INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 3)
Available online at: www.ijariit.com

Safety analysis for Building Automation and Control System in Metro Railway Station

Shaik Shashavali
shaikshasha12045@gmail.com
Jawaharlal Nehru Technological University, Anantapur, Andhra Pradesh

Anil Kumar Ammina
anilkr.ammina@beanalytic.com
BE Analytic solutions LLP, Bengaluru, Karnataka

V. Sankar
vsankar.eee@jntua.ac.in
Jawaharlal Nehru Technological University, Anantapur, Andhra Pradesh

ABSTRACT

Every Metro Station Master room is fitted with the local workstation which supervises and controls the station's Mechanical, Electrical and Plumbing (MEP) systems are controlled by Building Automation and Control System (BACS). BACS is a system that controls and monitors Electromechanical Systems like Heating Ventilation and Air Conditioning (HVAC), lifts, escalators, fire fighting, lighting, etc. BACS will work either in remote control mode through Supervisory Control and Data Acquisition (SCADA) controls or in stand-alone mode from the station master room. BACS is accountable for the functions influencing public safety, security and health. Thus BACS, should work reliably, safely, securely and competently. The level of quality and safety management required to avoid random and systematic failures in the design and engineering of the BACS is determined by the Safety Integrity Level (SIL). In this paper, the SIL is determined with the help of the Fault Tree Analysis (FTA) for the Safety Analysis of BACS in Metro Railway Station based on IEC 61508 and CENELEC EN 50129 standards.

Keywords— *BACS, MEP, FTA, SIL, SCADA, Functional Safety, IEC 61508, CENELEC EN 50129.*

1. INTRODUCTION

In metropolitan areas and cities, for the fast transit of a large number of people, metro trains play a major role. BACS is a Computer-driven control system equipped in a metro railway station that monitors and controls stations MEP systems like lighting, ventilation, security systems and plumbing systems [10]. BACS in the metro railway station requires inputs from the systems like HVAC, Elevators, UPS (Uninterrupted Power Supply) and Fire Detection and Alarm System etc. For the control and monitoring of all the systems included in the metro railway station, BACS uses a Programmable Logic Controller along with SCADA suite. The energy performance of the Metro Railway Station is provided by BACS with the Automatic Fault Detection System and diagnosis strategies [8]. BACS is implemented mostly in projects which consist of a huge amount of MEP systems. The controllers in the BACS consist of Programmable controllers for the monitoring and control of temperature, pressure, level, flow, etc, and the manual controls such as dimmers and switches. BACS in metro railway station aims at improving control, monitoring and administration of station's MEP systems.

2. COMPONENTS OF THE BACS

BACS is a computerized, intelligent system of hardware and software designed to control and monitors the MEP systems in a metro railway station. The components of the BACS are HVAC, uninterrupted power supply and fire detection and alarm system.

2.1 HVAC

For the indoor air quality and vehicular environmental comfort in a metro railway station, HVAC technology is implemented. Its main aim is to provide high indoor air quality by means of removing the heat, moisture, smoke and gases like Carbon-di-oxide and nitrogen in the metro railway station. It is the process of exchanging or replacing or refilling the air in the metro railway station. Humidity control is provided by the Air Conditioning system in the entire metro railway station. HVAC system used in a metro railway station is shown in figure 1.

Fig. 1: HVAC ventilation exhaust in the metro station

There are two types of configurations used in HVAC systems in the metro railway station. They are open loop configuration and closed loop configuration. When there is a difference between the inside and outside temperature of the metro railway station then the closed loop configuration is used otherwise the open loop configuration is used.

2.2 Uninterrupted power supply

When the main power fails in the metro railway station, UPS provides the power to the load. That power is only for the short duration of time for the running of the electrical systems. It protects the electrical systems of the metro railway station from the power surges. The UPS of the metro railway station consists of:

- Inverter and Converter Assembly
- Converter Input, System Battery breaker
- Battery System
- Microprocessor based controllers.

2.3 Fire detection and alarm system

The system shall be intelligently addressable for the fire detection and alarm system. The Components of Fire Alarm System are: an addressable fire alarm system will comprise of the Microprocessor based main Fire alarm panel, Sub alarm panel, Analogue addressable smoke detectors, heat detectors, combined optical and heat detectors, Addressable manual call points, Alarm hooter cum flasher lights, Batteries and charger, Electrical Wiring, Conduits, Trunking and Accessories. For the fire detection and suppression, the fire control panel is located in the station master room. Each and every fire detectors, alarm devices are connected to the interfaces to other systems via this panel, as shown in figure 2.

Fig. 2: Fire alarm system control panel in station master room

The purpose of BACS is to control and supervise station's MEP systems, acquire and display MEP equipment status and alarms. The design safety objective of each metro railway system shall be to ensure and demonstrate that all the risks to the safety of the passengers, workforce and members of the public who may be affected by the operation of the railways. While the Safety Policy aspires towards achieving a safety goal of zero harm, more realistic and demonstrable engineering safety targets need to be defined for use in the design and of the metro railway systems. It provides effective and reliable third-party interfacing services, storage and online/offline analysis of MEP systems acquired data, enable testing and commissioning of MEP systems [9]. The impact of failures varies from a minor inconvenience, costs to personal injury, significant economic loss, and death [7]. So the functional safety of BACS is most important. Thus the respective technology is supposed to work reliably, safely, securely and efficiently [6]. The safety analysis for BACS in a metro railway station is described with the help of the Safety Integrity Level (SIL).

3. SAFETY INTEGRITY LEVEL (SIL)

The concept of Safety Integrity Level (SIL) has been developed within a different system of standards (CENELEC EN 50129, IEC 61508) [11]. Safety is defined as the freedom from unacceptable levels of risk of harm. Functional safety is the part of the overall safety that depends on a system or 'equipment operating correctly in response to its inputs' [5]. Safety integrity is the ability of a safety-related system to achieve its required safety functions under all the stated conditions within a stated operational environment and within a stated period of time. Safety Integrity Level (SIL) is a number which indicates the required degree of confidence that a system will meet its specified safety functions with respect to systematic failures. The SIL determination is based on safety functions that are applied to mitigate high-level hazards. A SIL is determined based on a number of quantitative factors (to control random failures) in combination with qualitative factors (to avoid systematic failures) such as development process and safety life cycle management. There are four SIL levels, they are:

- SIL 4: represents the system is Dangerous to know!
- SIL 3: represents the system is best avoided if possible but may be necessary.
- SIL 2: represents the system is most likely for an interlock/safety system with logic.
- SIL 1: represents the system doesn't really need an interlock/safety system.

In this paper, the Safety Integrity Level (SIL) is determined based on IEC 61508 and CENELEC EN 50129 standards for the safety analysis of the BACS in the metro railway station.

4. FAULT TREE ANALYSIS (FTA)

Fault Tree Analysis (FTA) is an analytical technique that is used for safety analysis. FTA is one of the most commonly used Quantitative Risk Analysis (QRA) methods [1]. Quantitative Risk Analysis (QRA) is proven as a valuable tool in assessing the overall safety performance of any metro system. Here, QRA is used to understand the probability of BACS failure. In this paper, QRA is performed using FTA approach. To evaluate the probability of the top event using statistical methods is its main objective and also to find the root causes of the system failures before the failures really happen. These calculations need the system quantitative maintainability and reliability measures like repair rate, failure rate and failure probability. After completing an FTA, it can help focus efforts on improving system safety and reliability. At the system level, the different hardware failures are found by FTA as the top event. A fault tree diagram is formulated by finding the definite root for the failure of the top event. In this formulation process, it uses the top-down approach. Fault tree analysis employs the terminology such as a top event, basic event and intermediate event. These events are described as:

4.1 Top Event

System failure mode to be analyzed is termed as the "Top event" and each fault tree considers only one such top event for the analysis. The top event is normally an undesirable event or the critical failure mode of the system function to be analyzed.

4.2 Basic Event

It is the limit of resolution of the fault tree. Basic event is a component failure event beyond which development of fault tree branches is not useful.

4.3 Intermediate Event

The event which is further developed in the tree is termed as intermediate events.

5. ARCHITECTURE OF THE SYSTEM

The metro station master room is fitted with the system that controls and monitors stations MEP systems is termed as

BACS. There are of three main networks in the architecture of the system as shown in figure 3 namely:

- BACS Management (Servers)
- BACS Control
- BACS Field Control and Monitoring

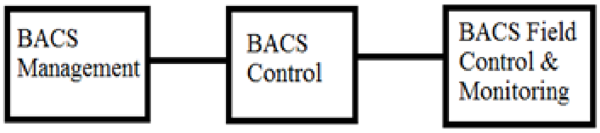


Fig. 3: Block diagram

BACS management has backup batteries, so in case the power device fails, it is backed with batteries and it is powered by UPS. BACS control is considered the PLC's of the BACS to be redundant. For the SIL assessments of the BACS, components/ subsystems used in Management, Control have been taken into account, and then all the modules used in BACS Field which are input/output modules communicate with end equipment. The failure of any input/output module will only fail to operate the end equipment connected to it. The Safety Function that is implemented by the whole system consists in a sensor which detects the hazard and transmits to the logic that processes the signal and activates the actuator which will mitigate the hazard to an acceptable level [4]. The SIL Determination starts with a Hazard Identification Session where the high level hazards associated with BACS safety.

6. CENELEC EN 50129 AND IEC 61508

6.1 CENELEC EN 50129

In European countries, this standard is the common base for the safety acceptance and confirmation of electronic systems for railway signaling applications includes both hardware and software aspects [2]. The standard contains the safety case which consists of:

- Proof of quality management report,
- Proof of safety management report,
- Proof of functional and technical safety report,
- Safety acceptance and confirmation

6.1.1 Proof of quality management: Quality Management System (QMS) document provides the information about the process adopted to minimize the risk of systematic faults in every stage of the product life cycle by satisfying the quality of the system, sub-system or equipment.

6.1.2 Proof of safety management: The safety management consists of a number of activities, they are:

- System Safety Plan is prepared to identify safety management structure, safety-related activities and procedures for safety reviews for both Software and Hardware.
- Identification of System Safety Requirements.
- Hazard Log is maintained to list out the identified Hazards.
- Quantitative Risk Analysis (QRA) is carried out.
- Tolerable Hazard Rate (THR) is computed at the system level.

6.1.3 Proof of functional and technical safety: Technical Safety Report (TSR) provides the reference to technical principles which guarantee the safety of the design and all supporting evidence. It provides the reference to the documents that discuss the practical measures taken to prevent the occurrence of identified hazards.

6.1.4 Safety acceptance and confirmation:

For the safety acceptance and confirmation of electronic systems for railway signalling applications, there are three conditions must be satisfied. They are as already stated in section 6.1.

CENELEC Standard uses the concept of Safety Integrity Level (SIL) based on the Tolerable Hazard Rate (THR).

THR is defined as a hazard rate which guarantees that the resulting risk does not exceed a target individual risk.THR based SILs for the CENELEC EN 50129 standard is presented in table 1.

Table 1: THR based SIL for CENELEC EN 50129

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level (SIL)
$10^{-9} \leq$ THR$<10^{-8}$	4
$10^{-8} \leq$ THR$<10^{-7}$	3
$10^{-7} \leq$ THR$<10^{-6}$	2
$10^{-6} \leq$ THR$<10^{-5}$	1

6.2 IEC 61508

This standard uses arisk-based approach to find the safety integrity requirements of Electronic/Electrical/ Programmable Electronic (E/E/PE) safety-related systems in the railway applications [3]. In this standard, functional safety is obtained by providing the necessary activities to the system safety function in the overall safety lifecycle. The safety life cycle is an engineering process that consists of all the steps necessary to obtain the system functional safety. Safety integrity levels are introduced to determine the target level of Safety functions. In this standard SIL is determined based on the Probability of Failure on Demand (PFD). PFD is defined as the system is not able to operate its safety function when needed due to the dangerous failure [8]. PFD is calculated as:

(a) Analyse the block diagram
(b) Identify the Architecture
(c) Collect the data required for theoretical calculations from Bill of Materials (BOM) and their corresponding failure rate information. Among the different architectures, in this paper one out of two (1oo2) architecture is identified, because there are two channels connected in parallel in which one channel is enough to process the required safety function and the theoretical calculations are carried out based on the formulas [3].

$$\beta_d = \frac{\beta}{2} \quad (1)$$

$$SFF = \left(\Sigma\lambda_s + \lambda_{dd}\right)/\left(\lambda_s + \lambda_d\right) \quad (2)$$

$$\lambda_{du} = \lambda_{total}(1 - SFF) \quad (3)$$

$$T_{ge} = (\lambda_{du}/\lambda_d) * (T/3 + MTTR) + (\lambda_{dd}/\lambda_d) * MTTR \quad (4)$$

$$T_{ce} = (\lambda_{du}/\lambda_d) * (T/2 + MTTR) + (\lambda_{dd}/\lambda_d) * MTTR \quad (5)$$

$$\begin{aligned} PFD = {} & 2((1-\beta_d)\lambda_{dd} + (1-\beta)\lambda_{du})\wedge 2T_{ce} * T_{ge} + \beta_d * \lambda_{dd} \\ & * MTTR * \lambda_{du} * (T/2 + MTTR) \end{aligned} \quad (6)$$

Where

β = %undetected common cause failures;

β_d = %detectedco mmon cause failures;

λ_s = safe failure rate;

λ_d = dangerous failure rate;

λ_{du} = undetected dangerous failure rate;

λ_{dd} = detected dangerous failure rate;

SFF = Safe Failure Fraction;

T_{ce} = Channel equivalent down time;

T_{ge} = system equivalent down time.

T = Test Interval

In these calculations, the Meantime to restoration (MTTR) is 26 min or 0.4326 hours. Proof test interval (T) is listed for each table and assumed as 8760 hours (1 year). Common cause failure percentage (**β**) and detected common cause failure percentage (**β_d**) values used in the calculations presented in this paper are 10% and 5% respectively. These theoretical calculations required as the input data to the FTA. There are two modes of demand in this standard, they are low demand mode and continuous/high demand mode. The high demand should be used when demands are expected to arise:

- Greater than once per year, and
- Greater than twice as regularly the system is checked out.

The low demand mode is used if the high demand conditions fail. Based on the PFD value the SIL for the IEC 61508 is taken from the SILs as shown in tables2 and 3 respectively.

Table 2: PFD based SIL for on/low demand operation for IEC 61508

Low demand mode of operation (probability of failure on demand per hour)	**Safety Integrity Level (SIL)**
$\geq 10^{-5}$ to $<10^{-4}$	4
$\geq 10^{-4}$ to $<10^{-3}$	3
$\geq 10^{-3}$ to $<10^{-2}$	2
$\geq 10^{-2}$ to $<10^{-1}$	1

Table 3: PFD based SIL for continuous/high demand operation for IEC 61508

High demand or continuous mode of operation (probability of a dangerous failure per hour)	**Safety Integrity Level (SIL)**
$\geq 10^{-9}$ to $<10^{-8}$	4
$\geq 10^{-8}$ to $<10^{-7}$	3
$\geq 10^{-7}$ to $<10^{-6}$	2
$\geq 10^{-6}$ to $<10^{-5}$	1

7. ANALYSIS AND RESULTS

To determine the SIL for the safety analysis of metro railway station, FTA is developed in the ITEM software for both the standards CENELEC EN 50129 and IEC 61508. In both the standard, FTA is varied according to the input data given to it. FTA accordance with the CENELEC EN 50129 standard is shown in figure 4.

In CENELEC EN 50129, SIL is assigned to the BACS of the metro railway station based on the THR. The results of the FTA accordance with the CENELEC EN 50129 standard are shown in table 4.

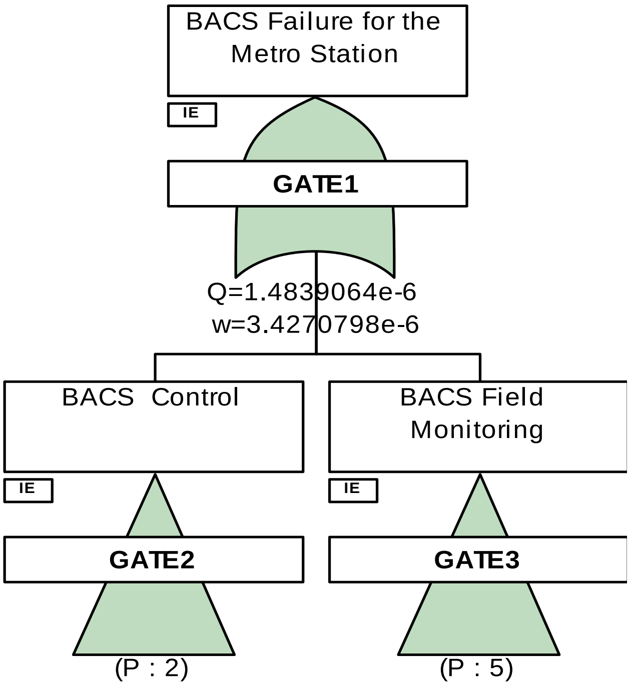
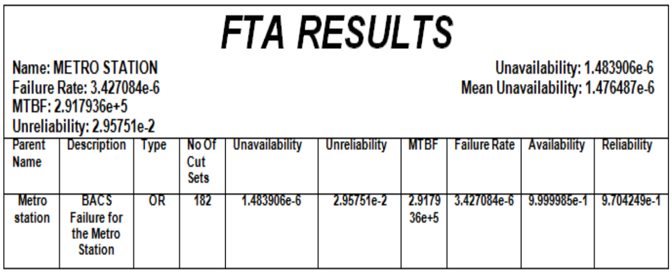


Fig. 4: FTA for BACS accordance to CENELEC EN 50129 standard

Table 4: FTA results accordance to CENELEC EN 50129 standard



FTA RESULTS

Name: METRO STATION
Failure Rate: 3.427084e-6
MTBF: 2.917936e+5
Unreliability: 2.95751e-2

Unavailability: 1.483906e-6
Mean Unavailability: 1.476487e-6

Parent Name	Description	Type	No Of Cut Sets	Unavailability	Unreliability	MTBF	Failure Rate	Availability	Reliability
Metro station	BACS Failure for the Metro Station	OR	182	1.483906e-6	2.95751e-2	2.917936e+5	3.427084e-6	9.999985e-1	9.704249e-1

In IEC 61508, SIL is assigned to the BACS of the metro railway station is based on the PFD. The calculations made according to the formulas are the inputs to the FTA accordance to the IEC 61508. FTA in accordance with the IEC 61508 standard is shown in figure 5.

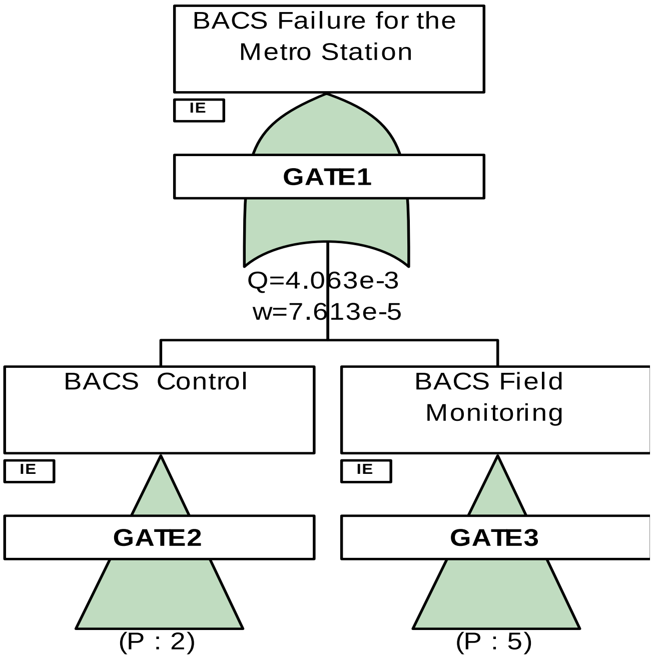
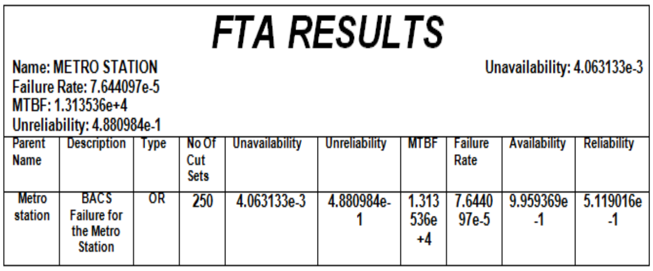


Fig. 5: FTA for BACS accordance to IEC 61508 standard

The results in according with the corresponding IEC 61508 is shown in table 5.

Table 5: FTA results in accordance with IEC 61508 standard



FTA RESULTS

Name: METRO STATION
Failure Rate: 7.644097e-5
MTBF: 1.313536e+4
Unreliability: 4.880984e-1

Unavailability: 4.063133e-3

Parent Name	Description	Type	No Of Cut Sets	Unavailability	Unreliability	MTBF	Failure Rate	Availability	Reliability
Metro station	BACS Failure for the Metro Station	OR	250	4.063133e-3	4.880984e-1	1.313536e+4	7.644097e-5	9.959369e-1	5.119016e-1

8. CONCLUSION

In this paper, the Safety Analysis of BACS in Metro Railway Station is determined with the help of the FTA to analyse Safety Integrity Level (SIL) based on IEC 61508 and CENELEC EN 50129 standards. According to CENELEC EN 50129 standard, the Tolerable Hazard Rate (THR) is 3.42e-6 i.e., SIL 2 is assigned to the system. According to the IEC 61508 standard, the PFD is 3.42e-6 i.e., SIL 2 is assigned to the system. In both, the standards SIL2 is assigned to the BACS in Metro Railway Station. The system is most likely for an interlock/safety system with logic to avoid the failures.

9. REFERENCES

[1] W. E. Vesely and N. H. Roberts, "Fault Tree Handbook", U.S. Nuclear Regulatory Commission, January 1981.

[2] CENELEC EN 50129, "Railway applications Communication, signalling and processing systems Safety related electronic systems for signalling", British Standards Institute, February 2003.

[3] IEC 61508, "Functional Safety of Electrical /Electronic/ Programmable Electronic Safety-Related Systems", Parts 1-7, International Electro – technical Commission, Geneva, Switzerland, 2005.

[4] PV Varde, A Srividya, VVS Sanyasi Rao and Ashok Chauhan, "Reliability and Safety and Hazard", published by Nrosa Publishing House Pvt.Ltd., 2005.

[5] Thomas Novak, Albert Treytl, Peter Palensky, **"**Common Approach to Functional Safety and System Security in Building Automation and Control Systems", IEEE Conference on Emerging Technologies and Factory Automation at Patras, Greece on 28/09/2007.

[6] Thomas Novak, "Functional Safety and System Security in Automation Systems –A Life Cycle Model", IEEE International Conference on Emerging Technologies and Factory Automation at Hamburg, Germany on 03/10/2008.

[7] Ajit Kumar Verma, Srividya Ajit, Durga Rao Karanki, "Reliability and Safety engineering", published by Springer in 2010.

[8] J. Börcsök, P. Holub, **"**Considering and Comparing Safety Parameters –using Different Calculation Approaches of PFD/PFH/HR", XXIII International Symposium on Information, Communication and Automation Technologies at Sarajevo, Bosnia and Herzegovina on 28/10/2011.

[9] Anna Pellegrino, Valerio R.M. Lo Verso, Laura Blaso , Andrea Acquaviva, Edoardo Patti, Anna Osello," Lighting control and monitoring for energy efficiency: a case study focused on the interoperability of building management systems", IEEE Transactions on Industry Applications Society on 08/02/2016.

[10] T.Babu, S. Sripriya, Divya. V, "Building Management System in Metro Rail", IEEE 3rd International Conference on Sensing, Signal Processing and Security at Chennai, India in 2017.

[11] James Li, "SIL Implementation on Safety Functions in Mass Transit System", International Journal of Mathematical, Engineering and Management Sciences at Kingston, Canada on August 2018.