# Clarifying design guidelines of level crossing logic with functional resonance analysis method

Akimasa Okada, Researcher, East Japan Railway Company
Satoru Kitamura, Chief researcher, East Japan Railway Company
Takashi Kunifuji, Principal chief researcher, East Japan Railway Company,
Keita Sakemi, Researcher, Japan Manned Space Systems Corporation
Hideki Nomoto, Manager, Japan Manned Space Systems Corporation

## *SUMMARY*

*In this paper, we clarified design guidelines of level-crossing (LC) control logic with functional resonance analysis method (FRAM). At present complex control logics used for LCs in stations are implemented with electric relays. Those logics includes much tacit knowledge. Extracting the tacit knowledge helps to design software-based LC logics in stations. FRAM, which is proposed in a resilience engineering field, enables a system to be modelled with its functions and their connections. When the system works successfully, it can be said that the model expresses factors for successful behaviour thus those factor that are often tacit, can be extracted. Since LC control logics achieve high safety, the design guidelines can be extracted as the successful factors from the FRAM model. We found tacit design guidelines for LC logic from the FRAM model of a reference logic and evaluated them by comparing with the FRAM model of the control logic in operation. Finally we ensured that the extracted guidelines are valid.*

## 1 INTRODUCTION

Railway transportation becomes more important due to properties such as safety, energy-saving, and mass transit. Safety is the most important for the railway and availability is also required for stable operation. Recently, in addition to those properties, resilience that enables operation at least partly under disorder and quick restoration is drawing attention. Researches to make the railway more resilient are conducted in many fields, for example transportation networks [1][2], or tracks [3]. In the field of signalling systems, resilience is also necessary to develop safer and more stable railway system. In order to embed resilience into the signalling systems, deep understanding of safety is important.

Among signalling equipment level crossings (LCs) are crucial facilities because roads and railways intersect at LCs. Hence the LC control logic must achieve high safety under any situation. This requirement indicates that the logic needs to be resilient because the logic ensures safety under irregular train operations as well as system failure. East Japan Railway Company (JRE) [4] operates more than 6,000 LCs. While train disorder sometimes happens in the JRE's railway network, safety at all the LCs is kept. This fact indicates that the control logic ensures high safety even under operation disorder.

An issue regarding the LC control logic in JRE is implementation of the logic. While the control logic of a LC between stations is developed with software, that of one near a station is still configured with electric relays. In general, there are many train running routes in a station thus the control logic becomes complex to warn properly for all the routes and requires an amount of relays, which reduces maintainability and workability. Therefore the software control logic for LCs in stations is desired to improve the two properties. The similar issues are described in [5].

The software logic can be developed by emulating the relay logic. While many know-hows regarding the relay logic are documented, many design guidelines are tacit at present. It is difficult to intrinsically understand reasons why know-hows are generated without design guidelines. Therefore extracting of the tacit knowledge is necessary. The tacit knowledge also plays an important role in various fields other than railway signalling[6] and methods to clarify the tacit knowledge have been developed[7]-[9]. Since these researches are mainly focused on extraction from human activities such as narratives and virtual reality, application to the logic seems not to be effective.

In this paper, we extracted the tacit knowledge by using a safety analysis method called functional resonance analysis method (FRAM) [10]. In FRAM a system is modelled as the functions and their connections. The model includes the way for the system to behave correctly if the system works as it is intended. Thus factors leading to the successful behaviour can be extracted. Details of FRAM are described in the next section. The relay-based LC logic works successfully for almost all the operation cases thus the successful factors, some of which are tacit knowledge can be extracted from the FRAM model of the LC logic. The extracted knowledge is exploited as design guidelines for the software LC control logic. In addition to the extraction of the design guidelines, we also evaluated validity of the extracted guidelines with a LC control logic in operation.

The rest of the paper is organized as follows: in section 2, FRAM is introduced and basic LC logic in JRE is presented in section 3. Then, the modelling of the logic with FRAM and the extraction of the design guidelines are conducted in section 4. After the validity of the extracted design guidelines is evaluated in section 5, the paper will be concluded in section 6.

## 2 FUNCTIONAL RESONANCE ANALYSIS METHOD

FRAM is one of the safety analysis methods. Its significant property is that FRAM focuses on interactions between functions and provides an overview about how a system works while conventional methods such as fault tree analysis focus on how a system fails. When the successful system is modelled with FRAM, factors that lead to the successful system can be obtained. Those factors can be exploited as design guidelines to replace the system with new technologies as well as to prevent undesired events.

The FRAM model of a target system is developed by connecting hexagon-shaped elements shown in Fig. 1. The element represents a function of the system and every function has six aspects: input, output, precondition, time, control, and resource and the elements are connected through the aspects.

Fig. 2 shows an example FRAM model about a LC. There are two elements: “Train detection at A” and “Start warning”. The output of “Train detection at A” is connected with the input of “Start warning”. This connection indicates that warning at the LC starts when the warning-start function receives the information from train detection at A. The six aspects of the elements enable to analyse interactions of a system in detail and clarify the successful factors.

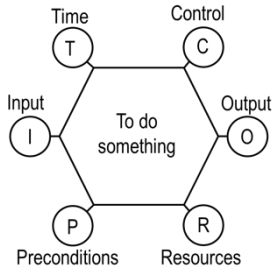



*Figure 1: Element of FRAM. One element has six aspects*

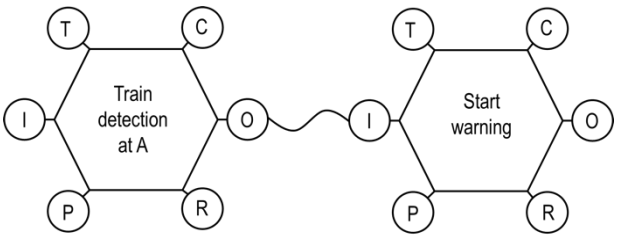



*Figure 2: Connection example. The output of “Train detection at A” is connected with the input of “Start warning”. This connection shows that warning starts when the information of train detection at A is on input to the warning-start function.*

# 3 BASIC CONCEPT OF WARNING LOGIC

The LC control logic must achieve high safety because roads and rails intersect at a LC. Although each logic of LCs differs because of differences in equipment deployment such as routes of a station and positions of signals, basic concept of warning logic is common among LCs described as below.

Fig. 3 shows the schematic diagram of equipment involved in warning. The equipment consists of a logic controller, two train detectors deployed at both sides of the LC, barriers, and warning lights. When one train detector (train detector 1 in Fig. 3) detects a train, the logic controller orders the barriers to close and the warning lights to start blinking. After the train passes the other train detector (train detector 2), the logic controller orders the barriers to open and the warning lights to stop blinking. In short, the warning continues while a train is running in a "warning zone" which ranges from one train detector to the other. In some cases, especially the case of the LC in a station, the warning zone is defined as a section from a track circuit to another track circuit. The logic controller is implemented with either electric relays or a programmable logic controller. If the logic controller fails to start the warning, the state of the barriers and the warning lights is the same as one in the case of no train. Since this situation has possibility to cause an accident, it is a hazard and we call it "no-warning situation". The control logic must be developed so that the no-warning situation does not occur.

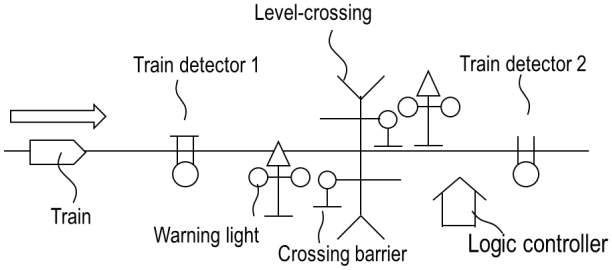



*Figure 3: Basic LC configuration. Warning starts when one train detector (train detector 1) detects a train and stops when the train passes the other train detector (train detector 2).*

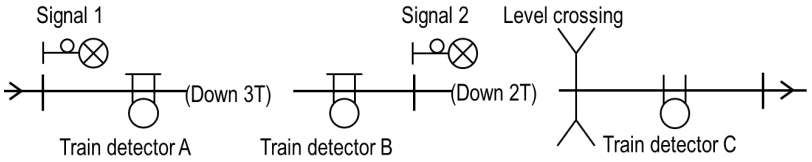
# 4 ANALYSIS AND RESULT

## 4.1 Analysis target

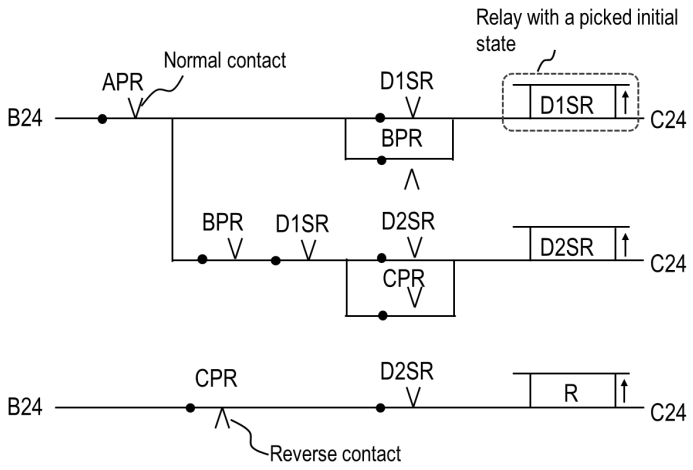
In the operating area of JRE, there are more than 6,000 LCs and they work successfully every time trains pass them. Although the control logics of the LCs are designed based on facilities around LCs: signals, rail network, track circuits and so on, typical logic patterns are defined in the case of the relay-based logic. Since the operating logics based on those patterns work successfully, design guidelines for the relay-based LC logic are useful to develop software-based LC logic. Few guidelines, however, are described while know-how is documented. In this paper, therefore, we analysed the reference logic patterns with FRAM to extract the design guidelines.

Fig. 4 (a) and (b) show the facility deployment and the connection diagram of the analysed logic. The brief warning logic and characteristics of the analysed logic are described as follows. Since the warning zone ranges from train detector A to train detector C, the LC starts warning when train detector A detects a train and stops warning when the train passes train detector C. While one train detector is enough for warning start in the control logic shown in section 3, an additional train detector B is necessary in the case of the signal deployment in Fig. 4 (a). In this facility deployment, two trains can run within the warning zone in the same time because there are two blocks in the zone. If train detector B is not deployed, the LC stops warning when one train passes the train detector C and the other is running in the track circuit "down 3T". Then the LC remains silent even though the following train reaches the LC. This is because the relay-based control logic in JRE cannot count the number of trains and only control warning based on information of train detection. However with train detector B located before signal 2, the LC can keep warning even in the same situation. Thus, the hazardous situation is avoided by deploying train detector B.

A connection diagram expresses connections among relays to implement logic and Fig. 4 (b) shows the connection diagram for the above logic. An arrow-like figure represents a used side and initial state of a relay. A downside arrow indicates that a normal contact of a relay is used. If the downside arrow has a contact to the line, the initial state of the relay is picked. If there is no contact, the initial state is dropped. In the case of an upside arrow, a reverse side is used and a contact to the line indicates that the initial state of the relay is dropped. For example, APR that is a relay for train detector A, has a contact with the line and the downside arrow is used. In this case, the default state of APR is picked and a normal contact is used. Fig. 4 (c) shows the legend of the arrows. D1SR and D2SR represent a relay to indicate a section where a train is running and "D" stands for down. A LC starts warning when the state of the relay "R" is dropped and it stops when picked.




(a)




(b)

| | | Initial state | |
|---|---|---|---|
| | | Picked | Dropped |
| contact side | Normal | V | V |
| | Reverse | Λ | Λ |

(c)

| Train detector | Steady state | State in train detection |
|---|---|---|
|  | Picked | Dropped |
|  | Dropped | Picked |

(d)

*Fig. 4 An example of the analysed logic. (a) Facility deployment diagram. (b) Connection diagram corresponding to (a). The contact symbol of each relay indicates the initial contact side. The legends of them are shown in (c). The upward arrows shown at the side of the relays show that the initial state of the relay is picked. (c) Legends of the relay contacts. There are four patterns in terms of the used side and initial state of the relay. (d) Legends of the train-detector states. The behaviours of the two train detectors are opposite.*

## 4.2 FRAM Model

The FRAM model shown in Fig. 5 was developed based on the connection diagram in Fig. 4 (b). In this paper, functions used in FRAM were defined as state transition of each relay. If an analyst abstracts the connection diagram to a few function blocks, the abstraction could hide some design guidelines. Therefore we developed the model with the most primitive functions, which are the state transitions, so that guidelines can be extracted as many as possible.

Although the connection diagram expresses the control logic, only connections between the relays are described. Hence the analyst has to interpret the meaning of the diagram. Meanwhile the FRAM model expresses the meaning of the connections in detail because the hexagonal FRAM element has six aspects. For example, the function D2SR-drop has two inputs from A-in and B-in. These connections indicate that the LC starts warning when either train detector A or B detects a train. The D2SR-pick function has one input and three preconditions. These connections shows that the relay D2SR is picked with the input after three preconditions are satisfied. In this way the six aspects of the elements enable the system to be modelled with detail information whereas the arrows on the same line seem to have the same meaning in the connection diagram.

The modelling regarding D1SR and D2SR is described below. Since D1SR relay changes to the dropped state with detection of the train by train detector A, the output of A-in which represents that the train enters the detection section of A is connected to the input of D1SR-drop. Then after the train is detected by train detector B that corresponds to B-in, D1SR is picked. Thus the output of B-in is connected to the input of D1SR-pick. Similarly when train detector A or B detects the train, D2SR changes to the dropped state and warning starts. Hence the input of D2SR-drop has connections with the output of A-in and B-in and the output of D2SR-drop leads to the start of warning. The train detection at train detector C allows D2SR to be picked after going out of A and B, entering C, and picked D1SR which corresponds to A-out, B-out, C-in, and D1SR-pick logics are satisfied. Thus, the three logics and C-in are connected with the precondition and input of D2SR-pick, respectively.

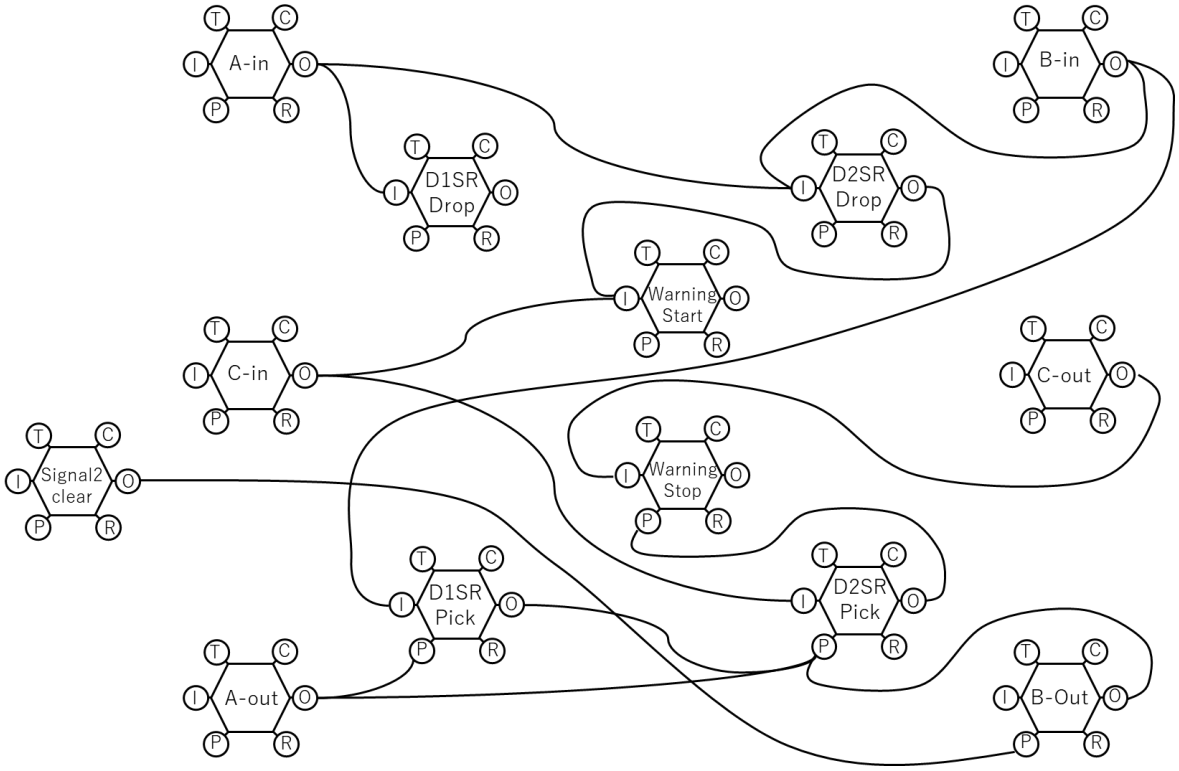



*Figure 5: The developed FRAM model corresponding to the logic shown in Fig. 4 (b).*

The input of R-drop has a connection with the output of D2SR-drop because the LC must start warning immediately when the train run into the warning zone. It is also connected with C-in. This is because detecting train by train detector C without any preceding sequences indicates that an unexpected event could happen. Thus the output of C-in is connected with start warning to avoid any hazardous situation. The input and precondition of R-pick has a connection with the output of C-in and the output of D2SR-pick, respectively. The transition of D2SR from the dropped state to the picked one shows that the last train within the warning zone reaches train detector C. In this situation, however, the train is still within the warning zone, thus C-out that indicates that the train passes train detector C is necessary to ensure no trains are in the warning zone.

The element of "signal 2 clear" is a function of a blocking system and represents that a clear aspect is indicated on signal 2. The output of "signal 2 clear" is connected with the precondition of B-Out. This is because a train can go out of train detector B only when signal 2 shows a clear aspect.

## 4.3 Extracted design guidelines

As a marked characteristic, a symmetry of the elements can be observed. Each element has two states. For example, there are the picked/dropped state for train detectors and the start/stop warning for R. One state is used for start warning and the other is for stop warning. The opposite status in the stop phase works to ensure that the state of the element is no longer the one used to start warning. Note that the train detector C crosses both sides. This is because it is involved in both start/stop warning. Therefore a design guideline extracted from this fact is that logic should be developed with the symmetry configuration.

Other significant design guideline is that the elements form a layered architecture. As shown in Fig. 6, there are three layers each of which represents a purpose of functions and connections are basically made between neighbouring layers. The bottom layer is a physical layer. The train detectors A, B, and C are sensors, or physical elements. They detect a train and send its information to a train-tracking layer, which is a middle layer and is composed mainly from relays with "SR" in their name. The elements in the middle layer work to trace train running, in other words, what section the train is running in. The trace information is connected to the top layer, or the warning layer which decides whether warning starts or stop. In this way, the connections are made between neighbouring elements and not made beyond the middle layer. This simple architecture enables safety control even though detail logic is different among LCs. Note that only C-in in the physical layer is directly connected with the warning layer. This is because train detection at C without any preceding sequence indicates possibility of any hazards and warning must starts immediately to avoid accidents.

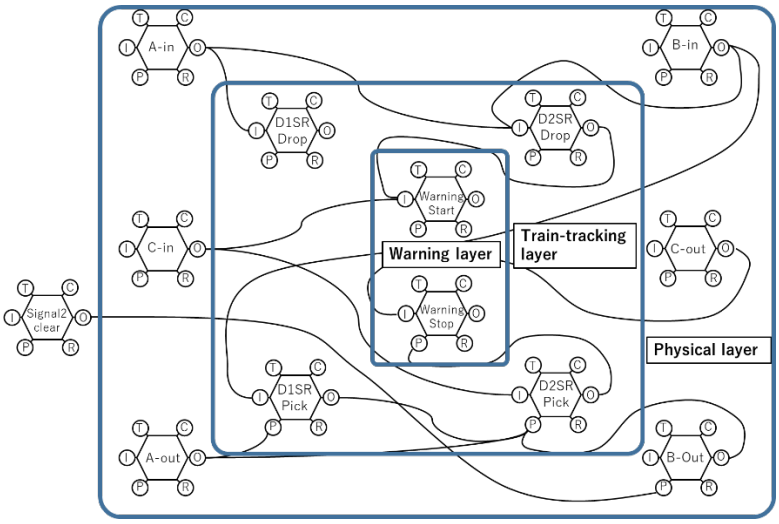



*Figure 6: pyramid architecture. There are three layers: a physical layer, a train-tracking layer, and a warning layer in the order from the bottom to the top. Connections are made between the neighboring layers except C-in.*

Fig. 7 shows a part of the FRAM model regarding warning start. The suggestive point is that no logic is connected with the precondition of D2SR. One of the important LC-control functions is to start warning immediately when the train reaches the warning zone. Thus, no preconditions is necessary to start warning.

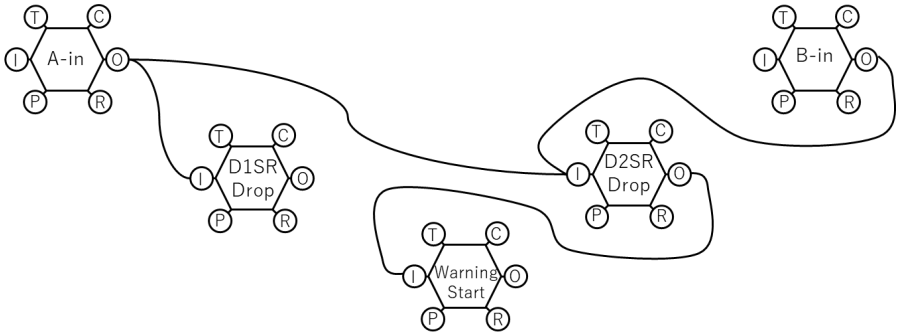



*Figure 7: The warning start part of the FRAM model.*

In additon to reliable warning start, a warning stop with confidence of no train in the warning zone is also important. Fig. 8 is a part of the FRAM model regarding warning stop. As described in section 4.2, the input and the precondition of warning stop is connected with the output of C-out and the output of D2SR-pick, respectively. D2SR has to be picked with sufficient confidence because D2SR-pick indicates that no trains are running in the warning zone. Such a confidence is formed as follows. While the input of D2SR-pick has a single connection with the output of C-in, there are three connections into the preconditions of D2SR-pick: D1SR- pick, A-out, and B-out. The satisfaction of these three conditions shows that no trains are running in the section from A to B. With that information, train detection at C assures that the train reaching C is the last train in the warning zone thus D2SR is picked. In this way, train-tracking information of the passed section helps to change the train-tracking state of the section safely.

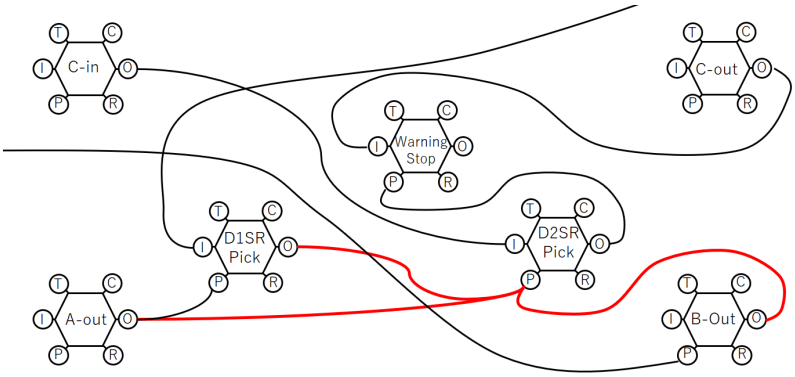



*Figure 8: The warning stop part of the FRAM model.*

## 5 EVALUATION

The validation of the extracted guidelines is evaluated by comparing with operating LC logic. Fig. 9 shows the network and the facility deployment diagram of the evaluated LC. There are five warning patterns: one for an outbound train shown by the solid line and four for an inbound one shown by the dashed lines. Since warning logic for the outbound train is simple and similar to the logic in section 4, we focused on the logic for the inbound train to evaluate the validity of the guidelines from a viewpoint of a different logic.

The warning logic of the four warning patterns is briefly described as follows. The logics of Inbound-1 to 3 are similar. Before the warning starts, the train is stopping at the platform. The departure route is set and a clear aspect is indicated on the departure signal and warning starts. The warning continues until the train passes a train detector beyond the LC. In the case of Inbound-4, the train passes through the station without stopping at the platform. The home signal and the departure signal are set and the warning starts when the train passes the home signal. The warning stops by the train passing the train detector. Inbound-3 and Inbound-4 are selected according to a route selection. Note that the connection diagram for this logic is not shown because it is too complex to explain in this paper.

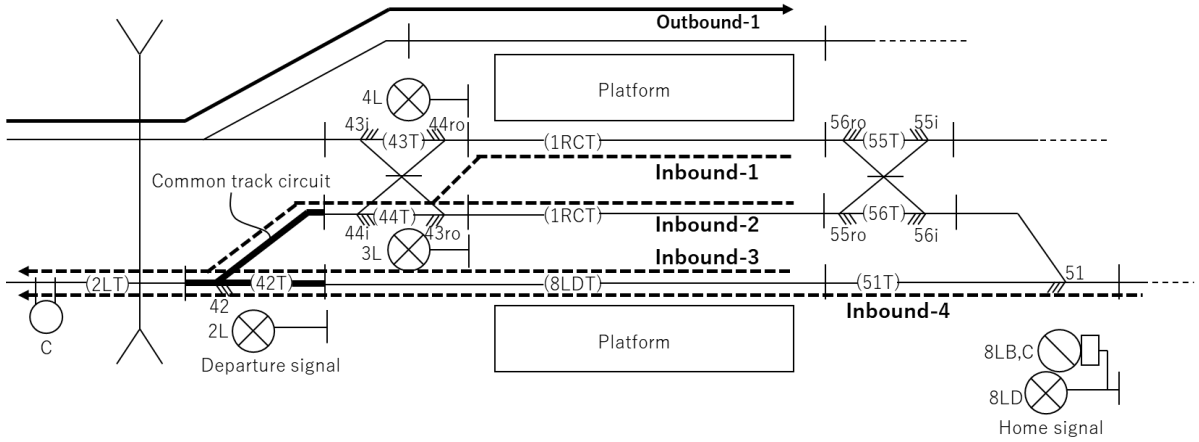



*Figure 9: Network and facility deployment diagram of the evaluated LC. One rounte for an outbound train and four routes for an inbound train. The track circuit depicted with a bold line is common for all the outbound routes.*

Fig. 10 indicates the FRAM model for the warning logic. Boundary colours of the elements show types of functions: orange and blue elements represent interlocking-related functions and physical sensors like track circuits whereas green and red elements correspond to train-tracking functions and warning functions. The symmetry of the elements and the pyramid structure are clearly observed. The outputs of C-in and Up-SR-drop are not connected with the input of the warning-start but Up-SRPR-drop. This is conducted just to improve visibility of the logic. Since the output of Up-SRPR-drop is connected with the input of the warning-start without preconditions, this logic pattern is equivalent to that of the reference logic. In the warning-stop logic, the model also follows the extracted guidelines. The input of the warning-stop is connected with the output of Up-SRPR-pick, and the output of the C-out and the precondition of Up-SR-pick drive the Up-SRPR-pick. Furthermore, Up-SR is picked when C-in happens after FEHSR, which indicates all trains are going out of a common track circuit shown in bold line in Fig. 10, is picked and all track circuits in the routes are vacant. In this way, warning stops by using train positions as preconditions. This logic structure that collects train position information as preconditions satisfied the guideline in the warning-stop phase.

From above discussions, all the guidelines extracted in section 4 is observed in the evaluated LC logic. Therefore we ensured those guidelines are valid for logic designs. Moreover, when we ask signal engineers in JRE about usefulness of the guidelines, they answered that the guidelines are natural for the signal engineers but not documented so the guidelines are useful. This answer supports that the guidelines can be also practical as well as valid.

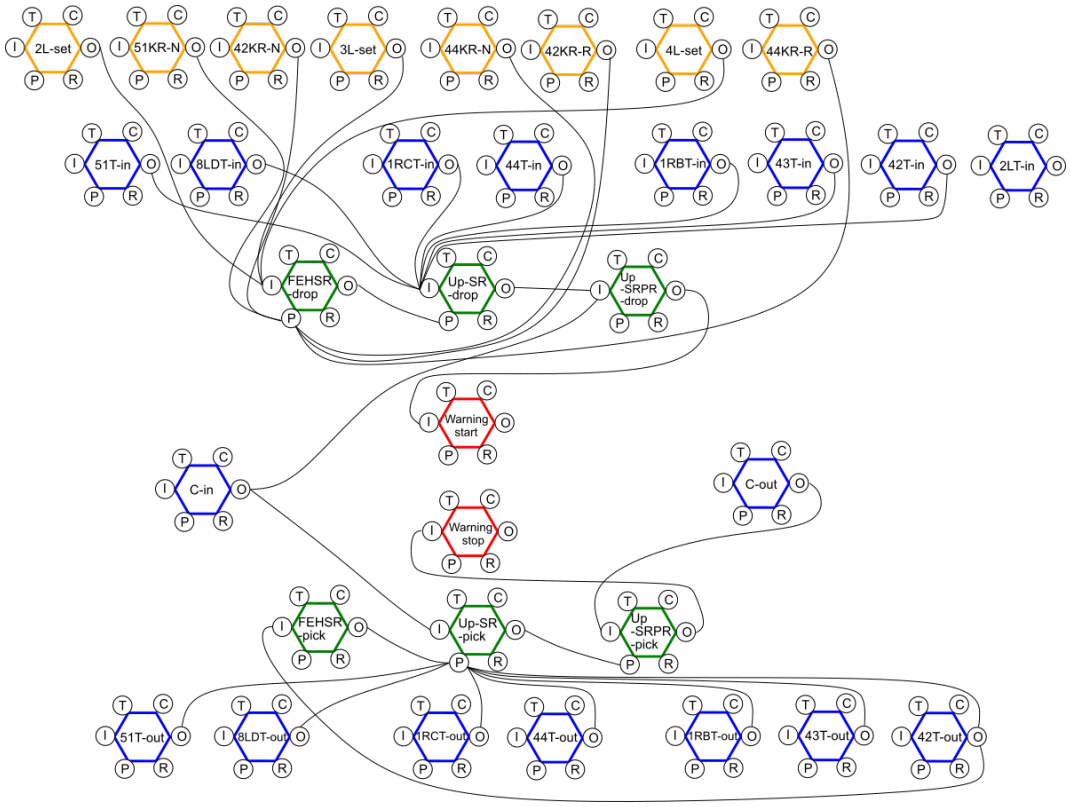



*Figure 10: FRAM model of the evaluated logic. All the extracted guidelines in section 4 are observed in this model.*

# 6 CONCLUSION

In this paper, we clarified four design guidelines for LC logic which are considered to achieve high safety at LCs. Functional resonance analysis method (FRAM) was applied to the reference logic patterns of JRE that can include tacit knowledge and know-how. We extracted the four design guidelines, which are essential but tacit for signalling engineers of JRE. The validity of the extracted guidelines was also evaluated by modelling a LC logic in operation with FRAM and comparing the FRAM model with the guidelines. As a result, all the guidelines are observed in the FRAM model. Therefore we ensured that the extracted guidelines are valid and FRAM is useful to clarify implicit knowledge from an existing system. The extracted guidelines will be utilized for the next development of LC controllers.

# 7 REFERENCES


1. Tamvakis, P. and Xenidis, Y. (2012). Resilience in transportation systems, *Procedia – Social and Behavioral Sciences, 48, pp. 3441-3450.*

2. Adjetey-Bahun, K., Birregah, B., Châtelet, E., and Planchet, J. (2016). A model to quantify the resilience of mass railway transportation systems, *Reliability Engineering & System Safety,* 153, pp. 1-14.

3. Ngamkhanong, C., Kaewunruen, S., and Costa, B. (2018). State-of-the-Art Review of Railway Track Resilience Monitoring, *Infrastructures,* 3(1), p. 3.

4. East Japan Railway Company, [online] Available at: https://www.jreast.co.jp/ [Accessed 15th May 2019]

5. Teramoto, M., Miyaguchi, N., Okada, A., Fukuta, Y. (2015). Development of microelectronic level crossing controller with a built-in constant warning time control logic, *The proceedings of International Symposium on Speed-up and Service Technology for Railway and Maglev Systems (STECH)*, 2015(0), pp._1A23-1_-_1A23-12_.

6. Alwis, R. S., Hartmann, E., and Genmunden, H. (2004). The role of tacit knowledge in innovation management, *The proceedings of 20th Annual IMP Conference*.

7. Nonaka, I., and von Krogh, G. (2009). Tacit Knowledge and Knowledge Conversion: Controversy and Advancement in Organizational Knowledge Creation Theory, *Organization Science*, Vol. 20, No. 3, pp. 635-652.

8. Prodgorski, D. (2010). The Use of Tacit Knowledge in Occupational Safety and Health Management Systems, *International Journal of Occupational Safety and Ergonomics 2010*, vol. 16, No. 3, pp. 283-310.

9. Hadikusumo, B. H. W. and Rowlinson, S. (2004). Capturing Safety Knowledge Using Design-for-Safety-Process Tool, *Journal of Construction Engineering and Management,* Vol. 130, No. 2, pp. 281-289.

10. Hollnagel, E. *Home*. [online] Functionalresonance.com. Available at: http://www.functionalresonance.com/ [Accessed 16th May 2019].

11. Bhardwaj, M. and Monin, J. (2006). Tacit to explicit: an interplay shaping organization knowledge, *Journal of Knowledge Management*, Vol. 10(3), pp. 72-85.

12. Grabowski A. and Jankowski J. (2015). Virtual Reality-based pilot training for underground coal miners, *Safety Science,* Vol. 72, pp. 310-314.