Safety Science 112 (2019) 18–37

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

The Holistic Risk Analysis and Modelling (HoRAM) method☆

Simone Colombo

Department of Chemistry, Materials and Chemical Engineering "Giulio Natta", Politecnico di Milano, Piazza Leonardo da Vinci 32, 20133 Milan, Italy

A B S T R A C T

Making decisions in complex systems and for complex phenomena is a challenging task to accomplish. As complexity and uncertainty increase, the use of scenarios to exploring that uncertainty becomes essential to support decision makers. Yet, the increasing complexity of and interrelatedness amongst systems/phenomena is imposing to the risk analysis world a paradigm shift from traditional, "paper and pencil" approaches toward simulation-based approaches, not least because the cognitive demand required to envisage all the possible alternatives the system/phenomenon might unfold is too high to manage for the human mind. The paper presents how the Holistic Risk Analysis and Modelling (HoRAM) method allows, on the one hand, to holistically account for the Human, the Technological and the Organisational (HTO) elements of the system/phenomenon being analysed and, on the other hand, thanks to the use of artificial logic, to create complete partitions of sizes that are unthinkable to achieve with traditional, paper and pencil methods. The paper also explains how the method allows to systemically and systematically account for the consequences scenarios might generate, thus allowing to include in the decision both the possibility of the unwanted outcomes and the associated effort needed to make them less likely or less severe. Finally, it explains how the scenarios can be managed at different level of abstraction to deriving the well-known risk curve, the newly defined risk spectrum, and the critical functions list, which are all necessary tools to better discriminating which alternative to pursue and where exactly investing the (always limited and scarse) resources to reduce the risk.

1. Introduction

1.1. The importance of scenarios in decision making

Making decisions in complex systems and for complex phenomena is a challenging task to accomplish. To be supported in their daily activity, decision makers have appealed, "since the oil shocks upset the business world in the 1970s" (Bood and Postma, 1997), to multiple scenario analysis as "the goal of scenarios is to provide a structured means of communicating uncertainty" (Tourki et al., 2013). Despite scenarios might be defined in different ways (Domenica et al., 2007; Gelman, 2010; Pomerol, 2001; Porter, 1985; Schwartz, 1991; Tucker, 1999; Weinstein, 2007), it is commonly understood that they are meant for anticipating the opportunities (as well as the risks) associated with the possible alternatives and not for developing new strategies (Schoemaker, 1993). Nevertheless, given they (ought to) include a wide range of options against known facts and trends (typically prompted in the analysts' mind in the form of "what if" stories), scenarios might even support strategic thinking (Porter, 1985; Cole, 2014; Means et al., 2005; Schoemaker, 1995; Simon, 1960; Svedung and Rasmussen, 2002; Van der Heijden, 1996; Wright, 2000), increase situation awareness (Endsley, 1995; Wickens and McCarley, 2008) and foster a dubitative attitude (Weick and Sutcliffe, 2001), which is beneficial to increase personal and organisational resilience. Yet deriving credible and reliable scenarios is not an easy task to accomplish. The reason does not only lie on the conceptual model (more or less consciously) adopted by the analyst in "describing" the analysed system/phenomenon (Andersen and Mostue, 2012; Leveson, 2004; Leveson, 2011; Rasmussen, 1997), but even on the methods and (the associated) tools available to the analyst to perform the analysis and to analyse historical data for priority setting (Connelly and Lambert, 2016; Connelly et al., 2016; Hamilton et al., 2016; Karvetski and Lambert, 2012; Lambert et al., 2013; Lambert et al., 2012; Parlak et al., 2012; You et al., 2015; Thorisson et al., 2017, Hamilton et al., 2013, You et al., 2014).

Starting from the shortcomings of the current approaches, the article presents how the Holistic Risk Analysis and Modelling (HoRAM) method can allow to overcoming both the structural and practical limitations imposed by the current approaches in enabling the decision-making process. Specifically, it explains how the method, which is dynamic in nature as grounded on the Artificial Logic Bayesian Algorithm (Colombo, 2016), allows to unveil all the forms (i.e., stories/scenarios) the system/phenomenon being analysed might dynamically unfold (and not just a part of them), thus guaranteeing both consistency and completeness in the characterisation of the logic-stochastic side of the risk. Further, it explains that, in order to identifying the critical functions, the method requires the analyst(s) to couple the logic-stochastic side with the phenomenological side (i.e., the consequences), thus allowing to identifying and prioritising the critical functions on the basis of their relative contribution to the overall risk and not just on the basis their probability of occurrence (hence implying a probability

E-mail address: simone.colombo@polimi.it.

https://doi.org/10.1016/j.ssci.2018.09.018
Received 3 March 2017; Received in revised form 28 September 2018; Accepted 29 September 2018

analysis and not a risk analysis).

Methodologically, the article explains how the 3 (three) phases foreseen by the method to analyse and model the risk are to be accomplished by the analyst(s) to properly analyse the system/phenomenon, what are the 3 (three) decision-making tools the method gives in the hand of the decision makers to make their decisions, and, finally, why they are all essential to enable the decision and give consistency to it. To increasing clarity and dispel ambiguities, the method is described and demonstrated through a relatively simple, yet not at all trivial, industrial use case. Aim of the article and the method is to foster the paradigm shift from the currently diffused "paper and pencil" approach to the new and more adequate "simulation-based" scenario approach to the analysis of risk. The sections to follow formalise the analytical method, provide a demonstration, discuss key assumptions and results, and offer conclusions.

1.2. Shortcomings of current approaches

The first and foremost restraint of current approaches lies in the difficulty or impossibility of creating a complete partition[1] (De Finetti, 1974; De Finetti, 1975; Jaynes, 2003; Savage, 1954), i.e., reconstructing the whole universe of possible alternatives. The most known and widely used risk analysis methods, which conceptualisation (for the majority of them) roots back in the late 60ies and 70ies of the past century, such as the Delphi Method (DM) (Dalkey and Helmer, 1963; Woudenberg, 1991), the Political, Economic, Social, and Technological (PEST) method (Aguilar, 1967), the Hazard and Operability (HAZOP) analysis (CIS&HCCIA, 1977; Lawley, 1974), the Preliminary Hazard Analysis (PHA) (MIL-S-38130, 1963; MIL-STD-882, 2012), the Failure Mode, Effects and Criticality Analysis (FMECA) (MIL–P–1629, 1949), the Bow-Tie Method (BTM) (Gill, 1979), the Fault Tree Analysis (FTA) (Haasl, 1965; Hauptmanns, 1988; Watson, 1961), the Event Tree Analysis (ETA) (WASH-1400-MR, 1975), the Analytical Hierarchy Process, (AHP) (Saaty, 1980; Saaty, 1987), and the Cross-Impact Analysis (CIA) (Glenn and Gordon, 2009), cannot guarantee the creation of a complete partition. Basically, the reason can be ascribed to two, not mutually exclusive, reasons: (1) an inherent limitation of the underlying methodological construct (such as in the Fault Tree Analysis)[2] and/or (2) a practical limitation associated with the necessity of "manually" creating the possible scenarios. From a decision-making standpoint, this constraint is a serious impediment as it does not allow to verify whether the solutions envisaged to diminish the overall risk, they actually do so or, on the contrary, they increase it (a situation that is more frequent than one might think of) and where. This structural or practical impossibility prevents analyst(s) from keeping a systemic (and systematic) approach to the analysis of risk and, ultimately, from being consistent.

The aforementioned methods fall into what might be defined as a "paper & pencil" approach as, despite supported by more or less structured software, they all require the analyst to manually deriving scenarios (by leveraging on his/her creativity and experience). And, indeed, when systems/phenomena become complex, they are practically (not necessarily theoretically) inadequate to identify the criticalities as they require to manage a complexity that is too high for the human mind (Dekker, 2014). In contrast, the "simulation-based" approaches require the analyst to identifying the elective random variable[3] and correlate them logically and stochastically, letting the burden to create the scenarios to the algorithm. The Bayesian Belief Networks (BBN) (Pearl, 1986, 1988; Pearl and Russell, 2002; Constantinou et al., 2016; Wu et al., 2017) fall in this second typology. Conceptually and theoretically, the BBN represent a huge leap ahead with respect to the traditional paper and pencil methods as, by construct, they are meant to create a complete partition. However, they might turn out to be a bit awkward to apply as, in addition to the identification of the elective variables and their logic and stochastic correlations (i.e., correctly modelling the problem), they even require the analyst to train the network to get consistent results. Further, the management of the binary explosion by the currently known algorithms might turn out to be, for complex systems, not enough accurate as the calculation of the joint probability, which is the indicator of the partition completeness, might easily not sum up to 1. This practical "incompleteness", despite underpinned by a robust theoretical construct, does not allow to calculate the information entropy of the partition, which is a useful parameter for the analyst to understand the quantity of information included in the analysis.

A second, often underestimated, constraint is the capability of managing scenarios. As Ahmed et al. (2010) highlighted, although "conventional decision support systems provide a strong database, modelling and visualization capabilities for the decision maker, they do not explicitly support scenario management". Yet managing scenarios is of paramount importance as it practically translates into the capability of analysing systems/phenomena at different levels of abstraction, from different angles, and for different purposes. For instance, an insurer is interested to know what are the risk implications (in terms of risk shape, expected damage and critical elements) associated with the risk slice the insurant is interested to insure and not those of the entire risk spectrum. The capability of manipulating scenarios to look at a part of the risk while keeping a systemic approach is then beneficial both for the insurer and for the insurant. Conceptually and methodologically, this translates into the manipulation of scenarios to represent, on the one hand, the risk at system (or sub-system) level, and, on the other hand, the risk composition reflecting the risk profile. The former is essential to figure out whether the risk associated with a new configuration increases or decreases with respect to the *status quo*, while the latter to understand whether the risk does change its profile both in terms of risk density and range of magnitude.

A third macroscopic limitation lies in the possibility of systematically accounting for the consequences brought to the system/phenomenon by each envisaged scenario and then, ultimately, for the entire partition/universe as a whole. Given that a risk-based decision-making process requires to compare the risk and not just the probability of occurrence, scenarios are to be coupled with the consequence they might bring to the system/phenomenon should they manifest. None of the methods falling in the paper and pencil typology allows to accommodate the consequences in their process. In practice, what happens is that, once the analyst has manually derived the scenarios, s/he performs a consequence analysis and then manually couples it with the (heuristically) selected scenarios, i.e., multiplies the probability of the chosen scenario(s) with the calculated value of the magnitude, to end up with the aimed risk value. Further, this is usually not systematically performed for the entire partition, i.e., for all scenarios, but just for those (heuristically) chosen as critical and deemed distinguished to influence the decision (typically on the basis of their probability of occurrence). Within the simulation approach, the Belief Decision Networks (BDN) (Van de Stadt, 1994) have been purposely developed to accommodate for the consequences (not conceived in the original theoretical construct of the BBN), thus allowing to transform the BBN

[1] A partition is defined as an exhaustive set of discrete (mutually exclusive) alternative choices. The characteristic of a partition is that its probability, i.e., the sum of the probabilities of all its constituents (defined as each of the alternative choices), must sum up to 1.

[2] The widely-used Fault Tree Analysis, being a logical correlation of faulty events only, cannot guarantee the completeness as mixed scenarios, i.e., those produced by a mix of success and failure events, cannot be accounted for by construct. Theoretically, the only method that can guarantee, by construct, the creation of a complete partition is the Event Tree Analysis.

[3] The elective random variables can be defined as those variables strictly needed to describe the behaviour of the system to the extent strictly needed to enabling the decision maker for the specific decision at hand.

into risk-based decision support tool (Sadoddin et al., 2005; Catenaccia and Giupponi, 2013). Yet, even in the new and evolved version, the BDN suffer of the same practical limitations of their predecessors.

A fourth (critical) limitation lies in the prioritisation of the critical functions on the basis of their contribution to the overall risk (micro level). In decision making is of paramount importance to know where and, most of all, to what extent investing the always limited (and scarse) resources. To satisfy this need is then necessary to know the weight each critical function brings with itself in generating the overall risk. All "traditional" methods in that respect do not allow to differentiate the critical functions on the basis of their contribution to the overall risk. On the contrary, they allow to producing an undistinguished list of critical functions on the basis of their logical-stochastic (not phenomenological) influence in generating the undesired scenarios. The weight of each critical function and, thus, the prioritisation of the associated remedies to reduce the risk, is heuristically decided/assessed by the analyst(s) or left to the decision maker. Yet, the systemic search of the system/phenomenon's critical functions and their prioritisation on the basis of the relative contribution they bring to the overall risk, is of paramount importance to underpinning a consistent, justifiable cost-benefit-driven analysis for the identification of risk reduction alternatives.

2. The Holistic Risk Analysis and Modelling method

The HoRAM method has been conceived to solve the aforementioned limitations; it actually enables to:

- Analyse the system/phenomenon by simultaneously accounting for the Human, the Technological and the Organisational (HTO) elements (at functional abstraction level) independently on the field of application (process industry, health care, finance, ICT, aviation, critical infrastructures…);
- Generate the complete partition associated with the identified elective variables (practically not achievable with any of the currently available methods);
- Accommodate the consequences associated to each scenario for a risk-based (and not just a probability-based) identification of the critical functions;
- Prioritise the critical functions on the basis of their relative contribution to the overall risk (and not just on the basis of their contribution to the logic-stochastic part of the risk only);
- Manage the scenarios at different level of abstraction and for limited portions of the risk;
- Perform complex analyses in a manageable timeframe (unthinkable to achieve with traditional "paper and pencil" approaches);
- Provide decision makers with easy-to-interpret results allowing both to clearly decide where (and to what an extent) investing the resources and to justify why they have been invested in such a manner.

Methodologically, in line with the ISO31000 spirit, to be accomplished, the HoRAM process requires 3 phases, namely: (1) the system/phenomenon characterisation, (2) the risk level identification, and (3) the risk treatment. Fig. 1 schematically represents the HoRAM approach versus traditional approaches.

As it can be noticed from Fig. 1, the HoRAM method changes the paradigm of analysis in that it shifts the generation of the scenarios from the heuristics of the analyst(s) to the artificial logic of the algorithm. This paradigm shift allows, on the one hand, to guarantee completeness and consistency of analysis and, on the other hand, to reach a much higher complexity of analysis (thus facing problems "not affordable" with traditional approaches) while significantly reducing the time of analysis for "ordinary" problems. Further, it makes it viable, both methodologically and temporally, the systemic and systematic verification of the potential impact the identified solutions might have on the overall risk level (i.e., verify that they do not increase the risk instead of diminish it), thus allowing an efficient selection of the solutions to reduce the risk (not always the most expensive and articulated solutions are the most effective to reduce the risk).

2.1. Phase 1 – the system characterisation

The first phase is meant to comprehend the system/phenomenon to analyse. Methodologically, it requires the formal representation, at functional level, of the overall Human-Technology-Organisation (HTO) system, namely: the technological components (both hardware and software), the human activities/tasks (the "liveware") and the organisational roles and business processes (the "organisationware").

In the HoRAM perspective, this is achieved by deriving (up to) 4 types of schematisations (dependently on the problem tackled): (1) the Functional Analysis (FA), (2) the Command, Control and Communication Diagram (C3D), (3) the Task Analysis (TA), and, finally, (4) the Decision Action Diagram (DAD).

The FA and the C3D are, so to say, preconditions to achieve a sufficient level of understanding of how the HTO system works, while the TA and the DAD might be deemed not necessary or performed just for some specific human activities, not least because they might turn out to be extremely time consuming.

2.1.1. The Functional Analysis (FA) schematisation

Conceptually, the functional[4] analysis is all but new. Attributed to Lawrence D. Miles, a design engineer of General Electric, the concept of functional analysis (in system engineering) born during World War II "*to address difficulties in satisfying the requirements to fill shortages of high demand manufactured parts and electrical components*" (Wixson, 1999). The concept was subsequently extended by Charles Bytheway to give rise to a more structured methodology called Function Analysis Systems Technique (FAST) (Kauffman, 1979). Since then the functional analysis was adopted in systems' engineering as a structured approach to design complex systems (NASA, 2007; Viola et al., 2012; INCOSE, 2015, Pinna et al., 2016). "*In system engineering, a functional analysis is the systematic process of identifying, describing and correlating the functions a system must perform in order to be successful at any foreseen life-cycle phase or operational state/mode*" (Pinna et al., 2016).

In the context of the HoRAM methodology, the functional analysis is performed by means of the Gantt chart representation (Wallace and Gantt, 1923), "borrowed" and conceptually adapted from the project management community, instead of the 3 more classically diffused forms, namely: The Function Analysis Systems Technique (FAST), the Functional Flow Block Diagram (FFBD; NASA 2007), the Integration Definition for Function Modeling (IDEFØ; NIST, 1993). The reason of this methodological revisiting and adaptation relates to the twofold need (associated with the creation of the input file for the subsequent ALBA analysis) of simultaneously representing, on the one hand, the lengths, the temporal disposition, as well as the reciprocal interdependencies (logical links), of the activities that are to be performed (the "correlational" view), and, on the other hand, their indented list (the "narrative" view) reflecting and describing the functional and logical level of decomposition (i.e., the deepness). Fig. 2 shows how the Gantt chart representation of a functional analysis looks like. The narrative view is particularly useful to allow for building an input file with a homogenous granularity, i.e., made up of queries at the same level of indentation, which is a fundamental prerequisite to produce a balanced and credible risk analysis. In that respect, the Gantt chart allows for checking at a glance whether the elective variables being selected (i.e., the functions) belong to the same level of abstraction (i.e., the same level of indentation). Fig. 3 shows how immediate is the checking of the

[4] Functions might be defined as "discrete actions necessary to achieve the system's objectives" – SMC (2001).

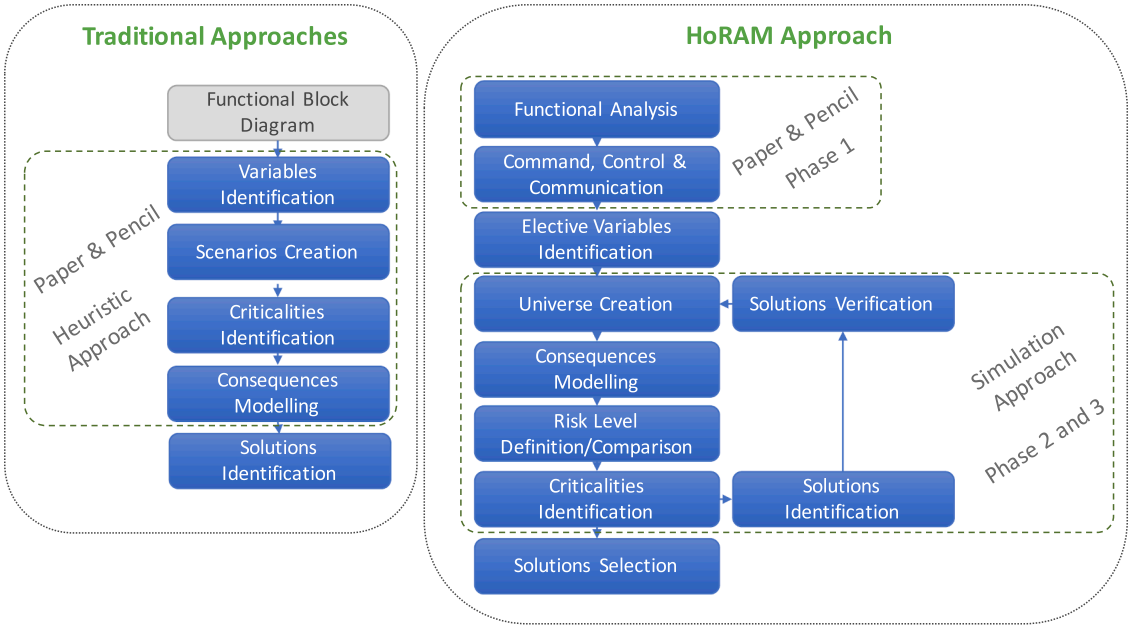

Fig. 1. HoRAM process vs. traditional processes.

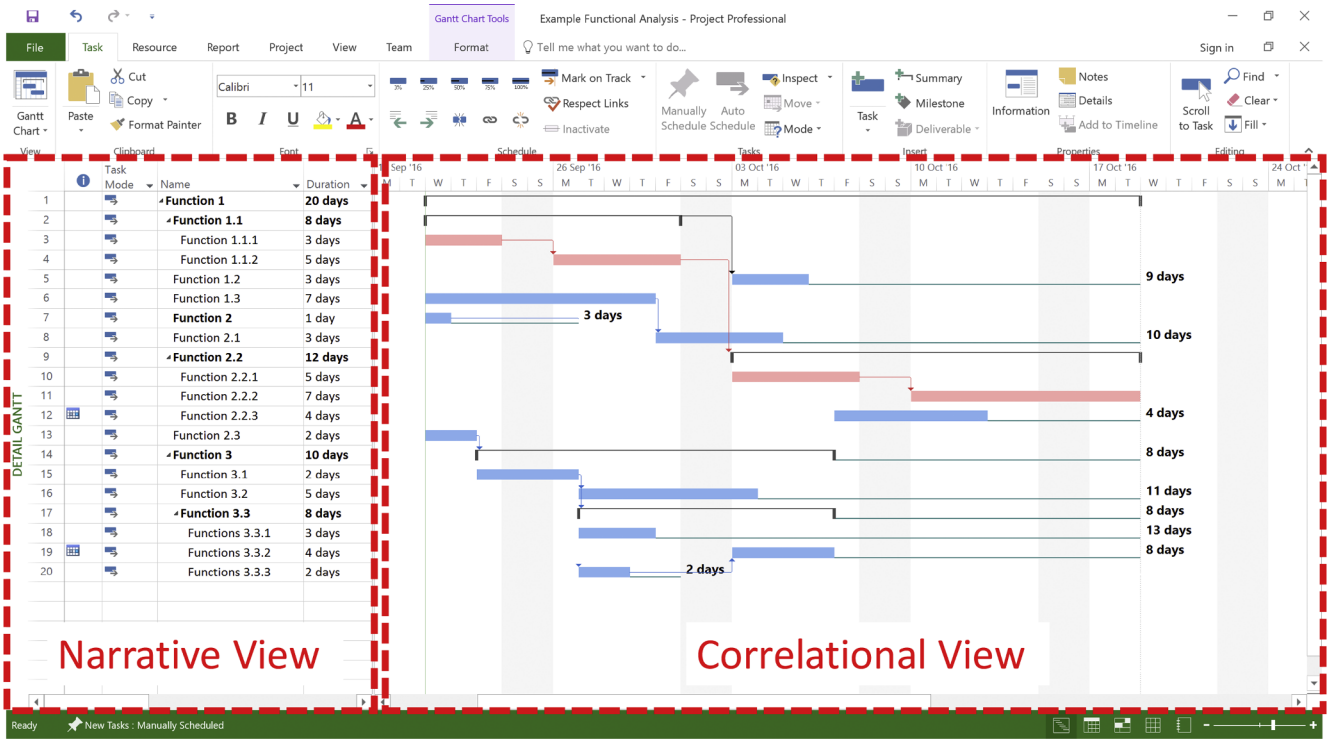

Fig. 2. Gantt chart representation of a functional analysis.

granularity for a level 3 of indentation.

The correlational view, instead, facilitates the analyst to think about the reciprocal dependencies (both logical and temporal) amongst the different functions and eases their visual representation.

2.1.2. The Command, Control and Communication Diagram (C3D)

The functional analysis itself does not, unfortunately, solve all the modelling needs. Actually, to thoroughly understand and model whatever system/phenomenon involving people, it is necessary to couple a functional analysis with a Command, Control and Communication Diagram (C3D). Analogously to the functional analysis, the C3 concept is all but new. Born in the military domain, the first concept of Command and Control (C2) might be reasonably attributable to the Swedish commander Gustavus Adolphus (1594-1632). The first structured and probably most known approach is the Observe, Orient, Decide, and Act (OODA) Loop (Frans, 2006), devised in 1975 by John Boyd, a military strategist and USAF Colonel that applied the OODA decision cycle (based also on feedback) to the combat operations process at the strategic level in military operations. The concept was subsequently extended to the emergency and disaster management domain (Huang, 2015) and, ultimately, to the industry world. Today, under the C3 "label" there are (several) industrial products, typically Information

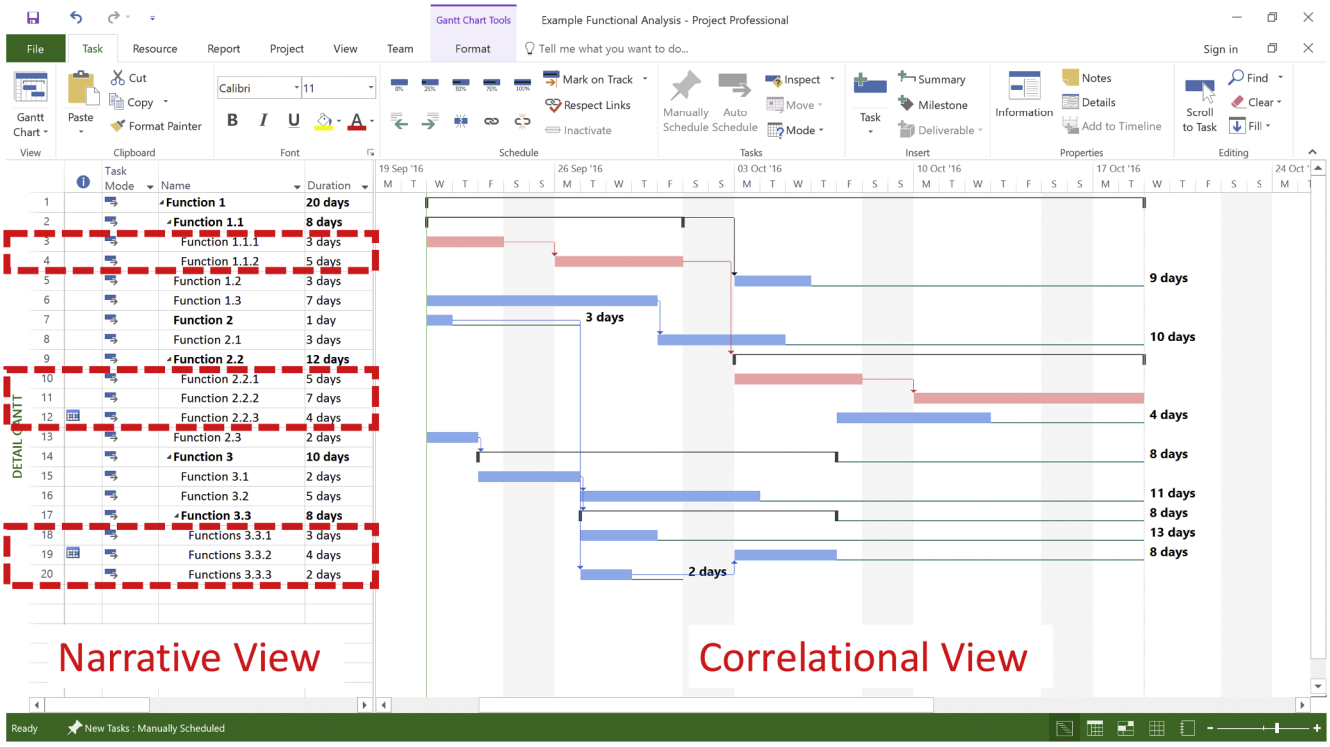

Fig. 3. Granularity check for level 3 of indentation.

and Communication Technologies-based (ICT) solutions.

In the context of the HoRAM method, the C3D is fundamental to comprehend, amongst the human functions involved, who is doing what, namely: who is commanding whom/what, who is controlling whom/what, who is supposed to communicate with whom/what, and, finally, whom and how many persons are covering each needed system function. It is worth noting that the word "command" is to be meant not in the "military sense" of ordering but, rather, in a "civil sense" of co-ordinating, instructing or guiding and, in any case, reflecting the different decisional power (and, most of all, the associated responsibility) of a subject in making a decision.

Figs. 4, 5 and 6 show an example of the Command, Control and Communication scheme respectively for emergency response within an airport (colours represent the different macro functions involved).

2.1.3. *The Task Analysis (TA) schematisation*

In Human Factors Engineering (HFE) the Task Analysis (TA) is a known and widely used tool by human factors practitioners since years (Rasmussen et al., 1994; Grandjean and Kroemer, 1997; Annett and Stanton, 2000, Shepherd, 2001).

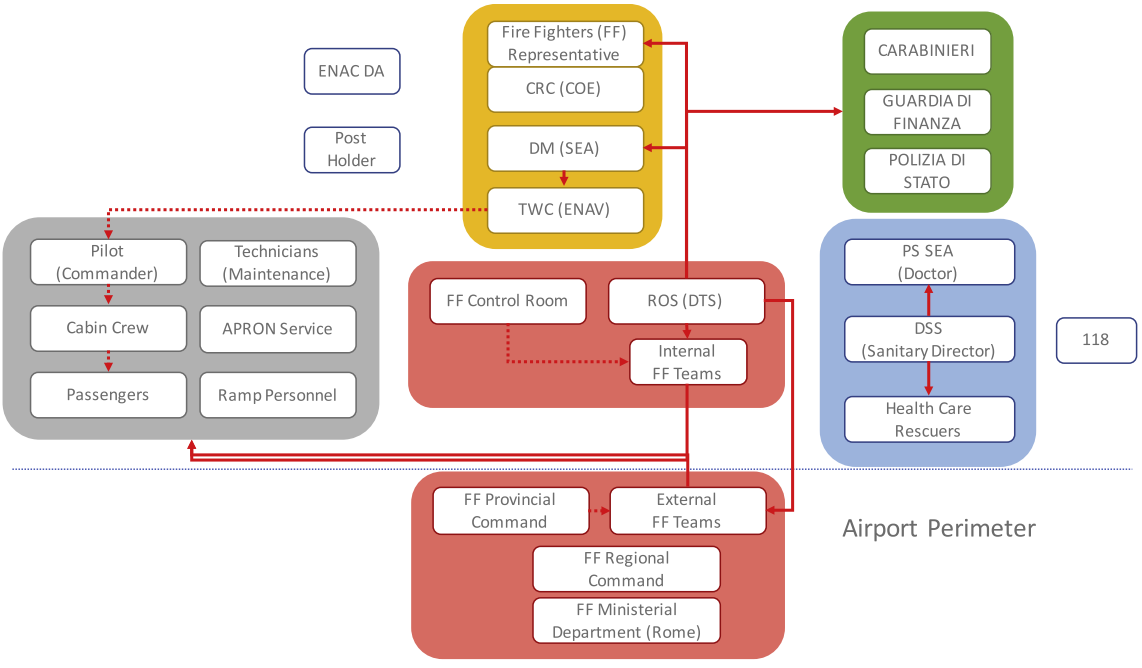

Fig. 4. Example of the "Command" schematisation.

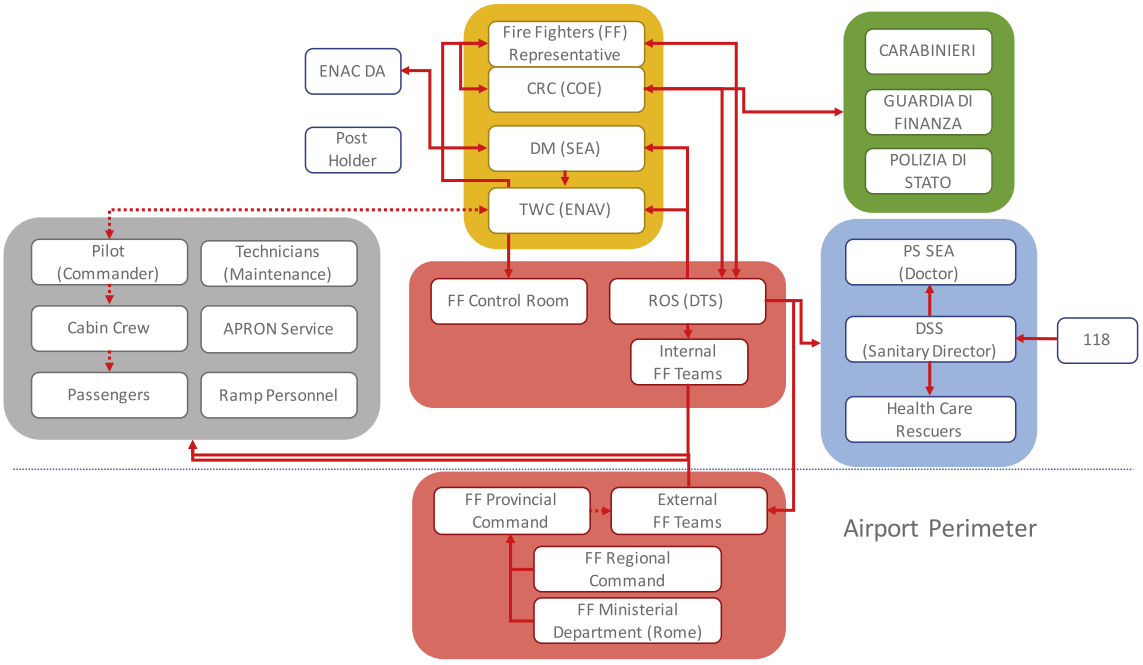

Fig. 5. Example of the "Control" schematisation.

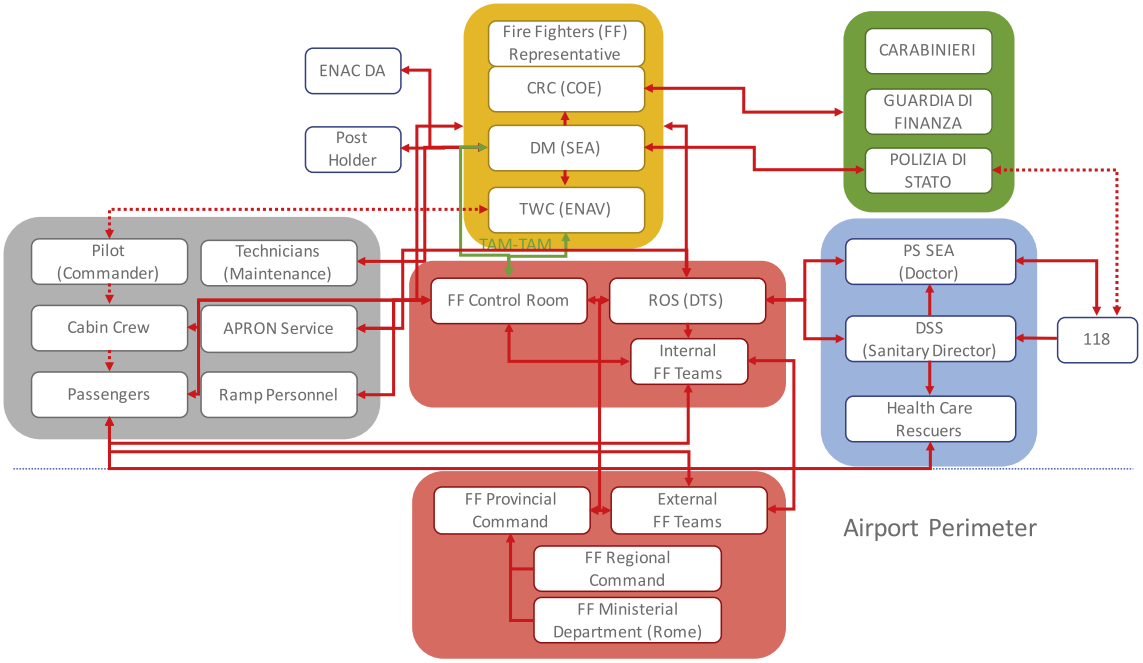

Fig. 6. Example of the "Communication" schematisation.

In the context of the HoRAM methodology, amongst the many declinations available, the Hierarchical Task Analysis (HTA) is preferred as it better couples, should it need to be performed, with the Decision Action Diagram schematisation that might follow. Overall, the HTA is meant to producing a comprehensive description of the tasks involved in a hierarchical structure of goals (and sub-goals), actions and plans (Shepherd, 2001). In the HTA process, tasks are broken down into progressively smaller units. Fig. 7 shows an example, reported in the Shepherd's book, referring to the activity of a distillation train start-up process.

The TA is extremely useful when it is necessary to clarify the activities, both manual and cognitive ones, an operator is expected to perform in the analysed context. The TA induces the analyst to put him/herself in the shoes of the operator(s) and look at the system/phenomenon from their perspective. It then helps to better understand whether, at the chosen level of abstraction, there might be relevant (human) variables to account for, thus making the analysis more reliable and reflecting the complexity of the system/phenomenon being analysed.

2.1.4. The Decision Action Diagram (DAD) schematisation

Should the functional and/or the task analysis cast any decisional shadow, the Decision Action Diagram (DAD) ought to help clarifying it. The DAD is particularly useful for representing decisions that would otherwise involve cumbersome planning in an HTA format.

The DAD is especially useful in diagnoses and control activities as it

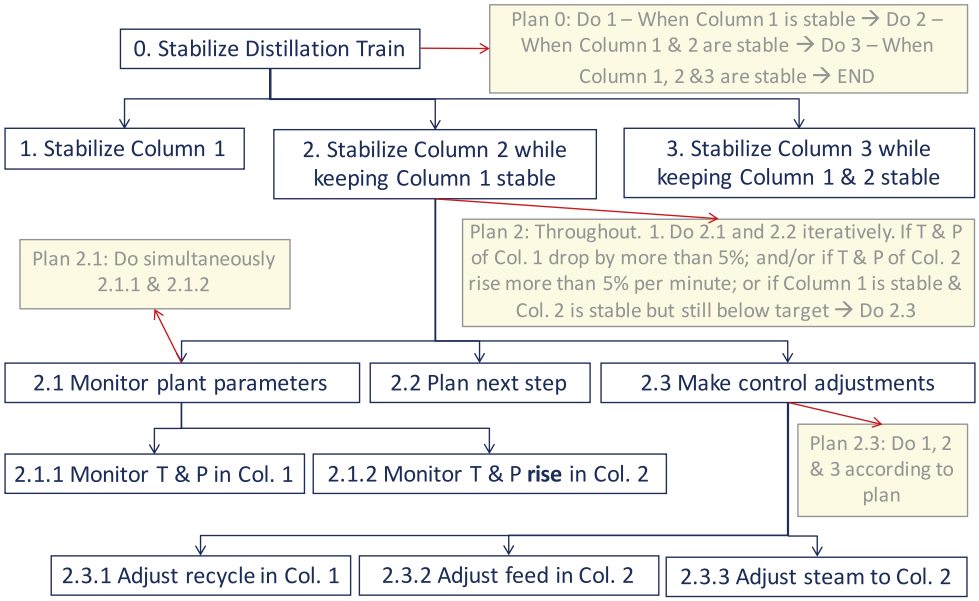

Fig. 7. Example of the HTA for the start-up of a distillation train. from Shepherd (2001).

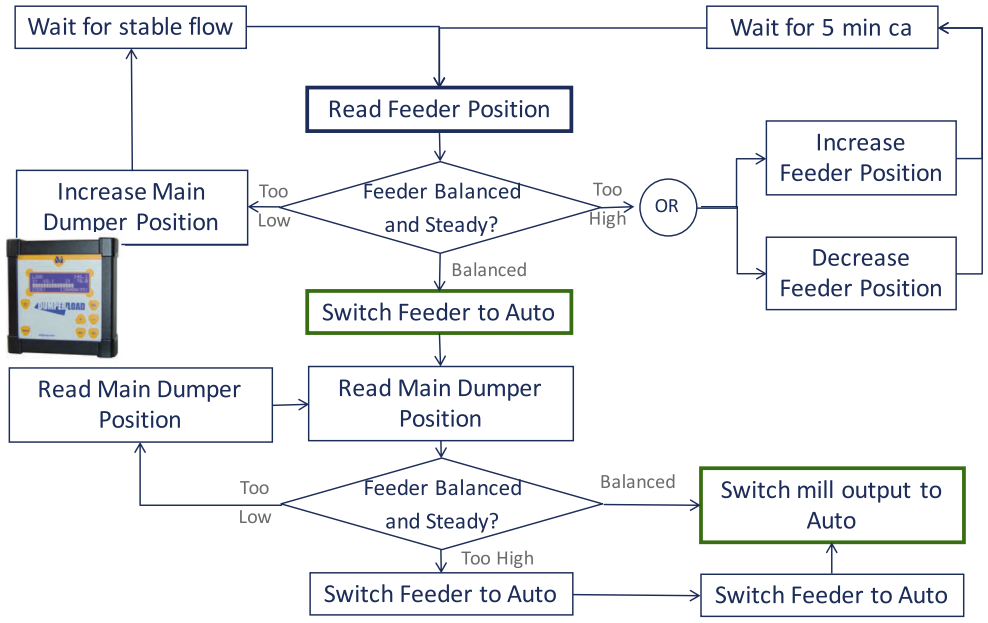

Fig. 8. Example of the DAD for the stabilisation of a mill feeder.

helps highlighting the decisional points where the operator(s) would review their diagnoses and, hence, potentially mistaking. From a different perspective, while the FA's main driving force is on the system's process and that of the TA is on the human tasks composing the process, that of the DAD is on the decisions preceding and/or following the actions. Analogously for the aforementioned analyses, even the DAD is all but new (Stanton et al., 2005). Born in the Human Factors domain, contrary to the aforementioned other methods, is less diffused and applied. Fig. 8 shows an example of a DAD diagram.

Typically, the DAD might be seen as a detailing of the TA and, as such, ought to be performed after the TA. Yet, this is more a personal choice (of the analyst) than a methodological requirement. It might actually happen that the TA is not performed (as the activities where sufficiently covered by the functional analysis) but a DAD is deemed necessary to better clarifying some decisional problems only. This is typically the case of tasks which are manually simple but cognitively intensive and demanding. A typical situation of this kind is represented by control room operators (e.g., air traffic controllers, power plants operators…), which manual actions are extremely limited (e.g., clicking the button of a mouse or a key of a console and/or communicating with a colleague) but the associated cognitive implications are extremely demanding and full of decisional points.

2.2. The link between phase 1 (system/phenomenon understanding) and phase 2 (risk analysis)

Understanding how the system/phenomenon works is the first step a risk analyst ought to perform and, in the HoRAM perspective, this is achieved through (at least) the FA and C3D. Clearly, any further tool, such as a (dynamic) process simulator that helps understanding the characteristic variables and their behaviour might further help the understanding; yet this is not sufficient to enable the risk analysis process. Actually, the list of variables derived from the FA, as well as those that might be induced from the C3D and the (dynamic) simulator,

describe the system/phenomenon in a "narrative way" from the perspective of an observer that sees the system/phenomenon evolving in its nominally functioning without looking at the potential failures and the associated possible system/phenomenon reactions. On the contrary, the list of variables composing the input file of the subsequent ALBA process are derived from the perspective of an observer that looks at the nominal evolution of the system/phenomenon and wonders whether it is capable to correctly perform the designed/aimed steps, and, in case of a failure, whether it is capable to recover from the failure to reach the goal identified by the decisional problem, e.g., is the system/phenomenon capable to accomplish the goal/reach a certain state within 35 min? Typically, the two "lists of variables" significantly differ from one another as the one derived by the systemic analysis (i.e., FA and C3D), on the one hand, might contain a number of variables not necessary to reply to the decisional problem and, on the other hand, does not include the variables necessary to model the "defensive barriers" the system/phenomenon might leverage on to react to a failure. Transforming the first prompting list of functions derived from the systemic analysis into the final input file for the ALBA analysis containing all, and only, the functions strictly necessary (i.e., the elective random variables) to generate a universe that answers the decisional problem at stake, is where the real work (and value) of the analyst lies (as it reflects the problem to solve).

2.3. Phase 2 – the risk level identification

The second phase is aimed at the identification of the risk level through the ALBA process that consists of 5 steps (Colombo, 2016), namely: (1) the input file creation, (2) the semantic check, (3) the consequences definition, (4) the risk profiling, and (5) the critical functions identification. Overall, the risk level identification can start once the system/phenomenon's (nominal) functioning is made clear through the aforementioned analyses, on penalty of misrepresenting it due to built-in inconsistencies both in terms of incorrect representation and inhomogeneous granularity (deepness). Given its articulation, phase 2 will be explained through a simple, yet not trivial, (real) industrial use case.

2.3.1. A practical use case: the supplying of hydrofluoric acid through a tanker

The supplying of hydrofluoric acid through a tanker is a risky, manually performed, industrial activity. Fig. 9 should give an idea of the working environment.

The Standard Operating Procedure (SOP) can be shortly summarised by the following 14 steps:

1. Receive the track and secure it (brakes on)
2. Check that tanker's nozzle pressure valves are correctly closed
3. Remove blind flanges from the nozzles
4. Connect tanker with the plant through 2 hosepipes: 1 for N2 (inlet) and 1 for HF (outlet)
5. Check HF hosepipe tightness with pressurized N2 (sent through a bypass line)
6. Open the head vessel valve to depressurise hydrofluoric acid vessel (to be "filled in") by venting the N2 into a blow down
7. Close the head vessel valve after depressurisation of the hydrofluoric acid vessel
8. Open the head tanker valve and that of the storage vessel
9. Check the tanker is fully depressurised
10. Close the vessel's valve
11. Depressurise the tanker through the vent line
12. Close tanker's shut-off valves
13. Disconnect the hosepipes
14. Unlock the track (brakes off)

In order to perform the operation, according to the prescription of the SOP, two operators ought to be on shift. Let's now see how the input file is created.

2.3.2. The input file creation and the generation of the partition/universe

Jointly with the consequences definition, the creation of the input file represents the value of the analysis as it reflects the knowledge and the reasoning value, in terms of system/phenomenon modelling, expressed by the analyst(s). In the Artificial Logic Bayesian Algorithm (ALBA) scheme, the decisional problem to solve is to be modelled as a progressive sequence of queries related to either the "truth" or "untruth" of subsequent/correlated "random events" (the elective random variables). Each random event/variable is to be formulated in the form of a bet or, put it differently, in a way than can be easily verifiable whether the hypothetic gambler has lost or won the bet; this way each random event/variable can be considered as a "bit of information". Should a multiple random event need to be represented, it has to be "binarised". This way the description of the system/phenomenon is kept "binary", thus making easier its representation and allowing to derive the information entropy of the partition.

2.3.2.1. The elective random variables/events. At the beginning of the process the random events/variables ought to be those stemming from the systemic analysis performed in phase 1. Yet, as the analyst proceeds with the analysis (and then with the understanding of the decisional problem to solve), the list of random events/variables considered differ from those initially identified (for the reasons explained in Section 2.2). An abstract of the final input file is shown in Fig. 10 (the full file contains 62 levels, amongst which 8 are conclusions, i.e., possible outcomes – the complete file is not included for length reasons).

Each random event/variable is to be syntactically described to the

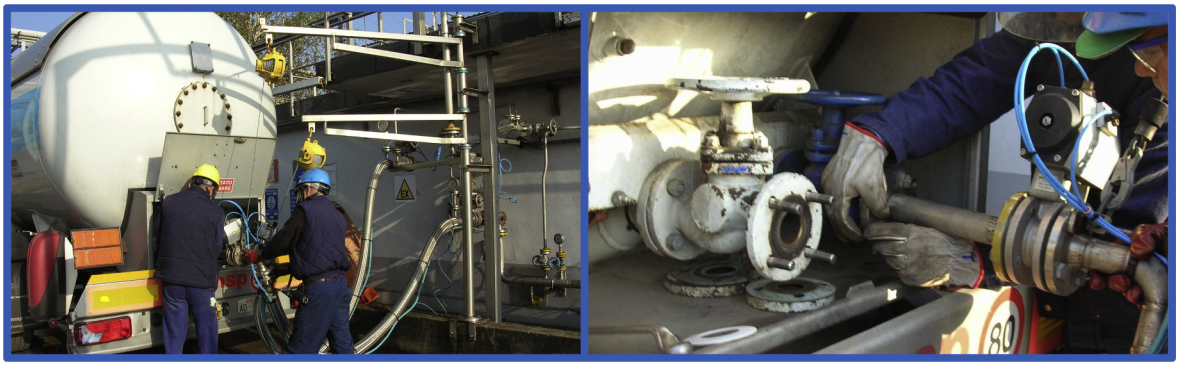

Fig. 9. Hydrofluoric supply through a tanker with details of the manual operations.

```
: Analysis start
1    0.   0.    18   0    0    'Start'   'Analysis'    '  '

: Number of efficient operators
18   3.E-2   0.5200743 20   20   3   'Nr. of Operators'   'TWO'  'ONE'
24   200   0.      0.
20   24    3.E-2   0.5200743
20   26    0.2     0.2130814
20   32    5.E-2   0.3435165
20   42    5.E-2   0.3435165
20   56    0.3     0.2130814
20   68    5.E-2   0.3435165
20   78    5.E-2   0.3435165
20   80    5.E-2   0.3435165
20   82    0.1     0.3435165

: Tanker anchoring
20   3.E-3  0.7951804   22   22   3   'Tanker'   'Anchored'   'Not Anchored'
13   48    0.      0.
13   50    0.      0.

: Tanker pressure valve status
22   1.E-2  0.7951804   24    26   2    'Tanker Pressure Valves'   'Closed'   'Opened'

: Valve linking, when correct
24   3.E-3  0.7951804   28   28    3   'Valve (When Correct)'    'Correctly Linked'  'Wrongly Linked'
24   28     0.    0.

: Valve linking, when wrong
26   1.E-2  0.7951804    28    28    3    'Valve (When Wrong)'   'Correctly Linked'   'Wrongly Linked'
24   28     0.    0.

: Correct opening of blind flanges
28   1.E-4  0.7951804    30    200    3    'Blind Flanges'   'Correctly Removed'    'Wrongly Removed'
2    300   300   220   220
20   204    1.E-3    0.7951804
20   206    0.1      0.3435165
20   210    1.E-2    0.7951804
20   212    0.5      0.2130814

: Tanker-Vessel hooking up with hosepipe
30   1.E-4  0.7951804   32     32    3    'Tanker-Vessel Hooking'   'Correct'  'Inverted'
24   50     0.      0.

: Test Hosepipe containment
32   3.E-2   0.5200743  34      34     3    'Hosepipe'   'Tight'   'Leaks'
13   42    0.    0.
24   41    0.    0.
```

Fig. 10. Abstract of the final input file of the hydrofluoric supply through a tanker.

code as a line of 9 (nine) elements, which syntax is as follows (fourth line of Fig. 10 – Appendix A explains the input file structure):

18	3.E − 2	0.5200743	20	20	3	'Nr. of Operators'	'TWO'	'ONE'

Overall, the line reads as follow: level/event/variable 18, probability 3.E − 2, CoV 0.5200743, level to go in the positive case/success ('TWO') is 20, level to go in the negative case/failure ('ONE') is 20, always print the line (in the output file), variable name 'Nr. of Operators', status in the positive case/success is 'TWO', status in the negative case/failure is 'ONE'. Each random event/variable is typically preceded by a comment line (starting with a colon), that serves as a reminder for the analyst; in case of level 18, the comment line is ": Number of efficient operators". The comment line is not mandatory and can be avoided given it is skipped by the code.

2.3.2.2. The logical constraints and the stochastic conditionings. Once the random variables have been identified, they are to be complemented, both for the negative and positive answers, by the logical constraints (if any) and/or the stochastic conditionings (if any) on the subsequent, correlated events/variables. The final input file is reached by trial and subsequent semantic corrections (till the correct phenomenological representation is reached).

In order to allow for modelling complex systems/phenomena, ALBA has 2 (two) types of logical constraints and 2 (two) types of stochastic conditionings (detailed explanation of constraints is given in Appendix B).

Conceptually, the 2 (two) logical constraints area as follows:

- address change of subsequent random events/variables (levels) in case of success or failure of the considered random event/variable (change of the logical lattice), and;
- state determination (success or failure) of subsequent random events/variables in case of success or failure of the considered random event/variable (constraints on the status of subsequent levels). For the second type of logical constraints, ALBA allows to modulate the strength amongst the low, the medium and the high values.

The identification and (correct) modelling of the logical constraints is the fundamental step that allow to transform an input file from a useless list of variables (as it typically does not allow to respond to the decisional problem at stake), into a reasoned, essential and (correctly) correlated list of variables allowing to respond to the decisional problem at stake with the minimum possible effort (i.e., the minimum number of variables and consequent minimum computational effort).

2.3.2.3. The generation of the universe. Once the input file has been written, the universe is generated through the cloud-based *KlaRisk®* platform, which is the online platform designed and built to implement the ALBA algorithm.

Provided that the syntax control gives a positive result, in order to create the universe, *KlaRisk®* requires 3 types of information, namely: the starting level (as the input file might be made up of multiple blocks

```
                    UNIVERSE SUMMARY
-------------------------------------------------------------------

Input File Name      : scolombo/TANKER.INP
Universe File Name   : scolombo/TANKER0.OUT

Starting Level       :    1

Lowest Probability   : 0.0000E+00
Highest Probability  : 1.0000E+00


     Mission Time             :

     Total Nr. of Constituents :    131196

     Cumulative Probability    :  1.00000000E+00
     Residual Probability      :  0.00000000E+00

     Partition Entropy         :  1.15133480E+00
```

Fig. 11. Simulation results of the hydrofluoric supply use case.

or phases and the analyst might want to analyse one of those at a time), the lowest and the highest probability values.

The probability values reflect the range within which the analysis is to be performed, i.e., the "perimeter" of the universe. Fig. 11 shows the outcome of the simulation performed in the *KlaRisk*® platform for the hydrofluoric supply.

As it can be read from Fig. 11, ALBA provides the analyst with all the necessary information to assess the goodness of the performed simulation and the generated universe, namely: (a) the chosen lowest and highest probability values – in the specific case 0.000E + 00 and 1.000E + 00; (b) the total number of constituents present in the generated universe (bounded by the chosen lowest and highest probability values) – in the specific case 131,196; (c) the residual probability (equal to 0. in case no cut is applied to the simulation as in the analysed use case), which is the fundamental value for the analyst to assess whether the cut be acceptable or beyond the acceptability limits – in the specific case 0.00E + 00; (d) the partition entropy, which is the second important value reflecting the amount of information needed, in terms of bits of information, to know the true constituent (i.e., the one that will manifest amongst those possible, thus transforming the prevision into a prediction) – in the specific case 1.15133480E + 00.

Despite the hydrofluoric supply use case was not at all trivial to analyse and model, it turned out to be computationally extremely light for the potentiality of the ALBA algorithm as it was possible to perform the entire simulation, from the generation of the universe down to the identification of the critical functions, within a timeframe in the order of dozens of minutes.

2.3.3. The semantic check

ALBA is an inductive method that requires the analyst(s) to create the final input file by trial and subsequent semantic corrections. To help the analyst in this crucial task, ALBA allows to perform an analysis on the generated universe to identifying the constituents of peculiar length. Fig. 12 shows the result of the analysis for the hydrofluoric acid supply use case. The analysis provides the mean length value, the inferior long and the superior short, the total number of long and short constituents, as well as the maximum deviation on the shorts and longs. The analyst can then start analysing the identified longest and shortest constituents as, typically, is where the logic inconsistencies reside and, for every inconsistency identified, the input file has to be properly adjusted to reflect the correct (or aimed) phenomenology.

The first constituent of all to analyse is the number 1 as, by methodological construct, is the one reflecting the theoretical design conditions where everything goes perfectly well (i.e., as expected/desired).

The analyst has then to verify that the first constituent is both semantically and descriptively (entirely) correct, namely: the story makes sense (there are no logical inconsistencies) and all elective random variables/events appear in their positive status. Fig. 13 shows the first constituent for the analysed use case.

A further parameter to check for the overall significance is the probability of occurrence. The first constituent tells the analyst whether s/he is stochastically on the right track or not.

The first constituent ought to be in the correct order of magnitude and, within that, in the same factor of the recorded operational experience (if any) or the design goal. In this respect, Fig. 13 says to the analyst that the probability of having everything going perfectly well is equal to 8.66E − 1, i.e. the supply of the hydrofluoric acid goes perfectly well in 86.6% of the cases. That value must reflect either the operational experience or the design target. Should that not be the case, given the logic and semantic correctness, the analyst has to revise the stochastic values of the elective variables/events, as well as those of the stochastic conditionings, till the value of the operational experience is reached (i.e., s/he has to adjust the model).

2.3.4. The consequences definition

In order to allow for decisions to be grounded on the risk and not on the probability only (as it often happens), each and every constituent is to be coupled with the consequences it generates and the risk calculated for the entire partition (and not just for the scenarios chosen on the basis of their probability of occurrence or, even worse, heuristically). Same as for the logical part, the consequences are to be defined and modelled coherently with the problem at stake, i.e., every time is a new story.

ALBA allows to define 2 (two) "families" of consequences, namely: the "magnitude assignment" and the "phenomenology modelling". The former is suited for "loosely coupled", "unstructured" systems (such as the organisational, the financial or the social systems), while the latter is more suited for "tightly coupled", "structured" systems (such as process plants where the functioning of the system/phenomenon can be, more or less easily, simulated). In principle, every HTO system could be modelled through a simulation approach. The point is the cost-benefit that might be derived from a more articulated, simulation-based approach.

In the magnitude assignment scheme, the analyst assigns, to every random variable/event generating a consequence, the weight the variable has with respect to the other random variables (typically expressed in terms of percentage value). This approach is made possible thanks to the structure of the ALBA algorithm that, by construct, produces a complete partition, whose probability value sums up to 1. Having the possibility of working with a complete partition practically means having a close world in which what counts is the relative weight, in terms of probability, that each variable has with respect to the others

```
      Max Deviation Longs = 1.039443E+01
      Max Deviation Shorts  = 2.960557E+01

MEAN    = 4.06E+01     INF. LONG  =     49     SUP. SHORT =     18

TOTAL   =   131196     LONG ones  =   9600     SHORT ones =    176

   ANALYSIS of CONSTITUENTS of PECULIAR LENGTH

   Ordinal of Long Constituents and Their Length

                    1            65013            51
                    2            65012            51
                    3            65010            51
                    :              :              :
                 9598              427            49
                 9599              424            49
                 9600              421            49

   Ordinal of Short Constituents and Their Length

                    1           131195            11
                    2           131193            11
                    3           131191            11
                    :              :              :
                  174            19185            13
                  175            19183            13
                  176            19182            13

   END of Analysis of Constituents of Peculiar Length
```

Fig. 12. Analysis of constituents of peculiar length.

and not (only) each value *per se*.

To link the logical status of each random event/variable with the phenomenological consequence it might bring to the system/phenomenon, ALBA allows to define 3 parameters, K1, K2, and K3, whose meaning is as follows: K1: level-name (generating the consequence); K2: state of the random event/variable according with the usual notation: 1 for success and 2 for failure; K3: constraint state of the event according to the following notation: 0 without constraint, 1 constrained

```
     ---------------------------
     CONSTITUENT Ordinal :      1

 18  Nr. of Operators      TWO                  +       1.-3.00E-02     9.70E-01
 20  Tanker                Anchored             +       1.-3.00E-03     9.67E-01
 24  Valve (When Correct)  Correctly Linked     +       1.-3.00E-03     9.55E-01
 28  Blind Flanges         Correctly Removed    +       1.-1.00E-04     9.54E-01
 30  Tanker-Vessel Hooking Correct              +       1.-1.00E-04     9.54E-01
 32  Hosepipe              Tight                +       1.-3.00E-02     9.26E-01
 34  N2 Pressure           Normal               +       1.-1.00E-04     9.26E-01
 39  Vessel Service Valve  Closed (N2 Normal)   +       1.-1.00E-02     9.16E-01
 40  Tanker Service Valve  Opened (N2 Normal)   +       1.-1.00E-02     9.07E-01
 42  Tightness Test        Effective            + V     1.-0.00E+00     9.07E-01
 43  Service Valve Line    Opened               +       1.-1.00E-05     9.07E-01
 44  Service Valve Pressur Sufficient           +       1.-1.00E-03     9.06E-01
 45  Tanker Service Valve  Opened               +       1.-1.00E-02     8.97E-01
 52  Hook Up Leakage       Absent               + V     1.-0.00E+00     8.97E-01
 54  HF Flow               Present              + V     1.-0.00E+00     8.97E-01
 68  Tanker Emptying       Complete             +       1.-3.00E-03     8.95E-01
 70  Vessel Service Valve  Closed               +       1.-1.00E-03     8.94E-01
 72  Venting Line          Effective            +       1.-1.00E-02     8.85E-01
 74  Air Filtering         Effective            + V     1.-0.00E+00     8.85E-01
 76  Tanker Pressure       Normal               +       1.-1.00E-02     8.76E-01
 78  Tanker Service Valve  Closed               +       1.-1.00E-03     8.75E-01
 82  Hosepipe Unlinking    Correct              +       1.-1.00E-02     8.66E-01
340  Escape                Successful           + V     1.-0.00E+00     8.66E-01

                                                PROBABILITY equal to  :  8.66E-01
```

Fig. 13. First constituent.

on success, and 2 constrained on failure;

The (simplest) syntactic structure of the magnitude scheme might be as follows:

IF (K1.EQ.28.AND.K2.EQ.2.AND.K3.EQ.0)	XDT = XDT + XC(17)
IF (K1.EQ.30.AND.K2.EQ.1)	XDT = XDT + XC(34)

where the parameter XC(x) represents the value (percentage? €uro? kg?) of the consequence generated by the random event.

The first of the aforementioned consequence lines then reads as follows: if level/event/variable 28 (i.e., K1.EQ.28) is in its negative/failure status (i.e., K2.EQ.2) and is not constrained (i.e., K3.EQ.0), then the consequence value (of level 28) is 17. The value 17 might then correspond to 17%, €17, 17 kg or whatever other unit defined by the analyst to reflect the consequences of the phenomenon considered.

On the other hand, the phenomenological modelling scheme is significantly more sophisticated: it requires the analyst to create (i.e., coding) an approximated dynamic simulation (so-called fast running) of the process being analysed[5]. In general, the phenomenological modelling is a blank page with no specific restrictions as for the type of system to simulate; the only restriction is given by the modelling and programming capability of the analyst(s).

2.3.5. The risk profiling

As Ahmed et al. (2010) highlighted, "currently available scenario management processes are cumbersome and not properly supported by available tools and technologies. They support neither the top-down approach — the breaking down of a scenario into executable and assessable component scenarios at various levels of abstraction; nor the bottom-up approach — the combining of small scenarios into the development of a high-level scenario that represents a complex set of problems".

ALBA in this respect allows the analyst to move both ways, i.e., upwards (bottom-up), by condensing the risk associated with each constituent into that of the partition, and downwards (top-down), by fragmenting into classes (technically the so-called "consequence bins") the partition's risk into a spectrum. Further, by means of a matrix selection of 10 × 10 elements, ALBA permits to extract whatever scenario, scenario sequence and scenarios set one might wish to.

The "condensation" process gives rise to the well-known Complementary Cumulative Distribution Function (CCDF) – also known as "risk curve", defined as:

$$CCDF = 1 - CDF[Bin] = \sum_{i=0}^{Bin} PDF_i$$

where the Cumulative Distribution Function (for a continuous random variable) is the one classically defined as

$$CDF = p[a < X < b] = \int_a^b f(x)dx$$

Left side of Fig. 14 represents conceptually the shape of the CCDF, while the right side represents the risk curve for the hydrofluoric acid supply use case achieved through the *Klarisx*® platform.

On the other hand, the "fragmentation" process creates the newly defined Risk Distribution Function (RDF), a novelty of the ALBA approach, which is the risk spectrum built by spreading the partition's constituents into 100 (hundred), equally sized consequence bins defined as:

$$Bin = \frac{C_{Max} - C_{Min}}{100}$$

Conceptually, the RDF describes how the risk shapes along the consequence range, thus providing the decision maker with a meso-level perspective.

Left side of Fig. 15 represents conceptually the shape of the RDF, while the right side represents the risk curve for the hydrofluoric acid supply use case achieved through the *Klarisx*® platform.

The RDF plays a fundamental role as it allows the decision maker to consciously applying the utility factor while deciding the strategy of where and how (re-)distribute the (always) scarse resources to reduce the risk: investing more on high-consequences, low-probability events or vice versa (or a mix of both)?

Methodologically, the decision maker can select one or more consequence bins (e.g., those circled in Fig. 15), and transform them into the new "universe of decision", i.e., the universe within which the decisions are made and criticalities identified.

ALBA provides also the details of each consequence bin/class, jointly with the total risk, the total probability and the (total) expected damage (extremely useful for insurance purposes). Fig. 16 shows these details. As it can be read from the bottom of the figure, the expected damage of the hydrofluoric supply is nearly 81 (precisely 8.09377E+01).

Given that the consequence values were taken as relative percentage weights, and not as absolute monetary values, and that it was chosen as 100-reference-value the death of an operator, an expected damage of nearly 81 practically means that the current system carries a potential damage of four-fifths of a death and a risk of nearly 2.5 (precisely 2.55773E+00). The analyst can then monetise this value to transform it into something much more "explicit" for the decision maker.

2.3.6. The critical functions identification

The identification of the critical functions is the final, decisive step in the risk level identification as it allows to precisely identifying where the decision maker ought to spend the resources to diminish the risk. Actually, the CCDF and the RDF are macro and meso decision-making tools allowing to "orientate" the decision but not to identifying where to concentrate the efforts. To this purpose, ALBA produces as "final step" the Critical Function List (CFL), which is the list of critical functions prioritised by contribution to the (overall) risk. Fig. 17 shows the first 4 critical functions contributing to the 80% of the total risk (precisely 8.03520E+01%).

As it can be read from Fig. 17, for each critical function, ALBA provides: its priority number, the risk associated to it, the percentage contribution to the overall risk, the cumulative risk percentage, as well as the number of constituents in which the event/variable/function is present and their range.

2.3.7. The stochastic cut

Should the analysed system/phenomenon be much more demanding in terms of computational timing of the hydrofluoric acid supply, then the analysis of the entire universe might turn out to be practically not viable as requiring months or even years to complete. In order to allow for these cases to be practically analysed and the decision-making process be supported, ALBA allows to apply a stochastic cut.

For the case at hand, should the analyst apply a stochastic cut of 1E−12, the simulation provides the results shown in Fig. 18.

The number of constituents then drops down from the original 131,196 to 15,451, i.e., nearly 12% of the entire universe. Left side of Fig. 19 shows how the residual probability trend shapes in relation to the stochastic cut. As it can be noticed, beyond a probability cut of 1E−17 the residual probability reaches a plato with a value of 1.121325E−13; it is then meaningless to proceed further with the simulation.

Computationally the difference is significant as, with a probability cut of 1E−17, the number of constituents produced is equal to 62,113, which is less than a half the complete universe/partition. The point is that the part of the universe ignored by the cut does not bring any significant additional information to the analysis (neither from a

[5] Given its length, an example of the phenomenological modelling will be presented in a subsequent paper.

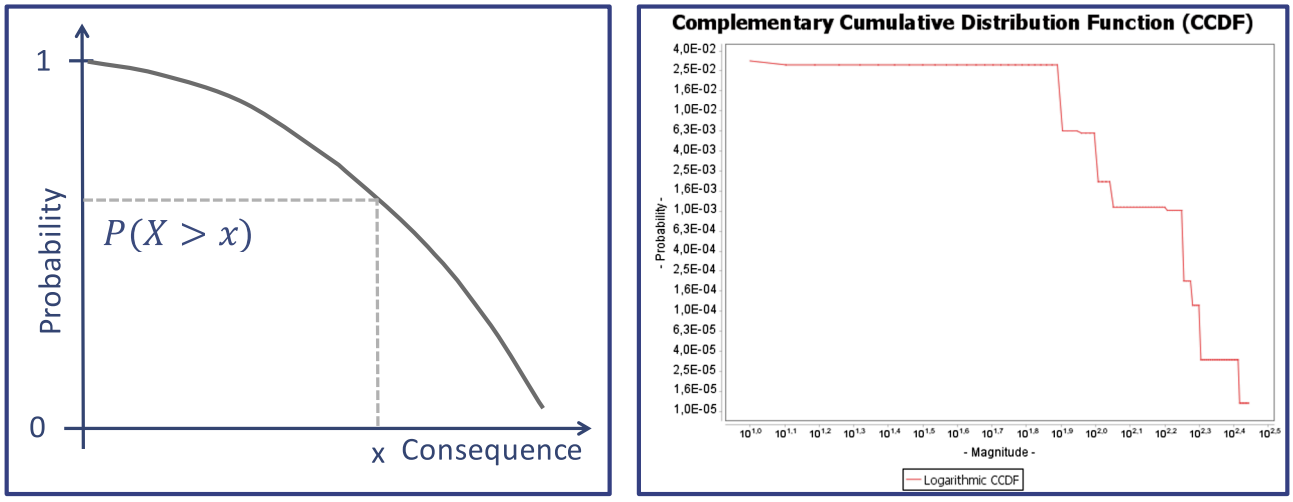

Fig. 14. Complementary Cumulative Distribution Function (CCDF) or "Risk Curve".

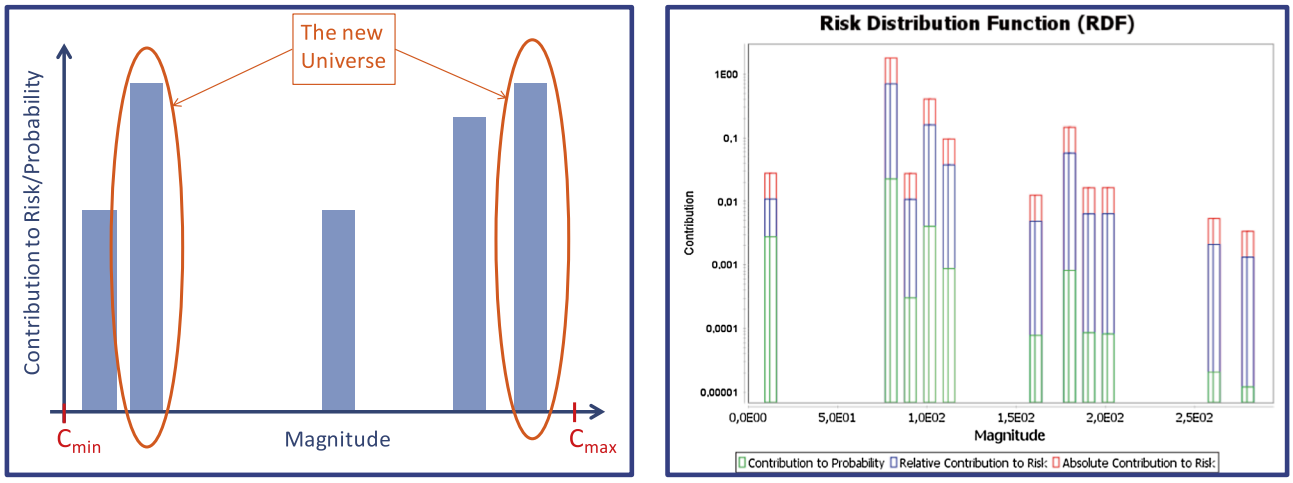

Fig. 15. Risk Distribution Function (RDF).

;Bin Nr.	Limits	Constituents	Risk	Probability	Risk Cum.%	Probability	Cumulative
1	2.800E+02	1	3.384E-03	1.209E-05	1.323E-01	1.209E-05	2.800E+02
	2.773E+02	242					
8	2.611E+02	243	5.374E-03	2.067E-05	3.424E-01	3.275E-05	2.600E+02
	2.584E+02	11518					
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
75	8.020E+01	71405	1.801E+00	2.251E-02	9.892E+01	2.883E-02	8.000E+01
	7.750E+01	129788					
100	1.270E+01	129789	2.767E-02	2.767E-03	1.000E+02	3.160E-02	1.000E+01
	1.000E+01	129820					

;	Total Probability	= 3.16013E-02
;	Total Risk	= 2.55773E+00
;	Expected Damage	= 8.09377E+01

Fig. 16. Consequence classes details, total probability, total risk and expected damage.

computational nor from a decisional standpoint). Right side of Fig. 19 shows how the number of constituents increases in relation to the probability cut.

Borel (1963), on the basis of appropriate considerations, concluded that it is reasonable to consider an event "practically impossible" in relation to the scale of analysis. At the human scale an event might be considered as "practically impossible" when it reaches a value of 1E−6 (one in a million). This is clearly a decisional value as, theoretically, from a stochastic standpoint, having a probability of occurrence of 1E−6 does not mean the event will never come true. It means that beyond that value is not practically useful, from a decisional standpoint, to consider the event.

In this regard, it is worth clarifying that, methodologically (and algorithmically), the choice of considering 1E−6 a decisional value for "practically impossible" events do not imply that the calculations are to be performed considering event with probability values higher than 1E−6 (i.e., 1E−5, 1E−4, 1E−3…).

On the contrary, should the probability values go well below the

```
          CRITICAL FUNCTION                    PRIORITY       RISK          RISK %          MIN. CUT.

  40 Tanker Service Valve  Closed (N2 Normal)      1        8.232E-01     3.21834E+01 %          1
------------------------------------------- ----
Cumulative Risk %    :  3.21834E+01 %
Nr. of Constituents :  14580
Constituents Range  : (     1 -  14580)



  45 Tanker Service Valve  Closed                  2        7.854E-01     3.07088E+01 %          2
------------------------------------------- ----
Cumulative Risk %    :  6.28921E+01 %
Nr. of Constituents :  11604
Constituents Range  : ( 14581 -  26184)



  18 Nr. of Operators      ONE                     3        2.885E-01     1.12794E+01 %          3
------------------------------------------- ----
  82 Hosepipe Unlinking    Wrong
-----------------------------------------------
Cumulative Risk %    :  7.41716E+01 %
Nr. of Constituents :    512
Constituents Range  : ( 26185 -  26696)



  44 Service Valve Pressure Insufficient           4        1.581E-01     6.18038E+00 %          8
------------------------------------------- ----
Cumulative Risk %    :  8.03520E+01 %
Nr. of Constituents :  11584
Constituents Range  : ( 26697 -  38280)
```

Fig. 17. Critical Functions List (CFL).

```
                    UNIVERSE SUMMARY
_____________________________________________________________

Input File Name      : scolombo/TANKER.INP
Universe File Name   : scolombo/TANKER12.OUT

Starting Level       :    1

Lowest Probability   : 1.0000E-12
Highest Probability  : 1.0000E+00


     Mission Time             :

     Total Nr. of Constituents :     15451

     Cumulative Probability    :  9.99999997E-01
     Residual Probability      :  2.98838210E-09

     Partition Entropy         :  1.15133476E+00
```

Fig. 18. Simulation results for the use case at hand with an applied cut of 1E−12.

decisional threshold of 1E−6 (i.e., 1E−7, 1E−8, 1E−9…) while dynamically calculating the constituents, they are to be accounted for with their value as their decisional implications cannot arbitrarily be assumed. This means that the cut is to be applied at decisional and not at computational level.

Methodologically, it is good practice deeming acceptable a probability cut that produces a universe with a residual probability ranging from 2 to 3 orders of magnitude lower than a “practically impossible” event, i.e., in the order of 1E−9. For the analysed case of the hydrofluoric acid supply, a stochastic cut of 1E−12 produces a residual probability of 2.98838210E−09, which is a robust condition.

2.3.8. The cross-check of the probability cut

Beyond the control on the residual probability it is good practice to cross-check even the effect of the cut on the risk and, more precisely, on the 3 (three) decisional tools, namely: the risk curve (i.e., CCDF), the risk spectrum (i.e., the RDF), and the critical functions list (CFL). Fig. 20 shows the effect of the probability cut for the analysed use case, where TANKER0 reflects the situation of the entire universe and TANKER12 that of the universe with a probability cut of 1E−12.

As it can be noticed, the cut has not decisional effects as the two risk curves, as well as the two risk spectrums, are, within the decisional range, identical (neither the blue line, in the risk curve, nor the blue bars, in the risk spectrum, are distinguishable from the red line, in the risk curve, and green bars, in the risk spectrum, as perfectly lying underneath them, thus demonstrating that the probability cut has not effect on the decision). Computationally the difference is significant as with a stochastic cut of 1E−12 the simulation analyses 15,451 constituents against the 131,196 constituents analysed for the entire partition. This means that the analyst can work on a universe which is

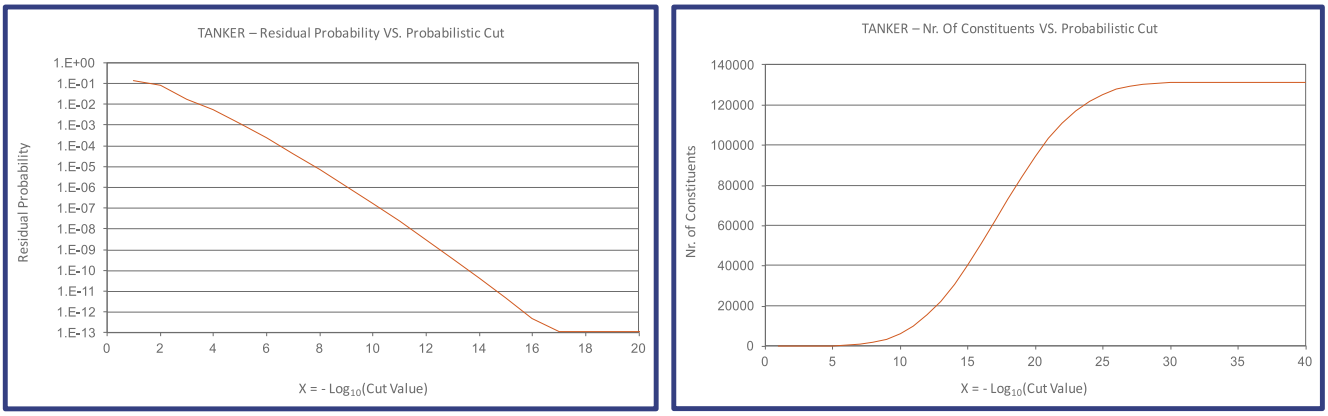

Fig. 19. Residual probability vs. Probability Cut (left) and No. of Constituents vs. Probability Cut (right).

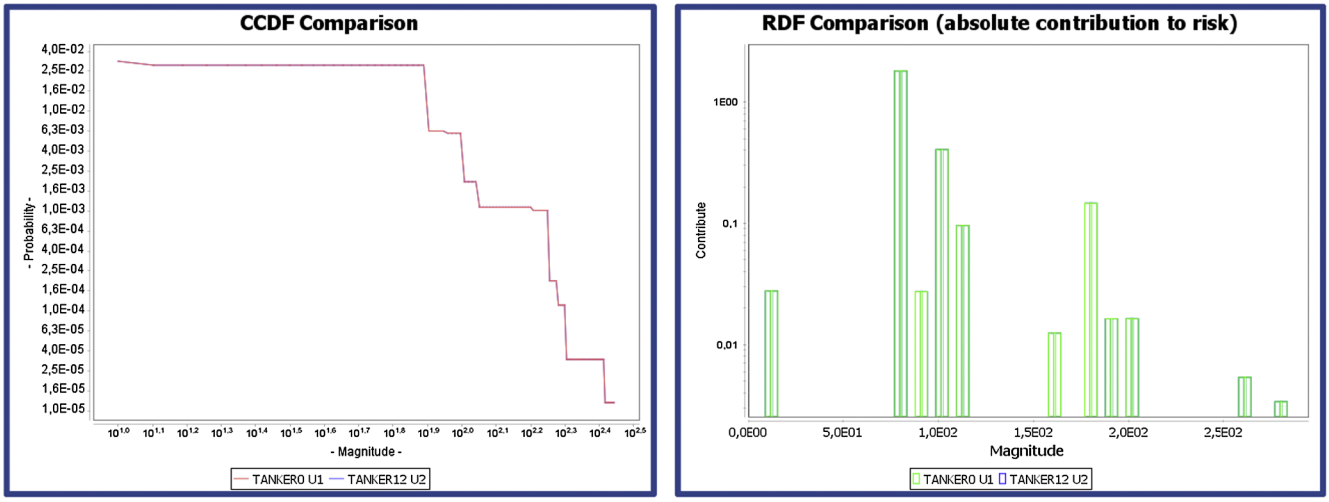

Fig. 20. CCDF (left) and RDF (right) comparison of different probability cut for the analysed use case.

nearly 12% the complete universe without losing decision-making significance. Unfortunately, not all cases are so generous. In the majority of complex cases, as in the example shown in Fig. 21 (a different case), the cut makes a not negligible difference.

The DGA001 (red line[6]) reflects the universe with a cut of 1E−8, while the DGA0011 (blue line) a universe with a cut of 1E−9. The difference is made particularly evident with the RDF as for the universe with a cut of 1E−8 (DGA001 – green bars), the highest magnitude value stops at 2.5E+2, while for that with a cut of 1E−9 (DGA001 – blue bars), the highest magnitude value stops at 2.9E+2.

Undeniably, a (nearly) 14% gap on the consequence value can make, from a decisional standpoint, a substantial difference. Yet, performing the analysis at a cut value of 1E−8 means producing a universe of 227,224 constituents with an overall computational timing (from the creation of the universe down to the identification of the critical components) in the order of 45 min, while at a cut value of 1E−9 means producing a universe of 1,132,583 constituents with an overall computational timing in the order of 8 h, i.e., more than 10 (ten) times as much the computational time required with the stronger cut 1E−8.

The potentially enormous (computational) benefits deserve to carefully select the cut to apply to optimise the simulation timing without negatively impinging the significance, from a decisional standpoint, of the results.

[6] For interpretation of color in Figs. 21–23, the reader is referred to the web version of this article.

2.4. Phase 3 – the risk treatment

According to the ISO3100 scheme, once the current risk level is identified, the risk is to be treated (i.e., modelled) in order to diminish it. With traditional approaches the risk modelling task is extremely weak as the analyst(s) either assume that the efficacy of the solution(s) be positive even at system level or assess their impact heuristically. Yet, this is a very risky approach as the complexity of today systems is sufficiently high to make the heuristic anticipation of what might be the effect of the solution(s) on the behaviour of the system/phenomenon beyond the human cognitive capabilities (Dekker, 2014). It might then happen that the envisaged solutions are not just neutral to the risk, i.e., they do not diminish it, but they even increase it, thus bearing the decision-making process in the wrong direction.

In the HoRAM perspective this condition would never occur as the goodness of the envisaged solution(s) has, methodologically, to be checked via both the well-known risk curve and the newly defined risk spectrum. Semantically, the risk curve tells the analyst(s) whether each envisaged solution increases or decreases the risk and where. The left side Fig. 22 shows a situation where the envisaged solutions (purple, yellow, green and blue lines) homogeneously diminish the risk throughout the entire consequence range. The right side of Fig. 22, instead, shows an awkward situation where the envisaged solution (red line), despite globally diminishing the risk, “locally” creates conditions where it increases (red line crosses the blue line twice and goes beyond it). The decision maker is to be made aware of the possible local behaviours the envisaged solution(s) might induce on the system/

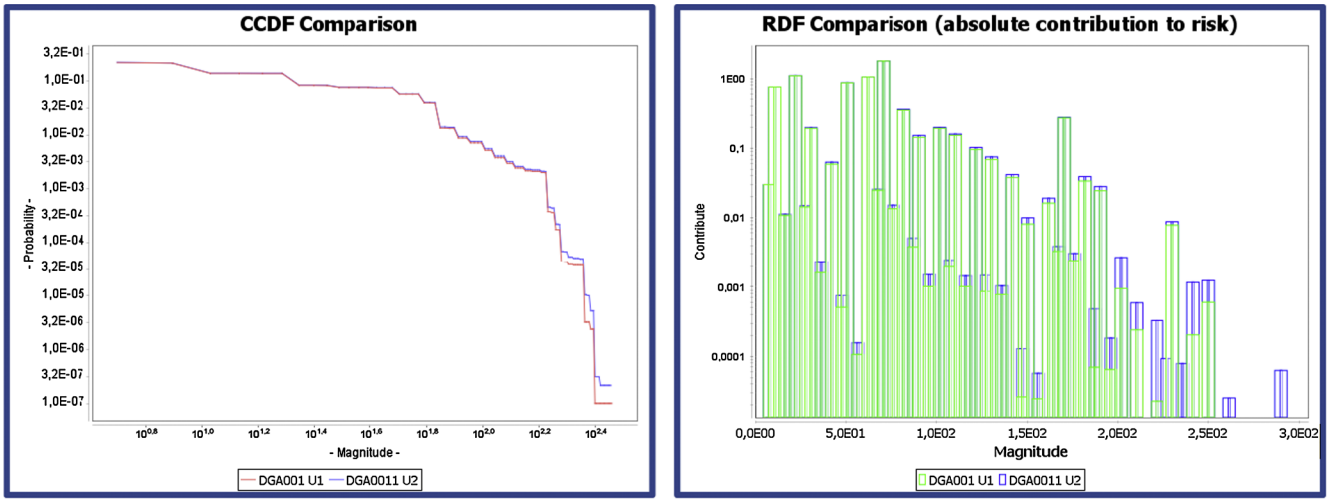

Fig. 21. CCDF and RDF comparison of different probability cut for a different use case.

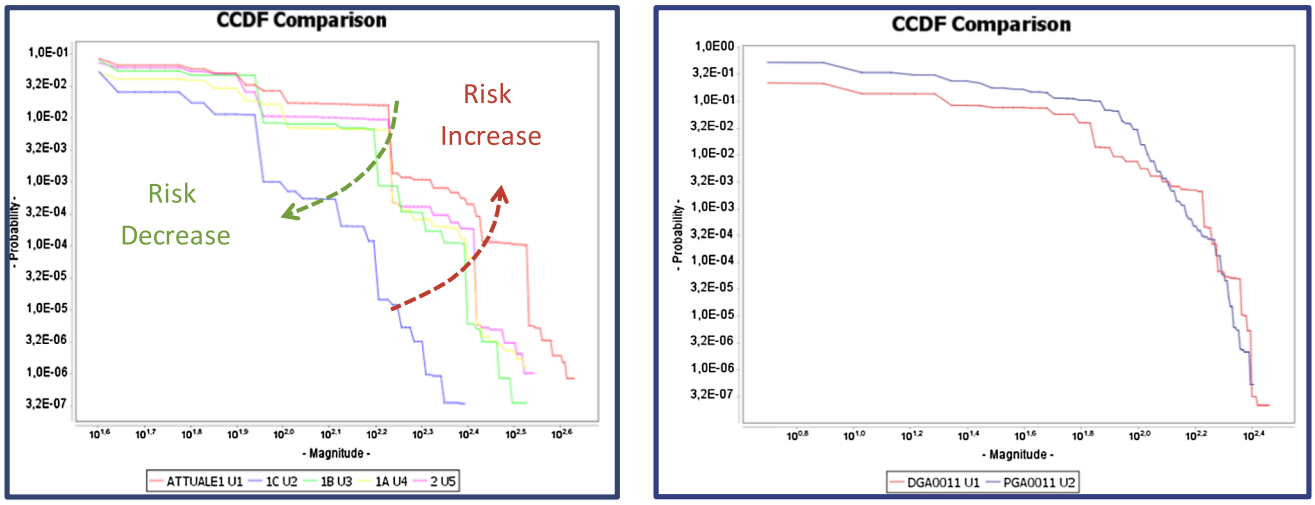

Fig. 22. Complementary Cumulative Distribution Function (CCDF) or "Risk Curve".

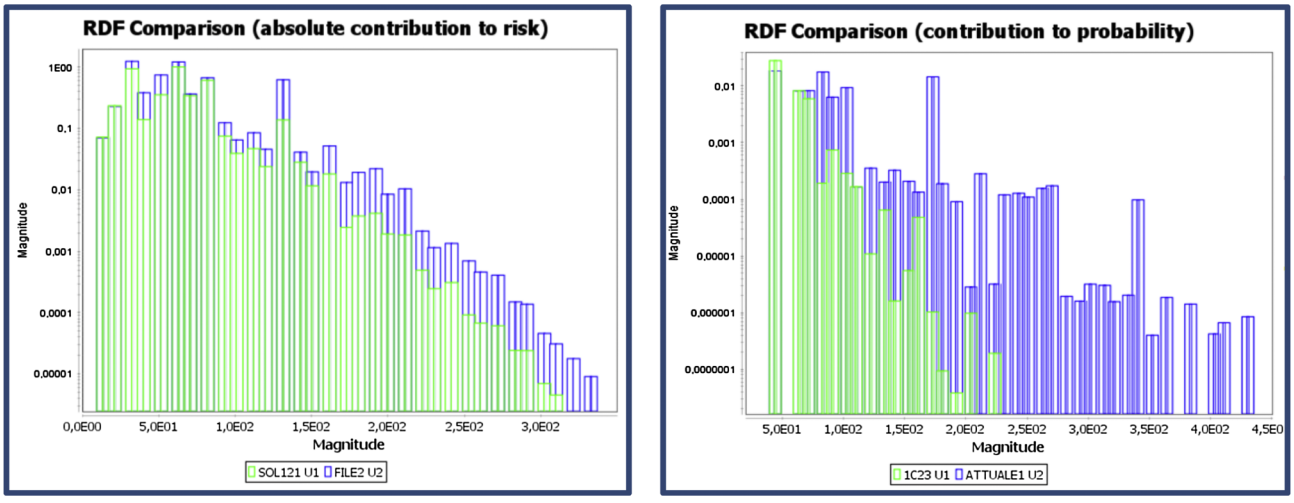

Fig. 23. Risk Distribution Function (RDF) or "Risk Spectrum".

phenomenon (along the entire consequence range) as it clearly influences her/his Utility Factor, which is function of both the probability and the consequence, i.e., UF = $f(p_i;c_i)$, and, consequently, the final decision.

On the other hand, the risk spectrum semantically tells the analyst (s) whether the risk changes even its profile, how and where (the risk might reduce either by keeping the same profile or by modifying it). Left of Fig. 23 shows a situation where the risk diminishes while

substantially keeping the same profile (to be precise it is not exactly so as the last two green classes disappear), while the right of Fig. 23 shows a situation where the profile significantly changes (as the magnitude value of the highest blue classes, reflecting the current situation, is twice as much the one of the green classes).

In the HoRAM method the risk modelling is achieved through the modification of the stochastic values of the elective random variables/events and/or the modification of the logical functioning of the system/phenomenon (if practicable), i.e., the modification of the human, the technological and the organizational functions, of the input file.

Should the modifications be of minor entity, they can be achieved through the sole modification of the ALBA input file. Else, the modification of the input file is to be preceded by the modification of the FA (and the associated C3D scheme and dynamic process simulator) to verify that the envisaged modifications do not negatively impinge on the granularity and homogeneity of the variables/events being considered. Having this done, the analyst can then run the simulation and check the impact of the envisaged solution(s) by comparing the CCDF and the RDF of the current situation with that of the new situation in which the modifications are accounted for. With the HoRAM approach the risk modelling task is then made operationally agile, conceptually robust and methodologically efficient as the analyst(s), once identified the current risk level (which is the most cognitive demanding activity), can nimbly modifying the input file and then perform the simulations to quickly comparing the goodness of the envisaged solutions in terms of both their impact on the overall consequence range and their cost-effectiveness. Everything in a timeframe which is a little fraction of that needed with traditional approaches (should they be methodologically comparable, i.e., allow to achieve the same results).

3. Discussion

Adopting a risk-based (instead of an opportunity-based) approach to decision making is of paramount importance as it allows to include in the decision both the possibility of the unwanted outcomes and the effort that would be needed to make the unwanted outcomes less likely or less severe. As complexity and uncertainty increase, appealing to scenario analysis to exploring that uncertainty and making clear what might be the impact becomes essential to support decision makers. Yet, to be supportive and not potentially misleading, scenarios are to be created by adopting a holistic approach that embraces all types of functions (i.e., human, technological and organisational) and unveils all possible alternatives/scenarios the system/phenomenon might unfold into (i.e., creating a complete partition). Further, to enable a risk-based approach, each possible scenario is to be coupled with the consequences it might produce and, altogether, the scenarios are to be consolidated to give rise to the overall risk. This done, the solutions to solve the identified scenarios-related criticalities are to be tested by keeping a systemic approach, on penalty of failing to verify whether they effectively decrease the overall risk. When systems become complex following this methodological line it is all but an easy task to accomplish. The first challenge lies in the generation of the complete universe of scenarios (i.e., creation of the partition) and the identification of the associated criticalities as the complexity is too high to manage for the human mind (Dekker, 2014). In any case, should it even be theoretically and practically possible, as for the Event Tree, it becomes not viable within a practically reasonable timeframe. Appealing to complex, logical simulations becomes then a must to cope with complexity. In the specific case of the hydrofluoric acid supply presented in the article, the HoRAM method allowed to creating and analysing a complete partition of some 131,000 different scenarios in a fist of minutes, which is a practically impossible objective to achieve with whatever “paper and pencil” approach. Overall, the use of artificial logic (or logic-based artificial intelligence) has the invaluable, practical benefit of alleviating the analyst(s) from the cumbersome and highly demanding activity of manually deriving scenarios, thus letting him/her full cognitive capacity to concentrate on both the identification of the elective variables/events (and their logic and stochastic correlation) and the characterisation of the consequences associated to them. Specifically, the HoRAM method, being a “neutral”, domain independent logical simulation, has already proved to work in anticipating the risk associated with highly complex systems/phenomena. Up to the time of writing the method has been successfully applied to different sectors (e.g., health care, process industry, manufacturing, transport, ICT, critical infrastructures…) and for different purposes (e.g., optimisation of highly optimised/consolidated processes, organisational (re-)design, counterterrorism, emergency response, systems design and retrofitting, quality optimisation, supply chain management…), all subject to ongoing scientific publications.

4. Conclusions

A proper scenarios management is of paramount importance for decision makers to thoroughly understand the matter of decision and properly assign the resources to reduce the risk. Scenarios are to be manageable in the sense that the adopted method ought to allow for both their “condensation”, into a higher, synthetic structure representing the risk (complexity) at system level, and their “fragmentation”, into their constituting functions describing the scenarios at various levels of abstraction. In the HoRAM perspective, the condensation function is achieved by generating the well-known risk curve (the CCDF), while the fragmentation function through the generation of the newly defined risk spectrum (the RDF). The risk curve and the risk spectrum are meant to orientate the decision and assess the goodness of the envisaged solutions to improve the risk level. Yet, once the decision is orientated, there is still the need to identifying what are the criticalities associated with the new configuration as they become the new variables/events either to keep under control (for audit purposes), should the risk level reached be deemed sufficient and/or the available resources to reduce it further be over, or to treat further to reduce the risk level (thus restarting the HoRAM process over again – as depicted in Fig. 1).

To conclude, having the possibility to foreseeing the real value of different alternatives and model the risk accordingly, allows to transform the risk analysis activity into an opportunity to improve complex systems’ efficiency and explore alternatives considered too risky. Further, making the risk analysis a time-efficient, economically sustainable activity allows to change its use (and perception) from a tool to appeal to only when strictly needed, to a daily tool of prevision to help decision makers transforming situations perceived as too risky into manageable (and socially acceptable) opportunities to pursue. This was the design intent that prompted the creation of the HoRAM method.

Appendix A. Explanation of the input file structure

The 9 elements respectively represent: (1) the number-name of the random event/variable (an integer number → 18); (2) the probability associated to the event/variable (a real number → 3E − 2); (3) the Coefficient of Variation (a real number → 0.5200743); (4) the number-name of the subsequent event/variable (level) in case of “success” (an integer number → 20); (5) the number-name of the subsequent event/variable (level) in case of “failure” (an integer number → 20); (6) the “printing” command (an integer number from 0 to 3 → 3); (7) the name of the event/variable (a string of 21 characters → 'Nr. of Operators'); (8) the status of the event/variable in case of success/positive condition (a string of 21 characters →

'TWO'); (9) the status of the event/variable in case of failure/negative condition (a string of 21 characters → 'ONE'). Overall, ALBA can accommodate up to 999 events/variables, which is more than sufficient even to analyse extremely complex systems (given that, from a combinatory standpoint, this would imply a universe of 2^{999} constituents).

Appendix B. Explanation of the logical constraints functioning

B.1. First type of logical constraint

The syntax for the first type logical constraints consists of 5 (five) integers, namely:

2	0	10	2	3

The meaning of the 5 numbers is as follows: (1) the state of the conditioning random event imposing the change of address(es) according to the following symbolism: 1 = in case of success, 2 = in case of failure, 3 = in both cases; (2) the new success address of the conditioned level (if the address of success does not change, the new address is = 0); (3) the new failure address in case of the conditioned level (if the address of success does not change, the new address is = 0); (4) the first level whose addresses must be changed; (5) the last level whose addresses must be changed.

The aforementioned constraint then (semantically) reads as follows: in case of failure of the compelling event (number 2) under which the constraint is positioned, the failure addresses of level 2 and 3 change from whatever current value to level 10 and those of success remain unchanged (number 0).

In the input file of Fig. 11, underneath level 28 (": Correct opening of blind flanges") there is the following logical constraint:

2	300	300	220	220

The constraint then (semantically) reads as follows: in case of failure of level 28 (number 2), i.e., in case the "Blind Flanges" are "Wrongly Removed", both the success and failure addresses of level 220 are to change from whatever they are to level 300.

B.2. Second type of logical constraint

The syntax for the second type of logical constraints consists of a sequence of 2 (two) integers and 2 (two) real numbers:

24	200	0.	0.

The meaning of the 4 numbers is as follows: (1) the first integer, i.e., the 24, is to be read as a couple of integers meaning respectively: (a) the state of the conditioning random event determining the status of the conditioned level (according to the usual notation: 1 = in case of success, 2 = in case of failure), and (b) the strength of the logic constraint, according to the following notation: 1, 3, 5 for success and 2, 4, 6 for failure strengths (i.e., odds numbers for success/positive and even numbers for failure/negative); (2) the number-name of the conditioned random event; (3) the third and fourth real numbers are meaningless placeholder.

The aforementioned constraint then (semantically) reads as follows: in case of failure (the number 2 of the 24) of the level under which the constraint is positioned, then level 200 has to fail with medium strength (the number 4 of the 24).

By the SOP, the number of operators carrying out the operation must be 2 (two). However, the number of efficient operators could be 1 (one). Should that be the case, i.e., should level 18 be on "failure", level 200 must be on failure as well. In this specific case the level 200 is a "service level" used to correctly direct the "event trajectory" and accounting for the number of injured operators:

200	0.	0.	202	203	0	'Injures	to'	'2 Operators'	'1 Operator'

The logic constraint "24" (failure-failure) put under the level 18 it is then necessary to change the status of level 200 from status 1 ("2 Operators") to status 2 ("1 Operator"), i.e., change the probability of level 200 from 0. to 1., thus correctly representing the situation that, in case the operator be 1, there cannot be injuries to 2 operators.

Overall, there are 12 possible logical constraints, namely:

- *Low strength* constraints: 11, 21, 12, 22. The constraints read as follows: in case of success (if 1)/failure (if 2) of the conditioning event, the conditioned event has to be put on success (if 1)/failure (if 2);
- *Medium strength* constraints: 13, 23, 14, 24. The constraints read as follows: in case of success (if 1)/failure (if 2) of the conditioning event, the conditioned event has to be put on success (if 3)/failure (if 4);
- *High strength* constraints: 15, 25, 16, 26. The constraints read as follows: in case of success (if 1)/failure (if 2) of the conditioning event, the conditioned event has to be put on success (if 5)/failure (if 6).

B.3. First type of stochastic conditioning

The syntax for the first type of stochastic conditioning consists of a sequence of 2 (two) integers and 2 (two) real numbers:

20	24	3.E − 2	0.5200743

The meaning of the 4 numbers is as follows: (1) the state of the conditioning random event/variable according to the following notation: 10 = in case

of success, 20 = in case of failure; (2) the number-name (level) of the conditioned random event/variable; (3) the new probability value of the conditioned random event/variable; (4) the new Coefficient of Variation (CoV) of the conditioned random event/variable.

The stochastic conditioning put under the level 18 then (semantically) reads as follows: in case of failure of level 18 (i.e., the number 20 as a whole), the probability and the CoV of level 24 change to 3.E − 2 and 0. 5,200,743 respectively, thus reflecting the situation that, should the operator be 1, the probability to perform correctly the linking reduces of an order of magnitude. Under the level 18 there are 9 (nine) stochastic conditionings (indicated by the number "20"). They all serve to indicate that, should the efficient operator be 1, the accomplishment of certain tasks (those stochastically conditioned) is negatively influenced.

The aforementioned structure (of logical constraints and stochastic conditionings) provides an extremely high flexibility of modelling, thus allowing to analyse whatever complex system/phenomenon.

References

Aguilar, F.J., 1967. Scanning the Business Environment. Macmillan, New York.

Ahmed, D.M., Sundaram, D., Piramuthu, S., 2010. Knowledge-based scenario management — process and support. Decis. Supp. Syst. 49 (4), 507–520.

Andersen, S., Mostue, B.A., 2012. Risk analysis and risk management approaches applied to the petroleum industry and their applicability to IO concepts. Saf. Sci. 50 (10), 2010–2019.

Annett, J., Stanton, N.A. (Eds.), 2000. Task Analysis. CRC Press ISBN: 0748409068.

Bood, R., Postma, T., 1997. Strategic learning with scenarios. Eur. Manage. J. 15 (6), 633–647.

Borel, E., 1963. Probability and Uncertainty. Physics and Mathematics. Walker and Company Press.

Catenaccia, M., Giupponi, C., 2013. Integrated assessment of sea-level rise adaptation strategies using a Bayesian decision network approach. Environ. Modell. Software 44, 87–100.

Cole, M., 2014. Towards proactive airport security management: supporting decision making through systematic threat scenario assessment. J. Air Transp. Manage. 35, 12–18.

Colombo, S., 2016. Risk-based decision making in complex systems: the ALBA method. In: IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bali 4–7 December 2016, pp. 476–480. https://doi.org/10.1109/IEEM.2016.7797921.

Computer Systems Laboratory of the National Institute of Standards and Technology (NIST), 1993. Integration Definition for Function Modeling (IDEFØ). Federal Information Processing Standards Publications (FIPS PUBS) 183.

Connelly, E.B., Lambert, J.H., 2016. Resilience analytics in research and development with application to future aviation biofuels. Transp. Res. Rec. 2600, 39–48.

Connelly, E.B., Lambert, J.H., Thekdi, S.A., 2016. Robust investments in humanitarian logistics to support disaster resilience of sustainable community supply chains. ASCE Nat. Hazards Rev. 17 (1).

Constantinou, A.C., Fentona, N., Marsha, W., Radlinskib, L., 2016. From complex questionnaire and interviewing data to intelligent Bayesian network models for medical decision support. Artif. Intell. Med. 67, 75–93.

Dalkey, N., Helmer, O., 1963. An Experimental Application of the Delphi Method to the Use of Experts. Manage. Sci. 9, 458–467.

De Finetti, B., 1974. Theory of Probability, vol. I John Wiley & Sons, New York.

De Finetti, B., 1975. Theory of Probability, vol. II John Wiley & Sons, New York.

Domenica, N.D., Mitra, G., Valente, P., Birbilis, G., 2007. Stochastic programming and scenario generation within a simulation framework: an information systems perspective. Decis. Supp. Syst. 42 (4), 2197–2218.

Dekker, S., 2014. Safety Differently: Human Factors for a New Era. CRC Press ISBN: 1482241994.

Endsley, M.R., 1995. Towards a theory of situation awareness in dynamic-systems. Hum. Factors 37 (1), 32–64.

Frans, O., 2006. Science Strategy and War, The Strategic Theory of John Boyd. Routledge, Abingdon, UK.

Haasl, F.D., 1965. Advanced concepts in fault tree analysis. System Safety Symposium. Boeing Company, Seattle, Washington.

Hauptmanns, U., 1988. Fault tree analysis for process industries engineering risk and hazard assessment. Engineering Risk and Hazard Assessment. CRC Press Inc, Florida (US).

Huang, Y., 2015. Modeling and simulation method of the emergency response systems based on OODA. Knowl.-Based Syst. 89, 527–540. https://doi.org/10.1016/j.knosys.2015.08.020.

Kauffman, J.J., 1979. Function analysis system technique (FAST) for management applications. SAVE Proc. 147–171.

Gill, D., 1979. Hazard Analysis (HAZAN). Course Notes (of ICI Plc), University of Queensland, Australia, Queensland.

Gelman, I.A., 2010. Setting priorities for data accuracy improvements in satisficing decision making scenarios: a guiding theory. Decis. Supp. Syst. 48 (4), 613–621.

Glenn, J.C., Gordon, T.J. (Eds.), 2009. Futures Research Methodology Version 3.0. The Millennium Project.

Grandjean, E., Kroemer, K.H.E., 1997. Fitting the task to the human. A Textbook Of Occupational Ergonomics, fifth ed. CRC Press ISBN: 9781482263046.

Hamilton, M.C., Lambert, J.H., Connelly, E.B., Barker, K., 2016. Resilience analytics with disruption of preferences and lifecycle cost analysis for energy microgrids. Reliab. Eng. Syst. Saf. 150, 11–21.

Hamilton, M.C., Lambert, J.H., Keisler, J.W., Linkov, I., Holcomb, F.M., 2013. Research and development priorities for energy islanding of military and industrial installations. ASCE J. Infrastruct. Syst. 19 (3), 297–305.

International Council on Systems Engineering (INCOSE), 2015. Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, version 4.0. John Wiley and Sons, Inc, Hoboken, NJ, USA ISBN: 978-1-118-99940-0.

Karvetski, C.W., Lambert, J.H., 2012. Evaluating deep uncertainties in strategic priority-setting with an application to facility energy investments. Syst. Eng. 15 (4), 483–493.

Jaynes, E.T., 2003. Probability Theory, The logic of Science. Cambridge University Press, New York.

Lambert, J.H., Wu, Y.J., You, H., Clarens, A., Smith, B., 2013. Climate change influence on priority setting for transportation infrastructure assets. ASCE J. Infrastruct. Syst. 19 (1), 36–46.

Lambert, J.H., Karvetski, C.W., Spencer, D.K., Sotirin, B.J., Liberi, D.M., Zaghloul, H.H., Koogler, J.B., Hunter, S.L., Goran, W.D., Ditmer, R.D., Linkov, I., 2012. Prioritizing infrastructure investments in Afghanistan with multiagency stakeholders and deep uncertainty of emergent conditions. ASCE J. Infrastruct. Syst. 18 (2), 155–166.

Lawley, H.G., 1974. Operability studies and hazard analysis. Chem. Eng. Prog. 70 (6), 45–56.

Leveson, N.G., 2004. A new accident model for engineering safer systems. Saf. Sci. 42 (4), 237–270.

Leveson, N.G., 2011. Applying systems thinking to analyze and learn from events. Saf. Sci. 49 (1), 55–64.

Means, E., Patrick, R., Ospina, L., West, N., 2005. Scenario planning: a tool to manage future water utility uncertainty. J. Am. Water Works Assoc. 97 (10), 68–75.

MIL-S-38130, 1963. General Requirements for Safety Engineering of Systems and Associated Subsystems and Equipment. USAF Publication.

MIL-STD-882, 2012. System Safety. Department of Defence Standard Practice.

MIL–P–1629, 1949. Procedures for Performing a Failure Mode, Effects and Criticality Analysis. U.S. Department of Defense.

NASA, 2007. Systems Engineering Handbook. NASA/SP-2007–6105, Rev1, Washington, D.C.

Parlak, A., Lambert, J.H., Guterbock, T., Clements, J., 2012. Population behavioral scenarios influencing radiological disaster preparedness and planning. Accid. Anal. Prev. 48, 353–362.

Pearl, J., 1986. Fusion, propagation, and structuring in belief networks. Artif. Intell. 29 (3), 241–288. https://doi.org/10.1016/0004-3702(86)90072-X.

Pearl, J., 1988. Probabilistic reasoning in intelligent systems: networks of plausible inference. Representation and Reasoning Series, second printing ed. Morgan Kaufmann, San Francisco, California ISBN 0-934613-73-7.

Pearl, J., Russell, S., 2002. Bayesian networks. In: Arbib, Michael A. (Ed.), Handbook of Brain Theory and Neural Networks. Bradford Books, MIT Press, Cambridge, Massachusetts, pp. 157–160 ISBN 0-262-01197-2.

Pinna, T., Dongiovanni, D.N., Iannone, F., 2016. Functional analysis for complex systems of nuclear fusion plant. Fusion Eng. Des. 109–111 (Part A), 795–800.

Pomerol, J.-C., 2001. Scenario development and practical decision making under uncertainty. Decis. Supp. Syst. 31 (2), 197–204.

Porter, M., 1985. Competitive Advantage. Free Press, New York.

Rasmussen, J., Pejtersen, A.M., Goodstein, L.P., 1994. Cognitive Systems Engineering. Wiley-Interscience ISBN: 0471011983.

Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. Saf. Sci. 27 (2–3), 183–213.

Sadoddin, A., Letcher, R.A., Jakeman, A.J., Newham, L.T.H., 2005. A Bayesian decision network approach for assessing the ecological impacts of salinity management. Math. Comput. Simul 69 (1–2), 162–176.

Saaty, T.L., 1980. The Analytic Hierarchy Process. McGraw-Hill, New York.

Saaty, R.W., 1987. The analytic hierarchy process—what it is and how it is used. Math. Modell. 9 (3–5), 161–176.

Savage, L.J., 1954. The Foundations of Statistics. Wiley, London.

Schoemaker, P.J.H., 1993. Multiple scenario development: its conceptual and behavioural foundation. Strateg. Manage. J. 14 (3), 193–213.

Schoemaker, P.J.H., 1995. Scenario planning: a tool for strategic thinking. Sloan Manage. Rev. 36 (2), 25–40.

Schwartz, P., 1991. The Art of the Long View. Doubleday, New York.

Shepherd, A., 2001. Hierarchical Task Analysis. CRC Press ISBN: 0748408371.

Simon, H.A., 1960. The New Science of Management Decision. Harper and Row, New York.

Stanton, N.A., Salmon, P.M., Rafferty, L.A., Walker, G.H., Baber, C., Jenkins, D.P., 2005. Process charting methods. Human factors methods: a practical guide for engineering and design. Ashgate, Great Britain ISBN: 1409457540.

Svedung, I., Rasmussen, J., 2002. Graphic representation of accident scenarios: mapping system structure and the causation of accidents. Saf. Sci. 40 (5), 397–417.

Systems Management College (SMC), 2001. Systems Engineering Fundamentals. Defence

Acquisition University Press, Fort Belvoir, Virginia, 22060-5565.
Thorisson, H., Lambert, J.H., Cardenas, J.J., Linkov, I., 2017. Resilience analytics for power grid capacity expansion in a developing region. Risk Anal (in press; appeared online September 2016).
Tourki, Y., Keisler, J., Linkov, I., 2013. Scenario analysis: a review of methods and applications for engineering and environmental systems. Environ. Syst. Decis. 33 (1), 3–20.
Tucker, K., 1999. Scenario planning. Assoc. Manage. 51 (4), 71–75.
Van de Stadt, E.C., 1994. Potentials of Bayesian decision networks for planning under uncertainty. Mach. Intell. Pattern Recogn. 16, 241–253.
Van der Heijden, K., 1996. Scenarios, The Art of Strategic Conversation. Wiley, New York.
Viola, N., Corpino, S., Fioriti, M., Stesina, F., 2012. Functional analysis in systems engineering: methodology and applications. In: Cogan, Boris (Ed.), Systems Engineering—Practice and Theory. INTECH ISBN: 978-953-51-0322-6.
Wallace, C., Gantt, H.L., 1923. The Gantt Chart, A Working Tool of Management. Ronald Press, New York.
WASH-1400-MR (NUREG-75/014-MR), 1975. Reactor Safety Study – An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants. US Nuclear Regulatory Commission.
Watson, H.A., 1961. Launch Control Safety Study, Section VII, vol. 1 Bell Labs, Murray Hill, NJ.
Weick, K.E., Sutcliffe, K.M., 2001. Managing the Unexpected. University of Michigan School, Management Series: Jossey-Bass.
Weinstein, B., 2007. Scenario planning: current state of the art. Manager Update 18 (3), 1.
Wickens, C., McCarley, J., 2008. Applied Attention Theory. CRC Press, Boca Raton.
Wixson, J.R., 1999. Function Analysis and Decomposition using Function Analysis Systems Technique (FAST). In: INCOSE International Symposium, Brighton, England, vol. 9(1). pp. 800–805. https://doi.org/10.1002/j.2334-5837.1999.tb00241.x.
Woudenberg, F., 1991. An evaluation of Delphi. Technol. Forecast. Soc. Chang. 40, 131–150.
Wright, A.D., 2000. Scenario planning: a continuous improvement approach to strategy. Total Qual. Manage. 11 (4–6), 433–438.
Wu, J., Zhou, R., Xu, S., Wu, Z., 2017. Probabilistic analysis of natural gas pipeline network accident based on Bayesian network. J. Loss Prev. Process Ind. 46 (1), 126–136.
You, H., Connelly, E.B., Lambert, J.H., Clarens, A.F., 2015. Climate and other scenarios disrupt priorities in several management perspectives. Springer J. Environ. Syst. Decis. 34, 540–554.
You, H., Lambert, J.H., Clarens, A.F., McFarlane, B., 2014. Quantifying the influence of climate change to priorities for infrastructure projects. IEEE Trans. Syst. Man Cybern. Syst. 44 (2), 133–145.