THE ASSESSMENT TO ACHIEVE SAFETY OF THE TRAIN DOOR SYSTEM IN IEC 61058 (THE CASE OF BUSAN-GIMHAE LIGHT RAPID TRAIN)

Tae Keun Park, Keun Woo Park and Koyu Uematsu

Received June 12, 2012

Abstract. This paper presents the hazard analysis of the events which caused passengers to fall to the ground due to an unscheduled opening of a train door while the train is moving in Busan-Gimhase Light Rapid Train. The train has the Door/Lock function and Safety Detection of the Door Close/Lock Status as safety functions to achieve safety in order to reduce the probability of that hazard. This paper discusses the assessment to achieve safety on an unscheduled opening by the inspection given in IEC 61058 of both the safety functions. The door system was provided for BGLRT by Vapor Europe srl and the assessment based on its Technical Report[6] and SIL Analysis[7] in IEC 61068 has been carried out. According to the assessment, it is concluded that the door system is designed to minimize the probability of an unscheduled opening of door while a train is moving and that residual risk of the system is acceptable.

1 Introduction Busan-Gimhae Light Rail Transit (hereinafter BGLRT) System has adopted Communication Based Train Control (CBTC) for full driverless system[5]. In order to secure safety, SIL (Safety Integrity Level) has been introduced at the phase of conceptual design for functionality of major systems based on ISO/IEC Guide 51 which was jointly prepared by ISO and IEC in 1990[2]. The ISO/IEC Guide 51 is a international safety guideline with which IEC 61508 is developed. The formal name of this standard is Safety Aspects - Guidelines for their inclusion in Standards. It stipulates basic definitions of Risk and Hazard as follows. Risk is defined as 'combination of the probability of occurrence of harm and the severity of that harm'. Hazard is defined as 'potential source of harm'. And for your reference, harm is defined as 'physical injury to the health of people either directly, or indirectly as a result of damage to property or to the environment'.

The IEC 61508 has been issued in 2000 as a standard regarding functional safety of safety related items of electrical/ electronic/ programmable electronic system and the second revison of it was issued in 2010. The formal name of this standard is "Functional safety of electrical/ electronic/ programmable electronic safety-related systems".

2 Mathematical formulas

2.1 Hazard Rate It is assumed that the system consists of the n components and all components are non-repairable. A k-out-of-n structure fails if and only if at least k of the n components are failed. In particular, an n-out-of-n structure is a parallel structure and a 1-out-of-n structure is a series structure.

2000 *Mathematics Subject Classification.* Primary 47N30.

Key words and phrases. IEC 61508, Tolerable Hazard Rate (THR), Safety Integrity Level (SIL), Fault Tree Analysis (FTA).

When the components in k-out-of-n which are independently and identically distributed as $Q_s(t)$, the *unavailability* $Q(t)$ of the system can be expressed as

$$Q(t) = \sum_{i=k}^{n} \binom{n}{i} [Q_s(t)]^i [1 - Q_s(t)]^{n-i}, \tag{1}$$

where $\binom{n}{i} = n!/(i!(n-i)!)$ and t is system lifetime.

Moreover, if $Q(t)$ is differentiable at t,

$$\begin{aligned} q(t) &= \frac{dQ(t)}{dt} \\ &= k\binom{n}{k} q_s(t)[1 - Q_s(t)]^{n-k}[Q_s(t)]^{k-1}, \end{aligned} \tag{2}$$

where $q_s(t)$ is probability density of the failure of components.

And the *hazard rate* $\lambda(t)$ is defined by

$$\lambda(t) = \frac{q(t)}{1 - Q(t)}. \tag{3}$$

Thus, we can obtain (4) by (1) and (2).

$$\lambda(t) = \frac{k\binom{n}{k} q_s(t)[1 - Q_s(t)]^{n-k}[Q_s(t)]^{k-1}}{1 - \sum_{i=k}^{n} \binom{n}{i} [Q_s(t)]^i [1 - Q_s(t)]^{n-i}}. \tag{4}$$

We assume that $Q_s(t)$ has exponential distribution with the *failure rate* r_s as below.

$$Q_s(t) = 1 - e^{-r_s t}. \tag{5}$$

Therefore, unavailability and hazard rate are (6) and (7) respectively,

$$Q(t) = \sum_{i=k}^{n} \binom{n}{i} [1 - e^{-r_s t}]^i [e^{-r_s t}]^{n-i} \tag{6}$$

and

$$\lambda(t) = \frac{k\binom{n}{k} r_s e^{-r_s t}[e^{-r_s t}]^k [1 - e^{-r_s t}]^{n-k}}{1 - \sum_{i=k}^{n} \binom{n}{i} [1 - e^{-r_s t}]^i [e^{-r_s t}]^{n-i}}. \tag{7}$$

Meanwhile, when the components do not have identical distribution, it is complex to write down k-out-of-n system.

2.2 Safety Integrity Level(SIL) Allocation with Demand Rate The safety function demand is divided into the low demand mode and the high demand mode. The low demand mode is that safety function is activated for every demand, while high demand mode is that safety function is activated consecutively by preinstalled protective system.

The level of SIL is defined from 1 to 4 in IEC 61508 which mentioned in Chapter 1, and allocated as Table 1.

In case of the low demand mode, the PFD (Probability of Failure on Demand) can be expressed as

$$PFD = \frac{\lambda(t)}{d(t)}, \tag{8}$$

Table 1: Safety Integrity Levels (IEC 61508)

SIL	Low Demand Mode	High Demand Mode
4	$10^{-5} \leq PFD < 10^{-4}$	$10^{-9} \leq THR < 10^{-8}$
3	$10^{-4} \leq PFD < 10^{-3}$	$10^{-8} \leq THR < 10^{-7}$
2	$10^{-3} \leq PFD < 10^{-2}$	$10^{-7} \leq THR < 10^{-6}$
1	$10^{-2} \leq PFD < 10^{-1}$	$10^{-6} \leq THR < 10^{-5}$

PFD: Probability of Failure on Demand per hour

THR: Tolerable Hazard Rate per hour

where $d(t)$ means Demand Rate, which is newly proposed in this paper.

In case of the high demand mode, absence of protection system for single safety related function can lead accidents anytime. It means, protection system should be operated consistently, so we assume that demand rate $d(t) = 1$ in (8).

Consequently, the THR can be expressed as (9).

$$THR = PFD = \lambda(t). \tag{9}$$

3 Assessment on achieved safety

3.1 Door Configuration A train for BGLRT consists of 2 cars and one car of the train has 2 doors on each side. Thus the train has 8 doors. Exterior configuration of one door is shown as Figure 1.

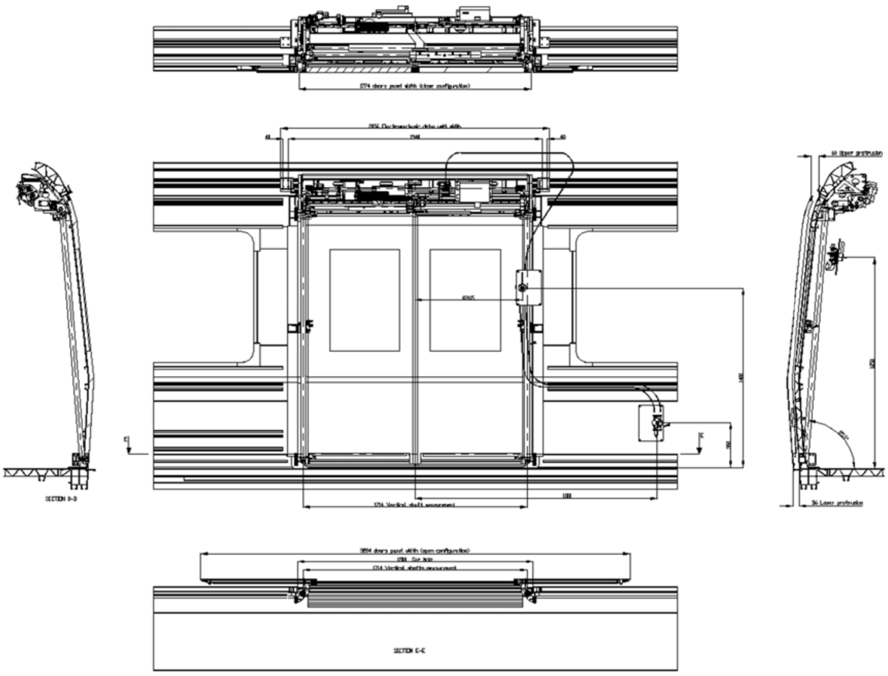


Figure 1: Exterior configuration of door system

For the BGLRT system, the ATP(Automatic Train Protection) system is adopted as a sytem protection. The door system is a motorized system, which can increase risk compared to legancy systems and it is electrically controled by an ATO and electrically monitored by an ATP system at train level which is installed in a car as a part of the ATP system.

Also, the ATP system authorizes train doors to be opened only if DC(Door Controller) received ZV(Zero Velocity) signal which is activated when the measured velocity of train by the ATP system is below 0.125m/s. Each door has its own DC. Figure 2 shows the interface connection between train door and signal.

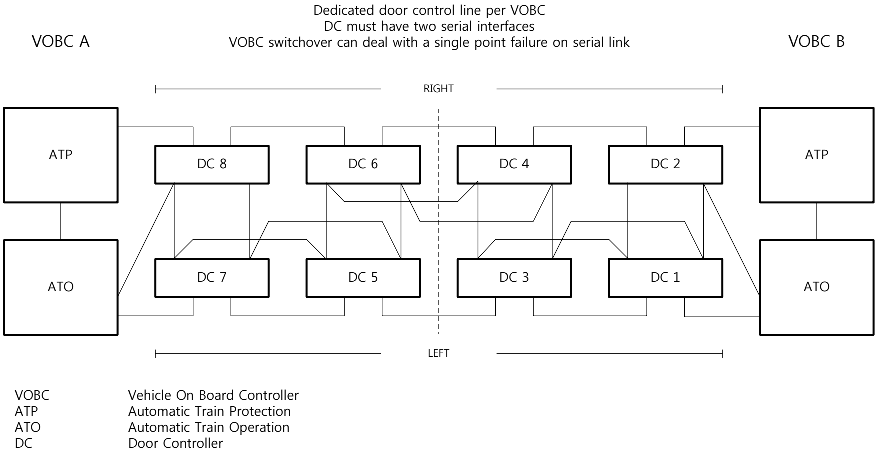

Dedicated door control line per VOBC
DC must have two serial interfaces
VOBC switchover can deal with a single point failure on serial link
VOBC A
VOBC B
RIGHT
ATP
DC 8
DC 6
DC 4
DC 2
ATP
ATO
DC 7
DC 5
DC 3
DC 1
ATO
LEFT
VOBC Vehicle On Board Controller
ATP Automatic Train Protection
ATO Automatic Train Operation
DC Door Controller

Figure 2: Interface between train door and signal

3.2 Door Closed/Locked Function Failure Door Closed/Locked function is to address the hazard which is related to the unexpected doors opening when the train is moving. Failures of this function in normally operating, which are identified in the Hazard Log are that one of the doors is not closed or not locked, that a door not closed is considered to be opened by an ATP system and that a door not locked can be manually opened.

3.2.1 FTA on Door not Closed Door closed status is kept by Sliding Bush and Dragging Support on the upper part and Vertical Shaft and Additional Retention Device on the lower part. Sliding Bush and Dragging Support is directly involved to the status of Door kept closed and Vertical Shaft and Additional Retention Device is involved to Door kept closed by combination of internal components. Vertical Shaft is installed parallel to train door at left/right side and guides train door lower part movement and supports up/down with Support Bracket. Also, it keeps door detachment or closed status by Additional Retention Device and Lower Retaining Device. Lower Retaining Device is consisted of Retaining Pin and Spring.

Sliding Bush and Dragging Support have basic failure rate of 1.25×10^{-8} failures/h and 5.00×10^{-11} failures/h respectively from FMECA analysis and the probability to have a failure is higher when train door is closing/opening than when it is static. Therefore, when we consider the failure rate of Sliding Bushes and Dragging Support is 10% of the basic failure rate, we have 1.25×10^{-9} failures/h and 5.00×10^{-12} failures/h to be applied for FTA. Loss of function of Support Bracket is lead to loss of function of Vertical Shaft. As these devices are retaining devices, basic failure rate of 3.75×10^{-9} failures/h from FMECA is applied as it is. Loss of function of Lower Retaining Device requires the condition that one of the two components of Lower Retaining Device must be broken status(Retaining Pin or Spring), and simultaneously, Support Bracket should be broken status. This is applied both for left-side door leaf and right-side door leaf. As these devices are retaining devices, basic failure rate of 1.667×10^{-7} failures/h and 2.000×10^{-7} failures/h from FMECA is applied to FTA as it is.

FTA related to door not closed is shown as Figure 3.

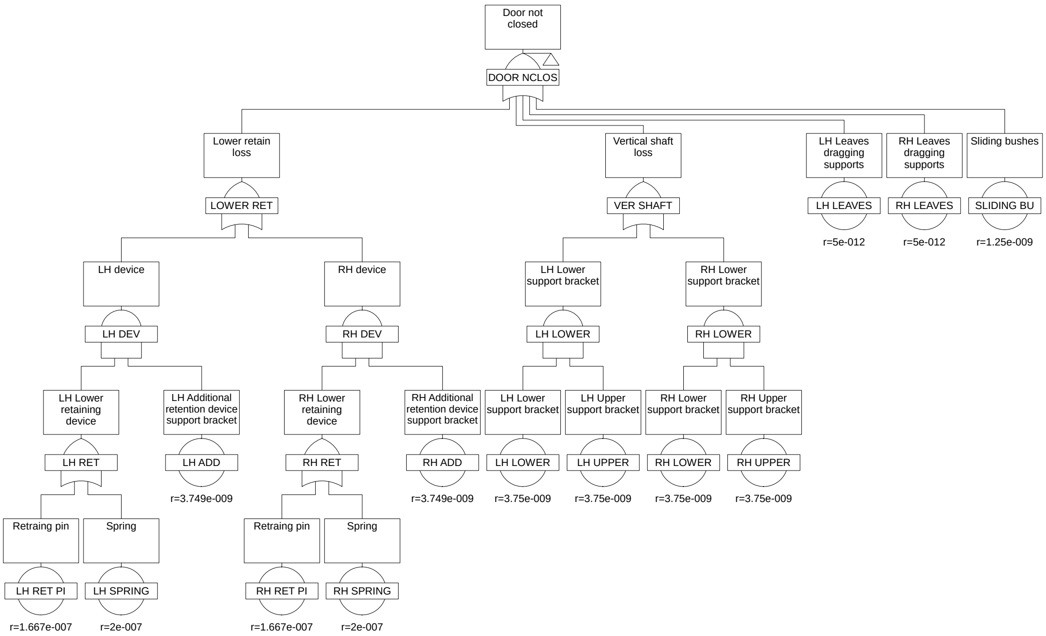


Figure 3: Door not Closed

3.2.2 FTA on Door not Locked Door locked is kept by Over Centre Connection Rod in order to fix the train in case of forces exerted from inside of train to the outside and the Over Centre Connection Rod is located one at each side of Over Centre Shaft. Door locked is lost when both connecting rods are broken, since in case of only one connecting breakdown, the other connecting rod maintains the locked.

From FMECA analysis, basic failure rate for each connecting rod is 5.00×10^{-9} failures/h, the probability to have a failure is greater when train doors are working instead of when they are static, we can consider that the failure rate of the connecting rods when the train is moving is 10% of the basic failure rate and we have 5.00×10^{-10} failures/h to be used for FTA.

FTA related to door not locked is shown as Figure 4.

3.2.3 FTA on Door Unscheduled Opening The hazard which is applied to unscheduled door opening is classified and considered as manual opening status and automatic opening status. Unscheduled manual opening train door during train is moving can be occurred by passenger activation of emergency handle and motor brake of train is not applied but released. There are 3 cases of motor brake releasing. First, the case of motor brake is always released, DCU failure commanding incorrect brake release, or ZVR(Zero Velocity Relay) wrong request, which is activated when the measured velocity of train is below 0.125 m/s.

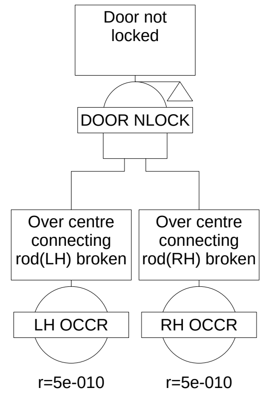

Door not locked
DOOR NLOCK
Over centre connecting rod(LH) broken
Over centre connecting rod(RH) broken
LH OCCR
RH OCCR
r=5e-010
r=5e-010

Figure 4: Door not Locked

When we consider that emergency handle activation by passenger occurs once a year while train is moving 19 hours a day, 1/(365 days × 19 hours) $= 1.442 \times 10^{-4}$ movement/h. Motor brake failure has basic failure of 8.333×10^{-8} failures/h from FMECA. The motor brake is power supplied and activated, only if the emergency handle is activated when the train is moving in order to prevent manual opening of train door. However, due to the reason of safety, the movement of brake is released by software when train stopping. Therefore, the probability of brake breakage when train is stopped is more higher compared to the case when it is moving. When we consider it is 5% of the basic failure rate, 4.165×10^{-9} failures/h is applied to FTA. Basic failure of DC is 1.25×10^{-5} failures/f from FMECA. When we consider the failure rate from FMECA for DC commanding incorrect brake release is 0.1% of overall DC failure rate, 1.25×10^{-8} failures/h is applied to FTA. ZVR signal is vehicle line signal and the failure rate 5.120×10^{-10} failures/h is applied from Signaling System Hazard Log[5]. Door opening signal is the case that opening command is activated from DC or train line, and simultaneously Enable 1, Enable 2 and ZVR(Zero Velocity Relay) signal from train line is activated. Otherwise, it becomes unscheduled train door automatic opening status.

As Enable 1, Enable 2 and ZVR is input signal from Signaling System Hazard Log[5], failure rate 5.120×10^{-10} failures/h is applied.

FTA related to unscheduled train door opening is shown as Figure 5.

3.2.4 Assessments on Door Closed/Locked Function Failures Through analysis from Chapter 3.2.1 to 3.2.3, Figure 6 shows the FTA on Door Closed/ Locked function.

A system lifetime t of 19 hours per train is considered. That means the time from train start-up with daily door test (system 100% available) to the end of daily service (train take-down).

System unavailability $Q(t)$ and hazard rate $\lambda(t)$ can be evaluated from (6) and (7). First we consider that door Closed/Locked function is high demand mode from Table 1 and using the (9). Thus, the result of calculation is as follows: $Q(19) = 2.483 \times 10^{-8}$ failures/h and $\lambda(19) = 1.354 \times 10^{-9}$ failures/h.

Meanwhile, according to Chapter 3.1, as the 1 train set has 8 sets of train doors, door Closed/Locked function has failure rate of 1.083×10^{-8} failures/h. Thus, the value is over SIL 3 according to Table 1.

3.3 Analysis on Safe Detection Function Failure of Door Closed/Locked Status

The Function Block Diagram(FBD) of normal condition of safe detection function door

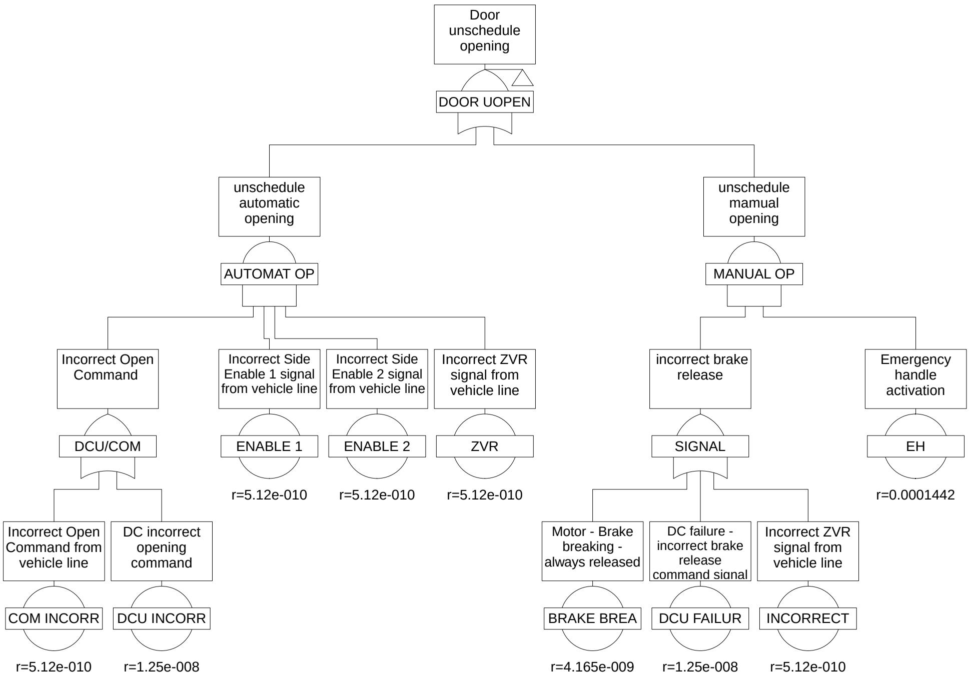

Door unschedule opening
DOOR UOPEN
unschedule automatic opening
AUTOMAT OP
unschedule mamual opening
MANUAL OP
Incorrect Open Command
DCU/COM
Incorrect Side Enable 1 signal from vehicle line
ENABLE 1
r=5.12e-010
Incorrect Side Enable 2 signal from vehicle line
ENABLE 2
r=5.12e-010
Incorrect ZVR signal from vehicle line
ZVR
r=5.12e-010
incorrect brake release
SIGNAL
Emergency handle activation
EH
r=0.0001442
Incorrect Open Command from vehicle line
COM INCORR
r=5.12e-010
DC incorrect opening command
DCU INCORR
r=1.25e-008
Motor - Brake breaking - always released
BRAKE BREA
r=4.165e-009
DC failure - incorrect brake release command signal
DCU FAILUR
r=1.25e-008
Incorrect ZVR signal from vehicle line
INCORRECT
r=5.12e-010

Figure 5: Door unscheduled opening

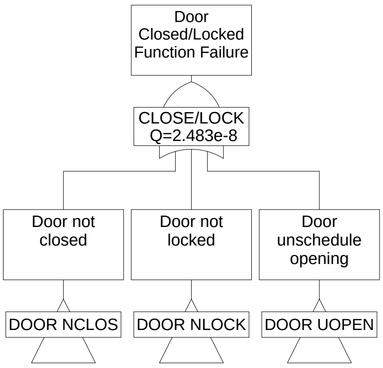
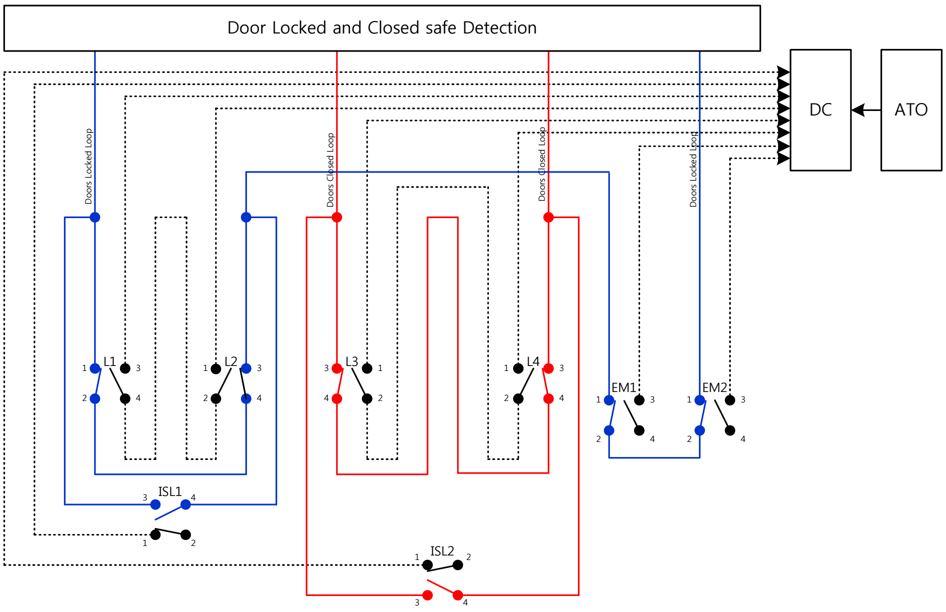


Figure 6: Door Closed/Locked function failure

Closed/Locked status is shown as Figure 7.

Safe detection function of door Closed/Locked status means safe detection at train line level, and we consider the signal composing traction loop as door closed loop and door locked loop(refer to Figure 7). Traction loop mentioned here is not signal line which is used to transfer status information of train door to vehicle, but train line in order to prevent train is moving under the situation that train door is opened or one or more train door couldn't perform closing function[9]. As shown in Figure 7, Safe detection function of door Closed/Locked status provides contact points such as 2 Close Door Microswitch, 2 Locked Door Microswitch, 2 Emergency Microswitch and 2 Isolation Microswitch. This traction loop is well known as a similarly or identically generally applied safety loop at train vehicle. This is based on the fact that the traction loop inhibits train motion when train door opens.



ATO	Automatic Train Operation
DC	Door Controller
L1	Locked Door Microswitch
L2	Locked Door Microswitch
L3	Close Door Microswitch
L4	Close Door Microswitch
ISL1	Isolation Microswitch
ISL2	Isolation Microswitch
EM1	Emergency Microswitch
EM2	Emergency Microswitch

Figure 7: FBD of safe detection function of door Closed/Locked status

Safe detection means that possible wrong detection of train door status does not impact on passengers safety. Therefore, to have unsafe situation, train line allows the train to move when train door is opened.

Train door Closed signal is configured in series with Microswitch L3 and L4, train door Locked signal is configured in series with Microswitch L1, L2, EM1 and EM2. Isolation Microswitch ISL1 bypasses Locked Microswitch L1 and L2, ISL 2 bypasses Closed Microswitch L3 and L4. The status information of each Microswitch of train door is basically monitored through DC.

Figure 8 shows door Closed/Locked status according to opening/closing of Microswitch under normal function.

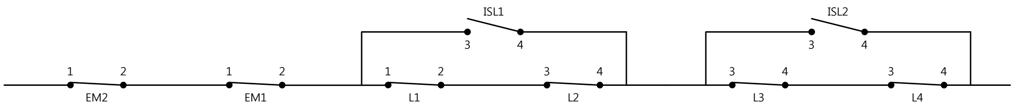


Figure 8: Door Closed/Locked status

From above analysis, probability of Safe detection of the status door Closed/Locked failure when train is opened can be classified to single fault and multiple faults. Single fault will be explained in Chapter 3.3.1∼3.3.3 and multiple faults will be explained in Chapter

3.3.4.

3.3.1 Case 1 Under the condition that 2 Isolation Microswitches are normal status, 1 among 6 Microswitch are closed status. At this time, if the rest Microswitch are open status, train door will be detected as opened status and it will be detected as unsafe condition from train line level and it will prohibit train is moving. Thus, failure of safe detection of the status door Closed/Locked is the case that EM1-EM2-L1-L2-L3-L4 are all closed status and eventually it cannot detect train door opening and cause a serious hazard to passenger.

For Emergency Microswitch and Closed/Locked Microswitch, the basic failure rate 8.333×10^{-9} failures/h and 5.882×10^{-7} failures/h are applied to FTA from FMECA. Therefore, FTA for all 6 Microswitch closed status is shown as Figure 9.

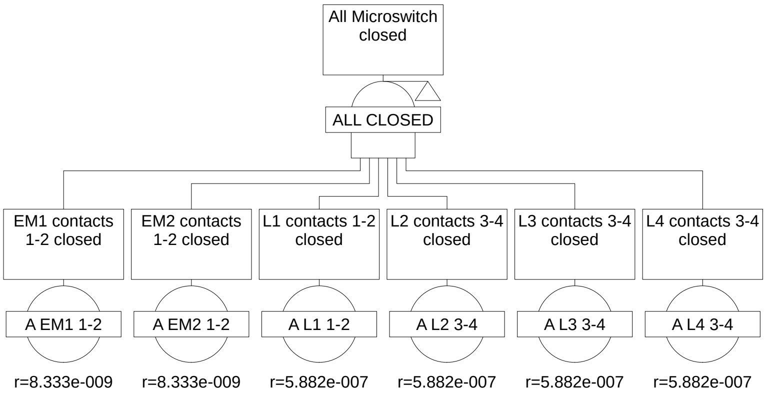


Figure 9: All Microswitch closed failure

3.3.2 Case 2 This is the case that Locked Isolation Microswitch is failed among Close/Locked Isolation Microswitch. At this time, if Closed Isolation Microswitch is normal status, it is detected as train door opened status and it will be detected as unsafe from train line level and it will prohibit train is moving. Thus, failure of safe detection of the status door Closed/Locked is Close Isolation Microswitch ISL 1 close and Microswitch EM1-EM2-L3-L4 are all closed status and eventually it cannot detect train door opening and cause a serious hazard to passenger.

Locked Isolation Microswitch has basic failure rate of 1.000×10^{-7} failures/h from FMECA and it is applied to FTA. At this time, basic failure rate of Emergency and Closed Microswitch is same as that of 3.3.1 Case 1. Therefore, FTA for the case that Locked Isolation Microswitch is closed status and Emergency and Closed Microswitch is closed status is shown as Figure 10.

3.3.3 Case 3 This is the case that Closed Isolation Microswitch is failed among Close/Locked Isolation Microswitch. At this time, if Locked Isolation Microswitch is normal status, it is detected as train door opened status and it will be detected as unsafe condition from train line level and it will prohibit train is moving. Thus, failure of safe detection of the status door Closed/Locked is Close Isolation Microswitch ISL 2 close and Microswitch EM1-EM2-L3-L4 are all closed status and eventually it cannot detect train door opening and cause a serious hazard to passenger.

Closed Isolation Microswitch has basic failure rate of 1.000×10^{-7} failures/h from FMECA and it is applied to FTA. At this time, basic failure rate of Emergency and Closed

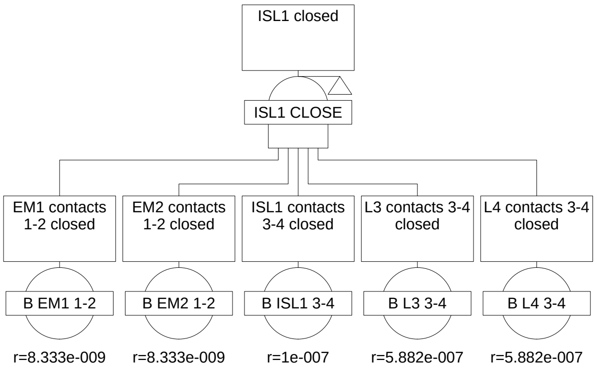


Figure 10: ISL1 closed failure

Microswitch is same as that of 3.3.1 Case 1. Therefore, FTA for the case that Closed Isolation Microswitch is closed status and Emergency and Locked Microswitch is closed status is shown as Figure 11.

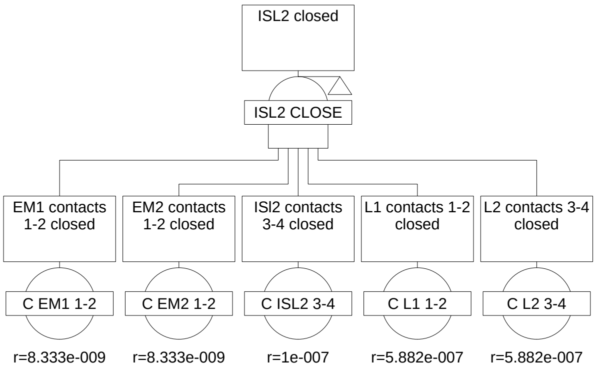


Figure 11: ISL2 closed failure

3.3.4 Case 4 The 2 Emergency Microswitch are failed under the condition that Closed/Locked Isolation Microswitch is normal, and Closed/Locked Isolation Microswitch is failed under the condition that Closed/Locked Isolation Microswitch is normal.

That is to say, if Closed/Locked Isolation Microswitch is normal status, it is detected as train door opened status even though 2 Emergency Microswitch are failure, and it will be detected as unsafe condition from train line level and it will prohibit train is moving. However, if 2 Emergency Microswitch are normal status, it is detected as train door opened even though Closed/Locked Isolation Microswitch is failure. Thus, failure of safe detection of the status door Closed/Locked is Closed/Locked Isolation Microswitch ISL 1-ISL 2 failure and simultaneously, 2 emergency Microswitch EM1-EM2 is failure. Eventually, it cannot detect train door opening and cause a serious hazard to passenger.

Basic failure of Closed/Locked Isolation Microswitch is same as that of 3.3.3 Case 3 and that of Emergency Microswitch is same 3.3.1 Case 1. Therefore, FTA for the case that Closed/locked Isolation Microswitch is closed status, and simultaneously Emergency Microswitch is closed status is shown as Figure 12.

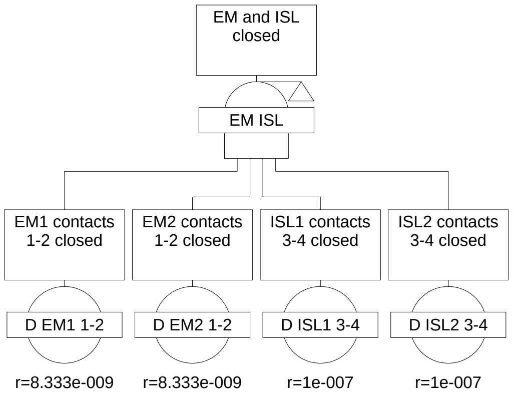


Figure 12: EM and ISL closed failure

3.3.5 Assessment on Safe Detection Function Failure of Door Closed/Locked status Through analysis from Chapter 3.3.1 to 3.3.4, Figure 13 shows the FTA on safe detection function failure of door Closed/Locked status.

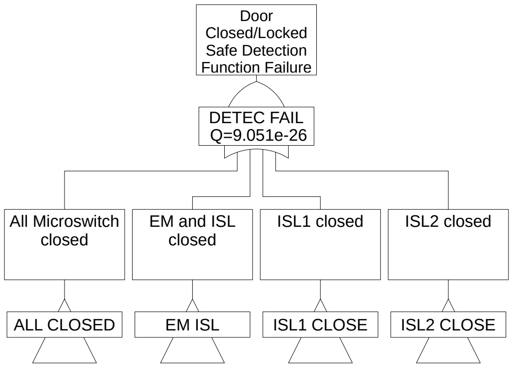


Figure 13: Safe detection function failure of door losed/Locked status

A system lifetime t of 19 hours per train is considered, and safe detection function of door Closed/Locked status is high demand mode from Table 1 the same as door Closed/Locked function. Thus the result of calculation is follows; $Q(19) = 9.051 \times 10^{-26}$ failures/h and $\lambda 19 = 1.905 \times 10^{-26}$ failures/h.

Meanwhile, according to Chapter 3.1, as the 1 train set has 8 sets of train doors, safe detection function of door Closed/Locked status has failure rate of 1.552×10^{-25} failures/h. Thus, the value is over SIL 4 according to Table 1.

4 Conclusion The assessment has been carried out for $Q(t)$, $\lambda(t)$, FBD, the Risk Analysis of Hazard Log and failure rates of FMECA in order to evalute safety functions that are the Door Closed/Locked function failure and the safe detection function failure of door Closed/Locked status. Finally we conclude that the tolerable hazard rate of the train door system is acceptable and the system is safe to passengers judging by the quantitative evaluation results which are required by IEC 61508 on the safety functions.

To get better safety assurance, an assessment on systematic failures such as failures regarding EMC or Software on the door system will be carried out later.

References

[1] Barlow and Proschan, "*Statical Theory of Reliability and Life Testing*", Holt, Rinehart and Winston, New York (1975)

[2] IEC 61508, "*Functional safety of electrical/electronic/ programmable electronic safety-related systems*" (1997)

[3] EN 50126, "*Railway Applications The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*" (1999)

[4] EN 50129, "*Railway Applications - Safety related electronic systems for signalling*" (2003)

[5] V. Hung, "*Hazard Log for BGL*, Thales, Rev.1 (2009)

[6] F.Davoli and M.Avidano, "*Technical Description of Passenger Side Door for BGL*, Vapor Europe srl, Rev.7, pp. 1–30 (2007)

[7] F.Davoli and M.Avidano, "*SIL Analysis for Passengers Doors System*", Vapor Europe srl, Rev.02, pp.1–41 (2009)

[8] F.Davoli and M.Avidano, "*FMECA for Passengers Doors System of RAM Analysis*", Vapor Europe srl, Rev.03, pp.1–36 (2009)

[9] W. S. Lee, J. W. Heo and J. H. Shin, "*BGLRT Door System Failure Review Report*", ADS Rail of Korea, Rev.00, pp. 1–20 (2011)

Communicated by *Hiroaki Ishii*

Tae Keun Park
Quality Management, Hyundai Rotem Company
85, Daewon-Dong, Uichang-gu, Changwon-city, Kyungsangnam-do, Korea
email: `tkpark@hyundai-rotem.co.kr`

Keun Woo Park
Department of Railway System, Hyundai Rotem Company
Hyundai Motor Group Bldg 9F, 231, Yangjae-Dong, Seocho-Gu, Seoul, 137-938, Korea
email: `keunwoop@hyundai-rotem.co.kr`

Koyu Uematsu
Department of Economics and Finance, Osaka International University
3-50-1, Sugi, Hirakata Osaka 573-0192, Japan
email: `uematsu@oiu.jp`