20079

HAZARDS OF REMOTE CONTROL IN MINING

PATRICK DONOHUE

JEAN CROSS

School of Safety Science

The University of New South Wales

Sydney 2052

CONTENTS

HAZARDS OF REMOTE CONTROL IN MINING

EXECUTIVE SUMMARY

Remote control has been introduced in mining operations primarily to enable the operator of mining equipment to be removed from dangerous areas. However over the years since its introduction there have been a number of incidents, some of which resulted in fatalities as a result of remote control. This report aims to identify the full range of issues which lead to fatality risks in remote control equipment before the lead to fatalities.

The primary sources of information for this study have been summaries of mining incidents, detailed studies of risks of automation in the aircraft industry and the academic literature on remote control. The State University of Oregon has carried out an in depth analysis of issues responsible for incidents in fly by wire aircraft funded by the FAA in the US. The issues they identify are generic and are as applicable to the mining industry as the aircraft industry. The structure of this Report looks at each issue identified in the US study in categories which relate to the different parts of the control system, human, electronic interface computer etc. The main focus of the US report was on human factors and automation issues. In addition to this ergonomic issues associated with the control interface were considered and risks associated with soft ware and hardware failure modes was obtained from the various handbooks on design of safety critical hardware and software.

Human Centred Issues

Fundamental limitations of human beings need to be considered when designing remote control systems and when assessing risks of remote control equipment and tasks. These limitations include

- A reduced understanding of the way the machine operates and is controlled as a result of the lack of knowledge about radio control systems and the computer software

- Incorrect or delayed decisions (particularly during unusual operating modes or unexpected behaviour) because of lack of feed back from the machine which results in greatly reduced information about the machine and its operation and condition. Lack of detailed understanding of the failure modes of the system as a whole but particularly those that may involve the computer software contribute to this problem.

- Inability of an operator to intervene and override a fault condition. (This may be either that the person is physically locked out of control by the software or hardware or that they have insufficient information on which to act with confidence)

- The poor capability of humans to maintain full concentration during a purely monitoring task where little action is needed

- Limited ability to visually monitor a large range of things simultaneously for extended periods

- Loss of situational and mode awareness for example due to lapsed concentration, cognitive overload or unexpected behaviour of the equipment. This can result in people inadvertently entering dangerous areas or initiating dangerous movements

- A possible desire of the operator to feel closer to the machine resulting in their desire to approach too close

- Over confidence that the machine will behave correctly

Most of these problems are associated with the removal of the operator from the direct control of the machine and from the feedback that the machine normally gives. The objective of automation is to remove the operator from the danger zone and also to increase production. Neither of these objectives require the operator to be removed completely from the actual control function. Consideration needs to be given to returning some control functions to the operator and providing greater involvement in control. In other words optimum operation may be obtained by not using the full capabilities of an automated system

The operator has at present too little information and feedback from the machine to make appropriate decisions under fault conditions. More real time information on system status and behaviour needs to be provided to the operator whether or not the operator is also given more direct control. There is a need to look at the potential for feedback and the different ways real time information can be given to operators. This would include considering from where in the control system and machine system signals should be taken to best inform the operator about machine status and behaviour and how this information should be given.

One of the advantages of software control is that it can be forced to follow standard procedures where people cannot. Consideration should be given to using this capability to enforce adequate pre-start checks prior to operation following maintenance.

Remote control has removed operators from one dangerous situation but provided the opportunity for them to enter another (the region close to the machine). There are both practical and psychological reasons why people may need to be in these regions. A study needs to be carried out to identify the occasions where people need to enter danger zones around the machine to perform their tasks and to identify safe alternative positions.

Educational requirements for automated operation are not well understood. For example the extent to which people need to have a degree of understanding of how the control systems work in order to recover from failure situations is not understood. This needs further study.

Ergonomic Issues

Control units used in remote control systems in mining are generally of very poor ergonomic design.

Control Units weighing several kilograms cause neck ache and create safety problems because they are uncomfortable and likely to be removed. Consideration should be given to a lighter switch unit with a convenient protective pocket attached by cable to heavier components carried on the belt.

They are too easy to operate inadvertently. Switches need to be more clearly identifiable by shape coding and by different heights of control. The orientation of the control unit should be clearly identifiable by touch. Recessed or guarded switches should be used in some situations. Toggle switches have inherent problems from design and controllability points of view. The use of levers or knobs for some functions should be considered particularly where analogue control or gradual start up would be advisable. Controls should be designed to minimise the likelihood of someone's finger slipping from the control

The control unit should be designed so the speed of operation of the machine is compatible with the speed of a person.

The number of different functions and different combinations of switches which must be operated may be excessive if errors are to be avoided.

Over the years a basically standard system for conventional controls has developed. With remote systems any switch configuration is theoretically possible and there is a very strong possibility of error as an operator reverts automatically to a previous configuration with which they were familiar. The industry should standardise on control unit configuration taking into account the ergonomic considerations above.

Automation Issues

With Automatic control there is the capacity for very high speed transfer of information from the operator to the actuator of the mechanical movement. This is translated into rapid mechanical movement with little prior warning or feedback to operators. Such high speed movements are not necessarily essential to production and add to the safety risks. Consideration needs to be given to providing a gradual start to motion so there is time for the operator to correct errors and to providing warning that movement is about to occur through some form of detection and feedback system

The use of a computer control system provides the opportunity for much greater use of error diagnostics than is currently used. The computer could be used to give real time information on machine status and control system command progress but and it could give diagnostic information following a fault. This feature of computer control is badly under utilised in mining control systems

Designers need to apply more thought to which functions are best carried out by an automated system and which by a human, At present the move to automation has been complete with humans now essentially acting as initiators and monitors. There is extensive literature on this subject which needs to be applied to the mining situation

There is a temptation to use the flexibility of a computer controlled system to introduce excessive complexity and more operational modes than are essential. Each mode of operation or functional capacity introduces new paths for potential errors and automated systems should be kept as simple as is compatible with production imperatives.

Automation Issues

Automation will bring offer new situations, new mining methods, new opportunities and new risks. Specific risk assessments will be required as these develop. Risk assessment will also be required for new manual tasks which intelink with automated tasks

For many reasons it is likely that operators will enter dangerous regions close to automated equipment. Reasons include difficulties in concentrating simultaneously on monitoring the equipment and on their own position with respect to it, a psychological need to be close to the equipment, loss of situational awareness and a need to be in danger zones to see what is happening or perform a task effectively. This is a key feature in injuries as a result of unplanned movements. It is essential that the individual procedures an operator and others must follow are assessed to identify when they may enter danger zones. Safe operating positions need to be explicitly defined for these occasions. For some tasks this may involve the operator being situated on the machine.

Electronic Hardware Issues

The design philosophy for radio remote control systems has to take into account the mining environment and culture. This means robust well protected design from both a mechanical and electrical view point.

A detailed assessment of risks needs to be carried out seeking failure modes and causes for unwanted failure effects. This should include consideration of the possibility of magnetic coupling from high current transients that may be generated during the control of some types of equipment. (either the remote controlled equipment or nearby machines)

Motion from stray electrical signals anywhere in the system can be prevented by a checking system whereby the software confirms with the control unit that the signal was indeed initiated before activating the actuators . This can be accomplished in fractions of a second and would not slow response. it does not catch any false signal from the control unit due to human error or switch failure

Testing of electronic equipment should include tests for mechanical robustness, response to stray signals as well as reliability testing of electronics.

The maintenance and regular testing required should be defined and documented.

Software Issues

The protocols and design and maintenance philosophy for software used in remote control systems in mining is very far from those required in safety critical systems in other industries. The extensive requirements reviewed above are only a subset of those required for Military and highly safety critical installations such as nuclear power yet may still seem impractical to implement in a formal way in mining as design requirements all of which will be verified. It is however necessary for the design philosophy of the software used in remote control to move towards safety critical design. This is a matter of expertise within the organisations that program the Units and a acceptance of safety critical design philosophy. There is a large difference in the programming philosophy used in standard programming applications and that used in safety critical systems and it is important that this is transferred into software in mines

Safety Critical software needs to be modular with links between modules minimal and clearly understood. New code to provide new functions should never be patched on to existing code without a full understanding of all the implications it has for interactions in the rest of the system. Self checking protocols should be introduced to pick up errors at safety critical positions. Particular attention needs to be paid to the potential for loops within the system and response to unwanted and multiple signals. Software also requires maintenance and checking and maintenance requirements need to be defined.

Although software faults have not been directly implemented in many incidents as yet, complexity is increasing with each new patch and each new version and the potential for such failures is increasing. It is also possible that the growing numbert of unplanned movements for which no cause can be found are software induced

The Industry has two options here. One is to rely on expertise in the software developers to move towards this philosophy. The other is to develop a check list for software design verification such as that published in the Software System Safety Handbook

Summary

Risk can be reduced by preventing unplanned movements, removing the person from the danger zone round the equipment or providing advanced warning of movement so that the person has time to move out of the way. Rasmussen (1987) suggests that errors in complex systems can be reduced but not be prevented.

For the reasons outlined in the report is not be practical to eliminate people from the danger zones simply by training. Physical means of separation need to be considered. This might involve providing a safe platform for operation of the machine, designing work systems so it is never necessary to enter unsafe regions to perform a task or installing barriers and stops so that when the machine hits the wall there is still space for a person. It is almost certainly feasible, but non trivial for the machine to detect the presence of a person in some way and not operate if they are too close. Each of these possibilities has its own practical problems but should be given serious consideration.

A further approach is to seek a means to control the error after it has entered the system. The control system could detect commands at the actuator and verify that they came from the control switches without introducing any additional delay. However this does not detect incorrect signals generated by switch fault or operator error. To check this it would be necessary for the system to seek confirmation from the operator dirtectly before proceding to action. This would introduce a delay while the operator considers the signal and responds to it. This may not slow production significantly but in any case could be considered for maintenance mode. Alternatively the control system could seek confirmation from the operator during the time it take motion to start.

HAZARDS OF REMOTE CONTROL IN MINING

1 INTRODUCTION.

Remote control equipment is being used in the modern mining environment at an ever increasing rate. It is used not just to eliminate the need for a human operator in difficult and dangerous situations but also to improve productivity. The various human and technical components that comprise the remote control systems of today have a distinct architecture which is completely different to the previously manually driven equipment. This introduces new risks. Remote control provides an evolutionary leap in design of mining systems which requires considerable attention on the part of management

The diagrams in figure 1a. and 1b. are generic system configurations showing conventional and remote control machine systems in the mining industry. The human, when 'on-board', starts and controls the equipment and remains in control of the operating machine. Therefore figure 1a. shows the conventional machine system as a serial linkage of control systems in the general order of operational control. The human chooses the particular sequence of motions desired and by controlling the electrical power to the devices initiates the relevant hydraulic system to start the mechanical motion

The second diagram, figure 1b., shows the essential characteristics of the equipment when a remote control system intervenes between the human and the standard electrohydromechanical system. This new form of system configuration is vastly different. After the human initiation it has an electronic based radio transmission and receiver system operating under strict protocol checks, governed by a computer software management system.

The human has moved both physically and cognitively, further away from the end goal of mechanical motions. This will change fundamentally the rate, nature and form of all the error sources, paths and effects. Whilst automation does remove the human from many of the dangers of the purely manual system it also distances them from the control of the system. This can have serious implications if the design of the system does not take cognisance of this fact.

For example the simple box representing the human represents their total ability to integrate into all the succeeding technology areas which he is supposed to control. Such a concept must regard the human not merely as the driver but as the manager of the entire system. From an engineering stand point this created a totally new control system. as the newly configured control system was essentially 'piggy-backed' onto the 'old' system designed for direct human control. This is one of the core issues of this report which will be elaborated on further..

Figure 1a. System configuration of equipment with on-board operator.

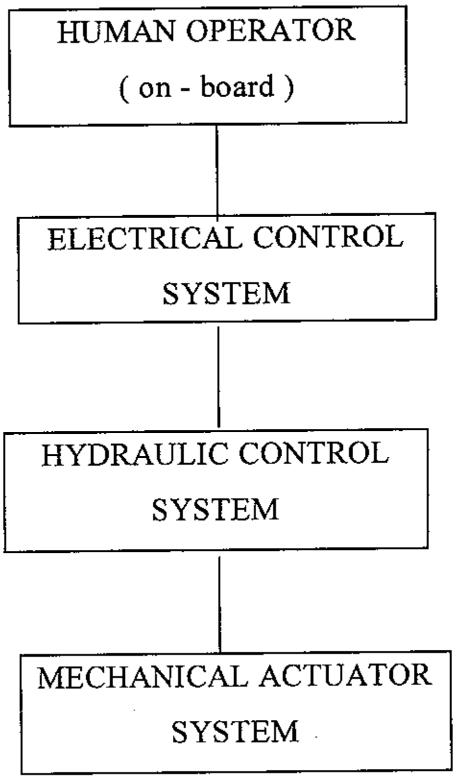
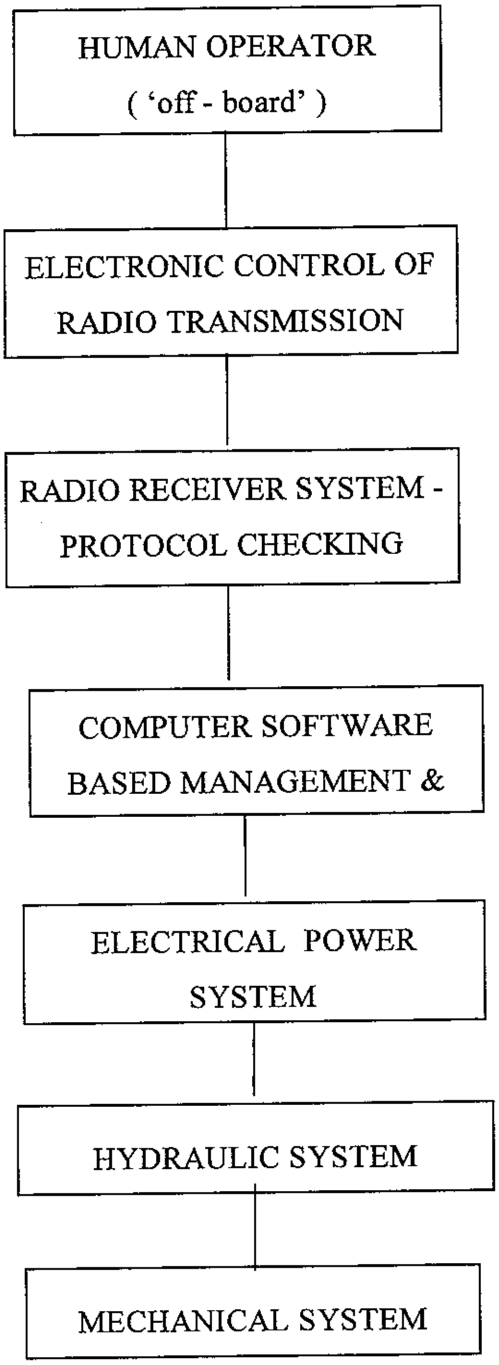


Figure 1b. System configuration for remote control equipment.



Remote control has substantially increased the number and complexity of control systems and interfaces. The following is a list of these new developments:

i. Between the operator and the remote control unit which he carries there is a new interface.

ii. The remote control unit has contains a new and substantial electronic control system.

iii. There is a new radio transmission and receiving system with its own protocols and operational characteristics.

iv. There is a substantial computer software system for the transfer and supervision of signals that is embedded in the overall system. This software, like most modern control systems is highly complex. This particular aspect of the system is especially new and difficult to analyse and control.

As the complexity of a system increases the number of potential error paths also increases. Although failure of any particular error path may be rare, there are many different potential error modes which could lead to disaster. This large pool of sources for errors is arguably one of the primary difficulties that remote control systems pose to both the designer and the end user.

With reference to the mining environment there are several aspects to automation that give rise to concern. On a practical level an article in CIM Bulletin, January 1996, points out that with automated systems new thought will need to be given to the mining process design, machine design, machine intelligence and intelligent mine production planning and control.

Specific questions that will require thought include:

i. How much disturbance can the rock mass be subjected to if machine security replaces human security as the prime concern?

ii. How selective can automated mining be?

iii. What types of ground control hazard do we need to protect machines against?

iv. How do we maintain, protect, recover, and repair machines?

v. Should working places be concentrated or dispersed? mined with large or small machine units, i.e., few or many machine units?

vi. Should extraction rates for individual stopes or benches be high or low? is continuity of excavation important?

As these issues are considered and decisions made, new procedures may be followed and new safety issues may also arise

1.1 Information Sources and report Structure

The aircraft industry has a long history of automation and "fly by wire" systems. Just as there have been unplanned movements during operation of remote control mining equipment there have also been similar incidents occurring in the area of flight operation. Naturally in the airline world this can and has had disastrous consequences. The Federal Aviation Authority (F.A.A.) in the United States has therefore funded an in-depth study and analysis taking evidence from both the experts and users of the complex aircraft automation systems, to identify what are believed to be the constituent culprits in the causes of accidents. The State University of Oregon has been the primary group responsible for the preparation of this study. (Funkk, Lyall and Suroteghal 1999) Theiresults are generic in nature, and are as applicable to the mining industry as the aircraft industry. An outcome of this study is a taxonomy of the causes of failures in automated systems. The full list of factors identified by these authors is outlined in Appendix 2. This study was in two phases. In phase 1 all issues that might create safety problems were identified. and in phase 2 the issues were ranked by a number of different methods. This list of automation issues identified in this work forms the basis of this report.

The report will consider each issue in the taxonomy from a mining perspective and make clear its link to the mining environment. Examples will be given of the situations, that operators of mining equipment can find themselves in as a result of each issue.

Although all the issues identified in the aircraft study are relevant to mining their relative importance may differ and the order followed in this report is the order of the the control system components. Under each heading evidence from other literature is also presented.

The issues discussed in the main body of the report begin by considering the critical human-centred aspects of the systems design which affect the ability of the human to fully and competently interact with the system. Ergonomic issues of the human control unit interface are then considered followed by operational issues. Issues associated with reliability of electronic and software systems are highly technical. Reliability and safety is assured by tight design specifications and by extensive risk assessment and testing. It is not possible to fully cover these issues in this report but a flavour of the type of problem that can arise and the methods which are used to ensure a high degree of reliability are described.

1.2 Preliminary Analysis of Issues from incident data

There have now been a significant number of remote control mining incidents in Australia and overseas. A list of these has been compiled by the Department of Mineral Resources and is presented in Appendix 1a In Appendix 1b these have been ordered by causal factor. ie the part of the control system where the error occurred. (Some incidents involved more than one identifiable failure

It can be seen that Ergonomic / human factors played a part in 15 incidents and Electronic systems failure in 16. While only 2 can be attributed to software failure there are also 8 incidents where no failure mode could be identified. Software failures are the hardest to diagnose and could have played a part in some of these.

In 9 incidents the person was standing in a dangerous position and there is no information on whether this was in fact necessary to perform the task. Four incidents involved accidental activation by the wrong radio transmitter. Three of these were early in remote control design, Four were hydraulic problems not detected by the operator prior to failure resulting in an unplanned movement. There is an increasing number of incidents where no cause can be determined.

2 HUMAN CENTRED ISSUES.

2.1 Operators are no longer a central part of the control system

From the schematic diagram, figure 1b, it is apparent that in a remote controlled system the operator is further from the output of the system than in a directly controlled machine. Several new systems elements have been introduced between the operator and any motion, (desired or otherwise) which complicate the overall control system. In essence the operator has become a more peripheral part of the equipment's control loop. This has a number of implications .

- The intervening systems can delay or reduce the person's interaction with the machine.

- The embedded software can freeze the human's ability to deal with any problems because the software is effectively the manager of the system giving the human no opportunity to intervene

- As a result of their more peripheral role operators are less often solely concentrating on the equipment's behaviour than previously. The opportunity for distraction is higher. Factors, which contribute to the potential for lack of full concentration on operating the machine include:

    i. the binary or digital nature of the hand controls on the remote control unit, (it is an accepted ergonomic principle that analogue control types are better at inducing full operator communication with the system.)

    ii. the new aspects outside the machine that warrant closer attention than with on board manual operation e.g., pinch points, etc.

    iii. the other personnel working nearby are more easily seen and hence have a higher capability for distraction,

iv. the new exposure to roof and the need to continuously monitor that aspect,

v. the need to monitor the front and back end actuators and their position vis-à-vis the overall productivity requirements.

2.2 Operators are psychologically more isolated from the machine

Not only is there a physical removal of the operator from the immediate environment of the machine and its work there is also removal from the hands-on control of the system. A valued characteristic for the operator of any system is his proximity to the actual control of the system in both a physical and psychological sense. (The latter is usually termed egogratification). By being removed from the machine the operator has lost this to a large degree. A possible reason for the operators to be drawn into those areas beside the machine which are potentially risky is that they are subconsciously trying to make up for the loss of closeness, control and feedback that the previous manual control of the system gave them. Hence the 'logic' of their being drawn into pinch points which ordinarily one would expect the operator to avoid. Zuboff, (1989) has referred to not just physical isolation resulting from automation, but also a mental separation . Since the operator has less in control of the machine in a psychological sense than before (ie it appears to work perfectly well on its own with little outside interference) the operator may feel less need to keep in close mental control of the system

A natural response by the operator to the lack of feeling of closeness and the limited need to do anything to control the machine is inactivity and a feeling that the task is easy. As early as 1980 Wiener & Curry, (1980) noted

"...One disturbing side of automation has appeared i.e. a tendency to breed inactivity or complacency."

With the machine now responding to a mere flick of a small number of switches there is very little, that an operator has to do. The task has been reduced to that of monitoring the process but essentially letting the machine get on with its workload. The operator can assume for the most part that the machine is essentially its own master. Keeping a few fingers on a number of toggle switches on the remote control unit is a considerable step down physically and psychologically for the operators.. It is implicit then that this introduction of automation has brought with it less need for the operator to be so fully involved in the various tasks that the equipment performs

2.3 Out of Loop performance problems

This refers to the situations where operators feel themselves to be peripheral to the control system and may therefore fail to take control when they (apparently) should

A particularly seminal report was printed in "Human Factors", 1995, entitled: "The Out-of-the-Loop Performance Problem and Level of Control in Automation." In it Mica R. Endsley, and co-author Esin O. Kiris, looked at the difficulties facing the operator in automated systems. Like most current work this paper tends to exonerate the operator even when he appears to be doing something strange and potentially dangerous since it is the system itself that is defining the actions and position of the operator. According to Endsley this type of operator error can be linked to two major issues associated with the implementation of automation:

i. The loss of manual skills

ii. The loss of awareness of the state and processes of the system.

Whilst loss of manual skills may not be a major issue yet in mining, since many operators remember and still use the manual operation modes, there may well be a need in the future to look at those personnel who have never had first hand experience of on-board manual operation of equipment.

At this time it is the area of situation awareness that needs the greatest attention

2.4 Mode and Situation Awareness.

Situation awareness (SA) is defined as: "the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future." (Endsley, 1988)

It is the term used to describe the perception of humans in automated man-machine systems of the space and time aspects of the system.

Mode awareness is the perception of the mode in which the machine itself is operating

Endsley discusses 3 levels of situation awareness .

Level 1 SA includes an operator's perception of relevant system state variables

Level 2 SA is an understanding of the meaning of that system state based on a synthesis of Level 1 data and in light of operator goals

Level 3 SA, is a projection of future trends and events in the system based on this understanding

A lack of situation awareness may be directly responsible for decrease in performance as well as for many incidents. Operators who have lost SA may be slower to detect problems and require extra time to reorient themselves to relevant system parameters in order to proceed with problem diagnosis and correction.

A spatial misperception of situation for example occurs when the operator concentrates exclusively on the machine and its task and has no perception of themselves in the scenario and hence places themselves in a dangerous position.. For example the equipment might swing and trap a miner against the rib, or he may get caught in a pinch point, or he may follow the machine out under exposed roof.

A failure in situational awareness where temporal aspects are misjudged is a possible explanation for the several fatalities which have occurred with LHD vehicles where the operator has apparently failed to stop the LHD in time and has crushed themselves against the wall. A remote control button is a positive action stop. It is possible that this is perceived at a subconcious level to be an instantaneous machine stop regardless of the fact that reason and experience dictates that a heavy vehicle requires substantial time to come to a halt.

Where machines have several capabilities (eg continuous miners with roof bolting capabilities) there can be situations where the operator in changing from remote to manual for testing and other similar situations could lose mode awareness.

2.4.1 Causes of loss of mode and situational awareness

Greater Potential for distraction

The operator is now outside the machine and free to observe other mining activities and the mine environment and to communicate with others while the machine is being operated This means that the balance of the signals the operator receives from the control system, the mining machinery, the environment and other people has changed and his attention may be divided. There is a risk that the operator may become momentarily unaware of the operation of the system. In effect a temporary loss of situation awareness.

Loss of mode and situational awareness has been identified as a frequent problem in laboratory studies when a person is operating an automation system while involved with other concurrent tasks. Distractions from the core task of control by the need to monitor general aspects of the mining environment can also result in loss of awareness of some part of the system..

Inability to remain alert

Studies which began in the 1970's focused on alertness of workers. Miller, 1973, implicated alertness as the single most important factor in human error accidents. As studies increased in number, disorientation of workers as it was also sometimes called, continued to receive attention with, for example, Riley & Cochran observed that :

"Often workers must focus their eyes and attention on the moving object for extended periods of time. ....as workers monitor such an activity, there is a decrement in perceptual and motor abilities during, or for a short time immediately following , the observed period.......a disoriented worker could leave a work position and encounter dangerous materials or situations."

Loss of vigilance in monitoring task

Loss of vigilance and increase in complacency while performing what is primarily a monitoring role can result in the operator losing track of what is happening. There is a long history of lack of operator awareness of automation failures and a decrease in the detection of critical system state changes when operating in an automated mode. Parasuraman (1987) reviewed vigilance problems associated with complex tasks and found that "vigilance effects can be found in complex monitoring and that humans may be poor passive monitors of the complexity of events being monitored."

Loss of feedback

The loss of feedback means that the operator is no longer receiving a constant reminder of machine state.

> *"Without appropriate feedback, people are indeed out of the loop: They may not know if their actions are being performed properly, or if problems are occurring." (Norman, 1989)*

It appears that system designers believe that operators no longer need information on system status as the relevant functions have been assumed by automation. However it is just those items which might be critical to the safety of the operator.

Multiple Goals

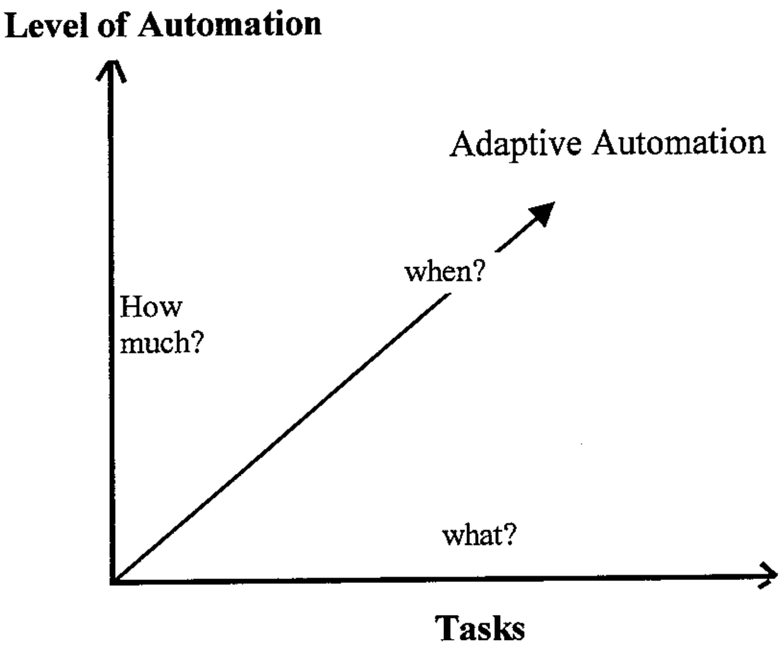
Martin and Jones (1984) pointed out that people who have trouble with distributed attention may be having trouble with multiple goals. An inability to keep multiple goals in mind could seriously degrade an operators receptivity to highly pertinent data related to the neglected goal, leading to significant errors. To take a mining example, an operator moving a continuous mining machine by remote control round a corner in a confined space needs to know where the front cutter heads are, where the back conveyor boom is, the turning moment required for the miner within the confined space, his own position and how it should change. He may also need to be aware of the position of others, e g., cable handler, and all the time must try to keep tabs on his position and orientation vis-à-vis the machine, the width of the heading for both ends of the CM, the speed of operation, the desire not to hit any part of the coal face/rib wall, and knowing that technically just one error could result in trouble.

2.4.2 Current work on situational awarenss

In his article "Situation Awareness: Proceed with Caution", Flach (1995) refers to the increasing concentration of the US human factors community on situation and temporal awareness. This area of study has only begun to be seriously looked at in the last 10 years and is still not well understood. Work is still in the initial stages of trying to discover how to design systems to overcome the problem. The data is primarily published in The Human Factors Society publications in the U.S.

Many of the problems with situation awareness have become evident when an operator is interacting with automated systems. The loss of manual effort has been replaced by a far heavier cognitive workload. The way in which automation is implemented at present needs to be carefully examined. Automation has typically decreased operator situation awareness through implementation strategies that remove the operator from involvement in system operation. An alternative approach to automation focuses on enhancing operator situation awareness by keeping the operator involved in the task. This can be accomplished by determining a level of automation that minimise negative impacts on operator situation awareness. At intermediate levels of automation the human may be far more involved in the operation of the system and able to deal more effectively with the automated system when needed.

As shown in the diagram below, taken from Endsley 1996, designers implementing automation must make decisions about which tasks are to be automated (traditionally labelled function allocation). In addition they have choices regarding how much to automate any given task (level of automation), and how that automation level may change over time (adaptive automation). Although traditionally automation has been implemented in anall or nothing fashion, both adaptive automation and level of automation may represent strategies for changing this, creating automated systems that allow the operator to be more involved in system functioning and therefore more able to interact as an effective part of the system..A means of allowing the operator to be in greater control of the equipment is required to avoid situational awareness problems



Design Considerations for Automation

2.5 Feedback issues

A remote control system provides considerably less feedback to the operator than a ride on system. A driver will be able to feel the response of the machine directly through his body and through the controls as well as seeing and hearing changes. A remote controlled machine provides only the feed back that can be seen and heard. (and visual feedback is reduced). Without adequate feedback from the system, the operator simply has not got the capability to fully understand the system he controls in real time. Norman, 1990, recognised the problem of feed back with systems at the present level of automation:

> '*.automation is at an intermediate level of intelligence, powerful enough to take over control that used to be done by people, but not powerful enough to handle all abnormalities. Moreover, its level of intelligence is insufficient to provide the continual, appropriate feedback that occurs naturally among human operators. This is the source of current difficulties.....it is possible to reduce error through appropriate design considerations. Appropriate design should* ***assume*** *the existence of error, it should continually* **provide** *feedback, it should continually interact with operators in an effective* manner, *and it should allow*

> *for the worst situations possible. What is needed is a soft, compliant technology, not a rigid, formal one.'*

Norman quotes a study by Zuboff (1989) who describes the control room of a modern paper mill: where once the operators roamed the floor, smelling, hearing and feeling the processes, now they are poised above the floor, isolated in a sound-isolated, air-conditioned, glass control room. The paper-mill operators do not get the same information about the state of the mill from their meters and displays as they did before from their physical presence. Though not the same as being in a coal mine clearly the principle is that loss of information sources and feedback from equipment results in a greater potential for error or delayed response to failures. Lack of feedback has a range of effects

(i) **Lack of true understanding of what the machine is doing**

If an operator presses a control switch on a remote control unit without any feedback of intent the operator has no guarantee that the actuator will only do what was intended. Since he has no pressure dials/gauges, no noise history, no vibrational record, no tactile input, he has not got the prior warning or trend information that the system would have to him when on-board and has to piece together more restricted information to understand exactly what the machine is doing,

(ii) **Reduced understanding of the mode in which the machine is operating**

The operator has no prior knowledge of the mode that the machine is in should it operate erroneously. Neither can he usually determine the cause of the behaviour of the machine after the event. Evidence for this is provided by Dept. of Mineral Resources reports into various incidents. There is usually little that can be determined in the radio control and especially the software system components when they are investigated after an incident has occurred.

(iii) **Reduced warning of being in a dangerous situation**

In many accidents, operators carrying out their required work are finding themselves in a position where they are exposed to a danger. There is no feedback or other prior warning to the operators of the danger of the situation, nor is there a system for the machine to be aware of the operator's location. In these situations the operator cannot assume full control of the system .

(iv). reduced time to respond to abnormal conditions,

There is also reduced information about abnormal operation when the machine is being operated remotely than when it is being directly driven. Forewarning of failure most often reaches a driver through his immediate senses often primarily tactile with sound as a secondary warning. With remote control sound warnings are reduced and tactile warnings removed altogether

(v). a reduced understanding of how the machine is controlled.

Equipment is made to be remote control by the addition of two primary technical systems namely, the radio control transmission and receiving system and by the embedded software control management system. Both of these systems are new to the operators not just physically but even more importantly from a knowledge standpoint. Operators are not likely to know much about software, radio transmission and receiving technology and microprocessors, etc. If the machine fails to do what is expected the operator has little or no knowledge understanding of these key aspects of the control system. Unlike mechanical items which make noise, vibrate and maybe even smell, etc., these new systems are effectively the silent partners with little or no direct external exhibition of effect. The operators cannot know or interrogate these systems like they could with the hydraulic/electrical systems. Their knowledge and understanding has not kept up and probably cannot keep up with the new system configuration they now work with.

2.5.1 Visual feedback may be too abstract.

The primary feedback from the remote control machine is visual -seeing the motion. Other feedback may still occur (such as noise), but mostly the only information the operator receives is visual. Even visual information may not be good depending on where the operator is located with respect to the machine.

The digital switches are on/off in nature. When the operator had direct analogue-control, response time was part of the information he could rely on as an additional means of feedback. Now the operator must try to mestimate rate of movement from a distance and recognise any deviation in the equipment's day to day operation. In essence the on board operator has a better feel for his machine. Visual information is too abstract to be effective as a means to make timely, informed decisions or corrective actions.

In many cases, certain critical cues may be eliminated with automation and replaced by other cues that do not result in the same level of performance. Young (1969) reported that hand movement information was important for detecting changes in system dynamics associated with a tracking task and that this was denied in an automated situation. Furthermore, De Keyser (reported in Moray 1986) cited the heavy use that process control operators make use of vibration and smell.

" The removal of operators from physical contact with the process may impoverish their diagnostic environment.... " (Moray, 1986)

2.5.2 Lack of data on development of conventional failure modes

Lack of feedback from the machine to the operator applies not only to faults that arise in the new control systems, but also to conventional failure modes. For example on 1st May, 1992. An operator was pinned against a drive wall by a failure caused by scoring on the steering spool in the pilot hydraulic circuit. This is an example of a fault that would probably have been spotted by an on board driver. Here the incident resulted in injury due to the position of the human operator outside the machine and the lack of feedback by the new automated system.

2.6 Monitoring requirements may be excessive.

The only core task that the operator has to accomplish continuously is to monitor the equipment as it goes about its work. There is general agreement amongst psychologists that monitoring a process or system for long periods of time is a task for which humans are perceptually and cognitively ill-suited.

A series of studies have shown that in tasks where people must provide sustained attention as monitors over a period of time it is difficult to maintain full attention and considerable fatigue is induced. Perceived workload is rated as fairly high (e.g., (Galinsky, Rosa, Warm, Dember, 1993 Becker , Warm, Dember, 1991; Dittmar, Warm, Dember and Ricks 1993; Scerbo, Greenwald, and Sawin, 1993), This is contrary to characterisations of monitoring activities as boring but non-demanding.

The operator of remote control equipment must not only continuously monitor the machines' performance but also monitor the surrounding environment (such as other equipment, people and roof structures). The monitoring requirements have increased considerably and the effort required to actually operate the machine has decreased.

Operators of remote control systems can be observed to be operating the machines via the control units by means of tactile sense and at the same time visually engaging in other tasks quite separate from the production operation. The range of tasks that the operator of a continuous miner for example could be engaged on simultaneously include:.

- Controlling the cutting heads
- Controlling the linear and/or rotational movements of the machine.
- Aligning the conveyor booms orientation with the shuttle car being loaded.
- Checking the roof condition above and around his location.
- Checking the cutting area generally around the cutting heads.
- Checking the cable handler and cable location.

Such a monitoring task load on the operator is not conducive to full attention being able to be given to the core tasks. This is an indication of conflicting goals in the system that will further tend to reduce the operator's full control of the system.

Molloy and Parasuraman (1996) quote Mosier et al. (1994) who examined NASA's Aviation Safety Reporting System (ASRS) database and found that 77% of the incidents in which over-reliance on automation was suspected involved a probable vigilance failure. The vast majority of incidents occurred during cruise, when the pilot's primary role was to monitor and supervise the automation. This suggests that even teleoperated remote control when personnel are completely removed from the danger zone may not be an ideal form of control . The monitoring requires the operator to sit in front of a console and for the entire duration of a shift look at the console organising the equipment's path and tasks on a second to second basis. Little work has come to light on this aspect of machine control in the mining environment

2.7 Operators may be overconfident in automation

This issue was placed third highest in importance of the aircraft accident study overall and the highest of the human centred issues. The fact that the role of the operator has become that of a supervisor rather than a driver creates a tendency for the operator to rely on the machine to make its own decision. The operator may ignore information which they would normally have considered if they had more direct control. Over confidence in the machine continuing to do what it is supposed to (which it does for most of the time) can also result in failure to notice the first signs of incorrect behaviour. Poor understanding of the control system may also make the operator inclined to ignore the situation and let it continue rather than stopping production. In these situations operators must be able to completely override the system regardless of external production or other constraints.

The opposite problem ie lack of trust in the automated equipment also occurs.

2.8 Operators may lack confidence in the automated equipment.

As off-board supervisors of the system operators can easily believe themselves to be less in control of the equipment should it act in an unexpected way. Any time the machine acts unexpectedly is an extra opportunity for the operator to further lose his sense of control over the equipment, especially if there is little he can do to get the machine to act in accordance with his instructions. Since the complexity of the machine inherently means the operator does not understand all the various components in the control system, he knows he is in control of a piece of equipment that need not obey him!

2.9 Operators may be reluctant or unable to assume control

Operators may be reluctant or unable to assume control from automation as a result of a lack of full understanding of the way the control system operates. Hence when automation malfunctions this may lead to unsafe conditions. One of the accidents that occurred in the United States involved a continuous miner trapping a miner against the rib. The uninjured operator, not understanding how the switch he had just operated could have caused this, became naturally perplexed. He worked out that to set the machine in a motion away from his colleague would require him, as he perceived the circumstances, to press the same switch that caused his colleague to be crushed in the first instance. This did not seem to him a very sensible thing to do so he ended up entirely unsure which switch to operate. fearing that either way he would further injure his colleague. Effectively he ended up being unable to act.

When the system fails, apart from the overall lack of feedback that the system generates, there may well be critical decisions to be taken. For example if, upon failure, an operator finds the remote control unit useless then the only option available may be to go over to the machine and operate it manually which of course, under particular failure circumstances may itself be highly dangerous.

2.10Automation may adversely affect operator workload.

Physically automation generally reduces workload but on the mental awareness/ vigilance side workload may increase. Endsley of Texas Tech. University., USA. In his paper 'Level of Automation: Integrating Humans and Automated Systems' argues that the reductions in workload that are assumed to accompany automation have not necessarily been realised. He quotes Hart and Sheridan (1984) who concluded that automation often replaces workload involving physical activity with workload involving cognitive and perceptual activity. In the aircraft industry pilots are to an extent trained for this, but in the mining environment it may not be so.

Work load may also be more variable. Weiner (1989) states

> *"...workload seemed to be reduced when it was not heavy or critical, [yet] may be increased by automation when it was already heavy or critical."*
> *(Wiener, 1989.)*

The fact that some tasks have become easier as a result of remote control and some more difficult may result in boredom and hence lapses of concentration during some tasks while other tasks now require excessive concentration, cognitive overload or require the operator to take a dangerous position in order to perform the task well

Studies indicate that this situation tends to lead to errors occurring. In studying adaptive automation techniques Harris, et. Al., (1994) found that when operators were required to initiate automation in response to an unanticipated increase in workload, it was accompanied by a significant increase in performance error in other tasks. This confirmed work by Parasuraman, et. al. (1992) who showed that operator initiation of automation was likely to increase demands when they were already high

2.11 New tasks and errors may exist.

> *"Technology change creates potential for new kinds of error and system breakdown as well as changing the potential for previous kinds of trouble." (Woods et al., 1994.)*

One of the more common aspects of automation, mentioned by Woods in connection with aircraft automation is that automation may change and/or add to operator tasks, making new and often more serious errors possible.

2.12Task overload in critical situations – automation may demand attention

There are several documented cases in the aircraft industry where the need to make sudden or critical changes to a remote control system has resulted in loss because the pilot fails to appreciate some external aspect of the situation.

On 20th Dec. '95 an American Airlines Boeing 757, on a flight from Miami, Florida, to Cali, Columbia, crashed while in a descent for landing. The pilots, having been offered a more direct route to land from the air traffic control, took up the 'offer' and in the short time available proceeded to change their course and make the necessary changes to the automated flight management system. What they forgot to realise was that at the time of the change they were already in a descent mode so the changes were not all appropriate. They did not notice anything wrong until they found their 'ground proximity warning system' signalled their imminent collision with terrain by which time it was too late. One key conclusion was found to be the pilot's over-concentration on the immediate needs of changing the control system to the detriment of consideration of where they were in time and space.

In 1989, a USAir Boeing 737-200 on an approach to Kansas City (NTSB, 1990) struck electrical transmission wires just 50 feet above the ground. Six minutes prior to landing the crew were offered and accepted the opportunity to execute a different runway. In attempting to prepare for the new approach the crew failed to notice, until it was almost too late, that they had descended prematurely. After striking the wires only their immediate recognition of and response to the wire strike prevented a catastrophic accident.

In January, 1992, an Airbus A-320, operated by the French airline, Air Inter, crashed while in descent for a landing at Strasbourg, in eastern France. After a change commanded by air traffic control to accommodate another aircraft, the crew, having to reorganise their landing, failed to notice that they inadvertently pre-selected the wrong descent mode, did not realise that the aircraft had begun a high speed descent!, and so the aircraft struck a hill 10 miles from the runway with total loss.

In all these accidents highly trained and experienced pilots operating automated flight management systems, as opposed to manual control, were incorrectly controlling the planes actual progress due to their lack of appreciation of the existing situation (what the plane was doing or where they were). In each case their normal tasks of control involved them to such a degree that, being so engrossed, they forgot to take notice of some very 'basic' and even visual aspects of the situation. Automation demanding attention when other critical tasks needed to be performed was the highest ranked caused of incidents in the aircraft industry. While this aspect may be less critical in mining because the operator has fewer other critical tasks to perform than does a pilot there is still the possibility that the need to make changes to the preset control commands or control modes could distract the operator from noticing other safety critical information. The operator can become too engrossed in the control changes to notice critical situational information.

As with aircraft, mining equipment has several modes of operation For example with a continuous mining machine there is

Manual Control Mode

&

(Production Operation (testing or tramming) or Maintenance Operation).

OR

Automated Control Mode

&

(Production Operation (cutting or tramming) or Maintenance Operation).

The need to make changes between modes or between different functions in operational mode could distract operators from other critical safety or situational problems

2.13Job satisfaction.

The type of tasks that the operator of a remote control system now undertakes is generally less complicated than it was previously. The inherent skills and abilities that they would have been able to display are evidently considerably reduced.

Automation reduces the challenges that are the source of job satisfaction, and hence may adversely affect operator performance. (Billings 1991) The airline industry found this to be of concern to pilots, operating the new generation of aircraft.

2.14Visual requirements.

Though the remote operator has a greater overall view of the entire system operation than before he is nevertheless further away from the cutting heads as they travel out under unsupported roof. Apart from the temptation to follow, albeit subconsciously, the freedom to move may bring him into more overtly dangerous circumstances than when he was confined to the cab. The operator may enter dangerous areas in order to see what the machine is doing. This tendency may be increased because the lighting in underground collieries is relatively weak due to the reflections that the coal produces. (Note is taken of this area being already researched through the JCB under a separate investigation.)

The 'scan pattern' that the operator follows with a remote control machine is very different to that of the previously manual system. The tasks to be performed require a greater diversity of attention and hence visual foci for the operator. The way this may affect attention levels and concentration is not well understood

2.15 Envelope limitations

For some mining equipment, for example continuous miners, the equipment is nearly as wide as the heading cut into the coal face. There is little room left for the operator beside the machine. Previously there was little need to worry about this aspect since the operator or other mine personnel seldom needed to be adjacent to the side of the machine whilst a colleague was operating the machine. People need to get very close to the machine in extremely narrow openings, both to see where the equipment is going and how it is cutting and for maintenance purposes. The inevitable requirement for operators to be in these restricted spaces will cause injuries or fatalities in the event of an unplanned movement.

This mismatch between the operator, the machine, and the restricted space which they share is a risk that needs to be considered in detail. For both practical and the psychological reasons discussed above, defining a rule that people may not enter the danger regions around the machine will not work.

For some equipment, displays and controls which the operator may need to access are situated on the side of the machine itself. While there may be rules which require that manual controls on the machine are not approached while the equipment is in any way under remote control It seems likely that this will not be adhered to in practice and indeed may well be impractical. On some machines the computer display is also situated on the machine. If this display is to give any useful information about the condition of the equipment during operation it clearly will need to be approached.

Observation of operation of a remote control continuous miner revealed many occasions when people (including ourselves as observers) were in a position of danger between the machine and the wall. It appeared that many of these occasions could not be avoided although the time spent in such areas could be reduced. There are situations where the operator or others do need to approach close to the machine in order to perform their tasks. The cable handler in a continuous miner will frequently need to be near the equipment, people who want to inspect the heading or the roof will need to walk past the equipment and the operator needs to see the way the machine is cutting without placing themselves sufficiently far forward to be under unsupported roof. In metaliferous mining the LHD operator moves between remote operation for loading and then on board operation to drive the LHD to the dump position. He must approach the machine to board it.

Regulations which rely on people learning particular danger zones around the machine to avoid are unsatisfactory because if there is sometimes a need to be in the danger zones people will not perceive them as no go areas. A rule that appears impractical will not be obeyed.

The need for people to be close to a remote control machine with no means of escape is a fundamental problem of the current design of remote operation

For each task and machine those occasions when people do enter danger zones should be identified. The extent to which being in that position is essential or makes the task easier or improves performance should be assessed

Consideration needs to be given not only to where the operator and others should not be but where they should be in order to perform each task effectively and easily. For some tasks the most appropriate position may in fact be on the machine itself.

There may be a need to deliberately limit the chance of sideways movement when the machine is working one heading. Indeed the fixed nature of the heading resulting from such a system of operation could assist better mining. While inhibiting instantaneous sideways movement during cutting should partially limit the potential for pinch points to injure humans, there remains a situation of narrow 'aisles' close to moving parts in which the operator would appear to have to position himself in for proper operation of the equipment.

2.16Over familiarity

The operators of remote control equipment may come to ignore some of the dangers associated with this kind of equipment due to familiarity with it. This applies equally to non remote control systems

2.17Operator may be under pressure to break rules

There may be conflicts between the goal of production and the goal of safe operation. This raises the issue of how much authority the operator has, (or perceives himself to have) when equipment is being operated to a production schedule. The core task for the operator is to operate the machine for production purposes. Can an operator take decisions which may slow production if by not taking them, he may be putting himself and others at risk?

In other words production requirements of the system can act as an override on the operators good judgement. With remote control machinery pre start checks and checks following maintenance are more complex and more critical than with conventional equipment ... A typical situation that could arise is only perfunctory.testing when a machine is restarted after a fault has been fixed during production. (This issue also arises with conventional machinery but control failure modes tend to be less frequent and are more likely to be failure to start than uncontrolled motion)

On start up there have been instances of several mechanical system elements acting simultaneously. For example on the 27th of August, 1995 at Cordeaux Colliery when power was restored to a continuous miner all operational equipment onboard proceeded to operate as if selected to do so. The operator had to quickly reach into the cab to shut down the system.(Thus intrinsically placing himself in a dangerous position with an out of control machine)

One solution is to put the machine through a full unavoidable pre-start software controlled test with the operator checking to ensure that all the motions are correct?

This would force adequate prestart checks and avoid inappropriate decisionsbeing made by the operator on the choice of the appropriate automation level for the checks.

2.18 'Workarounds' may be necessary.

Operators may have to use the automated system in a manner that was not intended by the designers so as to get desired results or to avoid undesirable consequences. For example, apart from the 'normal' use a continuous miner could be used for scraping the roof to loosen already cracked roof.

In automated and computerised systems there is a common problem that the picture the operator has of the ways in which the controls operate is not the same as the way the designer actually designed the system. This leads to errors when the system is being used in a way or for a purpose that the designer did not foresee. It is important to test the machine and seek failure modes in all the tasks and modes of operation that the machine will have to perform.

2.19.Training Issues

In essence some of their loss of direct driving skills are being replaced with those more akin to managerial/ supervisory roles. This implies that a different sort of training is required which takes into account the cognitive rather than manual skills which are now required.

On the other hand, the advent of operators who have never been on a machine when it was purely manually controlled, may lessen their full appreciation of the machines capabilities. Different forms of training are required for operators who are familiar with on bord operation and those who are not.

2.19.1Variations in control design

The remote control equipment produced by different manufacturers will differ from each other. In addition changes occur as the machine improves over the life of the particular equipment type. The flexibility of a software control system means that there are many different ways controls can be configured to bring about particular actions and it is possible to make significant changes in the function of controls very easily. Since changing the software is relatively easy compared with redesigning a conventional control system, changes to equipment function during its operating life may be more frequent than changes to a conventional machine. The changes can be subtle and not easily grasped or far reaching with major changes in operational function for minimal change in the actual operation of the controls

This has implications for training and there is an increased need for both a new risk assessment and refresher training whenever changes are made to the way the controls operate. . Any change in design, especially in the physical layout of controls, will need retraining of the operator including simulation of what the operator may do in an error situation to assess whether a stereotype has been built up in their preferred use of the machine and the controls.

The need for specific training applies not only to changes of controls but also where a machine has an additional function. For example where a machine of identical type to that of another in the same colliery may have roof bolting capabilities on-board. The change from one to another would be sufficient to warrant close attention from this perspective of standardisation and operator expectancy of operational characteristics.

Training and risk assessment will not solve all the problems brought about by this increased flexibility in the control system. Operating machinery, like driving a car becomes an automatic skill, "programed" into the operator. Training does not necessarily completely reprogram the operator and there is a very high risk of error where the control unit of different machines operate differently or when software upgrades change the way the control unit functions.

There is a strong argument for similarity to be maintained throughout the industry. As equipment types increase there will also be a need to assess how close completely different machines can be manufactured to be reasonably similar in the nature of their controls.

2.19.2Training needs

There are two means of operation of equipment, manual and automatic, together with two types of operator, miners and maintenance crews. The training that each of these groups receive must be assessed closely and frequently. Aspects to be considered include

(i) the frequent changes that are at present made on an ongoing basis to the control systems of operating machinery as discussed above

(ii) Lack of understanding of the precise modes of operation of the equipment, particularly the software control. This is a potential cause of accidents both because of incorrect operation and because operators will not be able to work out how to correct a developing hazardous situation .

(iii) The changed mode of operation will have flow on effects to the way in which mining is carried out. (For example place change mining). It needs to be recognised that specific risk assessment and training will be required as these new methods are tried

2.19.3Skills required for automated vs manual operation

With the loss of on-board feedback the psychomotor and cognitive skills required to operate equipment are very different. This has already been addressed in relation to the loss of specific feedback factors. The essential skills base is different with the role of the operator now being reduced to that of monitor. The psychological impact and effects of this on the operator is little studied. The further aspect of the operator being placed in varying orientations to the equipment on a very frequent basis is also addressed further in this report.

There are few if any experts on the particular training issues that need to be addressed when using human and automation systems together especially in close proximity to one another. The key skill requirements to maintain situational awarenss are still not understood and may be cognitively impossible.

2.19.4 Understanding automation.

It is necessary to define the level of understanding of automation which is needed for correct operation of the system and performance of operators duties. In most cases the individual operators knowledge does not cover the entire machine system. Pilots when tested have been found not to understand adequately what the plane will do when particular controls are operated in particular circumstances. This occurs particularly when moving between auto and manual modes. In mining inadeauate understanding of the automatic controls might cause problems either when changing modes or in unusual conditions such as start up following fault conditions.

When the system fails there have been incidences of operators falling into an abyss of non-action due to the particular motions that the system exhibited. This may be an aspect of situational awareness that the operator is unable to work out what the machine is doing or may be due to lack of knowledge and understanding of the control system

There is a strong likelihood that the developments in the mining environment will continue and the complexity of the system will increase accordingly. This should be accompanied by a concomitant increase in understanding by the operators of the systems technology.

From the accidents that have occurred two categories of failure are common. One is where there is a different motion to what was thought to be enabled and the other is where the system does not respond to a switch and remains in an on-state and hence the operator is effectively locked out of the decision/control process. These aspects will be looked at further when the nature of the hardware and software is assessed. However it is clearly the case that the operator to have any hope of dealing with such situations must be given sufficient understanding of the way the control system works to deal with them.

The degree of knowledge required to provide the ability to intervene correctly if a fault occurs and confidence to do so should be defined

2.20Summary Recommendations - Human Centred Issues

There are a range of related problems associated with the removal of the operator from the direct control of the machine and from the feedback that the machine normally gives. These include situational awareness problems, difficulty of error diagnosis and inability to take effective control in a fault situation, over confidence in the machine to behave correctly, difficulties in performing a monitoring task adequately. All of these problems follow from removing the operator too far from the control system The objective of automation is to remove the operator from the danger zone and also to increase production. Neither of these objectives require the operator to be removed from the actual control function. Consideration needs to be given to returning some control functions to the operator and providing greater involvement in control and more information on system status and behaviour. .

Fundamental limitations of human beings need to be considered when designing remote control systems and when assessing risks of remote control equipment and tasks. These include

- the reduced understanding of the way the machine operates and is controlled as a result of the lack of knowledge about radio control systems and the computer software
- lack of ability of an operator to intervene when the rest of the control system is in control. (This may be both that the person is physically locked out or that they have insufficient information on which to act with confidence)
- Inherent human limitations of maintaining concentration during a purely monitoring task where little action is needed
- limited ability to visually monitor a large range of things simultaneously for extended periods
- Loss of situational and mode awareness for example due to lapsed concentration, cognitive overload or unexpected behaviour of the equipment

○ the lack of feed back from the machine which results in greatly reduced information about the machine and it operation and condition. This may result in incorrect or delayed decisions during abnormal operating conditions

○ A possible desire of the operator to feel closer to the machine resulting in their desire to approach too close

○ Potential (and inevitable) confusion in the operators mind about exactly how to recover the situation if the machine does something unexpected. This follows from the lack of detailed understanding of the failure modes of the system as a whole but particularly those that may involve the computer software.

Several of the above issues arise because of lack of adequate feedback to the operator As stated previously radio and software systems are so instantaneous in operation that there is perhaps little opportunity to obtain real time feedback,. There is a strong need to look at the potential for feedback and to consider where precisely in the control system the system is a signals should be taken to best inform the operator about machine status and behaviour.

Over the years a basically standard system for conventional controls has developed. With remote systems any switch configuration is theoretically possible and there is a very strong possibility of error as an operator reverts automatically to a previous configuration with which they were familiar. The industry should standardise on control unit configuration taking into account the ergonomic considerations discussed in the next section.

One of the advantages of software control is that it can be forced to follow standard procedures where people cannot. Consideration should be given to using this capability to enforce adequate pre-start checks prior to operation following maintenance.

Remote control has removed operators from one dangerous situation but provided the opportunity for them to enter another (the region close to the machine). There are both practical and psychological reasons why people may need to be in these regions. A study needs to be carried out to identify the occasions where people need to enter danger zones around the machine to perform their tasks and to identify safe alternative positions.

Educational requirements for automated operation are not well understood. For example the extent to which people need to have a degree of understanding of how the control systems work in order to recover from failure situations is not understood. This needs further study.

3 ERGONOMIC ISSUES.

The human/machine control interface for a remote control system is very different from the on board interface. The changes have a profound impact on the ability of the human to control the system. The primary form of control is through the use of a hand-held remote control unit. The following issues are concerned with the ergonomic aspects of remote control units.

A major study of ergonomic design of remote control systems has been carried out in Finland in the remote control crane industry. (Pesonen, and Lahtinen 1987), This focused on the design and operation of the radio control systems. The same general issues were raised as have been identified in the mining industry that is

- ○ outside interference from other radio sources,
- ○ false operation due to a defect in the radio system electronics (similar to problems with for example loose nuts/washers running along a circuit causing a short to occur),
- ○ loss of control due to blind spots,
- ○ operation from an unsafe distance.

However as stated above, much of the effort of the study was directed at the ergonomic properties of the units . The diagram in Appendix 3 include the three foci around which the systems were assessed.

Manageability	Controllability	Safety
Carrying Equipment Size Weight Storage Battery capacity and charging	Symbols Compatibility size of controls placement of controls sensitivity of controls possibility of control errors	safety devices standards placement and design of emergency stop devices

Included in the report were various examples of hazards they found were associated with the use of remote units including:

- tripping,
- hit by adjacent objects,
- control errors,
- operator too close to the equipment,

amongst the list of disadvantages the following were particularly referred to:

- increased risk of slipping (note this is distinct from tripping)
- unskilled users,
- increased number of operators,
- difficult handling of the portable device,
- signal disturbances.

On the basis of much of the above the safety inspectors noted certain deficiencies and suggested improvements. Some of these are especially pertinent for unplanned movements in the mining industry.

i. The core risks are insufficient space, crossings, and obstacles.

ii. Identification codes must be clear and unambiguous and logical.

iii. The speed of the crane must correspond with that of the operator.

iv. The operator has to see the load at all times.

v. Surfaces must be orderly and in good condition.

vi. The use of the radio control system must be so organised that untrained or unauthorised personnel cannot use the system.

vii. There must be regular maintenance and inspection of control units.

The third point. is perhaps of crucial importance and is not the case at present as unplanned movements, when they occur, tend to be very fast much faster than the operator can respond. It is not clear that this is essential for productivity as most machines do not operate 100% of the time. A more gradual start to motion could make a large difference to safety with no effect on production.

With regard to the ergonomic properties several features were important for flexible and safe use. Specifically the report referred to the following issues

- the impossibility of operator error in using the controls

○ ease of change of battery

○ size and weight due to carriage requirements throughout the day

○ the switches should be easily distinguishable

3.1 Weight.

The standard weight is of the order of 3kg. This weight is carried by the operator for the duration of the shift and is often designed to be suspended from the neck. In fact, due to the weight and other the requirements of the tasks, the unit is frequently placed on the ground, on the machine itself, or given to a colleague to hold. This tends to increase the inadvertent misuse of the unit. The unit may fall from the equipment through a 1.5 - 1.8 metres resulting in an impact load to an equivalent mass of 10 + kg. Alternatively, it may be operated by a cable, or a fragment of falling debris, or it may be dropped into water. There are records of all of these things occurring. The list of scenarios that could potentially have an adverse impact on the unit are manifold.

To reduce discomfort some operators hang the control unit over their shoulders and operate the switches with the unit on the hip. This is not the design intention of the switches and may increase the likelihood of error in switch operation

From a biomechanical perspective the concept of using a thin strap on the neck for suspension of a weight is poor practice. There are alternatives which would be more effective for use, would reduce fatigue and which would be a strong factor in influencing the number of times the unit gets placed elsewhere other than on the individual who is using it.

One solution would be to attach the unit (or at least the heavy parts of the unit) to the belt as with other weighty units the miner must carry such as the battery for the cap lamp.A

3.2 Inadvertent operation

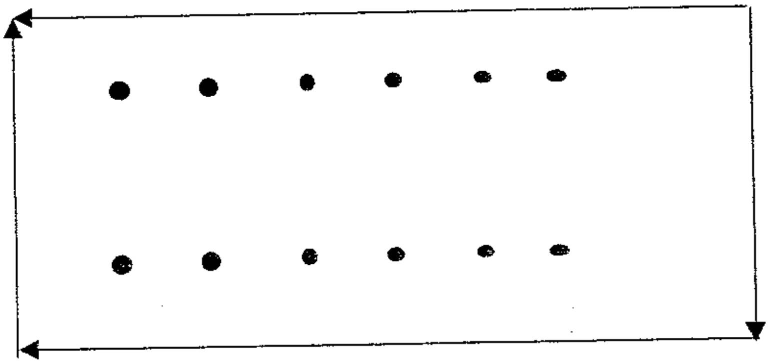
To reduce the possibility of inadvertent operation of the unit through falls etc. the top cover and switches which can be light weight could be designed as a separate unit from the battery/transmission section, linked by a cable. The battery could be carried on the belt and the controls could be designed to fit into a suitable attachment carried on the chest of the operator for storage when not in use. The switches would then be fully enclosed so they could not be operated accidentally. Fatigue would be lessened and the operator could conveniently carry the unit while engaged in other tasks.

If the control section remained with the operator at all times it would also decrease the chance of units being mistakenly exchanged with another unit e.g. in the crib room. (Again this has been the cause of incidents in the past). The cable that would link the two parts could act be easily and simply disengaged from the battery to guarentee that there was no accidental use of the controls.

A system for easily stowing the control section while not in use would make it less likely that an operator would accidentally lean on a switch while undertaking other tasks. An operator was fatally injured while adjusting pick heads on a continuous miner. It is believed that he may have inadvertently pressed the unit against the cutter heads while leaning over to reach the picks.

3.3 .Interface design.

The ergonomic design of the remote control unit's interface with the operator is essentially a symmetrical rectangular box with rows of switches on one face. Through this interface the operator must undertake all the tasks that the machine must carry out. All the motions of the complex machine system must be done via this simple instrument. No matter what developments the system undergoes the unit will be controlled in basically the same way but the number of switches on the interface and the combinations in which they are operated will have to accommodate these changes in operational characteristics.



Typical schematic of top surface of remote control unit.

3.4 Ergonomic design of switches

The switches themselves are very small and are either metallic finish or covered by small plastic sleeves. They operate in an on/off fashion with one primary up/down or left/right sequence depending on whether the operator is holding the unit in front or at their side. The small size of the switches are in conflict with several ergonomic rules:

- ○ They should be easily operated without causing fatigue to the operator (Continuous finger operation of a control is not a recommended practice due to the susceptibility of cramp and fatigue.)
- ○ Controls should be designed to minimise error in operation

In many remote control units used in mining the control switches are very small and close together making incorrect selection of a switch likely. Even with plastic sleeves placed on top of them there is a real likelihood that a finger could slip from a switch because of the wet and dusty nature of the mine. Even allowing for the limitation of using specific toggle switch types that may be on the there is ample scope to manipulate the design of these switches by adding on to them to make them more distinguishable from each and to include ribbed features to prevent finger slip.

Switches on control units are all at the same height which makes them more easily operated simultaneously in any number of combinations. However the means by which they are operated by the human can be more easily mimicked, by a foreign object, than if they were at different heights. Switches should have different push resistance as well as different heights to minimise inadvertant operation. (Alternatively switches could have different base reference points so achieving different effective heights with the same switches.)

Many of the remote control units require the operator to keep the switches pressed for the duration of the motion desired. This is designed toguaranteeing fail-safe operation should the unit, for example, fall out of the operators hands and control. However using fingers to keep the motion continuing is tiring and likely to lead to error. It is ergonomically unsound to use buttons or switches for this purpose.

3.4.1 Switch types

Toggle switches are prone to several problems and alternatives need to be considered. Switches, like any other controls, can be used in a number of ways. For example they can be used in sequentially. Ie the controls are used by the operator one at a time in some form of logical sequence governed by the process itself. The use of remote control equipment in mining requires the operator to follow a variety of tasks either simultaneously or in a sequence that need not necessarily be in a fixed order. Consequently sequential use of controls is not very useful in this application.

The other main means of the operation of controls is simultaneous. Here two or more of the controls are used at once to achieve a particular aim at any given time. An advantage with this technique is that by allowing several controls to be used at once there is ample scope for future adaptation of the controls to accommodate future additions. Any required modification can be arranged from the existing number of controls by using new combinations. This method pf control operation is used by most of the remote control units on the market.

Chapanis, 1972, carried out a study on the use of various types of controls including pedals, buttons, toggle switches levers cranks and knobs. An outcome of the study was that only cranks/levers and knobs should be used simultaneously. Push buttons, toggle switches or pedals should be so used.Levers or cranks or knobs can also be analogue forms of control which has some advantages

3.4.2 Inadvertent operation.

As there are no means of determining, particularly after a serious accident, which control switch an operator or other source pressed care must be given to eliminating any and all possible means of inadvertent operation.

i. Strap.

A strap can easily become entangled resulting in the control unit being dragged along the ground if it is removed from the person.. Not only therefore are there sound biomechanic based reasons for eliminating the strap there are good safety reasons as well. During April, 1992, in Ontario following an accident in which an operator was pushed over a stope the recommendations included a look at the use of the harness portable transmitter and suggested they be ‘discouraged’.

ii. Guard rail.

There are some units that have a guard rail surrounding the switches as a means of partially eliminating inadvertent operation,. Although this design may lessen the erroneous operation of a switch they introduce the possibility of inadvertent operation due to something catching in the guardrail or accidental operation when using the guardrail as a carry handle

iv. Configuration

The units rely on a form of rows of switches. There is little to distinguish the units orientation. The unit looks and feels basically the same from either direction. Operators rarely look at the unit when they pick it up, relying instead on tactile information from their hand to tell them where they have their hand on it. If the latter is to be relied on then a means of making the unit asymmetric is desirable to reinforce the tactile orientation. This asymmetry can be equally applied not just to the overall shape of the unit but also to the rows of controls so that they too are asymmetric in form. This will lessen the likelihood of incorrect operation because the unit is being held the wrong way round or the fingers are placed over the wrong switches.

iii. Recessing.

A common means of eliminating some of the possible causes of inadvertent operation is to recess the controls to some level that is below the general switches level. This would have the extra advantage of giving the operator more tactile feedback of where his finger/hand is located on the unit.

(iv) Identification

Due to the illumination of the mining environment there could be improvements to the means of identifying the control functions by some form of coding. Usually this can be achieved by greater illumination, use of LED’s, colour coding or if appropriate shape coding of the control designs and layout characteristics.

The sheer number of switches that are in use on the top of the unit is indicative of the range of functions that it is carrying out. Even allowing for the desirability of change from toggle to lever or some other more suitable type of control there is still a need to look at the number of operations that the controls are expected to carry out especially simultaneously.

3.5 Summary of Ergonomic issues

Control units used in remote control systems in mining are generally of very poor ergonomic design.

Control Units weighing several kilograms which are hung round the neck are unsound from a biomechanical viewpoint and introduce safety problems because they are uncomfortable and likely to be removed. Consideration should be given to a lighter switch unit with a convenient protective pocket attached by cable to the power source carried on the belt.

Switches need to be more clearly identifiable by shape coding and by different heights of control. The orientation of the control unit should be clearly identifiable by touch.

Toggle switches have inherent problems from design and controlability points of view. The use of levers or knobs for some functions should be considered particularly where analogue control or gradual start up would be advisable.

Controls should be designed to minimise the likelihood of someone's finger slipping from the control

The control unit should be designed so the speed of operation of the machine is compatible with the speed of a person.

The number of different functions and different combinations of switches which must be operated may be excessive if errors are to be avoided.

The control system needs to provide more feedback to operators

4 AUTOMATION CENTRED ISSUES.

There are a large variety of safety issues that are applicable to automation generally and to the mining industry in particular. It has already been discussed that the configuration of the new systems 'piggy-backed' onto the 'old' system are creating a new type of interface between the operator and the machine system. The operator is reduced primarily to a monitor and the intervening systems, electronic, radio control and computer software are now taking over the management of the control. of the machine to a much greater extent. The replacement of a person by electronic and computer communication and decision making has several new implications. ..These are outlined below.

4.1 Information integration.

From the schematic diagram, Figure 1b it can be seen that the new systems are, acting as a conduit for the commands from the operator to the machine, The path that the information follows is no longer clear and defined. This means it is not easy for the operator to assess how the information is flowing when either an unplanned movement or a valid task takes place. Many of the issues that follow are either directly or indirectly related to the difficulties associated with the level and quality of the information flow. However, the more complex system also provides the opportunity for much more detailed tracking of the way in which the system is operating. Greater use of this could be made in the analysis of incidents. This is particularly true for the software control system. If the data flowing in and between the systems shown in figure 1b could be recorded on an on-going basis it could be interrogated after an incident to give an understanding of the errors leading to unplanned movements as they progress through the system.

The addition of new systems and interfaces adds greatly to the complexity of the control system. Figure 1b. shows that there are two new interfaces and one substantially different one.. The new systems are the transfer of data from the radio receiver to the computer and the transfer of computer commands to the electrical power system. The substantially different system is the interface between the person and the machine and the environment in which it operates. Not only is the operator interacting with a remote control unit in his hands, a purely ergonomic interface, but he also has the issue of interacting with the entire environment from an 'off-board' position .

4.2 Speed and detection of movement

The speed of data flow (or errors) through the systems as they process operator commands creates a design which is geared towards immediate operation of actuators. From the movement of a switch to the command reaching the hydraulic or electrical actuator takes only a few milliseconds. A complex system with immediate response achieves what is termed a tightly coupled system..

Transfer of a command to a heavy machine through hydraulic and mechanical controls is inherently slower than issuing a command by electronic means. In addition, as discussed earlier, the traditional on board controls provide much better feedback to the operator about the machines behaviour than remote control units. This means the automated systems move very rapidly and any initial slow movement of parts of the equipment is undetected because of the loss of the feedback. There is therefore less opportunity for an operator to correct an error in control.

Since the remote control operator is no longer protected by being on board the machine, the fact that the machine has a faster response and intended movement is more difficult to detect adds a significant risk. It is therefore necessary to look closely at the protection afforded to the operator and those in the vicinity of the machine to see if it could be improved.Issues of Control

4.2.1 Communication between automated systems may be unsupervised.

A considerable degree of radio signal checking is carried out on a frequent basis by the computer software system to ensure that the system is not affected by extraneous signals. The software is designed for this and when operating normally will undertake this function according to the software designers intent. However many of the software systems used in the control of mining equipment are already well into their double figure 'nth' revision resulting in increasing complexity. This tends to result in an increasing number of possible paths for information flow through the software and an increasing potential for the information to follow an unplanned path. The multiplicity of paths opens up the possibility that the person will be cut out of a control path where they should have the ability to intervene.

In an article entitled 'Automation Surprises'(Billings 1994) Billings gives the following synopsis on his views on the area of automation:

> *'In a variety of domains, the development and introduction of automated systems has been successful in terms of improving the precision and economy of operations. At the same time, however, a considerable number of unanticipated problems and failures have been observed. These new and sometimes serious problems are related for the most part to breakdowns in the interaction between human operators and automated systems. It is sometimes difficult for the human operator to track the activities of their automated partners. As a result, the operator is surprised by the behavior of the automation and asks questions like, 'what is it doing now,' 'why is it doing that,' or 'what is it going to do next.' Thus, automation has created surprises for practitioners who are confronted with unpredictable and difficult-to-understand system behavior in the context of ongoing operations. The introduction of new automation has also produced surprises for system designers/purchasers who experience unexpected consequences because their automated systems fail to work as 'team players.'*

Incidents can occur because once the operator has authorised commands, the system is in full control. All the operator can do is act as initiator should the system malfunction. There are several cases of equipment of all types not responding to valid operator commands. This lock-out effect prevents the operator from undertaking any action that could override the system. When this has occurred the software is thought to be inside a loop and will simply keep reiterating through it indefinitely. There are few means devised to overcome this problem except by designing the software to be 'safety-critical' and specified to very demanding rules and protocols at the design phase.

This potential source of error about which we know little at present could be analysed in real time with the result communicated to the operator if full use were to be made of the softwares' self-analysis capability.

4.2.2 Disengagement may be impossible.

Just as the system may lockout the operator from the control loop equally it may prevent him from entering the system. This could have consequences for the operator if he decides to attempt to override the system by using the manual controls. He will be uncertain of the consequences of his actions since the equipment could bypass his commands in unforeseen ways..

A typical illustration of this problem is the situation where, due a short term electrical power glitch, the operator is unable to get the remote control unit to work and so will go over to the machine to operate it manually. He may then check to see whether it is something on-board the machine that is at fault, or just check the fault details on the screen on the side of the equipment (if provided) In either case he has placed himself in a position of danger due to his proximity to a machine with an unknown fault.

4.2.3 Mode transitions may be uncommanded.

Automation may change modes without an operator command, potentially causing surprising behaviour. This is particularly likely to be a problem in maintenance mode when the operator needs to be inside the machine with the machine in 'off'-mode. Unfortunately this has happened on a number of occasions causing fatal injuries. (For example an electrician helper fatally injured in Daniel's Branch Coal Co. Inc. No.1. Mine West Virginia, 18th April, 1995; Maintenance trainee fatally injured, White Oak Mine No.2. Utah, March 1995.)

4.3 Diagnostics in Automated Systems

> *"We are long overdue in developing systems that can forecast trouble rather than merely waiting for it to occur." (Wiener, 1993.)*

The meta analysis of flight deck automation issues identified a range of problems associated with diagnostics of abnormal operating conditions and fault conditions.

This could be greatly improved by using the capabilities of the software control system to record commands of the operator and various parts of the control system and to feed them back to the operator. A system which informs the operator continuously about the status of the equipment can be envisaged but at the very least there should be a record kept for post analysis of incidents.

With automated systems there is ample opportunity to detect error development prior to its actual through some form of mechanical motion. It is generally only this mechanical motion that is responsible for injuries. The path that the error must travel can be detected in real time by the software or alternatively, the error can be detected at the power source that the error triggers . Specific problems related to diagnostics which have been identified are listed below.

4.3.1 .Failure assessment may be difficult.

In the mining industry it is difficult to detect, diagnose and evaluate automation failures (errors and malfunctions) because of the complexity of the control system and the difficulty of back-tracking to determine where and what precisely went wrong . As pointed out by Wiener (1993)

> *one difficulty lies in the lack of awareness on the part of the operators that an abnormal condition exists especially if the system is compensating for it. After an incident the operator may be totally unaware of how it occurred"*

4.3.2 Failure recovery may be difficult.

There is very little in the way of feedback from either the control system itself or from the machinery to help diagnosis and solution in the event of unexpected behaviour.. When automation fails, operators may have difficulty taking over monitoring, decision making and control tasks because they cannot work out how the error occurred or what mnethod should be used to correct it. For example at Elourea Colliery on the 11th of September, 1996 a continuous miner machine started up and both the cutter and conveyor motors started when the operator pressed the relevant switch for just one function. If the system had recorded what signals it had received and what decisions and commands the software had passed on some degree of diagnosis of the cause of the failure and how to stop the unplanned motion would have been possible.

1.3.3 Error and status information may be inaccessible.

Information on errors, or system status needs to be accessible to the operator while he is operating the machine . The use of a screen on the side of the machine as in continuous miners is only of limited benefit to the operator, particularly in the coal mine environment where dust can clog up such sites for visual inspection. It is clearly not ideal that the operator should be drawn towards a dangerous piece of equipment which has just failed in order to see the screen. Ergonomic and safety considerations suggest an alternative location for the screen if not a complete redesign of the feedback device.

Thought should be given to the form and amount of information which should be made available to the operator. In parallel with this much can be gained by ensuring information is recorded so that unplanned movements and other types of malfunctions can be investigated by tracking the actions of operator, control system and machine. Brazier and Skilling (1996) in a report entitled "Human Factors Data form Near Miss Reports" suggest that much valuable information is being lost by not undertaking a thorough analysis of near misses.

1.3.4 Trend information may be lacking.

It is rare to find the normal variance and information on wear and tear in machine elements being traced and fed back to the initiator or operator of the equipment. For example poor evidence of deterioration in hydraulic circuit performance, demonstrated perhaps by vibration or slow response to start up, is not provided by automated systems. Should a situation develop where the operator has to react to a hydraulic failure they must make instant decisions without any history and very limited information. Since the operator is likely to have had little training in the specific occurrence facing him, he is not really in much of a position to do anything. There is usually also no information from, say, a previous shift to determine what could occur over the following hours of the next shift.

Where the failure is in the software itself the problem is even greater. In Software, unlike in mechanical elements, a fault does not normally develop gradually but may be instantaneous with few if any warning signs.

Just as procedures such as condition monitoring of equipment can be used to optimise mechanical maintenance programs software can be designed to monitor or at least self-test its operational characteristics as it goes about executing commands. This could be used to look for any early signs of abnormality

It would be quite feasible for the software to record its normal operation of code and to record the values of such variables as flags, interrupts and other sequence values throughout its use per day, per week. This would give some opportunity to ascertain the likelihood of error formation and any consequences that may result. In this regard the software is itself condition monitored for variation from some predefined norm.

4.4 .Design Issues .

4.4.1 Failure modes may be unanticipated by designers

Software designers design the control system to meet a specification for a working machine. They may not be fully conversant with the possible failure modes of the machine and hence their software may perform unexpectedly when the hardware of the machinery is in a fault mode. (For example reduced hydraulic pressure, or faults in the electrical supply).

This may be due to the inadequacy of design specifications. The automation may well do what it is designed to do yet the design specifications may not take into account certain unlikely but very possible conditions, leading to fault modes or to a need for an operator to take an unsafe position or act in an unsafe.

Risk assessment of automated equipment should explicitly consider how the control system will function with these types of general engineering failure of the equipment and the actions that the operator will need to perform.

4.4.2 Designers may not understanding the expectations of the operator

The design of remote control may take insufficient account of the operational knowledge of the operator and the operators expectations. When designing automation it is easy to unknowingly apply different control strategies than the human operator might rely on. This can contribute to loss of situational awareness and other errors.

4.4.3 Automation may be too complex.

There is a temptation to use the flexibility of software and switch control system to make the system over complex. This makes it difficult for the human operator to visualise the different operational modes and also increased complexity increases the number of potential error modes. Automated systems should be kept as simple as is practical for effective operation.

> *"..as system complexity increases, and depending on the feedback mechanism available, predicting the system's behaviour in context may be much more difficult." (Sarter and* Woods, 1994)

> *"..The use of computers leads to interactively complex and tightly coupled systems, often where these features were not originally present and not necessary for the operation of the systems. They therefore contribute to 'system accidents'." (Mellor, 1994.)*

4.4.4 Complex automation may have an overly simplistic interface.

The simplicity of the operator automation interface may hide important complexities, possibly leading to unexpected behaviours and difficulty performing complex operations.

> *"Such systems appear on the surface to be simple because they lack large numbers of physical display devices and controls: however underneath the placid surface of the workstation there may be a variety of characteristics which produce cognitive burdens and operational complexities," (Woods, 1994)*

4.4.5 Modes may proliferate.

> *"Modes proliferate as designers provide multiple levels of automation and various optional methods for many individual functions." (Sarter and Woods, 1994).*

In order to perform a large number of different actions in several different modes (eg maintenance, manual and automatic mode) with a limited number a switches, it is necessary to operate the switches in different combinations to produce each different function. The result is numerous mode switch combinations distributed over the remote control interface. As the complexity of the combinations of switches increases, due to the increased number of permutations used for operation there is a growing risk that the operator may inadvertently choose the wrong combination in a given situation.

4.4.6 Automation may be unexpected and unexplained.

Automation may perform in ways that are unexpected and unexplained by operators creating confusion, increasing operator workload to compensate, and sometimes leading to unsafe conditions. If one looks at the range of potential system reactions to commands initiated by the operator one can see the potential for the apparent incoherent reactions._The permutations available for the machine in response to a command is evidenced by the list below. Such a variety can make it very difficult for the operator to backtrack on his commands from memory if he enters a faulty sequence of commands. In a time of emergency this could be liable to make the operator compound the error.

Potential error modes for valid switch movements by operator include:

i. Switches moved, nothing happens.
ii. Switches moved, actuator goes in undesired direction.
iii. Switches moved, actuator goes slowly.
iv. Switches moved, undesired actuator moves, desired actuator remains stationary.
v. Switches moved, all actuators move simultaneously.

Comparing accidents that occurred prior to automation to those that have occurred after it would appear that there are now more varied ways for the system to operate in unusual ways when errors occur.

4.4.7 Automation may lack reasonable functionality.

Automation design may prevent the equipment from performing a function that seems reasonable to the operator. When the equipment was primarily manually controlled the driver could operate the equipment according to his preference. Now much of this control has been lost by the more explicit nature of the control system. The operator now has to follow the internal operational characteristics that the automation design has set. He can't drive it slow or fast. He has to stick to the systems design speed. Everything has become more black and white, more discrete. Many of the actions of remote controlled equipment occur at a single speed or at one of a range of discrete speeds where previously the operator had gradual, analogue control. It may be that if some of these motions could occur more slowly in the remote control situation and operator would have more warning that the machine was in fault mode which would have considerable implications for safety but without any impact on productivity.

Unplanned operation might be decreased by limiting through design the number and speed of start-up motions possible. For example must the continuous miner be capable of turning so fast? making this motion slower would not significantly affect production. It is not clear how the design speeds of various movements has been defined and whether safety has been adequately considered.

4.5 . Function allocation may be difficult.

Automation designers may have difficulty in making good decisions about allocating functions to humans or to automation, possibly leading to poor function allocation decisions.

> *" There's a pretty extensive literature devoted to function allocation, and designers do have problems with it. The biggest problem is simply not doing it; just automating everything possible."* *(Riley, 1995)*

4.6 Summary of Automation Centred Issues

With Automatic control there is the capacity for very high speed transfer of information from the operator to the actuator of the mechanical movement. This is translated into rapid mechanical movement with little prior warning or feedback to operators. Such high speed movements are not necessarily essential to production and add to the safety risks. Consideration needs to be given to providing a gradual start to motion so there is time for the operator to correct errors and to providing warning that movement is about to occur through some form of detection and feedback system

The use of a computer control system provides the opportunity for much greater use of error diagnostics than is currently used. At best the computer can be used to give real time information on machine status and control system command progress. At worst it can give diagnostic information following a fault. this feature of computer control is badly under utilised in mining control systems

Designers need to apply more thought to which functions are best carried out by an automated system and which by a human, At present the move to automation has been complete with humans now essentially acting as initiators and monitors. There is extensive literature on this subject which needs to be applied to the mining situation

There is a temptation to use the flexibility of a computer controlled system to introduce excessive complexity and more operational modes than are essential. Each mode of operation or functional capacity introduces new paths for potential errors and automated systems should be kept as simple as is compatible with production imperatives.

5 OPERATIONAL AND RELATED ISSUES.

5.1 Flow on effects as a result of changed operational modes.

The introduction of remote control will have flow on effects allowing new methods of mining.. Expanding the use to which equipment will be put to will require extra policies and procedures to be put in place. It is necessary to check the applicability of a machine's design to a new task and consider how well the original design can deal with a development of its role. While the machine may be able to cope with a new role, changed operation may place a greater burden on the operator. The following example illustrates this situation

Place change mining will require the operator to move more frequently with the continuous miner from operational coal face to operational coal face. Being off-board the operator will be walking alongside a machine in a position where he can see where he and the machine are going. With the equipment in a non production mode the operator may well become complacent believing that he is on the equivalent of a break. This is true to the extent that he is not using the machine for its primary role which is for cutting purposes. However the changes in the environment as the machine is being moved may in fact require an increase in attention.

On the other hand the operator may become engrossed in some movement of the machine which requires his full attention to the detriment of realising where he is There is therefore an increased risk of a trip or fall or other incident relating to the mine environment.

The increased movements of the continuous miner during place change mining also increases traffic control risks.

On the introduction of highly automated aircraft pilots found a greater increase in risks when the plane was on the ground than in the air because of the proximity of other objects while they were manoeuvring a plane on the ground.

5.2 The degree to which procedures assume automation.

Non automated tasks may not be integrated into operational procedures-

> *"the operator can be left with an arbitrary collection of tasks and little thought may have been given to providing support for them."*
> *(Bainbridge, 1987.)*

An example of tasks which may not be properly integrated is provided by maintenance. The maintenance crew may be required to make some repairs at the location of production and to work beside a machine that is broken down. The use of automation in these circumstances is avoidable and should be so, especially when the technician has to get inside the equipment to undertake the repairs. This type of incident occurred on 18th of April, 1995 at the Daniel's Branch Coal Co. Inc. No. 1. Mine in West Virginia. The electrical helper was carried by the conveyor whilst inside the chain enclosure checking an hydraulic relief valve. Complete electrical shut down had not occurred. Often the operator and the maintenance crew remain close to the machine for testing, both so they can more easily see whether the fault has been fixed, and to get the machine back into production more quickly. Maintenance by its very nature is more prone to error creation as the machine is not in its normal operational mode to start with. Design of a remote control system for correct operation with the range of breakdowns that might occur is so difficult as to suggest that automatic or even semi automatic operation should not be used at all during maintenance. Automatic operation should only be re-engaged for prestart tests after the fault is fixed. The alternative is design, risk assessment and testing of the automation system for specific maintenance tasks where there are no unknown fault modes present.

5.3 Safe work procedures and control zones.

Whilst the remote controlled equipment is operational the operator may have difficulty also concentrating on ensuring their locational safety both from normal mining hazards and from the risks posed by the equipment itself. Coupled with these risks are the situations discussed earlier where operators need to be close to the machine to do the job required effectively. One way of reducing these risks is to institute policies concerning control zones where the operator must remain regardless of position and orientation of machine. These may be instituted on a mine to mine basis in keeping with the present practice of requiring the mine to ensure the safety of its own employees. Thus there could easily be differences between mines with no coherent rules throughout the industry. The guide for use of remote control equipment published by NSW Dept of Mineral Resources shows maps of unsafe zones round individual items of remote control equipment, providing a degree of industry standardisation however there are occasions that may need the operator to enter potentially unsafe situations (eg for visibility or other purposes).. Whilst removal of the operator from on board has brought some advantages and safety improvements it is worth considering whether it might be safer if the operator was onboard again for some tasks. Consideration would also need to be given to the ideal location of an on board operator for these particular tasks as the conventional cab may not be the best position. A simple retrofitted foot stand which would leave the operator untouched by any movement of parts of the machine could be considered.

The construction of elevated operator platforms was one of the recommendations made following an incident in April, 1992, in Ontario where an operator in a metaliferous mine was pushed over the edge of a stope by an LHD. (The transmitter belonging to another machine at a draw point below took over control of the LHD above) On board or off board operator platforms in a safe position would also have prevented this and other incidents

5.4 Risk assessment of sample tasks

It is important to consider the procedures that an operator must follow and to identify the risks to which this might expose him. This will highlight tasks where, if an unplanned movement should occur, it would cause extreme danger to the health and safety of the employees.

While each machine and task would need to be assessed for a particular mine the example of the continuous miner below illustrates some of the issues

Regardless of the system configuration and the use to which the system is put, there are times when the operator and others need to be adjacent to the remote control machine. It may not be practical or even improve safety for a mode change to be made when ever this occurs. In production mode the operator may for example:

i. have to get close to machine whilst it is turning through 90 degrees at cross junctions. The sheer length of some machines (eg continuous miners at about 11.5 metres) means that to avoid hitting the rib walls and possibly the coalface the operator has to see quite clearly exactly where the conveyor boom and cutting heads are, (often simultaneously). Consequently it is highly probable that the miner may need to be near the unsupported roof boundary or to walk from one end of the machine to the other He cannot see round corners and yet he must stay within safe zones. Such conflicting requirements are very difficult to combine simultaneously.

ii. whilst tramming forwards the cable handler has to ensure that the lengths of electric cable and water supply are sufficient for the likely movement of the miner as it progresses through the face. There is just enough room for the cables to trail linearly behind the continuous miner with room left for the shuttlecar, but the bulk of the cables, both for their own safety and that of the operator, are stored on the ground at the side of the continuous miner. This therefore means that the operator and the handler have several coils of cable constantly at their feet. This is not only a trip hazard but also means that the cable handler will most certainly be alongside the continuous miner often when it is operating.

iii. if the amount of coal dust suddenly becomes excessive then the water jets emanating from the front of the continuous miner can be greatly enhanced by the application of a larger single water jet from the top of the miner typically on the side the operators work at. This facility will very quickly reduce the amount of dust and improve visibly. Yet inevitably the miner is likely to be in operational mode whilst this task of setting up the jet takes place.

iv. Inspection and change of the picks requires a person to approach the cutting head of the machine. This task figures significantly in incidents of error motions and therefore needs particular consideration

v. Should an electrical fault cause a power failure the operator will wish to check the data window, (if its still on of course,) or, he will do so when the power resumes. This will require the operator to get very close to the machine.

vi. During maintenance a person may not only have to approach close to a machine but actually get inside it. it is during maintenance that many of the horrific accidents have occurred. The incident already referred to at the Daniel's Branch Coal Co. Inc. No.1. Mine West Virginia is a typical example of one such fatal incident where the electrician positioned inside the conveyor chain was crushed after a short caused it to operate. They are any number of possibilities for a maintenance person to get inside the continuous miner. If all isolating procedures are fully followed then there should be no reason for such incidents however there is a temptation to leave some power present to facilitate testing so the person does not have to continually get on and off the machine while trying to fix a fault. Design needs to ensure that power cannot be present while the person is in the machine. Maintenance of the internal components of the electrical, hydraulic and mechanical systems is necessary at varying stages in the life of the equipment and there are many occasions when a person needs close access to the moving parts.

vii. Maintenance normally requires the person to be close to the machine. Some of the machines still have the manual controls at the side of the machine with little room between the machine and the rib. The location and orientation of the machine when it breaks down are beyond the control of personnel since it may have broken down at any point in its use at the face. Maintenance which has to occur during operation may require people to take an unsafe position

The above examples clearly show that the nature of the environment coupled with the dimensions of the equipment does not lend itself to risk free operation should an unplanned movement occur.

5.5 Summary and Recommendations for Operational Issues

There will be flow on effects as new mining methods are developed as a result of increased automation. This will result in new situations new opportunities and new risks. Specific risk assessments will be required as these develop.

Risk assessment will also be required for manual tasks which intelink with automated tasks

For many reasons it is likely that operators will enter dangerous regions close to automated equipment. Reasons include difficulties in concentrating simultaneously on monitoring the equipment and on their own position with respect to it, a psychological need to be close to the equipment, loss of situational awareness, a need to be in danger zones to see what is happening or perform a task effectively. This is a key feature in injuries as a result of unplanned movements. It is essential that individual procedures an operator and others must follow are assessed to identify when they may enter danger zones. Safe operating positions need to be explicitly defined.for these occasions. For some tasks this may involve the operator being situated on the machine.

6 HARDWARE QUALITY CONTROL ISSUES

In a survey of remote control incidents carried out by the Department of Mineral Resources 16 incidents had electronic failure as a significant cause. Types of failure included loss of power, component failure, dirt or water ingress, incorrect wiring after maintenance and a defective switch. A precise diagnosis of the failure mode is not given in several cases. These issues do not arise in the literature from the aircraft industry, probably because of the much higher levels of quality control on electronics in that industry. It is possible that some of the unplanned movements wher no cause could be identified were due to faulty recognition of signals at some stage in the system

There are three aspects to control of this problem

(i) specifications and design philosophy which fully understands the conditions in which the equipment must operate the use to which it will be put and the culture of the mining industry

(ii) robust design with components well within design capability and strong mechanical construction

(iii) fail safe design where fault conditions are identified and design ensures that for all fault conditions the equipment fails to safety

(iv) quality control in building, maintenance and testing

(v) effective testing perhaps including reliability stress screening

(vi) Risk assessment to identify fault modes and effects and to consider potential sources of error. Failure modes and effects analysis and HAZOP are formal processes which can be applied to do this.

(vii) Extensive verification of behaviour identified in the risk assessment

Methods of design for Reliability and Maintainability are covered in Australian and IEC Standards. Techniques have been developed for electronic circuitry that has to undergo extremes of condition such as vibration and shock, and high humidities.

Some of these techniques need to be used in control units as identified in the risk assessment and specifications.

6.1 Faults leading to Unplanned Movements

False signals which might lead to unplanned movements can in theory enter the control system via the control and transmitter electronics, through the receiver and its associated electronics or directly at the computer controller. Extensive protocols have been developed to ensure that the receiver will not act upon stray radio signals from other control units or remote control equipment, from communication equipment or from general background radio frequency signals The most likely way for false signals to enter the system is therefore direct magnetic coupling into the electronics or computer hardware. Digital electronics can be switched from one state to the other (and hence recognise a command) by induced currents which flow as a result of magnetic coupling from high current transients. Mining is an environment where very high current transients may exist. Likely culprits for the source of high current transients are switching of electrically operated machines or machine components and electrical relays which drive hydraulic components. The problem is solved by appropriate positioning and shielding. This fault mode needs to be recognised in the risk assessment design needs to take account of the need for shielding and tests carried out on the units both prior to installation and in situe.

6.2 Risk Assessment of electronic systems

6.2.1 Failure Modes Effects and Criticality Analysis (FMECA)

Failure modes, effects and criticality analysis is a formal method of considering each component considers each component or subsection of the hardware and asking the following questions

- How can it fail
- What would be the effect
- How critical are the effects (ie what would be the consequences and how likely are they)

- How would one know the failure mode existed before a hazardous situatiin was produced

For example a switch could have the following failure modes

permanently short circuit

permanently open circuit

intermittent contact

depending on the intended function of the switch and the extent to which it is operated simultaneously with other controls each of these faults could produce a different failure effect with varying consequences and likelihood. For safety critical failure modes a means of identifying the problem before it causes a hazard is recommended or where this is impossible maintenance and testing programs should pay particular attention to this component.

6.2.2 Hazop

Hazop looks at the problem starting from the failure effect.

Design conditions are first identified. For example the transmitter is designed to transmit a signal with a particular frequency and signature and a particular amplitude. The process considers each design condition with a set of key words which represent deviations from the design condition.and looks for possible causes and consequences of this problem.

For example for the design condition frequency key deviations are too high, too low other than regular signal. The cause and effect of deviations in frequency are considered and risks are assessed.

6.3 Summary Recommendations – Electronic Hardware Issues

The design philosophy for radio remote control systems has to take into account the mining environment and culture. This means robust well protected design from both a mechanical and electrical view point.

A detailed assessment of risks needs to be carried out seeking failure modes and causes for unwanted failure effects. This should include consideration of the possibility of magnetic coupling from high current transients that may be generated during the control of some types of equipment. (either the remote controlled equipment or nearby machines)

Motion from stray electrical signals anywhere in the system can be prevented by a checking system whereby the software confirms with the control unit that the signal was indeed initiated before activating the actuators . This can be accomplished in fractions of a second and would not slow response. it does not catch any false signal from the control unit due to human error or switch failure

Testing of electronic equipment should include tests for mechanical robustness, response to stray signals as well as reliability testing of electronics.

The maintenance and regular testing required should be defined and documented.

7 SAFETY CRITICAL SOFTWARE ISSUES

7.1 Introduction.

This section considers the risks associated with the use of embedded software in complex safety critical systems. While software errors have been established as a major cause in only two of the incidents collected by the Department of Mineral Resources, this type of error at present leaves no evidence and may well play a part in the 8 incidents for which no cause could be identified. Software problems can be expected to increase as the practice of modifying machine capabilities by patching new functions on to existing software increases. This practice leads to unknown interactions developing between different parts of the software which can result in major failures in control.

The use of software control systems introduces a high degree of flexibility and the capacity for more precise adjustments in control in response to a range of signals. In the mining industry the potential for precision and for diagnosing the state of the machine is not fully utilised. With the potential for increased flexibility there is also increased complexity and an increased range of failure modes. These can have important safety implications.. The vast majority of work on safety in software systems was until recently in the domain of the military due to the highly complex and sophisticated needs of that industry. Now however safety of software control is a major issue in process control and in the petrochemcial and nuclear industries. Much of the documentation on safety critical software systems derives from Military and Air Industry Standards including: MIL-STD-498 (Software Development and Documentation); MIL-STD-882C (System Safety Program Requirements); FAA safety document (RTCA)/DO-178B (Software Considerations In Airborne Systems and Equipment Certification); Def Stan 0056 (Safety Management Requirements for Defence Systems).

The following notes give an overview of the issues of safety in computer control systems. In the petrochemicals and nuclear industries and in Military applications there are extensive specification requirements for such safety critical software. Extensive check lists are published to give assurance that potential risks are identified and controlled. While it may not be appropriate to apply all of these to the mining industry, current practices in software design for remote control systems are very far from good practice for safety critical software.

7.2 Causes of software failures - generic reasons.

Chen and Yang quote a range of potential sources for error in engineering software systems which have been identified from past accidents these include

(i) Unrealistic software risk assessments

(ii) designers fail to understand the contribution of software to the system risk factor.

(iii) Poor software design leading to human errors designers fail to incorporate an understanding of the real world and human factors.

(iv) For complex real-time software, failure to understand that timing is of critical importance

(v) the erroneous belief that the quickest response is better. Too early can also be an error.

(vi) Putting too much confidence in software Replacement of hardware control components by software is made too quickly without consideration for the maturity and confidence level of the software.

(vii) Failure to understand differences between hardware and software reliability concepts. Although software is not subject to random failure and wear- like hardware, software design deteriorates over the product life cycle due to modifications. These errors are much harder to find and eliminate.

7.3 Software Risk Assessment

There are several forms of software risk assessment specified in different standards, such as:

Preliminary Software Hazard Analysis
Software Safety Requirements Analysis
Software Safety Design Analysis
Software Safety Code Analysis
Software Safety Test Analysis
Software Safety Change Analysis

All these forms of hazard analysis stem from the software safety plans outlined in the various sections in the military literature referred to above.

A large number of tools and techniques from technical risk analysis have been adapted to examining safety critical software. These include:

- Petri Nets
- Software Fault Trees
  - Cutset analysis
  - Quantitative analysis
  - Common Cause Analysis
- Software Sneak Circuit Analysis
  - Desk Checking
  - Code Walk-Through
  - Structural Analysis
  - Proof of Correctness
- Event Tree Analysis
- Hazard and Operability Studies (CHAZOP)
- Monte Carlo Simulation
- Cause Consequence Analysis
- Cross Referencing Listing Analysis
- Traceability Analysis

- Hierarchy tool
- Compare and Certification Tool
- System Cross Check Matrices
- Software matrices
- Topological Network Trees
- Critical Function Flows

This list is not complete but gives an indication of the number of types of such tools and techniques that are available to those involved in designing safety critical software.

The tools must be used in conjunction with high quality software engineering practices including configuration control, reviews and audits, structured design, and related systems engineering practices.

The following methodology is taken from "Software System Safety Handbook"' produced by the Joint (U.S.) Services Computer Resources Management Group,

7.4 Determination of Safety-Critical Computing System Functions.

Safety Critical systems are those which may involve

i. An unsafe condition,

ii. Malfunction of a fail-safe system,

ii. Non-operation of a safety function.

7.4.1 Specifications.

The safety critical functions of the computing system should be determined from the analysis of the system and its specifications. These computing system safety functions are designated 'Safety-Critical Computing System Functions' (SCCSF's). The risks of such SCCSFS should be assessed

Examples of these SCCSF'Sare :

i. Any function which monitors the state of the system for purposes of ensuring its afety.

ii. Any function that senses hazards and/or displays information concerning the protection of the system.

iii. Any function which controls or regulates the energy sources in the system.

iv. Fault detection priority. The priority structure of fault detection and restoration of safety or correcting logic should be considered safety critical, i.e., those software units or modules handling or responding to these faults.

v. Interrupt processing software. Any interrupt processing software, interrupt priority schemes and routines which disable or enable interrupts.

vi. Autonomous control. Any software components that have autonomous control over safety-critical hardware.

vii. Software controlled movement. Any software that generates signals which have been shown through analysis to directly influence or control the movement of hardware components or initiate safety-critical actions.

viii. Safety critical displays. Any software that generates the outputs that display the status of safety critical hardware systems. Where possible, these outputs should be duplicated by non-software generate output.

ix. Critical data computation. Any software that may not be connected to or directly control a safety-critical hardware system. Design and Development Phase - Process Requirements and Guidelines.

Configuration control

A configuration control group should be set up with the responsibility for evaluating all software changes to ensure that they do not conflict with existing systems or introduce potential safety problems.

Software quality assurance.

Assurance is defined as the confidence that the risk associated with using a system conforms to some expectation of tolerable risk. Since no one assurance approach is adequate information from several methods should be used to make decisions

Two person rule.

At least two people shall be thoroughly familiar with the design, code, testing, and operation of each software module in the system.

Program patch prohibition.

Patches shall be prohibited throughout the development process. All software changes should be coded in the source language and complied prior to entry into operational or test equipment.

Software design verification and validation.

A system safety team should verify and validate that the safety design requirements have been correctly and completely implemented. Test results should be analysed to identify potential safety anomalies that may occur.

7.4.2 System Design Specification Guidelines.

The following represents examples of design guidelines for safety critical systems

i. Designed safe states

The system should have at least one safe state identified for each logistic and operational phase.

ii. Standalone computer.

Where practical safety critical functions should be performed on a standalone computer. If not practical safety critical functions should be isolated to the maximum extent practical from non-critical functions.

iii. Ease of maintenance

The system and its software should be designed for ease of maintenance by personnel not associated with the original design team. Documentation specified for the computing system should be developed to facilitate maintenance of the software. Strict configurational control of the software during development and after deployment is required. The use of techniques for the decomposition of the software system for ease of maintenance is recommended.

iv. Safe state return.

The software shall return all hardware subsystems under the control of software to a designed safe state when unsafe conditions are detected.

v. Restoration of interlocks.

Upon completion of tests and/or training wherein safety interlocks are removed, disabled or bypassed, restoration of those interlocks should be verified by the software prior to being able to resume normal operation. While overridden, a display should indicate the status of the interlocks..

vi. Input/Output registers.

Input/output registers and ports shall not be used for both safety-critical and non-safety critical functions unless the same safety design criteria are applied to the non-critical functions.

viii. External hardware failures

The software shall be designed to detect failures in external hardware input or output hardware devices and revert to a safe state upon their occurrence. The design shall consider potential failure modes of the hardware involved.

ix. Circumvent unsafe conditions

The system design should not permit detected unsafe conditions to be circumvented.

x. Fallback and recovery.

The system should be designed to include fallback and recovery to a safe state of reduced system functional capability in the event failure of system components.

xi. System errors log.

The software shall make provision for logging all system errors detected. The operator shall have the capability to review logged system errors. Errors in safety-critical routines shall be highlighted and shall be brought to the operator's attention as soon as practical after their occurrence.

xii. Positive feedback mechanisms.

Software control of critical functions should have feedback mechanisms that give positive indication of the function's occurrence?

xiii. Peak load conditions

The system should be designed to ensure that deign safety requirements are not violated under peak load conditions?

xiv. Endurance issues.

It is possible that the context in which a program executes can degrade over time. Systems that are expected to operate continuously are subjected to demands for endurance – ie the ability to execute for the required period of time without failure. Long-duration programs are exposed to a number of performance and reliability problems that are not always obvious and that are difficult to expose through testing. This makes a careful analysis of potential endurance-related defects an important risk-reduction activity. Duration requirements should be explicitly identified and possible changes with time should be considered. (examples are memory and disk fragmentation, cumulative drift in clocks, cumulative jitter in scheduling etc)

xv. Error handling.

Causal analyses of software defects frequently identify error handling as a problem area. One such common defect is failure to consider all error conditions or error paths. Some studies have shown that many system failures have been traceable to design faults in that portion of the system responsible for detecting and responding to error conditions. It would appear that frequently the problems were due to oversight or simple logic errors. In many such cases the errors were encountered far along in the development process.

The presence of simple logic errors appears to illustrate the fact that error handling is typically not as carefully inspected and tested as other aspects of system design.

xvi. Redundancy management

In order to reduce the vulnerability of a software system to a single mechanical or logic failure, redundancy is frequently employed. However, the added complexity of managing the redundancy in fault-tolerant systems may make them vulnerable to additional failure modes that must be accounted for by the developer.

If the developer's design includes redundancy have the additional potential failure modes from the redundancy scheme been identified and mitigated?

xvii. Safe modes and recovery

A common design idiom for critical software systems is that they are self checking and self protecting . This means that software components protect themselves from invalid requests or invalid input data by frequently checking for violations of assumptions or constraints. In addition, they check the results of service requests to other systems components to make sure that they are behaving as expected. Finally, such systems typically provide for the checking of internal or external states to determine if the routine is itself working as expected. Violations of any of these kinds of checks require transition to a safe state if the failure is serious or if the confidence in further correct execution has been seriously reduced. Failure to address this defensive approach can allow a wide variety of failures to propagate through the system in unexpected and unpredictable ways, potentially resulting in a hazard.

xviii. Isolation and modularity

High resources are required for safety critical software assurance and this is one of the reasons that a major design goal for critical software is to keep the critical portions small and isolated from the rest of the system. This also reduces potentially safety critical error modes. Confidence that unanticipated events or latent defects in the rest of the software will not introduce an operational hazard is in part correlated with the confidence that isolation of safety critical parts of the software has been achieved.

Design should include attention to the implementation of "firewalls" in the software ie boundaries where propagation of erroneous values is explicitly checked and contained?

7.4.3 Power-Up System Initialisation Requirements

The following requirements apply to the design of the power subsystem, power control, and power-on initialisation for safety-critical applications of computing systems

Power-up initialisation

The system should be designed to power-up in a safe state. An initialisation test should be incorporated in the design that verifies the system is in a safe state and that safety-critical circuits and components are tested to ensure their safe operation. The test shall also verify memory integrity and program load.

Power faults

The system and computing system shall be designed to ensure that the system is in a safe state during power-up, during intermittent faults or fluctuations in the power that could adversely affect the system.

Primary computer failure.

The system should be designed such that a failure of the primary computer will be detected and the system returned to a safe state.

Maintenance interlocks.

If the system include maintenance interlocks, safety interlocks? They should not be able to be inadvertently overridden?

System level check.

Software should designed to perform a system level check at power up to verify that the system is safe and functioning properly prior to application of power to safety-critical functions including hardware controlled by the software? Periodic checks should be performed by the software to monitor the safe state of the system?

Control flow defects.

This refers to the sequencing of instructions executed while a program is running. The consequence of defects in control flow may be program termination. however the consequences may simply be continued execution in an invalid or unpredictable state. For example, a "computed goto may branch to a legitimate instruction sequence that is simply not the correct sequence given the current state of the system. Another sequencing failure could be where two tasks are executing in the software concurrently and the outcome depends on which completes first. There should be evidence in safety critical systems that these kind of defect have been considered and mitigated. identification and mitigation for the concurrent requirements?

7.5 Computing Environment Issues.

7.5.1 CPU Selection.

The following guidelines apply to Central Processing Units (CPU's)

i.CPU's that process entire instructions or data words are preferred to those that multiplex instructions or data (e.g., an 8-bit CPU is preferred to a 4-bit CPU emulating an 8-bit machine.

ii.CPU's with separate instruction and data memories and busses are preferred to those using a common data/ instruction bus. Alternatively memory protection hardware, either segment or page protection, separating program memory and data memory is acceptable.

iii.CPUs, microprocessors and computers that can be fully represented mathematically are preferred to those that cannot.

7.5.2 Minimum Clock Cycles.

Analyses and measurements should be conducted to determine the minimum number of clock cycles that must occur between functions on the bus to ensure that invalid information is not picked up by the CPU.

7.5.3 Read Only memories.

If Read only memory is used there should be systems to ensure that the data cannot be corrupted or destroyed.

7.6 Self Checking Requirements

7.6.1 Watchdog timers

Watchdog timers or similar devices should be provided to ensure that the microprocessor or computer is operating properly. The timer reset should be designed that the software cannot enter a loop and reset the timer as part of that loop sequence. The design of the timer should ensure that failure of the primary CPU clock cannot compromise its function. The timer reset should be designed such that the system is returned to a known safe state and the operator alerted.

7.6.2 Memory Checks.

Periodic checks of memory, instruction, and data bus should be performed. The design of the test sequence should ensure that single point or likely multiple failures are detected. Checksum of data transfers and Program Load Verification (PLV) checks should be performed at load time and periodically thereafter to ensure the integrity of safety-critical code.

7.6.3 Fault detection

Fault detection and isolation programs should be written for safety critical subsystems of the computing system. The fault detection program shall be written to detect potential safety critical failures prior to execution of the safety-critical function. Fault isolation programs shall be designed to isolate the fault to the lowest level practical and provide this information to the operator and/or maintainer.

7.7 Interface Design Requirements.

i. Feedback loops.

Feedback loops from the system hardware should be designed such that the software cannot cause a runaway condition due to the failure of a feedback sensor? Known component failure modes should be considered in the design of the software and checks designed into the software to detect failures.

ii. Interface control.

Safety-Critical Computing System Functions and their interfaces to safety critical hardware should be controlled at all times. The interface should be monitored to ensure that erroneous or spurious data does not adversely affect the system, that interface failures are detected, and that the state of the interface is safe during power up, power fluctuations and interruptions, event of system errors or hardware failures.

iii. Decision statements

Decisions statements in safety-critical computing system functions shall not rely on inputs of all ones or zeros, particularly when this information is obtained from external sensors.

iv. Data Transfer Messages

Are parity checks and checksums used for verification of correct data transfer. Should Cyclic Redundancy Checks (CRC's) be used as well? No information from data transfer messages should be used prior to verification of correct data transfer.

vi. External Functions.

External functions requiring two or more safety-critical signals from the software should not receive all of the necessary signals from a single input/output register or buffer.

vii. Input Reasonableness Checks.

Limit and reasonableness checks should be performed on all analogue and digital inputs and outputs prior to execution of safety critical functions based on those values. No safety-critical functions should be executable based on safety-critical analogue or digital inputs that cannot be verified.

7.8 Critical Timing and Interrupt Functions.

i. Safety-critical timing.

Safety-critical timing functions should be controlled by the computer and not rely on human input. Safety-critical timing values should not be modifiable by the operator from consoles.

ii. Valid interrupts.

Is the software capable of discriminating between valid and invalid (e.g., spurious) external and/or internal interrupts? Invalid interrupts should not be capable of creating hazardous conditions. Valid external and internal interrupts should be defined in system specifications. Internal software interrupts are not a preferred design as they reduce the analysability of the system.

iii. Recursive loops.

Recursive and iterative loops should have a maximum documented execution time. Reasonableness checks should be performed to prevent such loops from exceeding the maximum execution time.

iv. Time dependency

The results of a program should not be dependent on the time taken to execute the program or the time at which execution is initiated. Safety-critical routines in real-time programs should ensure that the data used is still valid (e.g., by using senescence checks).

7.9 Software Design Requirements

i. Modular code.

All software design and code should be modular. Modules should have only one entry and one exit point.

ii. Number of Modules.

The number of program modules containing safety-critical functions should be minimised within the constraints of operational effectiveness, computer resources and good software design practices?

iii. Execution path.

Safety-critical system functions should only one possible path leading to their execution.

iv. Halt instructions.

Halt, stop or wait instructions should not be used in code for safety-critical functions. Wait instructions can be used where necessary to synchronise Input/Output, etc., and when appropriate handshake signals are not available.

v. Unnecessary features.

Software should contain only those features and capabilities required by the system? It should not contain undocumented or other unnecessary features?

vi. Indirect addressing features.

Indirect Addressing features should only be used in well controlled applications. If used the address should be verified as being within acceptable limits prior to execution of safety-critical operations. Data written into the arrays in safety-critical applications should have the address boundary checked by the compiled code.

vii. Uninterruptable code.

If interrupts are used, sections of the code which have been defined as uninterruptable should have defined execution times monitored by an external timer.

viii. Unused memory.

All processor memory not used for or by the operational program should be initialised to a pattern that will cause the system to revert to a safe state if executed. It should not be filled with random numbers, halt, stop, wait, or no-operation instructions. Data or code from previous overlays or loads should not be allowed to remain.

Examples:

If the processor architecture halts upon receipt of non-executable code, a watchdog timer should be provided with an interrupt routine to revert the system to a safe state.

If the processor flags non-executable code as an error, an error handling routine should be provided to revert the system to a safe state and terminate processing.)

In such instances information should be provided to the operator to alert him to the failure or fault observed and to inform him of the resultant safe state to which the system was reverted.

ix. Flags and variables.

Flags and variables should be unique?

x. Loop entry point.

Loops should have one and only one entry point? Branches into loops should not be used. Branches out of loops should lead to a single point placed after the loop within the same module.

xi. Software maintenance design.

Software should be annotated, designed, and documented for ease of analysis, maintenance, and testing of future changes to the software.

xii. Variable declaration.

All variables or constants used by a safety-critical function should be declared/initialised at the lowest possible level?

xiii. Unused executable code.

Operational program loads should not contain unused executable code.

xiv. Unreferenced variables.

Operational program loads should not contain unreferenced or unused variables or constants.

xv. Assignment statements.

Safety-critical computing system functions and other safety-critical software items should not be used in one-to-one assignment statements unless the other variable is also designated as safety-critical (e.g., it should not be redefined as another non-safety-critical-variable).

xvi. Conditional statements.

Conditional statements should have all possible conditions satisfied and under full software control (i.e., there should be no potential unresolved input to the conditional statement). Conditional statements should be analysed to ensure that the conditions are reasonable for the task and that all potential conditions are satisfied and not left to a default condition. All condition statements should be annotated with their purpose and expected outcome for given conditions.

xvii. Strong data typing.

Safety-critical functions should exhibit strong data typing. Safety-critical functions should not employ a logic "1" and "0" to denote the safe/non-safe states. If appropriate the safe state should be represented by at least a unique four bit pattern. A non-safe pattern should not be the inverse of a safe state pattern.

xviii. Timer values annotated.

Values for timer should be annotated in the code. Comments should include a description of the timer function, its value, and the rationale or a reference to the documentation explaining the rationale for the timer value. These values should be verified and should be examined for reasonableness for the intended function.

xix. Global variables.

Global variables should not be used for safety-critical functions.

7.10Summary Recommendations Software Issues

The protocols and design and maintenance philosophy for software used in remote control systems in mining is very far from those required in safety critical systems in other industries. The extensive requirements reviewed above are only a subset of those required for Military and highly safety critical installations such as nuclear power yet may still seem impractical to implement in a formal way in mining as design requirements all of which will be verified. It is however necessary for the design philosophy of the software used in remote control to move towards safety critical design. This is a matter of expertise within the organisations that program the Units and a acceptance of safety critical design philosophy. There is a large difference in the programming philosophy used in standard programming applications and that used in safety critical systems and it is important that this is transferred into software in mines

Safety Critical software needs to be modular with links between modules minimal and clearly understood. New code to provide new functions should never be patched on to existing code without a full understanding of all the implications it has for interactions in the rest of the system. Self checking protocols should be introduced to pick up errors at safety critical positions. Particular attention needs to be paid to the potential for loops within the system and response to unwanted and multiple signals. Software also requires maintenance and checking and maintenance requirements need to be defined.

Although software faults have not been directly implemented in many incidents as yet, complexity is increasing with each new patch and each new version and the potential for such failures is increasing. It is also possible that the growing numbert of unplanned movements for which no cause can be found are software induced

The Industry has two options here. One is to rely on expertise in the software developers to move towards this philosophy. The other is to develop a check list for software design verification such as that published in the Software System Safety Handbook

8 GENERAL CONCLUSIONS AND RECOMMENDATIONS.

Remote control is a major design change from on board control which has been essentially piggy backed on to existing systems without any consideration of the design that equipment ought to take with remote operation. The complexity of control system has increased considerably providing more possible paths for error. The improvements in safety for the operator gained by removing him or her from the cab have been replaced by new risks. This report does not attempt to address the issue of the risks of conventionally controlled machines or to make any comparison between conventional and remote operation. it outlines the possible sources of error and unplanned movements from remote control equipment based on experience in the aircraft and mining industries and on a review of literature.

The report can be used to provide guidance on issues which need to be included when assessing the risks of remote controlled operations in mines and makes recommendations to reduce risks. Detailed recommendations to reduce risks are summarised at the end of each chapter and in the Executive Summary

Risk can be reduced by preventing unplanned movements, removing the person from the danger zone round the equipment or providing advanced warning of movement so that the person has time to move out of the way. Rasmussen (1987) suggests that errors in complex systems can be reduced but cannot be prevented. Applying the recommendations in this report will reduce the risk of injury from unplanned movements but will not eliminate it. For the reasons outlined in the report it will not be practical to eliminate people from the danger zones simply by training. Physical means of separation need to be considered. This might involve providing a safe platform for operation of the machine, designing work systems so it is never necessary to enter unsafe regions to perform a task or installing barriers and stops so that when the machine hits the wall there is still space for a person. It is almost certainly feasible but non trivial for the machine to detect the presence of a person in some way and not operate if they are too close. Each of these possibilities has its own practical problems but should be given serious consideration.

An alternative is possibity is to seek a means to control the error after it has entered the system, regardless of source, and do so before it has yielded an actuator motion. There are several options open to do this. One is to introduce a gradual start to motion with feed back so the operator has time to respond if the motion is unwanted. An alternative is to look at the properties of the error signal and to seek some point in the control path where it can be detected prior to any motion. A request for confirmation signal could be sent back to the operator from the point of the control path just before the actuator. This would in effect mean double initiation of some critical signals which would create the delay required for the person the consider whether the action is required and confirm. If a delay creates real (as opposed to perceived) production problems it may be appropriate to limit it to maintenance mode. An extension of this idea would be a control system that provided confirmation information to the operator about the nature of the signal initiated, during the time it takes the movement to occur.

9 REFERENCES.

Bainbridge, L., (1987). The change in concepts needed to account for human behaviour in complex dynamic tasks. In IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, Vol. 27, No.3, May 1997.

Becker, A.B. et al, (1991). Effects of feedback on perceived workload in vigilance performance. Proceedings of the human Factors Society 35th Annual Meeting (pp.1491-1494). Santa Monica, CA: Human Factors Society.

Billings, C.E. (1991). Human-centred aircraft automation philosophy (Technical Memorandum 103885). Moffett Field, CA: NASA Ames Research Center.

Brazier, A. J. and Skilling J. M. (1996) Human Factors Data from Near Miss Reports. 14th International System Safety Conference, Albuquerque, New Mexico.

Chapanis, A. (1972). Design of controls. In H.P. Van Cott and R.G. Kinkade (Eds.), Human engineering guide to equipment design (rev. ed.) Washington, DC: Government Printing Office.

Chen, B. and Yang, L. (1995). Design, Testing and Verification of Safety Critical Software. In Hazard Prevention, 4th quarter, 1995, Pub: System Safety Society, 1995.

Department of Mineral Resources, Remote Control of Mining Equipment, Task Group One, NSW, Sydney, 1998.

Dittmar, M.L. et al, (1993). Sex differences in vigilance performance and perceived workload. The Journal of General Psychology, 120(3), 309-322.

Endsley, Mica R., and Kiris, Esin O., The Out-of-the-Loop Performance Problem and Level of Control in Automation. Human Factors, 1995, Vol 37(2).

Endsley, Mica R., Level of Automation: Integrating Humans and Automated Systems, Proceedings of the Human Factors and Ergonomic Society 41st Annual Meeting, 1997.

Flach, J.M. (1995) Situation awareness: Proceed with caution. Human Factors, 1995, 37(1), 149-157Rasmussen, Jens., Reasons, Causes, and Human Error, in New Technology and Human Error, 1987, Wiley and Sons.

Funkk, Lyall and Suroteghal 1999 http://flightdeck.ie.orst.edu/metaanalysis

Galinsky, T. L. et al, (1993). Psychophysical determinants of stress in sustained attention. Human Factors, 35(4), 603-614.

Hart, S. G., et al. (1984). Pilot workload, performance, and aircraft control automation. In Human factors considerations in high performance aircraft (AGARD-CP-371 (pp. 18/1-18/12). Neuilly sur Seine, France: NATO-AGARD.

Harris, W.C., et al (1994).The comparative effectiveness of adaptive automation and operator initiated automation during anticipated and unanticipated taskload increases. In M. Mouloua and R. Parasuraman (Eds.), Human performance in automated systems: Current research and trends (pp. 40-44). Hillsdale, NJ: LEA.

Martin, M., and Jones, G.V., (1984). Cognitive failures in everyday life. In J.E. Harris and P.E. Morris (Eds.), Everyday memory, actions and absent-mindedness (pp.173-190). London:Academic.

Molloy, R. et al, (1996). Monitoring an Automated System for a Single Failure: Vigilance and Task Complexity Effects. Human Factors, 1996, 38(2), 311-322.

Moray, N. (1986). Monitoring Behaviou rand supervisory contorl. In K. Boff (Ed.), Hasndbook of Perception and Human Performnance (II), (pp 40/1- 40/51). NY: Wiley.

Mosier, K. L. et al. (1994). Cognitive and social psychological issues in flight crew/automation interaction. In M. Mouloua & R. Parasuraman (Eds.)

Human performance in automated systems: Current research and trends (pp.191-197). Hillsdale, NJ:Erlbaum.

Norman, S. D. & Orlady, H. W. (Eds.) (1989). Flight deck automation: promises and realities. Moffett Field, CA: NASA.

Norman, D.A. (1990). The 'problem' with automation: inappropriate feedback and interaction, not 'over-automation'. Phil. Trans.R.Soc.Lond. B 327, 55-593 (1990).

Parasuraman, Raja., Human Computer Monitoring, Human Factors, Vol. 29(6), Human Factors Society, 1987.

Parasuraman, R., et al (1992). Theory and and design of adaptive automation in aviation systems (AWCADWAR-92033-60). Warminster, PA: Naval Air Warfare Center, Aircraft Division.

Pesonen, J., and Lahtinen, K., 1987 Safety Aspects in the Use of Radio-Controlled Cranes in Finnish Industry, The International Journal of Human Factors in Manufacturing, Vol.2 (4).Rasmussen, Jens., Reasons, Causes, and Human Error, in New Technology and Human Error, 1987, Wiley and Sons.

Rasmussen, Jens., Reasons, Causes, and Human Error, in New Technology and Human Error, 1987, Wiley and Sons.

Riley, V. (1994). A theory of operator reliance on automation. In M. Mouloua & R. Parasuraman (Eds.), Human performance in automated systems: current research and trends (pp. 8-14). Hillsdale, NJ: LEA.

Sarter, N. B., and Woods, David D.1995 , How in the World Did We Ever Get into That Mode? Mode Error and Awareness in Supervisory Control, Human Factors, 1995, Vol 37(1).

Sarter, N. B, Woods, D. D. and Billings C. E. 1996 Handbook of Human Factors and Ergonomics, 2nd ed. (G. Salvendy, editor); NY: John Wiley & Sons, 1996

Scerbo, M. W., Greenwald, C. Q., and Swain, D. A., (1993). The effect of subject controlled pacing and task type on sustained attention and subjective workload. The Journal of General Psychology, 120 (3), 293-307.

Wiener, E.L and Curry. (1980) Flight deck automation: Promises and Problems. Ergonomics, 23, 995-1011.

Wiener, E. L. (1989). Human Factors of advanced technology ("glass cockpit") transport aircraft (Tech. Report 177528). Moffett Field, CA: Human Factors and Ergonomics Society.

Wiener, E. L. (1993). Life in the second decade of the glass cockpit. In R.S. Jensen and D. Neumeister (Eds.). In Proceedings of the Seventh International Symposium on Aviation Psychology (pp 1-11). Columbus, OH:Ohio State University, Dept. of Aviation.

Young, L. R. A. (1969). On adaptive manual control. Ergonomics, 12, 635-657.

Zuboff, S. (1989) In the age of the smart machine: the future of work and power. NY: Basic books.

9.1 Handbooks

"Software System Safety Handbook"' produced by the Joint (U.S.) Services Computer Resources Management Group,

Defence Standard 00-56, Safety Management Requirements for Defence Systems, Ministry of Defence, United Kingdom Government.

Defence Standard 00-55, Requirements for Safety Related Software in Defence Equipment, Ministry of Defence, United Kingdom Government.

MIL-STD-882B System Safety Program Requirement, Department of Defence, Washington, United States Government.

IEEE Standard for Software Safety Plans 1228-1994, IEEE Computer Society, Institute of Electrical and Electronic Engineers, Inc. New York.

Joint Services System Safety Committee, Software System Safety Handbook, Electronic Industries Association, G-48 Committee.

APPENDIX 1

UNPLANNED MOVEMENTS

DEPARTMENT OF MINERAL RESOURCES

Remote Control of Mining Equipment: Known Incidents worldwide.

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
4 Jan 1989	Remote control LHD did not respond to signal - David Bell Mine	A remote control LHD did not respond to the operator's transmitter signal. It backed toward the operator causing him to fall backwards over loose rock. The operator sustained bruises. The operator was not aware that the spare transmitter differed in control signal for braking from the unit he had been accustomed to using. Also, he was standing too close to the machine while on remote control. Note - the spare unit was borrowed from an adjacent mine.	• Remote control was taken out of service and returned to its owner. • The operating procedure was reviewed. • A system for positive machining identifying and recording the transmitter units assigned to receiver units is being developed.
1 Feb 1989	JS5OO LHD ran away 140 feet - Creighton	While mucking on remote control the operator lost control of a JS500 while changing from the remote to manual mode The scooptram travelled 140· down a ramp striking the wall and coming to rest. The operator was not on the machine. CAUSE: The park brake toggle was defective and the operator changed from "remote" mode to "manual" mode on an incline.	• Personal contact given to loader operators on the danger of using defective unit. • Remote control stations should be maintained. • Do not change from remote to manual mode on an incline unless safety berms are installed to prevent loader movement.
13 June 1989	JS500 squeezed operator against wall - Creighton	While mucking on remote control with a JS500 LHD a worker was squeezed against the wall by the scoop. CAUSE: There were a number of possible causes. • Inadequate clearance for both the operator and the loader in the drawpoint heading. • The steering on the loader was found to be sluggish and could have been a factor because of slow steering response. • The operator was too close to the loader while the unit was on remote control.	• Remote control stations installed where possible. • The company has set up a Fail Safe Committee to review all remote control procedures. • More training for remote control operators. • Ensure operators check their remote control devices before using them.
5 July 1989	Operator fell as LHD came towards him - Golden Giant	Operator was caught when the JS500 he was operating on remote control rolled downgrade in neutral. The transmitter for remote control became caught and was damaged against a rock wall. The worker fell. The loader stopped against the rock wall with the operator's legs under the rear section of the loader. The operator was not injured.	• The JC500 models have now been refitted with air brake solenoids which have a larger orifice, providing a faster airflow. • The brake response time on remote operation is now reduced and is comparable to the response time for manual operation. • A safety bay was immediately excavated. This enables

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
		CAUSE: The operator is reported to have misjudged the stopping capability of this loader while it was backing on a downgrade. The lag time of the air brakes permitted the unit to roll rearward in neutral. A difference in brake response time between two models JS500 and ST8 loaders is reported to exist and operators use both units interchangeably. The operator was standing in an unsafe area.	the operator to safely control the loader.
18 July 1989	Fire on remote control LDH - Fraser	A small fire in the dump cylinder area of an ST4 loader was extinguished with the fire suppression system. CAUSE: The loader was on remote when some muck rolled down the muckpile striking th dump cylinder hose and the lighting wires. The sparks from the severed wires ignited the hydraulic oil.	• More protection added to the wiring and the hose and wiring was repaired.
12 June 1990	Remote control LHD pinned operator - Magancon	Remote control loader pinned the operator against the wall. The control box was destroyed and the operator received severe bruising to his leg. CAUSE The operator was not standing in the safety bay while operating the loader remotely. Since the control box was destroyed, it is impossible to check its operation.	• The company will retrain operators on the remote control loader and ensure that they follow the written procedure for their operation.
18 Dec 1990	6yd Toro fire on brakes - Winston Lake	An operator was using a Toro 6yd loader using remote control when he noticed smoke and flames at the front end of the machine. He brought the machine out using the remote control and put out the fire with an extinguisher. CAUSE The brake application lever is positioned in line with the remote control on/off switch. Investigation discloses that the operator must have inadvertently caused the brakes to be partially applied with his sleeve cuff.	• A guard plate has been installed behind the brake lever to divert sleeves or cuff of gloves away from this lever

Remote Control of Mining Equipment: Known Incidents worldwide.

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
8 Mar 1991	2 5yd electric LHD turned off on side - Dona Lake	A remote operated Wagner 2.5yd electric LHD tipped over onto its left side as it was backing up. The right side of the machine rode up onto a high spot on the floor CAUSE Operating the machine over a high spot and poor visibility because of sandfill and water caused the incident.	• The high spot on the floor was removed
27June 1991	Remote controlled LHD fell 60 feet - Magino Mine	A remote controlled Wagner ST3.5 LHD unit did not respond to the operator's control, drove into an open stope and fell approximately 60 feet. rolled on the muckpile of this stope to a drawpoint where it was retrieved. CAUSE No records were kept of transmitter battery usage. The low battery indicator on the transmitter was inoperative. It was concluded by mine personnel that due to low battery voltage, the new signal may have been insufficient to override the previous signal.	• A system was instituted to closely supervise battery operation. • Batteries are not to be used longer than four hours.
28 Aug 1991	Elphinstone caught fire in battery area - Williams Mine	A 6yd Elphinstone LHD vehicle was operating under remote control. The operator noticed smoke and flames coming from the vehicle's battery compartment. He activated the fire suppression that shut the vehicle down and extinguished the fire. • A battery post shorted against the steel battery box cover.	• Replaced battery cables. The battery box will be redesigned to prevent battery post contact with the cover.
25 Nov 1991	JS100 turned on side - A.J. White	In the longhole stope the operator of a remote controlled JS100 loader rolled over in the stope. CAUSE The worker was about 150 feet from the loader when he looked down to kick a piece of muck out of the way. The front wheel of the loader ran up a high area of the roadway to the muckpile (loose muck) and it rolled over.	• Loader operators were instructed to stop the remote operated machine and apply the brake when doing other tasks.
13 Dec 1991	Remote control LHD turned on side - A.J. White	A worker was operating a JCI 125 LHD by remote control and was attempting to backblade muckpile. The front wheels were partway up the muckpile when the operator	• The loader operator has had similar experience in the past. • The employer has removed the operator from the job

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
		turned the LHD and the LHD tipped on its side. • The operator did not follow the proper mucking procedures.	of remote LHD operator, pending a review of his work performance.
18 Dec 1991	Operator pinned, left leg amputated - Winston Lake.	A remotely controlled Wagner ST3.5 pinned the operator against a wall when the machine did not respond to a right turn signal. The operator's left leg was amputated as a result of this accident. CAUSE A small stone jammed the steering controls, preventing the LHD from turning right	• Safety bays will be provided for all remote mucking stations.
10 Jan 1992	Faulty electronic card - David Bell	A remote control unit mounted on a EJC- 210, 6yd LHD vehicle was tested after the vehicle's fire suppression system had inadvertently operated when power was applied to the remote control unit. It malfunctioned and operated several vehicle functions at one time. The emergency switch was activated., stopping the machine. CAUSE Receiver electronic circuit failure, no foreign material was found on the component card.	• Faulty electronic component card was replaced.
26 Feb 1992	Fire from faulty electronic signal - Crean Hill Mine	Two remote loaders were in the same area when the starter on a JCI 1.25yd LHD momentarily engaged. The starter and wires burned CAUSE The remote 1.25yd loader started when it received an erroneous signal from the transmitter for an 8yd electric LHD.	• When two remote units are operating in close proximity, the frequency of one of the units will be changed. • A Hazard Alert is being issued.
April 92	An operator was pushed over the edge of a stope by an LHD in Ontario	A transmitter at the draw point below took over the control of the LHD	1. Transmitters: • Should be fitted with an emergency stop that immediately shuts down the engine and applies the brakes. This should also occur on loss of signal. • To eliminate possible interference between transmitters, the digital ID should be checked on a regular basis.

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
			• The ID code or frequency should only be changed by authorised personnel and should be inaccessible to others. 2. Testing and Operating: • The unit should be tested on manual and then on remote at the start of every shift • No worker to be in the path of the vehicle when being tested under remote control. • There should be some method to warn other workers that the unit is under remote control. 3. Operator Protection: The operator must remain in a safe location with a suitable place to retreat. Examples are: • Elevated safety bay designed to prevent inadvertent access of the mobile plant. • Elevated portable platform designed to protect the operator. Platforms should be one foot higher than the bumper height of a machine or located behind an effective barrier. • The selection of the operating location should be made in consultation with the supervisor. • The use of the harness portable transmitter should be discouraged. Because of the inherent dangers to the operator, some companies are using moveable pedestal units.
1 May 1992	An operator was pinned against drive wall	• The reason the loader veered off course was attributed to an intermittent fault with the RC loader's steering controls. A full inspection revealed that scoring on the steering spool in the pilot hydraulic circuit was responsible for that fault.	• Drawpoints that are to be used by remote controlled loaders will be designed so that tramming does not have to take place close to or past the operator. • Existing drawpoints to be provided with a 2m high, 1 m deep refuge cut into wall when remotes are used. • Remotes required to be fixed to a stand will not be located close to a wall.
Sept 92	An LHD caught fire when a starter motor engaged in a mine in Ontario	• The LHD was operating erratically under radio remote control. • Another radio remote control was in close proximity. • Both radio units operated at the same frequency with	Radio remote control systems should detect and block false signals.

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
		different ID codes. • The radio system allowed the signal from another transmitter to ride on top of a signal from the valid transmitter • The second transmitter was not able to make the vehicle respond unless the valid transmitter was also operating.	
22 Feb 1993	5yd LHD turned on side - Lockerby Mine	An operator was dumping into a partially filled stope using remote controls, he raised the bucket to dump and loader turned on its side. • Uneven muckpile at the dump • Boom raised too high. • Poor visibility	
24 Feb 1993	An operator was crushed by an LHD at Cobar	• Remote control operating units had some faults in the joy stick and emergency stop function. • Remote control units failed repeatedly, faults were incorrectly diagnosed and variation in their operation was common. • Poor communication and adherence of procedures.	• Rewiring of the emergency brake circuit in VHF and UHF capable LHD's. • Re-issue of safe operating procedures. • Modifications to repair procedures. • Trialing of new joy sticks.
4 April 1993	Fire on remote LHD - Lockerby Mine	The operator was mucking using remote controls, while backing up the transmission filter bleeder got hooked on a piece of screen (mesh) and broke off, oiled spilled onto exhaust and started a fire. Screen (mesh) protruding from the wall.	• All protruding screen (mesh) cut off. • Operator told to check entrance to workplace.
13 April 1993	JS100 LHD turned on side - Dickenson Mines Ltd A.W. White Mine	An operator was operating JS 100 LHD using remote control when it tipped over in a stope • Poor travelway conditions in stope (rock on roadway)	• Try to maintain the roadway in better condition.
20 April 1993	JS500 LHD turned on side - Fraser Mine	While dumping backfill waste using remote control a JS500 tipped on its side. The operator had the bucket in a raised position while turning the LHD on an incline.	• Safety meeting and muckpile talks will include a review of operating procedures.
26 April 1993	Remote control loader failed to stop and struck operator fracturing his right leg - Pasminco Southern Operations Broken Hill	The injuries sustained by the operator can be attributed to the combined events of faulty brake relay/dump valve in the loader and also the close proximity in which the operator positioned himself when operating the machine.	• Highlight to operators the hazards to positioning when undertaking remote loading and include training manuals. • Ensure other loaders on-site do not have faulty brake relay/dump valves. • Contact manufacturers and request improved fail safe systems. • Identified safe working position for remote operators

Remote Control of Mining Equipment: Known Incidents worldwide.

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
			in co-operations with operators and planning.
27 May 1993	ST8B LHD turned on side - McCreedy West		•
28 Aug 1993	Elphinstone caught fire in battery area - Williams Mine	A 6yd Elphinstone LHD vehicle was operating under remote control. The operator noticed smoke and flames coming from the vehicle's battery compartment. He activated the fire suppression system that shut the vehicle down and extinguished the fire • A battery post shorted against the steel battery box cover.	• The battery box will be redesigned to prevent battery post contact with the cover.
25 Nov 1993	A truck driver in WA, was killed by a remote controlled LHD	Procedures ?????	???????
1 Feb 1994	Significant Incident Report No42. Miner killed by coal cutting machine slewing unexpectedly.	Undetermined	Operational/procedural
15 Feb 1994	Significant Incident Report No.43. A loader caught fire in an open stope	Persons had to enter an open stope to recover/save the loader.	• Remote controlled loaders should be fitted with systems that will allow their retrieval without any person having to enter an open stope. • Maintenance should reflect the need for high reliability. • General design features should minimise risk of component failure.
March 95	Maintenance trainee was fatally injured when continuous miner conveyor boom crushed him against the wall - White Oak Mine No 2 Utah	The operator was walking in front of the machine as the machine moved towards him. The maintenance trainee was attending to the continuous mining machine's power cable at the rear of the machine when the continuous miner moved the conveyor boom crushed the trainee against the wall. The victim had only three weeks mining experience	• To provide inexperience personnel with adequate training • Safe operating procedures for remote control operations.
18 April 1995	An electrician helper was fatally injured while making repairs to a remote control continuous mining machine - Daniel's Branch Coal Co Inc No 1 Mine West Virginia	An electrical helper was positioned in the conveyor of the continuous miner during the installation of a hydraulic relief valve. He remained in the conveyor to observe the relief valve for oil leaks while a miner energised the remote control. When the pan switch was engaged on the remote control. the conveyor chain also started pushing the electrician helper against the roof. An electrical short circuit inside the remote control send unit caused inadvertent activation activation of the chain conveyor.	•

Remote Control of Mining Equipment: Known Incidents worldwide.

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
14 May 1995	An operator was crushed between a loader and a wall while he was operating a remote control loader by Bounty Mine WA.		•
26 May 1995	Significant Incident Report No57. The operator of a LHD was crushed between the machine and a sidewall.	No fault could be found with the radio remote control.	• Proper procedures derived from guidance in AS4240
13 Jun 1995	The operator of a LHD was killed when crushed by the LHD, at a NT mine.	• No fault could be found with the radio remote control. • Non-adherence to safe working procedures. • No cuddy for the operator	• Provision of cuddies for operators
-/-/95	Cordeaux Colliery, NSW. When the pump was switched on, on a Joy continuous miner, the cutting head and conveyor started.	• The IS receiver interface relay was incorrectly wired.	• Relays to be wired in a fail safe mode.
27 Aug 1995 FMEA done on 10-12 Sep 1995	An unplanned movement of a Joy CM occurred at Cordeaux Colliery. The power was turned off the CM using the pilot control switch. On restoration of power to the CM all operational equipment on the CM started simultaneously and the CM moved forward approximately 1.5m before the driver reached into the cabin and shut down the CM.	Design deficiencies in the radio remote system. • Total failure of the microprocessor leads to unknown outputs on the microprocessor with no remote method of shutting down the machine. • Relay drivers susceptible to dust and water ingress. Water in the form of condensation could collect on boards and other components and short the circuits. this could lead to faults as experienced. • Frozen RCR/CSR relays could cause a problem (however two simultaneous faults are required).	• Provide an "external watchdog" that is fail safe with appropriate hardware [protection and software monitoring. This watchdog should be independent and ensure the integrity of the microprocessor and software controls. It should trip into the machine safety circuit. It should be made up of discrete components and the trip circuit should be completely independent of the microprocessor. • All PCBs to be Conformal coated. • Radio emergency shut-down (safety) circuitry on the machine to have its integrity continually tested whilst the machine is under radio control. This shall not be bypassed by the starting of the machine in any mode. • "Log-in" system for transmitters in close proximity. • PSA (Pre start alarm) should be standard on machines (Pempek PSA is optional). • Joy/Cordeaux review the list of safety and operational functions listed in the Joy Operational Manual • Cordeaux to inspect Joy quality systems. • Provide individual current feedback for the miner controls. Joy to investigate its implementation. • Cordeaux recommend Joy assess CM99 against AS4240 and provide an appropriate plan of action • The next generation of radio systems should have. transmitter coding, spare transmitters locked out and be immune from "cross talk"

Remote Control of Mining Equipment: Known Incidents worldwide.

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
18 Sept 95	A continuous mining machine operator was killed by a roof fall - USA	The operator, utilising a remote control, was operating the continuous mining machine as the machine mined an extended cut in a crosscut. The mining machine had completed mining the right side of the crosscut through to the adjacent entry when the machine operator walked about 1.5m in by the last row of the roof bolts when a portion of the roof, 3.5m long by 2m wide by 200mm thick fell on him causing fatal injuries.	
7 Dec 1995	Operator fatally injured by falling rock - USA	A continuous mining machine operator was operating the continuous mining machine utilising remote control when a section of the newly exposed roof fell and struck the operator.	
15 Mar 1996	Significant Incident Report No 63. An LHD went out of control and narrowly missed injuring the operator.	• The radio remote control equipment was functioning correctly. • An air operated shuttle valve for the brakes failed. • Brake maintenance was less than adequate.	• Ensure brake air supply filtration systems and maintenance practices are appropriate. • Improved operator training and procedures.
6 May 1996	Elourea ABM20-035: • The PSA activated 2 or 3 times in quick succession whilst the machine was idle. • With the pump running, the PSA activated, the tramming stroke activated and the conveyor started.	No faults were found with the equipment. A FMEA identified: The microprocessor was unable to detect an unplanned processor output or motor contactor operation	The OEM developed a system using fail to safety feedback logic - a safety pack upgrade
26/6/96	An operator was struck and killed by falling roof. USA	• Acontinuous mining machine helper and a section foreman were observing the remote control continuous mining machine as the machine operator directed the machine in mining the final push out on the pillar block. After mining four shuttlecars of coal, the roof suddenly began to fall from the crosscut and into the intersection. The foreman and helper cleared the intersection uninjured, however the remote operator was struck and killed by the falling roof.	
11 Sept 1996	Elourea Colliery - ABM20: Whilst starting the pump motor the cutter motor started and the conveyor motor started.	• Only secondary functions were operating. • The machine operated as though the select button was stuck. • The radio emergency stop did not function. • There was a fault in the supporting electronic components • The software that ensures the select switch has to be	VACS not comfortable with a design change that had been made which was a Forced Potato standard design diode network.

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
		re-enabled each time a secondary function is started was erased from the receiver code	
21 Oct 1996	An operator fatally injured while tramming continuous mining machine using remote control - Little Otter Mining Inc. No 2 Mine West Virginia	The victim was using a remote control device to operate the continuous mining machine. The lift lever actuator slide which must be fitted to an upward position before the tram features of the machine can be utilised, had been taped in an upward position. While tramming the machine, the victim placed himself between the machine and the wall, the trailing cable fell from its carry position contacting the remote control and splitting the tram control levers which caused boom end of the machine to move to the right, crushing the victim.	
1 Nov 1996	A continuous mining machine operator was run over and killed USA	A continuous mining machine operator and two co-workers were located near the rear of the machine. As the off standard shuttle car was being loaded pieces of roof began to fall. One of the miners yelled a warning and ran from the area. The other miner ran as well and the continuous miner operator began the last to run was carrying the remote control box, apparently fell over just after passing the outbye end of the shuttle car. As the shuttle car was tramming out of the area the continuous miner operator was run over and killed.	
5 Nov 1996	Laleham No.1 Colliery, QLD. An operator was crushed between the rib and a Joy continuous miner and fatally injured. The operator was attempting to tram the machine in manual mode.	• The deceased placed himself in a confined space between the miner and the rib and failed to recognise the hazard. • The manufacturers operating manual does not adequately highlight the potential hazard with the manual operation. • The design, installation and configuration of the manual controls on various machines lack consistency, create confusion and do not appear to conform to basic ergonomic principles.	
Mid Dec 1996	Wambo, Joy miner: Whilst the pump was running and when the hydraulic drill rig diversion handle was pulled out the machine slewed clockwise, the boom slewed to the RHS and the shovel lifted	• Suspected moisture in the transmitter.	
30 Dec	Wambo, Joy miner, 3 unplanned movements occurred on	• Two nuts were found floating in the transmitter.	1. Transmitters:

Remote Control of Mining Equipment: Known Incidents worldwide.

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
1996	one shift: • Whilst the pump was running and when the hydraulic drill rig diversion handle was pulled out the machine trammed backwards and slewed anti-clockwise, the boom slewed to the RHS and the cutting head lifted • Whilst filling a shuttlecar with the cutting head shearing down, the cutting head lifted, the machine trammed straight back and the conveyor boom slewed to the LHS. • Whilst filling a shuttlecar with the machine trammed forward and the conveyor boom slewed to the RHS	Testing at PEMPEK showed that with the pump running the operation of hydraulic solenoids could be simulated by moving a nut along PCB (printed circuit board) tracks. • There was no insulated coating on the PCB. • In summary a single fault in the radio transmitter can cause the unplanned movement of a mining machine.	• Conformal coating of PCB's • Sheet of closed cell foam placed under the microprocessor PCB to prevent loose objects from touching the solder side of the PCB • Solder joints on the top side of the microprocessor PCB to be covered with silastic • Loctite or tamper proof nuts fitted • Tamper seal to be fitted • Maintain the equipment in accordance with the manufacturers recommendations. • Review operational and maintenance procedures so operators are not exposed to hazards associated with the inadvertent movement of machines.
March 6 1997	Myuna Colliery, NSW. A Continuous miner conveyor swing cylinder operated when not initiated	• An hydraulic spool valve jammed due to contaminated oil	• Improve the oil filtration system. • Provide feedback on the control system to prevent such actions.
6 March 1997	Myuna Colliery, NSW A continuous miner waws tested in emergency control to see if the potential for an incident similar to that at Laleham No 1. The miner immediately started to tram	• The manual tram handles were damaged and corroded and did not return to neutral	• Improve maintenance of manual tram handles. • Limit tram speed in manual or emergency to slow speed only. • Improve ergonomics of both emergency and manual control.
16 March 1997	Tahmoor Colliery, NSW whilst tramming a Joy Continuous miner the cutting heads started for no apparent reason	• No reasons were found for the failure	
18 March 1997	Oakdale Colliery NSW. Whilst the machine pump was running and the operators were roof bolting the cutter motors started unexpectedly.	• No problem found	• New type transmitter to be used.
Apr 1997	PCS Rockville Potash Mine, Sakatchawen. An extensible conveyor of a continuous miner - extensible conveyor system shut down unexpectedly. All machines and associate extensible conveyors had the same signal address.	• A signal was transmitted from another mining machine in a separate area of the mine, causing the shutdown.	• All machines and associated extensible conveyors have been given unique signal addresses.
3 April 1997	Remote control loader was in stope when a rock fell striking lights - CSA Cobar		
15 April 1997	Tahmoor Colliery whilst tramming a Joy Continuous miner the cutting heads started for no apparent reason.	• No reasons were found for the failure	
30 April 1997	Tahmoor Colliery. An incident occurred when the miner moved forward when the pump was started.	• A sticking hydraulic solenoid valve.	

Remote Control of Mining Equipment: Known Incidents worldwide.

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
April 1997	It was reported to MSHA (USA) that a conveyor boom moved when the tram switches were operated on the transmitter. The emergency stop was operated and the machine stopped.	• After the machine stopped the transmitter would not operate the machine. • Exchanging the transmitter cured the malfunction. • The display on the transmitter battery charger unit displayed "unknown frequency" when the malfunctioning transmitter was connected to it.	The unintended operation could not be replicated during laboratory testing - testing included repetetive tesing of the transmitter, reduced signal strength and reduced battery voltage.
April 1997	It was reported to MSHA (USA) that a conveyor boom was swinging to the right when tram switches were moved to the tram forward position. This was repeated several times. The transmitter was taken to the surface and checked with the diagnostics on the battery charger unit and it appeared to work properly. The transmitter was returned to the section and the machine pump was started and the transmitter unit placed on the floor, within five seconds the machine trammed forward, the conveyor boom swung to the right without the transmitter being operated. The machine was stopped by turning the transmitter off. The machine was operated without further incident with a different transmitter.	• Untended conveyor boom swing and improper tramming could not be replicated in the laboratory. • The manufacturer (Pempek) reported that under the condition of elevated signal strength (1 watt vs 50 mW actual) and signal reflection, the RF could effect the microprocessor in the transmitter. This could have caused caused a problem because the keyboard was being scanned while the unit was transmitting. This could have allowed unintended operation due to operation of the key pad switches.	• Updated software was installed in the transmitter that caused cessation of key pad scanning during transmission. • A diagnostic/data logging system has been installed to monitor all control system functions.
May 1997	A worker was killed at a mine in Ontario when a pendant control box he was using failed, and he was pinned between a control panel and part of a drill boom on a drilling machine.	• Water and grit had entered the pendant control he was using to operate the boom. • Corrosion had affected several of the switches. • Some switches were in poor condition and either did not operate or operated erratically.	• Critical functions on pendant or radio remote controls must be tested as part of the testing of motor vehicles and equipment before the shift begins. • The control box, the transmitter, receiver and interface must also be included in the regular inspection and maintenance of motor vehicles and equipment by a competent person. • The design of the remote control should take into account the rugged service requirements of mining operations..
May 1997	It was reported to MSHA (USA) that a conveyor reversed upon activation of other function switches.	• The display on the transmitter battery charger unit displayed "unknown frequency" when the malfunctioning transmitter was connected to it. • The conveyor going into reverse was duplicated and an area of the transmitter was identified as a possible cause (fault of a barrier diode). This action could only occur if the transmitter is operating normally, and the fault condition occurs after the hydraulic pump on the machine had been started. Under this condition, if the operator operated the switch intended to move the	

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
		conveyor down, the conveyor would reverse. The switch is momentary, meaning that when it is released, the conveyor would stop.	
May 1997	Tahmoor Colliery. An incident occurred when the miner moved forward when the pump was started.	• A sticking hydraulic solenoid valve	
20 Jun 1997	Rock fell on remote and broke handles - CSA Cobar		
3 July 1997	Tahmoor Colliery, NSW. The jib of a continuous miner conveyor continued to swing after the signal was removed	• Sticking hydraulic spool valve.	
28 July 1997	Operator could not see (blind spot), ripped left-hand side mudguard off - CSA Cobar.		
	Fire in battery box on remote control LHD - Williams	Flames were noticed to erupt in the battery box of a ST6 loader while it was mucking on remote control. CAUSE The hold down stud broken which secured the hold down bracket on the 12 volt battery. The hold down bracket then shifted, grounding the positive post on the battery. The direct shaft to ground heated the cable insulation, and the end of the battery.	•
8 Aug 1997	Rock hit remote control loader on blind side ripping off mudguard - CSA Cobar.		•
27 Nov 1997	United Colliery, NSW. An operator was fatally injured whilst carrying out servicing near the cutting head of a Joy continuous miner. The operator was found under the cutting head.	• The main circuit breaker on the miner had not been turned off. • The continuous miner was operating on remote control. • The deceased had the remote control transmitter on his person at the time of the accident.	• When working in close proximity of continuous miner cutting heads, the main isolator of the continuous miner must be turned off.
3 Dec 1997	Teralba Colliery, NSW. An ABM20 malfunctioned when number 1 toggle switch on the transmitter was operated. The first occasion the ABM20 was in bolting mode, on attempting to start the pumps the machine went into maintenance mode. On the second occasion the ABM20 was in tram mode, the pumps were started and the toggle switch operated intermittently causing the left track to engage and cause the ABM20 to slew.	• Number 1 toggle switch was damaged causing it to switch on and off intermittently. • The operator did not notice the damaged switch. • The PSA did not operate as this is designed to only work in reverse tram. • Because the intermittent operation of this switch resembled normal switching functions, the watchdog safety circuit did not pick this up.	•
5 Dec 1997	West Wallsend Colliery, NSW. A fitter was performing maintenance work in the front of an ABM20 miner. When the fitter operated the remote control transmitter to start the conveyor in maintenance mode he pressed the wrong	• The fitter had not carried out appropriate isolation procedures.	• No person is to advance past the drilling rigs of any continuous miner unless the power has been isolated and tagged with a personal danger tag for each person in front of the miner.

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
	button and the cutter head rotated and a cutting pick brushed his hard hat.		• A risk assessment is being conducted for this matter.
9 Dec 1997	United Colliery, NSW. Whilst filling a Joy continuous miner with oil the conveyor boom control was activated and the traction motors engaged tramming the machine forward.	• Investigations continuing. • An industry group consisting of manufacturers, users, regulators and unions was formed and the content of a letter to industry was formulated.	• No person shall work beside or in front of a remote controlled continuous miner whilst power is connected, unless a management system has been developed and implemented to prevent employees from being injured by machine movement. • Whilst maintenance and servicing of continuous miners is being carried out and requires access to parts that may move or where inadvertent movement can cause injury then the continuous miner shall be isolated tagged and locked out. • Whilst roof bolting using facilities mounted on a continuous miner, all machine motions other than for roof bolting, that may cause injury by inadvertent movement shall be isolated. • A management system shall be developed and implemented which will prevent more than one radio unit operating a continuous miner. • Any person becoming aware of any unplanned movement of a remote controlled continuous miner operating at the mine, shall cause it to be shut down and the unplanned movement reported to the District Inspector of Coal Mines, the District Check Inspector and the continuous miner manufacturer. • In the event of an unplanned movement of a remote controlled continuous miner operating at the mine, the mine manager shall ensure all similar continuous miners at the mine are immediately shut down.
31 Dec 1997	Tahmoor Colliery, NSW. An ABM20 miner PSA activated for no apparent reason	• Investigations continuing.	•
6/1/98	Metalliferous mine, Condobolin, NSW. An operator received a hairline fracture of the hip when a remote controlled LHD pinned the operator against the rib.	•	•
7/1/98	Newstan Colliery, NSW. The District Inspector was informed of an incident in the recent past where an unintended movement of a Joy continuous miner occured.	• The operator was operating the miner with the remote control transmitter hung around his neck. On bending forward the operator's stomach pushed the select switch and the cutter head switch on the transmitter.	• The mine is purchasing a stainless steel guard manufactured by either Joy or Pempek (the remote system manufacturer) to fit to the transmitter, so as to minimize the risk of inadvertant operation of the

DATE	EVENT	CAUSAL FACTORS/IDENTIFIED ISSUES	RECOMMENDATIONS
		this caused the cutting heads to start.	transmitter switches.
8/1/98	South Bulga Colliery, NSW. A Joy continuous miner moved unexpectadly.	• The miner was switched from bolting mode and the miner moved backwards approximately 6 inches. • It has been known for the traction brake spool valve not to centre and when hydraulic pressure is transferred from the bolting rigs to the traction brake circuit, oil pressure cause the spool valve to centre and the miner to move a short distance.	•
9/1/98	Plutonic Gold Mine, WA. A LHD operator was killed by a remote controlled LHD.	• The deceased was found pinned by the LHD	•
13/1/98	Ulan U/G Mine, NSW. The C/V boom of a Joy continuous miner swung for no apparent reason	•	•

ACCIDENT TYPES

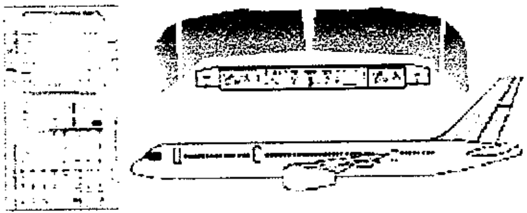
ERGONOMIC/OPERATIONAL ISSUES	**15**									
different from unit/ machine accustomed to		Jan-89	Jul-89	Nov-96						
delayed response time in remote		Jul-89								
attention on local object not machine		Nov-91								
inadvertantly pressed a control		Dec-90	Jan-00	Jan-98						
changing mode remote - manual		Feb-89								
use of remote during maintenance		Apr-95	Nov-97	Dec-97	Dec-97					
poor visibility		Mar-91	Feb-93							
standing in danger zone	9	Jan-89	Jul-89	Jun-90	4 92?	24.2.93?	May-92	Apr-93	Jan-00	Oct-96
unplanned movrment- hydraulic problem	5	May-92	Jan-00	Apr-97	Jan-00	Jan-00				
ELECTRONIC ISSUES	**16**									
low battery voltage		Jun-91								
switch deffective		Feb-89	Dec-91	Feb-93	Jan-00	Dec-97				
Receiver elecronic circuit failure		Jan-92								
electronic component fault		Sep-96								
emergency stop function circuit		Feb-93								
short circuit on send unit		Apr-95	Jan-00	Dec-96						
transmitter problem		Jan-00	Jan-00							
IS interfce incorrectly wired		/95								
Relay drivers dirt and dust		Aug-95								
RADIO CONTROL ISSUES	**4**									
signal from another unit		Feb-92	Jan-00	Jan-00	Jan-00					
SOFTWARE ISSUES	**2**									
microprocessor problem		May-96								
software problem		Sep-96								
No known fault	**8**	Feb-94	May-95	Jun-95	Mar-97	Mar-97	Apr-97	Dec-97	Jan-98	
NOT RELATED TO REMOTE										
Tip over	**4**	Nov-91	8.3,91	13.4.93.	Apr-93					
4 roof falls	**4**									

APPENDIX 2

FLIGHT DECK AUTOMATION ISSUES

http://flightdeck.ie.orst.edu

Meta-Analysis



Flight Deck Automation Issues

Synopsis: This page describes a meta-analysis performed to help summarize, interpret, and make recommendations from the data collected in our Flight Deck Automation Issues study.

Keywords: flight deck, flightdeck, automation, human factors

Last update: 12 Apr 99

Authors: Ken Funk <funkk@engr.orst.edu>, Beth Lyall <Beth.Lyall@ResearchIntegrations.com>, Candy Suroteguh <suroteca@engr.orst.edu>

Introduction

In our study we compiled a large amount of evidence on flight deck automation issues from a large number of sources. In an attempt to interpret this information, we conducted an analysis of this evidence. Because the prefix *meta-* comes from the Greek word meaning *after* and since our analysis came after the analyses reported in our evidence sources, we refer to our analysis as a meta-analysis.

Objectives

The objectives of the meta-analysis were to summarize the evidence collected in Phase 2 to identify those issues that are problems in need of solutions, those issues that do not appear to be problems, and those issues which require more research.

Method

First, we summized all data for each issue:

- **number of citations** -- the number of (possibly unsubstantiated) citations of each issue as a possible problem or concern, as found in Phase 1;
- **supportive evidence** -- the number of instances of evidence supporting the side of the issue suggested by the issue statement;
- **contradictory evidence** -- the number of instances of evidence supporting the side

of the issue opposite that suggested by the issue statement;
- **total evidence** -- the total number of instances of evidence related to the issue, both supportive and contradictory.
- **expert agreement rating** -- the mean agreement rating given to each issue by the experts in our Phase 2 expert survey (that is, the extent to which the experts agreed with the statement suggested by the issue statement);
- **expert criticality rating** -- the mean criticality rating given to each issue by the experts in our Phase 2 expert survey (that is, how critical to safety the experts felt the issue was); and
- **sum of strengths** -- the sum of all evidence strength ratings for the issue (that is, a total "weight" of evidence on both sides of the issue.

Next, we ranked the issues based on four of these criteria:

- number of citations
- expert agreement rating
- expert criticality rating
- sum of strengths

To form a composite ranking, for each issue we summed its ranks for each of these four criteria then produced a "meta-ranking" by sorting the issues in increasing order of this rank sum. To avoid "double-counting" evidence from our expert survey, the sum of strengths values used in this part of the analysis did not include strengths of evidence from the expert survey.

Results

- All Issue Data
- Issues Ranked by Citations
- Issues Ranked by Total Evidence
- Issues Ranked by Expert Agreement
- Issues Ranked by Expert Criticality Ratings
- Issues Ranked by Sum of Strengths
- Issue Ranked by Multiple Criteria (Meta-Ranking)

Discussion and Recommendations

In reviewing these results, the reader should keep in mind several limitations to our overall approach to evidence collection. First, while we attempted to include all published evidence related to flight deck automation issues available at the time of the study, we might have missed some, and there is certainly unpublished evidence of which we are unaware. However, we tried to identify as much evidence as possible to insure that the evidence used in our analyses was as representative as possible of the total population of evidence.

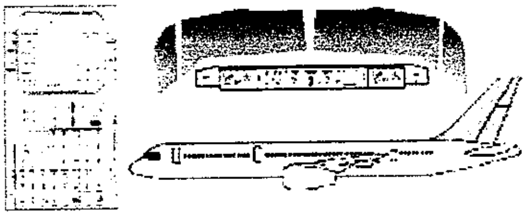
Second, the very nature of some of the issues and the nature of the sources we reviewed to discover evidence may have reduced the opportunity for obtaining contradictory evidence. For example, consider issue095: *Pilots may not be able to tell what mode or state the automation is in, how it is configured, what it is doing, and how it will behave. This may* *lead to reduced situation awareness and errors*. There is plenty of opportunity to produce supportive evidence for this issue by identifying cases (either experimentally or in line operations) where lack of mode awareness led to an incident or accident, and there are instances of this in our database. But producing contradictory evidence is not as easy; one cannot argue that lack of an incident or accident means that mode awareness was perfect. In fact, survey evidence suggests that there are many instances of imperfect mode knowledge that do not result in incidents or accidents. However, even though the opportunity for obtaining evidence is not evenly distributed across the two sides of an issue like issue095, the fact that supportive evidence outweighs contradictory evidence and that some of that supportive evidence comes from accidents gives justification to our findings.

After considering these two caveats, it is still possible to draw some conclusions and recommendations from our findings. We consider those issues with the greatest overall supportive evidence (i.e., the highest-ranked issues in Issues Ranked by Sum of Strengths) and especially those issues ranking highest in multiple criteria (i.e., the highest-ranked issues in Issue Ranked by Multiple Criteria) as problems which require solutions. Scarce resources should not be expended on further efforts to show that they are problems -- the evidence already exists. Now the resources should be applied to developing solutions. In some cases, this will require further research.

For example, consider the issue ranking highest in multiple criteria, issue102: *The attentional demands of pilot-automation interaction may significantly interfere with performance of safety-critical tasks. (e.g., "head-down time", distractions, etc.)*. While some very interesting progress has been made in addressing this issue in the design of alternative flight management system interfaces, we cannot say that we yet adequately understand the human attention allocation process and how various attributes of automation and other flight deck elements affect it. It seems clear that though some partial solutions are currently within reach, broader solutions may require additional research into both interface technologies and human attention.

We believe that the issues with the greatest overall contradictory evidence (i.e., the lowest-ranked issues in Issues Ranked by Sum of Strengths) are not significant problems, and resources would be better used in solving other problems (see above) or further exploring unresolved issues. There is one possible exception to this, issue079: *Automation may increase overall pilot workload, or increase pilot workload at high workload times and reduce pilot workload at low workload times, possibly resulting in excess workload and/or boredom*. This issue ranked eighth in number of citations collected in Phase 1, indicating that there is strong feeling that automation does increase workload in certain flight phases, which poses a safety hazard, yet it ranked ninety-first (next to last) in evidence strength (i.e., second in contradictory evidence) in Phase 2. But this may belie the real problem. Consider issue102, the issue ranking highest in multiple criteria. The underlying problem related to these issues may be not that workload imposed by concurrent tasks is too high (after all, it is usually the case that some tasks can be deferred) but that when faced with many competing tasks, flightcrews are susceptible to attending to the less critical but more salient automation interaction tasks.

Issues Ranked by Multiple Criteria (Meta-Ranking)



Flight Deck Automation Issues

Following is a list of flight deck automation issues, ranked by multiple criteria. The individual rankings are based on those presented in the other tables. However, to form this composite ranking we removed the expert agreement data from the sum of strengths data to avoid double-counting it, so rankings in that column may differ from the ranking based on the complete data.

		rankings					
issue ID	abbreviated issue statement	by citations	by expert agreement	by expert criticality	by sum of strengths	sum of rankings	meta-rank
issue102	automation may demand attention	1	2	10	18	31	1
issue108	automation behavior may be unexpected and unexplained	3	23	18	8	52	2
issue131	pilots may be overconfident in automation	2	32	23	5	62	3
issue025	failure assessment may be difficult	16	6	17	26	65	4
issue083	behavior of automation may not be apparent	7	20	34	6	67	5
issue044	mode transitions may be uncommanded	25	4	11	31	71	6
issue095	mode awareness may be lacking	11	54	3	10	78	7
issue145	mode selection may be incorrect	33	21	13	16	83	8
issue114	situation awareness may be reduced	17	50	6	12	85	9
issue105	understanding of automation may be inadequate	4	57	35	1	97	10
issue100	human-centered design philosophy may be lacking	32	15	12	39	98	11
issue133	training may be inadequate	5	46	45	3	99	12
issue142	crew assignment may be	49	3	20	30	102	13

	inappropriate						
issue150	automation may not work well under unusual conditions	28	33	28	15	104	14
issue106	pilots may over-rely on automation	15	47	39	4	105	15
issue002	pilots may be out of the loop	18	62	5	22	107	16
issue110	database may be erroneous or incomplete	30	8	44	32	114	17
issue065	manual skills may be lost	6	37	64	9	116	18
issue040	automation may be too complex	13	61	37	11	122	19
issue039	interface may be poorly designed	10	51	49	13	123	20
issue089	new tasks and errors may exist	27	11	24	65	127	21
issue070	false alarms may be frequent	24	68	1	38	131	22
issue092	displays (visual and aural) may be poorly designed	9	83	38	2	132	23
		rankings					
issue ID	abbreviated issue statement	by citations	by expert agreement	by expert criticality	by sum of strengths	sum of rankings	meta-rank
issue082	flightdeck automation may be incompatible with ATC system	21	27	41	44	133	24
issue014	information overload may exist	26	13	51	45	135	25
issue121	operational knowledge may be lacking in design process	52	30	31	23	136	26
issue071	data entry errors on keyboards may occur	12	24	65	37	138	27
issue127	commercial incentives may dominate	70	31	7	35	143	28
issue023	failure recovery may be difficult	34	55	2	53	144	29
issue138	standardization may be lacking	20	14	58	52	144	30
issue053	vertical profile visualization may be difficult	66	12	48	19	145	31
issue012	pilots have responsibility but may lack authority	22	76	27	20	145	32
issue005	monitoring requirements may be excessive	31	7	62	46	146	33

issue024	failure modes may be unanticipated by designers	56	5	16	69	146	34
issue126	automation performance may be limited	43	40	26	40	149	35
issue037	controls of automation may be poorly designed	14	85	36	17	152	36
issue026	pilots may be reluctant to assume control	44	41	22	48	155	37
issue112	data entry and programming may be difficult and time consuming	23	34	86	14	157	38
issue075	both pilots' attention simultaneously diverted by programming	46	29	54	29	158	39
issue055	manual operation may be difficult after transition from automated control	45	60	30	28	163	40
issue079	automation may adversely affect pilot workload	8	35	29	92	164	41
issue009	information integration may be required	38	17	68	47	170	42
issue007	manual skills may not be acquired	78	39	4	51	172	43
issue101	automation use philosophy may be lacking	68	10	25	75	178	44
issue063	deficiencies in basic aircraft training may exist	42	58	60	21	181	45
issue140	automation information in manuals may be inadequate	54	28	67	33	182	46
		rankings					
issue ID	abbreviated issue statement	by citations	by expert agreement	by expert criticality	by sum of strengths	sum of rankings	meta-rank
issue011	automation integration may be poor	40	22	66	56	184	47
issue109	automation may lack reasonable functionality	35	25	74	54	188	48
issue022	communication between computers may be unsupervised	65	18	33	73	189	49
issue165	cultural differences may not be considered	91	1	19	85	196	50
issue072	cross checking may be difficult	41	45	47	67	200	51
issue128	complex automation may have overly simplistic interface	61	48	21	71	201	52

issue132	older pilots may be less accepting of automation	37	69	69	27	202	53
issue116	automation may be over-emphasized in pilot evaluation	82	63	15	43	203	54
issue119	information processing load may be increased	71	65	14	60	210	55
issue161	automation use may slow pilot responses	90	16	43	63	212	56
issue099	insufficient information may be displayed	47	84	75	7	213	57
issue129	transitioning between aircraft may increase training requirements	63	9	73	72	217	58
issue015	protections may be lost though pilots continue to rely on them	79	71	32	36	218	59
issue103	automation level decisions may be difficult	62	53	46	59	220	60
issue130	transitioning between aircraft may increase errors	36	52	79	55	222	61
issue107	workarounds may be necessary	50	72	77	25	224	62
issue152	state prediction may be lacking	57	73	53	49	232	63
issue149	similarity may be superficial	86	26	40	82	234	64
issue137	automation skills may be lost	73	59	61	41	234	65
issue117	function allocation may be difficult	83	64	8	80	235	66
issue038	scan pattern may change	80	43	70	42	235	67
issue122	automation may use different control strategies than pilots	69	70	63	34	236	68
issue146	pilots may under-rely on automation	55	78	80	24	237	69
		rankings					
issue ID	abbreviated issue statement	by citations	by expert agreement	by expert criticality	by sum of strengths	sum of rankings	meta-rank
issue104	pilot control authority may be diffused	48	81	55	57	241	70
issue115	testing may be inadequate	51	82	42	68	243	71
issue084	crew coordination problems may occur	19	89	50	87	245	72
issue143	instructor training requirements may be	75	38	56	78	247	73

	inadequate						
issue160	automation requirements may conflict	89	66	9	84	248	74
issue134	software versions may proliferate	84	19	85	61	249	75
issue047	data access may be difficult	59	36	89	70	254	76
issue141	pilots may not be involved in equipment selection	74	44	71	77	266	77
issue144	pilot's role may be changed	39	74	87	66	266	78
issue148	traffic coordination requirements may increase	85	42	59	81	267	79
issue153	non-automated pilot tasks may not be integrated	88	67	57	62	274	80
issue046	pilots may lack confidence in automation	29	80	78	89	276	81
issue087	data presentation may be too abstract	67	56	83	74	280	82
issue136	pilot selection may be more difficult	72	88	52	76	288	83
issue123	inadvertent autopilot disengagement may be too easy	60	90	82	58	290	84
issue151	procedures may assume automation	87	49	72	83	291	85
issue166	company automation policies and procedures may be inappropriate or inadequate	58	79	81	86	304	86
issue158	planning requirements may be increased	77	87	90	50	304	87
issue139	inter-pilot communication may be reduced	64	75	76	90	305	88
issue013	job satisfaction may be reduced	53	86	88	91	318	89
issue049	data re-entry may be required	81	77	91	79	328	90
issue156	fatigue may be induced	76	91	84	88	339	91
issue167	task management may be more difficult	92	92	92	64	340	92