International Journal of Mathematical, Engineering and Management Sciences
Vol. 2, No. 1, 30–36, 2017
https://dx.doi.org/10.33889/IJMEMS.2017.2.1-003

Sneak Circuit Analysis: Lessons Learned from Near Miss Event

James Li

Centre of Competence for Mass Transit
AME, Bombardier Transportation, Kingston, Canada
Email: james.li@rail.bombardier.com

(Received September 6, 2016; Accepted October 24, 2016)

Abstract
Sneak Circuit Analysis is intended for critical applications which are essential to mission success and safety. A sneak condition will occur when a designed circuit inhibits a wanted function or results in an unwanted function. Sneak conditions originate from one of the four following scenarios: a sneak path resulting in a flow of electrical current along an unexpected route; a sneak timing that may cause the activation of some desired/designed functionality at an unexpected time; a sneak indication in monitoring functions that may result in an ambiguous or false display of system operating conditions; and lastly, a sneak label which may induce operator error due to inappropriate instruction. This paper introduces a near miss event that occurred in the Sao Paulo monorail which was caused by a sneak time condition. Root cause analysis and design modifications are also discussed in the paper.

Keywords - Sneak circuit analysis (SCA), Sneak timing, Door enable, Door inhibit, Propulsion enable

1. Introduction

On April 13th 2016 a near miss event occurred with the Bombardier Sao Paulo monorail. A train departed a station with its doors open during testing. The recorded video showed only operational staff on the train without passengers onboard when the train started moving with its doors open. One of operational staff noticed this undesirable situation, intervened and stopped the train with the emergency stop button on the driver control panel. No injuries were reported in the event.

During the investigation, it is noted that the Automatic Train Control (ATC) system sent an errant door open command in an arbitrary manner which caused doors to open. Although this is considered as one of the identified root causes which commanded the doors to open at an unexpected time it is not the main reason; because in the Bombardier developed driverless monorail, the door open command is considered as a non-vital function because it is transmitted through the CANBus network.

The vital function for safe door opening is built in the door enable function. The door enable function consists of the door enable command and the door safety circuit. The door enable command is generated by the Automatic Train Protection (ATP) system or Manual Train Control (MTC) system in a vital manner. This ensures that door opening is enabled when all the safe conditions are satisfied: train is stopped at the right location; aligned with platform screen doors; zero speed detected; parking brake applied and propulsion disabled.

In the door safety circuit, there is a safety relay to ensure safe door opening. The safety relay coil is energized when the door enable command and zero speed signal are presented which then closes the relay contact to feed the electrical power to the inverter which drives the door motor to open or close doors. Refer to Fig. 1.

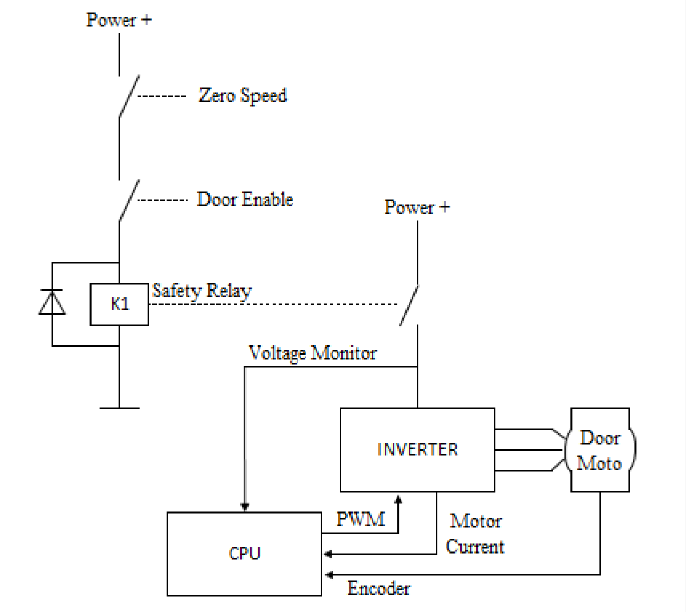

Fig 1. Door safety circuit

For ensuring safe train starting conditions, provisions have been made to inhibit a train moving unexpectedly with one or more train doors open. The safeguard is door closed and locked status supervision which is achieved by redundant door closed and locked status trainlines. When all the train doors are closed and locked, the door closed and locked status trainlines will make redundant closed loops and indicate to the ATP that all the train doors are closed and locked. If there is a discrepancy between the redundant train doors closed and locked status trainlines, ATP will treat it as an invalid state and announce an alarm.

After ATP assures all the train doors are closed and locked, it will disable the door enable command which will de-energize the safety relay coil; open the door safety relay contact; and cut off the power to the door drive inverter such that the train doors cannot be opened. ATP will then activate the propulsion enable to drive the train to move. In this situation, even if the door control unit receives the door open command it will not open the door because the safety relay contact has been opened to isolate the door drive circuit from electrical power. However, the recently occurred near miss event does not seem to respect this designed safety control logic. It reminds us that something is wrong in the Automatic Train Protection (ATP) design.

Sneak circuit analysis (SCA) was conducted to identify the root causes that lead to the occurrence of this undesirable event. SCA is an analytical procedure for identifying latent paths that cause occurrence of unwanted functions or inhibit desired functions, assuming all components are operating properly. Sneak conditions originate from one of the four following scenarios: a sneak path resulting in a flow of electrical current along an unexpected route; a sneak timing that may cause the activation of some desired/designed functionality at an unexpected time; a sneak indication in monitoring functions that may result in an ambiguous or false display of system operating conditions; and lastly, a sneak label which may induce operator error due to inappropriate instruction.

SCA was firstly developed in the late 1960’s for NASA to verify the integrity and functionality of their designs. In reference Military Standard MIL-STD-785B (1980), SCA definition was introduced. In reference Military Standard MIL-STD-338B (2005), the concept and methodology of sneak circuits were introduced. In reference System Reliability Toolkit (2005), sneak analysis including sneak circuit analysis and sneak software analysis were introduced. In reference RADC-TR-89-223, RADC-TR-90-109 and RL-TR-95-232, SCA methodology, tool and examples were presented. In reference RADC-TR-82-179, SCA applications were introduced. In reference Sneak Circuit Analysis Guideline for Electro-Mechanical Systems (1995), SCA implementation method was introduced. In reference Rankin (1997), application of SCA to prevent hazards was presented in reference Scappaticci et al. (2016), lessons learned from SCA application was discussed.

2. Sneak Circuit Analysis to Find the Root Cause

In the course of root cause investigation, we found something very interesting when we analyzed the logged timing diagram. We observed that the ATC sent an arbitrary door open command just after removing the door enable command. The time between when the door enable is de-energized to the time the propulsion is enabled is 0.125 seconds. The safety relay in the door control units takes almost 0.14 seconds to open up to remove the power from the door drive inverter. It is the sneak time interval of 0.14 – 0.125 = 0.015 seconds that will result in an unexpected and undesirable situation: propulsion enable is activated before the door control units have time to open the doors and break the train door closed and locked status. An unintentional door open command is received in this very short sneak interval as the doors still have all the door opening pre-conditions (zero speed detected, parking brake applied, door enable high and propulsion disabled) needed to act on the door open command. We noticed that within 0.125 seconds of the open command being received, at least 1 of the 14 doors has managed to break the train door closed and locked loops, which consequently resulted in an undesirable event: train departed the station with door(s) open. Refer to Fig. 2.

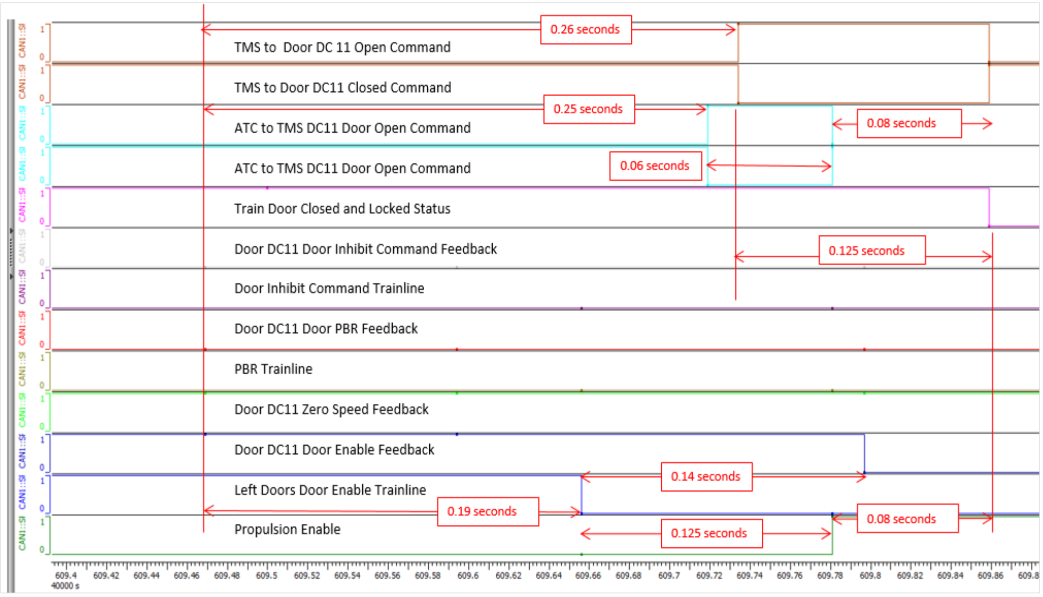

Fig. 2. Timing diagram

The root cause of this near miss event is that the door enable function and propulsion enable function are not isolated completely with an overlap among them in the time sequence. The propulsion enable function is activated prior to the door control units recognizing that all the doors had been completely disabled.

Further analysis was conducted to discover why the safety relay took 0.14 seconds to open up. Firstly, the Sao Paulo monorail has a length of 90 m and the ATP is installed in the front and end car. The signal transmission from the front car to the end car causes the time delay; secondly, after the door enable is removed by ATP, the safety relay will take time to open up. This can be analyzed by using the first-order transient response of RL circuit. Refer to Fig. 3.

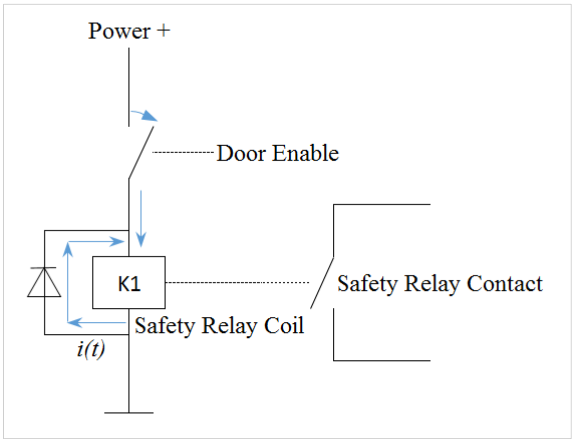

Fig. 3. Transient response of RL circuit

At the instantaneous moment that the safety relay circuit opens up by removing the door enable command, according to Kirchhoff's circuit law in K1 and Diode closed circuit:

$$L\frac{di}{dt}+Ri=0 \tag{1}$$

Taking Laplace transform to equation (1):

$$L\left(I(s)-I(0)\right)+RI(s)=0 \tag{2}$$

Rearranging equation (2):

$$I(s)=\frac{I(0)}{s+\frac{R}{L}} \tag{3}$$

Taking inverse Laplace transform to equation (3) to obtain:

$$i(t)=I(0)e^{-\frac{R}{L}t} \tag{4}$$

Where: I (0) is the initial current at the moment when the door enable is removed; R is the resistance of the coil and line cable; L is the inductor of the coil.

The current in the safety relay coil will be reduced exponentially and the current transient reduction curve is shown as Fig. 4.

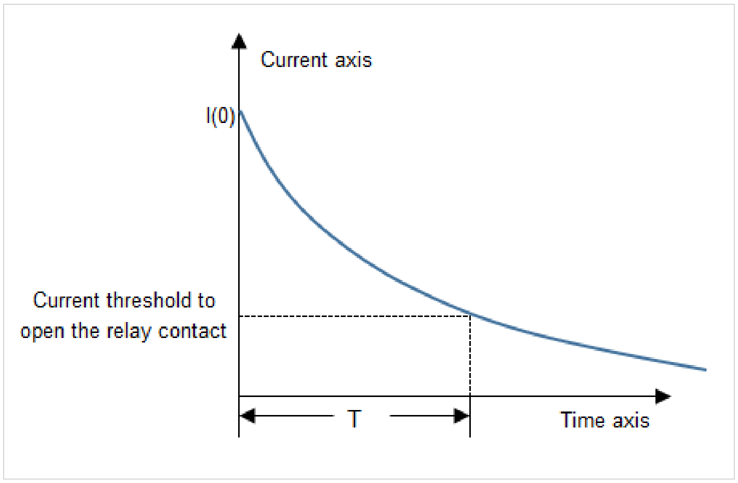

Fig. 4. Current reduction curve

T is the time delay from when the time door enable is removed to the time the safety relay opens up.

Another sneak time condition that attracted our attention was that the door inhibit function is activated very late in this near miss event. The time for doors to fully open takes 2.5 to 3.0 seconds. In this near miss event the door inhibit is activated 2.42 seconds after initiating train movement. That is why in the recorded video the train was moving with a widely opened door. Door inhibit is the vital function to inhibit door movement by applying the door motor brake. Door inhibit function is the safeguard to prevent passengers from opening the door by operating the emergency release handle when the train is in motion. Provided that the door inhibit were activated on time at the moment when the train initiated movement, the near miss event would also have been prevented.

3. Eliminate Sneak Time by Delay

It is obvious that if we increase the time interval between the time the door enable is set low and propulsion enable is set high to isolate these two functions completely without any overlap, it will eliminate the sneak time and prevent the same event from happening. The question is how long must the time interval be for it to be safe. It is absolutely clear that this time interval should be greater than 0.14 seconds. And also this time interval should be the worst case time delay which covers all the scenarios. Our door engineer also informed us that if the door closed and locked status is broken, the door safety relay will be energized again and allow the doors to open and close at any open command. This design provision is aimed to protect the passenger trapped between the doors by opening doors again. It is also called “obstacle detection”. During obstacle detection, the door can respond to any valid open requests to release the trapped objects. This reminds us that we should also consider the time for the door to break the door closed and locked status at an open command. Therefore the implementaion of time delay between the time the door enable is commanded low and propulsion enable is commanded high provides sufficiemt time to ensure all doors have removed power from the motors before initiating train movement. This delay also provides sufficient time to ensure any door that in the process of opening due to a errant open command has time to break the door closed and locked status before propulsion enable is commanded high, thereby halting the train departure.

Therefore, the time delay should be the sum of the time it takes for the relay in the door control units to respond to the door enable going low plus the time it takes the door to break the closed and locked status when commanded open. For safety reasons, the safety factor shall be added or multiplied to cover any erratic uncertainty.

The first time was determined by reviewing the Sao Paulo field data collected over the past two years. Times vary as expected, from 156 ms to 218 ms. The longest time shall be used as a safe and conservative approach.

The second time is the time it takes for a door to break the closed and locked status in response to a door open command. A conservative time was chosen as 317 ms.

Taking the sum of the first and second times (218 ms + 317 ms) we obtain a total of 535 ms. To account for the uncertainty mentioned above, a safety factor of 1.4 is multiplied which produces a time delay value of 750 ms.

4. Additional Mitigations

Notwithstanding the time delay implementaion still cannot cover all the undesirable scenarios, i.e. door safety relay contact fails welded. Provided that the door safety relay contact fails welded. The door motor is always energized and the door can be opened at any open command regardless of train movement. In the current design, the safety relay is monitored by the door control unit to ensure its state is correct. If the safety relay does not open when required, a fault is raised and the train will stop at the next station. The door will be isolated by an attendant or the train will be taken out of service.

The other additioanl mitigation is to activate the door inhibit at the instant when the zero speed is disappeared. This can inhibit the door operation and effectively lock the doors in their current position if the train has initiated movement. With this mitigation, the doors would not have opened fully, but would have opened 300 mm or so. It depends upon how fast the ATP can activate the door inhibit function.

5. Conclusion

Sneak circuits are designed-in and built-in and they do not result from component faults or failures. Sneak timing is an important aspect of sneal circuit. In this study the existence of sneak time in the electrical control circuit causes an unexpected function due to the time interval between the two control signals is not extensive enough to completely isolate the two control signals in time sequence, which results in the sequential function being activated prior to the preceding function completion.

From this sneak circuit analysis, it is interesting to note that a sneak time of 0.015 seconds could make a significant difference by enabling an unexpected function which leads to an unsafe situation. The lesson learned from this near miss event also warns our engineers that negligence of even milliseconds in the design could result in undesirable consequences which endangers the public. Prudence is always paramount being as engineers.

References

MIL-HDBK-338B, *Electronic Reliability Handbook, Notice 2* (pp. 468-480). Air Force Research Laboratory Information Publishing, 2005.

MIL-HDBK-785B, *Reliability Program for System and Equipment Development and Production* (p. 37). Department of Defense Publishing, 1980.

RADC-TR-82-179, *"Sneak Circuit Analysis Application Guidelines"*, Rome Air Development Center (RADC) Technical Report, June 1982.

RADC-TR-89-223, *"Sneak Circuit Analysis for the Common Man"*, Rome Laboratory, 1989.

RADC-TR-90-109, *"Integration of Sneak Circuit Analysis with Design",* Rome Laboratory, 1990.

Rankin, J. P., Origins, Application and extension of sneak circuit analysis on space projects *Hazard Prevent.* 33(2), 2nd Q, 24-30 (1997).

Scappaticci, A., Benson, R., Foley, D., & Kellner, D. (2016, January). Sneak circuit analysis: Lessons learned for beginners based on a successful application. In *2016 Annual Reliability and Maintainability Symposium (RAMS)* (pp. 1-6). IEEE.

SCAT: *Sneak Circuit Analysis Tool, Version 3.0*, RL-TR-95-232.

Sneak Circuit Analysis Guideline for Electro-Mechanical Systems, NASA Practice No. PD-AP-1314, Oct, 1995.

System Reliability Toolkit (p. 577). Reliability Information Analysis Center (RIAC) and Data Analysis Center for Software (DACS) Publishing, 2005.