BRAKE PRESS SYSTEM SAFETY EVALUATION WITH DEVICE AND HUMAN FAILURE MODES, REPAIR RATES AND REDUNDANCY

ĐÁNH GIÁ AN TOÀN HỆ THỐNG MÁY CHẤN THỦY LỰC KẾT HỢP CÁC YẾU TỐ LỖI THIẾT BỊ, LỖI NGƯỜI VẬN HÀNH, KHẢ NĂNG SỬA CHỮA VÀ DỰ PHÒNG

Tony Venditti[1], Nguyen-Duy-Phuong Tran[2,*], Anh-Dung Ngo[1]
[1]Department of Mechanical Engineering, École de Technologie Supérieure, Canada
[2]Department of Manufacturing Engineering, Faculty of Mechanical Engineering, Ho Chi Minh City University of Technology, Vietnam
**Email: tnduyphuong@yahoo.com*

ABSTRACT

Press brakes are machines widely used in the manufacturing industry to bend metal sheets. They pose risks in terms of equipment failure and worker accidents. In order to prevent these unwanted occurrences, the associated risks must first be analyzed. In this paper, such an analysis is conducted for a press brake system incorporating redundancies such as two operators and two point-of-operation safety devices. The probability of the system being in a failed state where an operator suffers an injury is estimated with the help of a Markov diagram which includes failure and repair rates not only for the devices but also in terms of operators' failures.

Keywords: *Failure rate; Repair rate; Human reliability; Markov diagram; Fuzzy logic.*

TÓM TẮT

Máy chấn thủy lực là loại máy được sử dụng rộng rãi trong công nghiệp để uốn các tấm kim loại. Thiết bị này tồn tại rủi ro về lỗi linh kiện và tai nạn lao động. Để ngăn chặn những sự cố không mong muốn, phải phân tích các rủi ro liên quan. Trong bài báo này, việc phân tích rủi ro được thực hiện đối với hệ thống chấn thủy lực kết hợp tình huống có áp dụng dự phòng như hai người vận hành và hai thiết bị an toàn tại khi vận hành. Xác suất lỗi được ước tính bằng sơ đồ Markov, bao gồm mức độ hỏng và khả năng sửa chữa không chỉ đối với linh kiện mà còn cả lỗi của người vận hành.

Từ khóa: *Cường độ hỏng; Khả năng sửa chữa; Độ tin cậy người vận hành; Chuỗi Markov; Luận lý mờ.*

☞

1. INTRODUCTION

This paper presents the case of a press brake operated by the two operators. This situation arises in actual work settings when large sheets of metal are bent in a brake press. In that case, the second operator is necessary to hold the workpiece properly where proper work-holding tables and fixtures are not present. However, in this study, the workstation setup will in fact be different. The second operator will assume the role of an assistant who is there to make sure that the work proceeds correctly and safely. For instance, if he notices the first operator making an error, he will be in a position to intervene and stop the machine. This set-up becomes a system which will be modelled mathematically and solved for safety-related variables of interest.

2. FORWARD PROBLEM

2.1. Safeguarding and human redundancy

Redundancy can be defined as "the existence, in an entity, of more than one means for performing a required function" [1]. In the context of machine safety, the function that needs to be performed can be:

- Stopping the hazardous motion.
- Assuring the safe position of a component of a machine.

To give a specific industrial example, maintaining the upper die in an hydraulic press brake in an elevated position, supported by the hydraulic pressure in a cylinder is a safety function.

On an industrial machine, redundancy can be achieved commonly in two important ways.

- Two safeguarding devices can be installed to prevent entry into the hazardous zone or contact with the hazardous zone of a machine. An example of redundant safeguarding is shown in the figure where a safety light curtain is used in conjunction with a two-hand control on a mechanical punching press to prevent entry into the hazardous zone (the dies, only partially visible on the photograph) of the press.

- Industrial machines' control systems are another area where redundancy is put in place. For instance, two electrical contactors can be placed in series with the motor of a machine. This way, if following a stop command, the contacts in one of the contactors fail by staying closed because of redundancy can assure, de-energizing of the motor provided the second contactor functions correctly.

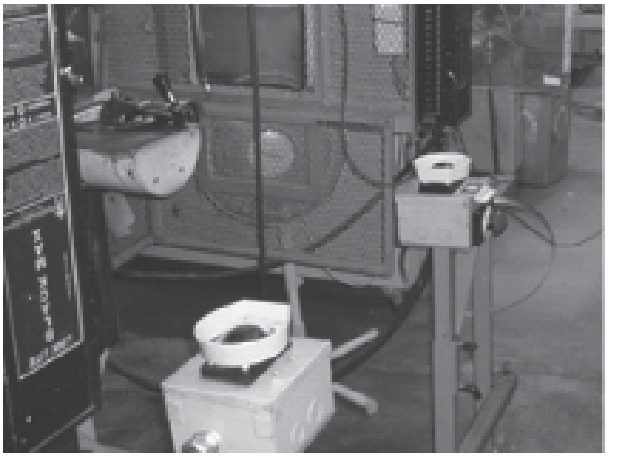

Figure 1. Mechanical punch press with redundant protective devices.

2.2. Press brake system

The press brake to be considered to incorporate elements of redundancy both at the hardware level and at the human level. Hardware redundancy will take the form of two safety devices between the machine and

ISSN 2615 - 9910 (bản in), ISSN 2815 - 5505 (online)
TẠP CHÍ CƠ KHÍ VIỆT NAM, Số 327, tháng 4 năm 2025
cokhivietnam.vn / tapchicokhi.com.vn

the operator. For example, these could be as shown in Figure 1, a two-hand device and a safety light curtain. It is also assumed that the workstation has been designed so that adequate support devices have been provided on the press brake so that the operator does not need to hold the workpiece at any time during the bending process. He only needs to handle manually the workpiece when repositioning is necessary for the subsequent bend.

Human redundancy will consist of two workers at the workstation. At any instant of time during production, one worker will act as the actual operator. The second worker will assume the role of a checker. This will set-up a humanly-redundant work situation in conformity with the definitions seen in the literature [2]. Both workers will be assumed to possess similar levels of training and experience.

Two human modes of failure are assumed to be necessary for accident generation. These failures result in the worker, Operator # 1, not withdrawing his hands from between the dies. In practice, such accidents have occurred due to contributing factors (modes of failures) such as, for example, worker fatigue due to high job repetition leading to loss of concentration, stressful work situations, very noisy or hot and humid work environment. Operator # 2 can fail to be alert and check the operator of the press for the same reasons (which, it will be noticed are not developed in the fault tree developed). This leads to the fault tree shown in Figure 2. The failure of the devices will be meant to encompass all modes of dangerous failures through the whole chain of machine controls linked to the devices.

3. ANALYSIS

This will lead to the fault tree shown in Figure 2. It will be noted that this fault tree is also dynamic in nature, in the sense that the accident depends on a sequence of events such as the event protective device failure, must occur before the bending action by the worker; otherwise a properly functioning device would stop (safely) the press and no accident then occurs.

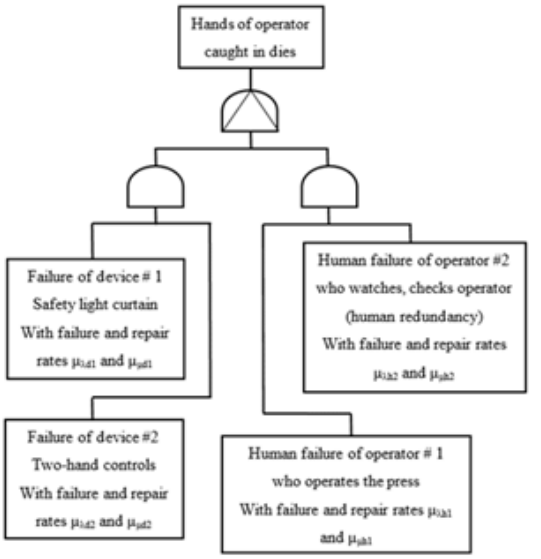

Figure 2. Fault tree with repair, redundancy and human error.

The equivalent associated Markov diagram is then:

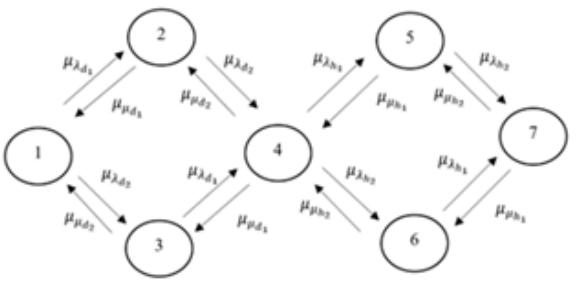

Figure 3. Markov diagram with repair, redundancy and human error.

The solution to the model is then (see [3]) for details applied to a similar problem):

$$\frac{d}{dt}\begin{bmatrix}p_1\\p_2\\p_3\\p_4\\p_5\\p_6\\p_7\end{bmatrix}=\begin{bmatrix}Q_{11} & Q_{12} & Q_{13} & 0 & 0 & 0 & 0\\ Q_{21} & Q_{22} & 0 & Q_{24} & 0 & 0 & 0\\ Q_{31} & 0 & Q_{33} & Q_{34} & 0 & 0 & 0\\ 0 & Q_{42} & Q_{43} & Q_{44} & 0 & 0 & 0\\ 0 & 0 & 0 & Q_{54} & Q_{55} & 0 & Q_{57}\\ 0 & 0 & 0 & Q_{64} & 0 & Q_{66} & Q_{67}\\ 0 & 0 & 0 & 0 & Q_{75} & Q_{76} & Q_{77}\end{bmatrix}\begin{bmatrix}p_1\\p_2\\p_3\\p_4\\p_5\\p_6\\p_7\end{bmatrix}$$

or:

$$\frac{\mathrm{d}}{\mathrm{dt}}\mathrm{P}=\mathrm{Q}^{\mathrm{T}}\mathrm{P}$$

$$Q_{11}=-\mu_{\lambda_{d_1}}-\mu_{\lambda_{d_2}}$$

$$Q_{12}=-Q_{43}=-\mu_{\mu_{d_1}}$$

$$Q_{13}=-\mu_{\mu_{d_2}}$$

$$Q_{21}=\mu_{\lambda_{d_1}}$$

$$Q_{22}=-\mu_{\lambda_{d_2}}-\mu_{\lambda_{d_1}}$$

$$Q_{24}=Q_{42}=\mu_{\lambda_{d_2}}$$

$$Q_{31}=\mu_{\lambda_{d_2}}$$

$$Q_{33}=-\mu_{\lambda_{d_1}}-\mu_{\mu_{d_2}}$$

$$Q_{34}=\mu_{\mu_{d_1}}$$

$$Q_{44}=-\mu_{\lambda_{h_1}}-\mu_{\mu_{d_2}}-\mu_{\lambda_{h_2}}-\mu_{\mu_{d_1}}$$

$$Q_{54}=Q_{76}=\mu_{\lambda_{h_1}}$$

$$Q_{55}=-\mu_{\lambda_{h_2}}-\mu_{\lambda_{h_1}}$$

$$Q_{57}=\mu_{\lambda_{h_2}}$$

$$Q_{64}=Q_{75}=\mu_{\lambda_{h_2}}$$

$$Q_{66}=-\mu_{\mu_{h_2}}-\mu_{\lambda_{h_1}}$$

$$Q_{67}=\mu_{\mu_{h_1}}$$

$$Q_{77}=\mu_{\mu_{h_2}}-\mu_{\mu_{h_1}}$$

With:

$\mu_{\lambda_{d_i}}$: Refers to failure rates of the protective devices;

$\mu_{\lambda_{h_i}}$: Refers to human failure rates;

$\mu_{\mu_{d_i}}$: Refers to repair rates of the protective devices;

$\mu_{\mu_{h_i}}$: Refers to human repair rates.

P is the vector containing the probabilities of the system being in one of the seven states of the system. The Markov diagram represents the transitions of the system caused by the occurrences of the various failures. As an example, state 2 in the diagram represents the state of the system after a failure of protective device 1 has occurred (with a failure rate $\mu_{\lambda_{d_i}}$, a fuzzy number). The system can return to state 1 from state 2 following a repair with a (fuzzy) rate of $\mu_{\mu_{d_i}}$. There are 7 states in this example because there are 2 device failure modes, 2 human failure modes as well as 2 repair modes, for the each device and for each human failure modes. The combinations of transitions leads to 7 states as seen in the Markov diagram.

The algorithm was run on Matlab using the data (see Table 1) from a previous paper (see [4]) where values for λ_{dl} the mode of failure associated with the safety light curtain and λ_{hl} the human mode of failure "Hands in dies" were obtained from an expert elicitation process (see [4], [5]). The other data are assumed and result from an elementary internet search. The repair rate is defined in reliability (see for example [6]) as 1/MTTR that is, the inverse of the Mean Time to Repair.

The concept of Human repair rate, on the other hand, is somewhat novel. In this work, it has been defined analogously to the technical repair rate in reliability as 1/MTTR i.e. the

Mean Time to "Human Repair" understood in the following sense. This is the mean time required to return a worker to his workstation after a human error such as having hands in dies. The time to return to work might be the time spent in safety training. In industry, in Quebec, Canada, safety training are often typically 2 to 4 hours (see for example [7], the website of an OHS training organization in Quebec). This then serves to calculate the value of the human repair rate (the middle value of a triangular fuzzy number).

The initial conditions for the problem are: $p_1 = 1$ because state 1 represents the system in working conditions and no failures occur. The complete set of input data is collected in Table 1. It shows, in particular, the device and human failure rates as estimated by experts as described in [4].

Table 1. Input data set case study including repair and redundancy.

Data	Lower values of TFN (h^{-1})	Middle values of TFN (h^{-1})	High values of TFN (h^{-1})
$\mu_{\lambda_{d1}}$	2.58×10^{-5}	2.71×10^{-5}	2.84×10^{-5}
$\mu_{\lambda_{d2}}$	2.58×10^{-5}	2.71×10^{-5}	2.84×10^{-5}
$\mu_{\lambda_{h1}}$	0.98×10^{-5}	1.03×10^{-5}	1.08×10^{-5}
$\mu_{\lambda_{h2}}$	0.98×10^{-5}	2.71×10^{-5}	2.84×10^{-5}
$\mu_{\mu_{d1}}$	0.119	0.125	0.131
$\mu_{\mu_{d2}}$	0.119	0.125	0.131
$\mu_{\mu_{h1}}$	0.47	0.50	0.52
$\mu_{\mu_{h2}}$	0.47	0.50	0.52

The calculations presented here show that systems with human and technical redundancy can result in probabilities of occurrence of accidents which are very low in the order of $1/10^{-8}$ (see Table 2). This can be explained by the safeguarding redundancies in the system. It is to be noted, on the other hand, that the individual probabilities of failure (technical and human) were estimated by the experts as less than what the safety standards demand (typically, $1/10^{-6}$, see for example, [8]). The reason for these findings will be investigated in further planned research. We see as well that the algorithm produces consistent TFNs (that is to say the fuzzy numbers are an ordered set), an indication of a valid numerical procedure.

Table 2. Results of calculations for case study.

Data	Lower values of TFN (h^{-1})	Middle values of TFN (h^{-1})	High values of TFN (h^{-1})
p_1	0.999568161467824	0.999566492623574	0.999566502486222
p_2	0.000215873120110	0.000216706011731	0.000216699909645
p_3	0.000215873120110	0.000216706011731	0.000216699909645
p_4	0.000000046617499	0.000000046977992	0.000000046975344
p_5	0.000000038771234	0.000000042278284	0.000000045647180
p_6	0.000000085386789	0.000000089254340	0.000000092620573
p_7	0.000000038773659	0.000000042280896	0.000000045650024

4. CONCLUSION

The safety a press brake system comprising redundant safeguarding both technical and human was analyzed. A methodology was developed to estimate the probability of an accident where an operator has his caught between the dies of a press brake for the setup described. The analysis included concepts of error rates (technical and human) as well as repair rates. A novel feature of the study is the concept of "human repair rate". Fuzzy data in part from an expert elicitation process was used. The algorithm produced consistent results, showing a valid numerical procedure.

Further work will attempt to refine the expert elicitation process used to generate the data. A press brake simulator will also be built to gather data on human error.❖

References:

[1]. IEC 60050-191 (1999), "*International Electrotechnical Vocabulary*". Chapter 191: Dependability and quality of service.

[2]. Clarke, D.M. (2005), "*Human redundancy in complex, hazardous systems: A theoretical framework*". Safety Science 43(9) : 655-6.

[3]. Venditti, T, Tran, N.P.D, Ngô, A.D. (2018), "*System Safety Analysis of an Industrial Process Using Fuzzy Methodology*". 4th International Conference on Fuzzy Systems and Data Mining (FSDM2018), Bangkok, Thailand November 16-19, 2018.

[4]. Venditti, T, Tran, N.P.D, Ngô, A.D. (2018), "*Expert elicitation methodology in the risk analysis of an industrial machine*". 9th International Conference on Applied Human Factors and Ergonomics (AHFE) Orlando, Florida, USA, July 21st to 25th 2018.

[5]. Nascimento C.S., R.N. de Mesquita (2012), "*Human reliability analysis data obtainment through fuzzy logic in nuclear plants*". Nuclear Engineering and Design, Vol.250, pp.671-677.

[6]. Lewis, E.E. (1996), "*Introduction to reliability engineering*". New York, N.Y.: J. Wiley and Sons.

[7]. [Online]. Available: www.asfetm.com/Répertoire-de-formations

[8]. Department of Defense USA. (1993) MIL-STD-882D Standard Practice for System Safety.