# From ARAMIS methodology to a "dynamic risk" monitoring system

Emmanuel Plot, Zoe Nivolianitou, Chiara Leva, Vassishtasai Ramany, Christophe Coll, Frédéric Baudequin

**From ARAMIS methodology to a "dynamic risk" monitoring system**

Authors: Emmanuel PLOT (INERIS), Zoe Nivolianitou (DEMOKRITOS), Chiara Leva (DIT), Vassishtasaï Ramany B.P. (MEEM, SNOI), Christophe Coll (DEKRA), Frédéric Baudequin (INTERACTIVE)

**Abstract**

The ARAMIS[1] project is believed to be able to address several goals, in particular: a) the use of state of the art methods to study processes to predict potential hazardous events and their likelihood; b) the achieved 'transparency' of processes that allows both the users and the regulating authorities to understand, validate and comment on risks in a consistent manner. The ARAMIS methodology first introduced the concepts of safety barriers and bow-ties, which, nowadays, are used on a daily basis by the European Industry and are considered as a valuable means to perform risk assessment and to share the results with stakeholders. However, in order to address a risk assessment usable for real time safety management a further step needs to be accomplished, namely: the dynamic monitoring of risk, i.e. how the actual status of equipment and or conditions in a moment in time can be taken into account to update the risk assessment and therefore estimate the risk exposure of the installation towards the accidental scenarios identified. This step was developed thanks to further EU funded project TOSCA[2] that built on ARAMIS achievements. The actual risk level of an installation in respect to hazardous phenomena is in fact a property that changes over time taking into account the actual status of equipment and the management of them. The present paper explains the progress achieved towards this specific goal along with the presentation of an applied case study.

## 1. Introduction

The ARAMIS methodology addresses several risk related industrial needs: a) the need for a methodology to identify, assess and reduce the risk and demonstrate the risk reduction as required by the SEVESO directive. This methodology has to be state-of-the- art and must also bring useful information about the ways to reduce the existing risk level and to manage it daily; and b) the need for a "reference" methodology, the analysis results of which are accepted by the competent authorities. The latter can also use it to assess the safety level of the plant.

A reasonable question to be asked is "How the owner could monitor his plant safety level over time?" A plausible answer to this question is by the using of the risk assessment methodology proposed by ARAMIS as a basis of an IT monitoring performance system. In our opinion, this system should be seen as a mandatory part of the SEVESO directive requirements[3]. However, both ARAMIS methodology and other existing solutions are not yet able to address completely this need. They are generally focused on a mere safety barrier monitoring (see for instance the DNV tool, 2016) or on "simplified scenario" monitoring (see

[1] Accidental Risk Assessment Methodology for Industries in the framework of SEVESO II directive - accepted for funding in the 5th Framework Program of the European Commission, which started on January 2002

2 TOSCA Total Operations Management for Safety Critical Activities accepted for funding in the 7th Framework Program of the European Commission, which started on December 2012 project ID 310201.

[3] SEVESO III

for instance the Petrotechnics, 2016). The idea is to extend the ARAMIS methodology by incorporating the time dimension, so as to address the plant "dynamic risk". The authors of this paper have tried to develop a monitoring system able to address completely this need through several research projects and real cases applications (Leva et al 2010, Demichela et al. 2014, Monferini et al. 2013, Leva et al. 2012). The IT tool developed (using Interactive platform[4]) supports the continuous assessing of the safety barrier status and the automatic recalculation of the actual risk level, together with its comparison with the target levels of the accidental scenarios. The developed Risk model and the relevant barriers selected can be connected to an overall plant model; then all data coming from the both the equipment and the critical task performing inflow as an input to the plant risk model and update the actual risk perception about plant running. Additionally, information can be visualized with appropriate tools and visualized to relevant stakeholders/operators through on-line decision support tools. In the following, the presentation of the whole methodology and procedure is detailed. At each step of the implementation process, the links between the ARAMIS methodology and the new product will be explained.

## 2. Description of the Methodology

This paragraph presents the links between the already developed ARAMIS methodology and the newly formulated dynamic risk assessment methodology.

**STEP 1: Bow ties**

The new methodology begins with the same first step as in ARAMIS, namely the Identification of the Major Hazards in the installation and the construction of the plant model in the form of bow-ties (BT, without safety barriers), which are designed using the MIMAH method[5]. Then these BTs are introduced into the IT Tool. The analyst has also the possibility to use directly the IT tool for the initial design of bow-ties, making the following steps, as depicted in Figure 1:

a) Draw the bow tie using the graph editor of the IT Tool by creating in a sequence:

- The Central event and its estimated frequency
- The Initiating event
- The Dangerous phenomena, and
- The Safety barriers and their estimated level of confidence

b) Activate the frequencies (probabilities) propagation calculations taking into account the estimated initiating event frequencies and safety barrier levels of confidence

[4]/ see: www.interactive.fr

[5]/ ARAMIS's Methodology for the Identification of the Major Hazards, 2001

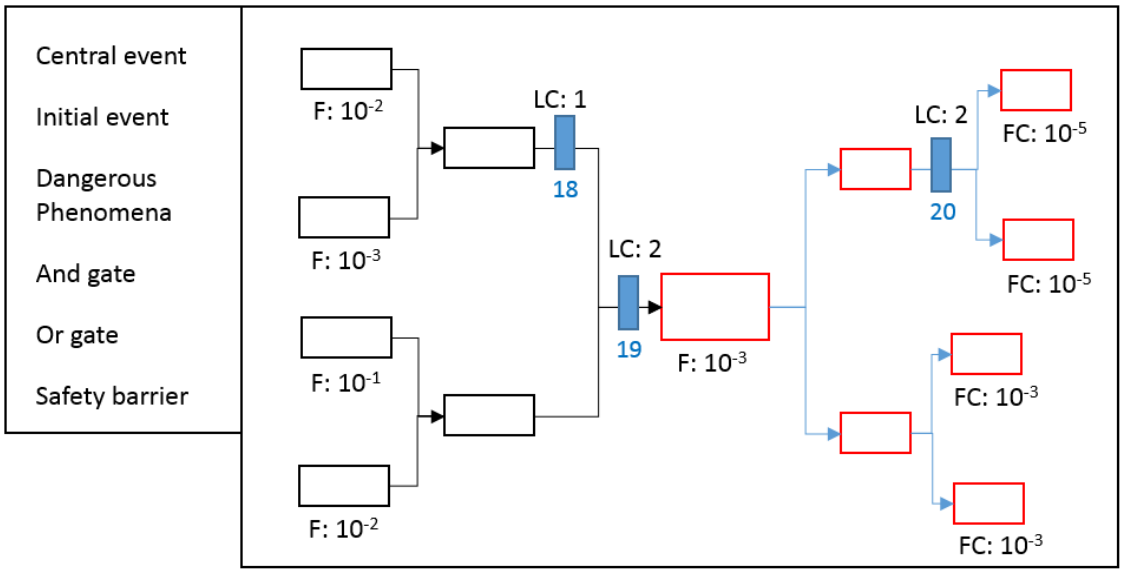


***Figure 1: Bow-ties graphical editor and calculator (on Internet)***

The calculations are done according to the ARAMIS proposed approach:

c) The analysis is made by a gate-to-gate calculation and taking into account the safety barriers on the fault tree. Briefly, the gate-by-gate method starts with the initiating events of the fault tree and proceeds upwards to the critical event. All inputs to a gate must be evaluated before calculating the gate output. All the bottom gates must be computed before proceeding the next higher level. In parallel, the influence of safety barriers on the accident scenario is taken into account. The prevention and control barriers decrease the transmission probabilities between two events in the fault tree and influence the critical event frequency. Indeed, if the level of confidence of a barrier on a branch is equal to n, then the frequency of the downstream event on the branch is reduced by a factor $10^{-n}$.

d) Calculate to the occurrence frequencies of the dangerous phenomena. The objective is to proceed step by step in the event tree to obtain, as output, the frequency of each dangerous phenomenon. First of all, in the generic event trees built with MIMAH, there is no AND/OR gate explicitly drawn. In fact, these gates are implicitly included in the event trees. AND gates are located between an event and its simultaneous consequences. OR gates appear downstream an event of one of the consequent events may occur and the others not. Secondly, when OR gates appear in the event tree, figures for the transmission probabilities linked with these gates is assessed. The transmission probabilities can be the following ones: probability of rain-out and leakage, probability of immediate ignition, probability of delayed ignition or probability of VCE. Finally, safety barriers related to the event tree side are taken into account, both in terms of consequences and frequency of dangerous phenomena. Briefly, it can be pointed out that the prevention and control barriers decrease the transmission probability between two events by their level of confidence and influence so the dangerous phenomena frequency. The limitation barriers reduce the consequences of dangerous phenomena in limiting the source term or in limiting their effects. In the event tree when a limitation barrier is met, two branches must be built, one if the barrier fails with a probability equal to the probability of failure on demand (PFD) and another one, if the barrier succeeds with a probability equal to (1-PFD). The PFD of a safety barrier is equal to $10^{-n}$, n being the level of confidence of the barrier. Both branches are kept in the event tree, because they will lead to different dangerous phenomena, one with less severe consequence but a higher frequency, and the other one with more severe consequence but a lower frequency.

**STEP 2: Equipment and bow ties**

To be able to identify the criticality of equipment according to the criticality of their related dangerous phenomena, links between bow ties and equipment have to be input into the IT Tool. However, Bow ties are often generic, abstract scenarios, designed for several equipment of the same type. Because of that, specific equipment is not directly linked to bow ties; in the data model, specific equipment is linked to generic equipment linked to bow ties.

**STEP 3: Safety barriers and equipment and critical tasks**

In this step, the level of confidence is estimated for a whole safety barrier (and not for a single device), including the different subsystems composing the barrier (detector, safety system, action). For each subsystem, level of confidence, effectiveness and response time will be estimated and combined to calculate a global level of confidence of the barrier. A proper acquisition of relevant information about a system and a task in a safety critical environment is the foundation of every sound Human Factor analysis. The scope of the analysis may cover a Human Reliability Assessment, an evaluation of a Human-Machine system as a whole, the writing of a procedure or the preparation of a training program. When this foundation is correctly set, the conclusions of the analysis will be already addressed towards a useful and reliable direction.

More and more studies have highlighted that this critical first step of the analysis has been taken for granted and not given the attention required for collecting and structuring the information about the tasks and contexts. Task analysis is the process of gathering data about the tasks people performs, acquiring a deep understanding of it and representing it. Traditionally the main steps for achieving a task analysis relevant also in the context of a bowtie are:

a) Preliminary data collection about the task to be modelled (especially if this is a safety barrier).
b) Update collected data through interviews or observations about the actual way the task is performed
c) Representation of the information collected
d) Evaluation of task reliability ( i.e., what is the reliability of a task if it is to be considered a safety barrier and what are the performance shaping factors influencing it, which includes an evaluation of the task demands against the operators' capabilities or an evaluation of specific safety issues related to it).

The estimation of safety barrier level of confidence therefore also needs:

- To monitor all equipment and critical task identified as a part of safety barriers; so it is mandatory to list of these equipment and tasks and to enter them in the IT Tool
- For each equipment and task, to know the impact of a failure on the safety barrier level of confidence; so the qualitative safety barrier structures (detection-treatment-action systems and subsystems) have to be described into the IT Tool.

**STEP 4: Critical tasks and Incidents**

The monitoring of the real time level of confidence for a safety barrier is then based on two types of information:

- The delay in a critical task realization (those directly involved in the safety barrier performances and those indirectly involved such as schedules in preventive maintenance of the equipment directly involved in the safety barrier performances). That gives an indicator of "non-confidence".
- The incidents which indicate the unavailability of an equipment or of person in charge of human barrier.

Based on these two type of information, it is possible to re-estimated the true safety barrier level of confidence.
As an example, one could take the following: If a detector is unavailable (or if there is a low-confidence indicator) more than 10% of time on a given period, then, one knows that the level of confidence of the related safety barrier is null (inexistent).

For being able to monitor the level of confidence of any given safety barrier, one should have daily measurements and insert them into the IT Tool.
Based on that, the tool is able to recalculate periodically the criticality of the dangerous phenomena.

**STEP 5: Changes**

If the hypothesis on which the bow ties are designed are no longer valid, then, the monitoring of the level of confidence and the periodic recalculation of the dangerous phenomena criticality is no longer legitimate. So, the IT Tool has to monitor through time the validity of these hypotheses. A set of related information has to be daily inserted into the tool, namely:

- The Quantity of hazardous substances handled
- The Type of hazardous substances handled
- The Frequency of initiating events
- Etc.

## 3. Case study

The methodology and IT tool presented above have been developed within the European TOSCA project (the tool is referred to as the Computerized Barrier Manager System - CBMS, TOSCA, 2014, Konstantinidou & al. 2015). The innovation lies in the fact that the latter switches from research to business case with the SNOI case study (a national pipeline system managing petroleum facilities and depots). In 2015, the SNOI officers decided to base their monitoring management on the TOSCA methodology and tool. This was an excellent opportunity for the steps of the approach and the IHM of the tool to be reviewed, improved and redesigned, so as to suite the daily industrial. Three major partners have played significant role in this process, namely: INERIS, SNOI and DEKRA industrial.

For this case study, it has been decided to select a prevalent accidental scenario. Having selected the one, four safety barriers have been positioned. At first glance it may have seemed too simple. Though, when we started to link in the IT tool the 88 storage tanks of the 15 SNOI sites concerned with the accidental scenario and to link the equipment involved in their safety barriers, the real complexity appeared. We realized, at the end, that we have to monitor a total of 314 equipment, proving how comprehensive a risk assessment could be. For each equipment the key data to be taken into account has been identified and providing for its storage, format and repetition patterns.

It has been decided then to collected the data every 6 months for updating the criticality calculation of the dangerous phenomena of the petroleum tanks concerned. The first run discovered several "mistakes" or missing data. For instance, analysis performed by subcontractors on a given type of equipment was not usable because it was neither conclusive, nor performed in same time interval and with the same measurement units. This was not known beforehand unless one tries to reuse the data to recalculate anew the risk level on the basis of a different risk assessment method; then the real problems in collected data appears. An additional example is the delays in preventive maintenance. The former were considered from the risk management perspective, but, nevertheless, adopted by the maintenance team because of organizational constraints and because no one in the field knew what was the actual risk assessment requirement to take into account.

It takes more than one year for the management to correct these inconveniences or the missing data. After that period, practices on field are on line, which is patently highlighted throughout the monitoring system put in place.

The methodology and IT tool has been presented to the regulating authorities. They considered it as step ahead in 'transparency' of processes that allows the confidence in the daily work of the industrialist according to what has been validate on risk management requirements.

## Conclusion

On the basis of this case study, it seems that the ARAMIS methodology has a better managerial impact when it is used to support a continuous monitoring.

As expected by the TOSCA researchers, it seems that this approach supports the development of a COP (Common Operational Picture) within a company. This approach seems as a kind of sting for bridging the gap between 'actual practice' and 'official work systems'. It's a support for Human Factor and Organizational improvements, addressing the fact that in complex process control industries, the different stakeholders, regulatory bodies, contractors, managers and operating teams may have their own idiosyncratic 'concept' or 'picture' of the conditions that give rise to risks. Even within the same operational departments, the term 'risk' means different things to different team members who may have different baselines and priorities. At the end, this approach tries to establish a common framework of safety performance, which is very important because these mechanisms of mutual understanding and inter-relating ultimately determine the level of system risk.
There are situations in the industry where the human actions are the main safety barriers to abnormal or accidental conditions. In order to maximize the reliability of good human and organizational barriers we need to ensure that the action-plans generated are based on a valid risk assessment of the situation to be addressed and informed by a relevant human factor analysis. This implies that the process needs to be participatory in nature, thus involving end user all the way through. For the example proposed we involved the end user also in suggesting possible improvement actions. The one to be selected were rated on the basis of their impact and the difficulty/cost of implementation, the impact was informed by the risk assessment effects on the reliability of the barrier but also by what priority the action was assigned during a focus group with the end users. Example of suggested actions are not reported in the current paper.
The evaluation of this work is based on the:

- coherence between the proposals themselves
- coherence between the proposals and the:
  a. the bow tie analysis
  b. The task analysis informing the bowtie and the list of the performance shaping factors selected

The benefit of the approach reflects not only on the quality of the background information provided for the risk assessment but more importantly on the involvement of the main end users of the system in assessing their own work performance and being proactively called to identify way of improving the reliability and safety of it. So even if a further level of automation is identified as a further safety barrier it will be designed in a way that will keep the user proactively in the loop.

The research team believes that an extension of this approach could also support binding a Plant Risk Model with Advanced Process Control based on emerging developments in cloud storage and computing so as to achieve Operational Optimization. We know that overall equipment effectiveness (OEE) can be significantly increased by networking various isolated solutions with the help of software agents in automation technologies. This will allow bottlenecks, cost drivers and process upsets to be better defined and energy consumptions precisely assigned. The data from a networked, integrated system can be used to optimize fuel usage, schedules and prevent plant trips or unwanted downtime. One of the industrial partners, an energy generation company, have estimated that a software agent able to better monitor trends and aggregate data from their DCS, PLCs and a risk model of the plant can help them save over 5M euro per year in unwanted process upsets and trips across their plants. Operations managers will only need to handle a uniform engineering tool system wide. These innovations have, on the other hand, increased the amount of data operations manager needs to handle to achieve a complete overview of plant performance.
The next step should be to set up a new project to build on these results and overcome these difficulties by:

- Providing a Real time framework to connect process data from SCADA, DCS, PLCs to enable real-time intelligence for operations control.
- Proposing an overall plant risk forecast model to be used in conjunction with predictive control techniques, to achieve production efficiency and downtime minimization.
- Offer a novel empirically proven Human Machine Interface to provide task support and training to increase human reliability and situational awareness

## References


1. DNV, 2016 decision support tool for dynamic barrier management
2. Konstantinidou M., Plot E., Leva M.C, G. Mavridis, O. Aneziris, Z. Nivolianitou. 2015 Effective identification and management of critical tasks for safer performance, EMChIE 2015
3. Leva, M.C., Kontogiannis, T., Balfe, N., Plot, E., & Demichela, M. 2015 Human factors at the core of total safety management: The need to establish a common operational picture, Contemporary Ergonomics pp.163-170.

4. Leva M.C., Bermudez Angel C., Plot E., Gattuso M. 2013 When the Human Factor is at the core of the safety barrier, Chemical Engineering Transactions 2013, VOL.33 pp439-444
5. Leva M.C., Kontogiannis T., Plot E., Demichela M. 2014. Total Safety Management: what are the main area of concern in the integration of best available methods and tools? Chemical Engineering Transactions, VOL. 36 pp559-564
6. Leva M.C., Pirani R., De Michela M., Clancy P. 2012. Human Factors issues and the risk of high voltage equipment. Chemical Engineering Transactions, 26, 273-278
7. Leva M.C., Cahill J., Kay A., Losa G., McDonald N. 2010. The advancement of a new human factors report – 'The Unique Report' - Facilitating flight crew auditing of performance/operations, as part of an Airline's Safety Management System. Ergonomics 53(2), 145-148
8. Monferini M., Konstandinidou M., Nivolianitou Z., Weber S., Kontogiannis T. Kay A.M., LevaM.C., Demichela M. (2013) A compound methodology to assess the impact of human and organizational factors impact on the risk level of hazardous industrial plants. Reliability Engineering & System Safety 119, 280-289
9. Proscient tool, 2016 Petrotechnics
10. TOSCA (February 2012 - February 2016; Funding provider : EU-FP7)
11. Demichela M., Pirani R., Leva M.C. 2014. Human factor analysis embedded in risk assessment of industrial machines: Effects on the Safety Integrity Level. International Journal of Performability Engineering 10 (5), 487-496.