OPTIMUM VENTILATION AND AIR FLOW CONTROL IN BUILDINGS

17th AIVC Conference, Gothenburg, Sweden
17-20 September, 1996

System Safety Analysis on the Performance of Mechanical Ventilation Systems

Johnny Kronvall

J&W Consulting Engineers
Slagthuset
S-211 20 Malmö
Sweden

Synopsis

System safety of the performance of mechanical ventilation systems can of course be analysed by means of general methods for system safety analysis. Such methods are used a lot in industrial practice, especially in manufacturing industry. However applications on ventilation systems are more or less non-existing today. This paper summarises today's methods for system safety analysis and shows possible future ways of applying the methods on performance analyses of mechanical ventilation systems..

1 INTRODUCTION

Reliability, in the context of ventilation performance can be defined as:

the probability that the ventilation system provides certain required air flow rates in each occupied part of a building during the time between scheduled maintenance occasions.

The required air flow rates may be, for example, a specified fraction of the nominal air flow rates or certain fixed values.

As the probability of failure (complete failure or malfunction) is a key issue, the result of an evaluation procedure should be expressed in such terms.

The impact of human behaviour on ventilation reliability can be extensive. For example, the user can hazard the ventilation performance of his dwelling by obstructing the supply air terminal devices in order to avoid draughts. The draught will disappear, but the intended air flow patterns in the dwelling are changed. The performance will also deteriorate if maintenance is performed badly or neglected.

In this paper methods for evaluating the system safety of mechanical ventilation systems for dwellings are outlined. The paper forms part of the Swedish contribution to the work of IEA-Annex 27 "Evaluation and Demonstration of Domestic Ventilation Systems".

2 SYSTEM SAFETY ANALYSIS IN GENERAL

Some different kinds of routines for system safety analysis are shown in figure 1.

The ***qualitative methods*** help us to understand the logical structure of different failure modes of the product, and how they interact. The ***quantitative methods*** use available data on the failure tendency of the components, estimations of times for repairing and human faults. These data can eventually be used for the calculation of the probability of a certain type of break-down of the system. The selection of a specific method depends

on the complexity of the system, the amount of available statistical data and the degree of influencing human factors.

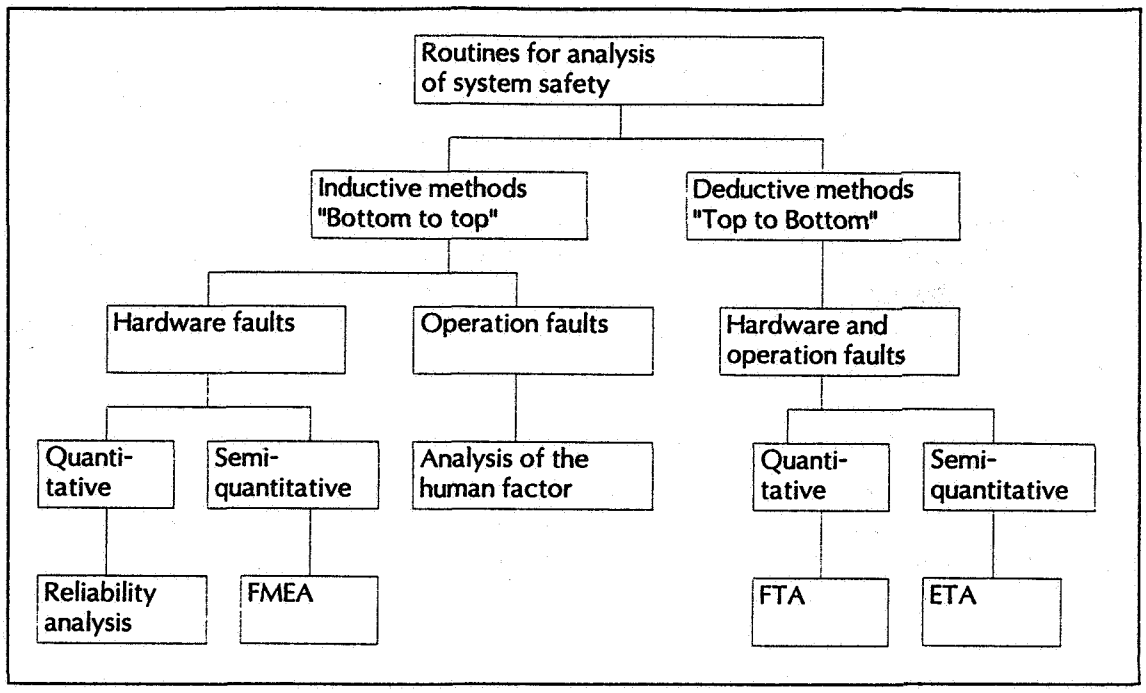


Figure 1 Different kinds of routines for system safety analysis. FMEA = Failure Modes and Effects Analysis, FTA = Fault Tree Analysis, ETA = Event Tree Analysis. After Rao (1992).

With the ***inductive methods***, the analysis work is started at components' level by finding the failure modes of them. After that, one tries to find out what consequences there are on the system as a whole caused by a break-down on components' level. Thus, the inductive analysis works gradually upwards from low component level up to part-system level and finally the system level. This is the way ***Failure Modes and Effects Analysis (FMEA)*** works. The military US standard US MIL-STD 1629 describes in detail how a FMEA-analysis should be worked out.

The ***deductive methods*** have a top-event as a starting point. Gradually one works downwards in the system and tries to find out the causes of the top-event. Thus, the way of working is opposite to the technique used in the inductive techniques. FTA (Fault Tree Analysis) and ETA (Event Tree Analysis) are examples of deductive methods.

FMEA is certainly the most commonly used technique for system analysis as far as product design is concerned.

ETA (Event Tree Analysis) is a graphical description of all possible events in a system. The method is based on binary logic, as events are seen in the perspective of if the have happened or not. A component is regarded as either working or non-working. Thus, it is not possible to take into account a "partially defect" state of a component. If the probabilities of each of all possible events in the tree is known, it possible to calculate the probability of (different) chains of events. The outcome of an ETA is a number of chains of events and their consequences for the system. The probability of each chain is

also shown. ETA is a good technique for comparing different system configurations with each other from a perspective of operational safety. The method was initially developed for evaluating the safety of nuclear power plants.

FTA (Fault Tree Analysis) is frequently used for the analysis of complex systems. The method is extensively used within the nuclear and the aerospace industry. It is a deductive tool and as the method is highly standardised it has been used a lot. The user easily decides the degree of complexity of the system studied, as the method allows for studying separate parts of the system (so called sub-trees) one at a time. Evaluations by means of fault-tree analysis was originally developed by H.A. Watson at the Bell Telephone Laboratories in 1962. The purpose was to analyse the safety concept in connection with the launching equipment for the Minuteman-missiles. After that Boeing used and developed the method further.

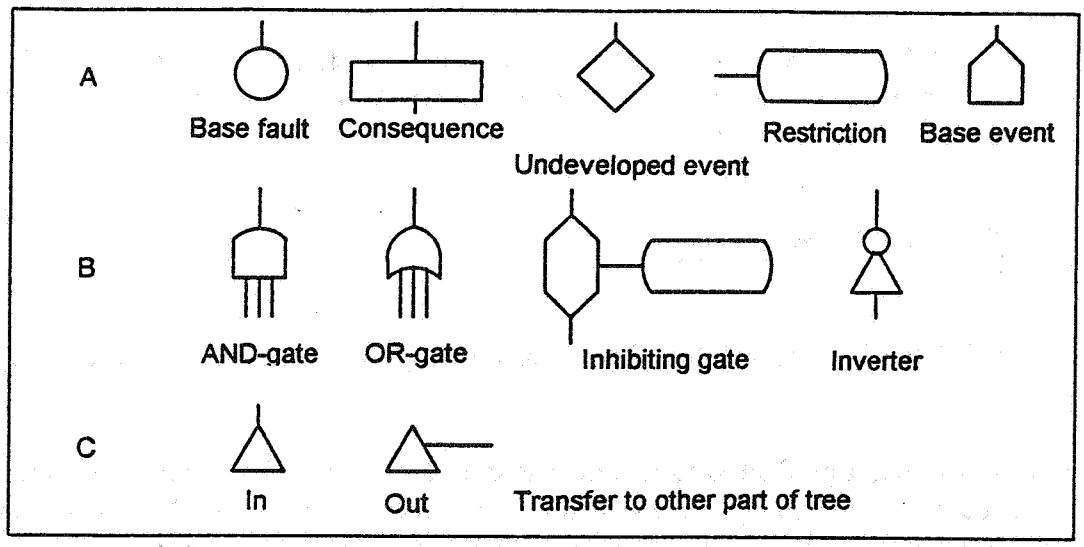
The purpose of FTA is to find the logical structure behind a fault event. Usually a FMEA is performed first, in which the system design, the operation of the system and the environment is analysed in order to find the causality of a fault. Thus FMEA is an important step towards the understanding of the system. Without such an understanding, it is not possible to perform a fault-tree analysis.

The performance of the product is described in a flow chart in which the flows of information, signals and other relevant aspects are specified. Then the flow chart is used for identifying the different functional sequences from inside to outside. Finally a logical chart is designed, in which the functional connections has been translated to logical relations.

In the logical diagram different logical symbols, see figure 2, are used.

Salem et al. (1976) has summarised the working methodology for fault-tree construction in the following six points:

1. The first step in the fault-tree analysis is to define a suitable TOP event that constitutes a serious system failure.
2. Usually several different, but equivalent, fault-trees can be constructed for a given system. Also different TOP events lead to different fault-trees.
3. For any specified TOP event, each possible event is examined to see whether it can, either alone or in conjunction with some other event(s), cause the TOP event.
4. The primary events that lead to the TOP event and the secondary events that cause each of the primary events are determined. The procedure is continued until all basic failures are identified.
5. The set of events that are all required to produce an event of interest are connected to AND gates.
6. The set of events that can individually produce an event of interest are connected to OR gates.



- Base fault: Faults caused by a component or a part-system, for which a probability can be assigned (from known empirical data).
- Consequence: A fault or event caused by a combination of other events via a logical gate.
- Undeveloped event: An singular fault, i.e. a fault that cannot be split up (developed) due to lack of information or lack of meaning.
- Restriction: Condition that must be fulfilled and directing an associated gate.
- Base event: An event normally occurring when the system is working.
- AND-gate: All in-signals must be true for opening the gate.
- OR-gate: One or more in-signals must be true for opening the gate.
- Inhibiting gate: No out-signal if the associated condition is fulfilled.
- Inverter: Changes one into zero (true turns false) or vice versa.
- Transfer symbols: Indicates that the branch continues into another tree (In) or indicates the top-event in a sub-tree (Out).

Figure 2 Standardised symbols for fault-tree analysis. Rau (1992).

3 MODELS FOR RELIABILITY

We use the symbol "*R*" for reliability. As *R*, by definition, is a probability it can be stated that

$$0 \leq R \leq 1$$

The reliability is often time-depending so

$$r = R(t) \qquad -\infty < t < \infty$$

When working with probabilities there are certain stochastic variables (SV) that are of primary interest. One of these determines the ability of the system to maintain the decided performance in an adequate way. This SV is named ***Time To Failure (TTF)*** or alternatively ***Time Between Failure (TBF)*** and is denoted T. The first one is used when non-repairable systems are considered while the other one is used to describe repairable

systems. The SVs TTF and TBF must have some kind of statistical distribution. The notation F(t) denotes the probability that TTF and TBF will not be greater than t, shortly noted $P(T \leq t)$. Thus we can write

$$F(t) = P(T \leq t) = \int_{o}^{t} f(\tau)d\tau \qquad t \geq 0$$

which is called the fault probability. The corresponding density functions are denoted $f(t)$.

The probability that a product is functioning within the given time interval is denoted $R(t)$ and is called the reliability of the system, or the survival function of the system. As survival is the opposite of fault the following equation describes the reliability.

$$R(t) = P(T > t) = \int_{t}^{\infty} f(\tau)d\tau \qquad t \geq 0$$

We also realises that:

$$F(t) + R(t) = P(T \leq t) + P(T > t) = 1$$

$$\frac{dF(t)}{dt} = f(t) = -\frac{dR(t)}{dt}$$

These models make it possible to quantify the operation safety by means of the theories of probability and statistics. By using the expressions above, some more definitions are possible. The expected life cycle or the ***Mean Time To Failure (MTTF)*** and the ***Mean Time Between Failure (MTBF)*** could thus be written (E(T) denotes the expectation value.).

$$E(T) = \int_{0}^{\infty} \tau f(\tau)d\tau$$

or

$$E(T) = \int_{0}^{\infty} R(\tau)d\tau$$

E(T) is regarded as either MTTF or MTBF.

4 OPERATION SAFETY ON SYSTEM LEVEL

The functional structure of a system is often represented by a block diagram with different structures; series or parallel structures or combinations.

Series structures are used when it is demanded that all components work. The following symbols are used:

E_i = the event that the component i works at the time $t = t_0$.

$r_i = P(E_i)$ = the reliability of the component i at the time $t = t_0$.

R_s = the system reliability at the time $t = t_0$.

Thus, we have:

$$R_s = P(E_1 \cap E_2 \cap \ldots \cap E_n) = \prod_{i=1}^{n} r_i$$

If the performance of the system only demands that at least one of the components works, we have a ***parallel structure***. We have:

$$R_s = P(E_1 \cup E_2 \cup \ldots \cup E_n) = 1 - \prod_{i=1}^{n} (1 - r_i)$$

The expressions above are special cases of the so called " k of n model ". This general model expresses the behaviour of a system that demands that at least k out of n components work.

$$R_s = \sum_{j=k}^{n} \binom{n}{j} r^j (1-r)^{(n-j)}$$

The general expression above is valid only if all r_i are the same.

General structures normally includes both series and parallel semi-structures. In many cases the problem can be broken down to a pure series case or a parallel case.

5 APPLICATION TO MECHANICAL VENTILATION SYSTEMS

Mechanical ventilation systems are built up by a number of mechanical and electrical components, such as fan(s), electrical motor(s), damper(s), silencer(s), air terminal devices, system(s) for automatic control etc. The way that these components influence the performance of the system can of course be described in a fault-tree analysis. An attempt to work out a fault-tree for a simple mechanical exhaust ventilation system of a building is shown in figure 3.

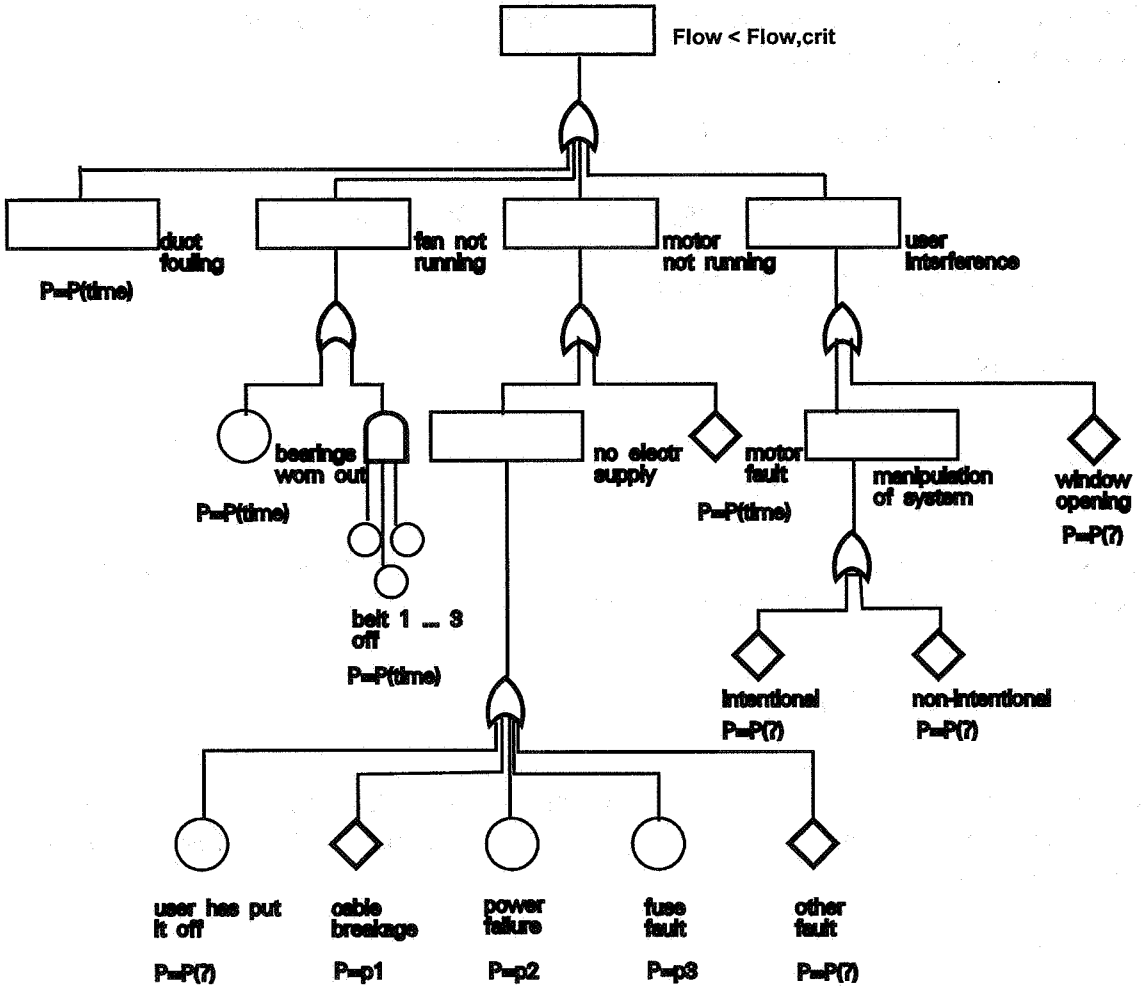


Figure 3 Fault-tree for a mechanical exhaust system in a building.

As TOP event is chosen a performance state of the system characterised by that the flow rate is lower than a critical value. At a level below the top event four different events that can cause malfunction are identified; *duct fouling* (which over time decreases the flow rates of the system), *fan not running*, *motor not running* and *user interference*. For each of these, other basic events at lower level(s) are identified. So far, as we work qualitatively, no major problems arises. What we do is essentially to find the logical structure for how different sources for malfunction influence the performance.

However, if we want to quantify the risk for malfunction or the probability of proper function, i.e. the reliability, we quickly run into a number of problems, most of them originating from the fact that we do not know the probability of failure for individual events. There are principally three different kinds of probabilities to estimate for individual events.

Fixed probabilities (marked as p1, p2 and p3 in figure 3). These are probabilities which are, in principle, not depending on time. For example power failure can be estimated if you can acquire data on how many hours per year you can expect power failure from the electricity company.

Time-depending probabilities. These are depending on in which state, i.e. at what time you analyse the problem. The failure intensity for mechanical components, for example, is not the same as long as the component is fairly new compared to when it grows older. Another example is duct-fouling with its consequences being gradually lower flow rates. The fact that failures appear independent of each other over time and that the failure intensity of individual components are depending on time, implies that a qualitative fault-tree analysis can not be performed as a single one, but be repeated with certain time intervals regarding the time of the use of the system.

More or less unknown probabilities. In the context of ventilation performance, typical examples are events based on user influence. These probabilities are very little known, not only because people are different, but also that the design of the ventilation system influences the behaviour.

The authors impression is that the current severe problems connected with the correct estimation of failure probabilities makes it very difficult and also very doubtful to perform accurate qualitative studies on system level for mechanical ventilation systems today. However, performing qualitative analyses based on construction of fault-trees can be very profitable in order to analyse how different failures are interconnected. Even quite rough guesses of probabilities of individual failures can be made, thus giving rough indications on performance on system level.

6 ACKNOWLEDGEMENTS

This work was sponsored by the Swedish Board for Building Research under research grant no. 940309-6. The support is gratefully acknowledged.

7 REFERENCES

Rau, S.S., ***Reliability Based Design***, McGraw - Hill, 1992

Salem, S.L., Apostolakis, G.E. and Okrent, D., ***A Computer-Oriented Approach to Fault-Tree Construction***, Report No. UCLA-ENG-7635 and NSF/RA-760320, UCLA, Los Angeles, California, April 1976.