



## **NDT MainCal Radiation Protection Services**

Unit 2 Dale Road • New Mills • High Peak • Derbyshire • SK22 4NW  
Tel: 01663 742549 • Fax: 01663 740967 • Email: rpa@maincal.com

---

### **Advisory Note - September 2012**

#### **The Design and Review of Radiation Enclosure and Cabinet Safety Systems**

As your Radiation Protection Advisor we have prepared this advisory note, the purpose of which is to provide a current overview of a complex set of Directives and Regulations that must be observed when designing new radiation enclosure and cabinet safety systems, as well as during the review of existing systems.

The design and/or review of any safety system should be carried out by a competent person with the necessary understanding and training to determine whether the circuitry and component parts will meet legal requirements.

As well as being a recognised RPA body under IRR99, NDT MainCal Limited employs several electrical engineers who have the necessary competences to carry out initial design or design review, should assistance be required.

#### **Legislation**

As with all work related activities, there are numerous Regulations and Directives that are considered relevant when designing, installing and operating a safety system for the use of equipment producing ionising radiation in a shielded enclosure. The most pertinent legislation that must be adhered to is listed below:

- Ionising Radiation Regulations 1999 /(ACOP)\* (IRR99)
- 2006/42/EC Machinery Directive
- 2006/95/EC Low Voltage Directive
- Management of Health and Safety at Work Regulations (MHSWR) 1999
- Provision and Use of Work Equipment Regulations (PUWER) 1998

\*The **Approved Code of Practice** is published with IRR99 and gives guidance as to interpretation and implementation of the Regulations.

#### **Standards**

Associated with the legislation are a number of standards and harmonised standards. These standards have no legal status and therefore they do not have to be adhered to. However, in the case of harmonised standards, compliance with them allows you to claim conformance with the Directives (which are legally binding). Otherwise it is necessary to show compliance with the essential health and safety requirements of the Directives by other means.

Within the harmonised standard BS EN ISO 13849-1:2008 Safety of Machinery, the most relevant section is 'Safety-related parts of control systems'.

In addition, EN 62061:2005 is an alternative standard preferred by some designers. Its application is more complicated. This standard is used on complex systems especially those containing programmable devices.

Both standards generally give the same result but use different terms.

## **Design**

In the early stages of a radiation enclosure/cabinet interlock design, the primary legislation to be considered is IRR99. This legislation requires that the first step in the design process must be to carry out a prior risk assessment (Regulation 7(1)).

Note: Due consideration should also be given to the requirements of MHSWR (Reg. 3) for risk assessments, including the requirement for a company with 5 or more employees to formally document the risk assessment.

## **The Purpose of the Risk Assessment**

A good overall definition of the purpose of the risk assessment is given by IRR99 ACOP (Para 45): -

“From the risk assessment it should be possible to determine what steps are necessary to the control of exposure by the use of engineering controls, design features, safety devices and warning devices (Regulation 8(2)(a)) and in addition, by the development of safe systems of work.”

NB: It is also worth noting that the machinery directive requires all “foreseeable” uses and misuses to be considered. The concept of ‘that won’t happen’ is not sufficient.

## **Risk assessment content**

IRR99 ACOP (Para 44) lists those matters which need to be considered as part of the risk assessment.

Matters that are particularly relevant to the safety system design include.

- Advice from manufacturer or supplier of equipment about its safe use and maintenance
- Engineering control measures and design features already in place or planned
- Possible accident situations, their likelihood and possible severity
- The consequences of possible failure of control measures-such as electrical interlocks, ventilation systems, warning devices etc.

## **Design Requirements**

From the risk assessment, and in consultation with the RPA and other interested parties, it should be possible to produce an “outline design” defining the type, number and position of devices such as illuminated warning signals, sirens, emergency stops, door interlock switches etc.

IRR99 offers this further advice on interlocks

### **REGULATION 8(2): Restriction of Exposure**

**ACOP Para 87:** 'Where control systems permit, interlocks or trapped key systems should be provided and properly used where they can prevent access to high dose rate enclosures (for example in which employed persons could receive an effective dose greater than 20 millisieverts or an equivalent dose in excess of a dose limit within several minutes when radiation emission is under way). They should be fitted so that the control system will ensure an exposure:

- (a) cannot commence while the access door, access hatch, cover or appropriate barrier to the enclosure is open;
- (b) is interrupted if the access door, access hatch, cover or barrier is opened; and
- (c) does not recommence on the mere act of closing a door, access hatch, cover or barrier'.

**Guidance Paragraph 92:** 'The ACOP advice in paragraph 87 means that effective interlock devices should normally be designed and installed in such a manner that if they fail to operate correctly no exposure of people can occur'.

**Guidance Paragraph 92-102** lays out the general requirements for warning signals:

Warning devices are required to indicate that:

1. System is powered and capable of emitting radiation
2. System is about to emit radiation
3. System is emitting radiation

These warning devices should be monitored for failure such that if a failure occurs, the exposure will be terminated/disabled.

In practice the primary warning device is an industry-standard 3 stage illuminated status panel with or without an integral siren. (Light Box)

### **Detailed Electrical Design**

Having constructed the outline design, it is now necessary to ascertain the required architecture and performance levels of the individual circuits and of the overall system.

This aspect of the design is covered by the machinery directive, which in turn points the designer to BS EN ISO 13849-1:2008 'Safety-related parts of control systems - General principles for design'.

The first step is a risk assessment using the graph provided in FIG 1 (on the following page). Unlike the risk assessment outlined in IRR99, the process invoked by BS EN 13849-1 is quantitative, to the extent that it defines the:

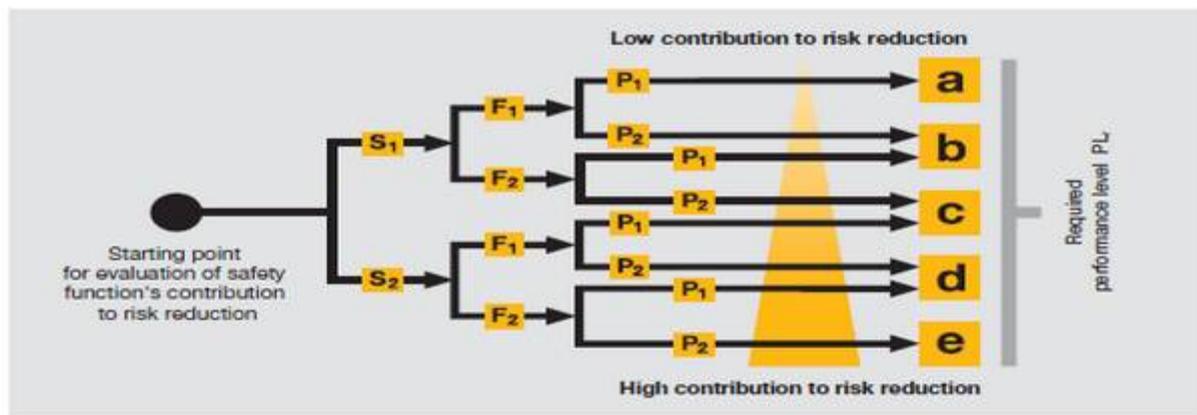
- *Performance Level (PL) Required*, which is the outcome of assessing 3 parameters using the graph below.
- *Performance Level Achieved*, which is a measure of a number of factors including the categories (architecture) of the safety circuits, fault types detected, fault tolerance, reliability data etc.

### **FIG 1**

<b>Severity of injury</b>	<b>S</b>
Slight (normally reversible injury)	S <sub>1</sub>
Serious (normally irreversible injury including death)	S <sub>2</sub>

<b>Frequency and/or exposure to a hazard</b>	<b>F</b>
Seldom to less often and/or exposure time is short	F <sub>1</sub>
Frequent to continuous and/or exposure time is long	F <sub>2</sub>

<b>Possibility of avoiding the hazard</b>	<b>P</b>
Possible under specific conditions	P <sub>1</sub>
Scarcely possible	P <sub>2</sub>



Risk graph in accordance with EN ISO 13849-1.

The *PL achieved* should always equal or exceed the *PL required*.

Taking each parameter in turn:

**Severity:** For uses of ionising radiation in most industrial applications, this must be classed as **S<sub>2</sub>** because the effects of a given exposure are variable and the severity of harm caused may not become apparent for many years. Additionally any substantial exposure will require investigation and may result in prosecution by the HSE.

**Frequency:** General industry guidance calls for **F<sub>2</sub>** to be used where the exposure is more than once per hour, or of a duration exceeding 15 minutes per shift.

**Possibility:** Because ionising radiation cannot be detected by human senses, there is no natural awareness of any hazard to avoid, therefore **P<sub>2</sub>** must be used.

Applying **S<sub>2</sub>**, **F<sub>2</sub>**, **P<sub>2</sub>** to the graph gives a Performance Level required of **e**

In practice this means that Category 4 architecture should be incorporated in the enclosure/cabinet entry door(s) interlock and the emergency stop circuits<sup>see note 1</sup>. This normally means using redundant cross-monitored circuitry. In such a system, the door position sensing circuit requires 2 switches connected to a 2 channel safety relay, which should operate as follows

- For its outputs to close (permitting radiation to be emitted) both the switches must close.
- If only one switch closes the safety relay output will open and remain open until the other switch has closed. (Some safety relays require that when one switch opens or closes, the other switch must operate within a given short time period so as to detect slow or intermittent switch operation).
- If both switches are closed and only one opens, the safety relay output will open and remain open until both switches have opened and then closed.

The effect of this is that the circuit is cross-monitored for circuit/switch faults such as stuck contacts (open or closed), broken switch actuators, short and open circuits which may have developed in the wiring. In addition, simple efforts to defeat the safety circuit such as disabling a switch or removing the circuit's power become impossible. It is also important to bear in mind that Category 4 safety relays themselves contain redundant monitored circuitry and other precautions against failing. By employing this type of circuitry in a safety interlock system the goal of "fail to safe" (as referred to in the IRR99 ACOP) should be achieved.

Category 4 emergency stop circuits are implemented by having dual contacts operated by a single force guided actuator (direct acting without spring return). Where possible an emergency pull cord with a switch at each end should be used as this has the added advantage of providing 2 separate switches and separated wiring.

It must be remembered that the architecture is not the only aspect of the design that needs careful consideration. The physical aspects of the design together with reliability data all contribute to achieving the required Performance Level.

As stated earlier in this document, all primary warning devices should be compliant with IRR99 requirements<sup>see note 2</sup>.

Notes:

1. The machinery Directive defines 'primary' safety circuits as essentially guard monitor circuits, which prevent access to a hazard and remove the hazard if breached. As Emergency stop circuits do not restrict access to the hazard, they are in strict terms considered secondary or complimentary safeguards. Therefore it may be argued that they do not form part of the Performance Level risk assessment and therefore need not be category 4. However common sense would dictate that because the emergency stops are inside the radiation exposure area, anyone needing to operate them is being irradiated or is in imminent danger thereof. Reliable operation is therefore of great importance, and NDT MainCal recommends that emergency stop circuits are implemented to Category 4 architecture.
2. Similar to emergency stops, warning devices are not a concern of the machinery directive. However, IRR99 requires that the warning devices shall be monitored for failure and be 'fail to safe'. Therefore, NDT MainCal recommends that at least two enunciator panels are used inside a radiation enclosure, preferably monitored by a 2 channel safety relay. This is because anyone in the exposure area would not be aware of radiation being present if the warning device failed.

***When a radiation generating device is connected to the safety Interlock, the safety circuitry used within the device must be considered.***

Ultimately the safety interlock will be connected to the radiation source. In the case of X-ray equipment and powered wind-out systems for radioactive sources, the act of connecting this equipment to the interlock will form a new “machine”, which must then be compliant with the Machinery Directive. This new machine must also meet CE marking requirements.

If the component parts are of recent manufacture and are in themselves compliant, there should be no major problems. However, bearing in mind that control circuits inside the attached X-ray equipment or powered wind-out must also be category 4, some older systems will not comply; for example if they have only a single interlock line, hence no redundancy or monitoring.

It is also worth noting that equipment designed solely for site radiography use (i.e. not in a permanent enclosure) may not meet the aforementioned requirements because portable equipment is not covered by the machinery directive.

### **Additional Considerations**

- Both IRR99 and The Machinery Directive require that there must be no automatic restart after activation of the interlock. Some equipment that normally operates in this manner may still not comply with current circuitry design requirements. In these cases, additional measures will be required, such as introducing safety contactors controlled by the interlock which isolate the power to the X-ray production circuit if a failure is detected, or incorporating a manual reset button to be used after a door has been opened or an emergency stop operated.
- When powered wind-out equipment is used with radioactive sources, although its operation will be similar to that of X-ray equipment, a radiation detector should also be incorporated into the safety system. A system which indicates a safe condition merely when the drive cable has retracted could lead to a dangerous situation where the radioactive source has detached from the wind out mechanism, or the drive cable has broken, and the source is still exposed when the system ‘thinks’ otherwise.
- Manual radioactive source wind-out equipment is particularly difficult because the interlock cannot influence the operation of the wind-out. Under these circumstances the safety interlock system must have a radiation detector incorporated. Even then, the interlock would only be considered as a warning device. The enclosure should be automatically or manually locked off when radiation is present. Generally an interlock incorporating a physical trapped key system is the recommended method by which the enclosure is secured during radiation exposure.
- Although most new interlocks will be +24V powered, the interlocking signals of older equipment may be at mains potential, and therefore non-compliant with the 2006/95/EC Low Voltage Directive - which should be considered best practice.

This advisory note is by no means exhaustive. There are many other factors influencing the final design of a safety system which have not been covered, such as motorised access doors and the specific legislation relating to the use of these doors. Also, there is a requirement for ‘search and secure’ systems in high-energy radiation enclosures, or where an exposure room is large or has a complex shape. We recommend that contact is made with competent advisors at an early stage of planning and designing any radiation facility, thus avoiding problems that can prove difficult and costly to rectify retrospectively.