An integral approach to safety management

Citation for published version (APA):

Document status and date:
Published: 01/01/1990

Document Version:
Publisher’s PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

• A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher’s website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the “Taverne” license above, please follow below link for the End User Agreement:
www.tue.nl/taverne

Take down policy
If you believe that this document breaches copyright please contact us at:
openaccess@tue.nl
providing details and we will investigate your claim.

Download date: 20. Jan. 2020
An Integral Approach to Safety Management

Door
T.W. van der Schaaf

Report EUT/BDK/42
ISBN 90-6757-046-X
Eindhoven 1990
An integral approach to safety management / Tjerk W. van der Schaaf. - Eindhoven : Eindhoven University of Technology, Department of Industrial Engineering and Management Science. - (Report EUT/BOK ; 42)
ISBN 90-6757-046-X
Trefw.: bedrijfsveiligheid.
An integral approach to safety management

Tjerk W. van der Schaaf

Eindhoven University of Technology

Report prepared for Exxon Chemical Holland B.V.
Rotterdam Aromatics Plant

October 1990

Extended version of a paper presented at the
Exxon Chemical International Safety Coordinators Meeting;
Marbella, Spain; April 2-5, 1990
1. Introduction and overview

In this report we will discuss the fundamentals of a new way of looking at industrial safety with special reference to managing safety-related aspects of human behaviour. We will also focus on the application of these theoretical ideas in a joint project between the Rotterdam Aromatics Plant (RAP) and Eindhoven University of Technology (EUT) in the Netherlands.

First the role of human behaviour in the occurrence of system failures (like accidents, injuries, production loss, environmental damages, etc.) is described relative to other major "causal" factors like technical design, construction, and management.

Then some recent developments in safety research are reviewed in as far as they are relevant to the (chemical) process industries. These are incorporated in the design of a framework for a so-called "Near-miss management system" (NMMS) which we consider to be a promising integral approach to safety management, especially in plants which have committed themselves to a "total quality" programme. The "Eindhoven Classification Model of System Failure" will subsequently be explained, placing special emphasis on operator behaviour. Finally we will describe how parts of a NMMS have been developed and introduced within RAP and what the preliminary results are.

2. Industrial safety and human behaviour

Discussions on the contributing factors of industrial safety have strong "fashionable" aspects. In the beginning of the post-world war II period the main interest was in technical design and construction factors, and much progress has been made indeed in these areas: think of the Exxon Basic Practices and Design Practices for instance. During the 1960's and 1970's the attention switched to studies of how individual persons (usually operators) performed their tasks, and how motivational-, ergonomical-, or training programmes could improve the performance of "man-machine" systems. It is clear by now that the "theme" for the nineties will be concerned with organisational and management aspects as the most important determining factors in safety performance.

In an attempt to clarify this issue we have done several studies on the relative roles of these three groups of main factors in the last 5 years. These studies looked at all kinds of system failures, with consequences varying from zero to (near-)disaster, in three different Dutch chemical plants (including RAP). Using the original in-house reports we could classify the main root cause in about 90% of all cases, with the following distribution:
It is interesting to note that these figures were practically identical for all three companies, in spite of large (cultural) differences between them.

We may predict a rise in the “Management” percentage and a somewhat lower figure for “Operator Behaviour” if we could have investigated these cases soon after their occurrence and according to the latest insights.

Nevertheless, the main conclusion must be that all three factors are of importance, with operator behaviour as the most dominant one. How then should we interpret the abundance of newspaper reports and other sources which constantly proclaim that 90% to 99% of all such incidents are caused by “human error”?

First it may refer to the use of “human” error in a useless way when “human” refers not only to the person(s) directly involved in the incident but also to the designers, constructors and managers who gave the “operator” the tools to be used during task performance: in the end of course practically any design aspect of these “tools” and tasks may be traced to some human action or decision. At the same time such a definition then becomes useless because it does not give a single clue as to where and how improvements might be made.

A second reason might be that the incident investigation usually is rather superficial in the sense that it often looks only at the events directly preceding the observable end components of a usually long and complex set of real root causes and their interactions. These observable end components clearly consist mainly of human actions (or the lack of them).

We propose therefore to define “human” by choosing a certain focus or starting point, dictated by the goal of the investigation. If one is interested in the behaviour of control room operators then their task should dictate the classification: “human” error refers to their behaviour, “organisation” might refer to the procedures they have to follow for instance, and “design” refers to control-room layout, equipment, etc. One could equally be interested in the role of the engineers of course, but in that case the engineers become the human/”operator” component in the analysis; Basic Practices and Design Practices are then part of the “organisation” factor, etc.

In short, we propose a goal-directed classification, because then we can fruitfully distinguish between the three main factors determining industrial safety.

Another “problem” in incident analysis so far is the fact that we usually have been interested only in why things went (almost) wrong, and not why many more similar things which were on their way to becoming an incident went right at the last moment or earlier. More specifically, we should not consider “operators” as system elements which may only be of interest when they “fail”, but should also be interested in the so called “recoveries” they produce: how is it
that humans can detect, diagnose and correct a series of events which could have produced an incident?

These issues will be mentioned again in the following section which deals with research developments in safety, reliability, and quality.

3. Recent developments in safety research

As we have seen in the previous section human recovery is gaining more and more recognition as the natural complement of human error, together forming the whole of safety-related human behaviour. Just as we have done in the past we should continue to determine the factors in the system which make human error more likely (or even provoke it!) in order to take effective preventive measures. Some kinds of human error however will never be effectively and efficiently prevented, either because they are very much part of natural behaviour sequences which are carried out inevitably in an "automatic mode", or because total prevention would mean unacceptable social working conditions (a "police state" within the company) and excessive costs. Therefore it would be much more practical in such cases to "accept" such human errors to a certain extent and analyse why these errors almost always do not lead to dangerous situations or even to system failures and accidents. In other words: what are the factors which promote human recovery of existing dangerous tendencies in the system? An insight into these factors should lead to a situation in which in the design stage of a plant not only error factors are tackled but also recovery factors are built in.

Due to large improvements (in the area of Technical Design and Construction for instance) in the chemical process industry its safety performance has steadily risen for a long time. The relatively low number of actual injuries of the major companies in general and of Exxon RAP in particular has, paradoxically, one main drawback: in a system which uses the number of actual accidents as its main index of safety performance the suggestions for further improvements become less and less numerous as fewer and fewer of these accidents occur! In many plants therefore we see a certain plateau being reached in terms of safety performance as defined in that way. A logical step then would be to shift the focus from actual but rare accidents to the much more numerous near accidents, or near misses. These are estimated to occur up to 30-100 times more frequently than actual accidents, which means that there is in principle a wealth of data hidden under "the tip of the iceberg", as accidents are often called. By definition these near misses must contain (human) recovery in the last phase of the usual chain of events, giving more insight in that phenomenon as well. Also near misses may be considered as precursors of real accidents in the sense that (in hindsight) it is usually possible to indicate several small system incidents long before a similar incident took the form of an actual accident. This of course is especially interesting from a prevention perspective.
Finally we may predict that registration and analysis of near misses may become a legal requirement in the next decade: in civil aviation and in the nuclear power plants this already is the case.

Due to the "automation" of more and more process-control loops the nature of the operator's task and therefore the type of errors has changed dramatically in the last decade: centralised control rooms have become the main working places for many operators, so we should be interested not only in operator actions "outside" in the plant but especially also in operator decisions and interpretations made inside the control room. It is there that some of the vital determinants of safety performance are located, but in most companies very few (if any!) errors or recoveries in control rooms are reported.

If we look at safety in a more fundamental way by registering and analysing not only accidents but also errors and recoveries in order to identify the system factors (root causes) behind these the conclusion is inevitable that those root causes must be identical whether we are starting from a Safety, a Reliability or a Total Quality point of view. In all cases it comes down to understanding exactly how the system works, determining all of the positive and negative factors, and ensuring that this awareness of system functioning is present at all levels of the organisation and supported by them. These objectives should therefore not be seen as separate programmes but merely as variants in the outcome of the same system.

A very important trend is the integration of human behaviour models within traditional risk analysis. It has now been recognised that a risk analysis without the human element is a rather futile, uninteresting exercise in terms of practical use in designing and improving complex man-machine systems such as chemical plants. Fault- and Event Trees for instance should include not only technical elements but also human errors and recoveries in order to give a complete description of system functioning.

Until now most of the developments mentioned above have been initiated in isolation within universities, research- and consultancy establishments, and in safety departments of the larger companies. In the Netherlands for instance the following universities and consultancy firms are actively engaged in process-plant safety: Universities of Delft, Leyden and Eindhoven; several institutes of the Dutch National Organisation for Applied Research TNO; British consultancy firms like Technica and Human Reliability Associates.

Also within Exxon several developments and programmes have been established with relatively little coordination. A picture arises now of many approaches to the same goal, each with their specific strong points which together could form the building blocks of a superior safety management system if proper concerted actions were taken.
4. A framework for near-miss management systems

The general developments mentioned in the previous sections have been translated into the following set of specifications for the design of a management system for the registration, analysis and follow-up of near misses in a chemical plant:

- It must be an integral approach, capable of handling all aspects of system safety, but at the same time with special attention for human behaviour as the dominant factor.
- It must primarily be a learning system, aimed at a progressively better insight into system functioning, and continuously improving itself by building in feedback loops: in this way for instance the effectiveness of suggested preventive measures may be traced by analysing their effects on the root causes in the period after their implementation in the plant.
- It must benefit from and be integrated with (other) Quality tools: near misses and their root causes are by definition important measures of system performance and could play an interesting role in a Total Quality Programme as such.
- The heart of any NMMS and therefore the first design choice should be a proper model of human behaviour: proper, not only in the sense that it should be scientifically respectable, enabling comparisons with other data sources, but also (and perhaps mainly!) proper for the company culture: it would be futile to introduce a NMMS, based on voluntary self reports by employees, in a company which is run in a very hierarchical, authoritarian manner, unless the NMMS would be an integral part of a Total Quality programme. The choice of a human behaviour model is vital because it determines in fact largely the design of the other components of a NMMS: the model tells you which data should be collected (and which not!); it gives you dimensions along which the most interesting reports may be selected out for further analysis; it guides the description of how the reported near miss may be seen as the “product” of existing root causes and their interactions; it dictates of course directly how the elements leading to the near miss should be classified, and interpreted in terms of suggestions to management of effective measures aimed at specific root causes.

Such a general framework for a NMMS consisting of seven modules or steps is depicted below:
1. The Detection module contains the **registration** mechanism, aiming at a complete, valid reporting of all near-miss situations detectable by employees. We are convinced that a voluntary self-report system which stresses the learning aspects of the NMMS is the only usable long-term “solution” for this vital input-phase.

2. A NMMS that works well will probably generate a lot of “deja vu” reactions on the part of the safety staff coping with a sizable pile of these reports. To maximise the learning effect some sort of selection procedure is necessary then to **filter out the interesting reports for further analysis** in the subsequent modules. Management objectives may of course lead to certain selection rules (e.g. special interest in possible personal injuries, or in product quality), but in general the presence of unique elements or unexpected combinations of elements, visible already by looking at the “raw” report, will have to ensure such reports of the extra time and effort needed by the safety staff to apply all modules in these cases.

3. Any report selected for further processing must lead to a **detailed, complete, neutral description** of the sequences of events leading to the reported near-miss situation. An analysis based on Fault Tree techniques enables the investigator to describe all relevant system elements (technical failures, management decisions, operator errors, operator recoveries, etc.) in a tree-like structure called the **Incident Production Tree**. This tree will show all these elements in their **logical order** (by means of AND- and OR-gates) and in their **chronological sequence**.

4. Every element in such a tree may be classified according to the chosen human behaviour model, or at least every “root cause” (the end points of the tree) must be. In this way the fact that any incident usually has **multiple causes** is fully recognised: each near-miss report is analysed to produce a set of classifications of causal elements in stead of the usual procedure to pick out one of these elements as “the main cause”.

---

The seven modules of the NMMS framework with their chronological relationships.
The model and the resulting classification scheme are fully described in a separate section later, because of their key roles in the whole NMMS.

5. Each near-miss tree as such generates a set of classifications of elements which have to be put in a data-base programme for further statistical analysis. This means that a NMMS is not meant to generate ad-hoc reactions by management after each and every serious near-miss report: on the contrary, a steady build-up of such a database until statistically reliable patterns of results emerge must be allowed in order to identify structural factors in the organisation and plant instead of unique, nonrecurring aspects.

6. Having identified such structural factors (the real root causes), the model must allow interpretation of these, that is: it must suggest ways of influencing these factors, to eliminate or diminish error factors and to promote or introduce recovery opportunities in the man-machine systems and indeed in the organisation as a whole.

7. These suggestions to management will of course in practice be judged on other dimensions (e.g. costs!) as well, but if they are accepted by management and actually implemented in the organisation they will have to be monitored for their predicted vs. their actual results, that is: for their effectiveness in influencing the structural factors they were aimed at. This may be done by the NMMS system itself (see the feedback loop depicted in the 7-module framework): in the period following the introduction of the measures, near-miss reports should show a different frequency of occurrence for these factors. If a plant has one or more safety-performance measuring systems apart from the NMMS (like auditing-based systems) then some effect will probably be detectable by these independent indicators of safety also, depending on the degree of "overlap of content" between such separate systems and the NMMS.

5. The Eindhoven classification model of system failure

In this section we present the model of human behaviour integrated with the resulting classification scheme of system failure, in the form of a classification model. In this way we hope to stress the intimate relationships between model and classification.

The model is based on Rasmussen's theoretical work on the analysis of operator tasks. According to his model three levels of operator behaviour may be distinguished.

- **Skill-based behaviour**, referring to routine tasks, requiring little or no conscious attention during task execution. In this way enough "mental capacity" is left to perform other tasks in parallel. Example: an experienced car driver travelling a familiar route will control the vehicle on a skill-based level, enabling him/her to have an intelligent discussion, parallel to the driving task, with a passenger.

- **Rule-based behaviour**, referring to familiar procedures applied to frequent decision-making situations. A car driver integrating the known rules for right-of-way at crossings with stop
signs or traffic lights, to decide whether to stop the vehicle or pass the crossing is functioning at this level also: the separate actions themselves (looking for other traffic, bringing the vehicle to a full stop, changing gears, etc.) will again be performed on a skill-based level. Making these familiar decisions and monitoring the execution of the skill-based actions requires some part of the total mental capacity available to the driver, but not all.

- Knowledge-based behaviour, referring to problem-solving activities for instance when one is confronted with new situations for which no readily available standard solutions exist: The same car driver approaching a crossing where the traffic lights have broken down during rush hour will first have to set his primary goal: does he want to proceed as fast as possible, or does he want to minimise the chance of a collision? Depending on this goal he will control the vehicle with varying degrees of risk taking (e.g. by ignoring some of the usual traffic rules whenever he sees an opportunity to move ahead somewhat).

Different levels of behaviour imply different types and frequencies of errors and recoveries which have to be classified subsequently.

We will now first describe the general structure of the classification scheme, and continue with a more detailed discussion of the part dealing with operator behaviour, taking examples from the implementation at Exxon-RAP.

General structure of the classification model.

The classification consists of two phases. In the first phase a rough classification is made between 3 main categories: Technical factors, Organisational factors, and Behavioural factors. Each main category is, in the second phase, subdivided into several subcategories for further detailed classification.

Each element of an Incident Production Tree can in principle be classified in a rough or detailed way, according to the following procedure: the first question to be answered always is whether it is a Technical factor, with subcategories such as: Engineering, Construction, Material Defects. If it doesn't fall in any of those subcategories, then the second question is whether the element is of an Organisational or Management nature: an example of a subcategory here would be the quality of operating procedures (completeness, accuracy, ergonomically correct presentation, etc.), or management pressure to let production prevail over safety.

When this second main category also would not be applicable, then, and only then, do we end up in the last main category, that of Operator Behaviour. This category has the most subcategories of all (namely 12) because we consider this category as our major point of interest, as stated earlier in this paper. There are four groups of subcategories here:

K - referring to knowledge-based behaviour,
R - referring to rule-based behaviour,
S - referring to skill-based behaviour, and
C - referring to physical and mental capacities which are “present” in the operator when he enters the company grounds.

9
The 12 subcategories of Operator Behaviour are listed below, along with brief examples of typical errors of a plant operator's task.

<table>
<thead>
<tr>
<th>code</th>
<th>description</th>
<th>example</th>
</tr>
</thead>
<tbody>
<tr>
<td>K1</td>
<td>system status</td>
<td>not realizing that part of the plant is inoperative because of maintenance</td>
</tr>
<tr>
<td>K2</td>
<td>goal</td>
<td>aiming at &quot;overspec&quot; production instead of at &quot;right-on-spec&quot;</td>
</tr>
<tr>
<td>R1</td>
<td>license (permanent)</td>
<td>not qualified for a certain task</td>
</tr>
<tr>
<td>R2</td>
<td>permit (temporary)</td>
<td>no permit obtained, although required</td>
</tr>
<tr>
<td>R3</td>
<td>coordination</td>
<td>not informing control-room operator of one's actions outside in the plant</td>
</tr>
<tr>
<td>R4</td>
<td>checks</td>
<td>not ensuring that system status is as expected</td>
</tr>
<tr>
<td>R5</td>
<td>planning</td>
<td>choosing wrong method for correct goal</td>
</tr>
<tr>
<td>R6</td>
<td>equipment/information</td>
<td>using wrong tools/process data</td>
</tr>
<tr>
<td>S1</td>
<td>controlled movement</td>
<td>making typing error on keyboard</td>
</tr>
<tr>
<td>S2</td>
<td>whole-body movement</td>
<td>slipping, tripping, falling</td>
</tr>
<tr>
<td>C1</td>
<td>permanent capacities</td>
<td>insufficient strength or eyesight</td>
</tr>
<tr>
<td>C2</td>
<td>temporary capacities</td>
<td>incidental use of alcohol or drugs</td>
</tr>
</tbody>
</table>

(Any element which may not be unambiguously classified in any of the above (sub) categories, is coded as "X", that is "unclassifiable").

Having described the NMMS framework, its 7 modules, and the essential classification model, it is now time to see how parts of these NMMS-design aspects have been implemented at Exxon-RAP.

6. Applications at Exxon-RAP

In this final section we will briefly describe the main features of the RAP modules for Detection, Description, and Classification, and some of their preliminary results.

Detection Module
The existing form for reporting incidents and near-misses has been simplified and its routing through the organisation has been changed in order to lower the threshold for reporting and quicken the feedback to the originator. As a result the number of reports is up 300% now. Some problems still exist though:
- not reporting a potentially interesting near miss is sometimes due to a lack of recognition of these situations as near misses: this means that some training will be required to explain to all employees what kind of information the NMMS specifically handles. An instruction film (showing how a series of very minor errors and mishaps create the conditions under which an operator at last becomes the victim of a serious accident) has already been tested for this purpose at EUT.

- organisational boundary conditions completely determine whether a well-designed NMMS also becomes a well-functioning NMMS or not: issues like the confidentiality of the reported information, and the form of feedback to the originator have not been resolved yet by management. The original idea of a NMMS of course would favour open and honest communication, making anonymity superfluous. In the same way we strongly support a guarantee being published by management to all employees that an originator of a report of a real near miss situation is freed from any sanctions related to such reported information, however "stupid" the originator's actions may have been. The only exception to this fundamental rule would be cases of open and wilful disobedience of basic safety laws (e.g. "no smoking in the plant"), sabotage, etc.

Description Module
The Incident Production Trees have proven to form a complete and understandable overview picture of a certain incident history. As such they are a powerful communication instrument, capable of showing for instance the combined understanding of operators, engineers and management, of the same incident. Just as in Fault Tree Analysis however there is the problem of the stopping-rule: how do you know when to stop extending the tree branches further and further? A sensible rule could be that you stop the description process as soon as elements appear which are largely beyond the control of the company. In order to "test" the Description and Classification modules a series of so called Critical Incident Interviews was held on a topic of special interest at RAP: 35 operators were asked to recall a recent personal near-miss situation originating from their control room duties. None of these incidents had ever been reported before, although some were potentially serious. On the average these interview-based near misses contained no less than 12 root causes per incident!. Indeed a clear demonstration of the fact that practically any incident is caused by a set of contributing factors, usually none of which may be considered as the main cause.

Classification Module
Descriptive labels for the (sub)categories and illustrative examples were fully adapted to RAP terminology and "culture". Use of the module is also supported by an interactive, PC-based software package which transforms the classification task to a set of yes/no questions, leading finally to a classification in a certain (sub-)category. This package was designed to enable any employee to understand exactly how the classification module was set-up. In the future it will be part of a Local Area Network where any connected terminal may be used by any employee to provide input to the data-base, without having to fill in a paperform first.

11
7. Epilogue

In this paper the design of an “ideal” NMMS has been outlined and partly illustrated by applications at Exxon RAP. At this point it is proper to stress the fact that this also is a “trial-and-error” project, partly based on the belief that it must work somehow because RAP wants it to work within their Total Quality Concept. The contributions of Mr. L.A.A. Bollen and Mr. J.C. Koppelman are therefore gratefully acknowledged.