ISBN: 978-3-95450-214-1 ISSN: 2673-5490 doi:10.18429/JACoW-IPAC2021-THPAB250

FIRE DETECTION SYSTEM RELIABILITY ANALYSIS: AN OPERATIONAL DATA-BASED FRAMEWORK

M. M. C. Averna†, G. Gai, CERN, Meyrin, Switzerland

Abstract

This paper describes a logical framework developed at CERN aimed at conducting reliability analysis of safety critical systems (fire detection and alarms) based on operational data. It applies Fault-Tree Analysis (FTA) techniques on maintenance-related data, which are categorized based on the component on failure. This framework, delivered as an automatic tool implemented in Python programming language, can account for all fire detection components installed in tunnels and surface buildings (control panels, detectors, etc.) and safety functions triggered upon detection (evacuation, alarms to the CERN Fire and Rescue Service, compartmentalization, electrical isolation etc.).

INTRODUCTION AND MOTIVATION

CERN (the European Organization for Nuclear Research) is a particle physics laboratory with the largest accelerator complex (LHC i.e. Large Hadron Collider) ever built. At the CERN site, over 700 buildings and 300 underground structures are present, for a total footprint of 435000 m^2 and 59 km of tunnels. Research facilities present often cutting-edge technology and innovative solutions, beyond scope of common safety standards.

Within the mandate of the CERN Engineering Department (EN), the Alarm Systems section design, install, operate and maintain safety critical systems i.e. systems deemed critical for the safety of people, assets and environment, such as the fire detection system and its related safety functions (e.g. alarms transmission to the CERN Fire and Rescue Service, evacuation, compartmentalization, etc.).

The CERN HSE (Occupational Health & Safety and Environmental Protection Unit) is the driving force of the implementation of the CERN Safety Policy, and encourages the use of risk assessment to guarantee safety of people, environmental and property protection as well as business continuity during normal operation and in case of accidents. CERN launched in 2018 a project called FIRIA [1] aimed at quantifying both the likelihood and the consequences of fire events in research facilities, with the ultimate goal is to define risk-informed and cost-effective mitigation strategies when necessary. In this regard, establishing a framework to characterise the availability of Fire Detection systems typically installed at CERN is paramount.

In order to quantify the likelihood of fire events (here intended as outcomes of a fire ignition initiating event), different levels of quantification are needed, including a quantification of the fire ignition frequency, the availability of fire detection and finally the probability of failure on demand of the associated safety actions.

Indeed, among the different technical systems contributing to the fire safety concept of an infrastructure, fire detection and alarm systems play certainly a key role. By detecting a fire at an early stage (incipient phase), they act as initiators of the safety functions foreseen by the fire safety concept to mitigate the consequences of the accident.

In general, despite the effort put in place and the high-quality standards used for design and periodic inspections, fire prevention and protection measures that involve technical systems (fire detection, smoke extraction, sprinklers, etc.) those are prone to faults. For instance, if the detection system fails to detect or part of it, is temporarily inhibited due to works or maintenance activities generating dust and or vapour and compensatory measures are not put in place, not followed or not effective for some reasons, an accident can happen.

For these reasons, a deep understanding of the system architecture and availability, and how this is affected by its components, is essential.

RELIABILITY DATA

Reliability data are in general difficult to retrieve. Qualitative or quantitative strategies can be followed to provide estimates.

Qualitative methods are used if no quantitative information about failure rates and failure modes is available. Considerations on the criticality of certain components can be made by expert judgement, and arbitrary estimates can be derived by using techniques such as Delphi method, etc. This approach can also be applied to a Failure Mode and Effects Analysis (FMEA) to provide a relative ranking of the different modes and identify areas of concern that will be object of more detailed analysis.

Quantitative methods are used if components' failure rates are known or if data to derive them are available. Failure rates can be made available by the manufacturers after the component is put on the market and there are after sales' return for malfunctions. Additionally, some general purpose database exist (Oreda Handbook, etc.) and include reliability data regarding data collected by large industrial organisations as well as Oil&Gas sector industries, which systematically keep track of the performance of their systems. Operational data are accurate in representing the environmental conditions of the domain of installation (project/installation specific), it's therefore crucial to verify and assess their applicability prior use in other domains.
The strategy used in the framework presented with this contribution relies on operational data collected at CERN. In fact, thanks to EN/AA/AS 20 years+ of experience with Computerised Maintenance System tools, working in collaborations with fire detection contractors, with an installed park of 22000 field equipment evaluated in

† melania.averna@cern.ch

ISBN: 978-3-95450-214-1 ISSN: 2673-5490 doi:10.18429/JACoW-IPAC2021-THPAB250

35 MCHF (as new) and following an extensive data structure consolidation over the past 5 years, the InforEAM data is now a powerful asset management database which contains, among others, data on all maintenance activities (replacement, repair, etc.) conducted on systems and specifically the safety critical ones. The data are classified based on the type of malfunction (Problem Code) as well as its origins (Cause Code).

HIGHLIGHTS ON THE FRAMEWORK

The overall idea is to create a calculation framework which is directly linked to the operational data source. Below, the main steps composing the framework are highlighted.

Identification of a Reference System

Detection systems include several components and can have different layout depending on the risks of the facility, the activities performed in it, technology in use etc. The first step of the framework consisted in the identification of a reference system including the minimum components necessary to identify a generic Fire Detection and Alarm System, considering also the Evacuation safety function . According with the EN54-1, a typical CERN detection system is identified by the following key components and represented in Fig. 1:

- Control panels
- Optical point detectors
- Aspirating smoke detectors
- Venturi smoke detectors
- Evacuation sirens.

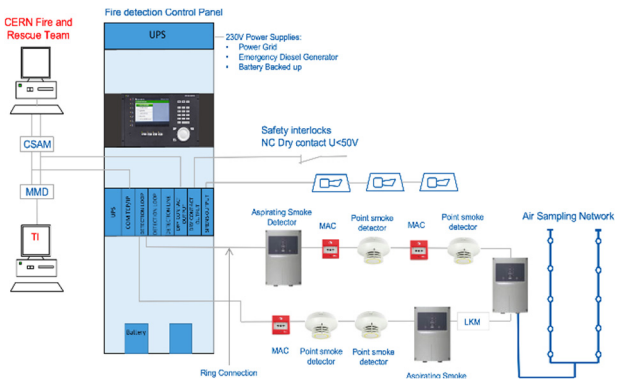

Figure 1: Identification of a Typical CERN Fire Detection System Architecture.

The Detection is ensured by a ring connected system. The control panel provides via its loops and lines power supply to the field equipment (detectors, sirens, manually activated callpoint) as well as the communication bus . The system is fault tolerant, meaning that it continues operating properly in the event of the failure of (or one or more faults within) some of its components. The Evacuation Sirens are connected in line complete with end of line device to ensure the integrity surveillance of the connections. In case of fault (short circuit or open line) it's able to auto diagnostic and raise a fault trip requiring immediate intervention and restoration within 2 hours.

Assumptions

Several assumptions have to be made at this point, including failure occurrence, failure tracking, failure and repair rate, model resolution, preventive maintenance etc. For lack of space it is not possible to detail all of them, but the reader can refer to the poster for additional information.

Operational Data

Considering how the data is archived in the CERN's asset management system a straightforward approach was implemented in this framework without an explicit use of FMEA for the definition of the fault tree scheme.

The database contains information about installed components and the performed works and actions conducted on them, in their service life. In terms of reliability, maintenance-related interventions are of interest, including both preventive and corrective maintenance. Every time an intervention is executed, the operator creates an entry in the database (Work Order) which specifies the conducted activity, the related problem code and whether possible, the cause code.

The alarm system activities are classified according to a complex coding system and each code is used under specific conditions. The introduction of the systematic use of the codes for fire alarm systems took place at the 1st of January 2019. Out of 21 codes, only 13 are considered as relevant for fire detection and alarm systems. Refer to the Poster for further details, on the matrix matching the component type with the related problem codes.

Reliability Parameters Estimation

The failure rate of every problem code on every component is calculated considering the occurred events during their operational time.

Generic Fault Tree Model

For the calculation logic of the failure rate a fault tree model is used. In order to cover as much different fire detection system layouts as possible a general fault tree model is created. The general model is built to represent the most complex configuration which can occur and can easily be scaled down to simpler layouts (Fig. 2).

All events of the generic fault tree model are connected with logical OR gates. In order to calculate the system availability every failure which leads to an intervention has to be counted as for an intervention the system will be disabled for a certain time. This is a very conservative assumption as detection systems are designed to be redundant (Field Equipment, power supplies, alarm transmission) and not to be impaired in case of faulty component; even in case of major failure the safety functions are endured.

ISBN: 978-3-95450-214-1 ISSN: 2673-5490 doi:10.18429/JACoW-IPAC2021-THPAB250

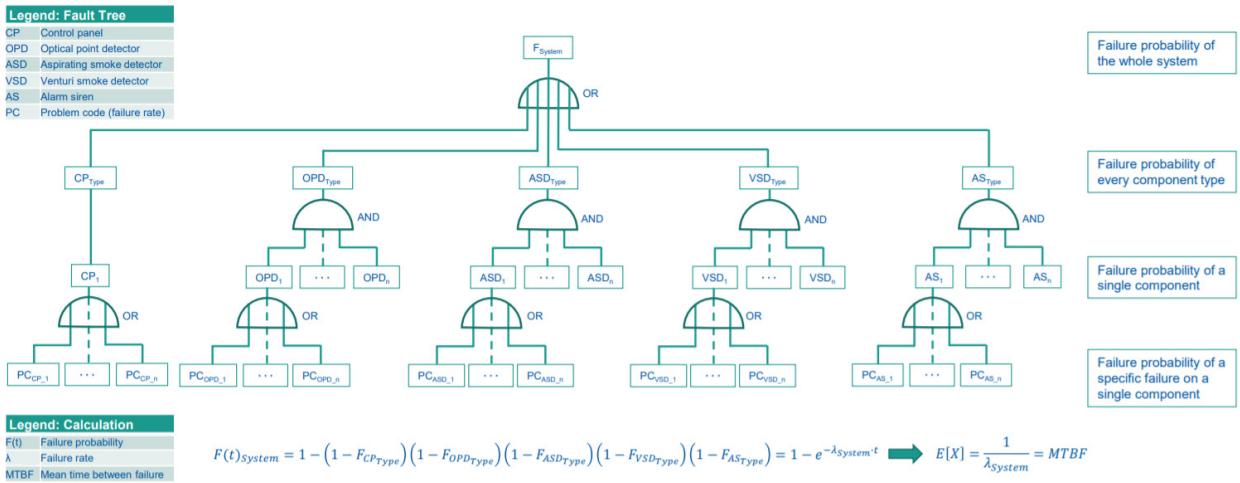

Figure 2: Generic fault tree implemented in the framework.

Output

From the failure probability of the system the MTTF (Mean Time To Failure) can be calculated. The MTBF can be used together with the MDT (Mean Down Time) to calculate the long run average availability of a certain detection system configuration. The MDT is an estimation of the average corrective maintenance time that the operator will take to intervene.

Computing Tool

The overall framework was implemented in a Python code using Jupyter Notebook, an interactive platform easy to use also for who is not familiar with the programming language.

The tool can be used for calculating the availability of a specific configuration, for layout design purpose, as well as for running sensitivity analysis for system optimisation.

FUTURE DEVELOPMENTS

This framework is an initial step for establishing a reliability framework for fire detection systems at CERN based on operational data. Future developments include, but are not limited to, extending the framework to account for additional safety functions such as compartmentalization, electrical isolation and alarm to the CERN Fire and Rescue Service.

A number of refinements are also identified to improve the applicability of this tool. The following points are of special interest:

- The framework could be refined in such a way that the availability considers those periods of the year in which the facilities are not accessible because they are on “beam” mode
- With the increase of data over the years, the effect of the radiological activation on the malfunction of components, therefore on their reliability. Although, the components are object, prior selection, to extensive qualification and characterisation test, prior and after dedicated irradiation campaign, this could be investigated further
- The availability definition used in the framework is an average one. More refined models such as Markov model, accounting for the effect of time on the reliability parameters
- The failure rate of components is assumed to be constant in this approach, as typically done in reliability engineering. A Weibull analysis could be carried out to investigate whether the actual failure behaviour of the components confirm that the data are in the random failure zone.
- The definition of the problem codes could be refined in order to track failures representative of the basic failure modes of the components as identified by dedicated FMEAs.

CONCLUSIONS

This calculation framework includes the basic functions of a fire detection system and provides an adaptable calculation model based on the most common components used at CERN; ensuring flexibility when it comes to future extension and applicability. The output of this analysis shows an order of magnitude of 1.04 % of unavailability i.e. probability that the system will not be able to perform its safety functions during a year (launching the evacuation and raising Alarms). This value is in line with the reference literature on the topic and it will be more accurate in the coming years.

ACKNOWLEDGEMENTS

The authors of this contribution wish to thank Sebastian Braendle who developed the approach during his internship at CERN in 2020.

REFERENCES

[1] FIRIA , https://hse.cern/content/firia