Journal of Traffic and Transportation Engineering 6 (2018) 241-254
doi: 10.17265/2328-2142/2018.05.004

Safety Assessment of Closed-Loop Level Crossing Control Systems by Means of STAMP (Systems-Theoretic Accident Model and Processes)

Tetsuya TAKATA[1], Akira ASANO[1] and Hideo NAKAMURA[2]

1. Kyosan Electric Mfg. co., Ltd, Yokohama 230-0031, Japan

2. The University of Tokyo, Chiba 277-8561, Japan

Abstract: There have been a large number of accidents at level crossings of railways and this has been considered to be a significant issue to be solved for the realization of safe and stable railway transport. A conventional level crossing control system is characterized by the use of two types of electronic train detectors; one detects a train approaching to a level crossing section and the other then detects the train having left the level crossing. By contrast, closed-loop level crossing control systems in which level crossing control equipment and train-borne equipment communicate with each other have been advocated and are expected to serve as an effective solution to the abovementioned issue. This paper describes the following three types of closed-loop level crossing control systems: decentralized level crossing control system, fully-centralized comprehensive level crossing control system and fully-centralized individual level crossing control system. This paper then assesses the safety of these systems in comparison to the conventional level crossing control system. For the purpose of the assessment of their safety, a new accident analysis model called STAMP (systems theoretic accident model and processes) that is suitable for software intensive systems is used to clarify the advantage of the proposed three types of level crossing control systems in terms of safety.

Key words: Level crossing control, railway signaling, closed loop control method, safety assessment, STAMP.

1. Introduction

The Act for Partial Revision of the Act on Promotion of Railway Crossings was enacted on March 31, 2016. This act provides a framework for road administrators, railway operators and local parties concerned to jointly examine specific countermeasures against dangerous level crossings or those that tend to cause traffic congestion, both of which are to be designated as such by the Minister of Land, Infrastructure, Transport and Tourism.

Since 2006, the number of accidents involving road vehicles etc. at level crossings has been decreasing. Nevertheless, there are still more than 200 accidents of that kind every year, most of which occur at class-1 level crossings equipped with protection devices such as level crossing alarms.

Corresponding author: Tetsuya Takata, B. Engineering, research field: railway signaling.

This situation implies that further technological development of level crossing protection equipment is required in order to improve safety in level crossing control, hence a practical study on such development is expected. This paper clarifies problems in the conventional level crossing control system and, as solutions to those problems, demonstrates the effectiveness of closed-loop level crossing control systems in which level crossing control equipment and onboard equipment of trains can communicate with each other to achieve level crossing control. The closed-loop level crossing control systems are classified by different control methods into the following two types; one is decentralized control system in which control equipment is distributed locally along the trackside, and the other is centralized control system in which control equipment is centralized in the control center. The centralized

control system is further divided into fully-centralized comprehensive control system and fully-centralized individual control system; the former manages all the relevant level crossings comprehensively from a central processing block by notifying each level crossing between stations of the expected time at which a target train will pass it and keeping the information updated according to the travel of the train, while the latter performs centralized control when there is a level crossing in a section within which the train is allowed to move.

This paper assesses these three types of closed-loop level crossing control systems in terms of their effectiveness and especially safety, by comparing them with the conventional level crossing control system.

The majority of level crossing control systems of today, including the abovementioned conventional system, are computer-controlled systems that rely on software for the control logic. Until recently, there was no effective method of assessing safety of software systems and FTA (Fault Tree Analysis) and FMEA (Failure Mode and Effect Analysis) have thus been used as mainstream safety analysis methods. On the other hand, a new accident model based on system theory, called STAMP (systems theoretic accident model and processes), has been spotlighted as being effective for software-intensive systems. There have been many reports on merits of STAMP such as its completeness in identifying HCFs (hazard causal factors). This paper extends the methodology of STAMP, which is generally applied to qualitative safety assessment, to quantitative safety assessment. To be more precise, the authors have assessed the safety of those systems in a quantitative manner by linking statistical data on the past level crossing accidents with the result of a STAMP analysis. This paper describes how the abovementioned four different types of level crossing control systems including the conventional one are assessed based on the extended STAMP methodology.

2. Different Types of Level Crossing Control Systems to Be Compared

This chapter introduces control principles of the different types of level crossing control systems subject to the safety assessment.

(1) Conventional level crossing control system [1]

Fig. 1 shows a level crossing control system for single-track sections that require a complicated control mechanism. One level crossing is provided with two electronic train detectors for activating level crossing control using a short track circuit; they are placed in contraposition to each other across the level crossing (one is for up trains and the other for down trains). When an up or down train enters the level crossing section by passing a corresponding detector and triggers a level crossing alarm, the function of the opposite detector beyond the level crossing has to be masked. Meanwhile, one more electronic train detector for deactivating level crossing control is also used for the level crossing in order to stop the alarm and raise the level crossing barrier. In addition, the following types of equipment are also installed at level crossings: obstacle detection equipment that detects an obstacle such as a road vehicles tuck on the level crossing and an obstruction warning device that warns a train driver of any obstacle detected to urge him/her to stop the train immediately.

As described above, in the conventional level crossing control system, wayside level crossing control equipment detects trains and executes required processing, and an obstruction warning device warns a train crew of any imminent danger; this means the whole level crossing control process is completed only by wayside equipment. However, the conventional system involves some negative aspects. In particular, a train collision cannot be avoided if a train crew misses a warning from an obstruction warning device of any obstacle detected. Moreover, the length of time from alarm activation to train arrival at the level crossing can

vary considerably because the conventional system starts level crossing control when a train reaches a specified point regardless of its speed.

In order to overcome these disadvantages and control level crossings effectively, not only the location but also the speed of trains should be taken into account in level crossing control, hence the closed-loop level crossing control systems which enable communication between onboard equipment and level crossing control equipment is expected. The following sections detail the proposed three types of closed-loop level crossing control systems.

(2) Decentralized level crossing control system

A decentralized closed-loop level crossing control system has been developed and in operation as part of ATACS (advanced train administration and communications system), which was introduced to Senseki Line of East Japan Railway Company as the first radio train control system of Japan. The system has been reportedly successful in actual service and helpful in shortening and equalizing the alarm duration [2].

In ATACS, a local controller on the trackside is informed of the location and speed of a train running within the area under the control of the controller by onboard equipment of the train and then notifies the onboard equipment of a movement authority limit for the train. The onboard equipment in turn creates a speed profile based on the given movement authority limit in order to protect the train. Basically, a movement authority limit for a train is set at a certain point behind its preceding train with a safety margin added. However, if there is a level crossing between the train and the set movement authority limit, the limit is moved to another point before the level crossing. When a train is approaching the level crossing, an order for alarm activation is transmitted to the level crossing control equipment via a local controller and then the train is allowed to move beyond the level crossing after the level crossing control equipment informs that the level crossing barrier has been completely lowered and there is no obstacle on the level crossing. If the communication between wayside and onboard equipment fails or any obstacle is detected, the train stops before the level crossing according to the speed profile which has been created as described above.

In contrast to the decentralized control method with processing equipment distributed along the trackside, it has been made possible to centralize logic processing block thanks to the recent progress in networking and communication technology. Two different types of centralized systems are proposed as described below:

(3) Fully-centralized individual level crossing control system

This system centralizes the functions which the decentralized level crossing control system performs locally such as tracking trains and setting and communicating their movement authority limit. It initially sets a movement authority limit for a train at a point in front of a level crossing and, once complete closing of the level crossing barrier and absence of an obstacle on the level crossing are confirmed, moves the movement authority limit to a farther point beyond the level crossing. In this way, this system can link level crossing control to train protection. This system is intended to centrally control level crossings that appear on the route of a running train one by one according to its travel. This control method is basically the same as that of the decentralized control system. However, this type of centralized control system can control the passage of all trains through level crossings collectively, hence group control of trains as well as improvement of the level crossing control function become possible.

(4) Fully-centralized comprehensive level crossing control system

This system was originally proposed during testing of DMV (dual mode vehicles) that were designed as a new-type transport means running both on railway tracks and roadways. As depicted in Fig. 2, level crossing control equipment is controlled based on the train location information managed by the central processing equipment.

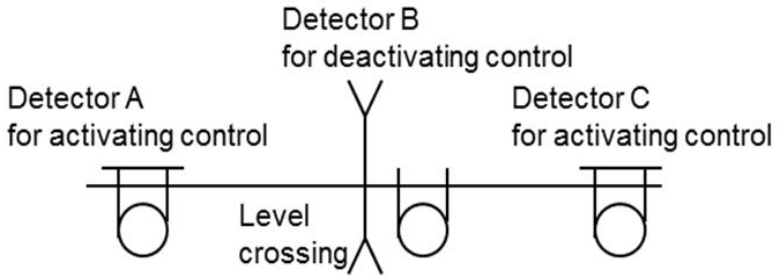

Fig. 1 The structure of the conventional level crossing system.

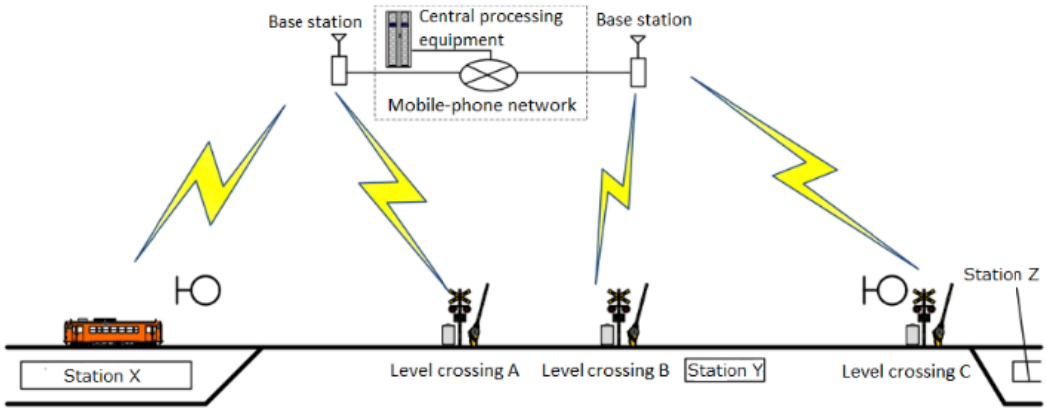

Fig. 2 Fully-centralized comprehensive level crossing control system.

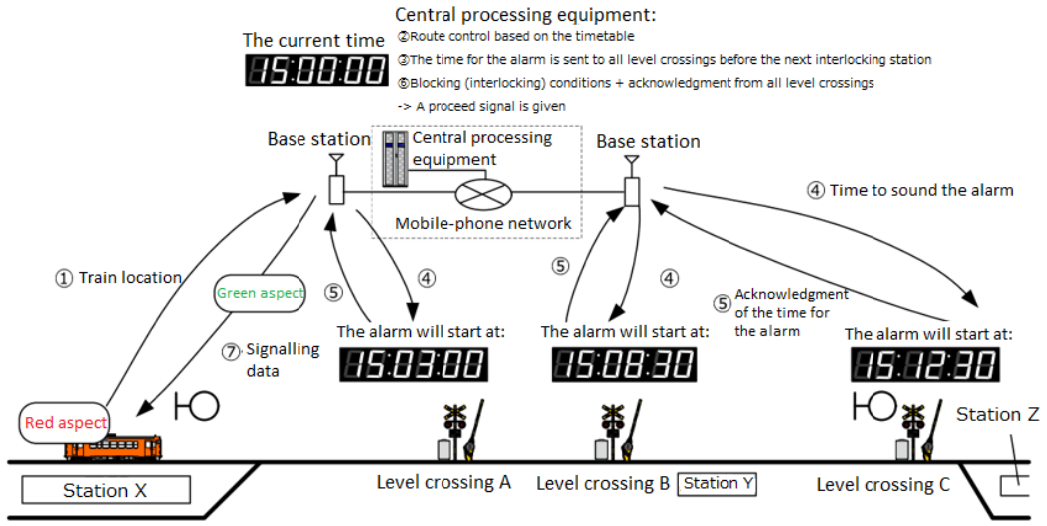

Fig. 3 Setting the time to activate an alarm.

Fig. 2 illustrates that level crossing control equipment installed at the level crossings (A, B and C) between Station X and Station Z is given instructions on when an alarm has to be activated during a travel of a train from Station X to Station Z. The time to activate an alarm is calculated based on the assumption that a train concerned is running at a maximum speed of the line so that the train will not pass an unclosed level crossing. A train cannot proceed without an acknowledgment from the level crossing control equipment of the instructions.

The level crossing control equipment placed at each level crossing issues an alarm at the required time.

The timing of alarm activation can vary according to

those factors such as the current location, speed etc. of a running train. The central processing equipment continuously times alarm activation by updating each level crossing on the required alarm-activation time based on the current location and speed of a train concerned. The level crossing control equipment issues an alarm for the train at the required time, closes the level crossing after a certain period of time, confirms the absence of an obstacle and then informs the central processing equipment that the train can pass through the level crossing. The central processing equipment in turn seeks a new movement authority limit beyond the level crossing and transmits it to onboard equipment of the train. Consequently, this system can control level crossings in the same manner as the fully-centralized individual level crossing control system.

Once the central processing equipment confirms that a train concerned has left the level crossing, it orders the level crossing control equipment to stop the alarm.

The subsequent chapter addresses the safety analysis and assessment method adopted for the closed-loop level crossing control systems.

3. Analysis of Software Failures with STAMP

3.1 Analysis of Software Failures

There are many failures caused by software malfunctions. Nevertheless, there is no suitable method of analyzing the impact of software failures on the whole system. Even FMEA and FTA contain some shortcomings, although they are often used as a method of failure analysis.

Fundamentally, FMEA has no means to define software failures and assess their impact. Loops, wrong branches and other failures may appear in many different locations, and besides, it is not possible to uniquely define how software behaves in the event of such a failure. Today, a common method of performing FMEA is to focus on the functionality of modules and predict their possible malfunctions. However, this is only a methodology that has been devised as a means of using FMEA instead of paying attention to software bugs. Likewise, FTA, which starts an analysis with a malfunction mode of a system toward deeper levels, can only end with clarifying malfunctions of functional modules, instead of finding out software bugs.

As a solution to overcome such limitations, an accident model called STAMP that focuses on interactions among modules and controls has been advocated by Nancy Leveson. STAMP is spotlighted for its effectiveness in analyzing safety of software-intensive systems.

3.2 Assessment by Means of STAMP

STAMP is characterized by the ease of identifying causes of accidents attributed to the design of an entire system such as system mechanism, technologies, human errors and miscommunication among projects, all of which have been difficult to discover by means of conventional accident assessment models (FTA, FMEA etc.). Hazard analyses are performed to identify the causes of accidents (hazards) prior to the occurrence of the accidents and STPA (System Theoretic Process Analysis) is used as a tool for the hazard analyses. The hazard analysis process using STPA consists of the following four steps.

(1) Preliminary Step 1: Identification of accidents, hazards and safety constraints

In this first preliminary step, accidents, hazards and safety constraints are prepared. This intends to predefine events which systems should prevent and such predefined events are in turn used as input to STPA Step 1.

- Accident: a system accident causing a loss;
- Hazard: a system state leading to an accident;
- Safety constraint: a rule necessary to maintain the safety of a system.

(2) Preliminary Step 2: Establishment of a control structure

A control structure is a diagram depicting the interrelation among functions that control a system. It represents the flow of orders for controls and feedback

exchanged among components using arrows.

(3) STPA Step 1: Identification of UCAs (unsafe control actions)

In this step, UCAs that may lead to a hazard are identified and categorized into the following four types:

- Not Provided: Control actions necessary for safety are not provided;
- Incorrectly Provided: Unsafe control actions that may lead to a hazard are provided;
- Provided Too Early, Too Late, or Out of Sequence: Control actions are provided too late or too early, or not provided in a predetermined sequence;
- Stopped Too Soon or Applied Too Long: Control actions stop too soon or are applied too long.

(4) STPA Step 2: Identification of HCFs (hazard causal factors)

In the last step of STPA, causal factors of UCAs identified during STPA Step 1 and expected accident scenarios are identified. Causal factors are potential flaws that may appear in a control loop, which are classified according to the following 11 guidewords:

- Control Input or External Information Wrong or Missing;
- Inadequate Control Algorithm (Flaws in Creation, Process Changes, Incorrect Modification or Adaptation);
- Process Model Inconsistent, Incomplete or Incorrect;
- Component Failures, Changes Over Time;
- Inadequate or Missing Feedback, Feedback Delays;
- Incorrect or no Information Provided, Measurement Inaccuracies, Feedback Delays;
- Delayed Operation;
- Inappropriate, Ineffective or Missing Control Action;
- Process Input Missing or Wrong;
- Unidentified or Out-of-Range Disturbance;
- Process Output Contributes to System Hazard.

4. Comparison among Level Crossing Control Systems by Means of STAMP

4.1 Analysis of the Conventional Level Crossing Control System Using STAMP

This section addresses locally-controlled level crossings for single-track sections according to Fig. 1. Electronic train detectors with a short track circuit are used for train detection. Once an electronic train detector for activating level crossing control detects a train having entered the level crossing section, an alarm is issued and, after a specified period of time, a level crossing barrier is lowered to close the level crossing. Afterwards, the train is detected by the next electronic train detector for deactivating the level crossing control, the alarm is stopped and the barrier is raised. If any obstacle is detected after the level crossing is completely closed, an obstruction warning signal warns the train crew of the obstacle in order for them to stop the train. However, with regard to this system, accidents such as collisions caused by a train crew having found a warning light late have often been reported. In summary, the characteristics of the conventional level crossing control system are wayside-based control completed by trackside sensors and wayside level crossing control equipment and reliance on the train crew's attentiveness for ensuring safety in the event of a hazard.

The conventional level crossing control system was previously analyzed by means of STAMP as shown in the reference document [3], in which the analysis ends with the closure of level crossings. However, there are actually many cases where an obstacle remains after the closure of level crossings but a train crew is not warned or becomes aware of it in a timely manner, thereby leading to an accident. Taking such cases into consideration, this paper extends the range of analysis.

Fig. 4 defines an additional control structure with role players involved based on the extended analysis:

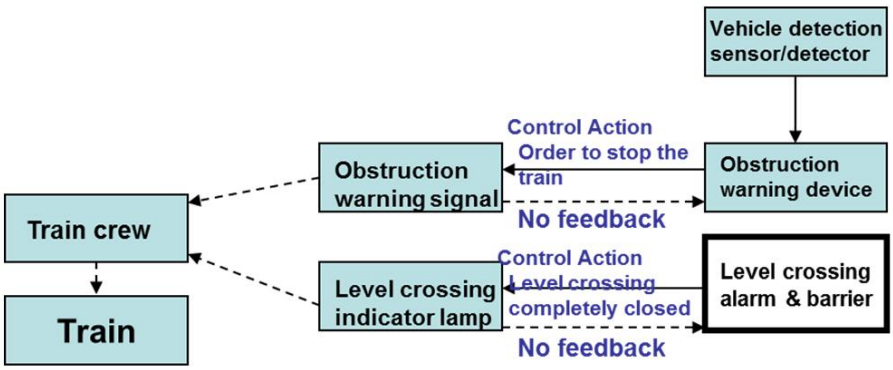

Fig. 4 An additional control structure.

The analysis performed in the reference document [3] identified six UCAs (UCA1 to UCA6) and the extended analysis performed in this paper adds six UCAs (UCA7 to UCA12); consequently 12 UCAs in total are identified for the conventional level crossing control system:

UCA1: A train passes a level crossing with no alarm activated (the level crossing is not closed).

UCA2: A train reaches a level crossing before it is completely closed (the level crossing closes later than the passage of the train).

UCA3: An alarm stops before a train completely leaves a level crossing (the level crossing opens too early after its closure).

UCA4: A train detection sensor is wrongly masked for no train, hence it cannot activate a necessary alarm for an incoming train. Likewise, a train detection sensor is wrongly masked together with the opposite sensor that has been correctly masked, hence it cannot activate a necessary alarm for an incoming train.

UCA5: An order to be given to mask a train detection sensor is delayed and the order remains unexecuted after the passage of a train over the sensor. Afterwards, if there are two consecutive trains coming from the opposite direction to the abovementioned train, a necessary alarm for the second one is not activated due to the surviving order.

UCA6: If a train detection sensor remains masked even after a train has passed the sensor, it cannot activate an alarm for the next train coming from the opposite direction to the abovementioned train. Masking of a train detection sensor is not canceled even after the passage of a train, hence the sensor does not activate an alarm for the next train coming from the opposite direction to the abovementioned train (this also applies to the case where a train turns back after a sensor is masked).

UCA7: Although there is an obstacle, an obstruction warning signal is not ordered to turn on, hence it does not light up.

UCA8: A level crossing indicator lamp mistakenly turns on according to false information that a level crossing has been completely closed although it is not completely closed.

UCA9: An obstruction warning signal lights up late due to a delayed order for the signal to turn on.

UCA10: It takes too long from finding an obstruction warning signal being lit to a brake application.

UCA11: An obstacle is detected after a level crossing is completely closed but an obstruction warning signal is controlled late, hence adequate braking distance cannot be ensured.

UCA12: An obstacle intrudes on a completely-closed level crossing through which a train is passing.

In addition, 27 causal factors in total that may induce each UCA have been identified; 17 are shown in the reference document [3] and additional 10 are listed below. It should be noted that there is no causal factor identified for UCA11 and UCA12 because they are attributed to those who intrude on level crossings.

UCA7: An order to stop a train is not issued, hence an obstruction warning signal does not light up.

(Guideword No. 1) Control Input or External Information Wrong or Missing

• An obstruction warning signal is not activated because a sensor has failed to detect an obstacle or a detector has failed to react to a detected obstacle.

(Guideword No. 2) Inadequate Control Algorithm, (Guideword No. 4) Component Failures, Changes Over Time

• An obstruction warning signal cannot be controlled due to an error in the processing of an order to stop a train.

(Guideword No. 9) Process Input Missing or Wrong

• An obstruction warning signal is not activated due to a wrong order given.

UCA8: A level crossing indicator lamp mistakenly turns on according to false information that a level crossing has been completely closed although it is not completely closed.

(Guideword No. 2) Inadequate Control Algorithm, (Guideword No. 4) Component Failures, Changes Over Time

• A level crossing indicator lamp turns on although a level crossing is not closed due to an error in the processing to completely close the level crossing.

(Guideword No. 9) Process Input Missing or Wrong

• Although a level crossing is not closed, a level crossing indicator lamp turns on due to a wrong order given.

UCA9: An obstruction warning signal lights up late due to a delayed order to turn the signal on.

(Guideword No. 1) Control Input or External Information Wrong or Missing

• An obstruction warning signal lights up late due to a delayed order from an obstruction warning device.

(Guideword No. 2) Inadequate Control Algorithm, (Guideword No. 4) Component Failures, Changes Over Time

• An obstruction warning signal is controlled late due to an error in the processing of an order to stop a train.

(Guideword No. 7) Delayed Operation

• An obstruction warning signal lights up late due to a delayed operation of an obstruction warning device.

UCA10:It takes too long from finding an obstruction warning signal being lit to a brake application.

(Guideword No. 7) Delayed Operation

• Sufficient time cannot be secured for the safe closure of a level crossing due to a road vehicle traversing the level crossing recklessly.

• An obstruction warning signal being lit is observed late by a train crew while they are involved in other operational tasks and consequently a brake is applied too late.

This analysis, which targeted the conventional level crossing control system, has revealed that the system relies on a train crew as the final means of preventing the abovementioned accidents. Nevertheless, this may rather tend to cause an accident because it is not unusual for a train crew to be warned or become aware too late of any obstacle detected after the closure of a level crossing.

4.2 Analysis of the Closed-Loop Level Crossing Control Systems

(1) The result of the assessment on the closed-loop level crossing control systems

Each type of the closed-loop level crossing control systems described respectively in (2), (3) and (4) of Chapter 2 has been analyzed in the same manner as the conventional system.

As the first step of this analysis, control structures with role players involved were defined. With regard to the decentralized control system and the fully-centralized individual control system, the only difference between them is whether control equipment is distributed along the track or centralized, hence a control structure common to the two types of systems is defined as shown in Fig. 5. Fig. 6 defines a control structure of the fully-centralized comprehensive control system.

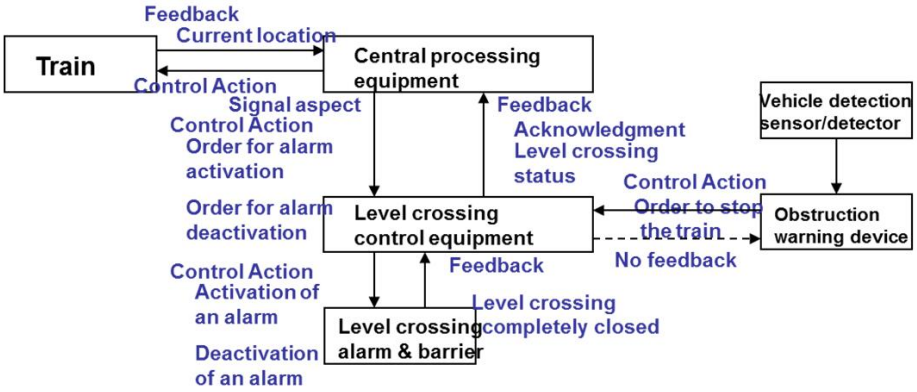

Fig. 5 The decentralized control system and the fully-centralized individual control system.

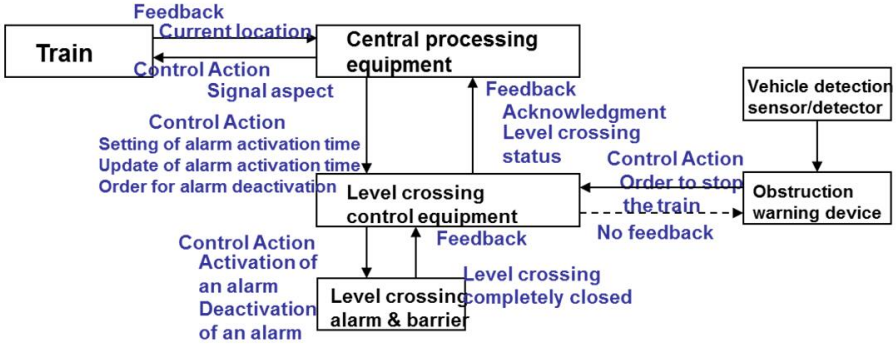

Fig. 6 The fully-centralized comprehensive control system.

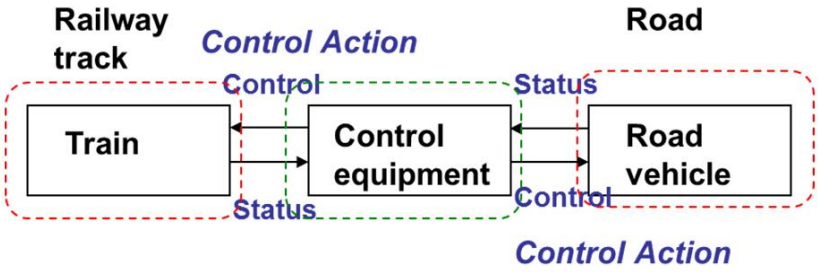

Fig. 7 A control structure of the accident-prevention system.

Above all, it is essential to consider an accident-prevention system that is required to avoid the risk of collision between a road vehicle and a train at a level crossing. The control equipment of this system is designed to control a train or a road vehicle depending on the situation in order for them not to collide with each other. Accordingly, the control structure of this system can be established as shown in Fig. 7.

The control structures shown in Figs. 4, 5 and 6, which are defined for different types of level crossing control systems based on Fig. 7, indicate that those systems rely on level crossing barriers and obstacle detection equipment for preventing accidents instead of controlling road vehicles directly. Furthermore, Fig. 4 demonstrates that the conventional level crossing control system has no direct control of trains but a train crew is entrusted with the control of trains for the purpose of preventing accidents.

Next, seven UCAs were identified for the decentralized, the fully-centralized individual and the fully-centralized comprehensive level crossing control systems. Like the conventional system, the identified

UCAs also include two UCAs associated with delayed operation that may be caused by any intruders on level crossings. The conventional system, which controls level crossings based on the train detection using a combination of three electronic train detectors (two for activating and the rest for deactivating level crossing control), has to distinguish between up trains and down trains running on a single-track section and disable (mask) a detector for activating the control whichever is placed on the far side of the level crossing from an approaching train. On the other hand, the closed-loop level crossing control systems do not require such masking of train detectors because central processing equipment can properly control level crossings

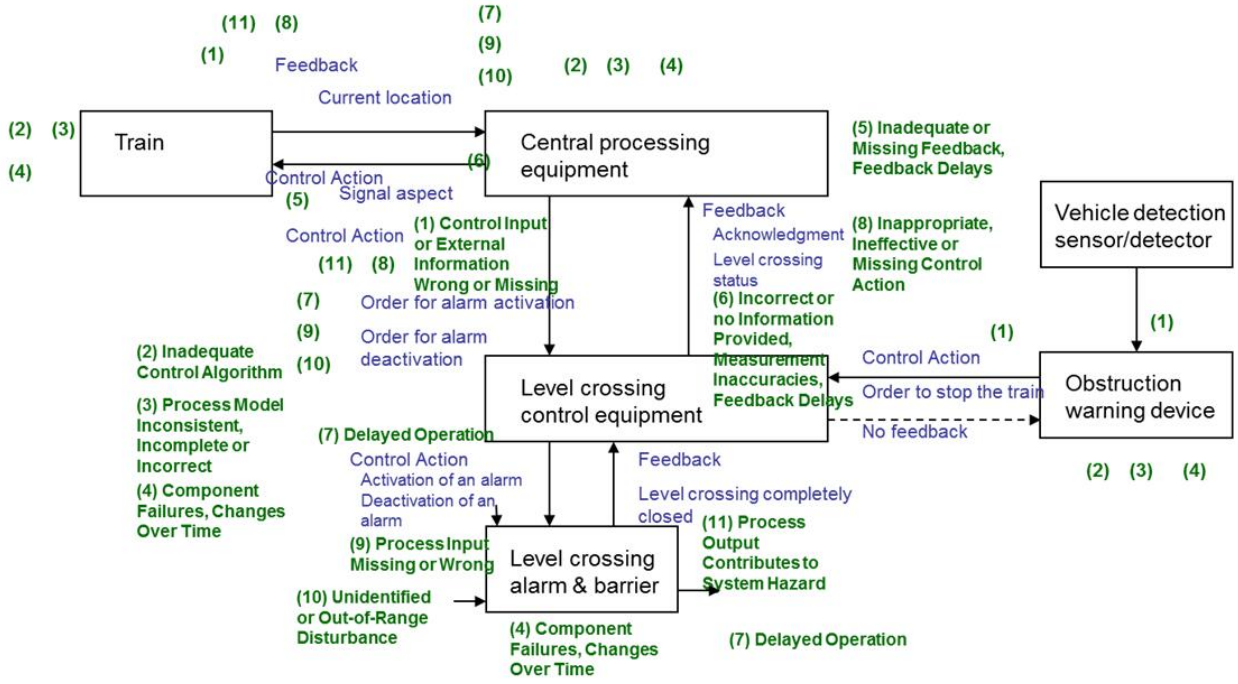

Fig. 8 A control structure for the decentralized and the fully-centralized individual control systems.

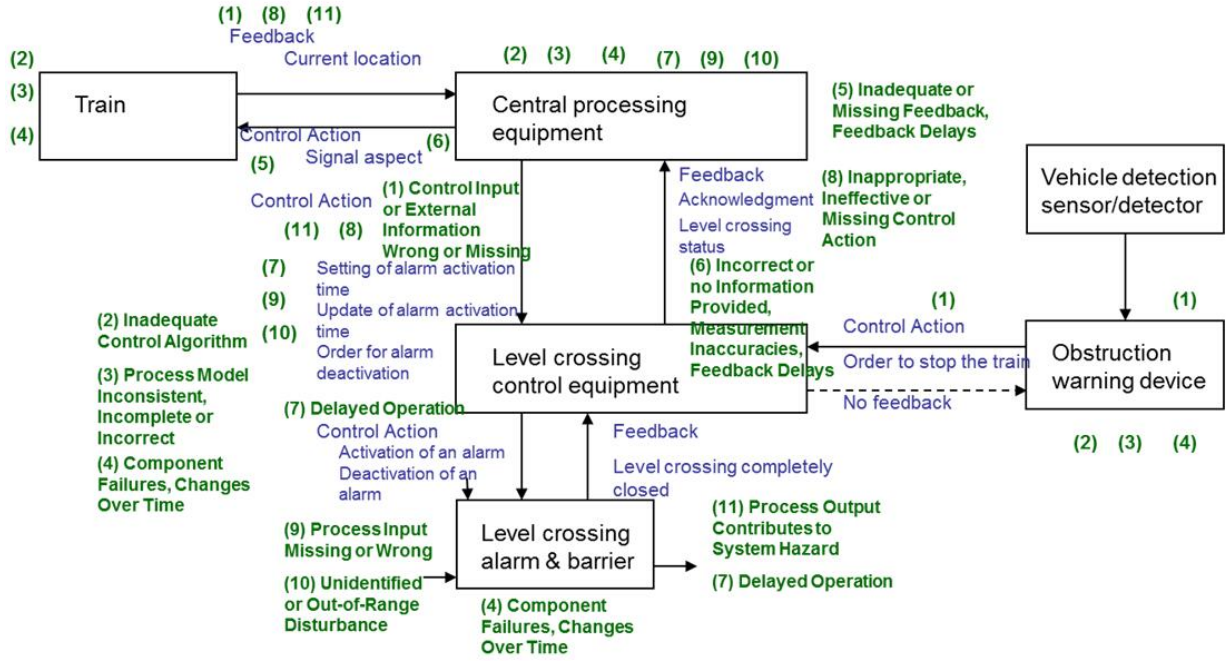

Fig. 9 A control structure for the fully-centralized comprehensive control system.

Table 1 UCAs and corresponding causal factors.

		Closed-loop level crossing control systems	
		Decentralized and fully-centralized individual control systems	Fully-centralized comprehensive control system
UCA1	A train passes a level crossing with no alarm activated (the level crossing is not closed).	(1) An alarm is not activated due to an incorrect order given to level crossing control equipment.	(1) An alarm is not activated due to an incorrect setting of alarm activation time given to level crossing control equipment.
		-	(2) Level crossing control equipment cannot initiate control procedures at a specified time due to an incorrect time management of the equipment.
		(4) Level crossing control equipment cannot initiate control procedures due to a component failure in the control block of the equipment.	(4) Level crossing control equipment cannot initiate control procedures at a specified time due to a component failure in the time management block of the equipment.
		-	(6) Alarm activation time cannot be set and an alarm not activated because level crossing control equipment wrongly returns an acknowledgment of alarm activation time before the time is set.
		(9) An alarm is not activated due to an incorrect order given to level crossing control equipment.	(9) An alarm is not activated due to an incorrect time setting of level crossing control equipment.
UCA2	A train reaches a level crosssing before an alarm is activated (the level crossing closes later than the passage of the train).	(2) A level crossing cannot be controlled correctly due to an incorrect order from level crossing control equipment.	(2) Level crossing control equipment cannot initiate control procedures at a specified time due to an incorrect time management of the equipment.
		(4) Level crossing equipment cannot initiate control procedures due to a component failure in the control block of the equipment.	(4) Level crossing control equipment cannot initiate control procedures at a specified time due to a component failure in the time management block of the equipment.
		(7) A level crossing fails to close in time due to a delay in the operation of a level crossing alarm or barrier.	(7) A level crossing fails to close in time due to a delay in the operation of a level crossing alarm or barrier.
UCA3	An alarm stops before a train completely leaves a level crossing (the level crossing opens too early after its closure).	(1) An alarm is deactivated while a train is running on a level crossing due to incorrect timing of alarm deactivation.	(1) An alarm is deactivated while a train is running on a level crossing due to incorrect timing of alarm deactivation.
		(2) An alarm is deactivated in an untimely manner due to an incorrect order from level crossing control equipment.	(2) An alarm is deactivated in an untimely manner due to an incorrect time management of level crossing control equipment.
		(4) An alarm is deactivated in an untimely manner due to a component failure in the control block of level crossing control equipment.	(4) An alarm is deactivated in an untimely manner due to a component failure in the time management block of level crossing control equipment.
		(6) An alarm is deactivated too early because an acknowledgment of alarm deactivation is returned before an order for alarm deactivation is given.	(6) An alarm is deactivated too early because an acknowledgment of alarm deactivation is returned before an order for alarm deactivation is given.
UCA4	An order to stop a train cannot be issued.	(1) A sensor fails to detect an obstacle or a detector fails to react to a detected obstacle.	(1) A sensor fails to detect an obstacle or a detector fails to react to a detected obstacle.
		(2) A train cannot be controlled due to an error in the processing of an order to stop the train.	(2) A train cannot be controlled due to an error in the processing of an order to stop the train.
		(4) A train cannot be controlled due to a component error in the processing block that handles orders to stop trains.	(4) A train cannot be controlled due to a component error in the processing block that handles orders to stop trains.
UCA5	An order to stop a train is issued late.	(1) A train is controlled late due to a delayed order from an obstruction warning device.	(1) A train is controlled late due to a delayed order from an obstruction warning device.
		(2) A train is controlled late due to an error in the processing of an order to stop the train.	(2) A train is controlled late due to an error in the processing of an order to stop the train.
		(4) A train is controlled late due to a component failure in the processing block that handles orders to stop trains.	(4) A train is controlled late due to a component failure in the processing block that handles orders to stop trains.
		(7) A train is controlled late due to a delayed processing of an obstruction warning device.	(7) A train is controlled late due to a delayed processing of an obstruction warning device.
UCA6	An obstacle is detected after a level crossing is completely closed while an obstruction warning signal is controlled late, hence adequate braking distance cannot be ensured.	* System-induced causal factors are not identified because these UCAs are caused by intruders on level crossings.	
UCA7	An obstacle intrudes on a completely-closed level crossing through which a train is passing.		

according to the movement of individual trains. Therefore, regarding the closed-loop systems, it is not necessary to identify UCAs associated with the masking of train detectors.

The last step of the analysis was to map 11 guidewords onto control structures (see Fig. 8 for the decentralized control system and the fully-centralized individual control system and Fig. 9 for the fully-centralized comprehensive control system). Accident scenarios were developed based on these control structures in the same manner as the conventional system. Consequently, 17 causal factors corresponding to the seven UCAs were identified for the decentralized and the fully-centralized individual control systems and 19 causal factors for the fully-centralized comprehensive control system, as shown in Table 1.

The result of analysis performed on each type of level crossing control systems is summarized as follows (please note that measures against the identified UCAs are not addressed herein). With regard to the conventional level crossing control system, the analysis revealed that a large number of UCAs lead to a variety of expected accident scenarios due to passive control performed by the system based on train detection by means of various sensors (train detectors).

By contrast, the closed-loop level crossing control systems are characterized by active control by which a control loop is established between the central processing equipment and onboard equipment and the result of the control is continuously monitored except for the obstruction warning device. For that reason, expected accident scenarios only involve level crossing control equipment, level crossing alarms and level crossing barriers as the target of the active control.

Therefore, the expected accident scenarios only pertain to abnormal control algorithms for time clock management, etc. and the occurrence of any other faults will result in stopping a train before a level crossing, thereby leading to a safe state. Moreover, since the control algorithms are supported by abnormality monitoring by FS-CPUs, the probability of the occurrence of wrong-side failures can be reduced as low as possible.

The level crossing control equipment of the closed-loop systems is supposed to notify onboard equipment of local conditions (e.g., no obstacle on a level crossing) via the central processing equipment once the level crossing has been completely closed. The onboard equipment does not allow the train to enter a level crossing unless the safety in the level crossing is confirmed. As well as this indispensable function for ensuring safety, the optimization of the timing of communication to achieve sufficient duration of a level crossing alarm without brake application of a train is also required. In relation to this, there is a report on the decentralized level crossing control performed by ATACS, showing that ATACS has succeeded in shortening the duration of an alarm.

There are two main differences between the causal factors identified for the decentralized and the fully-centralized individual control systems and those for the fully-centralized comprehensive control system. First, only the fully-centralized comprehensive control system among the three types of systems features the time management block and is thus accompanied by causal factors specific to the time management block. Second, the decentralized and the fully-centralized individual control systems involve causal factors concerned with level crossings that remain unclosed after a train has passed a designated point of triggering an alarm, while this is not the case for the fully-centralized comprehensive system because it is almost unnecessary for the system to take into account how to cope with such a situation owing to its control characteristics.

(2) Effectiveness of the assessment by means of STAMP

Japan Transport Safety Board investigated and announced 68 level crossing accidents from October, 2001 to July, 2016. According to the investigation, 17 accidents among them occurred at level crossings provided with obstacle detection equipment, which are categorized by accident factors and broken down in percentage terms as follows:

- A road vehicle etc. was stranded on a level crossing with an obstruction warning signal unlit: 11%;
- A road vehicle etc. was stranded on a level crossing with an obstruction warning signal lit: 23%;
- A road vehicle etc. intruded on the level crossing immediately before a train enters the level crossing (the fault of the intruder): 47%;
- A road vehicle etc. smashed into the flank of a train passing a level crossing (the fault of the intruder): 17%.

A quantitative assessment was then performed by categorizing the UCAs identified for the conventional system into the above categories and consequently it was found that the UCAs could be sorted into those that are almost impossible to take place and those that are of significance.

Concretely, for the conventional system, UCA1 through UCA6 and UCA8 among all the UCAs identified by means of STAMP are actually negligible. On the other hand, UCA7 corresponds to the first category (11%), UCA9 to the second (23%), UCA10

and 11 to the third (47%) and UCA12 to the fourth (17%), which means attention should be paid to these UCAs. This assessment thus demonstrates that STAMP, in spite of its completeness in identifying UCAs, will become meaningless unless significant UCAs and actually-negligible UCAs (although having been identified) are discriminated.

Those significant UCAs which correspond to the abovementioned actual accidents were further scrutinized in terms of what if a closed-loop system were used. UCA7 is caused by poor performance of obstruction warning devices in detecting obstacles, hence even a closed-loop system would not prevent such an accident resulting from UCA7 unless the ability of the devices is improved. By contrast, a closed-loop system is assumed to be able to provide protection against UCA9 because the system does not allow a train to pass a level crossing under the condition of UCA9, unlike the conventional system which has a limitation in coping with UCA9 because it has to rely on an effort of a train crew to ensure safety. A closed-loop system is also supposed to prevent UCA10 and UCA11 by the principle that, in the same manner as UCA9, a braking profile to stop a train in front of a level crossing remains valid and thus the train cannot enter the level crossing unless the absence of an obstacle is confirmed. Nevertheless, it is not possible even for the closed-loop system to protect level crossings against such road vehicles that recklessly crash into level crossing barriers. Among eight accidents that fall under the third category (i.e., a road vehicle intruded on the level crossing immediately before a train enters the level crossing, although the alarm was sounding and the barrier lowering), one (12.5% of the third category) is a kind of accident that might have been prevented if the train crew did not miss an intruder on the level crossing; in this regard, any closed-loop system would have been able to prevent it. The rest seven accidents (87.5% of the third category) pertain to a situation where the train crew detected an intruder when the train running at a speed of 70~100 km/h was located within 190 meters before the level crossing. In such a situation, a closed-loop system would not have been able to avoid an accident even if it expedited the control of the level crossing. As a preventive measure against such accidents, it will be necessary to develop a mechanism of inhibiting a road vehicle etc. from entering a level crossing after it closes (e.g., barriers such as flaps used in some level crossings in Russia) or incorporate a control mechanism against a trespassing road vehicle, etc. where a level crossing control system works in conjunction with an ITS (intelligent transport system). This solution will also be expected to be effective against UCA12 as well.

In summary, if a closed-loop system was used, seven among these 17 accidents would possibly have been prevented. Meanwhile, particular attention should be given to the difference of the number of logic blocks between the decentralized system and the fully-centralized systems. For a decentralized system, where the number of the logic blocks is n, wrong control resulting from a failure in a logic block will be n times more likely to take place than the fully-centralized systems. However, the processing performed by the closed-loop systems can move forward in a stepwise manner only if a series of messages is successfully exchanged and even any delay in the processing or missing message will always lead to a safe state, i.e., a speed profile generated to stop a train in front of a level crossing will not be cancelled. For that reason, a possible unsafe event that may stem from logic blocks will only be such an event that software fault in logic blocks will issue a wrong instruction to cancel the speed profile to stop the train in front of the level crossing by misjudging the situation as “level crossing completely closed and no obstacle on the level crossing” although necessary conditions are not met. These unsafe events can actually be prevented by means of prior elaborate testing etc. and, even identified as an additional UCA in the same manner as UCA1 through UCA6, will thus be considered negligible.

5. Conclusion

In this paper, the authors introduce the three types of closed-loop level crossing control systems: decentralized, the fully-centralized individual and the fully-centralized comprehensive systems and compare them with the conventional level crossing control system using the STAMP method. The comparison proves that the closed-loop systems can contribute considerably to improving safety by compensating disadvantages of the conventional system.

With regard to STAMP method, it was found to be capable of more rational assessment than FTA and FMEA, which have been conventionally used for software safety assessment. Software assessment using FMEA is accompanied not only by overwhelming workload but by persistent concern about the lack of plausibility of scenarios regarding how the impact of software failures will spread out. Likewise, FTA also has a problem; it can identify fatal factors in a top-down manner but cannot provide a valid answer to the question of what kind of failures in actual software modules will lead to those factors. By contrast, analyses by means of STAMP can be performed in terms of how relevant interfaces behave when a software module fails. In this regard, STAMP has given a positive impression to the authors as a credible analysis method.

In addition, the UCAs identified in detail were assessed in terms of their probability of occurrence in light of statistical data of accidents that occurred in the past. Through this assessment, one shortcoming in the use of STAMP was clarified; STAMP cannot distinguish between identified UCAs that may not happen actually and those that are of significance in that they may actually take place.

Acknowledgments

The authors would like to express gratitude to cooperators from Kyosan who provided us with much advice on our study.

References

[1] Japan Railway Electrical Engineering Association. 2015. *Railway Signaling.* Japan Railway Electrical Engineering Association.

[2] Yamazaki, I., and Uchiyama, D. 2015. "The Level Crossing Control Function of ATACS Coming into Use." *JREA* 58 (8): 22-5.

[3] Information-Technology Promotion Agency, Japan. 2016. *Introduction to STAMP/STPA.* First Copy. Information-Technology Promotion Agency, Japan.