

Risk: unexpected start-up

Yesterday at a recycling plant in Einbeck:

Fatal industrial accident

(Ms). A 43 year-old worker at a recycling plant in Einbeck, Lower Saxony, was killed yesterday (Saturday). According to the police, the man had been cleaning a shredder when a 51 year-old plant operator started up the machine in the usual way, unaware that maintenance work was being carried out. The fitter was then caught up in a worm thread, sustaining fatal injuries.

One may not wish to imagine the details of the events that took place in this accident which was recently reported in a Sunday paper. However again and again we hear about this kind of accident and others like it, that take place due to unexpected or unseen starting up of difficult to see machines and plant (even if, thank God, these do not always end in death, even less severe accidents affect the course of human lives). Without knowing the precise situation and associated circumstances, with reference to this individual case we will refrain from making any assumptions here about probable causes and what could have been done to prevent the accident.

Nevertheless we would like to take this opportunity to investigate a few aspects that must be heeded in connection with this and which illustrate the possibilities that today's safety components offer for minimising risks of this nature.

Firstly: the re-engaging of a machine, a mechanical plant or a production system is always a safety function if risks of unexpected starting up (restarting) exist by virtue of hazardous movements in accessible machine areas or it is possible to move behind the protective devices. This problem can be worked through while conducting the risk assessment that every machine manufacturer or system integrator is legally obliged to carry out and to document.

The question refers to the possible intended or chance presence of persons in the hazardous area of machines that have been shut down and concerns the probability of unexpected starting up (restarting). If it is relevant additional measures are required that, if they are of a control-related nature, will also be incorporated in a Performance Level assessment.

Last but not least the particular nature of the problem concerned here is also indicated by the fact that the subject has its own harmonised standard.

EN 1037: Prevention of unexpected start-up (current version: 2008)



Fig. 1: Reference source of the standard: Beuth Verlag GmbH, Berlin; www.beuth.de

EN 1037:2008 defines unexpected (unintentional) start-up (which includes the term “re-start”) as any start-up that is caused by the following:

- *a start command generated by a failure in or caused by external influence to the control system;*
- *a start command generated by an operating error on a start actuator component or to a different part of the machine, such as a sensor or power control element;*
- *return of the energy supply after an interruption;*
- *external/internal influences (gravity, wind, auto ignition of combustion engines etc.) on parts of the machine.*

NB: Automatic start-up of a machine in normal operation is not unintentional but can be regarded as unexpected from the point of view of the operator. In this case accidents are protected using protective measures (see EN ISO 12 100-2 Section 4).

The standard provides an overview of a number of aspects and requirements that must be heeded and stipulates design safety measures that are aimed at preventing unexpected start-up in order to facilitate safe contact for people in hazardous areas. It concerns unexpected start-up resulting from all types of energy, i.e. to the energy supply (e.g. electric, hydraulic, pneumatic), to easily overlooked stored energy (e.g. from gravity, springs under tension) or to other external influences (e.g. from wind). Figure 2 provides

a detailed over-view of the standard.

Some solutions to the problems on this subject offered by the Schmersal range are set out below by way of example.

Execution of the stop command

The assumption in the following executions is always firstly that a stop command is safely generated by the triggering of a protective device in the **I**nput, **L**ogic and **O**utput chain with the necessary Performance

Level and is implemented in the form of Stop Category 0, 1 or 2.

Please do not confuse the abovementioned “Category” term with control category or similar. What is meant here is rather the distinction in Paragraph 9.2.2 of EN 60204-1:2007^{*,*}, according to which a stop command can be implemented

- as uncontrolled shut-down (by immediate interruption to the power supply → Stop 0) or
- as controlled shut-down (by time-delayed interruption to the power supply → Stop 1)

according to the best possible hazard minimisation. A safety-related shut-down monitor-

DIN EN 1037:2008-11 (E)	
Safety of machinery - Prevention of unexpected start-up (includes Amendment A1:2008)	
Contents	Page
Foreword	3
Introduction	4
1 Scope	4
2 Normative references	4
3 Definitions	5
4 General	6
4.1 Isolation and energy dissipation	6
4.2 Other means to prevent unexpected [unintended] start-up	6
5 Devices for isolation and energy dissipation	6
5.1 Devices for isolation from power supplies	6
5.2 Locking [securing] devices	7
5.3 Devices for stored energy dissipation or restraint [containment]	7
5.4 Verification	8
6 Measures - other than isolation and energy dissipation - intended to prevent unexpected start-up	9
6.1 Design strategy	9
6.2 Measures intended to prevent accidental generation of start commands	9
6.3 Measures intended to prevent accidental start commands resulting in an unexpected start-up	10
6.4 Automatic monitoring of the category 2 stopped condition	13
Annex A (informative) Examples of tasks which can require the presence of persons in danger zones	14
Annex B (informative) Signalling, warning	15
Annex ZA (informative) Relationship between this European Standard and the Essential Requirements of EU Directive 98/37/EC	16
Annex ZB (informative) Relationship between this European Standard and the Essential Requirements of EU Directive 2006/42/EC	17
Bibliography	18

- 1 -

Fig. 2: Download from www.beuth.de → Box “EN 1037” → PDF table of contents (free of charge)

* Electrical equipment on machines; reference source for the standard: Beuth Verlag GmbH, Berlin; www.beuth.de

ing is additionally necessary (also see EN 1037:2008 Paragraph 6.4 in this respect), if a stop command is to be executed as Stop Category 2, i.e. likewise with a controlled shut-down but where the energy supply also remains when the machine has been shut down.

All protective devices and safety-related control devices in the Schmersal range have been designed precisely to offer numerous possibilities for the realisation of safety-related stop commands. For example, reference is made to the shut-down monitoring devices specifically intended for Stop Category 2 from the ranges AZR 31 S1 and FWS (see Figure 3) or, for more complex operations, the safety control systems of the PDMS range (see Figure 4).



Fig. 3: The shut-down monitors from the AZR 31 S1 and FWS ranges serve to safely record the machine shut-down. Depending on the external circuit in conjunction with a safety monitoring module from the AES or SRB range, it is possible to safeguard a protective device up to a PL “d”.



Fig. 4: The “Protect Drive Monitoring System” (PDMS) serves to expand the PROTECT PSC safety control system designed for universal use. With its modular construction, the PDMS represents a solution for safe shut-down and speed monitoring, e.g. of spindle or axle drives up to PL “e”.

Measure: permanently present stop command

The permanently present stop command plays an important role, especially if somebody has to work for a prolonged period in a hazardous area that is difficult to see.

“Permanently” is interpreted here in an exemplary manner, i.e. that the starting up of the machine cannot be set in motion or initiated by any third party. The difficulty in seeing a hazardous area for a third party can occur quickly if one considers linked individual machines, integrated productions systems and machine installations.

A simple but therefore more effective means of achieving this aim is offered by moving protective devices (guards, protective grids etc.) – so-called lockout tags in the terminology used by the Schmersal Group (see Figure 4). These accessories make it possible to secure interlocking devices (safety switches with and without latching) in an open state using padlocks so that renewed actuation of the devices is prevented, i.e. the renewed closing of the moving protective device and renewed starting up of a machine by a third party is effectively prevented both by mechanical and control-related means.

An execution example for Model SZ 200 electronic safety interlocks can be seen in Figure 5.

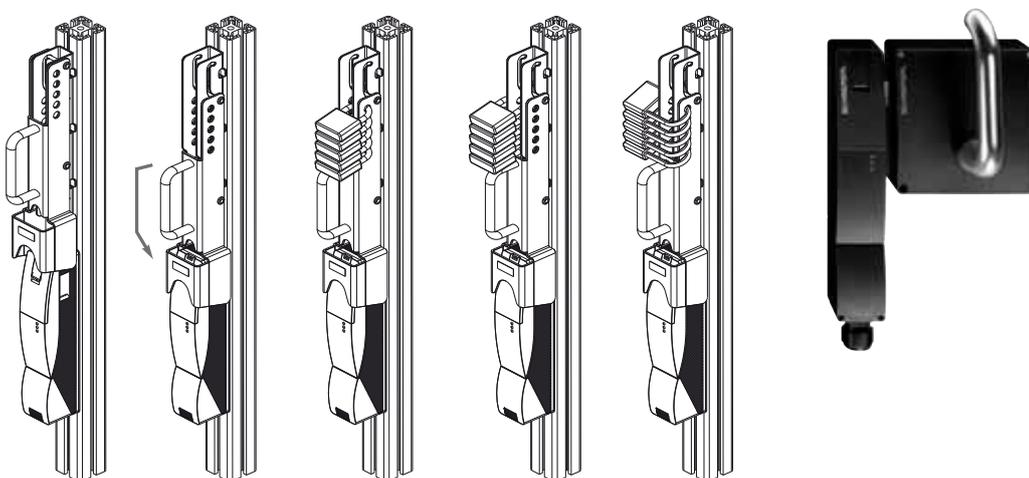


Fig. 5: A lockout tag (the example depicted here is a SZ 200 as solenoid interlock and safety sensors from the AZ/AZ 200 range) prevents actuation of an interlocking device by enabling the operating staff to protect themselves by latching individually coded commercially available padlocks.

Key transfer systems

Key transfer systems offer intelligent possibilities to protect against unexpected (unintentional) starting up where special operating modes also need to be performed by operators in the inside of a hazardous area that is difficult to see.

Actuation of a key-operated selector switch firstly ensures that the automatic operating mode is safely interrupted, i.e. the switch is moved from the I position to the O position and a contact with positive break opens; using the key that can only be removed in this position, the operator is then able to actuate a second key-operated selector switch in the

inside of the machine (O position → I position) that enables the special mode, whereby in this position the key cannot now be removed. Due to an individually coded closing nobody, apart from the operator himself, can reverse the setting on the outer control panel. The stop command for the automatic operating mode is permanently and safely present.

Diverse embodiments for using the philosophy behind a key transfer system are conceivable. It would, for example, be possible to place an interlock in the intermediate cycle, likewise equipped with a key transfer station, i.e. the key from the external key-operated selector switch would firstly be used to unblock the protective device, whereupon a second key could be removed which could then be used to enable the special operating mode in the inside of the machine (refer to Figure 6 to get a clearer understanding of this). The restarting of the machine takes place in reverse order.

Other possibilities for using the key transfer system idea to protect against unexpected start-up are provided by the key distribution stations (SVM range) and interlocking devices (SVE range).

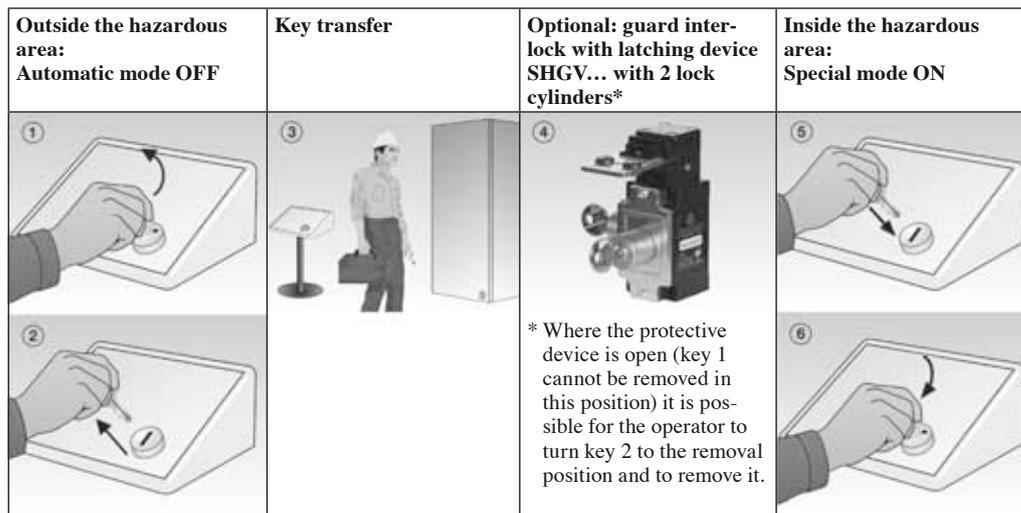


Fig. 6

Reset using double acknowledgement

These types of additional measures will not be necessary in all cases and – if we consider optoelectronics for example – the protective devices do not always involve moving guards that must be safeguarded using interlocking devices.

For other applications in hazardous areas that are difficult to see the use of the double

acknowledgement procedure comes into question, for example, that is illustrated using the PROTECT SRB 100DR safety relay modules (see Figure 7).

The function of the module ensures that it is only possible to restart the machine control system

- once the reset or restart button 1 has first been actuated by the operator

and after he has left the hazardous area and if necessary has closed and locked a guard again;

- once a reset or a restart switch 2 that is situated outside the plant has then been actuated. For executing this “double” acknowledgement an adjustable time frame of between 3 and 30 seconds is provided (set via a DIP switch) within which actuation must take place (exclusively in the order Button 1 → Button 2). The time frame can be oriented towards operational processes.



Fig. 7

If the operator fails to actuate button 1 or to actuate button 2 within the time frame, no enabling takes place and the double acknowledgement procedure must be repeated. Further signal processing of the reset signal then takes place via the commercially available safety relay modules such as those from the PROTECT-SRB range, i.e. in the case of the SRB 100DR module this concerns an upstream device that is implemented with Performance Level “e”.

Fundamentally in future: signal processing of the trailing edge with reset buttons

Irrespective of whether a reset signal (synonym for restart or acknowledgement signal) is implemented singly or doubly after leaving an accessible hazardous area or one that can be accessed from behind, whether with a key selector switch or using a commercially available pushbutton etc., the requirement for detection of the trailing edge will in future apply to signal processing. This means that the acknowledgement may only take place

by releasing the actuator element from its (actuated) ‘on’ position. This requirement will in future arise from Paragraph 5.2.2 of EN ISO 13 849-1:2008 (2006) irrespective of the type of protective device that is acknowledged.

This requirement for dynamic signal processing of the reset signal related to the trailing edge means that any failures and faults in the control device will be detected that would otherwise have constituted a potential risk for an unexpected restart.

The following also apply to the reset function:

- that it must be provided by a separate, manually operated device in the safety-related part of the machine control system; and
- that the device may only be reached if all safety functions and protective devices are fully functional;
- that it must not itself initiate any movement or hazardous situation and that the reset function is an in-tended action that permits the control system to accept a separate start command.

The Performance Level must not reduce the safety of the corresponding safety function here.

Further requirements on the subject of “acknowledgement” are also contained in EN ISO 12 100-2:2008 (2003) Section 4.