STSARCES

Standards for Safety Related Complex Electronic Systems

Annex 12

Applicability of IEC 61508 & EN 954

Task 2: Machine Validation Exercise

Final Report of WP4

Dr A M Wray

Health and Safety Laboratory

HSE

European Project STSARCES
Contract SMT 4CT97-2191

SUMMARY

Part ii of the "Divergences study" of Work Package 4 of the STSARCES (STandards for SAfety-Related Complex Electronic Systems) project is to examine the retrospective application of the EN 954-1 (Reference 1) and draft IEC 61508 (Reference 2) standards to existing machinery.

OBJECTIVES

To determine the links and divergences which are likely to exist between the requirements of EN 954-1 and IEC 61508 by carrying out a practical assessment of a machine.

MAIN FINDINGS

1)Machinery safety systems are not developed from scratch using a life-cycle approach. Instead, as a new machine is developed, the experience gained from previous machines is modified slightly in order to make improvements to the overall design. Hence, safety requirements are unlikely to be developed for any particular machine. Instead, the safety systems of new machines will be designed to be no worse than those of existing machines. The use of IEC 61508 will require a radical change to the machinery design/development process in that safety must be addressed using an absolute, rather than relative, approach.

2)IEC 61508 uses quantitative calculation of the overall failure rate as well as qualitative techniques, where insufficient information is available for a quantitative determination (e.g., for systematic failures), for determining safety integrity. EN 954-1 attempts to avoid the need for a quantitative calculation by using a simple methodology - the risk graph. Unfortunately, the application of the methodology is not straightforward in other than the simplest of systems, and requires a subjective application of engineering knowledge.

3)IEC 61508 covers all stages of the lifecycle of a system. EN 954-1 considers only the design (and validation of the design).

4)The greatest problem in using a quantitative approach to risk assessment, as described in IEC 61508, is the availability of suitable data. Two types of data are required:

v Failure rate data for the components and subsystems: It may be necessary to use data from generic components, or for outdated components; however, data can be obtained (or estimated) for most components, although it is likely that some assumptions may be necessary.

v Levels of acceptable risk: The level of acceptable risk is a societal parameter and is difficult to determine, being dependent on perceived, rather than actual, risk. The guidance in IEC 61508 uses the ALARP value but gives no help in determining what that value should be. The author made an assumption that existing hazard rates were acceptable but this assumption need not be valid in all cases. The author considers that this problem may present the most difficulty in using IEC 61508 until industry-specific guidance documents, based on IEC 61508, provide guidance in this area. However, the publication of such guidance could give alarm to those at risk.

5)A number of assumptions had to be made in order to carry out the quantitative analysis described in IEC 61508. These were subjective had a significant effect on the SILs. There may be a high dependence on basic (and possibly subjective) assumptions in the quantitative analyses of many other systems. Some of these assumptions will be difficult to challenge and could lead to failure-rate predictions being distorted to meet the needs of other agendas.

6)If a methodology, that will enable target SILs to be determined without significant subjectivity is not available, the uncertainty in the outcome of the quantitative analysis used in IEC 61508 may be large. In the author's opinion, the production of such a methodology should be given a very high priority otherwise it will not be possible to fully exploit the guidance provided by IEC 61508.

7)Generally, existing safety-related electrical control systems at machinery have not been designed using the guidance contained in IEC 61508 (of which all parts were not published at the time of writing of this report) and, as a consequence, suitable documentation, required in order to verify the various safety lifecycle stages, is not likely to be available. Documentation, in a form suitable for assessment purposes, will become available only when IEC 61508 gains credibility in machinery manufacture. Until this time, it will be difficult to carry out assessments of safety-related electrical control systems at machinery, especially in relation to the quantitative analysis.

8)IEC 61508 relies heavily on documentation to demonstrate that the various life-cycle stages have been carried out correctly and to allow following stages (e.g., validation) to be performed. At first sight, the documentation requirements for a simple machinery-control system appear to be excessive.

9)Because shortage/incompatibility of documentation may prevent an adequate determination of the qualitative measures when a retrospective examination is carried out on a machine designed prior to the publication of IEC 61508, it will not be possible to determine whether (or not) suitable measures have been put in place to deal with systematic failures. Therefore, a retrospective quantitative assessment using IEC 61508, may prove to be inaccurate as the actual failure rate may be dominated by systematic failures, which are unlikely to be predictable quantitatively. Unfortunately, this will lead to an underestimate of the failure rate, i.e., the estimate will indicate that a system will be safer than it actually is.

10)IEC 61508 takes a scientific approach to the matching of system integrity to risk. Wherever possible, it uses quantification, but uses qualitative measures where quantitative measures cannot be used. However, the qualitative measures have been determined (using engineering judgement) to be appropriate to the SIL. This should be compared with the approach taken by EN 954-1, which is arbitrarily based on fault tolerance in its entirety.

11)In the author's opinion, EN 954-1 was developed for relay-based systems as existed in the 1970s, an application for which it would have been ideal as it is simple to apply, and it would have led to in improvement in the safety standards at that time. Unfortunately, the standard has been overtaken by the technologies used in safety-related systems and it would be difficult to take into account: sophisticated automatic diagnostics; the use of systems which include different technologies having vastly different failure modes and reliabilities, and the use of software. The feature of the standard is its underlying simplicity; however, even in its present form, this simplicity has begun to be lost. If attempts are made to take these deficiencies into account, the simplicity of the standard will be completely lost, and it would be better to go directly to a standard, such as IEC 61508, designed to address these deficiencies from the outset.

12)This assessment has not proven to be an appropriate way of demonstrating the effectiveness of IEC 61508. The principles of IEC 61508 follow a methodology which encompasses all of the phases in the lifecycle of a system, e.g., concept, design, implementation, etc. If the methodology has not been used by the manufacturer, subsequent assessment using IEC 61508 will inevitably be difficult because of missing information. However, if IEC 61508 had been followed from the outset, the relevant information would have been available, facilitating the assessment.

CONTENTS

1 INTRODUCTION

Part ii of the "Divergences study" of Work Package 4 of the STSARCES (STandards for SAfety-Related Complex Electronic Systems) project is to examine the retrospective application of the EN 954-1 (Reference 1[1]) and draft IEC 61508 (Reference 2) standards to existing machinery.

The fundamental aim of the project was neither to assess, nor test, the machine, but to identify the differences between the approaches taken by the two standards. Therefore, the assessment is not carried out in unnecessary detail where this would not be beneficial to the aims of the project. (However, any problems that are encountered will be highlighted, where they occur.) For example, where the standards call other standards, the requirements of these other standards may not be considered. Because of this, the assessments described in this report should not be used as the basis for other assessments.

2 SELECTION OF THE MACHINE TO BE ASSESSED

The requirements for the safety-related control system to be assessed include that:

v it has sufficient technical complexity in the configuration of its control system(s) to allow sufficient application of either standard;

v it should include a programmable system;

v it is a practical application within an existing machine;

v the manufacturer, or its designer, should be readily contactable, if necessary, to elucidate design criteria or details of its operation, and,

v the manufacturer should be willing to co-operate with the project and to provide the necessary technical material to allow the assessment to be effected.

It was decided that a suitable machine for assessment would be a hydraulic press, manufactured in the UK. The anonymity of the manufacturer and actual machine designation will be maintained throughout this report as these are irrelevant to the outcome of the project. For example, documents, supplied by the manufacturer, have been suitably anonymized.

Technical details of the machine under examination are as follows:

v Multi-axis DNC controller

v Hydraulic operation, with individual servo control of the position of each end of the beam together with hydraulic pressure control

v Sizes from 30 to 3000 tonnes, specifically 100 tonnes on the machine examined

[1]

v Photoelectric curtain allowing normal photoelectric guarding[2] or guarding in association with single- or double-break stroke initiation.

The following information will be assumed for the purpose of the assessments:

v Stroke rate: 4 strokes/minute (when used in normal press-brake mode, estimated average)

v Maximum approach speed: 150mm/s

v Pressing speed: 10mm/s

v Return speed: 100mm/s

v Height of top-of-stroke position above tool: 200mm (estimated average)

v Stopping time: 90ms (manufacturers information - not measured)

1 OPERATION OF THE HYDRAULIC CIRCUIT

In order to provide a clear explanation of the operation of the electronic control system, it will be first necessary to explain the operation of the hydraulic circuitry that is shown in Appendix B.

There is a hydraulic ram at each end of the beam of the machine, which independently provide the motive power for the pressing and return strokes. These are controlled by two main hydraulic valves:

1)The Servo Valve. There is a separate servo valve for each cylinder. This are driven by servo amplifiers in the DNC in order to provide proportional control.

2)The Direction Valve. There is a separate direction valve for each cylinder.

1.1 Normal operation of the hydraulic circuit

Consider only the hydraulic circuitry associated with the Y2 ram, i.e., at the right-hand side of the diagram. It will be seen that:

1)With 18SVY2 and both 19WVPY2 and 19WVEY2 de-energized, both sides of the ram are isolated, so no movement is possible.

2)With the Direction Valve energized in the spool-left direction (i.e., solenoid 19WVEY2 energized), the Servo Valve (18SVY2) can control the descent of the beam under gravity (spool left). This is used to give a fast approach to the point at which the guard is muted. In this case, the flow of oil is as follows:

[2] A photoelectric system is colloquially referred to as a photoelectric guard, despite the fact that it does not prevent access to the danger area, and sometimes as an intangible guard. A more accurate term is an Electro Sensitive Protective Device (ESPD). However, as the term photoelectric guard is more commonly used and understood, this term will be used throughout this document.

v Oil flowing from beneath the piston cannot flow through AR2.2 but flows though AR1.2, through the Direction Valve (Port P to Port B), through the Servo Valve (Port P to Port B) and into the top of the cylinder.

v Because the direction valve has port A connected to Port T, CA 2 is open allowing oil to flow into the space above the system from the tank. This makes up the increased oil requirement resulting from the descent of the piston rod.

v Note that Valve CP will allow the output from the hydraulic pump to dump to tank during this process.

It will be seen that the servo valve can control the speed of descent, but the hydraulic pump is not required.

Only 2 valves need to be energized for a fast descent under gravity.

3)With the Direction Valve in the spool-right position and the Servo Valve controlling in the spool-right position, oil under pressure is applied to both sides of the piston. Valve CA.2 will be closed as a result of the connection between Ports A and B of the Direction Valve. The only source of the excess oil provided from the tank via CA.2 on the fast approach is now via the hydraulic pump. Therefore, irrespective of the position of the Servo Valve, the maximum speed of movement is determined by the swept volume of the hydraulic pump. In this case, the flow of oil is as follows:

v Oil flows from beneath the cylinder, via Valve AR.1.2, through the Direction Valve (Port P to Ports A [closing CA.2] & B).

v To this oil is added the flow from the hydraulic pump via AR.3.2. It is controlled by the Servo Valve (Port P to B) on its way to the top of the cylinder.

4)With the Direction Valve de-energized and the Servo Valve controlling in the spool-right position, the control input of CA.2 is connected to tank via Ports A & T of the Direction Valve, allowing oil from above the piston to flow to tank. Oil from the hydraulic pump is controlled via the Servo Valve and flows via AR.2.2 to the lower side of the piston, raising the beam.

1 THE ELECTRONIC CONTROL SYSTEM

The control system includes a complex Digital Numeric Controller (DNC) together with relay-based control providing a second channel for safety-related functions. Appendix A shows diagrams of the control system; however, only those diagrams that are relevant to this examination have been included.

Table 1 gives a description of the functions of some of the relevant components shown in Appendix A.

Table 1: description of the functions of the relevant components in Appendix A.

Relay identification	Function	Comment
18SVY1 18SVY2	Servo valves	Control the speed of both ascent and descent - one for each end of the beam
19WVEY1 19WVEY2	Direction valves: approach	Energized for gravity-powered descent - one for each end of beam

19WVPY1 19WVPY2	Direction valves: pressing	Energized for pressing stroke - one for each end of beam
11K1 11K2	Photoelectric guard: Output relays	Internally monitored by the guard
11K4	External mode select: Guard control	Guard control, single/double break
10K9	Down command: Channel 1	
10K8	Down command: Channel 2	
KRES1	Mute sequencing relay	
KRES2	Mute relay	
14K2 14K3 14K4	DNC output: Ram return	
14K6 14K6.1	DNC output: Mute point	
14K7	DNC output: TDC	
14K8	Synchro check	Energized if beam not parallel with horizontal
15K2	DNC output: OK	No primary safety function
15K3	Manual control	Energizes during manual control and mutes the p-e guard. The beam travel does not exceed 10mm/s.
15K7	Stopping-time test	No primary safety function
16K2	Auto ram return in sensitive mode	No primary safety function

1.1 Brief description of the operation of the control system

It should be noted that the author has details of neither the software nor the hardware of the DNC. For the purposes of this assessment, they will be treated as a single component.

The following sections briefly describe the operation of the control system in ensuring that the photoelectric guard prevents the machine making a downstroke and in ensuring that muting occurs only at the correct position.

1.1.1 Guard operation

The control section of the photoelectric guard is shown on the diagrams as 10A2 (LCU-P). The LCU-P is not the actual photo electric guard, but a control unit for up to 2 Type 4 guards or up to 4 Type 2 guards. Although the LCU-P allows normal, single-break and double-break operation, only its rôle in preventing machine movement will be considered as these are independent functions.

It will be seen that the two output relays of the guard are 11K1[3] and 11K2. Each of these has two sets of contacts: one set at 10.9[4], and, the other at 11.6. Those at 11.6 are used for monitoring the relays (failure of these contacts to close will cause the LCU-P to lock out) and those at 10.9 are the main guarding contacts.

The photoelectric guard used with the LCU-P and the LCU-P itself are shown as meeting the requirements of a Type 4 ESPE.

For the purposes of this assessment, the photo-electric guard will be assumed to be inviolate, and the assessment will consider the PES to extend from the guard contacts 11K1 and 11K2 at 10.9 (assumed to be the sensors of the PES) to the solenoids for the hydraulic valves (assumed to be the actuators). This will avoid any unnecessary and unproductive complexity.

It will be seen that the guard contacts have a contact of 15K3 in parallel with them. This is controlled by the MANUAL output of the DNC (15.3). A failure of the DNC such that it gives a MANUAL output would appear to bypass the guard contacts, leading to an unguarded stroke. However, it will be seen that the NC contact of 15K3 (10.9), will prevent the energization of 10K8 and 10K9 other than when the footswitch is depressed. Therefore, such a failure could mute the guard, allowing unguarded operation from the footswitch, or, potentially allow a (fast) gravity powered stroke, if accompanied by other DNC output failures, e.g., the outputs driving 14K6.1, 14K7, 14K6 & 16K8. However, it should be noted that a permanent failure of 15K3 would be identified as a failure to provide powered (pressing) strokes (See 10.9) and a permanent failure (to the energized state) of 14K6.1, 14K7 and 14K6 & 16K8 would prevent valves 19WVEY1 and 19WVEY2 from operating, precluding a fast approach (See 19.4.).

[3] The convention for relay numbering is (Sheet number - see bottom RHS of diagram)K(Number). For example, Relay 11K1 is the first relay to be numbered on Sheet 11

[4] The convention for component identification on the circuit diagrams is (Sheet number).(Horizontal co-ordinate). For example, The footswitch contact at 14.6 can be found on Sheet 14 at 6.

1.1.2 *Stroke initiation*

In the following description, reference to relay contacts not directly involved in stroke initiation, e.g., for monitoring purposes, will be omitted for clarity.

1)The operator presses the foot[5] switch. This has contacts at 10.8 and 11.8.

2)The contact at 10.8 causes 10K9 to energize, if the guard contacts 11K1 & 11K2 are closed (i.e., the photoelectric curtain is unobstructed) and the NC contact of KRES2 is closed (i.e., a check that the Mute Relay KRES2, is de-energized).

3)10K8 energizes via the NO contact of 14K1 at 10.8.

4)An NO contact of 10K9 gives an input to the DNC at 14.4.

5)The DNC energizes 14K1 and 14K5 allowing 19WVPY1 & 19WVPY2 to energize via the (already closed) contact of 10K9 at 19.3 (assuming the link at J11/13 to J11/12 is not in place).

6)The DNC provides an analogue output to 18SVY1 & 18SVY2, via the NO contact of 10K8. This analogue output is used to control the descent speed.

1.1.3 *Guard muting*

In the following description, reference to relay contacts not directly involved in stroke initiation, e.g., for monitoring purposes, will be omitted for clarity.

1)KRES2 controls guard muting, muting occurring when KRES2 is energized.

2)KRES2 must be de-energized before a stroke can be initiated, otherwise the NC contact of KRES2 at 10.8 will not enable power to the footswitch contact.

3)KRES2 is energized by the DNC output at 11.9 when the mute position is reached and when 11SA9 is closed. This can occur only if KRES1 is de-energized. (See the NC contact of KRES1 at 11.9, but note that, once KRES2 is energized, the state of KRES1 becomes irrelevant as a result of the NO contact of KRES2 at 11.9).

4)The press will stop at the mute position. When the footswitch is released, prior to it being pressed for a second time in order to initiate the pressing stroke, its NC contacts at 11.8 close, allowing KRES1 to energize and latch.

5)Both Inputs 35 and 37 of the LCU-P must be energized for muting to occur. These are energized by the KRES2 contact at 10.4 and the 14K5 contact at 10.2 (indicating approach at pressing speed), respectively.

2 THE HAZARDOUS EVENTS TO BE CONSIDERED

A full examination of the control system of the machine will neither be cost-effective nor yield applicable results additional to a limited analysis. Therefore:

[5] There are two foot switches fitted to the machine: the down footswitch and the up footswitch. As only the down footswitch is of relevance to this report, only it will be considered and for convenience, will be referred to as the footswitch.

v to avoid repetition in the analysis, the operation of the machine will be considered only in manual mode (i.e., neither single- nor double-break modes of initiation will be considered.)

v the most important hazards associated with the machine were determined in order to define the scope of the assessment. The hazardous events identified as being within the scope of the assessment are:

v Aberrant stroke: An uninitiated stroke occurs, which cannot be prevented by obscuring the photo-electric guard (referred to as an unguarded stroke).

v Incorrect mute: The muting position aberrantly changes so that muting of the photoelectric guard occurs with the tool more than 6mm above the workpiece or the guard fails in a dangerous mode.

v Failure of the rear-gate interlock: If this interlock were to fail, access could be obtained to the rear of the working parts of the machine.

It should be noted that the purpose of this assessment is to consider the rôle that the EN 954 and IEC 61508 standards may have in establishing the safety integrity of the electrical/electronic/programmable electronic (E/E/PE) control functions of the press (albeit through their retrospective application). Therefore, consideration of all hazards will not be cost effective, and so only a relevant selection of the hazards has been made - no other potential hazards will be considered.

The assessment will be carried out separately for each standard with the intention of minimizing the "cross-talk" between the assessments.

In order to make the assessments as realistic as possible, it has been decided to adopt an approach which will, as nearly as can be envisaged, follow that expected to be taken by a machinery designer who is faced with the use of the standards in a working environment, i.e., not necessarily as the designers of the standards would have intended.

1 ASSESSMENT USING EN 954-1

Reference 1 will be used for this assessment, and the step-by-step procedure described at Clause 4.3 of Reference 1 will now be followed.

1.1 Step 1 Hazard analysis and risk assessment

1.1.1 Identification of the hazards

Only the hazards previously identified will be considered. These apply only in the operational part of the lifecycle of the machine.

The hazardous events to be considered are:

v Hazardous Event 1: Aberrant[6] and unguarded stroke. It should be noted that:

v a movement of only one end of the beam is required for this hazardous event to occur.

[6] Note that this hazardous event does not include a normally initiated but unguarded stroke.

v the beam may descend either under power or under gravity - although less force is available under gravity, the approach speed is higher and the mass of the beam is sufficient to cause irreversible injury.

v Hazardous Event 2: Incorrect muting position including guard failure.

v Hazardous Event 3: Rear-gate interlock failure, i.e., the machine operates normally with rear gate open.

The first two of these hazards are applicable to normal operation and could lead to serious injury if they were to occur, for example, the amputation of both of the operator's hands.

The third hazard is applicable to maintenance, and could lead to similar levels of injury from both the action of the press or movement of the backgauge.

1.1.1 Assessment of the risk arising from those hazards

1.1.1.1 Hazardous Event 1

Although up to 15 strokes per minute may be used during "bumping", in order to allow one or both of the operator's hands into the tooling, the tool must be raised significantly above the workpiece. Therefore, it will be assumed that the press is used in normal press-brake mode with a stroke rate of about 4 per minute.

When using a pressbrake, it is not necessary for the operator to insert his hands into the tooling, and good working practice would ensure that he didn't. For the purpose of this assessment, it will be assumed that the operator must insert his hands between the tools only seldomly in order to retrieve the completed workpiece, there being sufficient material in front of the tools to allow the workpiece to be manipulated.

If injury occurs with a machine of this type, it is unlikely to be reversible, varying from the amputation of one or more digits to the amputation of one or both hands.

If the tool were to descend, in the author's opinion, the operator would not be able to withdraw his hand in order to avoid injury.

Use of the informative Annex B of EN 954-1 leads to the following:

v Severity = S2 (Injury irreversible);

v Frequency = F1 (Seldom to quite often);

v Possibility of avoiding injury = P2 (Scarcely possible), and

v a preferred category of 2 or 3.

1.1.1.1 Hazardous Event 2

If the programmed muting position were to change, such that the operator could put his hands between the tools with muting in operation, the hazard would not exist until the operator pressed the footswitch to initiate a stroke. Whilst an operator's hand may frequently enter the tooling, it is considered unlikely that he will deliberately press the footswitch with his hand there. Therefore, the rate of the hazard will be affected by the probability of the operator inadvertently pressing the footswitch with his hand between the tooling. It will be assumed that the probability of the operator inadvertently operating the footswitch, whilst one of his hands is between the tooling, is 0.1%. This leads to a potential hazard frequency of 0.06 per hour - see Annex 1.

Use of the informative Annex B of EN 954-1 leads to the following:

- Severity = S2 (Injury irreversible)
- Frequency = F1 (Seldom to quite often)
- Possibility of avoiding injury = P2 (Scarcely possible)
- A preferred category of 2 or 3.

1.1.1.2 Hazardous Event 3

Access will be required to the rear of the machine only infrequently, for example, to pick up a workpiece that has been dropped. Because of the automatic backgauge fitted to the machine that was examined by the author, it will be assumed that a workpieces are dropped no more frequently than once per day.

Maintenance must be carried out within the rear of the machine; however, this should be carried out using a safe system of work, i.e., whilst the power to the machine is isolated. The contribution of such a safe system of work (as an external risk-reduction measure) to risk reduction has not been fully evaluated as part of this research.

Use of the informative Annex B of EN 954-1 leads to the following:

- Severity = S2 (Injury irreversible)
- Frequency = F1 (Seldom)
- Possibility of avoiding injury = P1 (Possible under specific conditions)
- A preferred category of 1 or 2.

1.2 Step 2: Decide measures for risk reduction by control means

As the standard is being applied retrospectively, it is inappropriate to decide on any necessary risk reduction measures. Instead, those parts of the control system already in place, which, if they failed, could lead to the hazardous events, will be determined.

1.2.1 Hazardous Event 1

In order better to understand the events leading to the hazardous event, a fault tree has been drawn. This is shown in Appendix C as Figure C.1.

It will be seen that, in order for the beam of the machine to make an aberrant and unguarded stroke:

- two[7] hydraulic valves must simultaneously be open, and
- no single component failure can cause both of these valves to be open.

[7] Clearly, two valves must be open at each end of the machine, making 4 in total. However, as they effectively operate in pairs, this report will consider only one end of the beam.

The reader should note that a hydraulic press is unusual in that, as a general rule, an aberrant stroke will put the machine into a safe state. For example, a failure leading to a descent of the beam will leave the beam at the bottom of its stroke, and, assuming no further failures occur, the beam will not move from this safe position. This should be compared to a mechanical press where a similar failure could lead to the press continuing to cycle.

1.1.1 Hazardous Event 2

The fault tree shown in Appendix D as Figure C.2 applies to this event. It will be seen that, for Hazardous Event 2 to occur, Relay KRES2 must be in the energized state during the downstroke and Relay 14K5 must be energized or, either of these must be energized together with 16K2, 14K7 or 14K3. This can be the result of combinations of:

v early energization of KRES2 (It should be noted that 11SA9 prevents the photoelectric curtain being muted. Switching 11SA9 to the open-circuit position is used to prevent muting in those applications where muting is not required.);

v a failure of KRES2 to the energized state;

v contacts 25/26 of KRES2 failing to the closed state;

v a failure of 14K5 to the energized state, or

v a failure of the contacts which can bridge Inputs 35 and 37 of the LCU-P i.e., 16K2, 14K7 or 14K3. (See 10.3.)

Each of these faults will now be discussed.

1.1.1.1 Early energization of KRES2

A failure of the DNC could lead to early energization of KRES2 (assuming that muting has been manually enabled by means of 11SA9) which will provide a signal to Input 35 of the LCU-P. However, a second failure is required to energize Input 37 of the LCU-P and cause it to mute the guard. In the absence of any detailed information regarding the DNC, the DNC will be treated as a generic PES in regard to its failure rate.

1.1.1.2 Failure of KRES2 to the energized state

One must consider how KRES2 can fail. Like any other relay, it is highly unlikely to change from the de-energized state to the energized state without a source of power, i.e., without being energized. Therefore, the only credible failure to the ON state is for it to remain stuck in the energized state following its de-energization, i.e., the guard is muted normally, but KRES2 fails to return to the de-energized state after the stroke. If this were to occur, the normally closed contacts (21/22 at 10.8) would not close, preventing the energizing of 10K8 and 10K9. Therefore, no further stroke can be initiated, so the failure will not lead to an unguarded stroke. As a result, a failure of KRES2 to the energized state will be discounted from the analysis.

1.1.1.3 Contacts 25/26 of KRES2 failing to the closed state

KRES2 is a guided-contact relay manufactured by Hengstler, which means that a short-circuit failure (i.e., due to welding) of contacts 25/26 will be detected by the monitoring of the normally closed contacts. As a result, a failure of contacts 25/26 of KRES2 to the closed state will be discounted from the analysis.

1.1.1.4 Failure of 14K5 to the energized state

14K5: If this relay fails to the energized state, contact 11/12 at 18.8 will fail to close, preventing the pressure valve from energizing on the return stroke, leading to the beam remaining at the bottom of the stroke. (Once again, an unpowered energization of the relay is considered to be incredible - only a failure to de-energize is considered to be likely.) In addition, contact 21/22 will remain open, preventing fast down movement (19.4) and cause all downward movement to be at pressing speed.

1.1.1.5 Failure of the contacts which can bridge Inputs 35 and 37 of the LCU-P

If the contacts of 16K2, 14K7 or 14K3 at 10.3 fail to the closed state, Inputs 35 and 37 of the LCU-P will become connected. Therefore, a failure of either KRES2 or 14K5 will energize both inputs, leading to aberrant muting of the photoelectric guard. The short-circuit failure of single contacts of these relays will be neglected. Each of these failures will now be considered in turn:

v 16K2: A failure of this relay to de-energize will be detected by the LCU-P via contact 11/12 (11.6).

v 14K7: If this relay fails to the energized state, contact 21/22 will prevent fast down movement (19.4) and cause all downward movement to be at pressing speed.

v 14K3: If this relay fails to the energized state, contact 11/12 (11.8) will prevent pressing beyond the mute position.

1.1.1.6 Failure of the DNC

A failure of the DNC could lead to early energization of KRES2 (assuming that muting has been manually enabled by means of 11SA9); however, this would not mute the guard unless 14K5 were also energized.

A failure of the DNC could result in both KRES2 and 14K5 being in the energized state; however, this will result in downward motion being at pressing speed (10mm/s), i.e., there would be no fast approach.

1.1.2 **Hazardous Event 3**

The interlocking of the rear gate operates via the emergency-stop circuit (10.6). It will be seen that power for operating this circuit comes from the LCU-P, via the rear-gate interlock switch, the emergency-stop switches, the latching/reset contacts and drives 10K6 and 10K7.

In normal use, 10K6 and 10K7 are latched via contact 23/24 of 10K6. Any momentary loss of power, as would occur if the rear gate were opened, will result in these relays de-energizing and remaining de-energized until manually reset.

[Author's note: On the circuit diagrams, Contacts 11/12 of 10K6 and 11/12 of 10K7 are shown as being normally open. This is an error; they should be shown as being normally closed.]

Under emergency-stop conditions, or when the rear gate is open:

v Contact 13/14 of 10K6 disables the DNC outputs. *[Author's note: The documentation suggests that this may be the case but, as no details of the DNC are available to the author, the author has no definitive evidence as to whether the DNC outputs are disabled by removing* *the 24V supply to them (preferred), or via logic within the DNC. He has, however, been given verbal conformation that the former is the case and so this will be assumed in this assessment.]*

v Contacts 15/16 of 10K6 and 13/14 of 10K7 disable the X and X1 axes for workpiece positioning (sheets 4 & 5 of the diagrams are not included in Appendix A).

v Contacts 15/16 & 23/24 of 10K7 disable Z1 and Z2 axes for workpiece positioning (sheets 8 & 9 of the diagrams are not included in Appendix A).

v Contact 21/22 of 10K6 and contact 21/22 of 10K7 will prevent the hydraulic pump motor from **starting**, but will **not** stop the motor. Therefore, hydraulic power is available with the rear gate open.

v Contacts 25/26 of 10K6 will prevent the beam rising when the footswitch is released, via the DNC.

The fault tree shown in Appendix D as Figure C.3 applies to this event. Note that:

v a short-circuit failure of the reset-rear-gate switch, 10SB2, has been omitted. This is because this failure will not result in the machine operating with the rear gate open, the definition of Hazardous Event 3.

v No attempt has been made to individually consider the various hazards present at the rear of the machine.

It will be seen from Figure C.3 that, for Hazardous Event 3 to occur, either:

v relays 10K6 and 10K7 must fail to the energized state (For the purposes of this assessment, these will be considered to be a single relay.), or

v the rear-gate switch, 10S5, must fail to the ON state.

1.1 Step 3: Specify safety requirements for the safety-related parts of the control system

An assessment is being carried out, so it is inappropriate to specify the safety functions to be provided by the control system. However, we can identify the Category appropriate to the various parts of the control system at this stage.

In some cases, the author has looked at the components providing protection against the hazardous events as systems rather than individual components. This is because a higher (and, in the author's opinion, more appropriate) Category is applicable where monitoring of a number of components is carried out by, for example, monitoring the state of the final component in a chain of components.

1.1.1 Hazardous event 1

1)In the author's opinion, "well-tried safety principles" have been used in the design of the control system.

2)The fault tree at Figure C.1 shows that a single component failure cannot lead to an aberrant and unguarded descent of the beam.

3)What the fault tree does not show is that:

v the DNC controls the servo valves at each end of the beam separately and independently monitors the position of each end of the beam. If a failure resulted in the beam losing parallelism with the bed of the machine, the machine would be automatically halted by the DNC. Therefore, all non-DNC failures, which could result in the loss of parallelism (e.g., the servo valves, their control or one of the direction valves) will be revealed before they can become dangerous.

v a failure of the drive to the direction valve will not lead to a movement of the beam. However, a failure of the direction valve (or its drive), will prevent the normal operation of the press, e.g., a failure to return to stroke-top after a pressing stroke.

Therefore, a single failure will be detected. In addition:

v the DNC is carrying out many functions on the press. Therefore, the vast majority of internal failures will be detected as a result of other functions failing. These will be obvious to the user.

v if a failure of an output of the DNC occurs, this is unlikely to be intermittent and will lead to the output having a high probability of failing to a permanent ON condition, i.e., the dangerous direction.

v the DNC is likely to incorporate internal diagnostics; however, this has not been verified.

v a dangerous failure of the relays 10K9, 10K8 or 15K3 (i.e., to the energized state) is an unlikely mode of failure. The most likely cause of a relay failing to the ON state is the contacts welding. As the loads driven by these relays are relatively small, **and known to the designers**, such a failure is considered to be unlikely. In addition:

v a permanently energized failure of 10K9 will be detected via the relay monitoring input of the LCU-P at 11.5.

v a permanently energized failure of 10K8 will be detected via the relay monitoring input of the DNC at 11.5.

v a permanently energized failure of 15K3 will be detected because a fast approach will not be possible. (The NC contact at 10.9 must be closed for fast approach, i.e., before KRES2 energizes at the mute position.)

From the above, it is considered that the overall control system (rather than individual parts of the control system) meets the requirements of Category 4 with regard to Hazard 1.

1.1.1 Hazardous event 2

1)In the author's opinion, "well-tried safety principles" have been used in the design of the control system.

2)Figure C.2 shows if one of 14K3, 14K7 or 16K2 fails to the energized state, together with 14K5 or KRES2, muting will occur. However,

v if 14K5 fails to the energized state, the descent speed will be slow at all times and the beam will not rise. Therefore, this failure will be revealed during the first stroke in which it occurs.

v if 14K3 fails to the energized state, KRES1 will not energize at 11.8 to enable pressing speed, so the fault will be detected at the end of the stroke.

3)A failure of KRES2 to the energized state has been discussed. This will prevent any subsequent strokes so the failure must occur during the same stroke in which a person is at risk.

4)A short-circuit failure of Contact 25/26 of KRES2 has been discussed. This is considered to be incredible.

5)KRES2 and 14K5 may simultaneously be energized by the DNC. If the DNC energized BOTH of its outputs driving these relays, muting would occur; however, this would lead to all downward movement being at pressing speed (10mm/s) **and** no further strokes would be possible.

From the above, it is considered that the overall control system (rather than individual parts of the control system) meets the requirements of Category 2 with regard to Hazard 2. (To come to this conclusion, one must regard the DNC as a single complex component. If the DNC were not regarded as a single component, Category 4 may be more appropriate.)

1.1.1 Hazardous event 3

Single-channel interlocking is used for the rear-gate interlock; it is considered that the overall control system (rather than individual parts of the control system) meets the requirements of Category 1.

1.2 Step 4: Design

Because an assessment is being carried out, this step is not applicable.

1.3 Step 5: Validation

The categories attained by the systems for the three functions are compared with the target categories determined from the risk assessment in Table 2.

Table 2: Comparison of target and achieved categories

	Hazardous Event 1	Hazardous Event 2	Hazardous Event 3
Category required	4	2/3	1/2
Category achieved	4	2	1

Table 2 indicates that the control functions of the machine achieve the categories required for compliance with EN 954-1.

This report describes an assessment, not proof testing of the safety systems, and so is based on documentation, not the testing of a machine. Because the control system of the machine was not designed in the UK, access to design documentation, which could have indicated the degree of validation, is not available to the author. However, the author was supplied with a 36-page checklist used for verifying: the quality of manufacture; that the machine operated correctly following its manufacture, and that the safety functions were present.

1.1 Discussion regarding the application of EN 954-1

1)The standard is intended to be applied during the design of a control system, and not during an assessment. As a result, some of the steps in the methodology are inappropriate.

2)The standard does not have an underlying principle which follows from start to finish. Instead, there is a large number of minor requirements and 'give aways'. For example, the fundamental requirements of the various categories are simple to follow and relate to fault tolerance. However, having established the requirements for Category 3, for example, one finds that it is not necessary to detect ALL single faults but only SOME. (See Table Guide to the categories for safety-related parts of control systems from EN 954-1, in Reference 3.) A subjective decision must be taken as to which faults need, or do not need, to be detected.

3)EN 954-1 has been designed as a standard with a practical means of assessment and implementation. Unfortunately, what appears at first sight to be a very practicable method (i.e., based on a simple analysis of fault tolerance), becomes very subjective when applied. For example, before the author used Informative Annex B to carry out a risk assessment (6.1.2.1), he considered that once per minute was quite frequent, This would have meant an allocation of F1. However, after careful, but highly subjective, consideration, he decided to allocate F2. Similarly, estimating the "possibility of avoiding the hazard" (i.e., by the operator noticing an impending hazard and withdrawing his hand) is more like guesswork than subjective judgement. More detailed advice could have been given to users of the annex. For example, research could have established the probability of the operator avoiding hazards in a variety of industrial applications and under varying conditions (e.g., approach speed) and the data tabulated in the standard.

> Annex B of EN 954-1 is the only way of determining the required Category for a system, other then by examining an existing system, (which itself may not have been categorized correctly). Because of the subjective nature of Annex B, different assessors may come to different conclusions when determining the category as there is no absolute means of objectively determining the category required for any particular system.

4)Although BS EN 1050 (Reference 10) provides advice on risk assessment, it provides little, if any, guidance regarding the determination of risk in a non-subjective or (pseudo-) quantitative way. Therefore, the user of EN 954 is left with no guidance on the determination of risk other than that provided in Annex B. Even though Annex B is described as being an informative annex, in the absence of another methodology, users have no alternative but to treat Annex B as if it were normative. Therefore, for all intents and purposes, Annex B is a normative annex, and has been used as such in this assessment.

5)The principles of EN 954-1 are based on single/multiple component failures leading to a hazard being realized. This, at first sight, seems to be a very simple way of defining the integrity of the safety functions. However, the examination of the control system indicates that there are many component failures which, in combination, could lead to the hazard. Many of these failures are considered to be unlikely, highly unlikely or even incredible. The decision to exclude such failures from the analysis is a subjective task, making what appears, at first sight, to be a simple and objective methodology both difficult and subjective. In this respect, the standard, in effect, replaces reliability calculation with subjective judgement.

6)Because the requirements of EN 954-1 are somewhat vague, for example, in determining which faults may be excluded from an assessment, the independence of any validation may be compromized because of the need for the assessor to exclude exactly the same components.

7)EN 954-1 gives no means of assessing or ensuring the integrity of software.

8)The press may (or may not) have been designed using the principles of EN 954-1, and validated to its safety specification; however, neither a validation report (as described at Clause 8.5 of EN 954-1) nor the technical construction file were made available to the author.

9)EN 954-1 mentions maintenance, but does so very weakly. In any safety-related protection system (which may be called to operate only infrequently), regular manual proof testing (in the absence of automatic diagnostics) is an important factor in maintaining the integrity, which will vary approximately linearly with the frequency of the manual proof checks.

10)EN 954-1 is a design standard, so does not give advice on the manufacture of the system being designed. A well-designed system that is sloppily manufactured could have a reduced integrity. (For example, a multi-channel system, whose wiring has been designed to be kept separate in order to avoid common-cause failures, could have the wiring strapped together as a single loom leading to a potential for common-cause failures.) Surprisingly, advice is given regarding maintenance at Clause 9. (It should be noted that the validation stage, e.g., type testing, cannot account for variations between manufactured items resulting from, for example, a poorly specified manufacturing stage.)

11)By assuming that subsystems are single components and applying the fault exclusion principle, it is possible to determine a Category without the need for complex calculation. However, the failure rate of a complex subsystem may be considerably higher than that of a single component. Therefore, the Category of a dual-channel subsystem cannot be considered equivalent to a dual-channel system at the component level, e.g., an interlock based on 2 relays cannot be compared with one based on two complex PLCs, even if both interlocks achieve Category 3. Hence, two systems, each having the same Category, may be considered to be equivalent **only** if they use the same technology and a comparable number of components.

12)A number of factors will considerably distort the hierarchy of Categories. (Although the standard clearly states otherwise, it is inconceivable that the hierarchy was not developed on the basis that a monotonic relationship exists between the integrity and the Category.) For example:

v the standard is based on system behaviour in the presence of faults. Modern technology allows the incorporation of sophisticated automatic diagnostics with a coverage approaching 100%. A single-channel system with sophisticated diagnostics may have a higher integrity than a crude multi-channel system. Although the standard allows faults to be excluded, it does not give advice on how this problem should be addressed.

v a highly reliable system, based on simple technology (e.g., a mechanical scotch) and (because of its single-channel status) having a Category of 1, may in practice have an integrity comparable, or even higher than, that of a Category 4 system employing a complex and, therefore, difficult to assess technology.

13)The categories used to define the integrity of a system are based on fault exclusion. This is an arbitrary means of defining the probability of failure on demand and takes no account of the frequency of such failures, which could be vastly different for alternative technologies. The methodology is workable only if all components use the same technology.

14)Because of the subjective means of determining the required Category described in Informative Annex B, it is not very difficult to justify a change of the Category by one either up or down in order to suit other (e.g., commercial) requirements.

15)In the author's opinion, the standard was developed for relay-based systems as existed in the 1970s, an application for which it would have been ideal as it is simple to apply, and it would have led to an improvement in the safety standards at the time. Unfortunately, the standard has been overtaken by the technologies used in safety-related systems and it would be difficult to take into account: sophisticated automatic diagnostics; the use of systems which include different technologies having vastly different failure modes and reliabilities, and the use of software. The feature of the standard is its underlying simplicity; however, even in its present form, this simplicity has begun to be lost. If attempts are made to take these deficiencies into account, the simplicity of the standard will be completely lost, and it would be better to go directly to a standard designed to address these deficiencies from the outset.

1 ASSESSMENT USING IEC 61508: QUANTITATIVE EXAMINATION

IEC 61508 follows a comprehensive lifecycle approach in which many of the stages are appropriate to design and not to a retrospective assessment. The full lifecycle consists of the following stages: Concept; Overall scope definition; Hazard and risk analysis; Overall safety requirements; Safety requirements allocation; Overall operation and maintenance planning; Overall safety validation planning; Overall installation and commissioning planning; Safety-related systems realisation; Non-PES systems realisation; External risk reduction systems realisation; Overall installation and commissioning; Operation; Overall modification and retrofit, and Decommissioning or disposal. All stages will be considered in this assessment, and it will be decided at each stage whether this is inapplicable to a retrospective assessment.

In order to avoid repetition, the analysis already carried out for the assessment using EN 954-1, and described in Section 6, will be referred to wherever possible.

The assessment to be carried out is an assessment of the design of the machine, and not an assessment of the documentation for the machine indicating the integrity of either its design or manufacture, e.g., documentation indicating which quality control procedures had been implemented during the machine's development. However, most of the information used in the assessment was obtained from technical documentation supplied by the manufacturer.

This quantitative analysis will be carried out according to IEC 61508 (Reference 2) Parts 1 & 2; the remaining parts will be considered in Section 8 of this report.

1.1 Concept

Clearly, the design of the press will not be conceived as part of this assessment; however, this is an important stage in an assessment. It allows the assessor to become familiar with the design and operation of the system being assessed. As the author has already examined the control system for his assessment using EN 954-1, this stage will be considered already to have been completed - the reader is directed to Sections 3, 4 & 6 of this report which summarize the design of the machine.

1.2 Overall scope definition

This stage is intended to determine the boundary of the control system and the equipment it controls. However, in terms of evaluating the application of IEC 61508 to an existing machine, this stage can be used to determine the boundary of the assessment.

In the case of the assessment being described, the assessment will be limited to the 3 potential hazardous events that have already been described (See Section 5):

v Hazardous Event 1: Aberrant and unguarded stroke.

v Hazardous Event 2: Incorrect muting position including guard failure.

v Hazardous Event 3: Rear-gate interlock failure - machine operates with rear gate open.

1.3 Hazard and risk analysis

Several parameters are calculated in the tables within this report, which are ignored in subsequent calculations. These have been included to provide additional information to the reader.

1.3.1 Identification of the hazards

The hazards have already been identified - see Section 6.11.

1.3.2 Assessment of the risk arising from those hazards

Because the press being considered was designed prior to the publication of IEC 61508, no target Safety Integrity Levels (SILs) have been identified for the various safety functions carried out by the control system of the press. In the absence of these SILs, retrospective application of IEC 61508 is difficult. To overcome this problem, the author has proposed a method of SIL estimation to allow the assessment to proceed. This method is based on general information on accident rates involving presses within the UK but is not specific to any particular safety function, assumptions having to be made in order to provide an estimate of these. Because of these subjective assumptions, the results of the calculations based on them should not be used as a basis for further assessments.

Because the aim of this assessment is to compare the use of References 1 and 2, the actual values used in the quantitative calculations of this assessment are of a lesser importance than the procedures that have been used. Therefore, in order to minimize the intrusion of the calculations into the main body of this text, details of the calculations are shown in the annexes, starting with Annex 1 which shows the determination of the probability of the hazard being realized, assuming the relevant safety-related function fails.

1.4 Overall safety requirements

The author was not supplied with details of the overall safety requirements specification for the machine in a form compatible with IEC 61508. IEC 61508 requires that safety requirements are expressed in terms of safety functions; however, as the machine had been designed prior to the publication of this standard, one would not expect the safety requirements to be expressed in this way. The author would expect suitable documentation to be available for (future) machines whose designs take the requirements of IEC 61508 into account.

In the absence of safety requirements specification, the author has two choices for determining the target safety integrity level:

v calculate the safety integrity level of some other machines and use these as a benchmark, or

v estimate, or assume, an ALARP[8] level for the risk associated with each of the hazards.

The reader is reminded that the purpose of this assessment is not to provide an absolute assessment of the machine, but to compare the two standards, and it is not necessary to determine a meaningful ALARP level for this. Therefore, although the determination of the ALARP level described in Annex 2 is not considered to be unrealistic, the ALARP value should **not** be considered to be a recommended value for the assessment of other machines.

Annex 2 uses accident data to estimate the frequency of accidents associated with each of the hazardous events under consideration. For the purposes of this report, the existing accident frequency will be considered to be ALARP and will be used to obtain the target SIL for the functions of the machine's control system used to prevent each of the hazardous events.

It should be noted that appropriate accident data in a suitable form for calculating the mean accident rate for a particular type of machine may not readily be available. Consequently, it may not be possible to use this approach in other assessments.

1.1 Safety requirements allocation

Because an assessment is being carried out, on a single control and protection system no allocation of risk reduction between the various safety-related systems is possible.

1.2 Overall operation and maintenance planning

This section is not applicable to an assessment. However, the opportunity will be taken to examine the test/maintenance recommendations provided by the manufacturer in the instruction manual for the machine. Only those aspects affecting the safety integrity level of the control system will be listed:

v Daily:

v Using the test rod provided with the machine, test the operation of the light-curtain.

v Interlocking of rear door to beam or backgauge movement.

[8] ALARP = As Low As Reasonably Practicable

v Weekly:

v Functioning of all safety systems

v Function of rear and side safety doors

v Annually:

v Electrical cabinet (by a specialist, e.g., an engineer employed by the manufacturer)

These test/maintenance checks will be assumed to be carried out and act as proof checks to the relevant systems. Following a proof check, it will be assumed that all defects have been corrected and the relevant system is operating as defined by its specification. The intervals between these checks will be used as the relevant proof-test intervals in the reliability calculations.

1.1 Overall safety validation planning

Not applicable to an assessment which can examine only the output from this stage.

1.2 Overall installation and commissioning planning

Not applicable to an assessment which can examine only the output from this stage.

1.3 Safety-related systems realization

It should be noted that this stage will be subdivided during the development process (See Part 2 of IEC 61508); however, as this assessment can consider only the outputs from this stage, such division will not be considered.

The aim of this stage is the creation of a safety-related system meeting the requirements of the safety integrity levels defined earlier. However, because an assessment is being carried out, this stage will be used to determine the integrity of the existing safety-related system with respect to the three hazardous events selected for the assessment.

The failure rates used in this examination are for components thought to be similar to those used in the control system of the press and are based on the data in Reference 5. The author has no detailed firsthand knowledge of the components used in the press, but has used his experience/knowledge to provide a best estimate of the failure rate of the various components.

The calculations of the SIL achieved by each of the safety-related functions associated with hazardous event are shown in Annex 3. These are based on the information contained in the following subsections.

1.3.1 Hazardous Event 1

As with any reliability assessment, the operation of the system being assessed must be taken into account so that any confirmation of correct operation, as a result of diagnostics or normal operation, can be correctly allowed for, as these may not be obvious from the fault tree.

The failure considered is not a powered stroke (which would be slow), but relies on the beam falling under gravity, i.e., in fast-approach mode. The weight of the beam is sufficient for a fall under gravity to cause an amputation. An additional failure involving the pressure valve would be required for a powered stroke.

An analysis of the fault tree leads to the six minimum cutsets shown in Table 10, each of which could lead to Hazardous Event 1.

Table 3: Cutsets leading to Hazardous Event 1

Cut set	Primary events			Comment
1	10K9	DNC	-	
2	Direction Valve	DNC	-	
3	Direction Valve	Servo Valve	-	
4	15K3	DNC	Footswitch	Discounted, see 7.9.1.1
5	10K9	Servo Valve	10K8	Discounted, see 7.9.1.2
6	15K3	Servo Valve	Footswitch	Discounted, see 7.9.1.1

Each of the primary events will now be discussed:

1.1.1.1 Footswitch/15K3

A failure of the footswitch contact to the closed state at 10.8 must be accompanied by a failure of 15K3 to the energized state in order to cause 10K8/10K9 to become energized. If 15K3 fails closed, there will be no fast approach, the speed being limited to 10mm/s or less. Assuming a stroke of 200mm and a hand width of 50mm, the aberrant stroke would take 15 seconds before the operator's hand became trapped. The probability of injury being avoided under these circumstances would be high. (The operator's hands would be under the beam for only two seconds and so would have to be inserted within 2cm of the crushing point. It is inconceivable that the operator would not notice that the gap between the tools was only slightly wider than his hands.) Therefore, cutsets involving a failure of 15K3 (and, therefore, the footswitch) will be neglected in the calculations.

1.1.1.2 10K8 or 10K9

Both of these relays are checked prior to each pressing cycle by the LCU-P. Therefore, for **either** to have failed, the failure must have occurred **after** the start of the previous normal pressing stroke, i.e., within 15 seconds.

It is possible that a relay can remain in the energized state following its coil being de-energized. However, it is highly improbable that the relay will change from the de-energized state to the energized state without the application of external power.

Such a failure of **either** of these valves is considered to be unlikely, however, a failure of **both** 10K8 and 10K9 is inconceivable, so will be neglected.

1.1.1.3 DNC

The author has no details of the DNC nor its software, so is not aware of the internal diagnostics implemented within it. In the absence of such information and for the purposes of this assessment, it will be assumed that the level of diagnostics meets the requirements of

'Low' as defined in Appendix A of Part 2 of IEC 60508, i.e., a diagnostic coverage of only 60%. (Such a level of diagnostic coverage is likely to be achieved by the execution of the normal control functions of the DNC, which will either fail, preventing the operation of the press, or indicate the presence of a fault to the operator. The author has no information regarding the coverage of the automatic diagnostics carried out by the DNC; however, in the absence of any information to the contrary, and for the particular aim of this assessment, an assumption of 60% is not considered to be inappropriate.) For convenience, it will be assumed that the diagnostic cycle is repeated at no more than the stroke frequency, i.e., at 4 times per minute. Therefore, a dangerous DNC failure is unlikely to be detected until a stroke has been initiated.

This means that it may be too late to prevent a DNC initiated press failure; however, none of the Hazardous Events may be initiated by a failure of only the DNC. Because the failure of an additional non-DNC component is required in order to reach a Hazardous Event, the checking will ensure that the (detectable) faults within the DNC will not remain latent until a failure of the non-DNC component occurs.

1.1.1.4 Direction valve

A failure of the direction valve to the fast approach position will result in the beam being held up by the servo valve. Servo valves, designed for fast operation without sticking when powered by an amplifier, have large clearances, so tend to have a high leakage. Therefore, a failure of a direction valve to the fast approach state will result in one end of the beam descending at about 3 to 5mm/second for about a second before the DNC recognises that the beam is not horizontal. At this point, the DNC will command the relevant servo valve to raise the offending end of the beam.

The movement may not immediately be noticed by the operator and the press will operate, apparently as normal, in the presence of the fault. It will be assumed that the fault will be noticed, but the machine will continue to be used, and it will take a week before a maintenance engineer is able to attend in order to effect a repair.

1.1.1.5 Servo valve

If the direction valve were to fail in the down state, the beam would not return from the previous stroke. Therefore, any spontaneous failure must require the servo valve to revert from the off state to the down state. This could be the result of a seal or manifold failure.

A significant leakage past the servo valve would be detected during a normal stroke as it would lead to one end of the beam moving at a different rate to the other. (A coincidental, **and identical**, failure of both servo valves is highly unlikely.) As soon as the deviation exceeds 1.5cm, the DNC will put the press into STOP mode. Therefore, any failure of the servo valve must occur since the previous pressing stroke, i.e., within 15 seconds.

1.1.2 Hazardous Event 2

Table 4: Cutsets leading to Hazardous Event 2

Cut set	Primary events	Comment

1	KRES2	14K5	KRES2 must be in the de-energized state prior to a normal downstroke. Spontaneous failure from de-energized to energized state at any time is extremely unlikely (see 6.2.2.2). To cause Hazardous Event 1, KRES2 must revert from the de-energized to the energized state during the normally initiated stroke. No random failure mechanism for this can realistically be identified so Cutsets 1 to 6 will be discounted.
2	KRES2	16K2	
3	KRES2	14K7	
4	KRES2	DNC2	
5	KRES2	14K3	
6	KRES2	23/24	
7	25/26	14K5	Contacts 25/26 of KRES2 have a low-power load so welding is unlikely. In addition, a guided-contact relay is used, ensuring that the contacts must be open-circuit at the start of any normally-initiated stroke (See Row 1). Spontaneous failure from de-energized to energized state at any time is extremely unlikely; therefore, Cutsets 7 to 12 will be discounted.
8	25/26	14K7	
9	25/26	DNC2	
10	25/26	14K3	
11	25/26	23/24	
12	25/26	16K2	
13	14K5	14K7	14K5 must be de-energized to allow the previous return stroke. Spontaneous failure from de-energized to energized state at any time is extremely unlikely see 6.2.2.4. If 14K5 were energized, fast approach would not be possible, speed being limited to 10mm/s allowing the operator to avoid injury. Therefore, cutsets 3 to 16 will be discounted.
14	14K5	14K3	
15	DNC1	14K5	
16	14K5	16K2	
17	DNC1	23/24	Contacts 23/24 of 14K5 have a low-power load so welding is unlikely. In addition, a guided-contact relay is used, ensuring that the contacts must be open-circuit at the end of the previous stroke (See Rows 13-16). Spontaneous failure from de-energized to energized state at any time is extremely unlikely; therefore, Cutsets 17 to 20 will be discounted.
18	23/24	16K2	
19	23/24	14K7	
20	23/24	14K3	

21	DNC1	14K7	The tests applicable to KRES2 apply to the output of the DNC, which drives it (11.9). Therefore, for this output of the DNC to affect muting, it must fail during the **same** downstroke that the operator inadvertently initiates a stroke with his hand under the tool. 14K7 must be de-energized for a fast approach (19.4). Therefore, even though this may be energized by the DNC, the cutset will be discounted as the operator will have a significant chance of avoiding injury due to the low (10mm/s) approach speed. 16K2 must be de-energized to enable the previous return stroke. Spontaneous failure from de-energized to energized state at any time is extremely unlikely; however, 16K2 could be energized as a result of a failure of the relevant DNC output during the **same** downstroke that the operator inadvertently initiates a stroke with his hand under the tool 14K3 could remain energized following the previous return stroke. However, it must have been energized at the time of the previous pressing stroke. 14K1 must be energized on the downstroke, therefore, a DNC failure cannot cause 14K3 to remain energized (14.2).
22	DNC1	16K2 □	
23	DNC1	14K3 □	
24	DNC2	14K3	The tests applicable to 14K5 apply to the output of the DNC, which drives it (14.4). Therefore, for this output of the DNC to affect muting, it must fail after the completion of the return of the stroke **previous** to the stroke which the operator inadvertently initiates with his hand under the tool. In addition, if this output of the DNC failed to the ON state, fast approach would not be possible, speed being limited to 10mm/s allowing the operator a significant chance of avoiding injury. Therefore, cutsets 24 to 26 will be discounted.
25	DNC2	14K7	
26	DNC2	16K2	
27	DNC1	DNC2	Quantitative analysis can take into account only the random failures of these two DNC outputs and not systematic failures resulting from, for example, software faults, electrical interference, etc. In addition, the comments applicable to Cutsets 24 to 26 apply. Therefore, Cutset 27 will be discounted.

In the absence of more detailed information, and for the purposes of this illustrative assessment, the diagnostic coverage of the DNC will be assumed to be 60%, with a repetition frequency of 4/minute.

The manual for the machine suggests that the light curtain is manually checked on a daily basis; however, a functional check that the photoelectric guard will stop the press is not included. The manual recommends that all security functions are tested at weekly intervals; however, the recommendation is not specific as to the tests that should be carried out, so it must be presumed that no test of the muting position is recommended (or required)[9].

[9] If the test had included a determination of the mute position, it will be clear that:

v those parts of the DNC covered by the internal diagnostics (assumed to account for 60% of the failure rate of the DNC) will be tested at the frequency of the diagnostics (assumed to be 4 complete tests/minute), and

1.1.1 Hazardous Event 3

The circuitry carrying out this function is a simple single-channel system so no explanation is required. Annex 3 shows the calculations used to estimate the SIL of this system.

Maintenance must be carried out within the rear of the machine; however, this should be carried out using a safe system of work, i.e., whilst the power to the machine is isolated. For the purpose of this assessment, maintenance activities will be ignored; however, in practice, it may be necessary to determine the risk reduction provided by the safe system of work in conjunction with that provided by the E/E/PE systems.

1.1.2 Software

Because the DNC was not developed by the manufacturer of the press, no information regarding the development of the DNC was available to the author. Therefore, it has not been possible to determine the techniques that have been used to ensure that the integrity of the software, implementing the safety functions being assessed, is appropriate.

Had the DNC been developed using IEC 61508, it would be expected that documentation indicating the specification, tools, procedures, validation results, etc., from the software development would be available to the suppliers of OEM equipment. In the absence of such documentation, no comment may be made regarding the DNC software, nor, for example, the diagnostic coverage carried out by the software on the hardware.

1.1.3 Architectural constraints

Part 2 of IEC 61508 places a number of architectural constraints, based on fault tolerance, on the SIL that can be claimed for a particular design of system, when that system is built up from a number of subsystems.

The version of IEC 61508 described at Reference 3 takes into account only diagnostic coverage and hardware fault tolerance in determining the ceiling for the SIL that can be claimed. The author was given sight of a developing draft of IEC 61508, which differs slightly from Reference 3 with respect to the architectural constraints. As a result, Tables 2 and 3 of the developing draft, see below, will be used in determining the architectural constraints.

The difference between Tables 2 and 3 of Part 2 of Reference 2 and the draft version of December 1998 are:

v Diagnostic coverage is replaced by Fail Safe Fraction, and

v the rows labelled none (0%), low, (60%), medium (90%) and high (99%) are relabelled <60%, 60% to 90%, 90% to 99% and >99%.

This allows the predominant failure direction towards the safe state to be taken into account for those components which, although not having self diagnostics, have a behaviour on failure which is somewhat similar. For example, a relay fails predominantly to the de-energized state (i.e., about 90% of failures are to the de-energized state). This should be compared with a PES

v those parts of the DNC not covered by the internal diagnostics (i.e., accounting for 40% of its failure rate) will be subject to only a weekly proof test.

[0] As a result, if a probability of failure on demand were required, the relevant proof test intervals would be allocated according to the above fractions.

having automatic diagnostics, which will shut the EUC down safely for the majority of faults when these are detected by the internal diagnostics (e.g., with a diagnostic coverage of 90%). Viewed from a safety point of view, their behaviours are similar.

Annex 4 shows how the fail-safe fractions for the safety functions associated with each hazardous event were determined.

1.1 Non-PES systems realisation

For convenience, no distinction has been made between PES and non-PES in Section 7.12. The quantitative assessment methodology is equally applicable to either technology; therefore, as the two technologies are highly interdependent in the operation of this control system, they have not been differentiated.

1.2 External risk reduction systems realisation

Not applicable to this assessment for which the hazards have been predefined.

1.3 Overall installation and commissioning

The instruction manual for the machine supplied to the author includes chapters devoted to the installation and commissioning of the machine; however, the chapter on installation is mainly devoted to the lifting, assembly, etc., of the machine. This would suggest it is intended to be used whilst the machine is being located at its eventual operating position, i.e., prior to commissioning.

The chapter on commissioning gives details of the operation of the various controls on the machine and describes the operation of the machine but does not include details of any pre-start checks of the safety functions whose assessment is described in this report. This would suggest that the chapter is intended only to familiarize the user with the machine and is not intended to facilitate commissioning.

Instead, a short checklist is used to ensure that the various functions of the machine, which were tested following manufacture, have not been disturbed by transportation and installation. This checklist is used during commissioning, training and during maintenance visits. Although the checklist covers only a single A4 page, there are 68 check-boxes to be ticked. The author was verbally informed that the length of the checklist had been limited to a single A4 page, as the manufacturer considers that a longer document may not be completed in full, or as rigorously.

Apart from the functional tests, the checklist includes the following items, which are relevant to the Hazardous Events considered in this assessment:

v Rear guard reset system;

v Footswitch;

v Single break;

v Double break;

v Fully guarded;

v Stroke stop;

v Sensitive;

v Manual operation;

v Working under the guard mute position,

v Operation of the guards on

v Horizontal

v Vertical

v Mute light function.

There is a note which includes the following sentence: "Guarding system must be active from the TDC down to mute position (6mm above the die which is adjustable). The mute position must not be more than 6mm above the die."

At first sight, the checklist appears to include little detail as to the tests that should be carried out; however, taking into consideration that it is the manufacturer's engineer who carries out the installation and completes the checklist, the level of detail is adequate and the checklist is more of an aide memoir to ensure that no tests are inadvertently omitted than a definitive test specification.

The checklist includes details of the machine, including serial number, together with the engineers signature and that of the customer.

The checklist consists of two self copying sheets, which allow one copy to be retained by the user and the other by the manufacturer.

The author would expect a document similar to this checklist, setting out the safety checks to be carried out during the commissioning of machines designed using IEC 61508. However, it should be noted that this checklist is brief and to-the-point, because:

v commissioning is carried out by the manufacturer's engineer, who is familiar with the machine, and

v the tests necessary to confirm the operation of the safety functions of the machine are relatively simple.

Were the above not the case, the author would expect a definitive test specification giving full details of the tests and the results that would be expected from them.

1.1 Overall safety validation

1.1.1 Confirmation that the safety systems meet the requirement specification

The author was unable to obtain the safety-requirements specification for the control system for reasons mentioned elsewhere. However, he was supplied with the 36-page checklist used by the manufacturer to confirm the correct operation of the machine prior to its despatch from the factory. The use of this checklist effectively provides a confirmation that the operation of each machine conforms to the safety-requirements specification (whether or not such a specification exists).

The checklist requires the testing of a number of safety-related components, including the following, which are specific to the functions being assessed:

v the operation and resetting of the rear guard interlock;

v the stopping performance associated with the light curtain;

v the mounting position of the light curtain, and

v the position at which the light curtain is muted by the control system.

The above tests will confirm that the functions associated with the three hazardous events considered in this assessment are operational.

Clearly, the checklist provides confirmation only that the functions operate as required by the specification, it cannot provide any information on the integrity of the systems carrying out those safety functions. Had the control system been developed using the guidance in IEC 61508, this stage would have been used to confirm that the operation and integrity of the safety functions, and the systems in which they are implemented, enabled the requirements of the safety requirements specification to be realized.

In this assessment, a comparison between the author's (independent) estimate for the required integrity for each of the safety functions is compared with the calculated integrity for the function in Annex 5.

1.1 Overall operation, maintenance and repair

Those recommended items of maintenance, which affect the quantification of the integrity of the control system have been considered in Section 7.9. These were obtained by the author from the chapter of the instruction manual devoted to maintenance. Therefore, the maintenance procedures, required to ensure that the integrity level of the control system is maintained at the level determined by this assessment, have been made available to the user.

1.2 Overall modification and retrofit

Not applicable to this assessment of an as-new machine. The documentation required by IEC 61508 for this stage would not be expected to be produced until the design of any modifications or refits is undertaken and, hence, it is possible to establish the safety requirements for these.

1.3 Decommissioning or disposal

Not applicable to this assessment of an as-new machine. The documentation required by IEC 61508 for this stage would not be expected to be produced until decommissioning or disposal is to be undertaken and it is possible to establish the safety requirements for this.

1.4 Discussion regarding the quantitative assessment using IEC 61508

1)The first, and probably the most important, obstacle in using IEC 61508 involves the determination of what is an acceptable level of risk. This may require an iterative process in order to obtain an acceptable value, which will depend on a number of factors, such as:

v what may have been established as custom and accepted engineering practice in the industry concerned;

v the cost effectiveness of improving safety beyond any particular level (e.g., the "law of diminishing returns"), and

v what competitors and other organizations using similar types of equipment have deemed to be practicable.

It was convenient for the author base his determination of the ALARP level on the existing accident rate involving presses, which was obtained from internal HSE sources. Such information will not be easy to obtain by designers working for machinery manufacturers. Other methods may be more appropriate. In addition, it may be politically unwise in some circumstances for, for example, what is considered to be an acceptable rate of a particular level of injury, to be quoted. Therefore, it may prove necessary for target SILs to be determined by opaque means, possibly qualitative, for the various sectors of industry. The determination of target SILs is a critical and not necessarily easy task which would be helped considerably by the availability of a suitable, possibly industry-specific, methodology for dealing with it.

2)IEC 61508 has been conceived with the process industries in mind. As a result, the determination of SILs depends on the risk reduction provided by safety-related protection systems, which operate in parallel with the control system of the EUC and put the EUC into a safe state if a failure of the control system occurs.

Many machinery control systems are based on relay technology. Because machines are mostly cyclic in operation, it is possible to test most, if not all, of the individual components in the control system at every cycle of the machine and employ redundancy. This leads to a fault tolerance of 1, or more; a short interval between tests and consequently the control system having a high integrity. Therefore, in the case of many machinery safety functions, the concept of risk reduction, as used in IEC 61508, is inappropriate and a SIL must be calculated from the failure rate of the control system.

3)Because IEC 61508 is new (not published in its final form at the time of this assessment), few, if any, manufacturers have used it. Therefore, the manufacturer of the pressbrake under examination does not have documentation that has been prepared to show compliance with IEC 61508. This is especially true with respect to the quality procedures used in the design of the machine. As a result, it has not been possible to determine whether the quality requirements have been satisfied in the design. This is likely to be true of any retrospective assessments carried out using IEC 61508.

4)Documentation for installation, commissioning, operation and maintenance is available in the instruction manual. However, as IEC 61508 post-dates the design of the machine, it should not be expected that the form of this documentation matches the requirements of IEC 61508; however, the existence of the documentation indicates that the various life-cycle stages have been considered if less formally, and in less detail, than is required by IEC 61508.

5)The type of press that has been examined is manufactured in the UK, but the design of the control system originates from outside the UK. As a result, only documentation relating to the manufacture of the press resides in the UK. Therefore, documents relating to design procedures, e.g., quality assurance, were not available to the author for the examination. This may be true of all systems which are:

v manufactured in the UK using a foreign design,

v assembled in the UK according to a foreign design or using parts manufactured abroad, or

v imported from abroad in a fully assembled form.

6)For a quantitative assessment, good failure-rate data are required. Data are available on common modes of failure of most of the components, e.g., a relay failing to energize. However, in safety-related systems, many components are automatically tested to ensure that the common modes of failure are revealed. Therefore, the remaining modes of failure, on which there is likely to be insufficient data (e.g., the failure of a single relay contact or a relay spontaneously changing from the de-energized to energized states as a result of, for example, a spring breaking), are likely to be encountered in a reliability assessment of a safety-related system. Such data are unavailable, leading to speculative (and highly subjective) estimates of these data.

7)In order to determine the probability of injury if the relevant safety function were to fail, the author has had to make a number of assumptions. For example, in the case of Hazardous Event 1, the author has assumed that the operator places his/her hands in the press once per minute. Good working practice would dictate that the operator's hands were NEVER placed in the press, a tool being used where necessary. The author chose to make a worst-case assumption which leads to the requirement of SIL 4. If the author had assumed that the operator places his/her hands into the press once every 10 minutes, the requirement would be SIL 3. Once every 100 minutes would correspond to SIL 2 and once every 17 hours (i.e., once every alternate 8-hour shift) would correspond to SIL 1.

It should be clear that this highly subjective assumption has a considerable effect on the target SIL. There may be a high dependence on basic (and possibly subjective) assumptions in the quantitative analyses of many other systems. Without research, that will enable such values to be determined without subjective assumptions being made, the uncertainty in the outcome of the quantitative analysis used in IEC 61508 may be large.

8)Because the outcome of the quantitative analysis using IEC 61508 is likely to depend on a number of highly subjective assumptions, it will be possible to tailor the outcome of the analysis to suit one's particular needs. Some of these assumptions will be difficult to challenge.

9)Clause 7.4.4.3 of Part 2 of IEC 61508 requires that "Any failure-rate data used shall have a statistical confidence level of at least 70%". This level of confidence is unlikely to be realized in practice, for the reasons described in the previous paragraph. In the author's opinion, the use of the best available data is better than not carrying out a quantitative reliability assessment; if necessary, worst-case assumptions can be made.

10)The proof-test intervals used in this assessment were based on the manufacturer's recommendations. It is not improbable that machines may be passed on from user to user without their documentation, or be inadequately (if at all) maintained. In such cases, the recommended proof-test interval may, in practice, be unrealistic, and a value not less than the expected life of the machine should be used in any reliability calculations. The instruction manual for the machine recommends that the annual check is carried out by one of the manufacturer's engineers in order to ensure the competence of the person carrying out the work; however, this recommendation need not be heeded. (Similarly, the proof-test intervals used at the design stage should reflect realistic, rather than recommended, values.)

11)At first sight, the documentation requirement of IEC 61508 does appear to be burdensome. However, this need not be the case. What the standard is, in fact, requiring is that the development, etc., is broken down into discrete stages (i.e., the lifecycle), careful thought is given to each of these stages, and the results of this are put onto paper for use in later stages and for demonstrating the adequacy of the system. Looked at in this way, the IEC 61508 lifecycle is no different from any other well organized process. Clearly, for a complex system, the documentation requirements will be large. However, for a simple system, the documentation requirements may equally be simple.

12)It has been said that the documentation requirement of IEC 61508 is burdensome for the machinery sector. However, the 36-page checklist used for validating the operation of the various machine functions prior to despatch demonstrates that the documentation associated with IEC 61508 need not necessarily be more burdensome than current documentation.

13)If the press had been designed using IEC 61508, the assessment would have been much easier because the documentation for each stage would have been available and this could have been compared with the author's expectation of the requirements of that stage. On the other hand, an assessment carried out in this way loses the independence provided by an assessor, who may not be misled into making the same mistakes that may have been made by the system designers, by following the documentation too closely.

14)The application of quantified risk analysis to machinery is more complex compared to its application to process control systems due to the synchronous interactions between the persons at risk, the control system and the cyclic nature of operation of the machine. In such situations, a calculation (e.g., of probability of failure on demand) involving steady-state conditions, as would be applicable to the control system of a process plant, is unlikely to be realistic. Instead, the timing of the automatic tests and periods of high risk in relation to the machine cycle must be considered in detail in the calculations.

15)It may not always be possible to obtain a complete understanding of the functions carried out by the hardware by examining the circuit diagrams. [For example, from an examination of the circuit diagrams, it can be deduced that Input 35 of the LCU-P (10.4) controls the muting of the photoelectric guard. However, it is not obvious that Input 35 and Input 37 (indicating bending speed) are both required to be energized for the muting to occur.] Therefore, a complete understanding of the operation of the system is required for an assessment to be meaningful. This is true of an assessment being carried out using either EN 954-1 or IEC 61508; however, in the case of the latter, where a quantitative analysis is carried out, large variations in the calculated failure rate could result from minor mistakes in determining functionality.

16)At first sight, the use of the architectural constraints on the hardware safety integrity appear to have a number of failings, for example:

v the diagnostic coverage (fail-safe fraction) is used as a parameter to determine the SIL ceiling; however, in the case of automatic diagnostics, the rate at which the diagnostics are carried out is ignored;

v the diagnostic coverage may be irrelevant in calculating the architectural constraint. In reality, what may be most important, for example, is whether the PES output used by the function is monitored;

v no account is taken of the fact that some single-channel systems may inherently be reliable and so perform as well as a multi-channel system;

v the fail-safe fraction for a single component (e.g., such as a mechanical scotch) may be even more difficult to determine than the diagnostic coverage of a computer-based system;

vall that the diagnostic coverage could lead to (assuming an appropriate repetition frequency) is an effective reduction in failure rate. Therefore, a system with a failure rate of λ and no diagnostics is effectively no different to a system with a failure rate of 100λ and a diagnostic coverage of 99%; however, the former would be severely penalized by the architectural constraint, and

vno account is taken of manual proof checking.

However, the architectural constraints should be viewed as a means of ensuring that the quantified analysis is not abused or used in error. For example, in the case of the calculations for this press:

v a number of assumptions have been made;

v the calculations are inexorably linked to the architecture, self monitoring and cyclic operation of the press, and

v the manual for the press indicates that a daily check should be carried out on the rear-gate interlock. The frequency of this check will have a considerable impact on the integrity of the interlock. If no checks were carried out in practice, the actual (as opposed to the calculated) integrity of the interlock would be considerably reduced.

The architectural constraints are intended to put a ceiling on the SIL that can be assigned to any particular system in order to prevent either inadvertent (or deliberate) misuse of the quantitative analysis. As a result, the architectural constraints will ensure that the integrity level cannot be inflated significantly beyond the actual level achievable for any particular system. This will prevent inflated SILs being claimed and, as a result, ensure that an appropriate level of safety is maintained.

17)It is not easy to apply the architectural constraints to systems containing relays, which may be diagnosed as part of their normal operating function; the coverage of the tests on any particular relay (in terms of the failure rate) is difficult to determine. For example, in the case of a non-guided-contact relay, the effect of monitoring one set of contacts on the operation of another is difficult to determine from the limited amount of available data.

18)Tables 2 & 3 of Part 2 of IEC 61508, used to combine the architectural constraints of several subsystems, require clarification as to their use. (See Annex 4.)

1 ASSESSMENT USING IEC 61508: QUALITATIVE EXAMINATION

In the design of a safety-related system, the quantitative and qualitative requirements would be applied, as appropriate, throughout the life cycle of the system. However, for convenience, they will be examined separately in this assessment.

The target SIL for each of the safety functions under examination has been derived and they are shown in Annex 5. These target SILs have been derived on the basis that the DNC fails at a rate of 1 failure in 10^5 hours. As the target failure rates and the predicted failure rates are similar, it will be presumed that the risk reduction provided by the DNC is appropriate, i.e., if the DNC has a failure rate of 1 in 10^5 hours, the overall safety integrity requirement is achieved. Therefore, the qualitative requirements of the DNC should be determined assuming that the DNC has been designed to have a safety integrity of SIL1. The qualitative analysis will determine whether the techniques deemed appropriate in IEC 61508 for the safety integrity levels:

v SIL1, for the DNC, or

v SIL4, SIL1 or SIL2, for each of the systems used to prevent Hazardous Events 1, 4, 1[10] or 3, respectively,

have been used during the development of the system. For convenience, the various parts of IEC 61508, other than Parts 1 & 2, which have already been dealt with, will be considered in turn.

The aim of the qualitative assessment is to ensure that the measures taken to prevent systematic faults are sufficiently rigorous to ensure that the rate of systematic failures is significantly less than the rate of random hardware failures. In this way, random hardware failures become dominant, so their rate becomes a meaningful measure of the integrity of the system. Therefore, the rigour in which the qualitative measures are applied must increase with increasing SIL.

Because this report describes an assessment, not proof testing of the safety systems, it is based on documents, not the testing of a machine. This has led to two problems:

v the control system of the machine was not designed in the UK so access to design documentation, which could have indicated the rigour of the qualitative measures, was not available to the author, and

v the machine was designed prior to the publication of IEC 61508 and so was not designed with this standard in mind. Hence, the documentation required to show compliance with the standard is either not available or is incompatible with the standard.

Therefore, it has not been possible to assess compliance of the various stages of the lifecycle of the machine with the qualitative measures given in IEC 61508 in any significant depth.

1.1 IEC 61508, Part 3: Software requirements

This part describes the tools and techniques appropriate for use in systems of the relevant SIL. As with the development of the overall system, a lifecycle approach is adopted for the software.

[10] SIL1 is the maximum allowable from the architectural constraints.

Unfortunately, the manufacturer of the press is supplied with the DNC by the parent company, which is not resident in the UK. As a result of this, the press manufacturer is only aware of the functional capabilities of the DNC and has no knowledge of its internal design, nor the procedures used in the design. (The press manufacturer effectively builds a press around the DNC rather than producing a specification for the DNC according to the design of the press.). As a result, no documentation, giving details of the software design, is available.

In order to determine whether compliance with IEC 61508 has been achieved, it would be necessary to examine the documentation justifying the compliance with the standard, and to determine whether the tools and techniques required for the appropriate SIL had been used. In the case of the press under examination, for example, which has a target SIL of SIL1, the assessment would determine whether the package of tools and procedures used to produce the software was appropriate for SIL1.

As no documentation describing the development of the software within the DNC is available, no comments can be made regarding the compliance of the DNC with Part 3 of IEC 61508, or regarding the use of Part 3 itself. However, it should be noted that the principle used in the design of the hardware of the control system is to:

v use relay logic wherever possible in safety functions, and

v ensure that all relays are tested on each cycle of the press and provide fault tolerance for important safety functions.

1.2 IEC 61508, Part 4

This part gives only definitions for the various terms used in IEC 61508, so will be ignored in this assessment.

1.3 IEC 61508, Part 5

Part 5 of IEC 61508 gives examples of methods for the determination of safety integrity levels, and is intended to provide help to users of the standard. The author carried out the quantitative assessment described in Section 7 without recourse to Part 5. Therefore, this section will be used only to comment on the guidance provided by Part 5.

Part 5 gives no normative guidance, relying on informative annexes to illustrate the concepts behind, and application of, Part 1 of IEC 61508.

In the author's opinion, the determination of what is ALARP will possibly be one of the more (if not the most) difficult aspects of a design or an assessment using IEC 61508. The lack of guidance in IEC 61508 as to what should be considered to be ALARP will be a significant obstacle in the direct use of the standard. However, if sector-specific standards, based on IEC 61508, are developed, these could include such guidance and allow the principles of IEC 61508 to be applied, although indirectly.

The inclusion of Annex D of Part 5 of IEC 61508 appears to indicate that the difficulty in determining the ALARP value has been recognized and an attempt has been made to develop a pseudo-quantitative approach, whose basis is very similar to the risk-graph of EN 954-1. The method is not meant to be applied directly (and appears to have been made deliberately vague because of this) but is intended to be a starting point for the development of industry-specific standards which will develop the methodology further and define what is meant by the various parameters (e.g., at what point does the frequency of exposure change from seldom to frequent, etc.) and, presumably, calibrate the methodology against quantitative methods.

It is not known how realistic such a pseudo-quantitative approach can be made; however, at first sight, it appears to feature all of the deficiencies of EN 954-1.

1.4 IEC 61508, Part 6

Part 6 of IEC 61508 gives guidelines on the use of Parts 2 and 3, and is intended to provide help to users of the standard. The author carried out the quantitative assessment described in Section 7 without recourse to Part 6.

1.5 IEC 61508, Part 7

Part 7 of IEC 61508 gives an overview of the various techniques and measures that can be used to improve the integrity of a safety-related system. This part of the standard is intended to assist the designer in the selection of suitable techniques and measures to be used in his/her design, so has not been considered in this assessment as no documentation is available giving suitable details of the techniques used in the various stages of the machine's lifecycle which could be compared with the recommendations of the standard.

2 CONCLUSIONS

1)Machinery safety systems are not developed from scratch using a life-cycle approach. Instead, as a new machine is developed, the experience gained from previous machines is modified slightly in order to make improvements to the overall design. Hence, safety requirements are unlikely to be developed for any particular machine. Instead, the safety systems of new machines will be designed to be no worse than those of existing machines. The use of IEC 61508 will require a radical change to the machinery design/development process in that safety must be addressed using an absolute, rather than relative, approach.

2)IEC 61508 uses quantitative calculation of the overall failure rate as well as qualitative techniques, where insufficient information is available for a quantitative determination (e.g., for systematic failures), for determining safety integrity. EN 954-1 attempts to avoid the need for a quantitative calculation by using a simple methodology - the risk graph. Unfortunately, the application of the methodology is not straightforward in other than the simplest of systems, and requires a subjective application of engineering knowledge.

3)IEC 61508 covers all stages of the lifecycle of a system. EN 954-1 considers only the design (and validation of the design).

4)The greatest problem in using a quantitative approach to risk assessment, as described in IEC 61508, is the availability of suitable data. Two types of data are required:

v Failure rate data for the components and subsystems: It may be necessary to use data from generic components, or for outdated components; however, data can be obtained (or estimated) for most components, although it is likely that some assumptions may be necessary.

v Levels of acceptable risk: The level of acceptable risk is a societal parameter and is difficult to determine, being dependent on perceived, rather than actual, risk. The guidance in IEC 61508 uses the ALARP value but gives no help in determining what that value should be. The author made an assumption that existing hazard rates were acceptable but this assumption need not be valid in all cases. The author considers that this problem may present the most difficulty in using IEC 61508 until industry-specific guidance documents, based on IEC 61508, provide guidance in this area. However, the publication of such guidance could give alarm to those at risk.

5)A number of assumptions had to be made in order to carry out the quantitative analysis described in IEC 61508. These were subjective had a significant effect on the SILs. There may be a high dependence on basic (and possibly subjective) assumptions in the quantitative analyses of many other systems. Some of these assumptions will be difficult to challenge and could lead to failure-rate predictions being distorted to meet the needs of other agendas.

6)If a methodology, that will enable target SILs to be determined without significant subjectivity is not available, the uncertainty in the outcome of the quantitative analysis used in IEC 61508 may be large. In the author's opinion, the production of such a methodology should be given a very high priority otherwise it will not be possible to fully exploit the guidance provided by IEC 61508.

7)Generally, existing safety-related electrical control systems at machinery have not been designed using the guidance contained in IEC 61508 (of which all parts were not published at the time of writing of this report) and, as a consequence, suitable documentation, required in order to verify the various safety lifecycle stages, is not likely to be available. Documentation, in a form suitable for assessment purposes, will become available only when IEC 61508 gains credibility in machinery manufacture. Until this time, it will be difficult to carry out assessments of safety-related electrical control systems at machinery, especially in relation to the quantitative analysis.

8)IEC 61508 relies heavily on documentation to demonstrate that the various life-cycle stages have been carried out correctly and to allow following stages (e.g., validation) to be performed. At first sight, the documentation requirements for a simple machinery-control system appear to be excessive.

9)Because shortage/incompatibility of documentation may prevent an adequate determination of the qualitative measures when a retrospective examination is carried out on a machine designed prior to the publication of IEC 61508, it will not be possible to determine whether (or not) suitable measures have been put in place to deal with systematic failures. Therefore, a retrospective quantitative assessment using IEC 61508, may prove to be inaccurate as the actual failure rate may be dominated by systematic failures, which are unlikely to be predictable quantitatively. Unfortunately, this will lead to an underestimate of the failure rate, i.e., the estimate will indicate that a system will be safer than it actually is.

10)IEC 61508 takes a scientific approach to the matching of system integrity to risk. Wherever possible, it uses quantification, but uses qualitative measures where quantitative measures cannot be used. However, the qualitative measures have been determined (using engineering judgement) to be appropriate to the SIL. This should be compared with the approach taken by EN 954-1, which is arbitrarily based on fault tolerance in its entirety.

11)In the author's opinion, EN 954-1 was developed for relay-based systems as existed in the 1970s, an application for which it would have been ideal as it is simple to apply, and it would have led to in improvement in the safety standards at that time. Unfortunately, the standard has been overtaken by the technologies used in safety-related systems and it would be difficult to take into account: sophisticated automatic diagnostics; the use of systems which include different technologies having vastly different failure modes and reliabilities, and the use of software. The feature of the standard is its underlying simplicity; however, even in its present form, this simplicity has begun to be lost. If attempts are made to take these deficiencies into account, the simplicity of the standard will be completely lost, and it would be better to go directly to a standard, such as IEC 61508, designed to address these deficiencies from the outset.

12)This assessment has not proven to be an appropriate way of demonstrating the effectiveness of IEC 61508. The principles of IEC 61508 follow a methodology which encompasses all of the phases in the lifecycle of a system, e.g., concept, design, implementation, etc. If the methodology has not been used by the manufacturer, subsequent assessment using IEC 61508 will inevitably be difficult because of missing information. However, if IEC 61508 had been followed from the outset, the relevant information would have been available, facilitating the assessment.

3 REFERENCES

1)BS EN 954-1: 1997, Safety of machinery - Safety-related parts of control systems - Part 1. General principles for design., BSI Standards, ISBN 0 580 27466 7. [Although this report refers to the use of EN 954-1, the document actually used by the author was this technically identical standard published in the UK by BSI Standards.]

2)Draft IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1 to 6, 1998.

3)Use of EN 954-1: 1998 - Safety-related parts of control systems - Part 1. General principles for design, CEN/TC 114 - CLC/TC 44X - JWG 6 N 507.

4)The Highway Code, HMSO, Department of Transport, ISBN 0-11-550962-3t, 1993 (reprinted 1995).

5)Reliability, maintainability and risk, fourth edition, Smith, David. J., Butterworth Heinmann, 1993, ISBN 0 7506 0854 4.

6)Military handbook: reliability prediction of electronic equipment, MIL-HDBK-217E, U.S. Department of Defense, 27/10/86.

7)The sixth survey of machine tools and production equipment, Metalworking Production, 1988.

8)Trojan 5 universal tongue-operated interlock switch, Guardmaster catalogue: Machine safety devices, 1995-96 edition, Guardmaster, Hindley Green Industrial Estate, Wigan, WN2 4HR.

9)Programmable Electronic Systems in safety-related applications, Health and Safety Executive, HMSO, ISBN 0 11 883906 3, 1987.

10)BS EN 1050: 1997, Safety of machinery - Principles for risk assessment, BSI Standards, ISBN 0 580 27153 6, 1997.

11)Control technology: Fundamental safety aspects to be considered for measurement and control equipment, Deutsche Elektrotechnische Kommission, DIN V 19 250, May 1994.

ANNEX 1

DETERMINATION OF PROBABILITY OF THE HAZARDS BEING REALIZED IF THE SAFETY-RELATED FUNCTIONS FAIL

The determination of the target SILs for the IEC 61508 assessment identified a conceptual problem. This standard assumes that one has a basic control system alongside which one or more safety-related protection systems operate. A failure of the control system leads to a demand on the protection systems that have been designated as being safety related. The SIL for the safety-related protection systems is determined from the risk reduction required of them. For example, the failure rate of the control system will lead to a basic risk. These failures will lead to demands on the protection systems. When the demands occur, the equipment under control is put into a safe state by the safety-related protection systems. Therefore, the EUC risk, that would have resulted from the failure rate of the control system alone, is reduced to a level which is as low as reasonably practicable (ALARP) by the safety-related protection systems; hence, the operation of the safety-related protection systems leads to a reduction in the risk. This risk reduction can be mapped to the SILs of the individual safety-related systems.

In the case of the control system of the press under examination, the majority of the safety functions are carried out by relays. This leads to the first difficulty in that there are no separate control and protection systems. The DNC controls non-safety-related functions; the safety-related functions being controlled by a relay-based control system with no identifiably separate safety-related protection system, as would be the case with a process plant, for example. Therefore, the electrical control system of the press can be considered to be a fault tolerant safety-related system that has been engineered such that individual components are tested during the cyclic operation of the press. Potentially dangerous component failures are detected and further press operation is prevented to ensure that dangerous failures of the press do not occur. Therefore, although the systems carrying out the safety-related functions will tolerate single, and, possibly, multiple, faults, it cannot be split into separate control and protection systems or multiple protections systems.

The result of this is that it is not possible to determine the risk reduction referred to in IEC 61508. In order to get round this problem, the author could have taken the following approach:

1)Determine the probability of the hazard being realized if the safety-related function fails.

2)From accident data, estimate the frequency of accidents associated with the hazardous event under consideration throughout the UK and, hence, for each individual machine in the UK. This accident rate could be considered to be ALARP.

3)Calculate the failure rate of each safety function, which, in conjunction with the probability of the hazard being realized, will achieve the ALARP accident rate. This could be considered to be the target failure rate of the safety function, and, hence, the target SIL.

4)Estimate the actual failure rate of the control system, and, hence, the SIL.

5)Compare the actual failure rate and the target failure rate to determine whether the SIL has been achieved.

This annex deals with only Item 1, above.

HAZARDOUS EVENT 1

Although up to 15 strokes per minute may be used during "bumping", in order to allow one or both of the operator's hands into the tooling, the tool must be raised significantly above the workpiece. Therefore, it will be assumed that the press is used in normal pressbrake mode with a stroke rate of about 4 per minute.

When using a pressbrake, it should not be necessary for the operator to insert his hands into the tooling - there should be sufficient material in front of the tools to avoid the need for this. However, for the purpose of this assessment, good working practice will not be assumed. Instead, it will be assumed that a program of 4 strokes is carried out and then, at the fourth stroke, the operator inserts his hands between the tools in order to retrieve the completed workpiece. Therefore, the operator's hands are at risk once per minute for Hazard 1. It will be assumed that the operator's hands are between the tools for a period of 2 seconds.

It is conceivable that the operator will be able to react quickly enough to remove his hands from between the tools if an aberrant movement were to occur; however, in the author's opinion, the operator would have to be extremely alert in order to achieve this. The distance between the beam and the bed at stroke top will be between 200 and 500mm, with 200mm being the norm. With a descent speed of 150mm/s, a stroke of 200mm and assuming a hand width of 50mm, amputation would begin only 1s after the start of an aberrant stroke.

The situation would be somewhat similar to that presented to a car driver when an unexpected but dangerous situation arises. In the figure on its back page showing "shortest stopping distances" for cars, Reference 4 indicates that the "thinking distance" of a car driver is 9m (29.25 feet) at 30mph (44ft/s). This represents a time of 665ms, which includes both thinking time and the time taken for the driver to transfer his foot to the brake pedal. A car driver frequently applies the footbrake, so the movement of his foot will be part of a well-trained reflex action. The operator will not frequently need to remove his hands from the machine in an emergency. Even if he were watching the tool, his reaction to an unexpected movement would require a conscious appraisal of the situation, rather than just an unconscious reflex action, which could lead to a reaction time significantly in excess of 665ms. To this must be added the stopping time of the machine - about 90ms.

Therefore, it will be assumed that, if an aberrant movement were to occur, the operator would have little chance of avoiding injury. A value of 10% will be assumed.

It will be assumed that an aberrant unguarded stroke can occur at ANY time, including during a legitimate downstroke. This is because the unguarded stroke would cause the loss of muting if it were to occur during the legitimate stroke.

The risk is determined in Table A1.1.

Table A1.1: The probability of injury associated with Hazardous Event 1		unit
Frequency of exposure	1	per minute
Duration of exposure	2	seconds
Fraction of working time exposed	0.033	
Hazard	Irreversible injury	
Probability of injury if control fails and operator exposed	0.9	
Overall probability of injury if an aberrant stroke were to occur	0.03	

HAZARDOUS EVENT 2

If the programmed muting position were to change as a result of a fault[11], such that the operator could put his hands between the tools with muting in operation, the hazard would not exist until the operator pressed the footswitch to initiate a stroke. Whilst an operator's hand may frequently enter the tooling, it is unlikely that he will deliberately press the footswitch with his hand there. Therefore, the rate of the hazard will be affected by the probability of the operator inadvertently pressing the footswitch with a hand between the tooling. It will be assumed that the probability of the operator inadvertently operating the footswitch, whilst a hand is between the tooling, is 0.1%. This leads to the operator's hands being at risk once every 16.7 hours and, hence, a frequency of potential demands on the protection system of 0.06 per hour, see Table A1.2.

Table A1.2: The probability of injury associated with Hazardous Event 2		Unit
Fraction of time that operator's hands are within the tools	0.33	
Frequency of operator's hands entering the tools	1	per minute
Probability of operator inadvertently pressing the footswitch with a hand between the tooling	0.1	%
Frequency of potential demands on the muting function	0.06	per hour

HAZARDOUS EVENT 3

Access will be required to the rear of the machine only infrequently, i.e., once per hour. It will be assumed that access will be gained for 5 minutes with the machine under power. It will be assumed that the machine operates for one shift of 8 hours per day over 230 working days per year, and that faults manifest themselves only during machine operation.

Although it would be possible for a person in the rear of the machine to put his hand under the tool, it is thought that the most probable hazard would be associated with the positioning servos. It is considered that the probability of avoiding injury by these servos will be higher than that of avoiding injury from the tool. The following will be assumed:

v a 20% probability of avoiding injury, and

v demands for movement are frequent, i.e., the operator will not be aware that anyone will be in the rear of the machine, so a demand will be certain to occur during any entry to the machine when the interlocking has failed. This provides a worst-case condition.

Because movement is considered to be certain if the interlock fails, and the interlock may fail during, or before, the period of entry, the probability of injury must consider only the period during which entry is gained.

Table A1.3: The probability of injury associated with Hazardous Event 3		Unit
Hazard	Irreversible injury	
Probability of injury if control fails and operator is exposed	0.8	
Overall probability of injury if interlock fails	0.8	

[11] For this to occur, two outputs of the PLC must be affected (i.e., those driving 14K5 and KRES2). This requires a misinterpretation of both position encoders and would put the machine (via 14K5) into pressing mode, i.e., the speed would be limited to 10mm/s. Therefore, the fault would have to be complex involving an out put for a relay involved in another function (i.e., KRES2 and 16K2, 14K2 or 14K3). The nature of such a fault is difficult to determine.

ANNEX 2

DETERMINATION OF THE TARGET FAILURE RATE ASSOCIATED WITH EACH HAZARDOUS EVENT

The SIL for each safety-related function of a system must be determined from the risk reduction associated with that function. Part 1 of IEC 61508 sets out the requirements for determining this risk reduction and, hence, the SIL. IEC 61508 Part 5 provides example methods of a number of risk based approaches for SIL determination. The determination of the SIL will depend on many factors that cannot be taken into account in a generic standard. These will include:

v public perception of risk in general;

v public perception of risk in any particular industry;

v the background risk from everyday life and of the industry in question;

v custom and practice in any particular industry, and

v probability of death/injury if a failure were to occur. This will take into account the number of persons likely to be involved in any particular incident.

Therefore, the SIL must be determined from:

v a risk assessment;

v the risk reduction provided by other systems operating in parallel with it, and

v factors outside the scope of this document (e.g., public perception of what is an acceptability of risk in any particular industry).

BS EN 1050 (Reference 10) provides advice on risk assessment. This standard addresses the problem in a qualitative and informative way, giving advice regarding the many factors that contribute to risk (and how these factors may be reduced). Unfortunately, it provides little guidance regarding the determination of risk in a non-subjective or quantitative way. Therefore, although Reference 10 is adequate for its purpose, it is insufficient to meet the needs of users of IEC 61508 (or EN 954 for that matter).

Reference 11 describes how risk can be determined quantitatively but gives only a pseudo-quantitative (i.e., using the risk graph) means of determining a target integrity, explaining that this allows societal perception of risk, which is more influenced by consequence than probability, to be taken into account.

It will be seen that although there is guidance available which indicates how risk should be determined, there is little guidance available on the values of the various parameters that must be used in the estimates for determining the SIL for any particular safety-related function.

In order to get round this problem, the author could have taken an approach whereby he determined what is the existing hazard rate using available accident data, and assumed this to correspond to the ALARP level. Using the probability of a hazard being realized if the safety-related function fails together with the accident frequency, the author would have been able to determine a SIL for each of the safety-related functions. Unfortunately:

v the accident data would not be widely available to the public;

v although this report is an informative document, as a result of the dearth of other sources of information on the determination of SILs, any SILs that are quoted are likely to be used as if they were normative, and

v the SILs would not have taken into account custom and practice which may exist in this (and, more importantly, other industries).

Therefore, because the main aim of this report is to compare Reference 1 and 2 and not to determine numeric values for the SILs, no SILs will be determined. Nevertheless, it should be noted that there is an urgent need for a methodology to be developed which will allow the determination of SILs without which, the guidance in IEC 61508 (and EN 954) cannot be exploited fully.

ANNEX 3

DETERMINATION OF THE SIL OF THE SAFETY-RELATED FUNCTION ASSOCIATED WITH EACH HAZARDOUS EVENT

HAZARDOUS EVENT 1

Table A3.1: Quantitative analysis: safety function associated with Hazardous Event 1

	Item[1]	Value	Unit	Comment/assumption
A	Failure rate of 10K9	0.018	per 10^6hrs	1.8*10%*10%, i.e., failure rate of relay calculated using Reference 6 (1.8). 10% of failures are failure to release. **Assume** that spurious energization (as opposed to failure to de-energize) is 10% probable
B	Failure rate of the DNC	10	per 10^6hrs	20/2, i.e., bottom of range of PLC failures from Reference 5 as most failures will not affect relevant outputs, divided by 2 as only half will be in dangerous direction[2].
C	PFD of 10K9	0.0375	$*10^{-3}$	Tested every 15 seconds, the PFD of 10K9 is incredibly small.
D	Rate of cutset 1	0.38	per 10^9hrs	[B x C] May be neglected - the rate will be influenced more by systematic failures than random failures.
E	Failure rate of the Direction Valve	8	per 10^6hrs	Reference 5, upper end of typical range for solenoid valve
F	PFD of direction valve	0.0001		Press will run for a week (5 8-hour shifts=40 hours) with faulty valve
G	Rate of cutset 2	0.0016	per 10^6hrs	[B x F]
H	Failure rate of the Servo Valve	8	per 10^6hrs	Reference 5, upper end of typical range
I	Rate of cutset 3	0.0012	per 10^6hrs	[F x H]
J	Total rate of Haz. Event 1	5.76	per 10^9hrs	[(G + I) x 2] Doubled because two ends to beam
K	SIL calculated for Event 1	SIL4		

[1] All of the failure rates refer to failures in the dangerous direction.

[2] The fail-safe fraction has not been taken into account, as the diagnostics are unlikely to be able to put the system into a safe state before the hazard can be realized.

HAZARDOUS EVENT 2

Table A3.2: Quantitative analysis: safety function associated with Hazardous Event 2

		Value	Unit	Comment/assumption
A	Failure rate of a single DNC output	0.5	per 10^6hrs	1/10^6hrs, half of which are dangerous.
B	Failure rate of the DNC overall	10	per 10^6hrs	20/10^6hrs, 50% of which are dangerous.
C	Failure rate of the DNC assuming 60% diagnostic coverage[1]	4.0	per 10^6hrs	40% of B.
D	Failure rate of a single DNC output taking into account the processor system.	4.5	per 10^6hrs	A + C
E	Failure rate of two DNC outputs taking into account common cause output failures	4.1	per 10^6hrs	C + βA - a value of 0.2 is assumed for β.
F	Failure rate of 16K2 or 14K3	0.36	per 10^6hrs	1.8 x10% x 2
G	Failure rate of two DNC outputs and the relays driven by them	4.2	per 10^6hrs	E + βF - a value of 0.2 is assumed for β.
H	SIL calculated for Hazardous Event 2	SIL1		

[1] The diagnostic coverage may be in excess of 90% if, for example, an external watchdog is fitted. Unfortunately, the author has no knowledge of the DNC so a worst-case assumption has been used.

[Author's notes:

1) It may be surprising that the use of either Tables 2 & 3 of IEC 61508, Part 1, can lead to such wide differences in the SIL. However, it should be remembered that the SIL depends on the way in which the system is used, the automatic diagnostics, proof-test interval, etc.

2) The failure rate shown is that for the entire DNC. In reality, failures in only a fraction of the DNC will affect the function. However, without detailed information on the DNC, this fraction cannot be determined. Determination of the rate at which two DNC outputs may fail to the energized state is not easy without using fault simulation techniques. For convenience, half of all DNC faults will be assumed to be dangerous; however, this is likely to be a worst-case estimate. Systematic failures cannot be taken into account and failures of the processor are more likely to cause operation to cease rather than change the state of any output. Therefore, the author has taken into account the failure rates of the output devices using data from Reference 9 and the overall DNC, from an estimate provided by the manufacturer. Although the failure rate of the outputs may be included in the manufacturer's estimates (so may be included twice in the above table), it will be seen that they do not significantly affect the overall failure rate.

3) The failure rate of the encoder supplying positional information to the DNC has been assumed to be small compared to that of the DNC itself, so has been ignored for the purpose of this assessment.]

HAZARDOUS EVENT 3

Table A3.3: Quantitative analysis: safety function associated with Hazardous Event 3

		Value	Unit	Comment
A	Failure rate of rear gate limit switch	0.01[1]	per 10^6 hrs	
B	Failure rate of 10K6 or 10K7	0.36	per 10^6 hrs	1.8 x10% x 2
C	Overall failure rate	0.36	per 10^6 hrs	A + B
D	Proof[2]-test interval[3]	8	hours	
E	Probability of failure on demand	1.44	$*10^{-6}$	C x D/2
F	SIL calculated from failure rate for Hazardous Event 3	SIL2[4]		

Notes

[1] A positive-action tongue-operated safety switch is used, therefore, the failure rate of the switch will be extremely low. The value chosen is small compared to that in row B, which, as a result, dominates the calculations.

[2] The daily check recommended in the instructional manual is NOT a proof check as defined in IEC 61508, but is a functional check. However, because of the simplicity of the interlock, this functional check will test a large fraction of the dangerous failure modes of the components, so will be considered to be a proof test for the purposes of this assessment.

[3] It is assumed that a single 8-hour shift is in use **and that the daily check recommended in the instruction manual for the machine is carried ou**t. If a failure occurs outside the shift, it will be identified by the daily check prior to the start of the following shift. Therefore, only failures which occur during a shift are of interest.

[4] Whether the probability of failure on demand or the failure rate is used to determine the SIL will depend on the frequency of demands on the safety system. If access is required significantly less frequently than the proof tests are carried out, the PFD will be meaningful, otherwise the failure rate should be used. In this particular case, where access is likely to be required at least on a daily basis, the SIL for high demand mode of operation (Table 3 of Part 1 of IEC 61508) has been used. Therefore, rows D and E should be ignored.

ANNEX 4

DETERMINATION OF THE FAIL-SAFE FRACTIONS ASSOCIATED WITH THE SAFETY FUNCTIONS FOR EACH HAZARDOUS EVENT

HAZARDOUS EVENT 1

An examination of the fault tree shown in Figure C.1 indicates that at least two components must fail in order to lead to Hazardous Event 1, therefore, there is an overall fault tolerance of 1. A fault tolerance of 1 also applies to the electrical/electronic parts of the control paths.

Because the system is comprised of both PES and hardwired components, Table 2 of IEC 61508 will be used to determine the architectural constraint.

It is difficult to determine the fail-safe fraction for the circuit; however, an estimate can be determined as follows:

v 10K9 is tested at each cycle of the press;

v the DNC must carry out the normal control functions of the press. It is likely that these would not continue to be carried out normally if a fault occurred in 60% of the DNC (For the purposes of this assessment, it will be assumed that this fraction of the DNC contributes to 60% of the DNC's failure rate - in an actual assessment, the fail-safe fraction would need to be determined by taking into account the failure rates and failure modes of the various components.);

v 10K8 is tested at each cycle of the press;

v a failure of 15K3 would limit the approach speed to the pressing speed, which would immediately reveal the fault to the operator (and allow the imminence of accidents involving potential amputations to be seen), and

v if the footswitch fails to the depressed state, the press would make a single stroke, e.g., to the mute position.

Table A4.1 shows how the fail-safe fraction was obtained.

Table A4.1: Calculation of fail-safe fraction for Hazardous Event 1

Component	Failure rate	Fail-safe fraction (component)	Fail-to-danger rate	units
Direction valve	4	1	0	*10^{-6}hrs
Servo valve	4	1	0	*10^{-6}hrs
DNC	20	0.9	2	*10^{-6}hrs
10K9	1.8	1	0	*10^{-6}hrs
10K8	1.8	1	0	*10^{-6}hrs
15K3	1.8	1	0	*10^{-6}hrs
Footswitch	5	1	0	*10^{-6}hrs
Totals	34.4		2	*10^{-6}hrs
Fail-safe fraction (overall)			0.94	

As the components in the circuit providing protection from Hazardous Event 1 are of both programmable electronic and relay technologies, Table 3 should be used if it is applied to the entire system. However, SIL4 can be obtained by combining the effective SILs of the two channels.

[Author's note: 7.4.5.3 of Part 2 of IEC 61508 indicates that a subsystem is of Type B if the failure mode of any component is not well defined. Therefore, if the tables are applied to the system as a whole, Table 3 should be used. This leads to a SIL of 2 (fail-safe fraction 60% and fault tolerance of 1). The alternative, e.g., treating the channels as being separate would lead to SILs of SIL4 (fail-safe fraction 99% & fault tolerance of 0) and SIL1 (fail-safe fraction of 60% & fault tolerance of 0) for the non-PES and PES channels, respectively. Combining these would lead to an overall SIL4. The standard is somewhat ambiguous as to how the tables should be used. However, the large difference between the alternatives, SIL2 and SIL4, causes the author some concern.]

HAZARDOUS EVENT 2

The fail-safe fraction for the circuit can be estimated as follows:

v KRES2 is tested prior to each stroke;

v 14K5 must be de-energized to allow the return stroke;

v the DNC must carry out the normal control functions of the press. It is likely that these would not continue to be carried out normally if a fault occurred in 60% of the DNC (It will be assumed, for the purpose of this assessment, that this fraction of the DNC contributes to 60% of the DNC's failure rate.);

v KRES2 is a guided contact relay, so contacts 25/26 are monitored.

Table A4.2 shows how the fail-safe fraction was obtained.

Table A4.2: Calculation of fail-safe fraction for Hazardous Event 2

Component	Failure rate	Fail safe fraction (component)	Fail-to-danger rate	units
KRES2	1.8	1	0	*10^{-6}hrs
14K5	1.8	1	0	*10^{-6}hrs
14K5	1.8	1	0	*10^{-6}hrs
14K5	1.8	1	0	*10^{-6}hrs
DNC	20	0.6	8	*10^{-6}hrs
25/26	0	1	0	*10^{-6}hrs
Totals	27.2		8	*10^{-6}hrs
Fail-safe fraction (overall)			0.71	

As the major component in the circuit providing protection from Hazardous Event 2 is the DNC, Table 3 will be used. In the case of Hazardous Event 2, a single component (the DNC) can lead to the top event[12]. This leads to a maximum SIL of SIL1.

[12] It could be argued that, because different outputs from the DNC are used, more than one component must fail in order to cause a dual failure. However, the author has taken a worst-case standpoint and regarded the entire DNC as a macro component in which the failure of some of its constituent components (e.g., the CPU) could lead to an indeterminable failure of the entire DNC. One of these DNC failures, albeit unlikely, could be the aberrant (and concurrent) energization of a number of outputs.

HAZARDOUS EVENT 3

The interlocking of the rear gate is carried out by a single-channel electrical system. A single-channel system can fail on the occurrence of a single fault, leading to a fault tolerance of 0.

No automatic diagnostics are applied to the interlock; however:

v relays 10K6 and 10K7 have failure modes which are predominantly to the de-energized (i.e., safe) state. Approximately 90% of all relay failures are to the de-energized state, so the fail-safe fraction is 90%, and

v the Trojan (See Reference 8) tongue-operated safety switch fitted to the gate has positive-action contacts and has been designed to fail only to the safe state. As a result, its fail-safe fraction is considered to be in excess of 99%. The operating life of this switch is indicated to be $>10^6$ cycles. If the rear gate were opened as frequently as once per hour during the operation of the machine[13], this would amount to an operating life in excess of 360 years for the switch.

This indicates that the fail-safe fraction for the circuit is in excess of 90%. Using Table 2 of the *draft* Part 2 of IEC 61508 leads to a maximum claimable Safety Integrity Level of SIL3[14].

[13] Assumed to be 1.5 shifts for 230 days of the year.

[14] 10K6 and 10K7, together, have a fault tolerance of 1 and a 90% fail-safe fraction = SIL4 and the Trojan switch has a fault tolerance of 0 and a >99% fail-safe fraction = SIL3.

ANNEX 5

COMPARISON OF INTEGRITY REQUIREMENTS WITH THOSE ACHIEVED

Table A5.1: Comparison of integrity requirements with those achieved

	Hazardous event 1	Hazardous event 2	Hazardous event 3
Target SIL[1]	?	?	?
Calculated failure rate (per hour)	$5.8*10^{-9}$	$1.0*10^{-5}$	$0.37*10^{-6}$
SIL calculated from random hardware failure rates	SIL4	SIL1	SIL2
Architectural ceiling for SIL	SIL4	SIL1[2]	SIL3

[1] See Annex 2 for an explanation of why target SILs are unavailable.

[2] A diagnostic coverage of 60% for the DNC has been assumed, it being likely that the normal control functions of the DNC will achieve this coverage during their normal operation and, as a result, indicate the presence of a fault as a failure to carry out the normal control functions. However, in the author's opinion, it would be unlikely that the DNC would be able to prevent a muting failure (e.g., by stopping the machine) if the output driving KRES2 were to fail to the energized state, unless this particular output was monitored.