Industrial Health 2010, **48**, 460–469 **Original Article**

Logical Consideration on Lockout and Trapped Key Interlock for Machine

Makoto KIMURA[1]* and Noboru SUGIMOTO[2]

[1]Environment & Safety Office, Showa Denko K.K., 1–13–9 Shibadaimon, Minato, Tokyo 105-8518, Japan
[2]Department of System Safety, Nagaoka University of Technology, 1603–1 Kamitomioka, Nagaoka, Niigata 940-2188, Japan

Received September 30, 2009 and accepted December 3, 2009

Abstract: "Lockout" is an important method for hazardous energy control to protect humans working at a place where they may be injured by unexpected release of hazardous energy. Actually, this administrative control is used in order to compensate for the incompleteness of the ZMS (Zero Mechanical State). This paper proposes the basic requirements for the "Lockout" used for machine maintenance work by applying the "principle of safety confirmation". In view of the above, the relation of "locking up the power switch in the OFF position", "withdrawing and possessing the key for hostage control" and "unlocking the movable guard for accessing to the working space " of the "trapped key interlock", which is alternative to "Lockout", should be made unate in terms of system. This paper formulates these interrelations, presents them in the form of interlock structure, and shows an example of configuration that can meet the required safety functions.

Key words: Industrial machine, Maintenance work, Lockout, Safety confirmation, Unate, ZMS, Trapped key interlock

Introduction

Hazards that may be posed during maintenance work are various including crush, entanglement, electric shock, fall, tumble and lack of oxygen. They cause industrial accidents. Meanwhile, the maintenance work is diversified. Many of them do not need any energy source. Therefore, among industrial accidents, there are quite a few that can be prevented if the energy source is cut off properly as a protective measure.

In the United State, Occupational Safety & Health Administration (OSHA) obligated the application of the "Zero Mechanical State (ZMS)[1, 2)]" to the maintenance work of newly installed industrial machines in 1990 in order to ensure the safety of their maintenance work. Here, the ZMS refers to the state in which the energy sources for those machines are cut off and thereby the potential energy are reduced, dissipated or controlled not to cause any injury to the maintenance operators. Also, in order to keep the ZMS during the maintenance work, OSHA requires the maintenance operator to lock up the energy isolating device before starting the maintenance work and possesses the key so that the energy isolating device and the machine cannot be operated[2)]. This is a kind of hostage control called "Lockout".

Although the "Lockout", which is a method of securing the safety in the maintenance work, is used to make up for the incompleteness of the ZMS, it has not been examined logically until now. For this reason, the matters to be considered on the design of the "Lockout" system have remained unclear, and the adequacy evaluation for the designed device has been difficult.

In view of the above, the authors study the basic requirements of the "Lockout" for the maintenance work by applying the "principle of safety confirmation[3)]" to the man-machine working system.

Also, the authors propose design requirements of the trapped key interlock shown in ANSI/RIA R15.06-1999[4)] and ANSI/ASSE Z244.1-2003[5)] as a method alternative to the "Lockout".

*To whom correspondence should be addressed.
E-mail: Makoto_Kimura@sdk.co.jp

Principle of safety confirmation

There is the "principle of safety confirmation" that "the safety can be recognized only through confirmation of the safety state. If the safety cannot be confirmed, the state should be regard as hazardous". This principle includes the interlock that "the hazardous action should be executed based on the safety confirmation and should not be executed if the safety cannot be confirmed". Figure 1[6] shows the relation that the hazardous action is excuted depending on the safety confirmation. The relation of "Safety state" and "Excution of the hazardous action" of Fig. 1 is (Safety state) ≥ (Excution of the hazardous action) when "Safety state" and "Excution of the hazardous action" are binary (0, 1) logic variables. This relation is called logically "unate" relation.

Two interlocks shown in Fig. 2[6] are designed for safety machine operation. The hazardous action for the machine is the operation itself of the machine, and the hazardous action for the human is the entry into the movable range of the machine. Each hazardous action is excuted depending on each safety confirmation. The machine confirms that there is no human in its movable range, and the human confirms that the machine is at a stop.

Composition of man-machine working system

Figure 3 shows the definition of the working space applicable to the maintenance work of press machines, industrial robots or a production system composed of multiple machines.

Firstly, as shown in Fig. 3(a), the working space in the "normal operation mode" is divided into "human space (H_S)" outside the motion space of the machine, "machine space (M_m)" with no human entry and "common working space" for both the human and the machine. The "common working space" is divided further into "human detectable space (S_S)" in which the machine can detect the human and "human undetectable space (S_D)" in which the machine cannot detect the human. It is supposed that the machine body is fixed to the "machine space (M_m)", the movable part of the machine moves between the "machine space (M_m)" and the "common working space (S_S, S_D)". It is also supposed that the number of humans is one and the human moves between the "human space (H_S)" and the "common working space (S_S, S_D)".

The "human undetectable space (S_D)" refers to, for example, the blind corner of the sensor for detecting a human body, the overhead space of the mat switch or the inside of the light curtain. Although the "human undetectable space (S_D)" should be eliminated in designing, it is impossible to do so from a practical point of view. Therefore, as shown in Fig. 3(a), it is configured

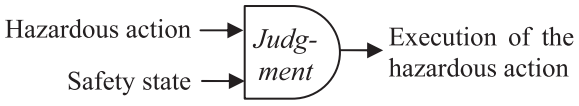


Fig. 1. The principle of safety confirmation[6].

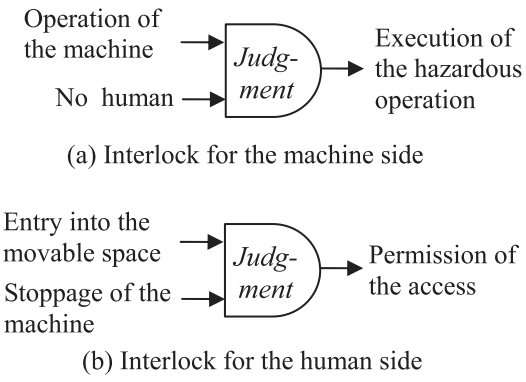


Fig. 2. Two interlocks for the machine and the human[6].

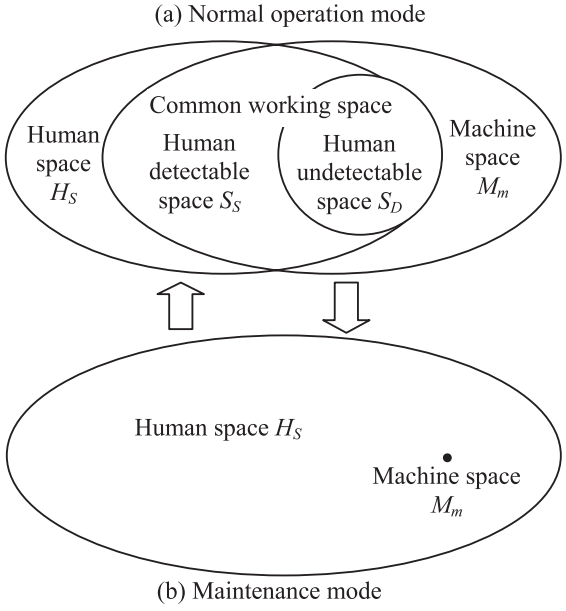


Fig. 3. Definition of the working space for the man-machine working system.

in such a manner that the human passes unexceptionally through the "human detectable space (S_S)" before entering the "human undetectable space (S_D)" and the body of the human passing through the S_S is detected and thereby the machine is stopped. In addition, the restart operation of the machine is executed by using the console panel provided in the "human space (H_S)" outside the joint working space.

In contrast, the working space of the "maintenance mode" can be defined as shown in Fig. 3(b). Since it is impossible for many maintenance work to regulate

the standard safety work and therefore it is uncertain to judge whether they are safe or hazardous, the best method that the system designer can employ in the design phase of the machine is to apply the ZMS. This is the true reason for the introduction of the ZMS by OSHA as afore-mentioned. In the sense that the machine in the ZMS has no movable space, the machine space is indicated in dots in Fig. 3(b). Once the ZMS is established, since all working spaces turns to the "human space (H_S)", no industrial accidents due to the energy of the machine occur at least in principle.

In this way, the working space structure is different between the normal operation mode and the machine maintenance mode, and the working space shifts according to the operation mode. In this paper, the maintenance work that requires energy source including the standard maintenance work to be performed in the normal operation mode is supposed to be a part of the normal operation work.

Safety Work in the Normal Operation Mode of the Machine

Since an industrial accident does not happen if the human and the machine are not in the same space, the following formula should be true for the human to operate maintenance work safely:

$$[H_S(t) \wedge M_S(t)] \vee [H_D(t) \wedge M_D(t)] = 0 \quad (1)$$

Where, the presence of the human in the joint working space (S_S) at the time t is expressed as $H_S(t) = 1$ or $\overline{H}_S(t) = 0$, and the absence of the human in the joint working space (S_S) at the time t is expressed as $H_S(t) = 0$ or $\overline{H}_S(t) = 1$. $H_S(t)$ is a binary (0, 1) logic variable, and the overbar symbol ($\bar{}$) means negation. Likewise, $H_D(t)$ expresses the presence of the human in the joint working space (S_D), $M_S(t)$ expresses the presence of the movable part in motion or ready for motion of the machine in the joint working space (S_S), and the presence of the movable part in motion or ready for motion of the machine in the joint working space (S_D) is expressed by the logic variable $M_D(t)$. The symbol ($\wedge$) expresses the logical AND operator, and the logical symbol ($\vee$) expresses the logical OR operator.

The first term of the equation (1) is realizable by configuring the system in such a way that the detection of the human body in the joint working space (S_S) causes the machine to stop. However, for the latter term of the equation (1), since there is no human detecting means in the human undetectable space S_D, the human detectable space S_S is designed so that the human can stop the machine and restarted in the human space (H_S) before entering the human undetectable space S_D as shown in Fig. 3(a).

The safety of the standardized maintenance work under the safety work standard is assured by realizing such man-machine working system. However, the safety of the human undetectable space S_D may be betrayed by a third person, i.e., there is a possibility that the third person restarts the machine erroneously when there is the human in the human undetectable space S_D. This erroneous operation is one of the reasonably foreseeable misuses defined in ISO12100-1[5].

Since the risk of the erroneous restart of the machine by the third person is unavoidable as long as the human undetectable space (S_D) remains, the system designer selects safety measures according to the results of risk assessment, such as providing an emergency stop button or the like in the human undetectable space (S_D), putting a warning tag against operation on the starter or introducing a Lockout device.

If a high risk is presumable, the adequate Lockout discussed below should be employed.

Safety Work in the Maintenance Mode of the Machine

Incompleteness of the ZMS

For risky nonstandard work, shutting down the energy is the most reliable safety measures for the system designer, which should be employed for as many maintenance operations as possible. On the other hand, it is also true that there are the following risky conditions as blind spots of the safety in the ZMS:

(1) The machine in operation cannot always stop immediately when the power supply is cut off. For example, it takes the roll in rotation several minutes to come to stop. Therefore, there are industrial accidents caused by contacting rolls remained rotating even after being de-energized.
(2) The maintenance operator was injured when a third person re-energized and restarted the machine erroneously.
(3) In the case of the group maintenance work, a serious accident was caused when the machine was re-energized and restarted while one of the maintenance operators still remained in the production system.

As exemplified above, the ZMS is configured by switching the operation mode from the normal mode to the maintenance mode. However, misuses that should be foreseen are possible in the mode switching. Therefore, the relation of ZMS and the maintenance work should be in logically unate relation. An interlock to counter these misuses related to the ZMS for realizing this relation is the Lockout.

This paper treats only the maintenance work to be performed after the machine stops completely on the assumption that the aforementioned hazardous state of (1), i.e., the hazardous state due to the inertia of the machine immediately after the machine is de-energized is pursuant to IEC60204[7].

Locked ZMS

Basically, the machine state is divided into the state in which energy is being supplied (hereinafter referred to as "energized state") and the state in which energy is being not supplied (ZMS). In this paper, since the lockout plays an important role in the relation of ZMS and the maintenance work as stated above, the authors add the new mechanical state, locked ZMS, in which energization by a third person is blocked as third mechanical state. The locked ZMS is also called "Maintenance Mechanical State (MMS)[8]". (hereinafter "locked ZMS" is referred to as "MMS")

Also, assuming the following four state-to-state transitions (i) through (iv) as respectively identical to (i) through (iv) shown in Fig. 4, the authors consider hazardous misuses foreseeable in such transitions.

(i) Transition from the energized state to the ZMS, such as de-energizing operation with the energy isolation device.
(ii) Transition from the ZMS to the MMS, such as locking operation for the energy isolation device in the OFF position.
(iii) Transition from the MMS to the ZMS, such as unlocking operation for the locked isolation device.
(iv) Transition from the ZMS to the energized state, such as power activating operation for the power switch.

Role of the human in the Lockout system

Generally, the power switch of the machine functions to receive the instantaneous intention of the human and maintain such human intention. For example, to energize the machine, setting the power switch from the OFF position to the ON position by the human is an instantaneous human operation, and the ON position of the power switch is maintained until the human or some other human sets the power switch from the ON position to the OFF position (self-hold circuit).

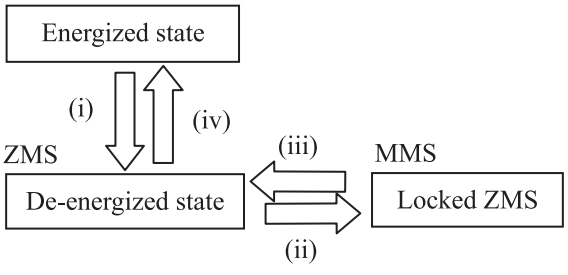


Fig. 4. Mechanical states and state-to-state transition.

When the machine runs in the normal operation mode, the machine always checks whether it has satisfied the safety state ($H_S(t) = 0$ of the equation (1)) or not, and starts or continues its operation only when the machine confirms its satisfaction of the safety state. This indicates that the machine confirms the safety on its own and determines its operation. For this reason, unlike the so-called operation start (activation), this power activating operation activates the safety device of the machine and leaves the subsequent safety confirmation to the machine.

Therefore, prior to leaving the safety confirmation to the machine, the human should adapt the work space to the initial conditions (the safety state of the machine with no human in the spaces S_S, S_D and M_m in the normal operation mode) to make the safety device effective and functional. This preparatory work is a role to be played by the human. When the machine is confirmed to be in the safe state and energized, the confirmation of the safety state of the equation (1) is taken over to the machine, and the safety state is maintained.

For example, prior to energizing the machine, the presence of no human in the "machine space (M_m)" and the "human undetectable space (S_D)" is confirmed by the human, the protective door of the machine is closed, and then the machine is permitted to be energized. Then, the safety switch of the protective door (safe in the closed position) can be monitored effectively. The safety confirmation by the human is taken over to the safety switch of the protective door, and thus the initial safety state is maintained.

In the maintenance mode, the safety confirmation cannot be left to the machine. Since the machine is in the ZMS, the human itself should confirm whether he is in the safety state ($M_S(t) = 0$ due to the ZMS) and start or continue his maintenance work ($H_S(t) = 1$) according to the confirmation results. However, since the human cannot keep confirming the safety due to the limit to his ability, an alternative method similar to the above should be created. That is, the human should set initially the safety conditions for maintenance work, activate a safety device of some sort, and have the safety device to take over the duty to maintain the safety confirmation.

The above safety conditions of the maintenance work are satisfied by the ZMS, where the role of the safety device is to block erroneous energy supply by a third person. While the human should have the safety device maintain the safety confirmation, possessing the key by the human corresponds to the continuous safety con-

firmation in the Lockout system. A series of preparatory work consists of realizing the ZMS before starting the maintenance work, preventing erroneous energizing operation. Maintaining the de-energized state is also a role of the human.

Safety ensuring for solitary maintenance work

When binary logic variables are used, the state in which the machine is in the ZMS at the time t is expressed as $ZMS(t) = 1$, and the state that the machine is in the MMS is expressed as $MMS(t) = 1$ and the state in which the human is in the maintenance work space is expressed as $H(t) = 1$, the conditions for safety maintenance work can be expressed as follows:

$$ZMS(t) \geq MMS(t) \geq H(t) \tag{2}$$

Where

$$ZMS(t) = \overline{I(E_{ON})}_h \,|\, I(E_{OFF})_t \tag{3}$$

$$MMS(t) = \overline{I(L_{UL})}_h \,|\, I(L_L)_t \tag{4}$$

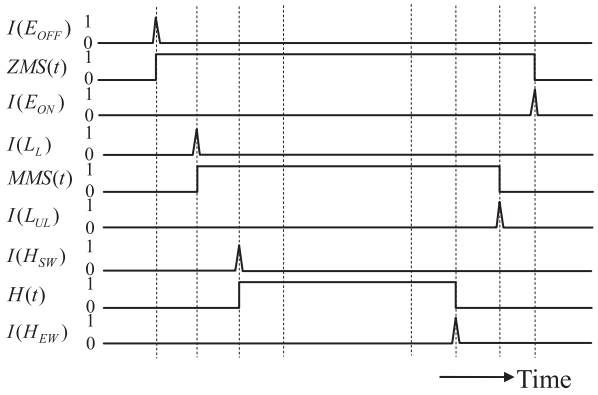
$$H(t) = \overline{I(H_{EW})}_h \,|\, I(H_{SW})_t \tag{5}$$

The logical inequality (2) provides unate logical relation in which the machine cannot be shifted to the MMS unless it is in the ZMS and that the human cannot start the maintenance work unless the machine is in the MMS.

On the other hand, the negation of the inequality (2) using De Morgan's laws provides also the procedure for energizing operation to be performed after the maintenance work, that is the MMS cannot be canceled unless the human exits from the working space and the ZMS cannot be canceled, i.e., the machine cannot be energized unless the MMS is canceled.

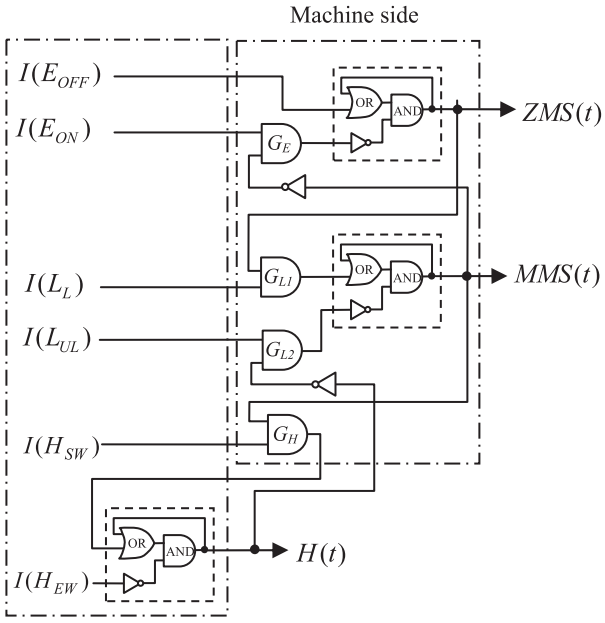
Here, $[B]_h \,|\, [A]_t$ is a logical function for data holding expressing that A=1 triggers the output of the value of B (1 if B=1) and maintains the output value until B=0 becomes true. In case of the equation (3), the equation means that $ZMS(t)$ turns to 1 when $I(E_{OFF}) = 1$ and turns to 0 when $I(E_{ON}) = 1$. I(content) expresses the momentary behavioral intention of the human, $I(E_{ON})$ expresses the energizing operation, $I(E_{OFF})$ expresses the de-energizing operation, $I(L_L)$ expresses the blocking operation (e.g., locking the power switch in the OFF position by using a padlocking) $I(U_L)$ expresses the unblocking operation, and $I(H_{SW})$ expresses the work starting intension, $I(H_{EW})$ expresses the work ending intension. These six different behavioral intentions of the human are supposed not to occur at the same time.

The inequities (2) through (5) are basic requirements for realizing the safety maintenance work. Figure 5 shows the time chart of these logic variables, and Fig. 6 shows the interlock model that can satisfy the basic safety requirements mentioned above.



$I(E_{OFF})$: Initiation of de-energizing
$ZMS(t)$: ZMS (1: ZMS)
$I(E_{ON})$: Initiation of energizing
$I(L_L)$: Initiation of locking energy isolation device
$MMS(t)$: MMS (1: MMS)
$I(L_{UL})$: Initiation of un-locking energy isolation device
$I(H_{SW})$: Initiation of maintenance work
$H(t)$: State of the maintenance work (1: working)
$I(H_{EW})$: Initiation of closing maintenance work

Fig. 5. Time chart of the ideal sequence of the safety maintenance work.



$ZMS(t)$: Zero Mechanical State
$MMS(t)$: Maintenance Mechanical State
$H(t)$: Human in the workspace
$I(\,)$: Initiation

Fig. 6. Interlock model of the maintenance work.

The logical function for data holding is expressed by using flip-flops (logical AND operator, logical OR

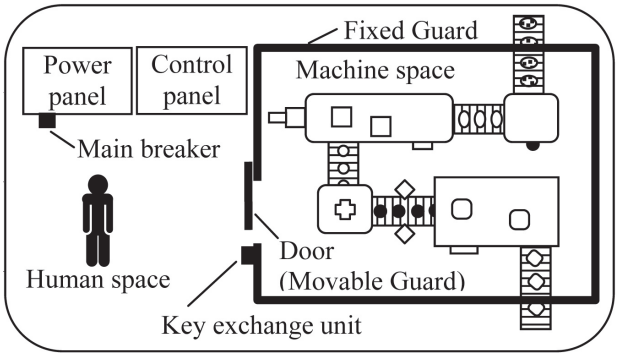


Fig. 7. Example of the maintenance working system.

operator and logical NOT operator framed in by broken lines). The logical AND operator G_E expresses the interlock for allowing to energize the machine in the block-canceled state ($MMS(t) = 0$), G_{L1} expresses the interlock for having the blocking operation performed in the ZMS ($ZMS(t) = 1$), G_{L2} expresses the interlock for having the blocking-canceling operation performed in the state in which there is no human in the maintenance working space ($H(t) = 0$), and G_H expresses the interlock for having the maintenance work started in the MMS ($MMS(t) = 1$).

Trapped Key Interlock

Safety requirements

Based on the above description, this section considers the requirements for the trapped key interlock.

The trapped key interlock is applied to such a working space as shown in Fig. 7 having no common working space of Fig. 3(a). This working space is enclosed by the fixed guard. To enter the machine space, it is necessary to pass through the dedicated movable guard. The control panel operating board and power panel of the machine are provided in the human space outside the fixed guard.

Figure 8 shows the general procedure for using the trapped key interlock. The system consists of a mechanism of locking when the power switch (main breaker) is in the OFF position (OFF-lock), a key exchange unit for exchanging the key for OFF-lock (Key-1) and the key for controlling the hostage (Key-2) with each other by using the holder for trapping the keys (Trap-1, Trap-2), and a lock-bolt for locking the movable guard as shown in Fig. 9 (Lock-bolt). The key (Key-1) is common between the OFF-lock and the Trap-1. The Key-1 can be withdrawn only when the main breaker is in the OFF position. Either the Key-1 for OFF-lock or the Key-2 for hostage control can be withdrawn from the key exchange unit.

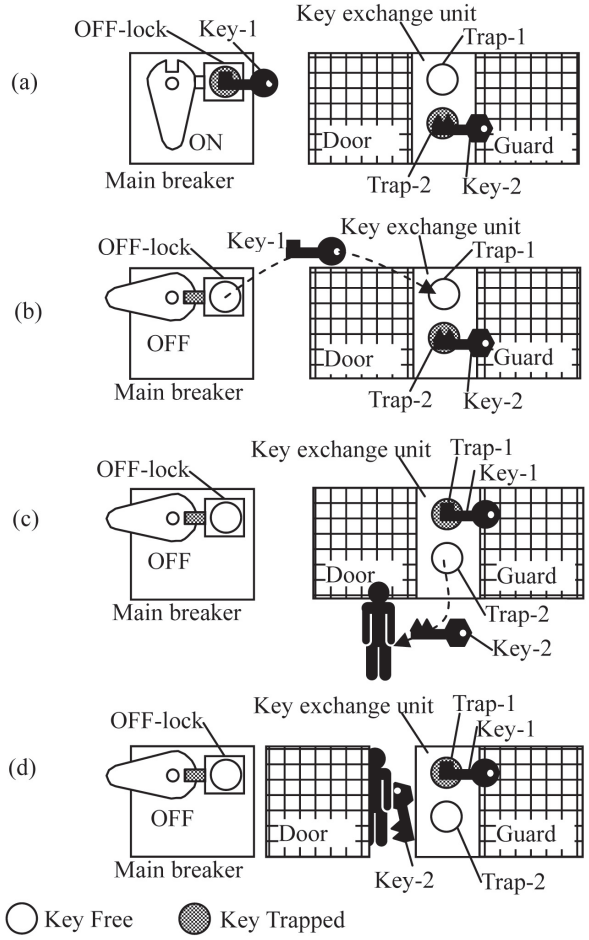


Fig. 8. Trapped key interlock system.

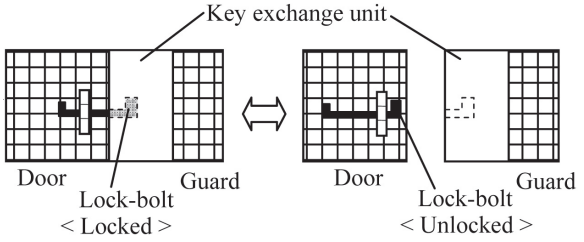


Fig. 9. Example of the lock bolt.

Figure 8(a) shows the state in which the movable guard is closed and the power supply is ON (energized) and the machine inside the guard is ready for start-up at any moment. For starting the maintenance work, the human enters entering the guard in the following procedure:

Firstly, the human turns off the main breaker, withdraws the Key-1, and then inserts the Key-1 into the Trap-1 of the movable guard. The Key-2 can be withdrawn when the Key-1 is trapped by the Trap-1. After that, the Key-2 is withdrawn from the Trap-2 as shown in Fig. 8(c). Then, the human withdraws the lock-

bolt, unlocks the movable guard, and enters the working space (machine space) with the Key-2 in his hand as shown Fig. 8(d).

To turn ON the main breaker after the completion of the maintenance work, the above procedure is reversed. The movable guard is locked by the lock-bolt, the Key-2 is inserted into the Trap-2, the Key-1 is withdrawn from the Trap-1, the OFF-lock is canceled by the Key-1, and lastly the main breaker is turned ON and the state of Fig. 8(a) is resumed. Such interlock for restricting the procedure by trapping the keys is called "trapped key interlock".

In the trapped key interlock treated in this paper, possessing the Key-2 is corresponding to the continuous safety confirmation of the basic requirements for the above-described safety maintenance work. Therefore, it is necessary to configure an interlock mechanism that does not permit the human to enter the working space unless he takes along the Key-2. Since the equalities $ZMS(t) = 1$ and $MMS(t) = 1$ of the inequality (2) are true when the main breaker is turned OFF and the Key-1 is withdrawn, the inequality $MMS(t) \geq H(t)$ should be established by using the key exchange unit and the lock-bolt that should be attached to the movable guard. Specifically, the following logical inequality should be established:

$$K1_I(t) \geq K2_D(t) \geq LB_U(t) \geq D_o(t) \tag{6}$$

Where,

$$K1_I(t) = \overline{I(K1_D)}_h \,|\, I(K1_I)_t \tag{7}$$

$$K2_D(t) = \overline{I(K2_I)}_h \,|\, I(K2_D)_t \tag{8}$$

$$LB_U(t) = \overline{I(LB_L)}_h \,|\, I(LB_U)_t \tag{9}$$

$$D_O(t) = \overline{I(D_C)}_h \,|\, I(D_O)_t \tag{10}$$

The logical inequality (6) expresses the unate logical relation in which the Key-2 should be able to be withdrawn from the Trap-2 ($K2_D(t) = 1$) on condition that the Key-1 is inserted in the Trap-1 ($K1_I(t) = 1$), the lock-bolt should be able to be unlocked ($LB_U(t) = 1$) on condition that the Key-2 is withdrawn, and the movable guard should be able to be opened ($D_O(t) = 1$) on condition that the lock-bolt is unlocked.

The equation (7) expresses that the operation of inserting the Key-1 into the Trap-1 ($I(K1_I) = 1$) triggers off the change of the value of $K1_I(t)$ to 1 and this value remains unchanged until the Key-1 is withdrawn from the Trap-1 ($I(K1_D) = 1$).

The equation (8) expresses that the operation of withdrawing the Key-2 from the Trap-2 ($I(K2_D) = 1$) triggers off the change of the value $K2_D(t)$ to 1 and this value remains unchanged until the Key-2 is inserted into the Trap-2 ($I(K2_I) = 1$).

The equation (9) expresses that the operation of unlocking the movable guard using lock-bolt ($I(LB_U) = 1$) triggers off the change of the value $LB_U(t)$ to 1 and this value remains unchanged until the movable guard is locked ($I(LB_L) = 1$).

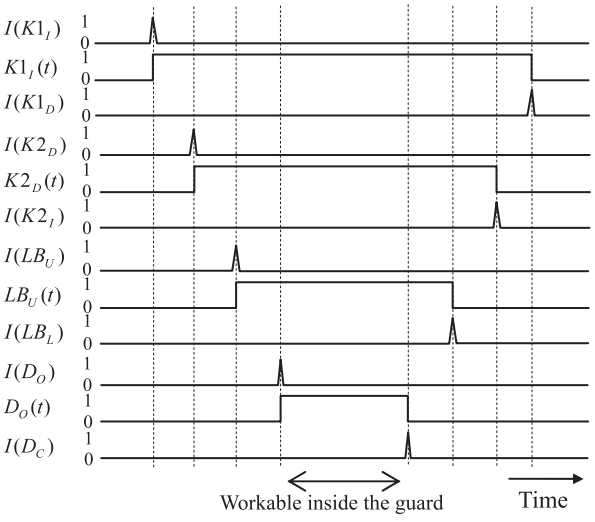
The equation (10) expresses that the operation of opening the movable guard ($I(D_O) = 1$) triggers off the change of the value $D_O(t)$ to 1, and this value remains unchanged until the movable guard is closed ($I(D_C) = 1$).

Figure 10 shows the time charts of these logic variables.

The OFF-lock mechanism of the power switch and the logical expressions (6) through (10) are safety requirements of the trapped key interlock system.

Figure 11 shows the interlock model satisfying the logical expressions (6) through (10) by means of the Key exchange unit, Lock-bolt and Movable guard.

Here, the logical AND operation G_{K1D} expresses the interlock against the withdrawal of the Key-1 ($I(K1_D) = 1$), which is subject to the untrapped state of the Key-1 ($K1_T(t) = 0$). (The "untrapped state" is the



$I(K1_I)$: Initiation of inserting the Key-1
$K1_I(t)$: State of the Key-1 (1: Inserted to Trap-1)
$I(K1_D)$: Initiation of drawing the Key-1
$I(K2_D)$: Initiation of drawing the Key-2
$K2_D(t)$: State of the Key-2 (1: Drawn from Trap-2)
$I(K2_I)$: Initiation of inserting the Key-2
$I(LB_U)$: Initiation of unlocking the door
$LB_U(t)$: State of the Lock-bolt (1: Unlocked)
$I(LB_L)$: Initiation of locking the door
$I(D_O)$: Initiation of opening the door
$D_O(t)$: State of the door (1: Opened)
$I(D_C)$: Initiation of closing the door

Fig. 10. Time chart of the ideal constraint operation of the key exchange unit the lock-bolt and the movable guard for trapped key interlock system.

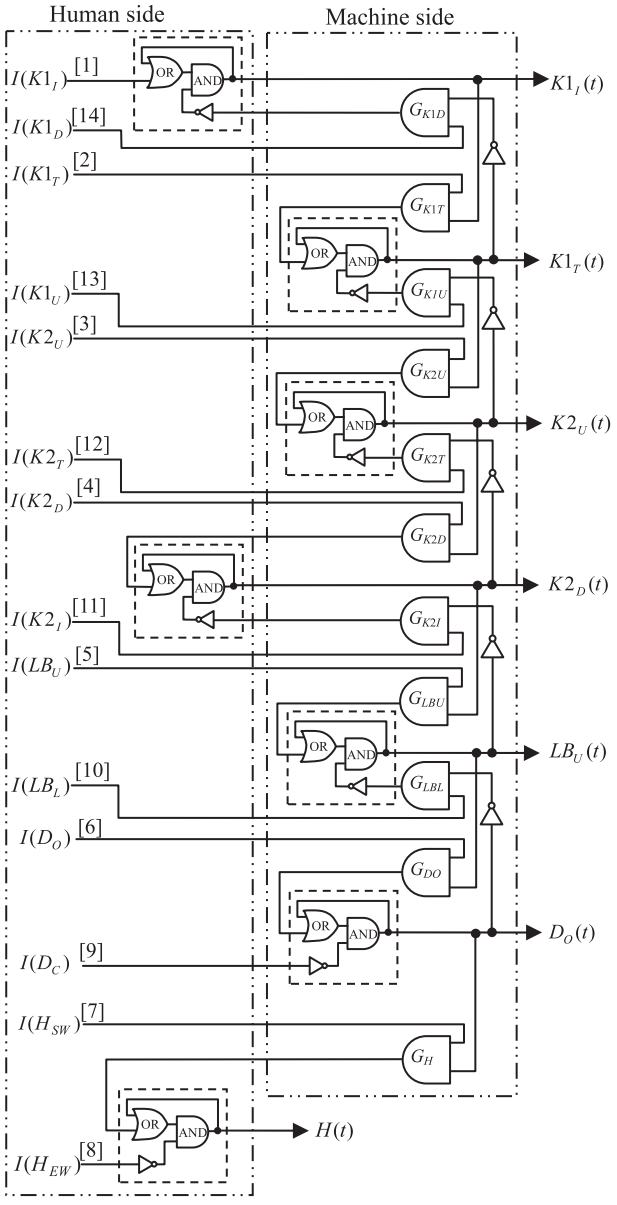


Fig. 11. Interlock model of the ideal trapped key interlock (key exchange unit, lock-bolt and movable guard).

state in which the key can always be withdrawn and the key is just inserted in the keyhole and generally cannot be withdrawn when the key is turned.) Similarly, G_{K1T} is the interlock against the trapping of the Key-1 ($I(K1_T) = 1$), which is subject to the inserted state of the Key-1 ($K1_I(t) = 1$), G_{K1U} is the interlock for the untrapping of the Key-1 ($I(K1_U) = 1$), which is subject to the inserted state of the Key-2 ($K2_T(t) = 1$), G_{K2U} is the interlock for the untrapping of the Key-2 ($I(K2_U) = 1$), which is subject to the trapped state of the Key-1 ($K1_T(t) = 1$), G_{K2T} is the interlock against the trapping of the Key-2 ($I(K2_T) = 1$), which is subject to the inserted state of the Key-2 ($K2_D(t) = 0$), G_{K2D} is the interlock against the withdrawal of the Key-2 ($I(K2_D) = 1$), which is subject to the untrapped state of the Key-2 ($K2_U(t) = 1$), G_{K2I} is the interlock against the insertion of the Key-2 ($I(K2_I) = 1$), which is subject to the locked state of the movable guard ($LB_U(t) = 0$), G_{LBU} is the interlock against the unlocking of the movable guard ($I(LB_U) = 1$), which is subject to the withdrawn state of the Key-2 ($K2_D(t) = 1$), G_{LBL} is the interlock against the locking of the movable guard ($I(LB_L) = 1$), which is subject to the closed state of the movable guard ($D_O(t) = 0$), G_{DO} is the interlock against the opening the movable guard ($I(D_O) = 1$), which is subject to the unlocked state of the movable guard ($LB_U(t) = 1$), and G_{HS} is the interlock against the work starting ($I(H_{SW}) = 1$), which is subject to the opened state of the movable guard ($D_O(t) = 1$).

Since the state with the Key-1 or the Key-2 withdrawn is maintained by the possession of the key by the withdrawer, the self-holding function depends on the human side. Incidentally, the numbers [1] through [14] of Fig. 11 show the interlock-induced operational sequence.

The designer of the trapped key interlock should design it in such a way that the interlock model of Fig. 11 is embodied. Especially, as described above, it is the linchpin of maintaining the MMS to have the human possess the Key-2. Therefore, among all requirements expressed by the equations (6) through (10), the following two design points are the most important:

(1) The movable guard cannot be unlocked unless the Key-2 is withdrawn from the Trap-2.
(2) The Key-2 cannot be inserted into the Trap-2 unless the movable guard is locked.

Example of the device configuration

This paper proposes a simply-structured trapped key interlock that can satisfy the safety requirements by using a combination of two movable structures partly sharing the movable space. Due to sharing the common space, when one structure occupies the common space, the other structure cannot use the common space. (Hereinafter, this configuration is called “common space occupying type mechanical interlock”).

Figure 12 shows the concept of the trapped key interlock using the “common space occupying type mechanical interlock”, and Fig. 13 shows the positional relation among the movable guard, the lock-bolt and the Key-2. For the slide door to be opened to the right, the key exchange unit is usually installed on the left side of the slide door but it is installed on the right side of the slide door in this proposal. The lock-bolt locks the movable guard when it passes though both the fixed guard and the movable guard. When the movable guard is open, it blocks the way of the lock-bolt not to move

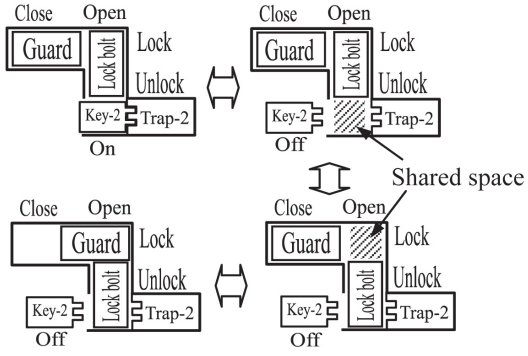


Fig. 12. Concept of the relation between the Key-2 and the Lock bolt.

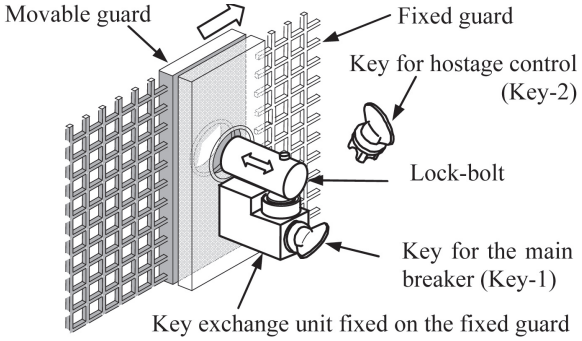


Fig. 13. Concept of the new trapped key interlock for slide door.

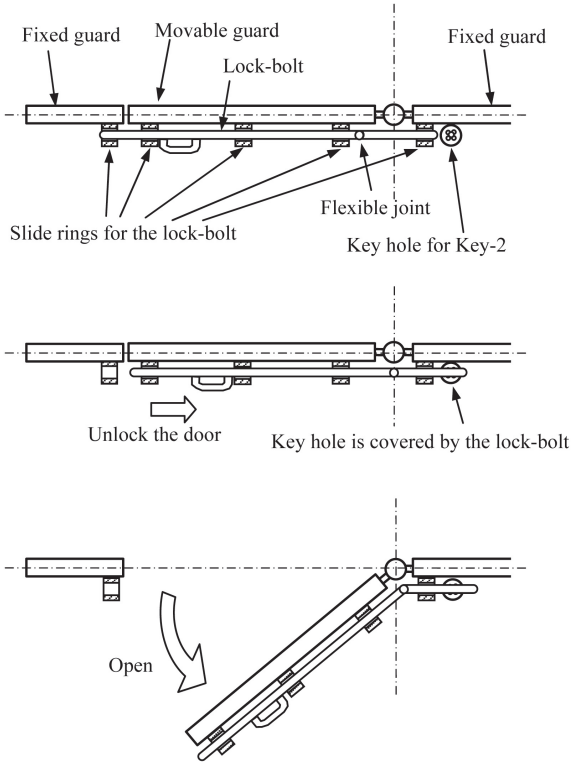


Fig. 14. Concept of the new trapped key interlock for hinged door (Key-1, Key2 and the body of Key exchange unit are omitted).

to its locking position. On the other hand, the Trap-2 is laid out in such a way that the space created when the lock-bolt moves from the unlock position to the lock position and the space for inserting the Key-2 into the key exchange unit overlap with each other. When the Trap-2 is laid out in this way, the Key-2 cannot be inserted into the Trap-2 while the movable guard is open. This concept can be used for the hinged door, if the design of lock-bolt is changed as Fig. 14.

Additionally, the lock-bolt is cylindrical in Fig. 13, but when its top plane area is made smaller, it is difficult to leave the Key-2 on the key exchange unit. This induces the human to possess the Key-2 by itself.

Conclusion

The International Standard ISO12100-1:2003 (Safety of machinery —Basic concepts, general principles for design—)[9] stipulates that the intended use shall be clarified between the manufacturer (designer) and the user and that risk assessment shall be conducted for reasonably foreseeable misuses deviated from the intended use and the adequate risk reduction by taking the necessary safety measures.

In this paper, the authors presented the safety requirements for the machine maintenance work in the ZMS by applying the "principle of safety confirmation", the safety requirements for the trapped key interlock, and the following two design points:

(1) The movable guard should be designed so that it cannot be opened unless the key for hostage control is withdrawn.
(2) The key for hostage control should be designed so that it cannot be inserted into the key exchange unit unless the movable guard is locked.

The trapped key interlock serves many uses as a hostage control device that requires no electric wiring. However, it has a drawback that its hostage control is apt to be invalidated if the key for the hostage control is left behind. In order to solve this drawback, the authors also presented the trapped key interlock using the common space occupying type mechanical interlock.

In the opinion of the authors, the example of the trapped key interlock shown in Fig. 13 and Fig. 14 can presumably be manufactured economically with no requirement of advanced technique or high manufacturing costs for commercialization and contribute to the improvement of the safety in the industrial fields. Also in the opinion of the authors, the "common space occupying type mechanical interlock" is useful for the

designer to devise a new mechanical interlock.

However, the examples shown in Fig. 13 and Fig. 14 are not yet complete with no inhibiting effect against the leaving of key on the floor or the attachment of a hook to the fixed guard for hanging the key, for example. Such inhibiting behavior should be left to the machine users.

Therefore, it is needless to say that the designer is required to explain to the machine users that the possession of the key for hostage control is the most important for the safety machine maintenance work through the description of the instruction manual and obtain their understanding.

References

1) ANSI Z241.1 (1999) Safety requirements for sand preparation, molding and coremaking in the sand foundry industry. American National Standards Institute, Washington, DC.
2) OSHA 29 CFR 1910.147 The control of hazardous energy (lockout/tagout). U.S. Department of Labor Occupational Safety & Health Administration, Washington, DC.
3) Sugimoto N, Futsuhara K, Mukaidono M (1987) The principle and logical structure of safety in man-machine system. Trans Inst Elect Eng Jpn **107-D-9**, 1092–8.
4) ANSI/RIA R15.06 (1999) Industrial robots and robot systems - safety requirements, American National Standards Institute, Washington, DC.
5) ANSI/ASSE Z244.1 (2003) Control of Hazardous energy Lockout/Tagout and alternative methods, American National Standards Institute, Washington, DC.
6) Sugimoto N (2009) Globally harmonized safety imposed on responsible engineers. J Jpn Soc Prec Eng **75-9**, 1045–9.
7) IEC 60204-1 (2005) Safety of machinery — Electrical equipment of machines - Part 1: General requirements, International Electrotechnical Commission, Geneva.
8) Kimura M, Sugimoto N (2009) Logical Consideration on Energy Isolation and Lockout for Machine. Trans Jpn Soc Mech Eng C **75-752**, 1201–8.
9) ISO12100-1 (2003) Safety of machinery - Basic concepts, general principles for design - Part 1: Basic terminology, methodology. International Organization for Standardization, Geneva.