The Safety Assessment of Human-robot Systems*
(2nd Report, Logic Models for the Analysis of the Accident-
causing Mechanisms---Part 1)

By Yoshinobu SATO** Koichi INOUE*** Hiromitsu KUMAMOTO†

This paper first develops Boolean logic models to represent accident-causing mechanisms where a robot body or arm strikes a human. The models can be used as a checklist to uncover various oversights which could pose hazards in human-robot systems. The necessity of dividing the system into phases to assure statistical independence among the basic events is emphasized, and examples of the system phase division are demonstrated. Minimal cut sets of the logic models in the typical system phases are then extracted to obtain the main system failure modes.

Key Words: Safety Engineering, Safety Assessment, Robot, Human-robot Systems, Hazard Analysis, Logic Model, System Phase, Minimal Cut Set

1. Introduction

In spite of the fact that some workers are inadvertently killed or injured by industrial robots, we are obliged to use them to increase productivity, even though we have not yet overcome such risks sufficiently. Nevertheless, the robot will be developed and utilized not only for the industrial sector, but also our daily life. In this context the safety of robots will become more important with greater social interest in the near future.

The purpose of this paper is to improve the safety of robot systems, ranging from their design to use. In the previous paper⁽¹⁾, a general technique to identify the hazards that can be posed in human-robot systems was discussed. The next step in the safety assessment is to analyze the logic of hazard-generating mechanisms. In general, such analysis is made of given concrete systems. On the other hand, the function to check the oversight in any implemented analysis is very important. Such function will be given by investigating, so to speak, comprehensive logic models made by assuming all cases of hazard-generating mechanisms. MORT⁽²⁾, for example, can be mentioned as a comprehensive logic model; but this, which is intended to check management oversights covering a wide range, can

not be applied to our aim. Another model for human-robot systems can be mentioned⁽³⁾, but this is limited to existing industrial robot systems.

In this paper, we will develop comprehensive logic models for the analysis of the accident-causing mechanisms (hereinafter referred to as logic models) which can also be applied to future robot systems. And we will examine the necessary condition for the next step in safety assessment, or quantitative analysis, and extract the minimal cuts of the logic models.

2. Description Style and Top Events of Logic Models

We describe the logic models with the symbols of fault-tree.^(4,5) The top events of the logic models represent the occurrence of accidents resulting in injury or death caused by hazards of robot to human.

Many types of hazards and injury accidents were identified in the previous paper. One of the hazards, the potential for occurrence of kinetic-energy transmission from robot to human, constituting an action chain of type 1, will cause the accident in which a human is struck by a robot.

The generalized top event "struck by robot" (E: the event identification code in Fig.1, and so forth) is divided into the following sub-top events: "struck by turnover of robot" (Ea01), "struck by fall of robot" (Ea02), "struck by moving body of robot" (Ea03), "struck by moving arm of robot" (Ea04) and "struck by moving object handled by robot" (Ea05). The subjects in this paper are sub-top events Ea03 and Ea04.

3. The Logic Model of Sub-top Event "Struck by Moving Body of

* Received December 14, 1984.

** Senior Research Official, The Research Institute of Industrial Safety, Ministry of Labor (5-35-1, Shiba, Minato-ku, Tokyo, 108 JAPAN)

*** Professor, Dept. of Aeronautical Engineering, Kyoto Univ. (Kyoto, 606 JAPAN)

† Research Associate, Dept. of Precision Mechanics, Kyoto Univ.

Robot"(Ea03 in Fig.1)

The event "struck by moving body" (Ea03) occurs when the events, "robot moves"(Eb07), "barriers to prevent the transmission of kinetic energy from robot to human are less than adequate(LTA)" (Eb08) and "human is in hazardous zone where he is exposed to the action"(Eb09) occur simultaneously. Moreover, the occurrence of injury depends on the condition "velocity and power of the movement"(Condition No.1).

3.1 "Robot moves"(Eb07)

This event is subdivided into "heteronomous movement caused by action of external force"(Ec05) and "autonomous movement caused by power source of robot itself"(Ec06) with a sorting OR gate.

The terms "sorting AND gate" and "sorting OR gate" shall be used to avoid the repetition of partial trees below the gate, each one of which can be similarly expressed because the trees are generalized and abstracted. Therefore outputs to the gate shall be generated at the parts sorted out from both upper sides of the gate and transfer triangles according to the practical meaning of the input to the gate, even though generalized logic expressions of inputs are equal.

3.1.1 "Heteronomous movement"(Ec05)

This event occurs when the two events "robot or backup system fails to stabilize kinetically the robot body"(Ed03) and "action of external force"(Ed04) occur simultaneously. The possible combination of each mode of the events "fail to stabilize" and "external force", however, depend on the condition "magnitude of external force"(Condition No.2).

a. "Fail to stabilize"(Ed03)

This event occurs under either one of the two robot states, "not automatically controlled"(Ee04) or "automatically controlled"(Ee05).

a-i "Not automatically controlled" (Ee04)

Event Ed03 occurs under not automatically controlled state of robot when the two events "unstable support of backup system"(Ef06) and "robot and backup system fail to fix robot body when external force acts"(Ef07) occur simultaneously.

a-ii "Automatically controlled"(Ee05)

Event Ed03 occurs under "automatically controlled" state of robot when any one of the events "overload on robot"(Ef08), "unstable support of device"(Ef09), "lack of utility"(Ef10), "generation of wrong command in control system"(Ef11) or "breakdown of mechanism to control robot"(Ef12) occurs; and, moreover, occurs even under the condition "normally controlled condition"(Ef13) according as the magnitude of the external force. Event Ef11 connects to the transfer triangle No.29 i.e. the sorting OR gate below event Ee17 in Fig.2.

b. "Action of external force"(Ed04)

This event is subdivided into "force of collision"(Ee06), "force of gravity"

(Ee07), "shaken artificially"(Ee08) and "earthquake shocks"(Ee09), with a sorting OR gate.

3.1.2 "Autonomous movement"(Ec06)

Autonomous movement occurs on either one of two types of passages—"on normal passage"(Ed05) and "on abnormal passage"(Ed06).

a. "On normal passage"(Ed05)

This connects to triangle No.28 below event Ec08 in Fig.2.

b. "On abnormal passage"(Ed06)

Event Ec06 occurs on abnormal passage when the four events "failure of guidance system"(Ee10), "interlocking to detect deviation from normal passage and to stop movement is LTA"(Ee11), "guard to prevent deviation is LTA"(Ee12) and "existence of power source to drive"(Ee13) occur simultaneously. Event Ee11 and Ee12 connect to triangle No.30 below event Ed10 in Fig.2 and triangle No.21 below event 0 in Fig.1 respectively.

b-i "Failure of guidance system" (Ee10)

This event happens when either one of the two events "generation of wrong command in control system"(Ef14) or "breakdown of guidance system"(Ef15) occurs. Event Ef14 connects to triangle No.29 below event Ee17 in Fig.2.

3.2 "Barrier LTA"(Eb08)

Barrier, here, means the function to prevent or to absorb the transmission of energy that could cause injuries, on robot or human, or between robot and human. This event connects to triangle No.21 below event 0 in Fig.1. Event 0 occurs when any one of the events "technically impossible to prevent"(Oa01), "possible but not provided"(Oa02), "provided but does not function effectively because of fault or in defect of performance"(Oa03), "provided but human turns it ineffective"(Oa04), or "provided but human does not fit it for use"(Oa05) occurs.

3.3 "Human in hazardous zone"(Eb09)

This event connects to triangle No.22 below event N in Fig.3.

4. The Logic Model of Sub-top Event "Struck by Moving Arm of Robot" (Ea04 in Fig.2)

Event Ea04 occurs when the three events "movement of arm"(Eb10), "barrier LTA"(Eb11) and "human in hazardous zone"(Eb12) occur simultaneously. Moreover, the occurrence of injury depends on the condition "movement power and velocity of arm"(Condition No.3).

4.1 "Movement of arm"(Eb10)

This event is subdivided into "arm moves together with body"(Ec09) and "arm moves independently of movement of body" which is further subdivided into "heteronomous movement"(Ec07) and "autonomous movement"(Ec08) with a sorting OR gate.

4.1.1 "Heteronomous movement"(Ec07)

This event occurs when the two events

"fail to stabilize arm"(Ed07) and "action of external force"(Ed08) occur simultaneously. The possible combinations of each mode of events Ed07 and Ed08, however, depend on the condition "magnitude of the external forces"(Condition No.4).

a. "Fail to stabilize"(Ed07)

This occurs under either one of the arm states "not automatically controlled"(Eel4) or "automatically controlled"(Eel5).

a-i "Not automatically controlled"(Eel4)

This connects to triangle No.49 below event Ee04 in Fig.1.

a-ii "Automatically controlled"(Eel5)

Event Ed07 occurs under "automatically controlled" state of arm when any one of the events "breakdown of mechanism"(Ef16), "overload"(Ef17), "lack of utility such as energy or information"(Ef18), or "wrong commands generated in the control systems"(Ef19) occurs; and, moreover, occurs even under the condition — "normal condition"(Ef20) according as the magnitude of the external force. Event Ef19 connects to triangle No.29 below Eel7 in Fig.2.

b. "Action of external force"(Ed08)

This event connects to triangle No.41 below event Ed04 in Fig.1.

4.1.2 "Autonomous movement"(Ec08)

This event occurs when the three events "command to move arm is generated in control system"(Ed09), "fail to interlock movement"(Ed10) and "power source to drive arm is live"(Ed11) occur simultaneously.

a. "Command to move"(Ed09)

This event is subdivided into "commands to be intended"(Eel6) and "commands not to be intended"(Eel7) from the aspect of arm control with an OR gate.

a-i "Command to be intended"(Eel6)

This event happens when either one of the two events "start of program to move arm"(Ef21) or "cancellation of halt condition"(Ef22) occurs.

a-ii "Command not to be intended"(Eel7)

This event happens when any one of the events "failure of automatic control"(Ef23), "program LTA"(Ef24), "failure of program choice"(Ef25) or "human fails to manipulate"(Ef26) occurs.

a-iii-i "Failure of automatic control"(Ef23)

This event occurs when any one of the events "malfunction of servomechanism"(Eg05), "malfunctions of electric circuit"(Eg06), "outbreak of faulty signal"(Eg07) or "breakdown of mechanism other than servomechanism or electric circuit"(Eg08) occurs.

(i) "Malfunction of servomechanism"(Eg05)

This event happens when any of such events as "contamination of oil"(Eh01), "trouble of servovalve"(Eh02) or "lack of utility"(Eh03) occurs.

(ii) "Malfunction of electric circuit"(Eg06)

This event happens when any of such

events as "disconnection of circuit"(Eh04), "short circuit"(Eh05) or "deterioration of electric part such as I.C. element"(Eh06) occurs.

(iii) "Outbreak of faulty signal"(Eg07)

This event happens when any of such events as "discharge of electricity"(Eh07), "momentary power cut"(Eh08), "outbreak of internal noise"(Eh09), "outbreak of external noise"(Eh10), "fault of internal sensor"(Eh11), "fault of external sensor"(Eh12), "outbreak of wrong signal from peripheral equipment"(Eh13) or "program readout error"(Eh14) occurs.

b. "Fail to interlock"(Ed10)

This event happens when any of such events as "fail to sense human being in dangerous zone"(Eel8), "failed operation of interlock device"(Eel9), "human turns interlock device ineffective"(Ee20) or "interlock mechanism is not provided"(Ee21) occurs.

4.1.3 "Arm moves together with body"(Ec09)

This event connects to triangle No.54 in Fig.3, and occurs when the two events "robot moves"(Ed12) and "arm connected with body"(Ed13) occur simultaneously. Event Ed12 connects to triangle No.23 below event Eb07 in Fig.1.

4.2 "Barrier LTA"(Eb11)

This event connects to triangle No.21 below event O in Fig.1.

4.3 "Human in hazardous zone"(Eb12)

This event connects to triangle No.22 below event N in Fig.3.

5. The Logic Model of Sub-top Event "Human in Hazardous Zone"(N in Fig.3)

This event is subdivided into "existence caused by functional approach"(Na01) and "by nonfunctional approach"(Na02) with a sorting OR gate.

5.1 "By functional approach"(Na01)

This is subdivided into "for job not related to robot"(Nb01), "for job related to robot"(Nb02) and "for being supported by robot like patient care robot"(Nb03) with a sorting OR gate.

5.1.1 "For job not related to robot"(Nb01)

This is subdivided into "essentially necessary"(Nc01) and "not essentially necessary but performed because job safety analysis LTA"(Nc02) with an OR gate.

5.1.2 "For job related to robot"(Nb02)

This is subdivided into "transport or installation of robot"(Nc03), "arrangement"(Nc04), "programming"(Nc05), "test running"(Nc06), "starting operation"(Nc07), "work in automated operation"(Nc08), "trouble-shooting"(Nc09) and "maintenance or repair"(Nc10) with a sorting OR gate.

Fig.2 Comprehensive logic model for the analysis of the accident caused by striking a human with a robot arm

5.2 "By nonfunctional approach"(Na02)

This is subdivided into "robot comes near human unnecessarily"(Nb04) and "human enters hazardous zone"(Nb05) with an OR gate.

5.2.1 "Robot comes near"(Nb04)

This happens when the events "robot moves"(Nc12), "to human"(Nc13), "but human does not get away"(Nc11) and "barrier to prevent robot from approaching LTA"(Nc14) occur simultaneously. Event Nc12 is subdivided into "heteronomous movement"(Nd01) and "autonomous movement"(Nd02) with an OR gate. And events Nd01 and Nd02 connect to triangle No.42 below event Ec05 and No.53 below event Ec06 in Fig.1 respectively. The event Nc14 connects to triangle No.21 below event O in Fig.1.

5.2.2 "Human enters there"(Nb05)

This event occurs when the two events "human is going to enter there"(Nc15) and "barrier like fence to prevent entrance LTA"(Nc16) occur simultaneously. The latter Nc16 connects to triangle No.21 below event O in Fig.1.

a. "Going to enter"(Nc15)

This event occurs when any one of the cases, "human-error"(Nd03), "human forced to enter by action of peripheral equipment"(Nd04) or "path for human overlaps with hazardous zone"(Nd05) occurs.

a-i "Human-error"(Nd03)

This is further subdivided into "human misjudges hazardous zone"(Ne01), "human is ignorant of hazardous zone"(Ne02), "illusion about conditional wait that is temporary stop of robot"(Ne03) and "intentional invasion of human who knows hazard"(Ne04) with an OR gate.

6. System Phase Division and Minimal Cut Sets

6.1 Independence among basic events and system phase division

It will become very intricate to evaluate the existence probability or the expected number of occurrences of the top events of the logic models if the basic events can not be assumed to be statistically independent of each other.

The basic events of the logic models, however, can not always be expected to be statistically independent of each other

under general conditions. For example, the basic events under the event "heteronomous movement"(Ec05 in Fig.1) and the event "autonomous movement"(Ec06), or the basic events under the event "by functional approach"(Na01 in Fig.3) and the event "by nonfunctional approach"(Na02) are mutually exclusive respectively.

Now, we propose a method of system phase division to cope with the difficulties. The system-phase-division method is defined as follows: to find out the factors dominating interdependence among the basic events and to divide the factors into appropriate modes, and then to give the basic events statistical independence in each fragmentary system phase made by uniting each mode of factors. The quantitative evaluation of all the system phases will be made by totaling all the results given to each fragmentary system phase.

6.2 Modes of system phases and the coherency among them

We offer the factors "robot-condition factor", "robot-movement factor" and "human-existence factor" for the logic models. We divide the condition factor into seven modes, the movement factor into three modes, and the existence factor into two modes as shown in Fig.4 respectively.

Next, we consider the coherency among the modes. The robot in the transport, installation or arrangement mode is often in the situation not automatically controlled, therefore such mode will cohere strongly with the heteronomous movement mode. Workers approaching the robot in the teaching, test-running, or starting mode usually know their normal movement; therefore, such modes will cohere strongly with the autonomous movement mode by commands that are not intended. The automated operation mode will cohere strongly with the autonomous movement modes by both intended and unintended commands. The maintenance or repair mode will cohere with every movement mode depending on the situation. The existence mode by functional approach will cohere with every movement mode depending on the situation. The nonfunctional approach will cohere strongly with the autonomous movement mode by intended commands, because the person who approaches a robot nonfunctionally often does not know how it moves.

Fig.4 Modes to obtain system phases and the coherency among them

Table 1 Important minimal cut sets for main system phases

Main Phases of the System	Important Minimal Cut Sets in The Phase
f)-(a)-(a)	(Nb01,Eel6,Ed10,Ed11) (Nc08,Eel6,Ed10,Ed11) (Nc09,Eel6,Ed10,Ed11) (Nb03,Eel6,Ed10,Ed11)
f)-(a)-(b)	(Nc15,Nc16,Eel6,Ed10,Ed11)
f)-(b)-(a)	(Nb01,Ef23,Ed10,Ed11) (Nb01,Ef24,Ed10,Ed11) (Nb01,Ef25,Ed10,Ed11) (Nb01,Ef26,Ed10,Ed11) (Nc08,Ef23,Ed10,Ed11) (Nc08,Ef24,Ed10,Ed11) (Nc08,Ef25,Ed10,Ed11) (Nc08,Ef26,Ed10,Ed11) (Nc09,Ef23,Ed10,Ed11) (Nc09,Ef24,Ed10,Ed11) (Nc09,Ef25,Ed10,Ed11) (Nc09,Ef26,Ed10,Ed11) (Nb03,Ef23,Ed10,Ed11) (Nb03,Ef24,Ed10,Ed11) (Nb03,Ef25,Ed10,Ed11) (Nb03,Ef26,Ed10,Ed11)

The results considered above are shown in Fig.4.

6.3 Important minimal cut sets in main system phases

Important minimal cut sets are extracted for the main system phases consisting of the automated operation mode and the modes which cohere strongly with it. These are (f)-(a)-(a), (f)-(a)-(b) and (f)-(b)-(a) respectively in Table 1. Here, the system phase is defined with symbols such as (f)-(a)-(a) corresponding to the symbols of (condition mode)-(movement mode)-(existence mode) in Fig.4. We assume that the output from any sorting AND or OR gate shall be given to only one sorted part and that the basic events are statistically independent of each other in the fragmentary system phase. From above, each one of the cuts will generate the event Ea03 or Ea04 according to the practical contents of the input events.

7. Conclusions

In this paper, the comprehensive logic models for the analysis of accidents caused by a robot body or arm striking a human are developed. Any hazard analysis of a concrete human-robot system, regarding such accidents, can be checked for oversights by using the models.

Furthermore, statistical independence

among the basic events of the models is estimated. It is concluded that statistical independence is not expected under general conditions, but that the three factors which dominate the independence are extracted. In addition, the assumption of statistical independence will be approximately satisfied in each fragmentary system phase which is defined by uniting the factor modes that are obtained by dividing each factor into several fragments. Minimal cut sets of the logic models for some important system phases are then extracted to obtain the main system failure modes.

References

- (1) Sato, Y. and Inoue, K., Bull. of the JSME, Vol.29, No.250(1986), pp.1356-1361.
- (2) Johnson, W.G., MORT Safety Assurance Systems, (1980), pp.155-178, Marcel Dekker, INC.
- (3) Kawaguchi, K., Sugimoto, N., Sato, Y. et al., RIIS TN-82-1(in Japanese), (1982), pp.1-10.
- (4) Barlow, R.E., and Lambert, H.E., Introduction to Fault Tree Analysis; Reliability and Fault Tree Analysis, (1975), pp.7-12, Society for Industrial and Applied Mathematics.
- (5) Henley, A.J. and Kumamoto, H., Reliability Engineering and Risk Assessment, (1981), pp.48-57, Prentice-Hall, INC.