Interlocking System Based on Concept of Securing a Train Travelling Path

Tetsuya Takata [a1], Akira Asano [a], Hideo Nakamura [b]
[a] Development Center, Kyosan Electric Mfg. Co., Ltd.
2-29-1, Heian-cho, Tsurumi-ku, Yokohama, 230-0031, Japan
[1] E-mail: takata-t@kyosan.co.jp, Phone: +81 (0) 45 503 8115
[b] The University of Tokyo
5-1-5, Kashiwanoha, Kashiwa, Chiba, 277-8561, Japan

Abstract
In recent years, the environment of railways and the systems such as CBTC (Communication Based Train Control) have been changing. To respond the changes and the needs of customers, a unified train control system (UTCS) has been developed to realize a system that evolves with customers.

Previous type systems consist of independent components such as ATC (Automatic Train Control) system, electronic interlocking system, and facility monitoring system, and there are a complicated overlap of system configurations and functions and difference in concept between the systems. On the other hand, the integrated train control system consists of horizontal layers such as function layer, network layer, and terminal layer. Therefore, the system has been developed to make it simple with no unnecessary redundancy and evolving to meet the needs of customers. In this paper, we explain a method that realizes the interlocking function in the function layer based on the concept of "securing a train travelling path" including path blocking and routing, and evaluate the safety of the method using STAMP/STPA (Systems-Theoretic Accident Model and Processes/System Theoretic Process Analysis).

Keywords
Railway signaling, interlocking System, safety assessment, train control system, CBTC, UTCS, FMEA, STAMP/STPA.

1 Introduction

Interlocking system is a train control system that realizes collaborative control of branching direction or permission for trains to travel, in order to prevent collision or derailment of trains.

As a result of individual development of block system, ATC system, interlocking system, and facility monitoring system, the train control system consists of vertically-divided independent components. Integrated train control system is developed by reorganizing the train control system to have horizontally-divided layers including function layer, network layer, and terminal layer. The reorganization of the system incorporates the control logic into the function layer and therefore the interface between the systems is rational.

Integrated train control system is developed by reorganizing the train control system to have horizontally-divided layers in "hierarchical configuration" including function layer, network layer, and terminal layer. This reorganization of the system not only integrates the functions and reduces on-site facilities, improving the system reliability, but also incorporates all the control logics into the function layer. Therefore, the interface between the systems is rational. Development of the rational interface reduces train accidents caused by an error of the interface and enhances the safety.

Necessary functions for a train to travel on a track can be roughly classified to the one to "secure a train travelling path" such as blocking and routing functions and the one to "control safety" such as signal and speed control functions. If the entire system is reorganized with the above-mentioned layer components on the basis of the concept of "securing a train travelling path" and "safety control," the "exclusive control" that has been considered necessary and the "overlapping functions" of each system could be eliminated and a simple system can be established.

In this paper, we explain a method to realize an interlocking function based on the concept of "securing a train travelling path" such as blocking and routing and evaluate its safety using STAMP/STPA.

2 Interlocking based on concept of securing a train travelling path

2.1 Concept of securing a train travelling path

Conditions for safe travelling of trains that were indicated before are as follows.

(1) The travelling path shall be fully configured and secured. Namely, the points on the path shall be switched and locked to the travelling direction.

(2) No train or carriage shall exist on the travelling path.

(3) There shall be no possibility of other trains to travel on the path.

(4) The above state shall be maintained until the train passes over the path.

This can be summarized as follows from a viewpoint of securing a train travelling path.

(1) The travelling path shall be fully configured and secured. Namely, the switches (points) on the path shall be switched and locked to the travelling direction.

(2) No train or carriage shall exist on the travelling path occupied by a train.

(3) Other trains shall not be able to travel on the occupied path.

(4) If the train passes over a division of the travelling path, it loses the right to occupy the division.

For a train travelling path, block points are introduced to define the points where a train on the path is blocked to allow other trains to travel on the path. If a block point is set on a train travelling path which a train requests to occupy, the train is given the right to occupy a distance from the head of the train to the block point and the right is used as the train control condition.

2.2 Setting of travelling path and block points for train interval control

A travelling path is defined as a set of sections. Then, block points are introduced to define the points where a train on the path is blocked. If a block point is set on a train travelling path which a train requests to occupy, the train is given the right to occupy a distance from the head of the train to the block point and the right is used for the train control.

For example, the block points are set as follows.

(1) Block point 1: End of a train travelling in front on the travelling path (moving point)

(2) Block point 2: Position of a point on the travelling path (fixed point)

(3) Block point 3: Position related to the travelling path occupied by an oncoming train (fixed point)

2.3 Interlocking function

Unlike the previous interlocking function which has individual circuit logics based on interlocking circuit data of each station, the interlocking function developed under the concept of securing a travelling path has a shared program as a logic to secure the safety of travelling paths. A conceptual diagram is shown in Fig. 2-1.

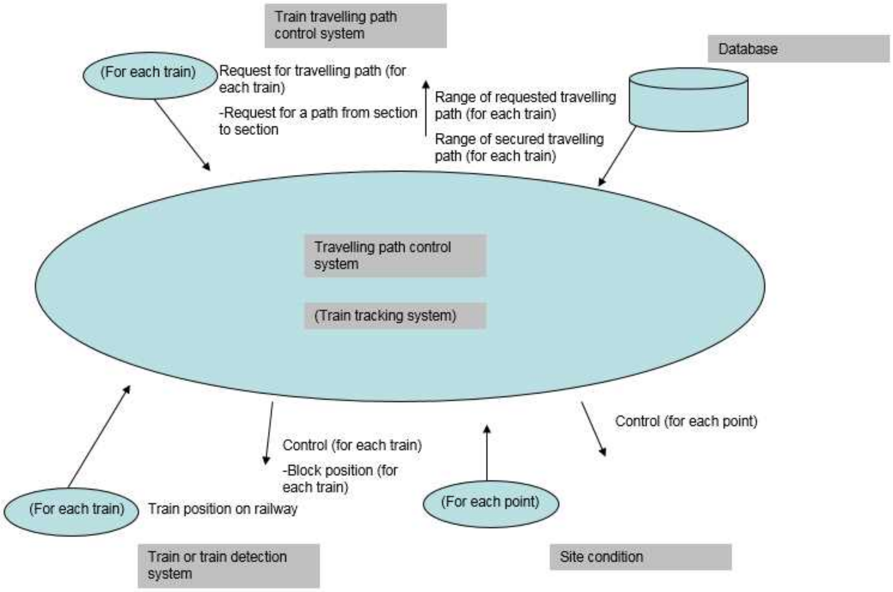

Train travelling path control system
Database
(For each train)
Request for travelling path (for each train)
-Request for a path from section to section
Range of requested travelling path (for each train)
Range of secured travelling path (for each train)
Travelling path control system
(Train tracking system)
Control (for each point)
Control (for each train)
-Block position (for each train)
(For each train)
Train position on railway
(For each point)
Train or train detection system
Site condition

Fig. 2-1 Logic of safety securing

The interlocking function works in the following steps.

(1) When a travelling path (which expresses a path from a starting point to a destination and is defined as a set of sections) is requested (under the control of each train), a travelling path status table for the travelling path is created and an interlocking processing is performed according to the table created. (The table is deleted when the path request is cancelled.)

(2) In the travelling path status table, a series of sections based on a travelling path data table are described and control status of points based on request-acceptance status of each train for a given request and the railway form data table are registered.

In addition, on the basis of the block point data table and the block point positions of each train, an allowed area of each section of the travelling path is registered.

(3) A point is controlled in accordance with its control status and the allowed area of the travelling path is updated on the basis of the indicated status of the point.

(4) Train interval control is made by transmitting the nearest block point position to the trains based on the allowed area of the travelling path.

(5) The current position information of a train is updated according to the train travelling. As the block point position of each train is updated, block point positions of the trains on the path and the released area of the travelling path are set in the travelling path status table.

2.4 Idea about each locking

Since the present system concentrates the logics to the processing unit, the locking conditions for the interlocking can be made as follows.

After the integration of the logics, the rout becomes a travelling path and the functions of route locking (which prevents relevant points from switching until the train or carriage passes over all points in a route so that other routes that could block the route would not be formed, when a train or carriage enters the route by following an aspect of a signal that directs proceeding or clearance indication of a shunting indicator,), sectional route locking (which divides the route-locked sections and successively unlocks the sections over which a train or carriage passes to improve the efficiency of the train operation and station work), detector locking for signal lever (which is an interlocking between a signal and track circuit to lock the signal to a normal state when a train or carriage exists in the track circuit of the signal on the route), and detector locking (which does not allow a train or carriage to switch a point if the train or carriage exists in the track circuit where the point is installed) are satisfied by the travelling blocking logic that controls a single blocking and single train on the basis of the right given to the train to occupy the path (blocking).

In addition, the functions of approach locking (When a signal is made indicate a sign of proceeding and then a train enters the approach locking section of the signal or when a signal is made indicate a sign of proceeding while a train is entering the approach locking section of the signal, the approaching locking locks points in a route to prevent them from switching for a certain period of time after the train proceeds to the protection area of the signal or after a stop signal is made.), stick locking (which locks points in a route to prevent them from switching in the following cases: During the time period after a signal or shunting indicator is made indicate a sign of proceeding until a train or carriage enters the protection area and during a specified time period after a signal is made indicate a sign of stopping), and time locking (which keeps locking for a certain period of time even when levers of a signal and point are changed from the reserve to normal position) are satisfied after the integration of the logics, since control is made on the basis of train position information by a closed loop between the central station and trains.

Check locking (installed between levers in different signal cabins) is not necessary because of the centralized control. Circuit processing for indicating locking (which checks the consistency between the status of the signals and points and that of the lever and prevents dangerous control if inconsistency is found) is not necessary since on-site conditions of the point control and signal control are compared.

Therefore, the locking logic that the previous type of interlocking system used in the interlocking circuit for each station is not necessary.

3 Failure analysis of software and STAMP

3.1 Analysis of software failures

Many faults occur due to failure of software, although there is no appropriate method to analyze influence of the software failure on the system.

Even FMEA（Fault Tree Analysis） and FTA（Failure Mode and Effect Analysis） 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 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 unsafe control actions (UCAs)

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 Step2: Identification of hazard causal factors (HCFs)

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 Safety assessment

4.1 Assessment result by STAMP/STPA

As mentioned above, the interlocking system controls a travelling path of a train at a station with points.

A conceptual diagram is given in Fig. 4-1.

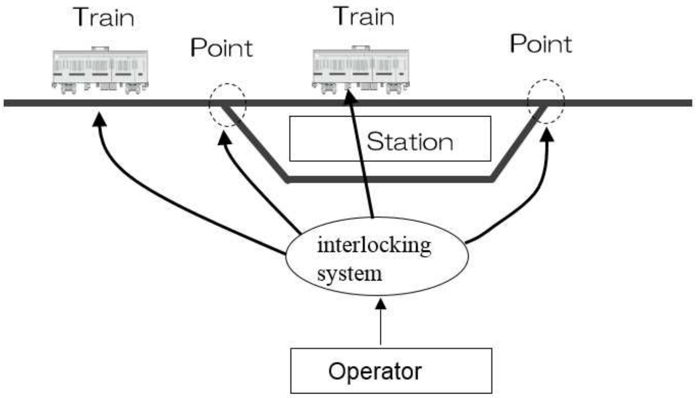


Fig. 4-1 Conceptual diagram of electronic interlocking system

An accident due to the travelling path control is defined as follows on the basis of the conceptual diagram.

(A1) Collision of trains

(A2) Derailing of a train

(A3) Contact of trains

As a result of the analysis of the interlocking system using STAMP/STPA for these accidents, HCF was identified for UCA, although details are omitted here. Possible measures and specific actions for the measures are summarized.

Some of the identified HCFs were categorized as the ones that should be handled by a method other than the interlocking system. Those include the HFCs which need to detect trains securely, such as (1) "A train travelling over a switch cannot be detected" or "A train cannot be recognized correctly," and the HFC such as (2) "Train collision could occur if a train start travelling when a travelling permission is issued."

Next, the HFCs of (3) "Switching restraint is not given due to inappropriate control algorithm" and "Switching control is output due to inappropriate control algorithm" require detector locking with an electric locking method. (4) "Travelling permission is immediately cancelled in a situation where a train cannot stop due to inappropriate control algorithm" requires approach locking or stick locking with an electric locking method. (5) "Disapproval of travelling is output but the output of the travelling aspect remained" requires indicating locking with an electric locking method. These were categorized as those associated with the locking conditions of the interlocking.

4.2 Analysis of existing electronic interlocking and present locking

Specific actions for the measures, listed below, are safety function requirements from the interlocking system.

(1) The input circuit for the switching direction of a point shall be constantly checked to make sure of its normality and be made unswitchable if an abnormality is found.

(2) The input circuit for the current position information of a train shall be constantly checked to make sure of its normality and be switched to choose presence of a train.

(3) Locking shall maintain if a signal does not indicate a stop aspect.

(4) A switch shall be made unswitchable while a train exists over it.

(5) Travelling permission control shall be monitored and, if an abnormality is found, it is switched to choose safety side.

(6) A travelling permission shall be cancelled with time for the train to stop in the allowed area.

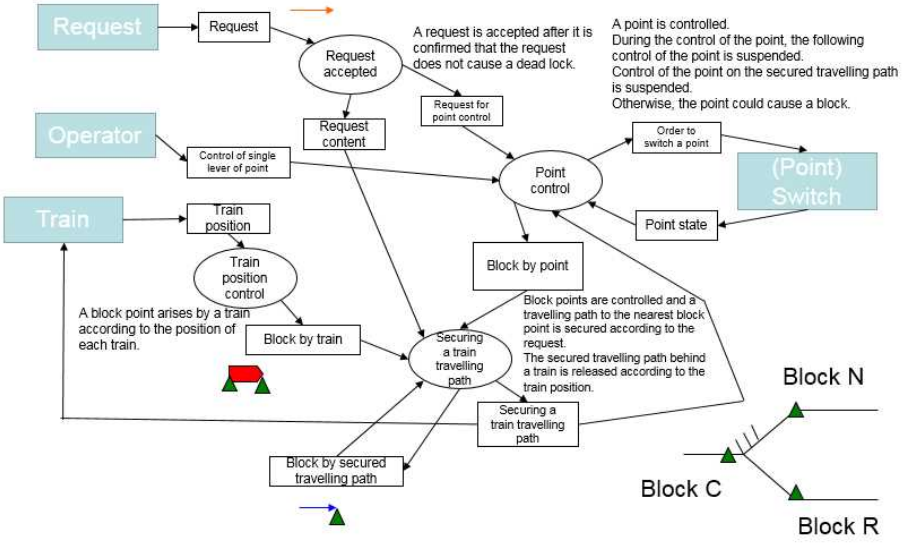
(7) Status of a point shall be constantly monitored.

(8) Switching restraint control shall monitored and, if an abnormality is found, it is switched to choose safety side.

(9) Switching control shall be monitored and, if an abnormality is found, it is switched to choose safety side.

It was clarified that, in the previous type of interlocking system, the safety function requirements depended on data of each station, while they depended on the software in the present system. Therefore, in a case where the interlocking function is realized by using circuit data of each station as done in the previous interlocking system, the present interlocking system does not need to verify the safety of the individual data of each station if the safety of the S/W is checked once.

There should be no particular problem in the software if the development method and in-company checking system for the software, which have been proved successful, are continued and if international standards such as IEC 62279 are referenced.



A request is accepted after it is confirmed that the request does not cause a dead lock.

A point is controlled.
During the control of the point, the following control of the point is suspended.
Control of the point on the secured travelling path is suspended.
Otherwise, the point could cause a block.

A block point arises by a train according to the position of each train.

Block points are controlled and a travelling path to the nearest block point is secured according to the request.
The secured travelling path behind a train is released according to the train position.

Fig. 4-2 Control flow of interlocking system

5 Conclusions

In this paper, we explained a method to realize an interlocking function based on the concept of “securing a train travelling path” and evaluated the safety of the interlocking system using STAMP/STPA. From the result of the evaluation, we showed the difference from the existing interlocking system and clarified that the interlocking could be realized even without circuit logic of individual stations.

The above method to realize the interlocking function of trains can also be applied to street cars (trams). In the case where interlocking with traffic signals is necessary, similar control can be realized if red signals are considered as hindering points. However, for the realization, it would be necessary to organize the timings of traffic signals and block points release for a train to travel forward and turn right and left. Then, specifications should be made for the organized timings. It would also be needed to make conditions to re-secure the secured train travelling path if the traffic signal condition changes because, for example, the path was secured once at the request of a train but the train could not start travelling due to too many people getting on and off the train.

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

References

Akira ASANO, Tetsuya TAKATA, Hideo NAKAMURA, 2015, Integrated train control system, STECH2015

Yoshihisa Saitou, Akira Asano, Hideo Nakamura, Sei Takahashi, 2016, A Proposal for the Design of integrated Train Control Systems Capable of Improving Reliability and Safety, Railways2016.

Information-Technology Promotion Agency, 2016, First STAMP/STPA,1sted., Apr.2016.

Railway Bureau, Ministry of Land, Infrastructure, Transport and Tourism Technical Regulatory Standards on Japanese Railways.

IEC62278:2002. Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS).