Automation and Robotics in Construction X
G.H. Watson, R.L. Tucker and J.K. Walters (Editors)

SAFETY CRITICAL SYSTEMS FOR ROBOT EXCAVATION

LiLi Zhang, D.A. Bradley, D.W Seward

Engineering Department, Lancaster University, Lancaster LA1 4YR, U.K.
United Kingdom

Abstract

A number of mathematical and analytical tools are available to assist in risk assessment for industrial and other robots. This paper is concerned with the use of a hazard and operability study (HAZOP) methodology to analyse the range of hazardous conditions and to assess the degree of risk associated with construction robots. In this context, the paper sets out to identify the various hazard conditions that occur in relation to the sequence of operations of an automated and robotic excavator and to provide an assessment of the levels of the risks that result in accordance with a classification of the working volume of the excavator.

1. INTRODUCTION

The deployment of robots to carry out a range of operations once performed by humans such as may be associated with firefighting, space systems, nuclear inspection, maintenance and decommissioning and construction affords the opportunity to remove humans from a hazardous environment. However, construction robots themselves are a source of potential hazard and risk which could result in death or injury, for instance as a result of collisions with site personnel or site structures. In order to ensure that the dangers inherent to the deployment and use of construction robots does not offset their usefulness, they must be accompanied by appropriate safety related systems to guarantee their operation is accompanied by an acceptable level of risk. This, in turn, requires that the operation of the safety system must be fully understood and analysed as part of the design process of any automated and robotic system.

The development and deployment of automation and robotic plant in the construction industry has been slow compared to other industries. A variety of factors contribute to this slow transfer including the highly variable operation environments. In order to ensure effective and safe operation, construction robots have to be highly adaptive, responding rapidly to changes in their local and overall environment in relation to their operation and capable of making a series of linked strategic and tactical decisions about their actions. An AI based control system for automated and robotic excavation has been implemented by the Lancaster University Computerised Intelligent Excavator (LUCIE) project [1]. LUCIE is capable of autonomously digging a trench to a controlled depth in a variety of ground types and conditions. Safety systems for this automated and robotic excavator are now being studied.

To date, there have been developed a number of International Standards on the safety considerations for the design, construction, programming, operation, use, repair and maintenance of industrial robots [2]. The International Standard "Manipulating Industrial Robots---Safety" [3] was established in spring 1992. The International Electrotechnical

Commission document "Functional Safety of Programmable Electronic Systems" [4] and presents the hazard analysis, risk assessment and safety integrity requirements associated with this standard.

A number of mathematical and analytical tools are also available to assist in risk assessment for industrial robots including "Guidelines for Hazard Evaluation Procedures" produced by the Battelle Columbus Division [5]. The work presented in the current paper is concerned with using a hazard and operability study (HAZOP) method to analyse hazardous conditions and to assess the level of risk for automatic and robotic construction machinery with particular reference to excavation. In this context, the paper identifies various hazardous situations in relation to the sequence of operations of a robotic excavator and assesses the level of the associated risks in accordance with a classification of the working volume. With regard to the analysis of the possible range of hazard situations, the safety requirements can be obtained. Finally, safety strategies, which minimize the risks to an acceptable level, are considered.

Operational and control software in construction robots can also be a source of danger when it malfunctions. Obviously, software on its own cannot pose a threat to anyone, but some hardware failures may be the ultimate result of software malfunction. Safety-critical software is however the subject of a parallel study and is not covered in this paper.

2. FUNCTION AND STATE OF AUTOMATED AND ROBOTIC EXCAVATOR IN OPERATION

The analysis of safety requirements must be on the basis of overall operational requirement. It is, therefore, necessary that the operating modes of an automated and robotic excavator and its operating procedure are properly understood.

In operation, an automated and robotic excavator has essentially two operating modes, namely static and dynamic. Static mode implies that the base is held in a fixed position while the digging task is being carried out while the dynamic mode is associated with the movement of the excavator within working area.

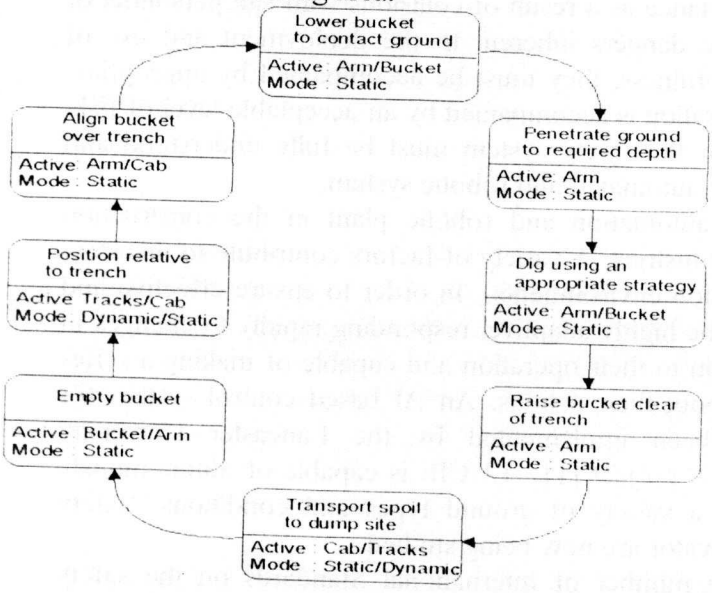

Figure 1 : An operational cycle for an excavator

When digging, the automated and robotic excavator is in static mode and the main active components are the bucket and arm of the excavator. The primary sources of hazards in this mode are collisions between arm or bucket of excavator and site personnel or site structures. When moving, the automated and robotic excavator is in dynamic mode. The highest level of risk is again associated with collision with site personnel or site structures. For spoil transport, the automated and robotic excavator can be either static or dynamic mode. Figure 1 sets out the main sequence of the operations and the corresponding modes of operation associated with the digging of a trench.

3. SAFETY REQUIREMENTS AND ANALYSIS OF OPERATION

The automated and robotic excavator is structurally essentially the same as a manually controlled excavator, working in an unstructured environment. However, its automated operating mode means that the excavator control system can itself define and implement operation in accordance with a specified task structure. As such, it has an enormous potential for initiating hazardous actions.

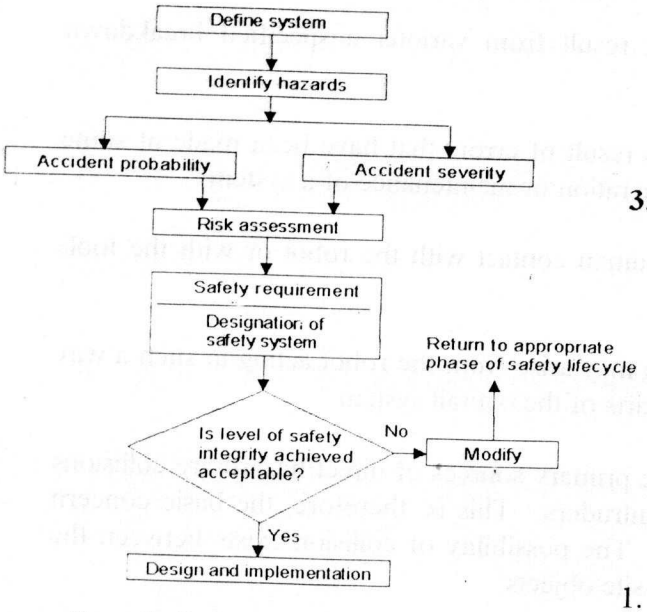

Figure 2 : Basic safety lifecycle model

3.1 The safety lifecycle of automated and robotic excavator

A safety lifecycle study provides a framework for the management of a safety system. The methods of development for safety systems must be fitted into this framework. Figure 2 presents a basic safety lifecycle model for an automated and robotic excavator.

The safety lifecycle may also be expressed as follows:

1. Define the required tasks for the foreseeable applications.
2. Identify the sources of hazard associated with any particular operation.
3. Evaluate and assess the associated risks.
4. Consider the safety strategies necessary to minimize the risks by reducing them to an acceptable level.
5. Assess the levels of safety integrity achieved for the system and ensure that these levels are acceptable.
6. If the safety integrity level achieved is not acceptable then repeat the appropriate steps.
7. If the safety integrity level achieved is lower than assessed tolerable risk level, design and implementation shall be carried out.

A number of analytical techniques can assist in the identification and structuring possible events leading to hazardous situations including:

- Fault Tree Analysis (FTA);
- Failure Modes, Effect and Criticality Analysis (FMECA);
- Hazard and Operability (HAZOP) Studies;
- Relative Ranking Techniques (DOW and MOND hazard indices)
- Preliminary hazard analysis;
- "What if" analysis [6].

The procedure associated with a 'Hazard and Operability (HAZOP)' study is specifically designed to identify any hazards and operability problems associated with the process. The possible deviations and their corresponding cause and consequences in relation to the execution of the process can then be analysed.

3.2 Preliminary hazard analysis

The definition of a hazard is a situation in which there is actual or potential harm to human life or limb, or to the environment. [7] These hazards and failures can be classified in one instance as, "Random Hardware Failure" or "Systematic Failures", [8] and in another as, "Direct Hazard" or "Indirect Hazard" [2]. In particular:

Random hardware failures are - "Those which result from various unspecified breakdown mechanisms that occur at unpredictable times."

Systematic failures are - Those which occur as a result of errors that have been made at some stage in the specification, design, construction, operation or maintenance of a system."

Direct hazards are - "Those which arise from human contact with the robot or with the tools and objects which it handles."

Indirect or secondary hazrads are - "Those which may arise from the robot acting in such a way that it is the cause of hazardous events in other parts of the overall system."

For the automated and robotic excavator, the primary sources of direct hazard are collisions with objects in the working volume, including intruders. This is, therefore, the basic concern for the design of the associated safety systems. The possibility of collision exists between the excavator and the following types and classes of site objects:

- Persons — Operator, other site personnel.
- Vehicles — Site vehicles such as dumpers, lorries and cranes.
- Site structures temporary — Buildings, pipes, columns, supports, scaffolding and associated structures.
- Site excavations — Trenches and holes.
- Site storage — Stocks of bricks, steel, and other material left on site.
- Site debris — General site debris, such as spoil heaps.

3.3 Hazard and Operability analysis

Unlike many conventional automated machines the spatial envelope within which the excavator can act is not immediately obvious to the casual observer. Hazardous situations can arise not only in the immediate locality of the automated excavator but also in a large surrounding volume. The different regions within this workspace then give rise to differing hazard conditions. To eliminate the main direct hazards, the classification of zones or levels of protection around the excavator should be considered. The definitions of the zones in the Figure 3 refer to those given in ISO 10218: 1992 "Industrial robots" [2], "Fault- Tree Analysis of Hazards Created by Robots" [9] and "A Robot Safety and Collision Avoidance Controller" [10].

Zone 1 — Maximum danger zone. A small volume surrounding the excavator arm.

Zone 2 — Restricted zone. The area bounded by the maximum reach of the automated and robotic excavator when stationary.

Zone 3 Dynamic danger zone. The region is outside the maximum reach of the automated and robotic excavator but within the emergency stop range.

Zone 4 Safety zone. The region within the working area of the excavator but outside the emergency stop range of the moving excavator.

Zone 5 Maximum detection zone. The region within the working area of the excavator but outside the minimum manoeuvring distance of the moving excavator.

Zone 6 Maximum working perimeter of the excavator.

As indicated, Zone 1 is a small volume surrounding the arm of the automated and robotic excavator. The arm and bucket perform their actions within this volume during a trenching operation. If the arm of the excavator impacts with obstacles in this zone, then severe damage is likely to be unavoidable. Maximum direct hazards will therefore occur in this zone. However, for the purpose of digging, impact with ground is also necessary and, as such, is not a hazard. Sometimes the surface of the ground is uneven and this unevenness must not be interpreted as obstacles. Thus the automated and robotic excavator must be able to distinguish likely hazards from necessary ground impact associated with the digging process.

The highest level of risk is associated with Zone 1. Collision between the excavator arm and site personnel or site structures could result in the death of site personnel and/or severe damage to site structures and possibly to the excavator.

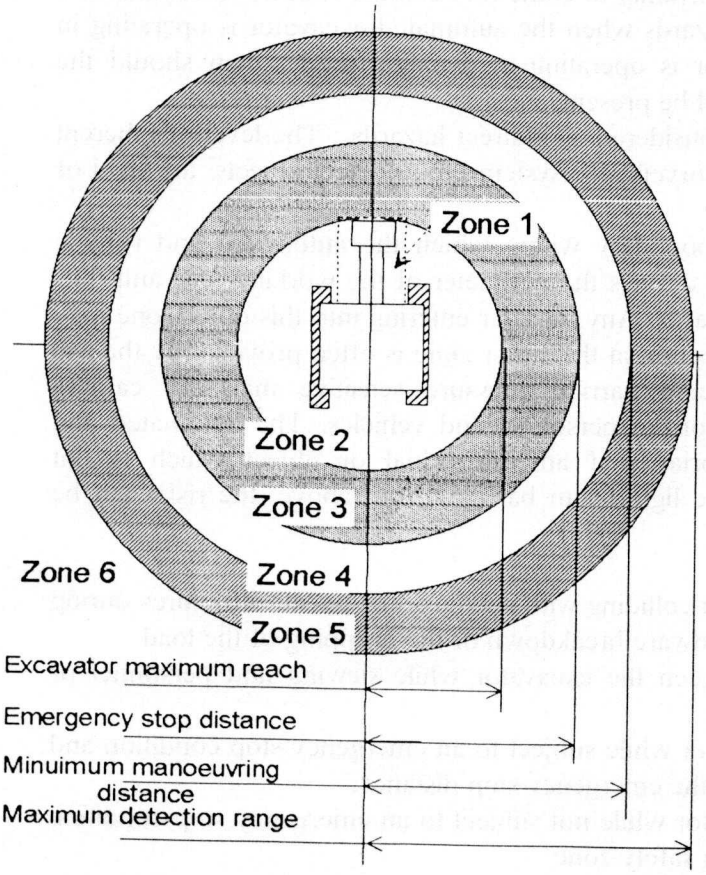

Figure 3 : The layout of the safety zones for an automated and robotic excavator

Zone 2 is a restricted zone relative to the excavator. It surrounds the excavator with the maximum reach of the excavator as its boundary. As for zone 1, any objects within this zone can be subject to a maximum hazard situation. Zone 2 therefore also encompasses the highest level of risk and hence should be kept clear of personnel and all fixed objects in the zone properly located and identified prior to operation. The risk evaluation in Zone 2 is therefore the same as that for Zone 1.

Zone 3 covers the volume outside the maximum reach of the excavator but inside the emergency stop distance of the moving excavator. Zone 4 is located between the emergency stop distance and the minimum manoeuvring distance of the excavator. Normally, there is no direct hazard situation associated with these zones when the excavator is operating in static mode. However, if the load was

accidentally ejected from the bucket as a result of some action this could constitute a risk for any personnel or structures in these zone. When obstacles are themselves dynamic, they may progress from Zones 3 and 4 to Zone 2 in a relatively short time and this could result in a maximum risk condition if the surveillance system fails to detect their presence.

When the automatic and robotic excavator is operating in dynamic mode, the distance between the obstacles in Zone 3 and the excavator is always less than emergency stop distance of the dynamic excavator. Even if the excavator is subject to an emergency stop condition, collision is still unavoidable. Therefore, any object that exists in Zone 3 constitutes a direct hazard when the excavator is operating in dynamic mode.

For obstacles in Zone 4, if the automated and robotic excavator is operating in dynamic mode, or obstacles are themselves moving, then collision can be avoided by an emergency stop. Although the excavator can be subject to a stop condition for any object or personnel in Zone 4, the reliability of the surveillance system must be high otherwise the possibility of collision increases. A limit on the performance of the surveillance system is therefore set by the maximum relative velocity of any object within zone 4 as this dictates the time available for detection.

Zone 5 defines the maximum detection range of the system sensors. Using an appropriate strategy excavator can manoeuvre to avoid collision with any static object detected this outer zone. Static objects which exist in this zone, for instance a buildings, piles of bricks or site material, do not of themselves have the opportunity to come into contact with the excavator and cannot therefore be considered as direct hazards when the automated excavator is operating in static mode. However, when the excavator is operating in dynamic mode, then should the surveillance provision fail, direct hazards will be present.

Hazards in Zone 5 may in general be considered as indirect hazards. The level of inherent risk is therefore low. However, should the surveillance system fail to detect objects, the level of risk associated with this zone will increase.

Zone 6 defines a maximum working boundary within which the automated and robotic excavator is allowed to operate. As such, it defines the perimeter of the working area and thus presents the first line of defence against hazards. Any intruder entering into this outer zone may give rise to a possible hazard situation. Protection at this outer zone is often provided by the use of wire fencing, a light or infra-red beam barrier, pressure sensitive mats, or camera surveillance, to detect the entry of unauthorised personnel and vehicles. The automated and robotic excavator should respond appropriately if any individual or object which is not registered enters via the gate or crosses the light-beam barrier. From above, the risks can be summarized as follows:

- Risks resulting from the arm or bucket colliding with personnel or on-site structures during controlled motion or as a result of hardware breakdown or the dropping of the load.
- Risks resulting from a collision between the excavator while slewing and personnel or dynamic obstacles.
- Risks of collision between the excavator while subject to an emergency stop condition and obstacles that exist or move to within the emergency stop distance.
- Risks of collision between the excavator while not subject to an emergency stop condition and personnel or dynamic obstacles in safety zone.
- Risks of collision between the excavator while manoeuvring and personnel or dynamic obstacles within the maximum detection zone.

The designation, construction, and implementation of the safety systems should consider the operational characteristics of the excavator and all possible hazards. There are two fundamental principles for the selection and designation of the appropriate safety related system:

- The exclusion of personnel from the safeguarded space during automatic operation.
- The elimination of hazards or at least their reduction by detecting possible onset as early as possible.

For Zone 6, the selected safety system should be able to detect the entry of unauthorized personnel or vehicles to the safeguarded space. Methods used could be a mechanical guard such as a perimeter fence or barrier which completely encloses the operation space or an optical or photoelectric "curtain" guard comprising a series of transmitters and detectors, activated when a beam is intercepted. In terms of the cost of the equipment, the mechanical perimeter guard is likely to be cheaper. However, the guard must be readily movable as the operating volume of the excavator is continually changing.

For Zone 5, the main aim of the safety system is to detect objects entering the zone and to determine their precise positional and dimensional data so that the control system can modify its strategy in order to avoid collision. Because of this, a laser rangefinder installed on the top of the excavator is suggested as a possible safety-related sensor to guard Zone 5. Its rotation period and associated processing time must be less than the shortest anticipated time required for a dynamic object to move through this zone.

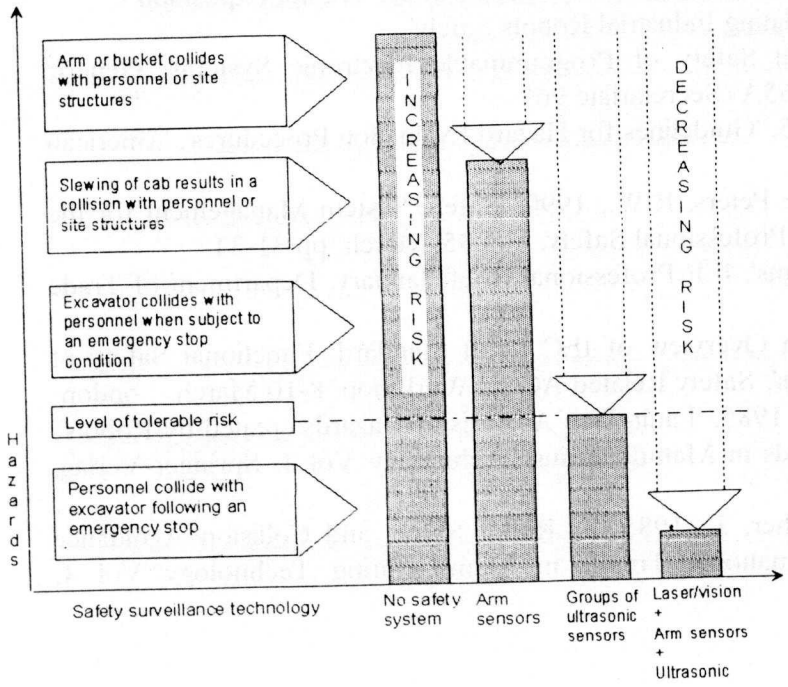

Figure 4 : Risk reduction with improvements in sensor technology and fit

For Zones 4, 3 and 2, the primary characteristic of the safety system is the detection of obstacles as early as possible. Their position and dimension are not necessary of major concern, but it must be known accurately whether an obstacle exists. Referring to the safety system requirements, a group of ultrasonic sensors installed around the cab of the excavator is suggested as a possible means of accomplishing this task. As infrared sensors are sensitive to the human body these could also be utilised for the detection of personnel.

The safety system is intended to ensure that the risks which exist in the operating environment are kept as low as possible, and certainly lower than the assessed tolerable risk. The safety integrity measure is intended to assess the degree of reduction of risks and to ensure that adequate precautions are taken against all possible hazards. Figure 4 shows the effect in reducing the level of risk after the adoption of the safety-related functions.

4 CONCLUSIONS

With the help of the Hazard and Operability Analysis method, we have presented a preliminary analysis of the safety requirements for an automated and robotic excavator. An initial prototype safety system for automated and robotic excavator has been proposed. However, to achieve implementation of the proposed the safety system, further work on the relevant criteria and integrity levels necessary for a more detailed assessment of risk are required. In conjunction with the design and implementation process safety verification and validation for the safety system as designed must be carried out.

It is, therefore, suggested that what is required is an Artificial Intelligent system for capable of simulating the operation of the safety system in order to verification and validation a proposed safety system. By answering various "what-if" questions the simulation process can quantitatively analysis possible deviations from expected behaviour. The results of simulation could then used to determine all possible states of the safety system to help to find and identify the potential hazards.

REFERENCES

1 Seward, D.W., Bradley, D.A., Mann, J. & Goodwin, M., 1992, 'Controlling an Intelligent Excavator for Autonomous Digging in Difficult Ground', 9th ISARC, Tokyo, Japan, Vol 2, pp 743-750

2 Schofield, M., 1992, 'Safety and Standards for Advanced Robots: A First Exposition'

3 ISO 10218, (BS 7228), 'Manipulating Industrial Robots Safely'

4 IEC Draft Standard, 'Functional Safety of Programmable Electronic Systems: Generic Aspects; Part 1', IEC Reference 65A (Secretariate 96)

5 Battelle Columbus Division, 1985, 'Guidelines for Hazard Evaluation Procedures', American Institute of Chemical Engineers

6 Kavianian, H.R., Wentz, C.A. & Peters, R.W., 1990, 'Safety System Management for the Design of Hazardous Processes', Professional Safety, Vol 35, March, pp 31-34

7 IEE, 1992, 'Safety Related Systems', IEE Professional Brief, January, Department of Trade and Industry

8 Bell, R. & Smith, S., 1990, 'An Overview of IEC Draft Standard: Functional Safety of Programmable Electronic Systems', Safety Related ACOS Workshop, 8-10 March, London

9 Sugimoto, N. & Kawaguchi, K., 1985, 'Fault-Tree Analysis of Hazards created by Robots', Robot Safety, International Trends in Manufacturing Technology Vol 4, Springer-Verlag, pp 83-98

10 Derby, S., Graham, J. & Meagher, J., 1985, 'A Robot Safety and Collision Avoidance Controller', Robot Safety, International Trends in Manufacturing Technology Vol 4, Springer-Verlag, pp 237-246