3 Categories as defined in EN 954-1

3.1 General

The requirements for safety-related parts of control systems are specified by five categories in the context of EN 954-1 [4]. The categories represent a classification of the safety-related parts of a control system (STS) with respect to their ability to withstand faults and their behaviour in the event of faults, this being achieved on the basis of reliability and / or the structural architecture of the parts (table 3, see page 30). A greater ability to withstand faults signifies a higher possible risk reduction. For this reason, the categories are fundamentally suited to reducing the risk associated with a piece of machinery to an acceptable extent by means of measures at the level of the control system.

Category B is the basic category, the requirements of which must also be observed in the other categories. In categories B and 1, the ability to withstand faults is mainly achieved by the selection and use of appropriate components. If a fault occurs, the safety function may become inoperative. Category 1 has a greater ability to withstand faults than category B thanks to the use of special components which have been well-tried in safety applications.

In categories 2, 3 and 4, an improved performance with respect to the prescribed safety function is achieved, mainly as a result of structural measures. In category 2, execution of the safety function is checked at regular intervals (usually automatically by technical measures). However, the safety function may fail between the test phases if a fault occurs. By appropriate selection of the test intervals (e.g. once per shift), an appropriate risk reduction can be achieved when applying category 2. In categories 3 and 4, the occurrence of an individual fault cannot lead to the loss of the safety function. In category 4, and whenever reasonably practicable in category 3, such faults are detected automatically. Category 4 also offers the ability to withstand an accumulation of unobserved faults.

When considering faults it is necessary to reach an agreement as to the component faults which are implied and the component faults which can be reasonably ruled out. Information concerning the faults to be considered is given in the following sections and also in Appendix B.

Systematic faults[7] are barely mentioned at all in EN 954-1. Only in categories 3 and 4, does the sentence “Common mode faults shall be taken into account“ point to a type of systematic faults, namely common mode

[7] Systematic faults can creep into the product at any time during the product‘s life cycle.

Table 3:
Requirements for the categories of safety-related parts of machinery control systems

Category	Requirements (in brief)	System Behaviour	Principle
B	Safety-related parts of control systems and / or their safety devices and their components must be designed, constructed, selected, assembled and combined in accordance with the relevant standards such that they can withstand the expected influence.	The occurrence of a fault can lead to the loss of the safety function.	mainly characterised by the selection of components
1	The requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function, but the probability of occurrence is lower than in category B.	
2	The requirements of B and the use of well-tried safety principles shall apply. The safety function shall be checked at suitable intervals by the machinery control system.	The occurrence of a fault can lead to the loss of the safety function between the checks. The loss of the safety function is deteced by the check.	mainly characterised by the structure
3	The requirements of B and the use of well-tried saftey principles shall apply. Safety-related parts shall be designed such that: 1. a single fault in any of these parts does not lead to the loss of the safety function, and 2. the single fault is detected whenever reasonably practicable.	If the single fault occurs, the safety function is still maintained. Some, but not all faults are detected. Accumulation of undetected faults can lead to the loss of the safety function.	
4	The requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed such that: 1. a single fault in any of these parts does not lead to the loss of the safety function, and 2. the single fault is detected during or prior to the next demand on the safety function, or, if this is not possible, an accumulation of faults should not as a result lead to the loss of the safety function.	If faults occur, the safety function is still maintained. Faults are detected in good time to prevent the loss of the safety function.	

faults[8]. In category 4, diversity and the use of special test methods are mentioned as examples of measures used to counter systematic faults when validating the category. In principle, it can be said that many of the basic and well-tried safety principles do, of course, have the effect of preventing systematic faults (see tables 4 and 6, pages 32 and 39).

3.2 Category Specifications

3.2.1 Category B

Safety-related parts of control systems must be designed, constructed, selected, assembled and combined in accordance with the relevant standards and using the basic safety principles for the specific application, such that they are able to withstand:

- the anticipated operating stresses (e.g. reliability with respect to breaking capacity and frequency)
- the influence of the material used in the operating process (e.g. cleaning agents in a washing machine)
- other relevant external influences (e.g. mechanical vibrations, external electromagnetic fields, interruptions or disruptions to the energy supply).

These general principles are illustrated in general terms and with reference to specific technologies in the basic safety principles specified in table 4. In this table, the general basic safety principles apply in full for all technologies, whilst the technology-specific principles are also necessary for the relevant technologies. As category B represents a basic category for each of the other categories (see table 3), the basic safety principles should be applied as a general rule to the design of safety-related parts of control systems (STS) and / or safety devices.

No further specific safety-related measures are necessary for the components which comply with category B[9].

3.2.2 Category 1

In addition to the basic safety principles, safety-related parts in category 1 must be designed and constructed by using components and principles which are well-tried with respect to safety.

---

[8] Common mode faults are those faults which cause a multi-channel system to fail.

[9] If a component failure occurs, it may lead to the loss of the safety function.

Table 4:
Basic safety principles for the design of safety-related parts of control systems, Part 1

Principle	Description	Significant Criteria
General		
Ensure adequate dimensioning for all components	All components are selected such that they can withstand the anticipated operating stresses.	❒ breaking capacity, breaking frequency ❒ withstand voltage-strength ❒ pressure level, dynamic pressure behaviour, volume flow ❒ temperature and viscosity of pressure fluid ❒ type and condition of pressure fluid or compressed air
Resistance to relevant external influences	Safety-related parts of control systems (STS) are designed such that they can fulfil their function even in the event of the external influences which are usual for the application in question.	❒ mechanical effects (shock, vibration) ❒ climatic effects (temperature, humidity) ❒ leak-tightness of the housing (protection provided by enclosure) ❒ electromagnetic compatibility (fields, conducted disturbances)
closed circuit principle (positive signalling to start)	The safety-related switching position of the STS is achieved by removing the control signal (electrical voltage, pressure), i.e. by switching off the energy supply.	❒ safe state in the event of an interruption ❒ valves with working springs in the field of fluid technology
Control of fluctuations in the energy supply, failure and recovery of the energy supply	In the event of fluctuations in the energy supply (voltage or pressure), the STS should not initiate any unexpected reactions.	❒ faults in the power supply ❒ changes in pressure, pressure loss
Compliance with the applicable technical regulations	The applicable technical regulations associated with the application should be observed	❒ completeness ❒ accuracy
Quality assurance measures during production	General quality assurance measures, e.g. as defined in EN 45000, guarantee constant product quality for the STS.	❒ reproducibility during production
Comprehensible and complete installation, commissioning, operating and maintenance instructions	Well-structured instructions which are generally comprehensible are available for the installation, commissioning, operation and maintenance of STS.	❒ completeness ❒ comprehensibility ❒ accuracy
Formalization of modification procedure	All modifications to STS should be documented and the effects on the parts of the STS which have not been modified should be recorded. The modified STS will only be released following successful acceptance.	❒ accuracy of modifications ❒ no effect on parts which have not been modified

Table 4:
Basic safety principles for the design of safety-related parts of control systems, Part 2

Principle	Description	Significant Criteria
Fluid Technology		
Pressure control in the system	One or more pressure control valves usually prevent the pressure in a system or in parts of systems from rising beyond a specified level. Pressure control valves with secondary venting are used primarily for this purpose in pneumatic systems.	❒ check dimensioning ❒ position in the system (number) ❒ design
Filtration of the pressure medium (hydraulic fluid, compressed air)	The necessary purity class of the pressure medium during operation as specified by the manufacturer with reference to the components used is achieved by the use of a suitable device (usually a filter) after taking account of the application in question. Adequate drainage of the compressed air is also necessary for this to be achieved in the pneumatics sector.	❒ check dimensioning ❒ type of hydraulic fluid / compressed air state ❒ component manufacturers' requirements ❒ ambient conditions and conditions of usage ❒ position in the fluid technology system
Prevention of dirt intake	In open hydraulic systems, one particular way of preventing contamination from penetrating the fluid technology system is by using an active vent filter. In pneumatic systems, exhaust air filters (filter-silencer combinations) are used for this purpose (negative pressure).	❒ check dimensioning ❒ component manufactures' requirements ❒ ambient conditions and conditions of usage ❒ exhaust air discharge direction
Disconnection from the energy supply (if the energy supply is not required for the safety function, e.g. clamping devices)	Disconnection from the energy supply and discharge of the residual energy (if necessary) is facilitated by suitable main control devices (e.g. isolating valves).	❒ reliable disconnection / safe discharge (also in the case of storages) ❒ switch position and operating state should be recognisable

Table 4:
Basic safety principles for the design of safety-related parts of control systems, Part 3

Principle Description		
Computing		
Simple functional tests	Safety functions must be checked.	❒ normal functional and operating sequences ❒ tests should be representative
Transmission protocols with timed sequence monitoring for data transmission via buses	When transmitting usable data, compliance with a communication specification (e.g. parity bit) is monitored.	❒ accuracy of data communication
Timed monitoring via Watch-Dog	A timing element is periodically reset by the program. If the program no longer reacts after being reset, the STS is switched to a defined state by the timing element.	❒ monitoring program sequence
Technical modification protection (ROM, EPROM)	Modifications to the safety-related software by unauthorized persons are prevented by technical measures.	❒ no modifications by unauthorized persons
Minimisation of real-time effects	Real-time effects on the program make analysis more difficult and may cause certain properties of a program to become erratic. There should, therefore, be as few interrupts and multi-tasking areas as possible. Cyclic detection of process states should take place in a fixed sequence. Rules for approving interrupts should be drawn up.	❒ software should be able to be analysed ❒ software should be easy to modify
Structured programming	Control sequence flow in programs and data flow in these programs are designed to be transparent thanks to this method. This thus avoids non-systematic, complex and awkward program structures.	❒ case of testing, comprehensibility ❒ adaptability ❒ case of maintenance ❒ portability

A component which is well-tried with respect to safety for a safety-related application is a component which

- ❒ has been widely and successfully used in the past with successful results in similar applications or
- ❒ has been manufactured and verified by applying principles which demonstrate its suitability and reliability for safety-related applications.

Table 5 provides an overview of known components which are well-tried with respect to safety in the field of electrical engineering and components from the fluid technology sector which may be components which are well-tried with respect to safety.

Requirements with respect to the design and construction of valves which are well-tried with respect to safety and requirements concerning the condition of the pressure medium involved have not yet been specified. For this reason, only valve manufacturers and / or users are usually in a position to nominate valves which are well-tried with respect to safety for defined applications on the basis of their practical experience. A valve which is well-tried with respect to safety is, in particular, a valve with a sufficiently high level of safety-related reliability in practical conditions. This reliability relates solely to switching function into the safety-related position. A valve of this type must fulfil the component-specific basic and well-tried safety principles in Tables 4 and 6. Filtration for a valve which is well-tried with respect to safety must be performed specifically. In the case of a low risk combined with simple installations, the system filter which is always present in the installation may be sufficient for the necessary filtration operation. In the case of a higher risk and in complex installations, filtration should be performed immediately in front of the relevant valve and / or the relevant valves by means of a full-flow pressure filter (referred to as DF in the examples in Chapter 4). The filter's contamination level should be monitored. In pneumatic installations, a full-flow pressure filter may also be necessary immediately in front of the relevant valves in the case of larger pipework systems, several users and in the case of valves which require a higher filtration grade than other components in the installation.

In order to protect the valve as much as possible from contamination in the pressure medium from the cylinder side, specific measures are necessary with respect to the piston rod in the hydraulic / pneumatic cylinders (e.g. working wiper rings). In pneumatic control systems, it should also be noted that contamination can be drawn into the system via exhaust air apertures. For this reason, exhaust air (vent) apertures (e.g. on valves)

should be fitted with working filters, so-called filter-silencer combinations.

In the fields of electronics and computing, there are also no known components which are well-tried with respect to safety at the present time. As explained in [17], the method which is described in detail below to establish whether components are well-tried in operation, is used to prove that the components used, e.g. including software, are sufficiently free of systematic design faults. However, being well-tried in operation does not yet in itself enable a hardware module to be classified as a well-tried component, as, quite apart from systematic faults, the random error rate for a component must also be very low [16][10]. If a component is well-tried in operation, this tells us that no faults, or only insignificant faults, were established when using a considered unit, whereby this unit has been operated for the most part without any modifications over an adequate period of time in numerous different applications [17]. According to [17], a component is said to be well-tried in operation if, for an unaltered specification, the following conditions apply:

- ❒ 10 systems in different applications and
- ❒ 10^4 operating hours and
- ❒ at least one year of operation and
- ❒ no faults or no safety-related faults have been observed.
- ❒ There must be a statistical confidence level of 95%.

Proof must be provided by way of documentation from the manufacturer or user. The documentation must include the following at the very least: a precise description of the system and its components including the versions of the hardware and software used, the user and the usage period, operating hours, a method for selecting the systems and application cases used to provide this proof and a method to detect faults and to record and eliminate faults [17]. This is a particularly useful way of proving that software or complex electronic systems are well-tried in operation with respect to systematic faults. A correspondingly higher number of operating hours is required for higher categories [16].

Certain faults which are used for assessment purposes can also be ruled out for some well-tried components, because the fault rate for

[10] IEC Draft 1508 classifies the specified aims of a safety-related system in category 1 with a failure probability of 10^{-1} to 10^{-2} per demand for systems with a low demand rate and a probability of one dangerous failure per year of 10^{-1} to 10^{-2} for safety-related systems with a continuous or high demand rate. This probability limit is lower by one decimal power in each case for categories 3 and 4.

this failure mode is known to be very low (e.g. switches not opening when forcibly opened in category 3). Fault exclusions of this type are described for specific technologies in the fault lists in Appendix B to this Report.

The decision as to whether to accept a specific component as being well-tried with respect to safety is dependent on the application in question.

The following are examples of well-tried safety principles:

- ❒ avoiding specific faults (e.g. avoiding short-circuits by separation)
- ❒ reducing the probability of faults (e.g. by overdimensioning) or stress on the components below the design limit
- ❒ specifying the failure direction for a fault
- ❒ fault detection in good time (e.g. detecting earthing)
- ❒ limiting the consequences of a fault.

Table 6 illustrates currently known well-tried safety principles of a general and technology-specific nature. Some of these principles are very general and are in some cases used depending on the category in question. The principle of automatic monitoring exists as a well-tried principle in categories 3 and 4, for example, whilst touch operation, which is limited by time or distance, represents a principle which is dependent on the application in question. On the other hand, the principle of a "control system with self-locking" can be used for all categories on a very general basis. These reflections make it quite clear that, unlike the basic safety principles, well-tried principles cannot all be applied in all circumstances, but are specific to each technology, application or category.

In general terms, it can be said that there is a lower probability of a dangerous failure in category 1 than in category B. It follows that the loss of the safety function is less likely[11].

At present, there are no specified well-tried safety principles in the field of fluid technology. These safety principles relate to both the components and the pressure medium. Part 3 of Table 6 lists the major well-tried safety principles for fluid technology, which in our opinion, although, depending on the application in question cannot all be achieved at the same time.

[11] The occurrence of a fault can lead to the loss of the safety function.

Table 5:
Components which are well-tried with respect to safety for the design of safety-related parts of control systems

Components which are well-tried with respect to Safety	Aim / Function
Electrical Engineering	
Fuse / automatic switch	Cut-off in the event of a short-circuit or earthing
Mechanical position switch with personal protection function with forcibly actuated normally closed contact EN 60947-5-1, chapter 3	Control voltage interrupted when actuated
Positive locking (see EN 1088)	Preventing dangerous access
Forcibly actuated camshaft switch	Actuation of switching contacts
Control circuit contactors[5] as per EN 60947-4-1 Power contactors [5]	Release when de-energized
Emergency Stop keys / cable control switch with forcibly actuated normally closed contact (EN 60947-5-1, chapter 3)	Control voltage interrupted when actuated
Wiring, installation in control cabinet Light plastic sheathed cable, protected installation in machinery frame	Avoid short circuit of wires
Touch controls	Control voltage interrupted when released
Mechanically actuated compliance switch (see EN 292)	
Terminals in switching cabinet / terminal box in the machinery (with adequate protection system)	Avoid crosses (short circuits)
Fluid Technology [6]	
Directional control valves with discrete switching positions (slide and seat valves)	Safety-related switching position is taken up by means of durable, working springs and the control energy is interrupted
Continuous directional control valves	
Stop valves (non-return valves, controlled non-return valves)	Preventing the flow in the closed direction
Flow control valves (throttles and restrictors) as a fixed resistance in fluid engineering systems	Retention of the set volume flow
Pressure valves in the safety-related part of the control system	Proposed function in the event of pressure values being exceeded or not attained
Pressure switches, pressure sensors	
Mechanically positively actuated valves (forcibly actuated) Manual lever valves with spring return or spring centring	Interruption of volume flow or control signal
Pipework in the safety-related part of the control system and to consumer	Leak-tightness, breaking strength

[5] Whilst there is no doubt that control and power contactors do not respond if the control voltage is absent (fault exclusion), there is some controversy as to whether these contactors should be regarded as "well-tried components" with respect to the way in which they are released when de-energized. In the author`s opinion, no fault exclusion can in fact be made for these switching devices, but it is possible and justifiable to classify them as "well-tried components". Otherwise, contrary to many years of practical experience, a position monitoring device for a movable safety guard with only one power contactor for switching off the potentially hazardous movement would have to be classified under category B.

[6] This details components which may be components which are well-tried with respect to safety, as the current situation in the field of fluid technology is such that it is only possible to specify components which are well-tried with respect to safety in specific individual cases.

Table 6:
Well-tried safety principles for the design of safety-related parts of control systems, Part 1

Principle	Description	Aim
General		
Control system with self-lock	This type of control system goes into a self-locking state after a brief command, e.g. by touch controls and retains this state for as long as the control energy is provided (voltage, pressure).	Protection ❒ against unexpected restarting ❒ after energy failure and return
Separation / insulation	Adequate leakage distances and air gaps are ensured, and suitable insulating materials and thicknesses are used.	To avoid short-circuits
Earthing control circuits	A one-sided connection is made between control circuits and the equipment earth (see EN 60204-1, Section 9.1.4).	Fault detection in the event of earthing
Torque / power limiting (reduced pressure)	Forces which may lead to a hazard are limited by electrical, mechanical or fluid technology devices.	Risk reduction by improved hazard protection
Limited distance touch operation	The distance of a movement is limited to an admissible value in touch operation.	
Limited time touch operation	The time taken by a movement is limited to an admissible value in touch operation.	
Reduced frequency / speed (reduced volume flow)	The frequency or speed of a movement is limited to an admissible value in touch operation.	
Overdimensioning (underloading)	All equipment is loaded to less than the nominal value.	Reduction of the failure probability
Start-up testing	The protection function is compulsorily checked before initiating a potentially hazardous movement.	Fault detection before initiation
Self-actuated / automatic monitoring	Faults in components are detected in good time by monitoring.	Pick up faults in good time
Hardware diversity	Different types and designs of technical devices are installed.	Avoid common mode faults
Use of standard circuits	Standard circuits are circuits for special applications, which have been checked to determine their behaviour in the event of faults and which have been well-tried in practice.	Safety function by means of well-tried or tested devices

Table 6:
Well-tried safety principles for the design of safety-related parts of control systems, Part 2

Principle	Description	Aim
Use of type-tested modules (e.g. control devices)	Type-tested modules are factory-built devices which fulfil particular validated requirements.	
Normally closed / normally open contact combination	This is concerned with the arrangement of two mechanical position switches in a safety device with fundamentally different actuation modes. One switch is always actuated and the other is not actuated whatever the position of the safety device.	❒ Maintain the safety function of mechanical position switches in the event of individual faults in the mechanism ❒ Detection if the safety device is removed
Electromechanical engineering		
Connected movement of contacts	Connected movement implies a mechanical connection of contacts in contactors and relays which rules out the possibility of normally closed and normally open contacts closing simultaneously even in the event of a fault.	Monitoring control contactors
Interlocking	Several relays / contactors are connected in such a way that other components can no longer be actuated in the event of a fault in one component thanks to the connected movement system.	Prevention of undesirable states
Forcible / positive actuation	This is a reliable means of actuation by rigid, mechanical parts without non-positive and spring-actuated connections.	Safe actuation, e.g. for mechanical position switches
Electronics / Computing		
Dynamic techniques	All safety-related signals change their state on a regular basis, with the result that static faults automatically initiate a safety-oriented function.	Static component faults can be picked up and dealt with in good time
Separation of electrical energy transmission lines from information transmission lines	Resistance to interference is increased, especially with sensitive analog signals, by spatial separation.	No capacitive or inductive disturbances of signal transmissions by electrical energy transmissions

Table 6:
Well-tried Safety Principles for the Design of Safety-related Parts of Control Systems, Part 3

Principle	Description	Aim
Non-equivalent signal control	When processing redundant signals, one channel uses a logical l when the other uses a logical 0 and vice versa.	Increased resistance to interference with respect to common mode faults
Fault detection via the technical process	Faults are picked up by means of specific expected events which are prescribed by the technical process. It is not usually possible to pinpoint the fault in this method.	Early fault detection
Plausibility checks	Plausibility checks are used to achieve a defined reaction in the event of inadmissible or unusual inputs and states or those which are outside the specified values.	Defined reaction ❒ in the event of incorrect user specifications and ❒ in the event of component failures
Use of an external watchdog	A watchdog is a timed program run monitoring system in which an external component expects signals from the microcomputer at regular time intervals. If these signals are not received, the watchdog is required to initiate a safety-oriented reaction by means of a second independent cut-off path.	Defined reaction in the event of defective program sequence
Fluid Technology		
Positive overlap	There must be an adequate positive overlap for contacts to be closed when using slide valves.	to stop potentially hazardous movements to prevent unintentional starting up
Positive dynamic effect	The actuating forces have a direct effect (forcible) on the moving parts, i.e. without frictional connections.	Reliable actuation of moving parts
Specific selection of materials and material pairing	This selection takes place by considering the properties of the hydraulic fluid on the basis of corresponding experience and / or specific tests.	Reduction of failure probabilities
Definition of operating data	The principal variables which are defined are the operating temperature range and the operating viscosity range for the hydraulic fluid.	
Monitoring the hydraulic fluid	The state of the hydraulic fluid is monitored on a regular basis, e.g. by sampling.	

3.2.3 Category 2

The requirements of category B must be fulfilled. Well-tried safety principles must also be used. In addition, in category 2, the safety-related parts of the control system must compulsorily be tested by the machinery control system at suitable time intervals (see table 3). Testing the safety function must take place:

- ❒ when the machinery is started up and before a hazardous state is initiated
- ❒ periodically during operation, if risk analysis and the operating mode indicate that this is necessary.

This test can be initiated automatically or manually. However, a positive test result is a prerequisite for starting up or continuing to operate the machinery. Each safety function test must either approve operation, if no faults have been detected, or, if faults are detected, it must generate an output signal to enable appropriate control system measures to be initiated[12]. The test itself should not lead to a hazardous state. Once a fault has been detected, a safe state must be maintained until the fault has been rectified. The testing device may be a separate device or may be part of the safety-related part of the control system which executes the safety function.

In some cases, category 2 is not applicable, as it is not possible to test the safety functions of all components, e.g. pressure switches or temperature sensors. In general terms, category 2 can be achieved with electronic techniques, e.g. in safety devices or specific control systems[13]. However, in this case it must be possible to guarantee that the testing device and the STS cannot fail at the same time as a result of a single fault as listed in Appendix B (e.g. in that they are not implemented in a single programmable logic controller).

---

[12] In the latest version of the standard, this requirement is reduced in that it now states: „If it is not possible to initiate a safe state, e.g. welding the contact for the limit switch, the output signal must provide a warning of the hazard.“ To date, category 2 has been defined more stringently within the BIA and a second independent cut-off method was required. The additional requirement to maintain a safe state until the fault is rectified can only be fulfilled by means of the second independent cut-off method. This inconsistency must, in our opinion, be ironed out by the standard maker before the second independent cut-off method can be replaced by a warning.

[13] This system behaviour accepts that:
– the occurrence of a fault leads to the loss of the safety function between tests,
– the loss of the safety function is usually detected in good time by testing.

3.2.4 Category 3

The requirements of category B must be fulfilled. Well-tried safety principles must also be used. In addition, the safety-related parts in category 3 must be designed such that a single fault in one of these parts as defined by the fault list in Appendix B does not lead to the loss of the safety function (see table 3). Common mode faults must be taken into account if the probability of a fault occurring is high. The individual fault must be detected during or before the next demand on the safety function whenever reasonably practicable.

The requirement that individual faults should be detected does not mean that all faults are detected. zThis is why, in the case of certain types of machinery, an accumulation of unobserved faults can, in certain circumstances, lead to an unintentional output signal and to the machinery entering into a hazardous state. zTypical examples of practicable measures for fault detection purposes are scanning the relay contacts with connected movement or monitoring redundant electrical outputs. If necessary as a result of the technology and application in question, the Type C standard maker should specify additional details with respect to fault detection. "Whenever reasonably practicable" means that the necessary measures for fault detection purposes and the extent to which these are incorporated, are chiefly dependent on the consequences of a failure and on the probability of occurrence of an accident within the application. The technology which is used influences the possibilities for incorporating fault detection[14].

3.2.5 Category 4

The requirements of category B must be fulfilled. Well-tried safety principles should also be used. In addition, safety-related parts of control systems in category 4 must be designed such that (see also table 3):

- a single fault (see Appendix B of this report) in any of these safety-related parts does not lead to the loss of the safety function and
- the individual fault is detected during or before the next demand on the safety function, e.g. immediately after switching on or at the end of a machine cycle. If this type of detection is not possible, an

[14] This system behaviour accepts that
– the safety function is always retained if a single fault occurs,
– some, but not all faults are detected,
– an accumulation of undetected faults may lead to the loss of the safety function.

accumulation of faults should not lead to the loss of the safety function[15].

If it is not even possible to detect certain faults due to the technology or circuit design in question during the next test, the occurrence of additional faults must be assumed. In this case, an accumulation of faults should not lead to the loss of the safety function. Fault review should be suspended if the probability of further faults occurring can be regarded as being sufficiently low[16].

---

[15] This system behaviour accepts that
– the safety function is always retained if faults occur,
– faults are detected in sufficient time to prevent the loss of the safety function.

[16] According to the experience acquired by the BIA, fault accumulation can be suspended after the third fault, irrespective of the technology in question.

Fault review can be restricted to two combined faults, if

- ❒ the components' fault rates are low and
- ❒ the combined faults mainly occur independently of each other and
- ❒ the safety function is only interrupted if the faults occur in a specific sequence.

If additional faults occur as a result of an initial individual fault, the initial fault and all resulting faults must be regarded as a single fault. Common mode faults must be taken into account, e.g. by applying diversity or special methods for detecting faults of this type.

In the case of complex circuit structures (e.g. microprocessors, complete redundant systems), fault review is generally performed at structural level, i.e. based on sub-assemblies.