CHEMICAL ENGINEERING TRANSACTIONS
VOL. 111, 2024
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Valerio Cozzani, Bruno Fabiano, Genserik Reniers

ISBN 979-12-81206-11-3; **ISSN** 2283-9216
DOI: 10.3303/CET24111005

Quantitative Risk Assessment: Common Pitfalls in Top Event Frequency Calculation

Giovanni Genna *, Sara Perelli, Leonardo Michele Carluccio, Andrea Gritti

DEKRA Italia s.r.l., Process Safety Business Unit, Via Fratelli Gracchi 27, 20092 Cinisello Balsamo (MI)
giovanni.genna@dekra.com

The main goal of process safety is to analyse and reduce risks related to industrial processes in order to ensure that the final risk on people and environment is as low as possible.
To establish whether the risk related to the process is tolerable or not it is therefore necessary to calculate the risk associated with the events under consideration and to compare the result with the selected tolerability criteria: this is the common approach used in Quantitative Risk Assessment (QRA) analysis.
The risk associated with an event, whatever is its nature (on people, on the environment or financial) is a function of the likelihood of the event (generally expressed in events/year) and the consequences (expressed in terms of damage) of the event itself.
The aim of this article is to focus on the first parameter (frequency evaluation): the main goal is not to write a math paper on frequency calculation (there are a lot of articles and specialised sources in the scientific literature that deal with the theory of probability calculation and, therefore, it would not make sense to focus on math) but to report the main conceptual errors in frequency calculation found in existing risk analysis reports.
Frequency calculation depends especially on the quality of the performed hazard identification study (e.g HAZOP) and on the proper identification of the common cause failures present within a complex system which, if not properly identified, can lead to an incorrect assessment of the likelihood of a dangerous event.
The final scope is to show how it is possible to fall into pitfalls during frequencies calculation if the hazards identification is not properly performed and if dependencies between safeguards are not properly assessed: usually these errors lead to obtain frequency values that have no physical meaning.

1. Introduction

The operation of industrial processes brings with it a certain level of risk, due to their potential negative impacts on health, safety and environment. In industrial activities, as reported by Schüller (2005), risk can be defined as a scale of an undesired event (an incident) in terms of probability of occurrence and magnitude of the consequences. This risk can be assessed either qualitatively or quantitatively: a qualitative risk assessment relies on assessor experience and/or application of good engineering judgement, while a quantitative risk assessment is based on numerical data and mathematical analysis.
The quantitative risk assessment, commonly called QRA, tries to describe a chain of events – what can wrong, with what probability, with which consequences - by assigning number and figures to each step of the sequence.
The chain of events leading to an undesired impact (the incident) always start with one or more initiating events: in process industries, these can be either plant upsets, equipment failures, or human errors. One of the most critical steps in a QRA is the calculation of the overall probability of occurrence of each accident sequence leading to an incident, as both underestimating or overestimating the probability will give unrealistic results. One of the possible methods to calculate the probability is to develop a Fault Tree, a structured visual representation of all the credible fault paths leading to the incident.

Paper Received: 21 February 2024; Revised: 7 May 2024; Accepted: 31 July 2024
Please cite this article as: Genna G., Perelli S., Carluccio L.M., Gritti A., 2024, Quantitative Risk Assessment: Common Pitfalls in Top Event Frequency Calculation, Chemical Engineering Transactions, 111, 25-30 DOI:10.3303/CET24111005

2. Fault Tree Analysis (FTA)

Fault Tree Analysis is a technique applied in Quantitative Risk Assessment, used to quantify the frequency of occurrence of complex scenarios and events which can lead to catastrophic failure of equipment and severe consequences.
In process industries, Fault Trees are usually employed to determine the frequency of occurrence of incidental hypotheses deriving from HazOp (Hazard and Operability) analyses, in those cases when the same final undesired event (incident or Top Event) can be caused by different chains of events.
A single Fault Tree is developed for each identified Top Event, detailing every potential identified cause (initiating events) and the specific barriers designed to protect or intervene on one or more initiating event. The frequency of occurrence of the Top Event is the calculated as a combination of the likelihood of the causes and the probability of failure of the barriers (failing to intervene when required). Both these values are usually derived from public resources and databases, such as OREDA (OFFSHORE & ONSHORE RELIABILITY DATA) or the Safety Equipment Reliability Handbook published by Exida.
The causes, or initiating events, of a Fault Tree are generally represented by components failure or human errors: both these elements can be statistically described with the demand model, which applies to components that have to change their status when a demand occurs. For these causes, their reliability inside a Fault Tree is summarized by the Probability of Failure on Demand, or PFD.
As mentioned by Gotti and Carluccio (2023), extreme care should be taken when extracting failure rates and PFD values from generic libraries and public resources, as these data may not represent the actual reality of the elements inputted in the Fault Tree (for example in terms of demand modes, aggressiveness of the working environment, etc.).
It is also worth remembering that in reliability analyses the same failure, intended as the loss of the ability to carry out a required task, may stem from very different faults, meaning the sum of conditions arisen during design, fabrication and/or use which are responsible for the loss of functionality.
As a consequence, a generic failure rate for a given component, taken from a public source without a detailed description of the failure modes or the use conditions, may not be representative of the fault subset required by a specific QRA.

3. Common mistakes in the evaluation of frequencies using FTA

A poorly reasoned choice of failure rates from generic libraries, as mentioned in the previous section, can lead to great, and sometimes undetectable, errors in the a frequency estimation for the Top Event of the Fault Tree: it would be difficult to spot a mistake if the final frequency is still within an expected range, while it would be somehow easier to find the error if the final result is several order of magnitude lower (or higher) than the expected outcome.
Selection of failure rates is not the only potential mistake that can lead to obtain frequency values that have no physical meaning: often, in actual industrial experience, it is possible to find calculated event frequencies smaller than 10^{-12} event/years, while the estimated age of the universe is $13.787 \cdot 10^{9}$ years.
When the calculated frequency by means of Fault Tree Analysis for a top event in the process industry is very low (e.g. $\leq 10^{-12}$ events/y), it is very likely that there is a construction error in the Fault Tree itself.
One of the most common errors is that Common Cause Failures (CCF) are not properly considered in the architecture of the Tree. Common Cause Failures can be defined as a subset of initiating events resulting in two or more components being unavailable at the same time, as a result of a shared failure cause.
Neglecting these elements can lead to an incorrect evaluation, even of several orders of magnitude, of the calculated occurrence frequencies.
When developing a Quantitative Risk Assessment for a process industry, Common Cause Failures can get overlooked or underestimated for the two main reasons described below.
(1) Low quality of the PHA / HAZOP analysis: when listing all existing barriers and safeguards against a given scenario, the HAZOP team omits to note down on which logic solver the Safety Instrumented System is implemented, or the HAZOP worksheet fails to specify that the identified safeguards are all implemented on the same logic solver. The logic solvers can be the machine local PLC, a dedicated Safety PLC, or the Distributed Control System (DCS). When these HAZOP worksheets are then used in the next phase of the QRA to develop the Fault Tree, the analyst in charge of the tree may not be aware of the of the dependencies between elements.
(2) Mistakes in the architecture of the Fault Tree: these mistakes are generally made up of omission of elements, as the analyst during the Tree construction deliberately excludes some initiating elements (causes) having a smaller likelihood of occurrence with respect to other initiating causes, under the belief that it will lead to a negligible error in the calculated frequency. As a practical example of this potential mistake, let’s consider

the calculation of the probability of failure on demand PFD of a high-level automatic interlock LSH-01 consisting of an initiator (level transmitter) LT-01, a logic solver PLC, and an actuator (gate valve) XV-01, as schematically represented in Figure 1. The purpose of interlock LSH-01 is to close the liquid feeding valve XV-01 in case the level transmitter LT-01 inside the tank.

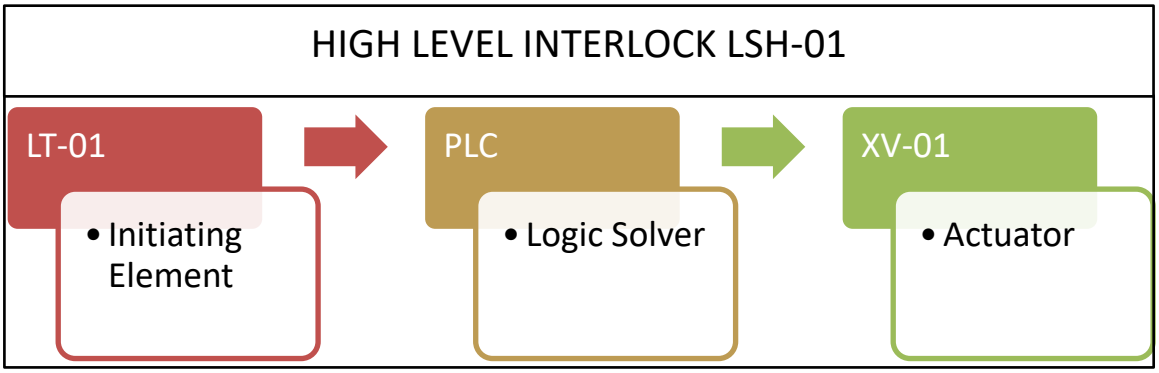

Figure 1: Schematic representation of a control loop

The PFD of the interlock can be calculated as:

$$PFD_{Overall} = PFD_{Initiator} + PFD_{Logic\ Solver} + PFD_{Final\ Element} \quad (1)$$

In its most basic configuration the PFD of the whole interlock, when all the other elements are in 1oo1 configuration, depends on the reliability of the initiator and of the actuator, while the contribution of the logic solver is generally negligible because it is usually more reliable. While neglecting the Logic Solver failure is acceptable if the Fault Tree only has one or two automatic interlocks on the same logic solver, it can quickly lead the calculation astray if multiple interlocks contribute to different branches of the same Fault Tree.
In both scenarios mentioned above, the initial mistakes may lead to devastating underestimations of the final calculated Top Event frequency, sometimes several orders of magnitude lower than the actual value.
When carrying out a QRA, the most commonly omitted element in the construction of Fault Trees is the failure of the logic solver, represented by the Distributed Control System DCS or the Safety-PLC, as these elements, taken individually, are much more reliable than the typical instrumentation of a process plant (transmitters, switches, valves, power breakers, etc.).
The error in making this simplification becomes increasingly greater as the complexity of the tree grows. In complex Fault Trees, a single Top Event is made up of several initiating causes and multiple barriers, with independent initiating elements and with completely independent final elements: each barrier contributes to the calculation of the final frequency with its own PFD.
If all the listed barriers (interlocks) are implemented on the same logic solver (be it DCS o S-PLC), it must be kept in mind that the overall reliability of all barriers (linked through a AND logic into the Fault Tree) cannot exceed the reliability of the logic solver itself, as the logic solver represents the Common Cause Failure (CCF) element.
The most reliable logic solvers used in process industries on the market today are those suitable for SIL 3 applications. With reference to IEC61511 standard, the SIL 3 level corresponds, for a system operating in demand mode of operation (typical for continuous plant), to an average probability of failure on demand PFD_{avg} between 10^{-4} and 10^{-3}, as shown in the table below.

Table 1: Safey Integrity requirement: PFD_{avg} (from IEC61511)

DEMAND MODE OF OPERATION		
Safety Integrity level (SIL)	PFD_{avg}	Required Risk Reduction
4	≥ 10^{-5} to < 10^{-4}	> 10,000 to ≤ 100,000
3	≥ 10^{-4} to < 10^{-3}	> 1,000 to ≤ 10,000
2	≥ 10^{-3} to < 10^{-2}	> 100 to ≤ 1,000
1	≥ 10^{-2} to < 10^{-1}	> 10 to ≤ 100

Consequently, if all the identified barriers for a specific top event scenario are implemented on the same logic solver and if the logic solver is suitable for SIL 3 applications (which is the maximum achievable reliability

today in the process industry) then the overall probability of failure on demand of all the barriers at the same time, that is represented into the fault Tree with an AND gate, cannot be lower than 10^{-4}.

3.1 Example adapted from a real case

In this section, a real case illustrating the above-mentioned pitfalls is described. The case study starts from a selected line of the HAZOP analysis, no flow of cooling water: by constructing the relevant Fault Tree, it can be observed how neglecting to insert the failure of the Safety PLC (that in this case represents the common shared element between all the identified safeguards) leads to an error in the estimation of the final frequency of several orders of magnitude.
The identified Top Event is the overpressure of a reactor due to the loss of cooling water. For the analysed system three safeguards (barriers) have been identified. All the identified safeguards have independent hardware instruments (independent initiators and independent final elements), except for the Safety PLC: the Safety Instrumented Functions are implemented on the same logic solver.

Deviation	Causes	Consequences	Safeguards	Recommendation	Responsibility / Notes
No / Less flow of cooling water	Malfunction of flow control loop FIC1 closing the flow control valve FV1	Increase of temperature and consequent increase of pressure inside the reactor exceeding the design pressure of the equipment. Overpressure, reactor damage and release of flammable material in the working area. Fire and/or explosion scenario leading to 1 fatality	1. Low cooling water flow interlock FSL1/2/3 (2oo3), set at 20 m3/h that open the emergency cooling water valves XVW1/XWV2 (valves in parallel) 2. High temperature interlock TSH1/2 (1oo2), set at 160°C, that closes the shutdown valves XVR1/XVR2 (in series) on the monomer feeding line 3. High pressure interlock PSH1/2/3 (2oo3) set at 3 barg, that opens the blowdown valve BDV		

Figure 2: HAZOP Worksheet adapted from a real case study. All the safeguards are implemented on the same logic solver, the Safety PLC.

Starting from the HAZOP analysis shown in Figure 2, two different Fault Trees have been developed:

- The first one, shown in Figure 3, is the Fault Tree for the above HAZOP line where the failure of the Safety PLC has been omitted.
- The second one, shown in Figure 4, is the Fault Tree for the above HAZOP line in which the failure of Safety-PLC has been explicitly considered.

The following assumptions have been made for the construction of the Fault Tree:

- Proof test interval for automatic interlocks: 1 year
- Mean Time To Repair (MTTR) for detected failures: 24 hours
- Failure data:
  - the failure rates for transmitters and valves incorporated in the Tree are those of generic equipment derived from Exida Safety Equipment Reliability Handbook (SERH);
  - the applied failure rate of the Distributed Control System (DCS) has been obtained by considering the sum of the failure rates of the main processor, power supply, analog in module and analog out module of a Generic PLC;
  - the failure rate of the Safety PLC has been obtained by considering the sum of the failure rates of the main processor, power supply, digital in module and digital out module of a Generic SIL 3 Certified PLC.

In any case the scope of this paper is not to use exact values of failure rates, but rather to demonstrate how neglecting common element leads to an underestimation of the top even frequencies of several order of magnitude.
By comparing the results from the Fault Trees shown in Figure 3 and in Figure 4, two main observations can be made.

EVENT NAME	DATA REF	DESCRIPTION	FAILURE RATE /yr	Trep hr Ttest yr	PROB	Type
FT1		Flow transmitter malfunction	7,88E-03	2,40E+01	2,16E-05	Revealed
DCS		DCS Failure	1,76E-02	2,40E+01	4,82E-05	Revealed
FV1		Flow control valve - fails to regulate	1,01E-02	2,40E+01	2,77E-05	Revealed
FSL1		Flow switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
FSL2		Flow switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
FSL3		Flow switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
XVW1		Emergency valve - Fails to open	1,53E-02	1,00E+00	7,61E-03	Unrevealed
XVX2		Emergency valve - Fails to open	1,53E-02	1,00E+00	7,61E-03	Unrevealed
TSH1		Temperature switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
TSH2		Temperature switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
XVR1		Shut down valve - Fails to close	1,30E-02	1,00E+00	6,47E-03	Unrevealed
XVR2		Shut down valve - Fails to close	1,30E-02	1,00E+00	6,47E-03	Unrevealed
PSH1		Pressure switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
PSH2		Pressure switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
PSH3		Pressure switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
BDV		Blow down valve - fails to open	1,53E-02	1,00E+00	7,61E-03	Unrevealed

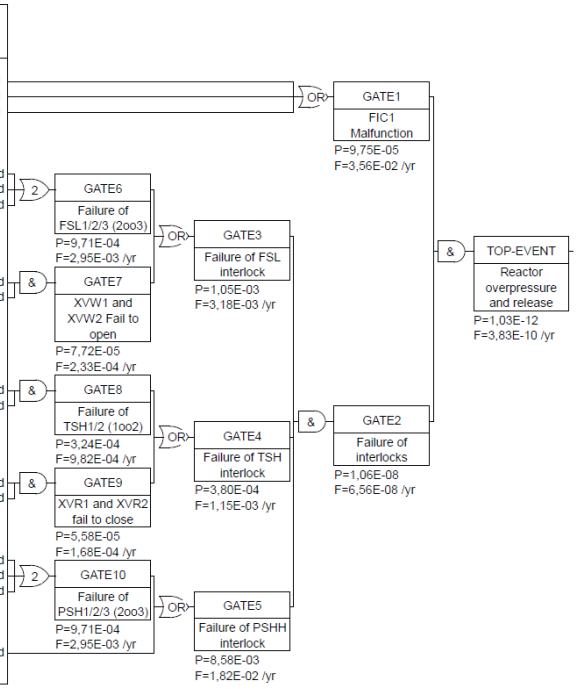

Figure 3: Fault tree with the omission of the failure of Safety-PLC.

EVENT NAME	DATA REF	DESCRIPTION	FAILURE RATE /yr	Trep hr Ttest yr	PROB	Type
FT1		Flow transmitter malfunction	7,88E-03	2,40E+01	2,16E-05	Revealed
DCS		DCS Failure	1,76E-02	2,40E+01	4,82E-05	Revealed
FV1		Flow control valve - fails to regulate	1,01E-02	2,40E+01	2,77E-05	Revealed
FSL1		Flow switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
FSL2		Flow switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
FSL3		Flow switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
S-PLC		Safety PLC - Failure	1,36E-03	1,00E+00	6,80E-04	Unrevealed
XVW1		Emergency valve - Fails to open	1,53E-02	1,00E+00	7,61E-03	Unrevealed
XVX2		Emergency valve - Fails to open	1,53E-02	1,00E+00	7,61E-03	Unrevealed
TSH1		Temperature switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
TSH2		Temperature switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
S-PLC		Safety PLC - Failure	1,36E-03	1,00E+00	6,80E-04	Unrevealed
XVR1		Shut down valve - Fails to close	1,30E-02	1,00E+00	6,47E-03	Unrevealed
XVR2		Shut down valve - Fails to close	1,30E-02	1,00E+00	6,47E-03	Unrevealed
PSH1		Pressure switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
PSH2		Pressure switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
PSH3		Pressure switch failure	3,15E-02	1,00E+00	1,56E-02	Unrevealed
S-PLC		Safety PLC - Failure	1,36E-03	1,00E+00	6,80E-04	Unrevealed
BDV		Blow down valve - fails to open	1,53E-02	1,00E+00	7,61E-03	Unrevealed

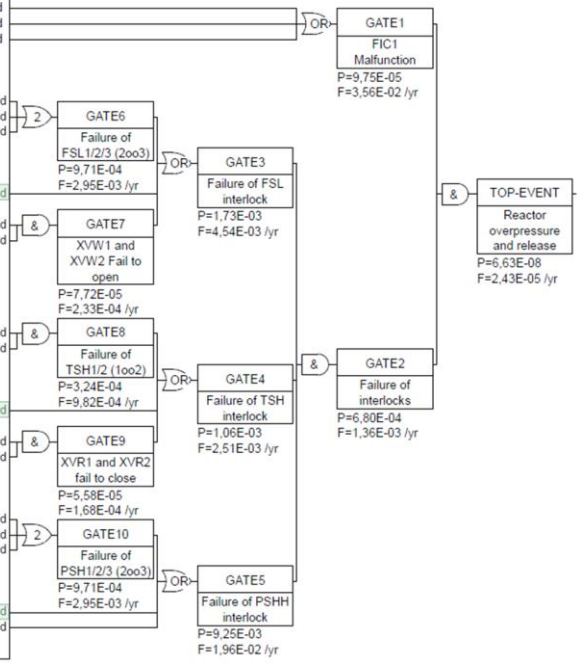

Figure 4: Fault tree which considers the failure of Safety-PLC.

The first aspect to observe is that neglecting to insert the failure of the Safety-PLC in the fault tree architecture leads to an error in the numerical value of the calculated top event frequency that is, for the specific example, of 5 orders of magnitude: the first incorrect Fault Tree leads to a Top Event frequency of 10^{-10} ev/y, while the correct architecture gives a Top Event frequency of 10^{-5} ev/y.

The second important aspect to note from the comparison of the trees is not immediate to see, and is also the most common mistake found in Fault Tree Analysis: where the failure of the S-PLC is not taken into account (Figure 3), the overall calculated PFD for all the safeguards under the same AND gate (see GATE 2 in Figure 3) is equal to $1.06 \cdot 10^{-8}$, which is well below the calculated PFD value of the S-PLC on which the safeguards are implemented (in Figure 3 it is possible to see that the calculated PFD of the S-PLC is $6.80 \cdot 10^{-4}$, a value that is consistent with the SIL 3 range). Clearly, it is unrealistic that the reliability of all safeguards is greater than the reliability of their dedicated logic solver.
This conclusion demonstrates how important it is to evaluate dependencies between safeguards, especially before the Fault Tree Construction, for example during HAZOP analysis and reporting. The aspects discussed so far are not intended to indicate a poor reliability of a S-PLC, but are intended to raise the awareness of people participating to hazard identification and risk analysis activities, as they should be careful when listing effective safeguards and their reliability (sometimes this is referred to as “giving credit” to a barrier): if several barriers are implemented on the same logic solver, it is not correct to assume that all of them are effective in reducing the frequency of occurrence of the fault path, as they are all limited by their common cause failure, the S-PLC. The maximum availability the group of barriers can achieve is the availability of the logic solver itself. Failing to recognize and address these mistakes will lead to calculated frequencies with no physical meaning, which in turn results in an underestimation of the actual risk for people and environment, with severe consequences if the mistake is found out too late.
This is true not only for existing plants and facilities, but also for engineering projects during design phases: if the frequencies (and therefore the risks) have been underestimated during the preliminary HAZOP analysis because the HAZOP team improperly assigned the reliability to the safeguards, then finding the technical solution to correct these mistakes when the error is found gets costly and time-consuming, since the design of the plant has already been finalized, and possibly the plant has already been built. In DEKRA experience, it has happened that due to a miscalculation in the Fault Tree Analysis, the plant had to be stopped until a technical solution to mitigate the risk was found.

4. Conclusions

When assessing risk tolerability, one of the main steps of the analysis is the evaluation of the likelihood of occurrence of a given incident scenario, or Top Event, since the risk is a function of the likelihood and the consequences of the event itself. One the most common techniques applied in Quantitative Risk Assessment to quantify the frequency of occurrence of complex scenarios is Fault Tree Analysis, thanks to its relatively simple and schematic method. This phase of a risk analysis needs to be approached with care and attentiveness, since even small errors or omissions often lead to calculated values with no physical meaning. Starting from a real HAZOP line, this paper has demonstrated how an incorrect evaluation of the dependencies between all the identified barriers (or safeguards) for a given scenario generates an error in the calculation of the Top Event frequency which can be of several orders of magnitude, which in turn leads to a severe underestimation of the process safety risk. Through a simple example, this article aims to highlight these potential pitfalls in Fault Tree Analysis, in the desire of improving the quality of process safety hazard analyses and properly manage the risk for people and environment.

Nomenclature

DCS	Distributed Control System
FTA	Fault Tree Analysis
PFD	Probability of Failure on Demand
PLC	Programmable Logic Controller
QRA	Quantitative Risk Assessment
MTTR	Mean Time To Repair

References

Exida, Safety Equipment Reliability Handbook, 4th Edition, 2015
Gotti M., Carluccio L.M., 2023, Quantitative Risk Assessment: Best Practices and Limitations, Chemical Engineering Transactions, 99, 187-192.
International Electrotechnical Commission, IEC 61511, Functional safety – Safety instrumented systems for the process industry sector, Geneva, Switzerland
Schüller, J., 2005, Methods for Determining and Processing Probabilities (“Red Book”), TNO (The Netherlands Organization of Applied Scientific Research), The Hague, 2005