International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 1, 136-146, 2020
https://doi.org/10.33889/IJMEMS.2020.5.1.012

A Glance at Transit System Safety

James Li
Transport Systems,
Parsons Inc., Kingston, Canada.
E-mail: james.li@parsons.com

(Received July 8, 2019; Accepted October 25, 2019)

Abstract
System safety is a discipline of applying engineering and management principles, criteria, and techniques to achieve acceptable or tolerable risk within the constraints of operational effectiveness, suitability, time, and cost throughout all phases of the system life. System safety engineering is the program to identify hazards, and to eliminate hazards or reduce the associated risks when the hazards cannot be eliminated. System safety management involves plans and activities taken to identify hazards; assess and mitigate associated risks; track, control, close, and document risks encountered in the design, development, test, manufacturing, installation, operation and maintenance, and the disposal of systems, subsystems, and equipment. In this paper, the concept and principle of system safety in the transit system is discussed. The paper also introduces the safety standards, safety life-cycle, Safety Integrity Levels (SILs), safety analysis techniques and safety cases etc.

Keywords – System safety, Transit system, Safety life-cycle, Safety plan, Safety standard, SIL, Safety case.

1. System Safety in Transit Systems

The scope of the transit system in this paper includes Automated People Mover (APM), light/heavy Metro, Trams, and Light Rail Transit (LRT), excluding city buses. In general, a typical transit system is a complex public transportation system that consists of guideways, stations, Automatic Train Control (ATC), Power Supply and Distribution, Platform Screen Door, Communications and Vehicles etc.

The primary objective of a Transit System in terms of safety is to develop a rail transit system free of hazards. However, absolute safety is not attainable particularly when a complex transit system is being developed. Therefore, the realistic goal becomes that of developing a transit system with acceptable or tolerable mishap risk. This is accomplished by seamlessly integrating safety into the overall transit system life-cycle which encompasses the concept, design, manufacturing, installation, testing and commissioning, operation and maintenance, and eventually disposal of the system, subsystem, and components.

System safety is defined in *MIL-STD-882E* as the application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness, suitability, time, and cost throughout all phases of the system life. There are two important aspects highlighted in this definition: operational effectiveness and cost. How effective is the mitigation going to eliminate the hazard, and how much is it going to cost? This means that during the system safety process when we are developing hazard controls, we are performing a cost - benefit analysis. It is not worthwhile to increase spending costs only to result in a minimal effect in eliminating the hazards or those with low risk. The limited resources should be focused on the critical and catastrophic hazards with undesirable and intolerable risks. From an industry historical viewpoint, it has been known that a proactive preventative approach to safety during system design

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 1, 136-146, 2020
https://doi.org/10.33889/IJMEMS.2020.5.1.012

and development is more cost effective than attempting to enhance system safety after the occurrence of an accident or mishap. Therefore, system safety from an initial economic investment point-of-view could save future losses resulting from potential mishaps.

2. Safety Standards

Prior to the 1940s, safety was generally accomplished by attempting to eliminate obvious hazards in the early design and then correcting any further problems as they appeared after a product was in use or in a testing phase. In other words, engineers relied on a trial and error methodology. In the aviation field, this is known as the "fly-fix-fly" approach. This approach was not acceptable for certain programs such as nuclear weapons and space program where safety in the initial launch is a strict requirement. (Braman, 2018).

The 1960s brought us *MIL-STD-882: System Safety Program Requirements*, which was based on an US Air Force document (*MIL-S-381308A, General Requirements for Safety Engineering of Systems and Associated Subsystems and Equipment*). Over the next 50 years this standard evolved into today's *MIL-STD-882E*. *MIL-STD-882* is sometimes called the "mother" of all safety management standards. *MIL-STD-882*, although a military standard, is the prevailing standard in North America for developing the system safety program plans (SSPPs) in the rail and transit industry.

A similar safety standard employed in military industries is *DEF-STD-00-56* which was published by the UK Ministry of Defense. Both *MIL-STD-882* and *DEF-STD-00-56* were originally developed for military industries, and are currently utilized by other industries including rail and transit.

ASCE 21 is also an influential rail and transit standard in North America. *ASCE 21* is the Automated People Mover (APM) standard published by the American Society of Civil Engineers, and was initiated in 1996. This standard establishes the minimum requirements necessary to achieve an acceptable level of safety and performance for an APM system. The safety topics covered in this standard incorporates: system safety program, hazard resolution process, safety principles, ATC system fail-safe design, verification and validation, and ATC system mean time between hazardous events. The system safety program in *ASCE 21* comprises of: system safety program plan, preliminary hazard analysis (PHA), subsystem hazard analysis (SSHA), system hazard analysis (SHA), operating and support hazard analysis (O&SHA). *ASCE 21* is also used in the safety certification process.

In the 1990s, CENELEC standards *EN50126/8/9* had attracted widespread attention. *EN50126* symbolizes the only international RAMS (Reliability, Availability, Maintainability and Safety) standard in the railway application. *EN 50128* provides comprehensive instructions for developing safety related software, as well as the tools and techniques that are required in the software life-cycle for different SIL categories. *EN50129* is a distinguished publication that describes how to formulate and create a well-reasoned safety case for a rail and transit system. In recent years an increasing number of rail and transit projects are referencing and requiring CENELEC compliance in North America.

IEC61508 is the basic safety publication of IEC (International Electrotechnical Commission). *IEC61508* is based on two fundamental concepts: safety life-cycle and Safety Integrity Level (SIL).

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 1, 136-146, 2020
https://doi.org/10.33889/IJMEMS.2020.5.1.012

Both fundamental concepts are also highly promoted in the CENELEC standards *EN50126/8/9* and *Yellow book*.

In reference Braband et al. (2003), the authors introduced the relationship and genealogy among *MIL-STD-882*, *IEC 61508*, CENELEC safety standards *EN 50126/8/9* and other related safety standards.

IEC62267 is the standard of safety requirements for Automated urban guided transport (AUGT) which outlines the safeguards and safety requirements for the hazardous situations that are encountered in the rail and transit systems. *IEC62278* is the IEC version of *EN50126* whereas *IEC62279* is of *EN50129*.

IEEE Std 1474.1 is the standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements. The safe braking distance model for the driverless rail and transit systems is defined in this standard.

Some railway application technical standards e.g. *EN13452* and *EN14752* also encompasses the safety functional requirements for safety related systems such as vehicle brakes and doors.

Some safety standards are specialized for performing detailed technical analysis. *EN60812* and *MIL-STD-1629A* are for Failure Modes, Effects and Criticality Analysis (FMECA); *IEC61882* is for hazard and operability studies (HAZOP studies); *IEC61025* is for Fault Tree Analysis. The US Department of Transportation Research and Special Program Administration has published Hazard Analysis Guidelines for Transit Projects which can be utilized as a good reference to perform the hazard analysis.

Yellow Book published by Railtrack on behalf of the UK rail industry delineates engineering safety management guidelines.

In terms of the safety for fire, material flammability and toxicity in the rail and transit system, *NFPA 130*, "*Standard for Fixed Guideway Transit and Passenger Rail Systems*"; *DIN 5510*, "*Preventive fire protection in railway vehicles*"; *ASTM E119*, "*Standard Test Methods for Fire Test of Building Construction and Materials*"; and *EN 45545*, "*Railway applications – Fire protection on railway vehicles*", lay out systematic technical guidelines in regard to Flammability, Smoke and Toxicity (FST).

In North America, Compliance with ADA (Americans with Disabilities Act) regulations are also required in the rail and transit system.

3. System Safety Program Plan (SSPP)

SSPP shall be drawn up at the start of the system life-cycle and shall be revisited at appropriate intervals. SSPP shall describe in detail a series of tasks and activities required throughout the life cycle of the system that comprises of the safety policy and strategy, scope of plan, planning of the safety activities, safety organization, hazard identification and analysis, risk assessment and acceptance criteria; hazard log management, verification & validation, safety-related deliverables, safety-related interfaces, safety review and audits, safety cases, safety acceptance and approval processes, safety-related procedures and training, constraints and assumptions made in the plan etc.,

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 1, 136-146, 2020
https://doi.org/10.33889/IJMEMS.2020.5.1.012

so as to identify, evaluate, eliminate or control hazards, or reduce the associated risk to a level acceptable to the authority having jurisdiction throughout the system life cycle.

4. Safety Life-Cycle

The safety life-cycle is a term utilized in *EN 50129* for the additional series of tasks and activities carried out in conjunction with the system life-cycle for safety related systems that are employed in the rail and transit systems. The safety management process shall consist of a number of phases and activities, which are linked to form the safety life-cycle; this should be consistent with the system life-cycle defined in *EN 50126*. Refer to Figure 1.

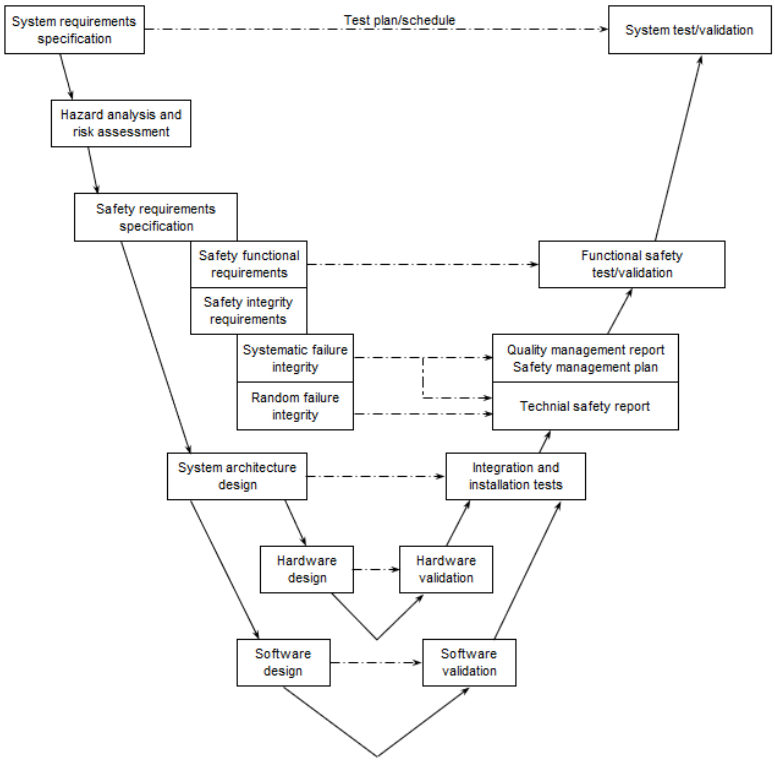

Figure 1. Example of design and validation portion of system life-cycle (EN 50129)

5. Safety Integrity Level (SIL)

The term 'Safety Integrity Level (SIL)' derives from a number of safety standards, principally *IEC 61508* and CENELEC standards *EN50126/8/9*. This SIL concept differs from the term 'Software Integrity Level (SIL)' defined in *IEEE 1012: Standard for Software Verification and Validation*.

Part 4 of *IEC 61508* defines Safety Integrity as the likelihood of a safety related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time; and a Safety Integrity Level (SIL) as a discrete level (one out of four) for specifying the safety integrity requirements of safety functions to be allocated to the safety-related systems.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 1, 136-146, 2020
https://doi.org/10.33889/IJMEMS.2020.5.1.012

Note two key points in terms of SIL:

- SIL relates only to safety functions and safety-related systems.
- Safety Integrity Levels are defined in terms of the reliability of the system in executing the safety functions.

The term 'Safety Integrity Level' or 'SIL' is one of the most misused and misunderstood terms in the rail and transit industry. The reason behind this is although *IEC 61508* initiated the SIL concept, principles and techniques (Part 5 of *IEC 61508*); the SIL interpretation in CENELEC standards *EN 50126/8/9* does not coincide with *IEC 61508* rigorously. The SIL determination methods include the risk graph, layer of protection analysis (LOPA) and hazardous event severity matrix.

It should be noted that a SIL should be principally allocated to a Safety Function (SF), and therefore to the safety-related system, subsystem, or component that is designed to execute that safety function. The SIL for a safety-related system, subsystem or component usually refers to the highest SIL of the safety functions within it. It should be understood that not all the functions within a SIL rated system, subsystem or component needs to meet the highest SIL. E.g. a brake system performs Service Brake (SB) and Emergency Brake (EB) functions. The EB shall be SIL 4 so as to prevent the train collision, whereas the SB can be SIL 0 because the SB is not considered as a safety function.

In recent years there has been an increasing tendency for customers to specify required SILs for subsystems or equipment without any knowledge or linkage to real safety requirements, functions or system architecture simply because of a misguided belief that a high SIL must be considered 'good' and is somehow 'state of the art'. They don't realize that SILs should be considered from a System-Level safety function, and top down allocated to the downstream subsystems and components that perform the specified safety functions. For example, a Train-Level SIL 4 EB function requires all the downstream subsystems, units, components and interfaces in the EB loop to achieve the same SIL level requirements, which includes the EB executing mechanisms in the brake system, EB command generated from the Automatic Train Protection (ATP) or Manual Train Control (MTC), EB control trainlines and Propulsion Enable Interlock in the propulsion system etc. Given that one element in the EB loop fails to meet SIL 4 requirements, the Train-Level EB would be compromised by the elements with the lowest SIL, e.g. EB command is transmitted through SIL 0 CANBus network.

6. Safety Organization

The safety management process shall be executed under the control of an appropriate safety organization. The safety organization herein shows the structure of the organization and independence relationship among the project management, designer, validator, verifier and assessor when developing a safety-related system, subsystem or product. An appropriate degree of independence shall be provided between different roles based on the stringency of SIL requirements, as shown in Figure 2.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 1, 136-146, 2020
https://doi.org/10.33889/IJMEMS.2020.5.1.012

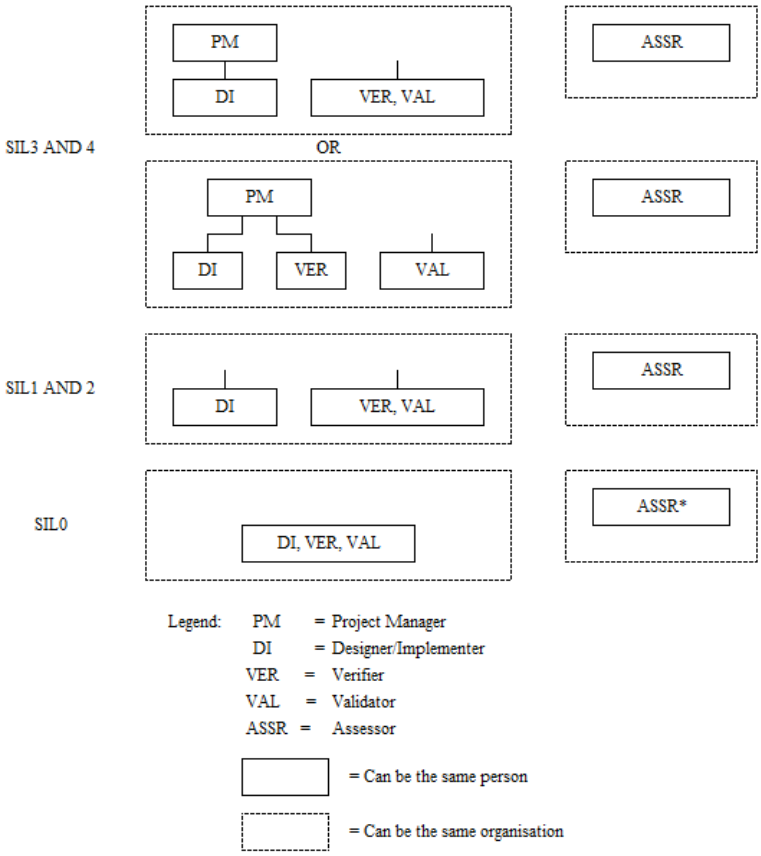

Figure 2. Arrangements for independence (EN 50129)

7. Safety Requirement

Literally, safety requirements are the requirements which are associated with safety. To perform this, a detailed Function Requirements Specification / Description is required as a basis to derive two parts of safety requirements: safety functional requirements and safety integrity requirements. Safety functional requirements should be singular, non-ambiguous, measurable and attainable. It describes what, not how. Safety integrity requirements specify the level of SIL for the safety functions that are required by the safety-related systems. Refer to Figure 3.

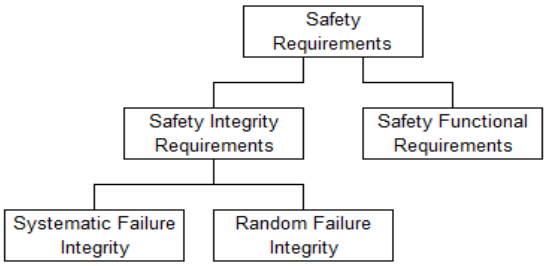

Figure 3. Safety requirements and safety integrity (EN 50129)

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 1, 136-146, 2020
https://doi.org/10.33889/IJMEMS.2020.5.1.012

8. Hazard Log and Hazard Analysis

A Hazard Log shall be developed and maintained throughout the system safety life-cycle. Hazard Log is a Hazard Management Process to identify a hazard, assess the associated risk, and eliminate or mitigate the hazard to an acceptable category. The Hazard Log shall be considered as a living document and subject to be updated if any modification or alteration is made to the system, sub-system or equipment.

Top Level hazard identification and analysis consists of a preliminary identification of hazards, and then assessment of the "Severity", "Frequency" and then the "Risk" for each identified hazard. The identification of high-level hazards should commence with IEC 62267, considering the project specific application, so as to ensure that each of the following accidents is considered so that appropriate Safety Requirements, and thus SFs will be established / provided:

- Train collision (train - train, train - object, train - person);
- Derailment ;
- Person falling from train in service;
- Human injury on train in service (caused by train in motion);
- Fire in train in service (depot, underground, above-ground);
- Fire (tunnel, station, depot, Operations Control Center);
- Explosion;
- Non-movement accident;
- Electrocution;
- Structural failure/collapse;
- Adverse weather or acts of god, and
- Evacuation.

The commonly employed hazard analysis techniques include preliminary hazard list (PHL), preliminary hazard analysis (PHA), subsystem hazard analysis (SSHA), system hazard analysis (SHA), interface hazard analysis (IHA), operating and support hazard analysis (O&SHA), safety requirement/integrity analysis (SRIA) and HAZOP etc.

The risk acceptance principles include As Low As Reasonably Practicable (ALARP), Globalement Au Moins Aussi Bon (GAMAB), Minimum Endogenous Mortality (MEM) or Common Safety Methods (CSM).

9. FMEA and Safety Critical Items

During the 1950s, FMEA was initially developed as an engineering methodology at Grumman Aircraft Corporation to analyze the safety of flight control systems for naval aircraft. In reference Bowles (2003), the fundamentals and principles of FMEA are introduced.

A FMECA is a tool that employs a systematic method of identifying and quantitatively or qualitatively evaluating potential failure modes and their associated causes / mechanisms within a system, subsystem or equipment. The Design FMECA (D-FMECA) functions as a design tool to help identify single point failures that may have significant impact on operational performance or safety.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 1, 136-146, 2020
https://doi.org/10.33889/IJMEMS.2020.5.1.012

Safety Critical Items (SCI) can also be identified through FMECA. The SCIs shall be monitored either by sensors for the detectable SCIs, or a periodic routine maintenance at scheduled intervals to inspect the deterioration state of undetectable SCIs that may potentially contribute to a hazardous accident before it has progressed to the point of causing a hazard.

10. Fault Tree Analysis

Fault Tree Analysis (FTA) was pioneered by H. Watson and A. Mearns at Bell Labs for evaluating the launch control system of the Minuteman intercontinental ballistic missile, then recognized by Dave Haasl of Boeing as a system safety analysis tool. In reference Andrews (2012), the author introduced the FTA from a qualitative and quantitative perspective respectively.

The FTA is a top-down approach which allows the analyst to identify the cause or combination of causes leading to an event. FTA graphically depicts the relationships between the different causes of a System Level Hazard. FTA conducts an evaluation of the undesired hazard, working backwards from the top event to its causes, and eventually leads to a multiple failure safety analysis. The analysis shall consider both hardware failures and non-hardware failures such as human errors and software interaction failure. The undesired events (top events of fault trees) will be identified early during design phases and as design progresses through the identification process which starts with the Preliminary Hazard Analysis.

FTAs will be performed for hazards of severity category ‘Catastrophic’ and ‘Critical’ identified and documented in the Hazard Log as well as those specified from the customer specification.

The FTA will be presented in the form of a logic flow diagram for analyzing hazards which result from component failures, human errors, or other conditions. The tree is pruned when risk and severity are insignificant, when independence of events is demonstrated, when further drill down does not provide more relevant information, or when the probability of occurrence of the top level meets the requirement.

11. Sneak Circuit Analysis

Sneak circuit analysis (SCA) is an analysis technique for identifying a special type of hazards known as sneak circuits. SCA is accomplished by examining electrical circuits (or command/control functions) and searching out unintended electrical paths (or control sequences) that, without component failure, can result in undesired operations, desired operations but inappropriate times and inhibited desired operations. In reference Li (2018), SCA methodology and techniques are introduced.

A sneak circuit is an inherent design flaw in an electrical system that inhibits a desired function or initiates an unintended or unwanted function. The objective of the SCA is to identify all sneak conditions that may lead to an unintended hazardous event resulting in catastrophic accidents such as loss of life, major system failure, or loss of mission. There are four types of sneak conditions including sneak paths, sneak timing, sneak indications and sneak labels.

12. Common Cause Failure Analysis

A common cause failure is the failure of more than one component due to a single cause. This single-point failure affecting multiple components can be due to a variety of issues, such as environmental stresses (temperature, humidity), improper maintenance and testing, manufacturing

defects, incorrect installation or calibration, use of identical components in multiple subsystems, common software design, or other similar causes.

Diversity is specifically provided as a defense against common cause failure. It can be achieved by providing systems that are physically different from each other or by functional diversity, where similar systems achieve the specified objective in different ways.

13. Safety Case

A safety case is the documented demonstration that the system complies with the specified safety requirements. Therefore, a safety case shall communicate a clear, comprehensive and defensive argument that a system is acceptably safe to operate in a specified environment. In reference Kelly (2004), a Goal Structuring Notation (GSN) approach is introduced for developing and presenting clear and structured safety arguments in the safety case. The service technique des remontées mécaniques et des transports guidés (STRMTG) in France also defines an alternate proposal for Safety Case structure.

EN50129 defines that the safety case shall typically have the following structure:
Part 1. Definition of the System (or sub-system / equipment)
Part 2. Quality Management Report
Part 3. Safety Management Report
Part 4. Technical Safety Report
Part 5. Related Safety Cases
Part 6. Conclusion

The definition of the System (or sub-system / equipment) shall precisely define the System (or sub-system / equipment) to which the Safety Case refers. The Quality Management Report shall show adequate evidence of an effective quality management process. The Safety Management Report shall show adequate evidence of a Safety Management Process. The Technical Safety Report shall show adequate evidence of functional and technical safety. The related Safety Cases shall provide any and all generic or product Safety Cases that are referenced to support the main Safety Case, and shall also demonstrate that all the safety-related application conditions specified in each related Safety Case is either fulfilled in the main Safety Case or carried forward into the safety related application conditions of the main Safety Case. The conclusion shall summarize the evidence presented in the previous parts of the Safety Case, and argue that the System (or sub-system / equipment) is adequately safe, subject to compliance with the specified application conditions.

14. Safety Acceptance and Approval

For safety acceptance and approval, the Safety Assessor shall assess the adequacy of the evidence of safety. The evidence of safety shall be in three categories: 1. Evidence of quality management, 2. Evidence of safety management, and 3. Evidence of functional and technical safety. The documents showing that evidence shall be:

- The System Requirements Specification,
- The Safety Requirements Specification,
- The Safety Case, and
- The Safety Assessment Report.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 1, 136-146, 2020
https://doi.org/10.33889/IJMEMS.2020.5.1.012

The Safety Assessor shall be responsible for the Safety Assessment Report. The report will explain how the Safety Assessor determined that the System was designed to meet its specified requirements, down to through the subsystems and equipment to the components, including software, and possibly specify some additional conditions for the operation of the system.

15. Conclusion

This paper provides a brief view to the system safety approach applied in the rail and transit industry. The paper mainly covers the safety standards, safety plan, safety life-cycle, Safety Integrity Level (SIL), safety organization, safety requirement, hazard log and hazard analysis, FMECA, FTA, Sneak Circuit Analysis, Common Cause Failure Analysis, Safety Case, Safety Acceptance and Approval Process. System Safety is an engineering discipline for developing safe systems and products, where safety is intentionally integrated into the system or product. It involves the planned application of engineering and management principles, criteria and techniques for the purpose of developing a safe system that achieves acceptable risk. The system safety processes executed throughout the life cycle of a project will prevent accidents, saving lives and money associated with the insured and uninsured costs of an accident.

Conflict of Interest
The author confirms that this article contents have no conflict of interest.

Acknowledgement
The author would like to thank reviewers for their constructive comments and valuable suggestions.

References

Andrews, J. (2012, January). Introduction to fault tree analysis. In *2012 Annual Reliability and Maintainability Symposium. USA (pp. 1-3).*

Bowles, J.B. (2003). Fundamentals of failure modes and effects analysis. In *Tutorial notes annual reliability and maintainability symposium*.

Braband, J., Hirao, Y., & Luedecke, J. (2003). The relationship between the CENELEC railway signaling standards and other safety standards. *Signal und Draht, 95*(12), *32-38.*

Braman, G.D. (2018). Introduction to system safety. In *2018 Annual Reliability and Maintainability Symposium, USA (pp.1-9).*

BSI Standards Publication (2006). *Analysis techniques for system reliability - procedure for failure mode and effects analysis* (*FMEA*) (BS EN 60812:2006).

BSI Standards Publication (2011, July 31). *Railway applications - communication, signalling and processing systems - Software for railway control and protection systems* (BS EN 50128:2011).

BSI Standards Publication (2017). *Railway applications – the specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 1: General RAMS process* (BS EN 50126-1: 2017).

BSI Standards Publication (2018, November 30). *Railway applications – communication, signalling and processing systems – safety related electronic systems for signalling* (BS EN 50129:2018).

Department of Defense (1980). *Procedures for performing a failure mode, effects and criticality analysis* (MIL-STD-1629A). Washington, DC.

Department of Defense (2012, May 11). *Department of Defense Standard Practice - System Safety* (MIL-STD-882E).

International Electrotechnical Commission (2006). *Fault Tree Analysis (FTA)* (IEC 61025).

International Electrotechnical Commission (2009). *Railway applications – automated urban guided transport (AUGT) – Safety requirements* (IEC 62267).

International Electrotechnical Commission (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels* (IEC 61508-5).

International Electrotechnical Commission (2016). *Hazard and operability studies (HAZOP studies) – Application guide* (IEC 61882).

Kelly, T. (2004). *A systematic approach to safety case management* (No. 2004-01-1779). SAE Technical Paper.

Li, J. (2018). Sneak circuit analysis: lessons learned from near miss event. *International Journal of Mathematical, Engineering and Management Sciences, 2*(1), 30-36.

National Fire Protection Association (2007). *Standard for fixed guideway transit and passenger rail systems* (NFPA 130).