

A consideration of the operation of automatic production machines

Toshiro HOSHI^{1*} and Noboru SUGIMOTO²

¹Nagaoka University of Technology, Japan

²Meiji University, Japan

Received August 12, 2014 and accepted January 26, 2015

Published online in J-STAGE February 9, 2015

Abstract: At worksites, various automatic production machines are in use to release workers from muscular labor or labor in the detrimental environment. On the other hand, a large number of industrial accidents have been caused by automatic production machines. In view of this, this paper considers the operation of automatic production machines from the viewpoint of accident prevention, and points out two types of machine operation – operation for which quick performance is required (operation that is not permitted to be delayed) – and operation for which composed performance is required (operation that is not permitted to be performed in haste). These operations are distinguished by operation buttons of suitable colors and shapes. This paper shows that these characteristics are evaluated as “asymmetric on the time-axis”. Here, in order for workers to accept the risk of automatic production machines, it is preconditioned in general that harm should be sufficiently small or avoidance of harm is easy. In this connection, this paper shows the possibility of facilitating the acceptance of the risk of automatic production machines by enhancing the asymmetric on the time-axis.

Key words: Safety, Safety control, Safety system, Industrial accident, Asymmetric on the time-axis

Introduction

At worksites, various automatic production machines are in use to release workers from muscular labor or labor in the detrimental environment. On the other hand, a large number of industrial accidents have been caused by automatic production machines. Even automatic production machines require the involvement of workers for troubleshooting, etc. However, because of being automatic, automatic production machines lack attention to workers, which often causes accidents. Conventionally, in order to prevent accidents related to machine operation, measures

have been taken to counter human errors by, for example, calling others' attention or working in pairs, which is significant also for raising operation rates. It should be noted, however, that there is no person who can operate machines without making a mistake. Considering this fact, it is requested to design machines on the premise of human errors so that human safety can be assured even in case of erroneous machine operation. Here, there are two types of human error – a hasty error made carelessly when it should not be made in haste, and a delay error made by neglecting the performance and missing the predetermined time. In this paper, a basic model is set for the operation of automatic production machines, and the safety conditions determined necessary based on the basic model are considered from the viewpoint of time. Using this basic model, this paper shows that (1) there are two types of operation of automatic production machines – operation that is not

*To whom correspondence should be addressed.

E-mail: hoshi@meiji.ac.jp

©2015 National Institute of Occupational Safety and Health

permitted to be performed in haste, and operation that is not permitted to be performed late, (2) in the interface and education in the safety of automatic production machines, it is appropriate to evaluate the operation by referring to the asymmetric on the time-axis, and (3) it is important to enhance the asymmetric on the time-axis of the human interface in order to improve the safety of automatic production machines.

Operation of an Automatic Production Machine

Circumstances surrounding automatic production machines

The industrial robot is a typical automated manufacturing machine. Table 1 shows the death toll due to industrial robots for ten years from 2000 to 2009¹⁾. From this table, it is apparent that fatal accidents are caused in most cases when workers are pressed by live robot arms during their engagement in troubleshooting. Not only industrial robots but also other automatic production machines often require human attendance when they have something of trouble. For example, even when a slight dislocation of a workpiece cannot be sensed by an industrial robot and the robot hand may be caught by the workpiece and come to stop. This requires the worker to enter the working area to position the workpiece correctly. However, assuming that automatic production machines continue to operate automatically without human attendance, many production lines are designed with no consideration of human entrance into the working area, which poses safety problems. For example, workers have to take an unnatural posture to force them to pass through production lines, workers have to pass through the movable sphere of automatic production machines, a person, if any, in the working area cannot be seen from the position of the operation panel, workers can freely enter the working area of automatic production machines, and there is no space available to workers for evacuation. With these safety problems, a number of accidents occur when workers enter the movable area of automatic production machines carelessly without stopping the machine. In this way, when a danger due to man-machine contact is left to workers and no consideration of workers is made in designing automatic production machines, labor accidents may occur. The Ordinance on Industrial Safety and Hygiene stipulates that when a machine is adjusted or cleaned, measures should be taken beforehand, such as shutting down the machine. The ordinance provides for the same stipulations for the industrial robots. Under present circumstances, however, these stipulations are not

Table 1. Fatal accidents due to industrial robots¹⁾

Operation contents specific to operators	Death toll
Normal operation	2 persons
Troubleshooting with live machines	18 persons
Maintenance of robots or peripheral units	3 persons

Analysis based on data released by Ministry of Health, Labour and Welfare.

observed, which leads to accidents.

In Japan, in this context, while the non-regular employment and short-term employment of workers are on the increase, safety education is provided less and less²⁾. On the other hand, while the speed and power of machines are ever-increasing, touch panels, for example, require only touching with no need of pressing. If the touch panel is touched involuntarily and carelessly, it activates the machine. As a result, potential risk of machines is ever-growing in Japan, and workers who operate machines can no longer avoid dangers by using their artisanship.

One of the protective measures used for maintenance and similar work is lockout. According to this measure, the start switch of a machine is made lockable so that the machine cannot be started by some worker by mistake when some other worker enters the inside of the production line fence and all workers who are to enter the inside lock the start switch respectively before entering the inside to prevent accidental turning ON of the start switch while they are working inside. This may be interpreted as an effective mechanism for enabling workers to signal to the machine that the machine is now permitted to start. However, this measure has not yet taken hold in Japan probably because even if only one of them comes out of the inside late, the machine cannot be started until he comes out. This measure is accompanied by two types of failure: one is that the machine cannot be started even though it is ready for starting because “some worker has lost the key” (delay error), and the other is that the machine starts even though the machine should not start now because “some worker enters the inside without having the key” or “some worker unlocks the start switch of the machine by mistake by using a spare key” (hasty error). It is the latter error that poses a safety problem.

With respect to the emergency stop operation, there are two types of failure: one is that some worker cannot press the emergency stop button when it should be pressed because he cannot locate the emergency stop button (delay error), and the other is that some worker hits and press the emergency stop button carelessly when it should not

be pressed (hasty error). It is the former error that poses a safety problem.

In the mistake which becomes early, and an overdue mistake, damage may differ very much. When it mistakes, it considers which is safe by the case. The characteristic that it operates to the safer one on a time-axis is referred to as “asymmetrical on a time-axis”.

Basic operation model of an automatic production machine

A basic model of automatically operating machines is conceived. As the ground rule for machine operation, the machine operation is permitted only when the safety has been confirmed, and expressed in logical AND as shown in Fig. 1³⁾. The following figure is a time chart. “Intention” of Fig. 1 is a logical variable to which those with intention are expressed with 1, and it expresses those without intention with 0. “Safety” is a logical variable which expresses 1 when safety is confirmed, and expresses 0 when not confirmed. “Execution” is an ethics variable to which those with execution are expressed with 1, and it expresses those without execution with 0. This figure shows on the time-axis that the operation is permitted as long as the safety has been confirmed but is not permitted when the safety has not yet been confirmed. Here, the time when the safety is no longer confirmed, T_{ac} , is assumed anew as an accident, the ground rule can be expressed as a temporary development between the present time T_{ob} and the time T_{ac} . These are expressed as a basic model in Fig. 2. In this model, in order to secure the safety, the machine has to be stopped before an accident occurs. In general, however, because the accident cannot be recognized until it occurs and when it occurs is unknown, the timing of applying the brake is unknown. For this reason, the physical amount of the dangerous event related to an accident is measured, and thereby the accident occurrence time T_{ac} is predicted and the brake is applied to stop (pause) the machine before an accident occurs. This is called “stop control”. The time when the stop control should be started, T_{wa} , can be shown by the following expression (1):

$$T_{wa} \leq T_{ac} - t_1 \quad (1)$$

where, t_1 is the time required for stopping (braking time).

Machinery stops in a few seconds or minutes. It may take a few days to stop the chemical plant. This expression shows the critical conditions for not an accident.

Because stopping the machine lowers the productivity and therefore should be avoided, if possible, control is performed beforehand to resume the normal condition so that the machine cannot fall into the state that requires the

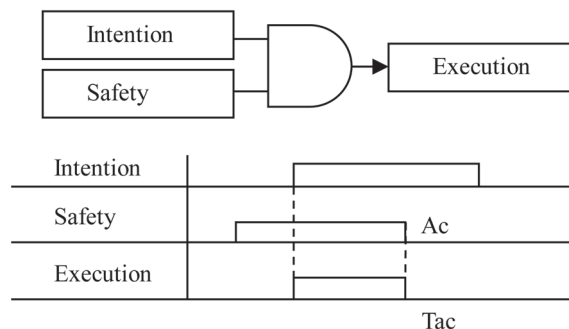


Fig. 1. Ground rule for safety.

machine to be stopped. This is called “regulation control.” The time to start the regulation control, T_{re} , can be shown by the following expression (2):

$$T_{re} \leq T_{wa} - t_2 \quad (2)$$

where, t_2 is the time required for regulation (regulation time).

Furthermore, before the machine comes into the state that requires the regulation control, the objective control is performed to maintain the original state that is the most appropriate to fulfill the original purpose of the machine. The objective control is being performed as long as the machine is in normal operation.

The model shown in Fig. 2 may be marshalled in two stages – the planning stage and the execution stage – as shown in Fig. 3. In the planning stage, an accident is assumed by risk assessment, and safety measures are planned in consideration of restriction of time. We have to make a plan so that it may count backward and may not be late for the time limit. Safety measures are planned on the time –axis. At this time, risk should be reduced on the automatic production machine side in the first place. On this basis, there is a hazard that should inevitably be entrusted to the worker for treatment. Now that the hazard is entrusted to the worker for treatment, it should be treated easily by the worker, and the treatment should be completed before an accident occurs. In the planning stage, whether the treatment can be completed within such time limit should be confirmed beforehand.

In the execution stage, the physical phenomena, such as electromagnetic waves as embodied by, for example, precrash brake, are used to predict an accident, and the accident is prevented by performing the control and operation as planned beforehand. It should be noted, however, that failures may occur in performing the control and operation in each stage. A failure in the objective control

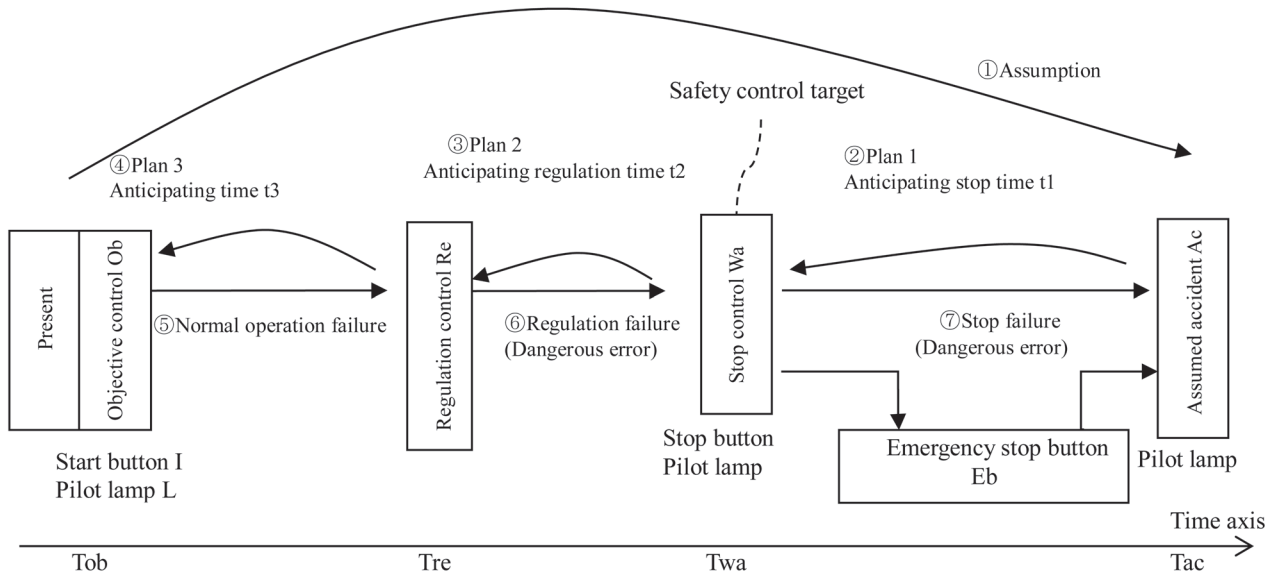


Fig. 2. Model of planning for automatic production machine operation and temporary development until an accident occurs.

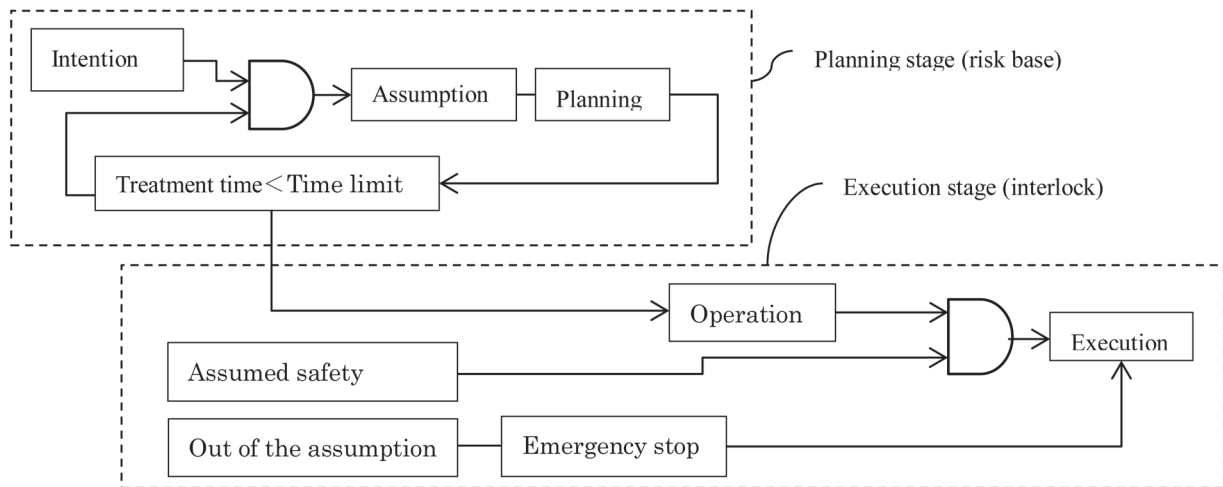


Fig. 3. Planning and implementation of the safety operation of an automatic production machine.

is coped with by the regulation control, and a failure in the regulation control is coped with by the stop control. If the failure in the objective control cannot be coped with, the failure in the regulation control and stop control cannot be coped with either, and the failure in the stop control cannot be coped with either, the emergency stop is applied as the last measure. This means that the machine is placed at last under the control by humans.

Furthermore, an event not expected in the planning stage (unexpected event) may occur but with a very low probability. For unexpected events, any countermeasure cannot be taken, and unplanned execution in the uncertain circumstances should be avoided. In case of an unexpected event,

there is no choice but to stop the machine immediately. This is reflected in the interlock during the execution as shown in Fig. 3. “Operation” is planned assuming an accident. This plan must be what can be carried out before the time limit. A safety measure is devised to the event which can be assumed. An emergency stop button is pushed at the event which cannot be assumed. The output of AND-Gate is set to 0 and a machine stops. If it is expected, a plan can be made in advance and safety can be confirmed. An emergency stop may not do about an unexpected thing.

Operation of basic model

The basic operation of the automatic production machine

and the basic behavior of the worker are consistently in accordance with the ground rule for safety shown in Fig. 1 (from safety confirmation to operation permission). That is, ① at the beginning of daily operation, the machine confirms the safety for itself, and indicates the worker that the machine is ready for starting by lighting the pilot lamp, ② in response to this indication, the worker presses the start button to indicate to the machine that he is also ready for starting, and the machine starts operation upon such mutual permission, ③ the worker adjusts the machine to improve the operation rates and the work efficiency, and ④ at the end of daily operation, the worker presses the stop button to stop (power OFF) the automatic production machine.

Referring to the basic model, the author makes a study of the following with a focus on the pilot lamp indicating the operation status of the machine and the push button indicating the intention of the worker. The lamp (pilot lamp L) indicating that the machine is ready for operation is characterized by lighting up only when the safety conditions are satisfied and not lighting up in any other case. In the same way, the start button I is characterized by being enabled only when the pilot lamp L is lighting and being disabled in any other case. This relational transitions with time as shown by the following expression (3):

$$Sc \rightarrow L \rightarrow I \quad (3) \quad (\rightarrow \text{ indicates the flow of time.})$$

and can be shown in the unate relationship³⁾ by the following expression (4):

$$Sc \geq L \geq I \quad (4)$$

where, Sc is the binary logical variable with 1 assuming the safety confirmed and 0 assuming the safety not confirmed, L is the binary logical variable with 1 assuming the pilot lamp ON and 0 assuming the pilot lamp OFF, and I is binary logical variable with 1 assuming the start button ON and 0 assuming the start button OFF.

When the machine is in operation, the machine operates normally under the operation command. However, when the machine is in automatic-control operation, failure may occur stochastically. To counter this stochastic occurrence of failure, the worker is to stop the machine by pressing the emergency stop button (the emergency stop button specified in ISO 13850:2006⁴⁾) as the last resort. An emergency stop button is pushed when the unexpected event of failure occurs. For the accident preventing purpose, the emergency stop button is permitted to be pressed before the brake is applied but is not permitted to be pressed after the brake is applied. Specifically, an accident of the machine in normal operation occurs when a dangerous error in the objective

control, a dangerous error in the regulation control, a dangerous error in the stop control and a dangerous error in the emergency stop button operation occur in series as shown in Fig. 2. The passage of time of such serial occurrence can be shown by the following expression (5):

$$\neg Ob^* \rightarrow \neg Re^* \rightarrow \neg Wa^* \rightarrow \neg Eb^* \rightarrow Ac \quad (5)$$

where, $\neg Ob^*$ is the logical variable with 1 assuming a dangerous error in the objective control and 0 assuming no dangerous error in the objective control, $\neg Re^*$ is the logical variable with 1 assuming a dangerous error in the regulation control and 0 assuming no dangerous error in the regulation control, $\neg Wa^*$ is the logical variable with 1 assuming a dangerous error in the stop control and 0 assuming no dangerous error in the stop control, $\neg Eb^*$ is the logical variable with 1 assuming a dangerous error in the emergency stop button (miss in pressing) and 0 assuming no dangerous error in the emergency stop button (no miss in pressing), and Ac is the binary logical variable with 1 assuming the occurrence of an accident and 0 assuming no occurrence of an accident. In addition, \neg is a sign which shows denial. * is a sign which shows the normality of a function. Then, because an accident occurs when dangerous errors occur in series and they are embodied to be actual errors with some sort of timing, Ac can be shown by the following expression (6):

$$Ac \leq \neg Ob^* \cdot \neg Re^* \cdot \neg Wa^* \cdot \neg Eb^* \quad (6)$$

It is shown that an accident occurs, when all the control fails in a formula (6) and also operation of an emergency stop button is overdue. Since recovery does not attach an accident, high reliability is required for these control. However, an error arises slightly. Although the error which stops a machine early in that case is allowed, recovery does not attach an overdue error. There is no control device which does not break down by any means. The characteristic with control asymmetrical on a time-axis is required. A human may waver in judgment. We don't risk fatal harm. When it wavers, you have to stop early. The characteristic with operation asymmetrical on a time-axis is required. In order to evaluate safety, it is required to evaluate by asymmetry on the time-axis of not only the frequency of a mistake.

International standards and asymmetric on the time-axis

The international safety standard was considered by "it is asymmetrical on a time-axis". Referring to the basic model, buttons, pilot lamps, etc. as information transmission means between the machine and the worker

Table 2. Number of worksites of industrial robot manufacturers and users classified by whether regulations for pilot lamp colors are in place (Surveyed on robot lamps for manufacturers and production line lamps for users)¹⁾

Manufacturers (Robot and operation panel pilot lamps)	Regulations in place	20 companies
	Regulations not in place	17 companies
Users (Production line pilot lamps)	Regulations in place	10 companies
	Regulations not in place	4 companies

are verified in the light of the International Standards ISO13850:2006⁴⁾, ISO3864-1:2011⁵⁾ and IEC60204-1:2009⁶⁾. According to these standards, red should be used for emergency case requiring immediate response and should not be used for any other cases, green should be used for indicating normality, the start button should preferably be colored white, and the stop button should preferably be colored black. Specifically, when the condition of the automatic production machine is normal, the machine is lighting the green lamp and waiting for a command from the worker, and the worker issues a command solemnly (start command by pressing the white button or stop command by pressing the black button) under the safety confirmed conditions. However, if some trouble occurs in the machine, the machine lights up the yellow lamp and wait for troubleshooting by the worker. Furthermore, if the machine no longer fulfills even this waiting function normally, the worker presses the emergency stop button as the last resort to stop the machine. Also, according to these standards, the emergency stop button should be shaped to be easy-to-press by hand and should be colored “red on yellow” to be obtrusive, all buttons excepting the emergency stop button are prohibited to be colored red to avoid confusion, the start button is colored white or whitish and of recessed shape or covered to prevent careless touching.

As psychological color effects, red is said to conjure up the images of passion, danger and activity, and green is said to conjure up the images of nature, safety, rest, composure and life⁷⁾. The order of colors according to perceptual closeness (perceptual distance of colors) is red, yellow/orange, purple, green and blue⁸⁾. From this color order, it is inferable that the red button tends to be pressed instantaneously upon danger is perceived (hasty side on the time-axis), and the green button tends to be pressed after calm judgment (delay side on the time-axis). The international standard about a push button or a lamp is considered to have been created in consideration of such a human being’s characteristic. It seems that it can be said that suiting an international standard considers people’s time characteristic.

Actual condition survey

In order to consider whether the machine used at the factory in Japan is considered in human’s time characteristic, the color of a push button or a lamp was investigated.

The first investigation was made in 2011¹⁾ as to industrial robots, typical automatic production machines, into ① the colors of pilot lamps of robots manufactured by robot manufacturers, and ② the colors of pilot lamps of robot-equipped production lines of robot users’ facilities (Table 1). According to this investigation, colors to be used were not specified by 45.9% of the manufactures and 28.6% of the users (Table 2); red or yellow/orange was specified as the color to indicate that the machine was in automatic operation by 7.9% of the manufacturers and 9.1% of the users, and green or blue was specified as the color to indicate that the machine was at a protective stop by 2.6% of the manufacturers and 9.1% of the users (Table 3).

According to the survey report of the Japan Machinery Federation⁹⁾ in 2011 (hereinafter referred to as “JMF Survey”), the colors of the pilot lamp when the machine is in normal operation (during power up) are green (59.5%), white (23.8%), and red (7.1%), and the colors of the pilot lamp when the machine is at a stop are red (35.1%), white (16.2%) and green (13.5%). It should be noted that this survey were intended for participants in lectures on the international standards for machine safety held by the JMF, and therefore the survey results do not apparently represent the domestic average picture in the same way as the aforementioned questionnaire. The problem considered from these three investigations is shown in the following chapter.

Results

According to the questionnaire results, not a few machine-using companies have no color regulations in place. This suggests that they do not provide any internal standardized directives or educations about machine operation and others in case of emergency. This also suggests that non-standardized color meaning, which varies from machine to machine would, could cause erroneous button

Table 3. Number of worksites of industrial robot manufacturers and users classified by pilot lamp colors (Surveyed on robot lamps for manufacturers and production line lamps for users)¹⁾

		Red	Green	Yellow/orange	Blue	Other colors	No pilot lamp
Manufacturers	In automatic operation	2	23	1	1	5	6
	In teaching	2	7	5	2	7	15
	At a protective stop	18	1	3	0	4	13
	In cooperative operation	2	2	2	0	4	20
Users	In automatic operation	1	5	0	1	3	1
	In teaching	0	2	6	1	1	2
	At a protective stop	6	0	0	1	0	4
	In cooperative operation	0	0	3	0	1	7

pressing when quick judgment is required, and could not allow the asymmetric on the time-axis to be satisfied. In actual fact, however, many companies are using colors in accordance with the international standards and the Japanese Industrial Standards. This suggests that the companies at whom the questionnaire targeted have high consciousness of compliance with standards. Including the JMF Survey, some companies indicate start in red color and stop in green color. This is probably because they are pre-conceived that “because the machine is dangerous when it moves, the start button should be colored red”, and “because the machine becomes safe when it stops, the stop button should be green”. On the other hand, the color combination specified by the international standards is probably based on the conception that “the confirmed safety is conveyed to the machine by pressing the green button to permit starting, and if the safety can no longer be confirmed, the machine is stopped by pressing the red button immediately”. Using red color for the start button suggests that the “danger detection type” control, i.e., the danger due to the machine operation is resorted as it is to the attentiveness of the worker, and when the state reaches a truly dangerous stage, the worker stops the machine, is performed. A problem with the danger detection type control is that, as already suggested³⁾, if the state reaches a danger detection disabled stage, it leads to an accident immediately.

In safety education and training for workers, it should be observed strictly that the worker should follow the basic model and, if he encounters anything he does not understand, “he should immediately stop the production line, call for the person in charge, and wait until the safety is confirmed”¹⁰⁾. In reality, however, many companies instruct workers not to stop the production line as much as possible. This means that there is the asymmetric characteristic on the dangerous side. Safety education and training is to shift the asymmetric characteristic from the dangerous side to

the safe side (if the worker encounters anything beyond his control, he should stop the production line). This is not easy to do, and therefore education and training should be provided over and over again from the start of daily operation until the practice of doing so is imprinted on workers. Also, safety education and training should be provided before the start of operation, and this temporal order should be observed strictly. The limit of education and training causes an accident. Conventionally, the avoidance of danger seems to have been resorted to the attentiveness of workers, and machine designers seems to have not pursued the safety measures diligently. As aforementioned, because the non-regular employment of workers is progressional and the safety education is not provided sufficiently to them, such a design that at least irredeemable accidents are not be resorted to workers is required.

An accident occurs in an automatic production machine when its safety system for stopping the machine before the accident occurs fails to function. In the automatic production machine, the state in which the emergency stop button has to be pressed is, in itself, an abnormal state. Therefore, even if the worker fails to press the emergency stop button and an accident occurs, the worker should not be attributed to the accident. Even more, if the worker is reprimanded for hasty pressing of the emergency stop button, he will hesitate to press the emergency stop button and, as a result, an accident will occur. They say that some companies protect the operation buttons of the machine with covers against careless pressing. From the viewpoint of the asymmetric on the time-axis, however, while covering the start button is appropriate, covering the emergency stop button may cause delay to pressing and raise the predictability of an accident. If an enormous loss is caused by the hasty pressing of the emergency stop button, the reliability of both the automatic production machine and the protective measure should be improved not to allow the state that re-

quires the pressing of the emergency stop button to occur.

The failure in each control of the basic model is reviewed. The objective control of the automatic production machine is intended for manufacturing, and its failure is evaluated statistically as a management risk. To prevent this failure, the regulation control and the standby control are performed. These controls are based individually on the information from dangerous events. However, because failure in these controls is possible, these controls are evaluated as the reliability of the control function on the probability. Furthermore, because these controls are subject to failure and the emergency stop button is pressed ultimately, they are requested to be characterized that the worker is free from hesitation in an emergency case, and he should be permitted to perform hasty pressing by mistake as aforementioned. Therefore, including the safety education in the emergency stop operation, it is appropriate to evaluate the control failure not by the reliability but by the asymmetric on the time-axis. In sum, it is important for the safety education to be “able to take safe behavior whenever something not uncertain occurs”. Any failure in the emergency stop should not be attributed to the worker who pressed the emergency stop button but should be treated under insurance or the like as a management risk of the entire system.

According to ISO/IEC Guide51:1999¹¹⁾, the safety is defined as the state with no existence of unacceptable risk. In order for a worker to accept a risk, the harm should be sufficiently small or the worker can treat (control) the hazard adequately. If the treatment is easy, specifically if the push button or pilot lamp of the emergency stop equipment colored or shaped so as to be operated easily is available for use, operations more acceptable in terms of time will increase. Then, the safety education is to increase the acceptable operations by widening the treatable extent of the hazard. At that time, because the sufficient asymmetric on the time-axis cannot be assured only by the human attentiveness, it is requested to implement equipment measures in a hierarchy way.

There are “mistake which was too early”, and “overdue mistake”. The former stops production and generates a loss. Although it should be made not to be generated as much as possible, it generates rarely. By foreseeing the frequency of a mistake, it is possible to calculate the amount of a loss. The latter causes personal suffering. It ends with a light injury, becomes a fatal injury, or, in advance, does not understand. It produces in the difference in the little timing of a motion of a machine and a human being. It is difficult to calculate the amount of a loss. That

the amount of a loss is unreckonable has a large management risk. “Too early operation” and “overdue operation” have an asymmetrical risk on management.

Discussion

In the company of our country, regulation may not conform to the international standard. It was shown that man’s time characteristic is not taken into consideration by regulation of a company. People make a mistake. It is important to design a machine in consideration of the time characteristic when a mistake is made. By a lockout key system, unless the worker who entered in the fence by maintenance work returns all the members, it cannot start. It is the characteristic which is overdue in time. For this reason, in Japan, it is disliked and mistaken action, such as making a duplicate key, is performed. Using form of the key which cannot make a duplicate key, and the safety control which does not make a duplicate key make are required.

Now, a machine almost ceased to break down by high reliance design. People’s mistake decreased by education and training. The accident occurs in the rare trouble and the rare mistake. In this paper, the operation model of an automatic production machine was built and considered. The automatic production machine requires human operation mainly for starting and stopping. Safety problem lies in starting due to hasty operation and in stopping, particularly emergency stop, due to delay operation. From the viewpoint of safety, therefore, the importance of safety problem lies not in making an operation mistake but in how the mistake is made. The authors have shown that this characteristic can be expressed as the “asymmetric on the time-axis”, and based on this, the “asymmetric on the time-axis” is important as a characteristic required by the operation buttons (start button, emergency stop button) and the pilot lamps (normal condition, dangerous condition). Also for the safety education, the authors have shown that, rather than not making an operation mistake, it is important to pre-teach what action the worker should take considering the asymmetric on the time-axis when he becomes torn.

Generally, because humans make both hasty errors and delay errors, they may have an object error characteristic. As described above, however, the authors have shown that the asymmetry error characteristic may be given to humans depending on the characteristic of human interface. The category of structure classification specified in ISO 13849-1:2006¹²⁾, the international standard for functional

safety, is the category related to the resistibility against obstacles and the characteristic of the safety-related part of the control system over the subsequent behavior under the obstacle conditions. The configuration is evaluated highly not only for not allowing any defect to occur by improving the reliability of the configuration part but also for not allowing the defect occurrence to incur the loss of the safety function. Here, the loss of safety function is either “hasty start of movement” or “not stopping (delay of stopping)”, and can be expressed on the time-axis. In this way, the occurrence of defect in the functional safety can be evaluated by the asymmetric on the time-axis. Thereby, the man-machine system can be evaluated by the asymmetric on the time-axis as an index.

Loss caused by stopping the machine can be assumed. But, assumption is difficult to human harm. Management risk is large that it can not be assumed. To prevent accidents has to be stopped the machine. When delayed is to stop the machine, resulting in human harm. Fast and economic loss is to stop occurs. Both losses. Human harm is managerial in there is a possibility that irreversibly. It is also important managerial to stop before the accident.

Even if the best available protective measure is taken considering this characteristic, there is a limit that disables the transition of errors to the safe side. For the state beyond this limit, it should not be neglected as an unexpected state but measures of different characters should be taken in a hierarchical way or the like further to the utmost limit.

The automatic production machine brings a benefit to humans of releasing them from dangerous work and working in the detrimental environment. In consideration of this benefit, the manufacturer and the user conclude an agreement. In concluding an agreement, however, it is preferable that both parties should also agree on the remedy in case of accidents caused by the limit of protective measures. It is extremely difficult for them to make such agreement after the occurrence of an accident. Here again, the asymmetric on the time-axis is existing.

Risk-based safety is permitted between the parties of agreements (including social contracts), and harm to third persons is not permitted because the third persons are not involved in the procedure for concluding an agreement for accepting risks.

It is pointed out that the nuclear accident of TMI (Three Mile Island Nuclear Power Plant, USA) in 1979 was caused by the delayed perception of the dangerous event because the cooling pump stoppage was indicated by a green pilot lamp¹³. Probably, human characteristics were not reflected in the design of the machine plant. For the safety of machine equipment that may pose irreversible accidents to third persons including local residents, extremely high legitimacy may be required in comparison with that between the contracting parties.

References

- 1) Hoshi T, Ikeda H, Okabe K, Saito T (2012) Analysis of industrial accidents caused by industrial robots and proposal on amendment to regulations based on questionnaire Results. *Ind Saf Hyg Study* **5**, 3–15 (in Japanese with English abstract).
- 2) Ministry of Health Labour and Welfare (2010) Basic survey of industrial safety and hygiene (in Japanese).
- 3) Sugimoto N, Kumekawa S, Fukaya K, Shimizu N, Umezaki S, Ikeda H, Hoshi T, Futsuhara K (1988) Basic configuration of safety confirmation type safety, *The Japan society of mechanical engineers, Collection of Academic Papers (Vol. C)*, **54**: 2284–2292 (in Japanese with English abstract).
- 4) ISO13850 (2006) Safety of machinery – Emergency stop – Principle for design.
- 5) ISO 3864–1 (2011) Graphical symbols – Safety colours and safety signs – Part 1: Design principles for safety signs and safety markings.
- 6) IEC60204-1 (2009) Safety of machinery – Electrical equipment of machines – Part 1: General requirements.
- 7) Yamanaka T (1997) *Elements of chromatics*, 188, Bunkashobo Hakubundo, Tokyo (in Japanese).
- 8) The Color Science Association of Japan (2004) *Color science*, Asakura Publishing, 118–121 (in Japanese).
- 9) The Japan Machinery Federation (2012) IEC60204-1/JISB9960-1 Survey report on actual situation and intention of readers (in Japanese).
- 10) Furusawa N, “Practical safety activities for making workplaces vivid,” JISHA pocket edition (in Japanese).
- 11) ISO/IEC Guide51 (1999) Safety aspects—Guidelines for their inclusion in standards.
- 12) ISO13849-1 (2006) Safety of machinery—Safety related parts of control systems—Part 1: General principles for design.
- 13) Yanagida K (1983) *Horror 2 hours and 18 minutes*, 64–70, Bungeishunjusha, Tokyo (in Japanese).