Automation and Robotics in Construction XI
D.A. Chamberlain (Editor)

Hazard Analysis Techniques for Mobile Construction Robots*

Mr D W Seward, Dr D A Bradley, Mr F W Margrave
Department of Engineering, Lancaster University, Lancaster LA1 4YR, UK

ABSTRACT

This paper introduces the problem of safety for mobile construction robots and explains the concept of a "hazard" in safety analysis. The well known Safety Lifecycle Model is described. This model is then expanded to illustrate the hazard analysis process in more detail. The documents required for the hazard and risk analysis are detailed, and three well known hazard analysis techniques reviewed - HAZOP, FMECA and Fault Tree Analysis. The shortfalls of these techniques are described, and a new technique known as Consequence Led Analysis of Safety and Hazards (CLASH) is proposed.

KEYWORDS

Safety, Mobile Robots, Construction Robots, Hazard Analysis

1. INTRODUCTION

Intelligent robots hold out the promise of removing humans from hazardous environments and thereby adding to construction site safety. However such robots require considerable size and power to be effective, and this means that the robots themselves can become a source of danger. This is particularly the case when software intelligence is added to such machines in order to increase their autonomy. Current trends indicate that it is no longer feasible for regulatory bodies to lay down simple rules or regulations that can define "safe behaviour" of such machines. As with other complex systems it has become the responsibility of the developer to prove reasonable safety by developing a "safety argument". Unless this issue is addressed, the introduction of robots to construction sites will be severely impeded.

2. THE PREVENTION OF ACCIDENTS

In recent years a specific vocabulary has been developed to describe safety critical issues. For this reason a glossary of important terms is provided at the end of this paper. A hazard

* This work is part of the Safe-SAM project, which is a joint programme of research between the Departments of Engineering and Computing at Lancaster University. It is sponsored by the DTI/SERC Safety Critical Systems Programme.

can be seen as an intermediate stage which, given corrective action, can be restored to a safe condition, or given inappropriate action, can result in an accident. This is illustrated in figure 1.

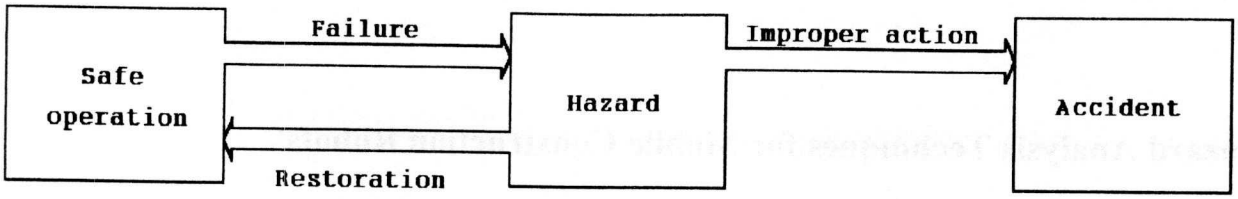

Figure 1. Effect of action on hazard.

It can therefore be stated that the aim of safe system design is to produce a system which has an "acceptable level of risk throughout its life". The question of "what is acceptable?" is a difficult issue for new and innovative systems. Where it is possible to compare a robotic system with an existing manual one, it is believed that the UK Health and Safety Executive would define "acceptable" as "at least as safe as the previous system". However it is recognised that adequate data on existing systems is not widely available. Also there may be social pressures to improve on past safety records.

3. MODELS FOR SAFETY CRITICAL SYSTEM DEVELOPMENT

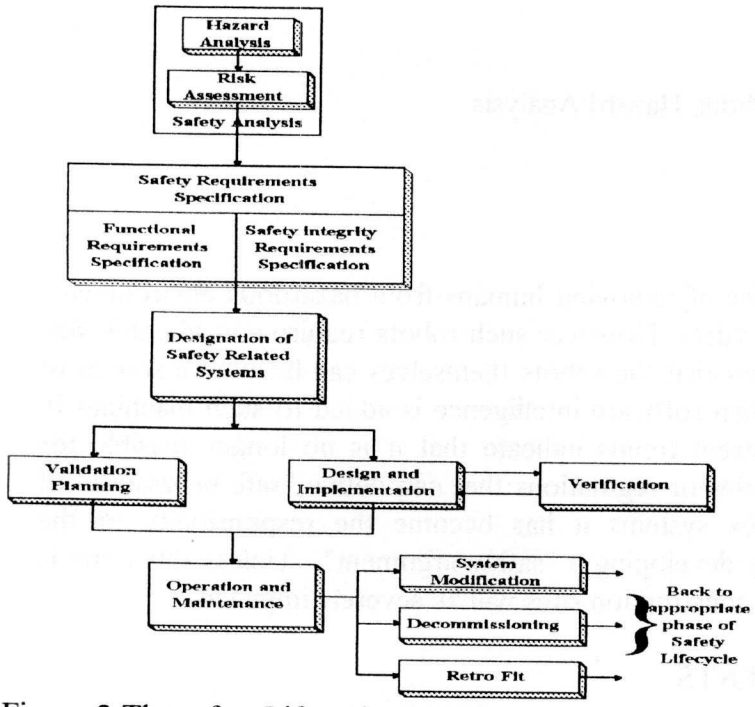

Figure 2 The safety Lifecycle Model

The process of developing safe systems is described in the "Safety Lifecycle Model" [1] and is illustrated in Figure 2. This shows that the first stage of the process consists of a safety analysis that is made up of a **hazard analysis** and a **risk assessment**. This paper is primarily concerned with the techniques available for this first stage of the safety life cycle. As with most complex design problems, it is not possible to define a simple sequence of activities that will yield an acceptable result. It is invariably necessary to go through several iterative loops. Redmill [2] reports the results of European

work to develop a set of guidelines that greatly expands the steps that lead up to the creation of a suitable safe system requirements specification. This is shown in slightly modified form in Figure 3.

4. DOCUMENTS FOR THE SAFETY ARGUMENT

Each of the steps will be briefly considered in relation to construction robots, and a simple example given that is relevant to the LUCIE project - (Lancaster University Computerised Intelligent Excavator)[3]. The starting point is the creation of five documents that contain the necessary data to carry out a safety analysis.

4.1. Robot physical characteristics

This contains such details as the dimensions, power and speed of the proposed robot. Much of this information will be presented in diagrammatic or tabular form.

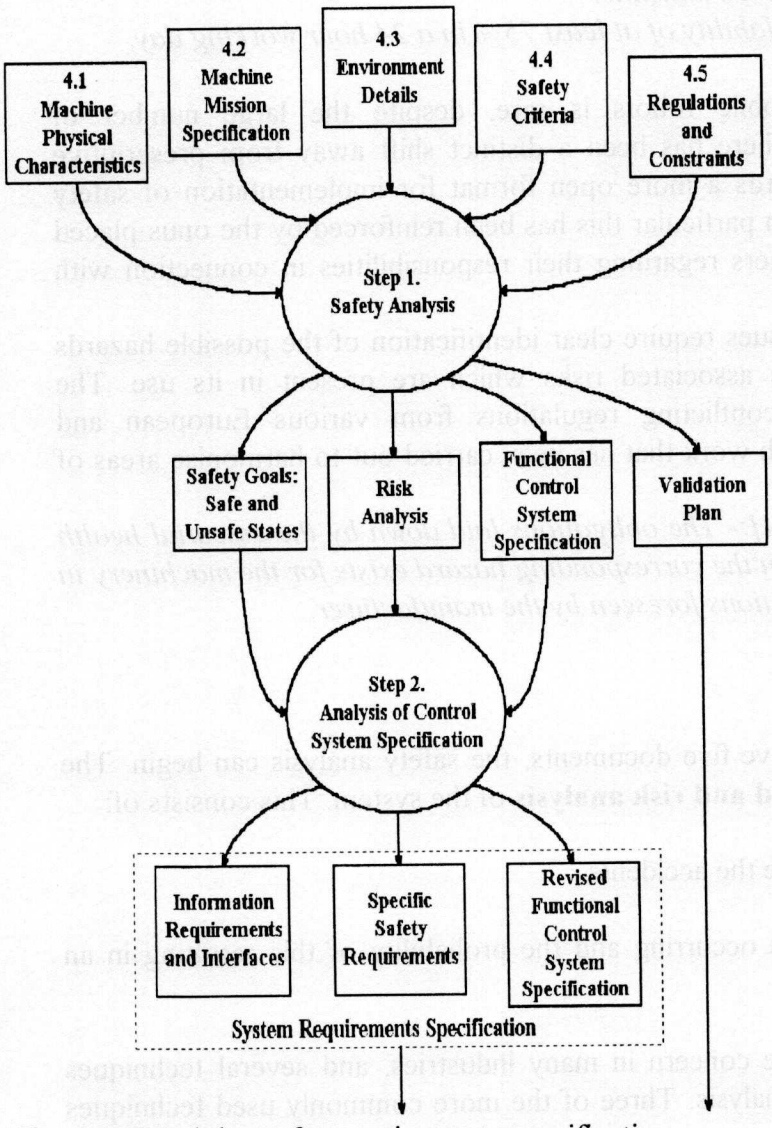

Figure 3 Breakdown for requirements specification

e.g. The excavator slewing mechanism can apply a torque of up to 30 kNm

4.2. Robot mission specification

This describes the range of tasks that the robot must actually perform. It is essentially the robot requirements specification minus the safety considerations. It is likely to be a substantial document and will contain both verbal high level descriptions of activities, as well as much more detailed information such as data-flow diagrams. If the robot is to handle hazardous materials, they must be clearly defined.

e.g. The excavator must deposit excavated material at the side of the trench by slewing the arm and cab.

The excavator may slew through a full 360° at a rate of up to 1.5 radians per second.

4.3. Environment details

A clear description of the working environment and conditions must be provided. This will contain details of such things as temperature ranges and noise

levels. It will also contain information about the proximity of the robot to humans and other objects, particularly objects which can provoke significant secondary hazards such as power cables or pressure vessels.
e.g. The machine operates on a site which has a site boundary fence to prevent access by members of the public, but no physical barrier exists between itself and human workers.

4.4. Safety criteria

This contains the information which will form the basis for decision making concerning safety, reliability and availability.
It includes the required safety performance for the robot in terms of accident probabilities as well as listing requirements for self-test facilities and redundancy.
Figure 3. Breakdown for requirements specification
This data can be both difficult to acquire and have an important influence on the economic viability of the robot.
e.g. The robot must operate in such a manner that it will not cause a higher incidence of accidents than a similar manually operated machine.
The machine must demonstrate an availability of at least 75% in a 24 hour working day.

4.5. Regulations and constraints

Existing legislation concerning mobile robots is rare, despite the large number of organisations developing legislation. There has been a distinct shift away from prescriptive technical structures, and a move towards a more open format for implementation of safety issues throughout the design process. In particular this has been reinforced by the onus placed on designers, manufacturers and suppliers regarding their responsibilities in connection with product liability.

Procedures which relate to safety issues require clear identification of the possible hazards which exist within equipment and the associated risks which are present in its use. The situation is further complicated by conflicting regulations from various European and International organisations, despite much work that has been carried out to harmonise areas of conflict.
e.g. Machinery Directive 91/368/EEC[4]:- The obligations laid down by the essential health and safety requirements apply only when the corresponding hazard exists for the machinery in question when it is used under the conditions foreseen by the manufacturer.

5. SAFETY ANALYSIS

Following the preparation of the above five documents, the safety analysis can begin. The first step is to perform a thorough **hazard and risk analysis** of the system. This consists of:

- Identifying all possible accidents
- Identifying the hazards that can cause the accidents
- Assessing the severity of accidents
- Assessing the probability of hazards occurring and the probability of this resulting in an accident

Safety issues have long been a prime concern in many industries, and several techniques have been developed for use in safety analysis. Three of the more commonly used techniques are:

- Hazard and Operability Studies (HAZOP)
- Failure Mode Effect and Criticality Analysis (FMECA) and Failure Mode Effect Analysis (FMEA)
- Fault Tree Analysis (FTA)

The basic principles of HAZOP analysis are published by The Chemical Industries Association [5], and are well documented in other works [6]. Any single method is insufficient in itself for application to autonomous robots and it is necessary to examine combinations of methods including Failure Mode Effect and Criticality Analysis (FMECA) and Fault Tree Analysis (FTA). It is proposed that the final safety analysis scheme will comprise a combination of all of these techniques to constitute a formal proposal for establishing safety aspects with unconstrained autonomous robots.

Each of these techniques will be briefly reviewed, and it will then be shown how they can be incorporated into the safety analysis for mobile construction robots. A common feature of all the techniques is that they are a group activity, that should be carried out by an experienced team of engineers, software and safety experts, this does however lead to a common failing in that apriori knowledge is required as a basis upon which decisions can be based.

5.1. Hazard and operability analysis

A Hazard and Operability study usually comprises of a team of specialists who systematically question every aspect of every part of a systems and its operation using a set of key "guide-words" *e.g. NO or NOT, MORE or LESS, AS WELL AS, etc.* to establish how deviations from the planned operation may cause hazardous situations. This study may result in several different theoretical deviations from normal operation for each aspect or component studied. Each is considered in turn to establish how it is caused and what consequence it produces, some of the causes may be unrealistic, and some consequences may be rejected as trivial or meaningless. However, some of the deviations with realistic causes and subsequent realistic consequences will be potential hazards, these are noted and examined at a later stage to establish how they may be reduced or preferably eliminated.

The use of this approach will generate many hypothetical situations in a mechanistic manner and the success or failure of the HAZOP study will depend upon four main factors:-

1. The accuracy of data, schematics and engineering drawings upon which the study is based.
2. The technical expertise of the team members.
3. The HAZOP study must only be used as an AID to assess the likely deviations, causes and their consequences.
4. The team must retain a sense of proportion in their examination of the seriousness of hazards identified.

The HAZOP technique is limited in its basic form in that it is more appropriate for use with existing technology and was originally conceived for use with continuous processes within the chemical industry.

5.2 Failure mode effect and criticality analysis

This is an established technique found in many engineering applications and is described in BS5760 [7]. Again expertise of individuals is employed when carrying out Failure Mode Effect and Criticality Analysis (FMECA). This is a bottom-up approach where inductive reasoning is employed to identify levels of criticality and investigate methods of reducing these problems.

Similar methods are used for Failure Mode Effect Analysis (FMEA) but these are not considered separately here. Using FMECA the objective is to determine the features of a product design, or its production and distribution which are critical to various modes of failure. The elements of FMECA are employed in the latter stages of design to perform the following tasks:-

1. Identify individual product or system components.
2. List all possible failure modes of each identified system or component.
3. Determine the probable effect that each mode of failure would have on the overall function of the product or system.
4. Identify all the possible causes of each of the determined failure modes.
5. Assess the failure modes on a numeric scale e.g., 1 to 10, to determine, using experience, reliability data and judgement, values for:
   P - the probability of each failure mode occurring. (1 = low, 10 = high)
   S - the criticality or seriousness of the failure. (1 = low, 10 = high)
   D - the difficulty of detecting the onset of failure. (1 = easy, 10 = very difficult)
6. Calculate the Criticality Rating by determining the product of the 3 categories above, e.g., C = P x S x D, and tabulate all of the findings.
7. Annotate briefly the action required to rectify or reduce the Criticality Index Rating (C).

After this has been completed for all foreseen possibilities the FMECA results can be ranked to establish areas of high criticality which are "Must Improve" areas down to those which are considered "As Low As Reasonably Practical (ALARP)". Once again the problem of human assessment outlined above will dictate the acceptability of the results of FMECA studies and the technique only identifies accidents that arise from failures, not incorrect requirements specifications.

5.3. Fault tree analysis

Fault Tree Analysis (FTA)[8], utilises a top-down or deductive reasoning approach to establish how a chain of events can be traced from a top event. An accident is analysed to discover what failure, event, or combination of these would cause the top event. These events or actions are then linked by a tree structure to the top event using logic AND/OR statements to establish relationships. The OR function indicating that either one event OR another may cause the event above, alternatively the AND function indicating that both the first event AND the second or subsequent event(s) must be present for the link to be established.

FTA is generally recognised as an ideal tool for reliability analysis of complex systems. It provides the engineer with a means of systematically describing logical sequences of events leading to the occurrence of a critical top event and of estimating accurately the corresponding mathematical probabilities associated with the top event. The two phases of Fault Tree Analysis combine a qualitative logical analysis with a quantitative probabilistic technique, the logical analysis is usually achieved in a rigorous manner using Minimum Cut Sets to determine minimal system failure modes to which the latter technique is applied. The major failing of FTA is that the initial identification of accidents is not covered

These three methods of analysis offer a combined approach to the solution of safety and hazard analysis, firstly hazards can be identified and risks reduced (HAZOP). Secondly predicted failures and their subsequent consequences can be assessed for the risk they pose (FMECA) and finally possible outcomes can be traced back to their original causes (FTA).

6. CLASH - A PROPOSED TECHNIQUE

Having established a need for risk and hazard analysis and then shown some of the problems which existing techniques pose for engineers this paper proposes a **Consequence Led Analysis of Safety and Hazards (CLASH)** technique as a basis for future work in this area. Existing analysis methods are employed but are tailored more specifically to this area of machinery by using a combination of techniques and keywords in a structured sequence to establish where risks and hazards exist.

The work currently being undertaken to develop a British Standard for Earth-moving Machinery - Safety[9], provides a useful section in Annex A which can lead the direction of analysis teams. This proposes a list of areas in which hazards may occur and hazards which may be found within each area, and this begins to form the basis of a keyword list upon which to begin hazard and risk identification.

e.g. Mechanical hazards caused by machine and its parts: Crushing, Shearing, Trapping, etc.; Electrical hazards: Electrocution, Arcing, etc.; Noise hazards: Interference with speech, Hearing loss, etc.

If the list of keywords of consequences is thus developed and then these used as guide words the HAZOP technique may then be applied to firstly identify risks, this is then followed by FTA to establish causes of the risks so that design principles may then be applied to reduce these. The use of FMECA is then proposed after several iterations of the above two methods have reduced the number or severity of risks to establish an order of criticality of those which remain. Then further design may be applied so that they are either ALARP or identified and managed by operating instructions, procedures or guarding.

Further work in the SAFE-SAM project is also investigating a second technique, Critical Event Analysis for Safety in Advanced Robotics (CEASAR) which is proposed as a method of in depth investigation into critical events , in particular with operating software and control systems.

7. CONCLUSIONS

There must not be any shortcut methods employed at this stage in the development of products within the Mobile Construction Robot Industry. The development of machines within this field is such a new area that in order to gain acceptance, safety standards must be thoroughly applied in an attempt to address all possible risks and hazards, CLASH attempts to do this by employing existing known techniques along with the ability to demonstrate that legislation and requirements have been addressed throughout the design and production stages.

GLOSSARY OF TERMS

Accident Is an unplanned event which can lead to human death or injury or cause unacceptable damage to the environment.

Hazard Is a non-standard situation which if proper corrective action is not taken can lead to an accident.

Hazard analysis Is the individual detection and characterisation of hazards within machine operations which are deviations from safe operation

Primary hazard Is a hazard which exists as a direct result of the energy contained within the robot itself. *e.g. The excavator arm colliding with a human.*

Risk Is a complex measure of the danger posed by the system as a result of a particular hazard. It is related to the **severity** and **probability** of the hazard and to the likelihood of the hazard causing an accident.

Risk assessment Is the process which is used to identify and apply a numerical rating to an established risk

Safe behaviour Defines behaviour characteristics of the machine which would not result in either direct or secondary damage to humans, plant or equipment, or damage to the operating environment or system within the currently accepted safety practices of the relevant industry, and takes into account current social and cultural factors

Safety argument Is the complete statement which defines the safety requirements of the system

Secondary hazard Is a hazard which can be generated by the robot acting on another object. *e.g. The robot overturns a container of toxic material.*

REFERENCES

1. IEC/TC 65A(Secretariat) 123, May 1992, Draft. Functional safety of electrical/ electronic/ programmable electronic systems: Generic Aspects. Part 1: General Requirements.

2. Redmill, F.J. (Ed), 1989, Dependability of Critical Computer Systems 2, Elsevier Applied Science.

3. D.A.Bradley, D.W.Seward, J.E.Mann and M.R.Goodwin, Artificial intelligence in the control and operation of construction plant - the autonomous robot excavator, *Automation in Construction 2,* Elsevier Science Publishers, (1993) pp 217-228

4. DTI, October 1991, The single market, Machinery, Machinery Directive 89/392/EEC as amended by Directive 91/368/EEC.

5. The Chemical Industries Association, 1977, HAZARD and Operability Studies.

6. Coulson, & Richardson, Chemical Engineering, Vol. 6, Safety and Loss Prevention,

7. BS5760: Part 5: 1991, Reliability of systems, equipment and components: Guide to failure mode effect and criticality analysis (FMECA and FMEA)

8. IEC 1025, (1990) Fault Tree Analysis

9. BS prEN474-1, Draft, Earth-moving Machinery - Safety: Part 1: General requirements