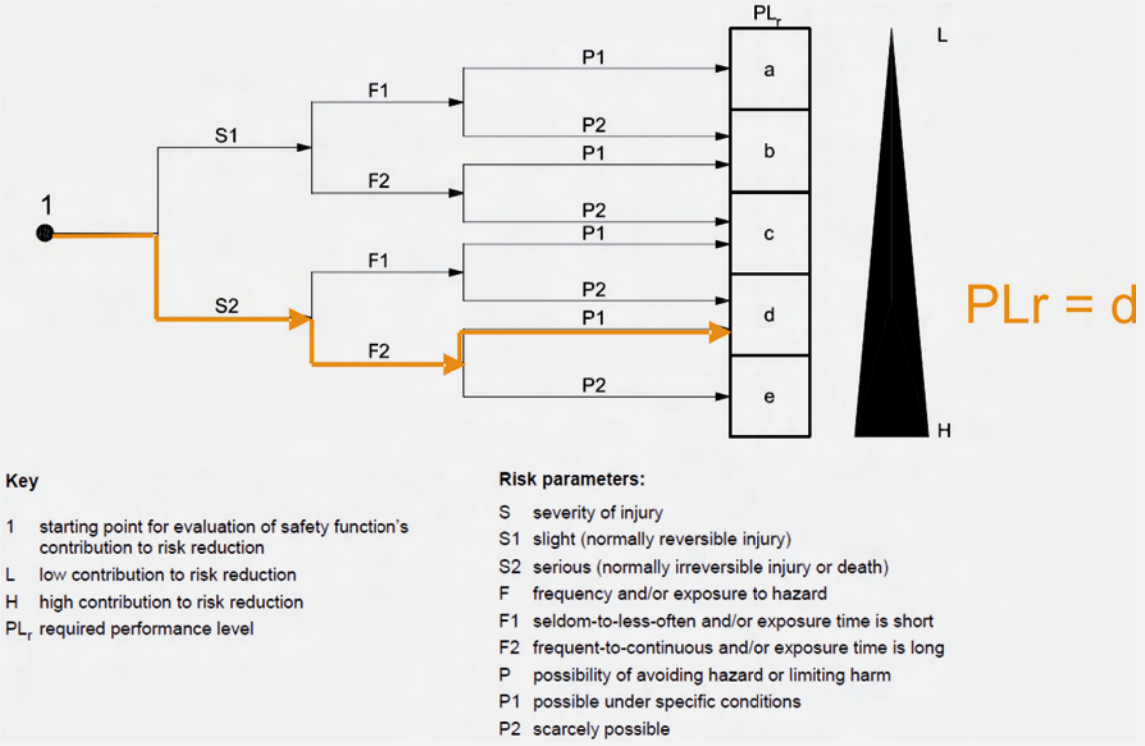

Fig. 11: Determination of the Performance Level, source: EN ISO 13849-1

tion of the limits of the machine, identification of the hazards and the risk estimation. The risk assessment also covers the risk evaluation. The risk assessment is either complete for the assessed safety function or a further risk reduction must be implemented on the basis of the assessment result as to whether the risk can be considered adequately low or has been reduced adequately.

The process is run through iteratively until the question "Risk adequately reduced?" can be answered with Yes. The process of risk assessment must be run through separately for every safety function. The risk assessment relates to all hazards which may occur on the machine.

Process of risk reduction from the point of view of the designer

The DIN EN ISO 12100 Standard defines the essential terminology and methodology which are applied for achieving machine safety. The stipulations in this Standard are intended for designers.

All safety measures applied for achieving this objective must be taken in the order designated the "3-step method".

- Step 1: inherently safe design measures: This phase is the only one in which hazards can be eliminated. This dispenses with the need for additional safety measures such as technical safety measures or complementary safety measures.
- Step 2: safeguarding (technical safety measures) and, possibly, complementary safety measures.
- Step 3: user information as regards the residual risk.

Application of these steps should commence with inherently safe design, and additional safety measures should be considered only if this does not allow further risk reduction to be achieved. User information as regards the residual risk should only be selected in 3rd place since the effectiveness of this measure basically depends on whether the information is also available to the owner or operator of the machine/thermoprocessing installation and whether the user information has been understood.

Process for risk reduction from the point of view of the owner

Safety measures which must then be taken by the user or owner relate to organizational measures, provision and application of additional safety devices, use of personal protective equipment, training and briefing, etc.

SIL/PL level of a safety function

The SIL/PL level is determined for a safety function (consisting of sensor + logic + actuator) (**Fig. 10**). Since thermoprocessing installations include different safety functions, it is not possible to determine or calculate a single SIL/PL level for an entire installation, but this must be determined separately for every safety function. The term

"safety function of a system" means the interconnection of "sensor" (acquisition), "control/logic" (processing) and "actuator" (switching).

Determining the required SIL/PL level

If the risk assessment of the thermoprocessing installation has shown that there is a need for an additional safety measure for minimizing the risk and that this should be designed in the form of an electrical safety device/safety function, it is required to initially determine the required SIL or PL level. This is where the use of so-called risk elements comes into play.

RISK = SEVERITY and PROBABILITY OF OCCURRENCE of that harm

The risk associated with a particular hazardous situation depends on the following elements:

a) the severity of harm;

b) the probability of occurrence of that harm, which is a function of

1) the exposure of person(s) to the hazard,

2) the occurrence of a hazardous event, and

3) the technical and human possibilities to avoid or limit the harm.

DETERMINING THE REQUIRED PERFORMANCE LEVEL IN ACCORDANCE WITH DIN EN ISO 13849-1

The required PL level is determined allowing for the severity of injury (S = S1 or S2), frequency and/or exposure to hazard (F = F1 or F2) and the possibility of avoiding hazard or limiting harm (P = P1 or P2). There is a required PL level of PL d for the specific hazard shown in **Fig. 11**, for which S has been determined as S2, F has been determined as F2 and P has been determined as P1.

DETERMINING THE REQUIRED SIL LEVEL IN ACCORDANCE WITH EN 62061

The required SIL level is determined allowing for the Severity of injuries, Consequences (Se = 4, 3, 2 or 1), Frequency and duration of exposure (Fr = 5, 4, 3 or 2), Probability of occurrence of hazardous event (Pr = 5, 4, 3, 2 or 1) and the Probability of avoiding or limiting harm (Av = 5, 3 or 1).

The Cl class is calculated according to the formula Cl = Fr + Pr + Av. The intersection of the severity of injuries Se and the Class Cl is the required SIL level.

The result is: Cl = Fr + Pr + Av = 4 + 5 + 5 = 14 for the specific hazard shown in **Fig. 12**, for which Se has been

Risk assessment and safety measures

Document No.:
Part of:

Product:
Issued by:
Date:

☐ Pre risk assessment
☐ Intermediate risk assessment
☐ Follow up risk assessment

Black area = Safety measures required
Grey area = Safety measures recommended

Consequences	Severity Se	Class Cl 3 - 4	5 - 7	8 - 10	11 - 13	14 - 15	Frequency and duration, Fr		Probability of hzd. event, Pr		Avoidance Av	
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hour	5	Very high	5		
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3	> 1 h - <=day	5	Likely	4		
Reversible, medical attention	2			OM	SIL 1	SIL 2	>1day - <= 2wks	4	Possible	3	Impossible	5
Reversible, first aid	1				OM	SIL 1	> 2wks - <= 1 yr	3	Rarely	2	Possible	3
							> 1 yr	2	Negligible	1	Likely	1

Ser. No.	Hzd. No.	Hazard	Se	Fr	Pr	Av	Cl	Safe

EXAMPLE: For a specific hazard with an Se assigned as 3, an Fr as 4, an Pr as 5 and an Av as 5 then:

Cl = Fr + Pr + Av = 4 + 5 + 5 = 14 SIL 3

Comments

Fig. 12: Determination of the SIL level, source: EN 62061

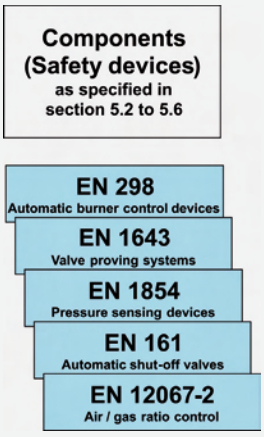

Fig. 13: Protective system, Version A, source: EN 746-2:2010

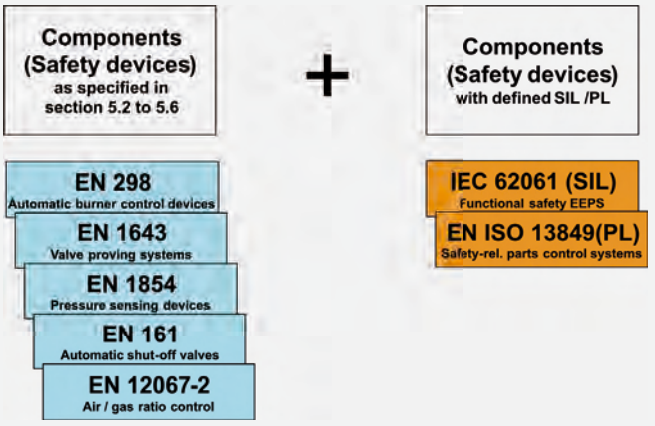

Fig.14: Protective system, Version B, source: EN 746-2:2010

determined as 3, Fr has been determined as 4, Pr has been determined as 5 and Av has been determined as 5. If the table is applied, this results in a required SIL level of SIL 3 at the point of intersection of Se = 3 and Cl = 14.

EN 746-2:2010 – ELECTRICAL EQUIPMENT AND PROTECTIVE SYSTEM

The general requirement of EN 746-2:2010 states that the electrical equipment of thermoprocessing installations must be designed in compliance with DIN EN 60204-1 (Electrical equipment of machines). One important new aspect in the current Standard is the requirements in respect of the functional safety of the protective system. The protective system must be designed either in accordance with Version A, B, C or D.

EN 746-2:2010 – REQUIREMENTS OF THE PROTECTIVE SYSTEM

The Standard describes a general classification of functions: Non-hazardous functions: No requirements as regards functional safety are specified.

Guarding functions not leading to immediate hazard in the case of failure: This demands the use of components in accordance with Product Standards (see EN 746-2, Sections 5.2 to 5.6) or components with SIL 2/PL d certification. For example, the Standard mentions guarding functions such as gas pressure and temperature.

Functions which will lead to immediate hazard in case of failure: This demands the use of components in accordance with Product Standards (see EN 746-2, Sections 5.2 to 5.6) or components with SIL 3/PL e certification. These requirements arise from the description of Versions A, B, C and D. For example, the Standard lists functions which will lead to immediate hazard in case of failure such as flame supervision and ratio control.

EN 746-2:2010 – PROTECTIVE SYSTEM, VERSION A

The protective system, Version A, is a hardwired protective system (non-programmable) and describes the use of safety devices in accordance with Product Standards (see Sections 5.2 to 5.6) (**Fig. 13**), i.e. the safety devices used here correspond to specific safety requirements, matched to the field of application and the functional requirements made of these devices, as demanded in the corresponding Product Standards for automatic burner control systems, valve proving systems, pressure sensing devices, automatic shut-off valves and gas/air ratio controls. It is not possible to apply EN 62061 or EN ISO 13849.

Example:

The "tightness check" safety function is structured in accordance with Version A with interconnection of a sensor (pressure switch to EN 1854) with logic (tightness control to EN 1643) and the actuators (gas valves to EN 161).

There have been extensive Product Standards, matched constantly to the state of the art, for firing technology for many decades now. The installations and products designed in accordance with these Standards feature a very high safety level. The example of the automatic burner control units, millions of which have been installed in the field, shows that damage attributable to lack of requirements in standards has never occurred.

Even without additional SIL/PL certification of safety

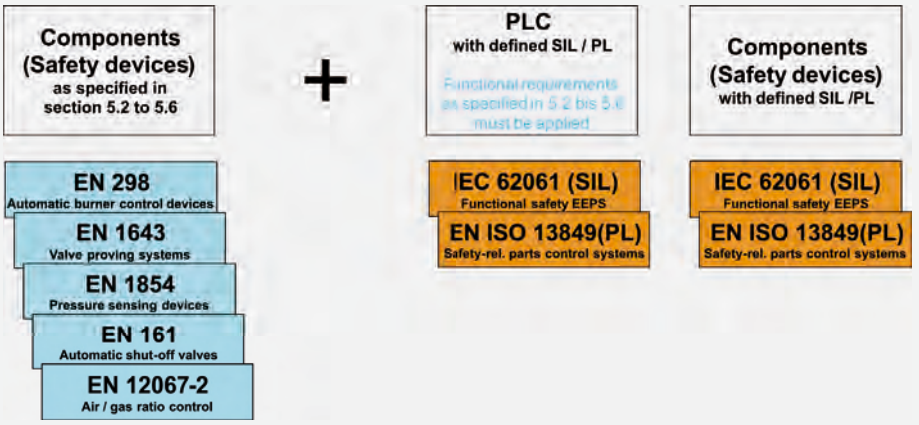

Fig. 15: Protective system, Version C, source: EN 746-2:2010

Fig. 16: Protective system, Version D, source: EN 746-2:2010

devices, the safety objectives and safety requirements for use of safety devices in accordance with Product Standards are guaranteed, and implementation of a protective system, Version A, must thus be viewed as one of several alternative options.

Standardization committees and study groups involving manufacturers and testing agencies are currently working intensively on sector-specific extensions to the aforesaid Product Standards in order to also include additional requirements from the standards for functional safety in the future. Additional SIL/PL certification of safety devices can be anticipated as the result of these efforts, and, currently, this is already being implemented by some of the manufactures of safety devices.

Additional SIL/PL certification of safety devices, however, will generally not be possible for older safety devices (exception: verification of suitability for proven operation), since the certification process is carried out as an accompanying process to development and is thus not possible retroactively.

EN 746-2:2010 – PROTECTIVE SYSTEM, VERSION B

The protective system, Version B, is a hardwired protective system (non-programmable) and describes the use of safety devices in accordance with Product Standards (see Sections 5.2 to 5.6) in combination with safety devices for which a corresponding SIL/PL level has been defined and verified (**Fig. 14**).

Components in accordance with Product Standards (see Sections 5.2 to 5.6) or components for which no relevant product standards are existing with at least SIL 2/PL d certification, must be used for "guarding functions not leading to immediate hazard in the case of failure" (e.g. gas pressure, temperature).

Components in accordance with Product Standards (see Sections 5.2 to 5.6) or components for which no relevant product standards are existing with SIL 3/PL e certification, must be used for "functions which will lead to immediate hazard in case of failure" (e.g. flame control).

Example:

The "high temperature limit monitoring" safety function, in accordance with Version B, is structured by interconnection of a sensor (safety temperature limiter with SIL/PL certification) with logic (automatic burner control unit to EN 298) and the actuators (gas valves to EN 161).

EN 746-2:2010 – PROTECTIVE SYSTEM, VERSION C

The protective system, Version C, is a PLC-based protective system (programmable) and describes the use of safety devices in accordance with Product Standards (see Sections 5.2 to 5.6) in combination with safety devices for which a corresponding SIL/PL level has been defined and verified and/or in combination with a PLC for which a corresponding SIL/PL level has been defined and verified (**Fig. 15**).

Components in accordance with Product Standards (see Sections 5.2 to 5.6) or components for which no relevant product standards are existing with at least SIL 2/PL d certification, must be used for "guarding functions not leading to immediate hazard in the case of failure" (e.g. gas pressure, temperature).

Components in accordance with Product Standards (see Sections 5.2 to 5.6) or components for which no relevant product standards are existing with SIL 3/PL e certification, must be used for "functions which will lead to immediate hazard in case of failure" (e.g. flame control).

The hardware and software of the PLC must meet the requirements of EN IEC 62061 or EN ISO 13849 and also allow for the functional requirements (e.g. total closing time), as specified in Sections 5.2 to 5.6.

Example:
The "gas max. pressure monitoring safety interlock" safety function, in accordance with Version C, is structured by interconnection of a sensor (pressure switch to EN 1854) with logic (safety PLC with SIL/PL certification) and the actuators (gas valves to EN 161).

EN 746-2:2010 – PROTECTIVE SYSTEM, VERSION D

The protective system, Version D, is a PLC-based protective system (programmable) and describes the use of safety devices for which a corresponding SIL/PL level has been defined and verified in combination with a PLC for which a corresponding SIL/PL level has been defined and verified (**Fig. 16**). All components should feature SIL 3/PL e certification in accordance with the Standard.

The hardware and software of the PLC must comply with the requirements of EN IEC 62061 or EN ISO 13849 and must also allow for the functional requirements (e.g. total closing time) as specified in Sections 5.2 to 5.6.

Example:
The "gas max. pressure monitoring safety interlock" safety function, in accordance with Version D, is structured by interconnection of a sensor (pressure switch to EN 1854 with SIL/PL certification) with logic (safety PLC or safety electronics with SIL/PL certification) and the actuators (gas valves to EN 161 with SIL/PL certification).

Note:
The requirement solely for SIL 3/PL e results in this case in a contradiction with the other Versions of the protective system in the Standard. What would appear practicable here is a distinction between SIL 2/PL d and SIL 3/PL e, as described in Versions B and C.

V MODEL FOR SOFTWARE DEVELOPMENT FOR SAFETY PLC

The procedure in accordance with the V model, for instance, is recommended for software development for safety PLCs and programmable safety devices.

"All lifecycle activities of safety-related embedded or application software shall primarily consider the avoidance of faults introduced during the software lifecycle. The main objective of the requirements is to have readable, understandable, testable and maintainable software.

The design activities comprise safety-related software specification, system design, module design and coding (the PLC program). The checking and testing activities

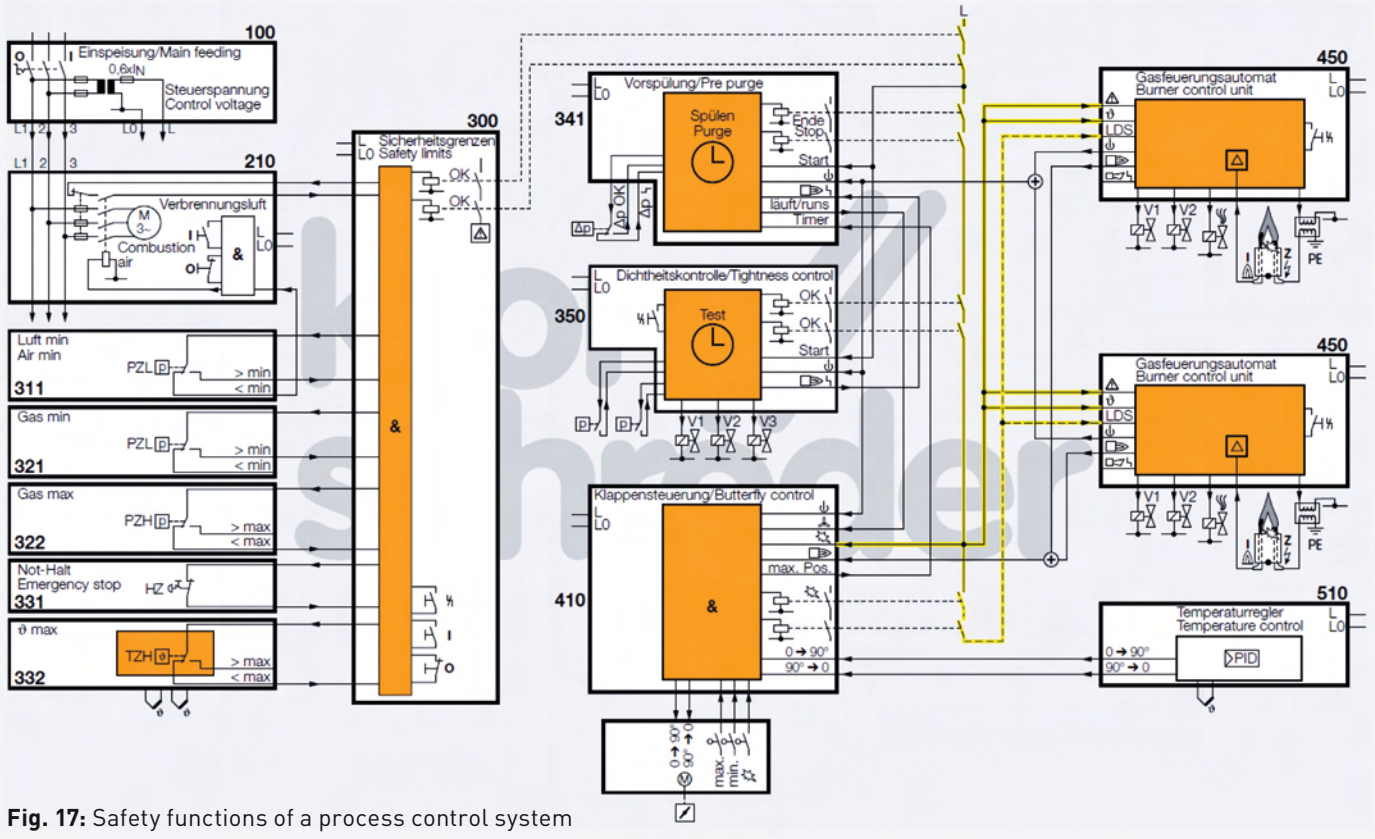

Fig. 17: Safety functions of a process control system

comprise the module testing, the integration testing and validation of the software".

Safe programming is very important so that the combination of SIL/PL-certified PLC hardware and the software of the safety PLC forms a safe unit. Software errors may lead directly to a safety risk. Corresponding measures must be taken in order to avoid software errors. Frequently, corresponding software modules are offered by the control system manufacturers. Specifically, Part 3 of IEC 61508 deals with writing software.

SAFETY FUNCTIONS OF A PROCESS CONTROL SYSTEM

Fig. 17 shows the fundamental safety functions of the protective system of the process control system of a thermoprocessing installation. Electronic safety devices are coloured orange. The supply voltage is supplied to the control system via the power supply unit (100). Start-up of the combustion air fan control system (210) includes the contact switchover check of the Air min. pressure switch (311).

The control block for monitoring the safety limits (300) assumes the safety-related monitoring of the safety limits Air min. (311), Gas min. (321), Gas max. (322), Emergency stop (331) and the monitoring of the safety temperature limiter (332).

Once the system has started and all safety limits (300) are present, pre-purging (341) of the thermoprocessing equipment begins and the tightness control (350) checks the valves. Once pre-purge (341) has been completed and the OK signal has been issued by the tightness control (350), the safety interlocks (shown in yellow) are set and the burners are started in the ignition position. Once the presence of the flame has been signalled to the automatic burner control units (450), the burners start. The temperature controller (510) takes over the temperature control of the heating equipment. The requirements as regards the required SIL/PL levels for the safety functions shown in Fig. 17 are listed in **Table 1**.

SIL/PL LEVELS REQUIRED FOR SAFETY FUNCTIONS

The safety functions listed in Table 1 are initially considered as regards their operating mode. In general, a distinction is made between so-called low demand mode (mode of operation in which the frequency of demands is no greater than one per year) and so-called high demand mode (mode of operation in which the frequency of demands is greater than one per year). In practice, low demand mode is not important on machines/thermoprocessing installations since, on the one hand, only a few safety functions could be classified as such anyway and, on the other, EN 62061 considers low demand mode to be irrelevant for application on machinery.

NOTE from EN 62061 – 3.2.26:

Equipment that is only designed in accordance with requirements for the low demand mode of operation described in IEC 61508-1 and IEC 61508-2 can be unsuitable for use as part of a SRECS in this standard. Low demand mode of operation is not considered to be relevant for SRECS applications at machinery.

Table 1: SIL/PL levels required for safety functions

		EN 746-2	EN 746-2	IEC 62061 (determined)	ISO 13849 (determined)
Safety function:	**Operating mode:**	**SIL:**	**PL:**	**SIL:**	**PL:**
Gas max. pressure monitoring	High / Low demand	2	d	2	d
Gas min. pressure monitoring	High / Low demand	2	d	2	d
Air min. pressure monitoring	High demand			2	d
Prepurge	High demand			2 (3)	d (e)
Tightness control / valve proving system	High demand			2 (3)	d (e)
Flame monitoring / burner control unit	High demand	3	e	3	e
Ignition Position monitoring (Single/Multipleburner)	High demand			2 / 1	d / c
Air / Gas - ratio monitoring	High demand	3	e	3	e
High temperature limit monitoring	High demand	3	e	3	e
Emergency stop / Emergency shut down	High / Low emand			2 / 3	d / e

As described in EN 62061, only the high demand mode is considered on machines such as thermoprocessing installations for the components of the protective system.

Required SIL/PL levels:
First of all, the SIL/PL levels required by EN 746-2 are plotted in Table 1. In addition, SIL/PL levels which were determined in discussions with manufacturers of thermoprocessing installations in accordance with the risk assessment from IEC 62061 and ISO 13849 are listed. The values given by way of example in Table 1 refer to typical thermoprocessing installations. The required SIL/PL levels may vary dependent on the risk assessment.

The following can be stated:
The requirements for monitoring the gas and air pressure mainly coincide with the requirement of SIL 2/PL d set out in EN 746-2.

EN 746-2 does not make any direct statements as regards the pre-purge and tightness check safety functions. Determining the values of SIL 2/PL d is based on the assessment that this safety function in general is always implemented together with other safety functions (e.g. use of two automatic shut-off valves to EN 161 or pre-purge and tightness check), i.e. a failure generally does not lead to an immediate hazard. SIL 3/PL e may be required in individual cases, depending on the risk assessment.

The SIL 3/PL e requirement for the flame control/automatic burner control unit safety function again coincides with the requirement set out in EN 746-2. Here, it is clear that, if the flame is not present on the burner, uncombusted gas flows into the combustion chamber which leads to an immediate hazard.

The risk assessment for monitoring ignition position resulted in SIL 2/PL d for individual burners and SIL 1/PL c for multiple burner systems since the risk drops greatly in the case of a multiple burner system (e.g. ignition of one of many burners).

Assessment of air/gas ratio monitoring was extremely difficult. Apart from the fact that the requirement of EN 746-2 for SIL 3/PL e and the implementation of this usually encountered on thermoprocessing installations frequently differ greatly from one another, it is hardly possible currently to implement SIL 3/PL e technically. Although differential pressure transducers for flow metering via an orifice are available in general as single-channel versions with SIL 2/PL d or two-channel versions with SIL 3/PL e, the corresponding certificates frequently feature only a PFD value for low demand mode in place of a PFHD value for high demand mode. The fact that, in accordance with EN 62061 (see above), low demand mode is considered irrelevant for machinery and, thus, for thermoprocessing installations and, consequently, devices for high demand mode are to be used, aggravates the problems even further. Ultimately, it can be stated that, in this case, manufacturers of devices and manufacturers of thermoprocessing installations must still develop solutions jointly which lead to the required, high technical-safety level on the one hand and which are affordable from an economic aspect on the other hand.

High temperature limit monitoring, which is used on thermoprocessing installations to switch from flame control to temperature monitoring as a function of the process temperature, must clearly be assigned to SIL 3/PL e since, in this case, the same requirements as with the flame control safety function apply. Here, in turn, there is correspondence with EN 746-2.

The emergency stop/emergency shut down safety function is conventionally classified in SIL 2/PL d or SIL 3/PL e. Occasionally, SIL 1/PL c may also be adequate as a function of the relevant system conditions. The required SIL/PL levels for safety functions of the protective system may differ in individual cases, but a risk assessment must be conducted on a general basis as described.

CONCLUSION

Table 1 shows that, for most safety functions of the protective system of a thermoprocessing installation, the requirements demanded by the standards on functional safety can generally be determined and implemented. Admittedly, there are still difficulties in this case here and there but, basically, the industry is on the right track.

Device manufacturers and the IFA (BGIA) offer corresponding tools for calculating the SIL/PL levels. Alternatively, however, calculation may be done in accordance with the description in the Standard IEC 62061 or ISO 13849.

It can be anticipated that more and more devices with SIL/PL certification will be offered by the device manufacturers and that the new requirements will gradually be included in the daily design work by manufacturers of thermoprocessing installations.

Not least, Versions A – D of the protective system in accordance with EN 746-2, which can be used as an alternative, are helpful.

SUMMARY OF RELEVANT EU DIRECTIVES AND STANDARDS

Machinery Directive 2006/42/EC
DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)

Low Voltage Directive 2006/95/EC
DIRECTIVE 2006/95/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 12 December 2006 on the harmonisation of the laws of Member States relating to electrical equipment designed for use within certain voltage limits (codified version)

EMC Directive 2004/108/EC
DIRECTIVE 2004/108/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 15 December 2004 on the approximation of the laws of the Member States relating to electromagnetic compatibility and repealing Directive 89/336/EEC

Gas Appliance Directive 2009/142/EC
DIRECTIVE 2009/142/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 30 November 2009 relating to appliances burning gaseous fuels (codified version)

SUMMARY OF RELEVANT EU DIRECTIVES AND STANDARDS - ProdSG:
Poduct-Safety Act - ProdSG
Gesetz über die Bereitstellung von Produkten auf dem Markt (Produktsicherheitsgesetz – ProdSG)
Artikel 1 des Gesetz über die Neuordnung des Geräte- und Produktsicherheitsrechts vom 8. November 2011

ISO 12100:2010-11
Safety of machinery - General principles for design - Risk assessment and risk reduction
First edition 2010-11-01

IEC 61508-1:2010
Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements; Edition 2.0 2010-04

IEC 61508-2:2010
Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems; Edition 2.0 2010-04

IEC 61508-3:2010
Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements; Edition 2.0 2010-04

IEC 61508-4:2010
Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations; Edition 2.0 2010-04

IEC 61508-5:2010
Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels; 01.04.2010

IEC 61508-6:2010
Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3; 01.04.2010

IEC 61508-7:2010
Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures; 01.04.2010

IEC 60204-1: 2008
Safety of machinery - Electrical equipment of machines – Part 1: General Requirements; Amendment 1; 01.11.2008

IEC 61511-1:2003
Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements; 01.12.2003 + IEC 61511-1 Corrigendum 01.11.2004

EN 50156-1:2004
Electrical equipment for furnaces and ancillary equipment - Part 1: Requirements for application design and installation; 01.10.2004

IEC 62061:2005
Safety of machinery - Functional safety of safety-related electrical, electronicand programmable electronic control systems; 01.01.2005

EN ISO 13849-1:2008
Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2006); 01.06.2008

EN ISO 13849-2:2008
Safety of machinery - Safety-related parts of control systems - Part 2: Validation (ISO 13849-2:2003); 01.06.2008

EN 61439-1:2009
Low-voltage switchgear and controlgear assemblies - Part 1: General rules (IEC 61439-1:2009, modified); 01.11.2009
EN 61439-2:2009

Low-voltage switchgear and controlgear assemblies - Part 2: Power switchgear and controlgear assemblies (IEC 61439-2:2009); 01.11.2009

EN 746-1:2010
Industrial thermoprocessing equipment - Part 1: Common safety requirements for industrial thermoprocessing equipment; German version EN 746-1:1997+A1:2009

EN 746-2:2010
Industrial thermoprocessing equipment - Part 2: Safety requirements for combustion and fuel handling systems; German version EN 746-2:2010

EN 746-3:2010
Industrial thermoprocessing equipment - Part 3: Safety requirements for the generation and use of atmosphere gases; German version EN 746-3:1997+A1:2009

EN 746-4:2000
Industrial thermoprocessing equipment - Part 4: Particular safety requirements for hot dip galvanising thermoprocessing equipment; German version EN 746-4:1999

DIN EN 746-5:2001
Industrial thermoprocessing equipment - Part 5: Particular safety requirements for salt bath thermoprocessing equipment; German version EN 746-5:2000

EN 746-8:2001
Industrial thermoprocessing equipment - Part 8: Particular safety requirements for quenching equipment; German version EN 746-8:2000

EN 13611:2011
Safety and control devices for gas burners and gas burning appliances - General requirements; German version EN 13611:2007+A2:2011

EN 298:2004
Automatic gas burner control systems for gas burners and gas burning appliances with or without fans; German version EN 298:2003

EN 1643:2001
Valve proving systems for automatic shut-off valves for gas burners and gas appliances; German version EN 1643:2000

EN 1854:2010
Pressure sensing devices for gas burners and gas burning appliances; German version EN 1854:2010

EN 161:2011
Automatic shut-off valves for gas burners and gas appliances; German version EN 161:2011

EN 12067-2:2004
Gas/air ratio controls for gas burners and gas burning appliances - Part 2: Electronic types; German version EN 12067-2:2004

BGIA – Report 2/2008e
Functional safety of machine controls
- Application of EN ISO 13849 -

AUTHOR

Klaus Kroner
Elster GmbH
Osnabrück/Lotte, Germany
Tel.: +49 (0)541/ 1214-360
klaus.kroner@elster.com