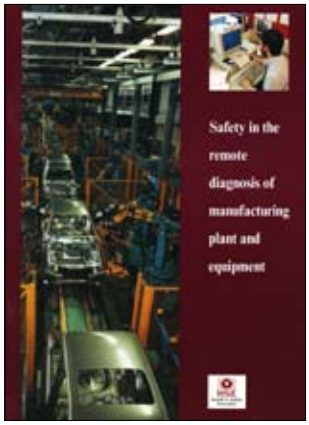
Safety in the remote diagnosis of manufacturing plant and equipment



This is a free-to-download, web-friendly version of HSG87 (First edition, published 1995). This version has been adapted for online use from HSE's current printed version.

You can buy the book at www.hsebooks.co.uk and most good bookshops.

ISBN 978 0 7176 0932 1
Price £12.00

This guidance is issued by the Health and Safety Executive. Following the guidance is not compulsory and you are free to take other action. But if you do follow the guidance you will normally be doing enough to comply with the law. Health and safety inspectors seek to secure compliance with the law and may refer to this guidance as illustrating good practice.

First published 1995

ISBN 978 0 7176 0932 1

This guidance is issued by the Health and Safety Executive. Following the guidance is not compulsory and you are free to take other action. But if you do follow the guidance you will normally be doing enough to comply with the law. Health and safety inspectors seek to secure compliance with the law and may refer to this guidance as illustrating good practice.

Contents

Introduction

1 This guidance concerns remote diagnostic systems fitted to computer-controlled machinery and associated equipment. It does not cover telemetry or remote control, nor does it deal with remote diagnosis in industries other than manufacturing. It does not, for example, deal with systems which may be encountered in process control in the chemical, offshore, mining or nuclear industries.

2 Remote diagnostic systems allow faults in machinery to be identified by a diagnostician at a remote location. Remedial action can then be agreed between the diagnostician and the user. The remote diagnostic system may allow the diagnostician to operate the machine from the remote location, or even correct the faults identified in the software. For the purpose of this guidance, remote diagnosis means:

- the monitoring of program execution from a location remote from the machine or process;
- the monitoring of the condition of computer-controlled plant from the remote location;
- operating the machine for diagnostic purposes from the remote location;
- identifying or correcting faults in the application software by modifying the software at the remote location and downloading the new version to the machine.

3 The publication is intended for controller manufacturers, designers, suppliers and users of computer-controlled machinery who are considering incorporating these facilities. It also questions the need for a remote diagnostic facility. It identifies the risks which may arise from a remote diagnostic facility and describes how machine design and working procedures can eliminate or reduce them. The overall objective is that the addition of the remote diagnostic facility should not increase risks or reduce the existing level of safety.

4 Depending on the circumstances, the user, designer, manufacturer, supplier and those providing diagnostic services may have duties under one or more of the following provisions, of which they should be aware:

- The Health and Safety at Work etc Act 1974;
- The Provision and Use of Work Equipment Regulations 1992;
- The Management of Health and Safety at Work Regulations 1992; and
- The Supply of Machinery (Safety) Regulations 1992.

5 This guidance applies to remote diagnosis used for corrective maintenance of machines including software in the application program. It does not deal with automatic diagnostic facilities or packages, either on the machine or at a remote location. (Where these are provided as part of a remote diagnostic system which does fall within the scope of this guidance, they will need to be included in the assessment of the overall system and conform with the appropriate standards.) It is not appropriate for:

- maintenance or modifications to the executive software, software upgrades or for installing software for new requirements;
- the commissioning and acceptance testing of new or modified machinery;
- making software changes in primary safeguards, eg photoelectric protection systems.

6 Where a remote diagnostic system is being considered for inclusion on machinery the guidance assumes that the machinery is designed and safeguarded in accordance with good practice, for example in accordance with the relevant international, European and national safety standards. These standards include those which concern guarding of dangerous parts, reliability and safety of the programmable hardware, and correctness and safety of software. When a remote diagnostic system is provided, the overall system (machine in combination with the diagnostic system) should be reassessed to ensure that the remote diagnostic system does not reduce the level of safety required at that machine.

Note:
Safe working procedures form an important part of the guidance but they are subordinate to the requirement to make the machine safe by eliminating hazards by design and by safeguarding against hazards which cannot be eliminated.

7 There is a Glossary at the back of this publication which explains terms used. However, the following definitions should be understood before reading further:

Main/remote control station: the main control station for a group of machines or cells from which supervision or control takes place in normal operation. It may be at some distance from the machinery it controls, on the same site or elsewhere. It may include diagnostic and reprogramming facilities – see "remote diagnosis".

Local control station: the control station dedicated to a particular machine or cell which is part of a system governed by a main control station. The local control station is in close proximity to the machine or cell, and enables it to be taken out of remote control and operated directly from the local control station.

Remote control: operating condition when the machine or cell is under the control of the main control station; normally in automatic mode.

Local control: operating condition when the machine or cell is removed from the control of the main control station and controlled by the local control station. It does not receive or respond to signals from any network, remote control station or plant external to the machine or cell.

Note:
1 the facility to switch to local control can be used for setting, tool changes, maintenance, or special operating conditions, eg involving manual intervention. The objective is to prevent unexpected start-up during work of this nature, arising from the machine responding to remote signals;
2 there may be a hierarchy of control systems involving several levels: machine, cell, line, main controller. In these circumstances, the line controller would be local in respect of the main controller, and remote in respect of the cell controller.

The extent of direct control from the remote station may also vary according to the system design. It may also vary between levels in the hierarchy, eg some levels may have a mainly supervisory role, while others directly control the movement of materials around part of the system and the operation of machines.

Software: intellectual creation comprising the program, procedure, rules, data and any associated documentation pertaining to the operation of a computer system.

Note:
Software associated with machine control can be divided into the following broad categories:

- embedded/systems/executive software. Software generic to a particular range of microprocessors or controllers, and an essential part of a specific programmable electronic system and fundamental to its proper functioning;
- applications software. Software to enable the machine to function and to perform a particular task or range of tasks;

– parts programme. Software in computer numerically controlled (CNC) machines which is dependent on the application software and which enables the machine to perform a specific task.

Operator: The person or people including setters and programmers etc who operate the machine in the user's premises.

Remote diagnosis: See paragraph 2.

Remote diagnostic station: the station from which remote diagnosis is carried out. It could be in the same premises, in another part of the country, or abroad. Those at the remote service station may be employees of the company using the machine, or of the suppliers of the machine or of a separate service company.

Note:
this is a facility additional to or separate from remote control, and allows the identification of faults and the alteration of plant parameters, programs, etc, in a way which would not be possible in normal operation from a main control centre.

Remote diagnostic system: comprises all components necessary to enable remote diagnosis to take place, including hardware; software; operating system routines; all interfaces to the control system and safety system; and communications systems.

Overall system: the combination of machine and remote diagnostic system.

Control system: a system whereby input signals from the machine and/or from an operator generate output signals causing the machine to operate.

Safety system: a system specifically intended to ensure safe operation of the machine by technical means, taking account of all conditions of use and reasonably foreseeable misuse.

Safety-related system: any part of the control system or safety system which could affect the safe operation of the machine.

Safety device: a device which eliminates or reduces risk, alone or in association with a guard.

Categories of remote diagnostic systems

8 Remote diagnosis falls into the following main categories:

- Remote Passive Diagnostics (RPD): this is a form of condition monitoring. The diagnostic station can be used to monitor program execution, inputs and outputs and the state of sensors, relays, etc and identify the likely cause of a fault. There is no means to alter the software or control the machine;
- Remote Active Diagnostics (RAD): in addition to condition monitoring, the machine can be operated from the diagnostic location but there is no means to alter the software via the remote diagnostic system;
- Remote Interactive Diagnostics (RID): in addition to RAD there is access to the software from the diagnostic location. This form of remote diagnostics may:

  – involve changes to the control system which could affect the safe operation of the machine (eg sequence of operations, speeds); and may
  – allow changes to be made to safety features (reduced speed, thresholds).

It is possible for the diagnostic system to be constantly on line, or connected only when required. See Figure 1 for guidance on the type of system involved, and where to look for information in this publication.

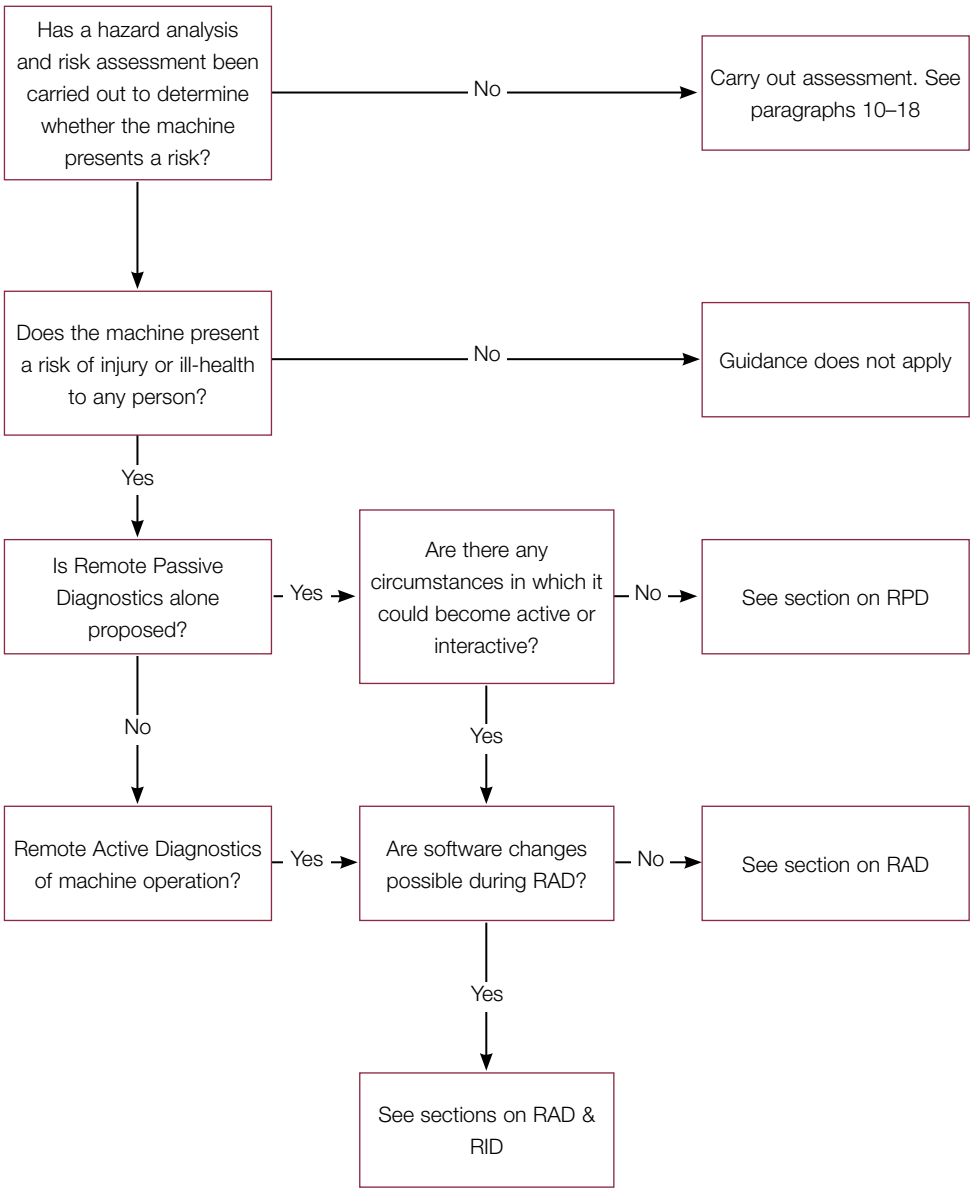
Hazards from remote diagnosis

9 The potential hazards from remote diagnosis are partly dependent on the nature and design of the remote diagnostic facility and partly on the nature of the machine. One way of identifying the relevant hazards is to undertake a hazard analysis specific to the application. Such an analysis will identify those hazards specific to the machine. In addition the following generic hazards and sources of hazards should be considered.

- **Unexpected start-up:** if the remote diagnostic station is capable of operating the machine, it could start up when someone is in a position of danger, eg when carrying out repairs or adjustments unknown to the diagnostician, or when attempting to act on the results of the diagnosis.

Figure 1 Remote Diagnostics

If Remote Diagnostics is proposed:



- Machine malfunction: the nature of the fault the diagnostician is seeking to identify may make continued operation of the machine, or certain operations dangerous. This may not be apparent at the diagnostic station. For example if a component is inadequately clamped, the diagnostician may be unaware of the risk because of false data from a sensor, faulty data transmission, or a failure to appreciate the significance of the information.
- Software change: changing the software concerned with the production process may create a hazard. Changing the sequence of a process, cutting speeds, clamping pressures, outputs from sensors, could all affect the safety of the machine.

Experience of accidents and analysis of available incident data has shown that even apparently minor changes can have a significant effect on the behaviour of the equipment the software is controlling.

Failure to restore the software to its original form after any temporary changes made during diagnosis may therefore cause a subsequent hazard. For example, the diagnostician, investigating a problem with workpiece clamping arrangements may deliberately amend the output from a clamping sensor so that it seems that the clamps have successfully closed, in order to advance the program and test the theory. This could cause danger immediately if the workpiece is moved during diagnosis, or during subsequent operations after diagnosis, if the signal from the clamping sensor continues to be falsified.

Any permanent changes made as a result of diagnosis could, if not properly checked, create a hazard. Failure to record changes properly can also lead to a hazard because any further changes or checks would be based upon incorrect information.

- Changes to the safety-related system: in current designs of computer-controlled machinery changes in software may affect safety functions. The diagnostician may wish to change only software related to the production process, but because of the design of the system software based safety features may also be changed. For example:

  – data changes can alter safety features such as reduced speed;
  – program changes could mean that a hold-to-run button becomes a cycle start button.

Even where the software has been separated into safety-related and non-safety-related modules there will, in most cases, be a need to exchange data. Faults introduced by inadequate control of changes made to the non-safety-related modules could have a ‘knock-on’ effect that could create a hazard.

- Software change caused by data transmission fault or unauthorised access
- Plant operation caused by data transmission fault or unauthorised access
- Failure or fault in the remote diagnostic system and station: eg loss of power at diagnostic end during diagnosis, breach of communications link during diagnosis.
- Design and implementation errors in the remote diagnostic system: these may create potential hazards, eg a design fault in the access control software may permit a system intended to be limited to passive operation to become active or interactive; a design fault in the remote diagnostic system or the way it interfaces to the machine could alter the way the machine operates.

See Figure 2 showing the hazards which may arise according to the type of remote diagnostic system.

Risk assesment

10 Risk assessment of the machine and of the overall system (machine and diagnostic system combined) is essential to enable the supplier and user to determine whether a remote diagnostic system can be used safely. If so, what safeguards should be adopted?

How to assess risks

11 The risks arising from remote diagnosis will vary according to the nature of the machine itself. Before considering a remote diagnostic system, the supplier should carry out a risk assessment of the machine. This should consider:

- the hazards posed by the machine, and the way it will be used, including normal operation, setting, adjustment, cleaning, maintenance and reasonably foreseeable misuse;
- interfaces with, and interactions with, other machines and the effect that changes could have on the safe working of such machines;
- what safeguards are currently fitted and how they operate, in the various operating modes, and whether they are adequate.

An essential part of the assessment is to identify how the safeguards function and what contribution to their correct functioning the programmable controller and the software make. It is very important that the safety-related systems and associated interfaces are clearly defined so that the potential impact of software changes can be assessed.

The type of remote diagnostic system, and the effect that its use could have on the safety of the machine should then be considered. An assessment should be made of the additional failure modes and risks introduced by such a system.

Although the safety of diagnostic software packages is outside the scope of this guidance, if such packages are used it is important to assess whether faults in them could propagate via the remote diagnosis facility and cause a dangerous failure of the overall system.

Figure 2

Type of diagnostic system	Unexpected start-up	Machine malfunction	Software change resulting in danger	Change in software based safety features	Software change from data transmission fault or unauthorised access	Plant operation from data transmission fault or unauthorised access	Malfunction/ failure of remote diagnostic facility
RPD (Remote Passive Diagnostics)						■*	■
RAD (Remote Active Diagnostics capable of causing machine movement)	■	■			■*	■	■
RID (Remote Interactive Diagnostics capable of software changes to the control system)	■	■	■	■	■	■	■

* The above takes into account the possibility that a passive system could be operated in active mode, or an active system in interactive mode, in the event of a design fault or omission.

Is the remote diagnostic system necessary?

12 In the light of this assessment, a decision should be made as to whether a remote diagnostic system of the interactive type is justifiable on safety grounds, or – in practical terms – necessary. Factors to be taken into account include the level of risk, the consequences of failure, eg serious injury, death, and whether practical precautions can be taken to eliminate or minimise the risk.

System design

13 System design is of fundamental importance. The machine itself should be designed using good engineering principles, as described in *BS 5304*[1] and *EN 292*[2]. Information concerning the electrical control system is provided in *EN 60204*[3] and principles for the design of programmable electronic systems are in the HSE PES documents[4]. Further European and International Standards are also relevant[5]. Future designs of safety-related systems may need to take into account the International Standards dealing with the topic. These are currently being prepared by the International Electrotechnical Commission (IEC)[6].

The overall system

14 Essentially, the principles contained in these documents require the designer, manufacturer or supplier to adopt the following measures in the order given:

- design the equipment to prevent hazards arising;
- modify the equipment to eliminate hazards;
- provide safeguarding to segregate people from the remaining hazards;
- provide interlocking or other features to isolate people from hazards;
- list any hazards which cannot be eliminated or guarded against; and
- inform the user of safe working practices and management controls to avoid hazards.

The effect of any modification to a machine, such as the installation of a remote diagnostic system in terms of creation of new hazards or increase in risk, should be fully considered. The above standards should be used when designing or incorporating a remote diagnostic system, to reassess the hazards and risks presented by the machine in conjunction with the remote diagnostic system and to ensure the remote diagnostic system is itself properly designed and suitable for safety purposes.

Security

15 Remote diagnosis opens up potential security risks. Security is concerned with:

- confidentiality – the prevention of the unauthorised disclosure of information;
- integrity – prevention of the unauthorised modification of information;
- availability – prevention of the unauthorised withholding of information or resources.

Typical security safeguards include segregation of vulnerable resources, passwords, encryption, and dial back modems.

This guidance is concerned with security insofar as it affects safety, particularly unauthorised access.

Further information on security risks, countermeasures and assessment criteria can be found in [7].

16 When a remote diagnostic system is to be provided, specific safeguards, in addition to those normally required for safe operation of the machine, will need to be incorporated. These are similar to those required when complex automated

machinery has local control panels and a separate main control station, in order to prevent risks to machinery operators, maintenance staff etc when the machinery is operated remotely. Additional safeguards are required for remote diagnosis because of the ability to change machine parameters, and modify or eliminate certain safeguarding features etc as part of the diagnostic operation. The assessment should identify these additional safeguards and specify them in a safety plan.

Safe working procedures

17 The safety plan should include functional and performance requirements, interface specifications (hardware, software and human), design methodology, verification and validation requirements and operation and maintenance procedures. In particular, the extent and limits of the diagnostic operations to be carried out should be specified. Cross reference should be made to the safety documentation produced in the original design of the machine.

18 Wherever possible, safety should be ensured by means of design changes rather than procedural arrangements. Nevertheless, in RAD and RID in particular, safe working procedures at the user end and the diagnostic end are essential. The system should therefore be designed to enable safe working procedures to be followed, and to reinforce them. Ergonomic design of the work stations, and clarity of information on screen or in supporting manuals are essential. Where software changes are possible (RID) remote diagnostics need to be brought within the software change control procedures of the user and subject to assessment, authorisation, verification and validation. The documentation should be accurate and up-to-date. Safe working procedures are dealt with in more detail in paragraphs 22–23, 30–43, 49–65 but are not exhaustive. See the flowchart, Figure 4, for an example of working procedures for RPA, RAD and RID. See Figure 3 for a summary of requirements for RPD, RAD and RID, covering assessments, safeguards and procedures.

The following three sections give recommendations on potential sources of danger, design safeguards and operating procedures for remote diagnostics. The advice given does not replace the need to apply the general requirements of this section to the particular application.

Figure 3 Summary of requirements: Assessment, safeguards, procedures for RPD, RAD and RID

RPD	RAD	RID
Assessment Active or inter-active mode possible?	Assessment Interactive mode possible? Effects of failure of diagnostic system.	Assessment Configuration of machine control system. Safety system – extent of reliance on software. Effects of software changes on machine operations. Effects of failure of diagnostic system. Can risks be eliminated or reduced by changes in design?
Safeguards Ensure system operates in passive mode only.	Safeguards Machine cannot respond to diagnostic station when access is possible. No means to become interactive. No permanent link. RAD via mode change. Indication – machine under RAD. Means to prevent conflicting commands, user end and diagnostic end. User veto. Communications link. Identify break in link/failure of RAD. Means to control access to RAD. Means to identify which machine is being diagnosed. Clear instructions – user manual. Good message quality.	Safeguards Machine will not respond to diagnostic station when access is possible. Protection against software changes which could affect safe running of machine, eg: – program structure ensures safety functions are executed as intended; – software-based safety functions protected against inadvertent change; – safety-related software inaccessible; means to identify unauthorised changes; – supervisory computer. No permanent link. RID via mode change. Indication – machine under RID. Means to prevent conflicting commands, user end and diagnostic end. User veto. Identify break in the link/failure of RID. Communications link. Means to identify which machine is being diagnosed. Means to record changes. Means to control access to RID. Clear instructions – user manual. Good message quality.
Procedures Safe system for access, maintenance, and for dealing with break in communications.	Procedures Training – user and diagnostician. Authorised people. Access control. Working procedures. Working log. Functional tests.	Procedures Training – user and diagnostician. Qualifications – diagnostician. Authorised person. Access control. Working procedures. Software change control procedures. Procedures if diagnostic system fails. Verification. Validation, including functional tests. Working log. Documentation.

Remote passive diagnostics (RPD)

19 This is a system where the remote diagnostic station can only be used to receive data for interrogation and analysis, and in which the diagnostician has no ability to alter the software or to operate the machine. The link between the diagnostic station and the machine may be permanently made, or activated only when required.

Potential sources of danger (RPD)

20 An assessment should be carried out of the additional failure modes and risks introduced by the RPD. See paragraph 10 for further information on assessment. The following particular matters should be considered in the assessment, but are not exhaustive:

- The system may have been intended to operate in the passive mode only, but due to a design fault may be capable of operating in an active or interactive mode in certain circumstances such as misuse or unauthorised access;
- If the link is permanent, or readily accessible, eg via a dial-up modem, unauthorised access into the system may be possible. Depending on the design of the system, this could be used to change diagnostic modes;
- Operation of the remote diagnostic system indirectly influences the application of a safety-related function. For example, there is a delay in checking the status of a guard because the control system is attempting to handle a communications process;
- Loss of the communication link could happen during diagnosis. If the user is relying on advice from the diagnostician during fault finding or rectification, loss of communication could interrupt the procedure at a crucial point.

The supplier needs to establish that the system can only operate in the passive mode, and to identify any circumstances including unauthorised changes or a fault in the diagnostic system under which the system could become active or interactive.

Safeguards

21 The overall system should be designed so that there are no means by which the diagnostic system could become active or interactive during intended operation or foreseeable misuse. Alternatively, effective measures should be taken to prevent it becoming active or interactive. If this cannot be done see the sections describing safeguards and procedures for RAD and RID. The use of a permanent or readily accessible (eg dial-up modem) link should be avoided where there is any possibility that the system could be operated in active or interactive modes.

Note:
In some systems a permanent dedicated communications link is provided. More usually, public networks are used. ‘Auto answer’ is a system by which the machine controller responds automatically to an appropriately coded message transmitted over the public network. ‘Auto call’ or ‘call on fault’ involves the equipment automatically dialling a pre-programmed number, usually in response to a fault condition being detected.

In manual answer the operator at the user end has to authorise the use of the link, eg the remote station attempts to make contact and the user presses a button to

connect the modem.

'Auto call back' is implemented (usually by a special modem) at the user end. Its main purpose is improved security compared with 'auto answer'. The call is initiated by the diagnostician. The special modem at the user's end answers the call and receives a code or password from the diagnostician, but does not connect the call to the PLC at this time. The call is then cleared and, after a short time delay, the user's special modem calls a pre-programmed number (the diagnostician) and connects this call to the PLC.

The security improvement results because the special modem only connects the PLC to calls which it has originated itself, to number(s) pre-programmed by the user. The worst that an unauthorised caller could do would be to cause an unnecessary call to the diagnostician's equipment.

Procedures

22 Depending on the arrangements between the user and the provider of the diagnostic service, the safe working procedures for access and maintenance will vary, eg:

- The diagnostician may inform the user by telephone link of what needs to be done. Reliance is then placed on the user following safe procedures for access to the machine and for maintenance which would apply under other circumstances: using correct access procedures, isolating the machine etc. Further guidance on machinery design and maintenance features is given in BS 5304:1988[1] and HS(G)43 *Industrial robot safety*[8]. If the user undertakes software changes as a result of RPD, the user will need to follow up appropriate change control procedures and ensure the diagnostician is informed. Procedures similar to those described in paragraph 51 will be needed.
- Alternatively the remote diagnostic station may identify the fault and send its own engineers to carry out the repair. The same requirements for following safe working procedures for maintenance will apply.

23 If the communications link breaks down during diagnosis, work at the user end which is dependent on advice from the diagnostician should be suspended, until communications have been restored and the machine put into a safe state. If communications must be maintained, a back-up link should be available.

Remote active diagnostics (RAD)

24 In this system it is possible for staff at the remote diagnostic station to interrogate the machine control system on the status of the machine and its program and, in addition, to operate the machine remotely, eg to start it up, stop it, execute certain routines etc. The machine may be connected via a dedicated line or a telephone link and there is likely to be an additional telephone link which allows direct communication between the user and diagnostician. The diagnostic station may be at another part of the same premises, or in a completely separate location.

Potential sources of danger

25 An assessment should be carried out of the additional failure modes and risks introduced by the RAD (see paragraph 10). The following matters should be considered in the assessment, but are not exhaustive:

- The system may have been intended to operate in the active mode only, but due to a design fault may be capable of operating in interactive mode in certain circumstances, such as misuse or unauthorised access;
- Unauthorised access into the system may be possible;
- The design of the machine may mean that certain types of remote operation are dangerous;
- Operation of the remote diagnostic system indirectly influences the application of a safety-related function. For example, there is a delay in checking the status of a guard because the control system is attempting to handle a communications process.

26 The supplier should establish that the machine can only be used for receiving data and machine operation. If software changes are possible, eg through changing the privileges of the remote terminal, either effective means will be required to prevent such change occurring, or further precautions for RID will be required.

27 The effects of a diagnostic system or communications link failure during the diagnostic operation should be considered:

- Can the machine be made to go automatically into a safe state, or does action need to be taken at the user end?
- Also, how will the failure of the diagnostic facility or the link be identified, and how rapidly?

Safeguards

29 This list of safeguards is not exhaustive:

- Machine safeguards should be designed so that when guards are open or safety devices such as photo-electric curtains or pressure sensitive mats activated, the machine will not operate, whatever commands are sent from the remote diagnostic station.

  Some machines have a setters override, which allows limited machine functions with the guard open, or a teach pendant which allows the machines to be moved or programmed under controlled conditions by an operator in the danger zone. In these cases selection of the override or use of the teach pendant should automatically preclude remote active diagnostics taking place at the same time.

- The RAD should either be designed so that there is no way in which it could become interactive during intended operation or foreseeable misuse or effective measures should be taken to prevent it becoming interactive. If this cannot be done, see the RID section.
- Unauthorised electronic access to the machine via the link should be prevented. For example, although the machine may be permanently connected to the diagnostic link when only capable of passive diagnosis, a permanent link established in active mode is not considered to be acceptable, because of the possibility of unauthorised access. Activation of the link should be subject to control or consent from the user end.
- Linking up to the remote diagnostic system in active mode should only be possible by a mode change, eg to remote/service by means of a key operated switch. The switch should be linked with the controls of the machine to prevent it being left permanently in the remote diagnostic state. This will make it possible to switch to active diagnostic mode only when the machine has been switched out of automatic mode and into manual mode, or switched off. A key exchange system could be used, along with a key or password held by an authorised person.
- There should be a way of preventing conflicting commands being given to the machinery at the user and diagnostic end. For example, when the diagnostic station can operate the plant directly, once the active diagnostic facility has been activated, all commands from the local control should be disabled, other than the emergency stop and a 'confirm' function key.
- There should be indicators stating "machine under remote diagnostic control for test/service" wherever machine movement can be initiated and, in addition, on large machines, on an indicator board visible from all working areas.
- The system should be designed so that any movement of the machine will only be possible after consent has been given at the user end, and the user should have effective veto over any action the diagnostician proposes. For example:

  – the diagnostic station may inform the user of the necessary action, and the operator at the user end carries it out; or
  – the operator may confirm every step of movements proposed by the diagnostician in single step mode; or
  – the operator may confirm the proposed operation of a sequence of movements.

  One method of achieving this is to have a message on the screen at the user end detailing the proposed action. For the action to be carried out, the user must press a confirm key. A telephone link should be set up to enable the implications of the proposed action to be discussed and clarified. Movement in automatic cycle should be avoided. If it is needed, the change from single step or manual RAD into automatic mode should be under the control, or subject to a further veto, of the operator.

- There should be effective communication links between the diagnostic and user end to enable the principle described in (g) to operate. The communication link should include a telephone link, to enable user and diagnostician to discuss the purpose and the implications of the proposed action. Operating manuals should describe how to use the telephone line, eg standard forms of words and procedures such as the receiver repeating the statement. A text message on a screen can also be used as part of the communication system. Instructions or proposals on the screen can be confirmed by the operator, who takes the appropriate action or confirms the action by the diagnostic station. There should be a way of recording what has been done, eg the text message can be recorded.
- There should be a way of identifying as rapidly as possible any failure in the communications link or diagnostic facility during remote diagnosis. There

should also be a way of putting the machine into a safe state automatically, or if appropriate an error message should be generated and displayed, which will enable the user to take the appropriate action.

- Access via remote diagnostic terminals should be capable of being controlled and restricted to authorised people only. The functions which a remote diagnostic terminal can perform should be strictly limited to what is necessary and the means to increase the range of functions available should either be initiated or made effective solely from the user end.
- There should be a way of identifying which machine has been connected to the diagnostic station. This should appear on the diagnostic screen. If a printer is available at the diagnostic end this information should be recorded on it.
- Instructions which appear on the user's VDU should be clear, unambiguous and sufficient for the instruction or proposed action to be understood by the user, so that they can either confirm or carry out an action proposed by the diagnostician. Any ambiguity, for example when a user is being asked to confirm a command to operate the machine, could lead to the operator unwittingly creating a dangerous situation. In addition to instructions on the screen being clear and unambiguous, there needs to be a comprehensive user's manual explaining the instructions and their effects.
- The performance of the data link (including the modems) should be such that the overall data error rate between the user terminal and remote diagnostic station is acceptable and does not lead to potentially dangerous data or program corruptions. The use of modems which implement an effective error detection and correction technique to protect against interference is advised.

Procedures

This list of procedures is not exhaustive.

Training

30 The user should ensure that anyone who has to initiate active diagnostic mode and respond to the remote diagnostic station is fully trained and competent. The training should include direct practical experience. Depending on the complexity of the machine and the type of work which needs to be done, there may need to be a team of trained people, including fitters and electricians under the general supervision of an authorised person who initiates interactive diagnostic mode, and is in general charge of the diagnostic and repair work at the user end.

31 On simpler installations, a supervisor, fitter, or plant operator may be trained and authorised to initiate active diagnostic mode. Staff at the user end need to know in detail how the machine operates, what hazards it presents, and how the diagnostic system is operated at the user end, and how they are expected to respond to the diagnostician. In addition to a diagnostic user's manual, the supplier should provide a description of the operator's duties, and may need to be involved in training the user's staff.

32 The diagnostician needs to know the machine in question and have first hand experience of it, and how it operates. They must know the hazards it presents so that they do not propose unsuitable actions to the user. The diagnostician should be competent in software engineering and capable of interpreting the program and the associated documentation.

33 A system of named authorised people is recommended at the diagnostic and user end, so that people at each end know that they are dealing with someone familiar with the machine and authorised to propose or confirm action.

Access control

34 Before the machine is put into diagnostic mode:

- it should be put into a known state, as set down in the remote diagnostics operating instructions;
- the area should be cleared of staff; and
- all safeguards which may have been removed or suspended for any reason before the decision to invoke remote diagnosis should be reinstated.

An authorised person should carry out these responsibilities.

Note:
If a fault has occurred it may be that maintenance staff have already been working on the machine and have removed guards and are in a position of danger.

The authorised person switches to diagnostic mode or makes the physical connection which links the remote diagnostic terminal to the machine. The authorised person or someone under their direct supervision then has the task of confirming the actions proposed by the diagnostician, if necessary after consultation with others with a more specialist knowledge of the machine.

35 Operation of the diagnostic system should be controlled, eg:

- access to the terminals should be restricted, (a key or identity card should be needed to enter the control room); or
- a password should be required to activate the terminal (user end computer denies access from any terminal unless the correct password is used).

The principle of the system should be that the linking up of a particular machine to the active diagnostic mode is dependent on actions of the user (machine) end. Procedures at the diagnostic end should ensure that the machine to be diagnosed is correctly identified.

Running the machine from the remote location

36 There may be a need for the diagnostician to operate the machine as part of the fault identification procedure. It should only be possible to do so after confirmation by the user. The diagnostician should, where possible, operate the machine at the lowest practicable parameters, eg speed and pressure, and limit the extent of the movement, and only operate the machine at normal speeds when the machine dynamics affect fault identification. Operating the machine on automatic cycle should be avoided except when this is found to be essential for fault identification.

Fault rectification

37 The fault finding process may involve some physical repairs or modifications to the machine, eg adjusting limit switches, photo cells, altering clearances. Such work would be followed by another diagnostic test from the remote station. The implications of these changes need to be considered before they are tried out on the machine. Any changes need to be recorded (see paragraph 42). This also enables a check to be made as the machine is put back to its normal state. See Figure 4. (This also covers remote interactive diagnostics.) This may involve staff at the user end working on the machine during the diagnostic operation.

38 Before such work begins the system should be switched from active diagnostic mode to passive mode or if there is any possibility of the diagnostic system indirectly influencing the operation of the safety functions, the diagnostic link should be broken. This should be part of the access procedure. If the repair work needs to be carried out with power on, it is essential that the active diagnostic link is broken.

39 After the work has been carried out at the user end, with guards replaced and safety devices activated, the machine and its control system can be restored to normal operating condition, before the diagnosis proceeds. The diagnostician can then check the effectiveness of the work.

40 If the communications link breaks down during diagnosis, work at the user end which is dependent on advice from the diagnostician should be suspended until communications have been restored and the machine should be put into a safe state.

41 If the RAD breaks down during diagnosis or operation of the machine from the remote location, the safe working procedures outlined in the operating manual should be followed to ensure the machine can be made safe. Even though RAD operation of the machine should only be possible with all safety devices operating, attempting to resume or continue rectification work at the user end could be dangerous if the machine has stopped mid-cycle. If software changes are implemented as a result of the RAD procedure, it will be necessary to follow appropriate change control procedures, similar to those described in paragraph 51.

Working log

42 A working log should be kept at the user and diagnostic ends. The working log is particularly important for the user, since it summarises for the benefit of the next shift, or the normal machine operator, the faults which have been dealt with and the physical changes made to the machine. An authorised person should check it regularly.

Functional tests

43 After changes have been made the machine should be returned to normal operating mode, and functional tests on safeguards, machine operation etc carried out. These should be outlined in the operating manual. The remote diagnostic station may continue to monitor the state of the machine, in passive mode only.

Remote interactive diagnostics (RID)

44 Some systems allow software changes to be made from the remote diagnostic station, as well as monitoring and machine operation already detailed. The changes may be to data, or programs, or, usually, both.

Potential sources of danger

45 An assessment should be carried out of the additional failure modes and risks introduced by the RID (see paragraphs 10 to 18 for further information on assessment). The following matters should be considered in the assessment, but are not exhaustive.

46 In addition to the points noted in the assessment of RPD and RAD, the supplier should consider the following:

- (a) Is the system suitable for RID? Systems which have a high level of complexity or which rely extensively on software for their safety may not be suitable for RID. An assessment should be carried out of the configuration of the machine control system to establish:

  – how many channels are there?
  – are they all PES based, or are any hard-wired?
  – is there cross monitoring?
  – what degree of interdependence is there?

  For example, if any part of the safety-related system relies on a single channel PES, software changes could affect the safety of the machine.

  If there is a dual channel PES based system, a change could be introduced on one or both channels which could affect the safety of the machine. If a fault on one channel is not detected by the other channel, eg via cross monitoring, the system becomes single channel. Depending on the level of interdependence of the channels, a change to one channel could affect both.

  Functional testing of a dual channel system after software changes have been made may not be enough: a safety feature may be deleted on one channel and masked by the correct performance of the other and the system may, as a result, become single channel for that feature.

  This assessment may reveal that the safety-related software is more extensive than was originally believed. It may also reveal a level of complexity which calls into question the suitability of the system for RID.

- Inadvertent changes to safety-related software may degrade safety functions or prevent them from being correctly implemented. Even when measures (eg use of non-volatile memory) are taken to protect safety-related software, there can be a risk resulting from changes elsewhere in the system which prevent the correct implementation of the safety routines.
- Is there a separate hard-wired safety system which in the event of a failure of the software-based system will carry out the appropriate safety functions? It is important that this channel has sufficient safety integrity to ensure these

functions are performed. It is important to consider that even when a separate system of this sort exists, there may still be safety functions (eg reduced speed) which are software based.

- Are there safety features applicable in certain modes which are software-based? Even a machine which has a totally independent hard-wired safety system for normal operation may use software-based safety features in certain modes, eg software-based speed reduction and hold-to-run button during teaching. These software-based features could be deleted or radically altered during software changes.
- What effect could changes to the software governing the operation of the machine have on its safe operation, in normal operating mode, in teaching, setting, cleaning or maintenance? Even with a totally independent safety system which cannot be altered from the diagnostic station, there may be some aspects of the machine's performance which, if wrongly amended, could lead to danger. These include speeds, feed rates, outputs from sensors, sequencing (which could result in collisions and ejections of parts if changed wrongly). Where control and safety systems are combined or overlap, great care will be required in assessing what the possible consequences of erroneous changes would be. In such cases, safe procedures for software change control will be particularly important.

Note:
Maintenance staff may have to carry out some fault-finding and adjustment with the machine under power. If the machine behaves in a way contrary to that expected, they could be at risk.

- What effects could a failure of the diagnostic system, or the communications link cause during the diagnostic operation? Can the machine be made to go automatically into a safe state, or does action need to be taken at the user end?

  How will failure of the diagnostic facility or the link be identified, and how rapidly?

47 If potential problems are identified, the supplier will have to determine:

- whether the risks can be eliminated by a change in design of the control or safety systems;
- whether they can be reduced by such changes, and by adopting safe working procedures, including software change control measures.

Safeguards

48 In addition to the safeguards listed for passive and active systems (types RPD and RAD) the following safeguards should be incorporated. They are not exhaustive.

- The safety system should be designed and be sufficiently reliable to ensure that when guards are open, or safety devices such as photo-electric devices activated, the machine will not operate, even when software changes are made at the remote diagnostic station. This can only be assured when the safety functions are hard-wired, or have a hard-wired back-up. This will not ensure absolute safety, as there are, on many machines, safety-related features which are part of the control system or which, although separate, are realised in software, and which are susceptible to deliberate or accidental changes. Nevertheless, properly designed safety systems involving hard-wired interlocked means of access provide greater safety for maintenance staff who have to carry out repairs to the plant during the diagnostic exercise than safety systems which rely solely on the correct operation of the PES.

- Software changes should be subject to user confirmation or veto – see paragraph 29(g).

  The nature of the veto will depend on the machine, its level of risk, and in particular on the level of skill and knowledge of the operator, who may be a software engineer or someone who is unfamiliar with software and programming. The veto may range from confirming every key stroke to confirming a series of changes displayed on a screen, and to giving confirmation for the diagnostic station to make a range of amendments.

  A text message on a screen can also be used as part of the communication system. Instructions or proposals on the screen can be confirmed by the operator, who takes the appropriate action or confirms the action by the diagnostic station. The text message can be recorded. This, along with the working log (paragraph 64) provides the raw data for improving procedures, and would also be useful in identifying the causes in the event of plant failure, and assist in verification of any software changes.

- Effective communication links should be set up – see advice in paragraphs 29 (h),(i),(j),(k),(m). In particular this allows the implications of software changes to be discussed.
- There should be a way of recording the work: the text message referred to in paragraph 29(h) can be recorded, or a printer used at the diagnostic end to record, eg which machine has been connected to the diagnostic station and the sequence of events.
- There should be access control – read the advice in paragraph 29(j).
- Safety-related software should be protected from inadvertent change. Several varieties of non-volatile semi-conductor memory can be used to decrease the risk of such change. Guaranteed execution of safety functions requires a detailed consideration of the programme structure and the local hardware.

  There is some benefit in storing safety functions in read only memory, eg EPROM. This protects against accidental or deliberate changing of this particular part of the program, but does not prevent the effect of the safety function being nullified by changes elsewhere in the program.

  Storing safety functions in ROM will not guarantee that the functions are executed on schedule. A remote RID operator may install some very high priority application functions which monopolise the CPU and lock out the safety functions (whether in volatile or non-volatile memory). To ensure that safety functions are executed as intended, a more general consideration is needed of the overall program structure and the local hardware.

  There may be considerable difficulty in isolating the safety functions from the application software. If a safety function consists of an operation (eg ‘check the limit switch’), then it is very likely that the operation will be contained within the application software. It will usually be impractical to isolate such safety functions into a special non-volatile area of memory. In contrast, if the safety function consists of a set of data values which the application software reads periodically, then it may be practical to isolate these values in non-volatile memory.

  Sometimes data essential to a safety function, such as the value of a reduced speed, are held in RAM to allow for adjustments and changes at the commissioning stage. Such data are readily accessible to the programmer of the remote diagnostic station, and if changed it could lead to danger when the machine is next run on what is anticipated to be reduced speed. Some protection is given if there are additional safeguards embedded in

the system, eg if there is also in ROM a threshold value for reduced speed which, if exceeded, triggers an emergency stop.

- There should be means to prevent unauthorised people from making program changes which could affect the safety-related software and the safe running of the machine.

  Wherever possible, the areas of software which can be accessed by the authorised person should be limited and safety-related software stored in an inaccessible area. It is recognised that this can be difficult and that much of the control program and data will affect the safe running of the machine. In these circumstances considerable reliance has to be placed upon strict procedures controlling the checking of the proposed changes before coding. Actual changes made need to also agree with those proposed – this is dealt with in the section on procedures.

  It is possible to identify that changes have been made, which is useful in the case of unauthorised access. For example, the machine can keep a running count of all program changes and raise an alarm whenever the number alters. Since an unauthorised person might delete the alarm facility, the changes should be capable of being detected on interrogation by the programmer.

  It is also possible to run an off-line comparison between previous and new versions of software via a separate computer, running a comparison test and flagging up inconsistencies.

  A more sophisticated system involves a supervisory computer which supervises the execution of the programme in the controller in real time and identifies programme and data changes. This has the advantage of pin-pointing the change, but the disadvantage of increased cost in terms of hardware and software. Its use may be justified when an additional PLC is used for other purposes, and in high risk applications.

Procedures

49 In addition to the procedures for remote active diagnostics the following further matters should be taken into account. They are not exhaustive.

Training

50 In addition to the requirements for RAD the diagnostician should be competent in software engineering, capable of making program amendments and documenting them and be fully familiar with the software running the machine. He or she should also be trained in verification and validation procedures and be aware of the implications of proposed data and program changes.

Change control procedure

51 The procedures for amending software during the course of and as a result of remote diagnostics should be subject to and integrated with the user's change control procedure. The procedures should involve:

- assessment of the effects of the changes proposed by someone with appropriate knowledge of the machine and its control system;
- authorisation of the change at an appropriate level;
- verification and validation of the changes made;
- amendments to documentation; and
- amendments to all back-up copies of software (at user and diagnostic ends).

Change control procedures are needed for any amendments made locally, eg by the user and to ensure that the diagnostician has an up-to-date version of the software in case changes are made. The diagnostician should be notified of any machine modifications which should be fully documented.

Software changes from the remote location

52 Remote interactive diagnosis should only be carried out when the machine is in a known state, as described in the remote diagnostics operating instructions. An authorised person at the user end should, in consultation with the diagnostician, ensure and confirm that this state has been achieved (see also paragraph 34).

Failure of diagnostic system or communications link

53 Failures should be identified quickly and the user informed automatically. Ideally the machine should revert to a safe state but if failure happens during diagnosis involving software changes, the machine is likely to be in an intermediate state, which means the consequences are hard to predict. Procedures should be set down to enable the user to bring the machine to a known state. This may involve bringing the machine to a stop, and reverting to a known, previous, good program, or completing the software change.

Verification, validation and testing

Verification

54 Diagnostic software changes amount to software maintenance and the appropriate procedures should be followed. The HSE PES documents[4] should be consulted for more detailed information. The emerging IEC Standards [6] also deal with this subject. The flow chart (Figure 4) gives an example of the sequence of procedures with respect to remote diagnostics.

55 A verification plan should be drawn up for the particular machine which details the procedure at the diagnostic end. This will include, as a minimum, checks of program changes made against the original program by someone other than the diagnostician, and who is competent in software engineering and validation and verification procedures.

56 The amended program should be supported by documentation which describes why the changes were made and what they intend to do.

57 The verification should also check that temporary changes, made as part of the diagnostic process, have been restored to their previous state. These changes should have been recorded on the working log.

58 The user will also need to integrate software changes arising from remote diagnosis into their normal internal procedures for software changes. The person at the user end, before confirming and downloading a software change, may therefore need to seek authorisation from within the user company structure before going ahead (this is particularly applicable in the example of a user veto given on page 31). If the installation has a separate computer which monitors the operation of the machine controller, that can be used to assist in identifying program and data changes, as part of the verification procedure at diagnostic and user ends.

Validation and testing

59 A validation plan should be drawn up for the machine, to cover validation of software changes. It should describe who will carry out the validation and how it should be done. Some validation can be done from the diagnostic end, but some will require action at the user end, eg testing particular functions.

60 As part of the validation plan a test plan should be drawn up. This should include functional tests of all safety devices, and a dry run in single block mode or at slow speed with no material or workpiece if this is feasible, during which essential functions are monitored – timings, speeds, clamping, transfer. It may only be possible to test certain functions with the material in place (clamping, transfer sequences) in which case appropriate safeguards should be in place to protect operators and maintenance staff from inadvertent ejection of parts or materials. The extent of tests on other functions will depend on the nature of the software change and its impact on these functions.

61 The functional test of safeguards should include interlocked access points, stop devices, and the function of safety-related devices such as jog buttons, slow speed devices, single-cycle buttons etc.

62 Before validation begins, the machine control system should be returned to its operational state. In order to do this, the record of changes made should be examined (eg by reference to the log from the printer, and the working log). If any changes have been made they should be removed or documented, as appropriate.

63 The outcome of the validation and testing should be recorded at user and diagnostic ends.

Working log

64 A working log should be kept at the user and diagnostic ends listing what, if any, software or physical changes have had to be made. It should include the name of the person at the user end, the name of the diagnostician, the plant and the PLC concerned, the faults which occurred, and a description of the changes made to software, both data and programs. It should describe any physical changes or repairs and their implications for plant operation and safety and state whether they were successful. It should include the date and the time diagnosis began and finished.

Documentation

65 It is important to keep documentation accurate and up-to-date. The following should be carried out:

- Record any software changes which have a life beyond the time of the diagnostic exercise, eg on a printer at the diagnostic end.
- Make a new back-up software disk which is suitably labelled, documented and marked with a unique version number. Destroy earlier versions or clearly label them as being superseded. The new version should be verified before being stored as a master copy.
- The diagnostician should send a description of the changes made to the user, containing enough information, as in the working log, to identify the machine, the software version, the change made and the date of the alteration. This should be done quickly, if possible, eg by facsimile transmission. The diagnostician should keep a master copy so that the documentation of the software specification and design, including flow diagrams, etc can be amended.
- The diagnostician should go through the appropriate procedures, as established by the diagnostic station in accordance with the user, to record these changes. The amended documentation, or amended sections, should be copied to the user.

Example of remote diagnostics facility

The system

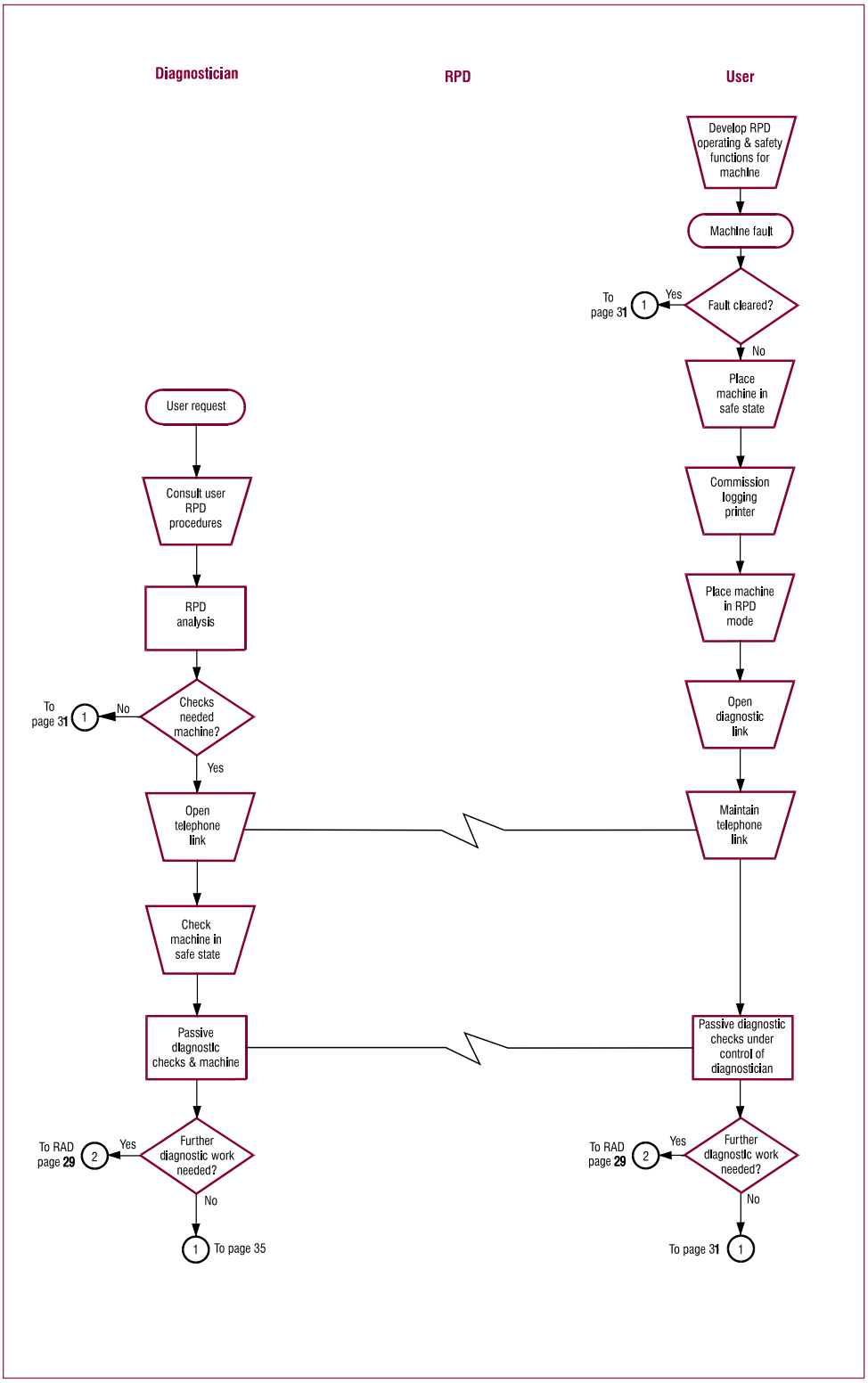
The remote diagnostic station is linked via a modem to a local programming unit within the factory which is connected at the user's discretion to the diagnostic station.

An authorised person (software engineer or technician with sufficient competence in software issues) at the user factory would have the facility to allow the diagnostician, via a switch mechanism, to monitor various statuses in the PLC via the link.

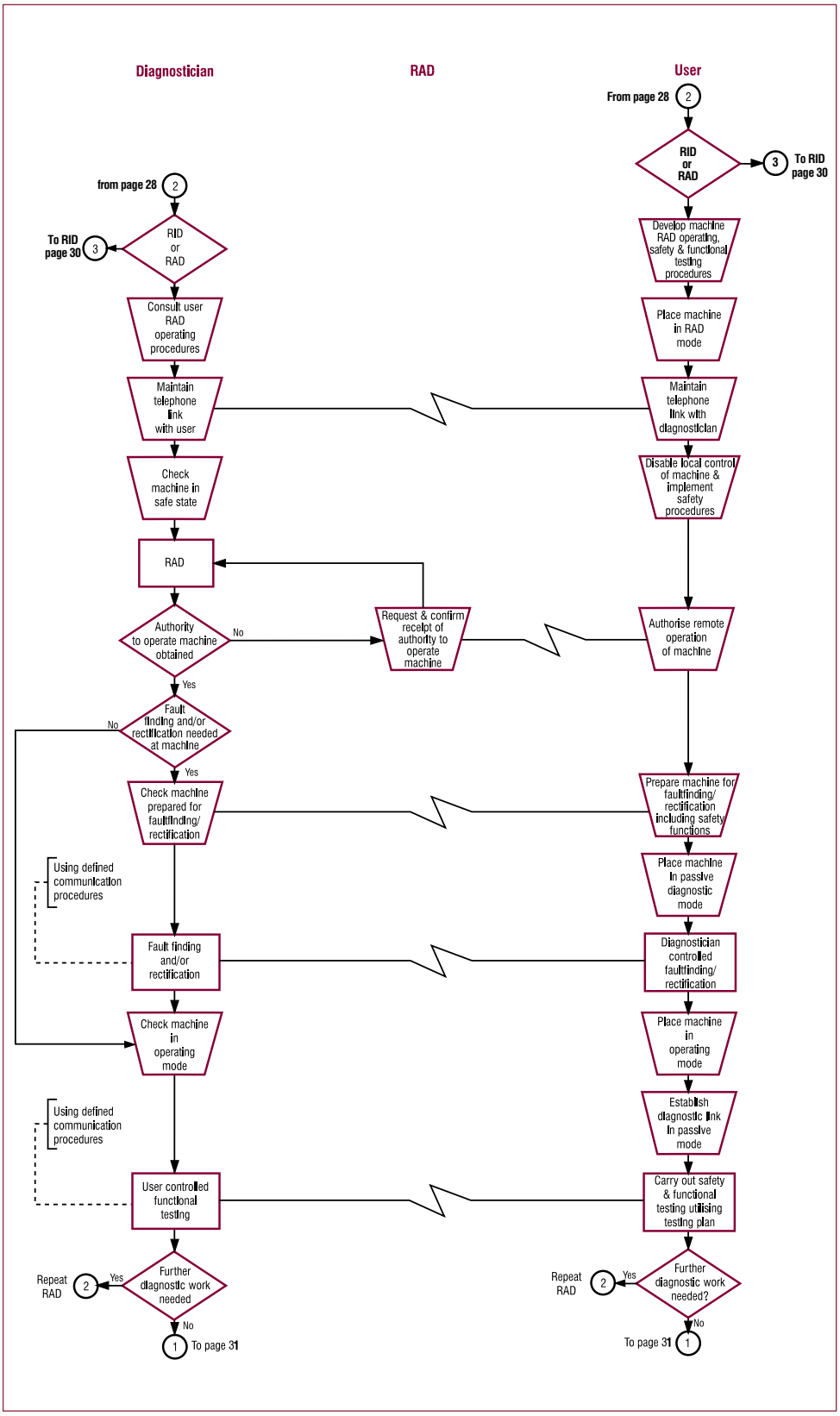
When a fault has been located the diagnostician recommends the change: this change would then be downloaded to the local programming unit only via the link. A telephone link is provided and should be used in addition to the modem data link, to discuss the implications of the proposals.

The user's authorised person then has the ultimate responsibility to download the change into the PLC, having followed the user's in-house systems for authorisation of software changes, for verification and validation of the changes and for amendment of the documentation.

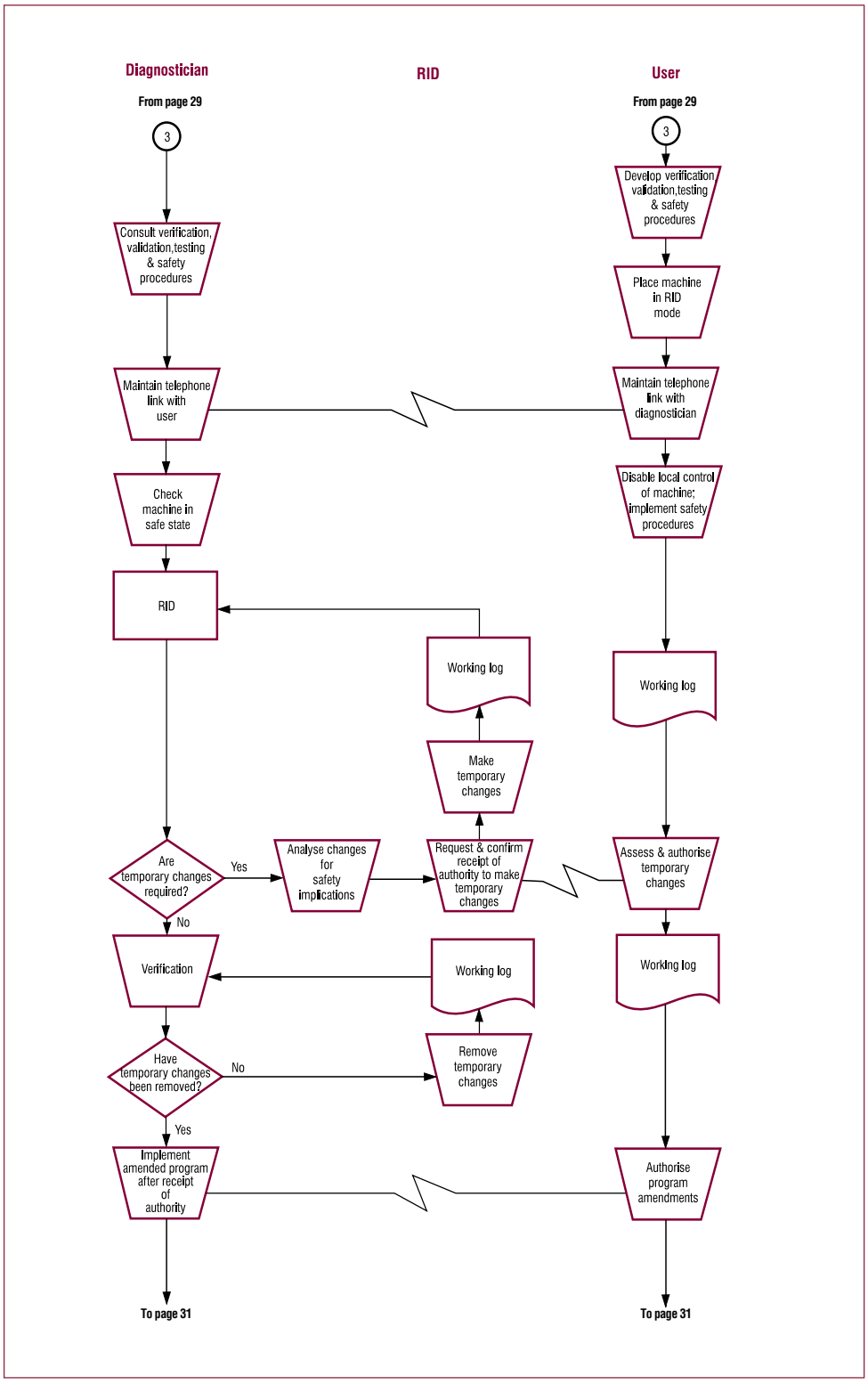
Figure 4 Flow chart: Remote diagnostics operating procedures



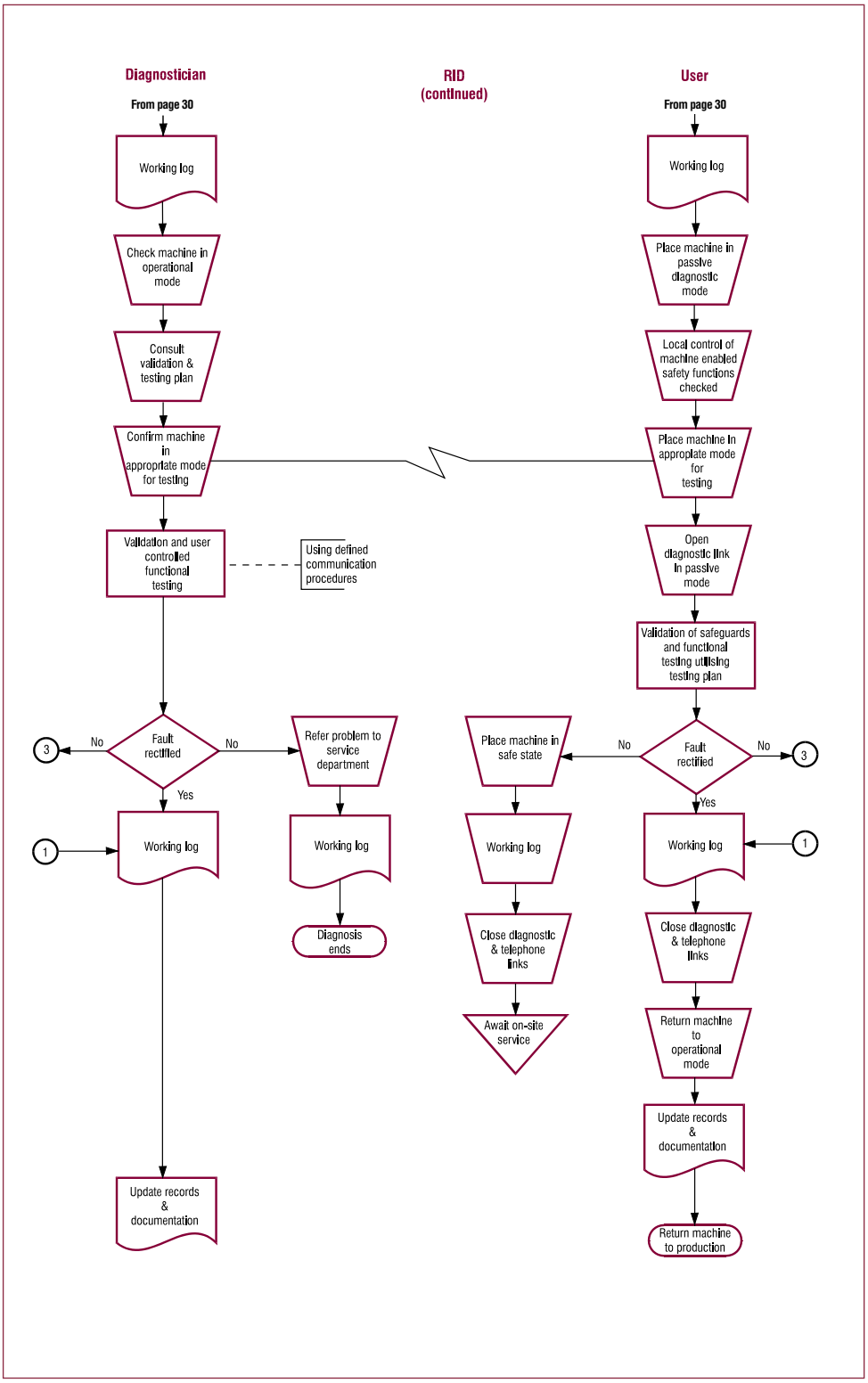
Flow chart procedures continued



Flow chart procedures continued



Flow chart procedures continued



Glossary

EEPROM chip: electrically erasable programmable read only memory, also called EAROM (electrically alterable ROM) is similar to EPROM, but can be erased electrically while in the computer. Either a single byte or the entire memory can be erased. This means that the data stored can be altered by the user and safety-related data can be altered or erased. The memory is non-volatile.

EPROM chip: the program on the chip can be erased by a specific action, eg removing the chip and exposing it to UV light, after which it can be reprogrammed. There is a limit to the number of times this can be done. Chip memory deteriorates over time because of charge dissipation – 10 years has been suggested as a limit.

Hazard: a physical situation with the potential for human injury.

Hazard analysis: a systematic qualitative analysis to identify hazards, event sequences, hazardous events and their severity and consequences.

PES: Programmable electronic system – a system based on a computer connected to sensors and/or actuators on a machine for the purposes of control, protection and monitoring.

Port: an access point in an electronic circuit, device, network or other apparatus where signals can be input or output, or where the variables of the system may be observed or measured.

RAM: means random access memory, but is always used to refer to a memory which can be read from and written into, and which can be altered by the user. It is also (usually) volatile, ie if power is removed the contents of the memory are erased.

Risk: the probability of harm (injury or ill health) arising from a hazard and the degree or severity of that harm.

Risk assessment: a comprehensive estimation of the probability and degree of possible injury or damage to health.

ROM: read only memory – a permanent means of storing data or instructions, such as a mask-programmed device. When the manufacturer puts the metallication on the chip, the connections are made which define the stored data. These devices can be incorporated into larger programs by designers of controllers. ROM chips are non-volatile and cannot be written into.

References

1 BS 5304:1988 *Code of practice for safety of machinery* ISBN 0580 1634 4X

2 BS En 292 1991 *Safety of machinery – Basic concepts – General principles for design Part 1:Basic terminology, methodology* ISBN 0580 2023 21

Part 2: Technical principles and specifications ISBN 0580 2036 46

3 BS EN 60204-1:1993 *Safety of machinery – Electrical equipment of machines Part 1:Specification for general requirements*

4 HSE *Programmable electronic systems in safety-related applications:*

Part 1: *An introductory guide* HSE Books 1987 and 1993 ISBN 0 11 883913 6

Part 2: *General technical guidelines* HSE Books 1987 and 1993
ISBN 0 11 883906 3

5 Further CEN Standards (non machine specific) relevant to this document:

BS EN 418: *Safety of machinery:Emergency stop equipment:Functional aspects. Principles for design* ISBN 0 58 020861 3

CEN pr EN 1050 *Safety of machinery:Risk assessment*

CEN pr EN 954-1 *Safety of machinery:Safety-related parts of control systems:Part 1:General principles for design*

CEN pr EN 574 *Safety of machinery:Two-hand control device*

CEN pr EN *Safety of machinery:Pressure sensitive protective devices:Part 1:Requirement and test procedures for pressure sensitive mats and pressure sensitive floors*

CEN pr EN *Safety of machinery:Pressure sensitive protective devices:Part 2:General principles for the design and testing of pressure sensitive edges and pressure sensitive bars*

CEN pr EN 1088 *Safety of machinery:Interlocking devices with and without guard locking:General principles and provisions for design*

CEN pr EN 953 *Safety of machinery:General requirements for the design and construction of guards (fixed, movable)*

CEN pr EN *Safety of machinery:Pressure sensitive safety devices Part 3:Requirements and test procedures for pressure sensitive bumpers and plates*

CEN pr EN 1037 *Safety of machinery:Isolation and energy dissipation:Prevention of unexpected start-up*

CEN pr EN 626 *Safety of machinery:Principles for machinery manufacturers on reduction of risk to health due to hazardous substances emitted by machinery: Part 2:Methodology leading to verification procedures*

International Standards relevant:

ISO 11161 *Industrial automation systems:Safety of integrated manufacturing systems:Basic requirements*

ISO 10218 *Manipulating industrial robots:Safety* (CEN EN 775:1992)

6 Draft IEC 1508–1 *Functional safety: Safety-related systems: Part 1: General requirements* 65A/179/CDV

Draft IEC 1508–2 *Functional safety: Safety-related systems: Part 2: Requirements for electrical/electronic/programmable electronic systems* 65A/180/CD

Draft IEC 1508–3 *Functional safety: Safety-related systems: Part 3: Software requirements* 65A/181/CDV

Draft IEC 1508–4 *Functional safety: Safety-related systems: Part 4: Definitions and abbreviation of terms* 65A/182/CDV

Draft IEC 1508–5 *Functional safety: Safety-related systems: Part 5: Guidelines on the application of Part 1* 65A/183/cdv

Draft IEC 1508–6 *Functional safety: Safety-related systems: Part 6: Guidelines on the application of Parts 2 and 3* 65A/184/CD

Draft IEC 1508–7 *Functional safety: Safety-related systems: Part 7: Bibliography of techniques and measures* 65A/185/CD

7 *Information Technology Security Evaluation Criteria* (ITSEC) Commission of the European Communities, Directorate X111/F SOG-IS Secretariat TR61 02/3 8, rue de la Loi, 200, B-1049 Brussels

8 HSE *Industrial robot safety* HS(G)43 HSE Books 1988 ISBN 0 11 883999 3

Further information

For information about health and safety ring HSE's Infoline Tel: 0845 345 0055 Fax: 0845 408 9566 Textphone: 0845 408 9577 e-mail: hse.infoline@natbrit.com or write to HSE Information Services, Caerphilly Business Park, Caerphilly CF83 3GG.

HSE priced and free publications can be viewed online or ordered from www.hse.gov.uk or contact HSE Books, PO Box 1999, Sudbury, Suffolk CO10 2WA Tel: 01787 881165 Fax: 01787 313995. HSE priced publications are also available from bookshops.

British Standards can be obtained in PDF or hard copy formats from the BSI online shop: www.bsigroup.com/Shop or by contacting BSI Customer Services for hard copies only Tel: 020 8996 9001 e-mail: cservices@bsigroup.com.

The Stationery Office publications are available from The Stationery Office, PO Box 29, Norwich NR3 1GN Tel: 0870 600 5522 Fax: 0870 600 5533 e-mail: customer.services@tso.co.uk Website: www.tso.co.uk (They are also available from bookshops.) Statutory Instruments can be viewed free of charge at www.opsi.gov.uk.

Published by HSE 02/10