CHEMICAL ENGINEERING TRANSACTIONS
VOL. 90, 2022
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Aleš Bernatík, Bruno Fabiano

ISBN 978-88-95608-88-4; **ISSN** 2283-9216
DOI: 10.3303/CET2290007

Advantages of the Recursive Operability Analysis in Updating the Risk Assessment

Marco Barozzi[a], Lorenza Soffientini[b], Gianluca Zanon[b], Sara Perelli[b], Martina Silvia Scotton[a], Sabrina Copelli[a,*]

[a] University of Insubria, Department of Science and High Technology, Via Valleggio 9 – 22100, Como, Italia
[b] DEKRA Italia s.r.l., Process Safety Business Unit, Via Fratelli Gracchi 27, 20122 Cinisello Balsamo (MI), Italia
sabrina.copelli@uninsubria.it

With the introduction of new regulations and sustainable technologies, revamping and upgrading already existing chemical plants is nowadays an important element in the framework of process engineering. Such important modifications must come along in parallel improvement of process safety. In this sense, risk assessment is a tool that should be versatile and easy to update by definition. However, even the most common methods currently used for accidental scenarios identification and risk assessment estimation (such as HazOp) may prove to be very time-consuming when discussing about safety from process modifications. The availability of a reliable and easy-to-update tool for safety engineering is crucial for process industries. In this work, we compare a risk analysis on a chemical plant subject of modifications performed with two different tools: HazOp and FTA vs Recursive Operability Analysis (ROA) and FTA. Both techniques have been applied to a tank dedicated to dust mixing that was subject of process modifications. Both methods come to the same conclusions, highlighting new failures and process criticalities, associated with the introduction of flow alarms and interlocks in case of excessive depressurizing. It is shown that the Recursive Operability Analysis, with its cause-consequence structure tied with process variable interactions, is much more effective in a risk assessment update.

1. Introduction

Process safety is an element of utmost importance in chemical and manufacturing industry, with the final aim of minimizing accidents and casualties. Unfortunately, such a target is yet far to be achieved. According to a recent statistic developed by the European Commission, in 2018 only, there were 3'332 fatal accidents at work in the EU-27 during 2018, an increase of 60 deaths compared with the year before, with a strong incidence of economic activities, including process industry (EC, 2020). Reconstructing industrial accident causes is an important subject in both academic and industrial frameworks, that can help in improving risk assessment. As an example, there is the historical work of Barton and Nolan (1987) on accidents triggered by thermal runaways. Several works can be found in the current literature about accident analysis, but this is often applied to specific sectors and countries, like a recent study performed on severe industrial accidents caused by hazardous chemicals in South Korea (Jung et al., 2018). However, many accidents are often related to process modifications that were not accounted in former risk assessments. At the infamous T2 laboratories accident, the company decided to increase the productivity of the plant by 30% without re-evaluating the effectiveness of the rupture disk installed on the reactor, causing an extremely severe runaway accident in 2007 (CSB, 2009). The follow-up of a risk assessment after process modifications is something that is actually accounted for by norms and standards. As an example, the main Italian regulation about process safety, represented by D.Lgs 81/08, implies to readapt risk assessment after each plant modification. However, in real cases, too often this aspect is not carefully developed, leaving risk assessment untouched even after deep process innovations. One of the causes is the lack of time and personnel that should be dedicated to carry on such a task. Often this is due to the complexity of updating a risk assessment, which can be time and energy consuming. For this reason, it is important to develop and propose easy-to-use tools for industrial companies, that would make updating a risk assessment an easier and faster job. In this framework, the scope of this work

Paper Received: 3 December 2021; Revised: 30 March 2022; Accepted: 12 May 2022
Please cite this article as: Barozzi M., Soffientini L., Zanon G., Perelli S., Scotton M.S., Copelli S., 2022, Advantages of the Recursive Operability Analysis in Updating the Risk Assessment, Chemical Engineering Transactions, 90, 37-42 DOI:10.3303/CET2290007

is investigating the effectiveness of alternative methods in updating a risk assessment. In particular, a well-known method, namely the Hazard Operability Analysis (HazOp) (Dunjò et al., 2010) is compared to a lesser known one, the Recursive Operability Analysis (ROA) (Piccinini and Ciarambino, 1997). The HazOp is widely used worldwide in chemical companies, and it has some important defects, such as leading to a time-consuming analysis, and the method itself does not give a structured information as output, but only a list of causes related to certain process variable deviations. By the other hand, the ROA is a method originally derived from the HazOp itself but structured in such a way that results can easily be used to construct a Fault Tree (Barozzi et al., 2020). ROA has already successfully been applied to analyse chemical risk (Barozzi et al., 2021), but still has a low visibility in process safety culture. To perform a comparison between the two methods, two project works have been formed (A and B), made of 3 persons each. Both groups carried out a risk assessment on a chemical process, that is a dust mixer for a combustible industrial product. The plant was subject of process modifications aimed at increasing the automatization of emergency measures, adding new instruments and interlocks. Team A updated its risk evaluation using the HazOp, while team B used the ROA. The aim of the analysis is to generate a Fault Tree for the top events identified.

2. Methods and case study

In the following, the case study is described in detail and the implementation of HazOp and ROA is discussed. FTA was carried out by using the same database for unavailability or human error probabilities.

2.1 Case study

The method was applied to study how risk assessment is updated when process modifications are applied to a tank dedicated to the mixing of combustible dust. The main unit, called DM-101, is basically a horizontal tank, installed with a rotating blade mixer M-101, where nitrogen, a mix of combustible and inert dust are added. The main process consists in maturation overtime of the mixture at 70 °C, granted by an external water jacket. After maturation, the product is unloaded in a big-bag B-101 by opening valve HV-103 with a control room switch HS-103. Since reagents are combustible, it is required to inertize the tank before dust loading, and a continuous flow of nitrogen is granted over the process. B-101 is also intertized before unloading the product. Pre-inertization is performed by fluxing nitrogen for 10 min, manually activated and checked by an operator, which opens valves HV-102 and HV-104 to allow a correct venting of the tank. Temperature is then kept under control thanks to 4 indicators installed through DM-101, since reagents my suffer thermal decomposition. In case of emergency, if pressure rises during pre-inertization, operators may close HV-105, to prevent further pressure rise inside DM-101. If temperature or pressure rise excessively during dust loading or maturation (which can be due to either a combustion or a thermal decomposition), operators may activate an emergency cooling by opening HV-106 and HV-107 (or closing HV-101 if this happens during dust loading). In case of excessive pressure, operators may open HV-106 to inject emergency cooling water in DM-101.

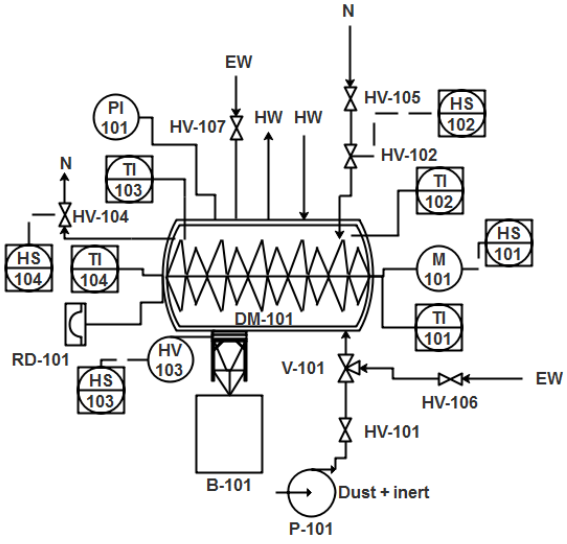

Figure 1a: P&ID diagram before modifications (HW: Hot water, EW: Emergency water, N: Nitrogen)

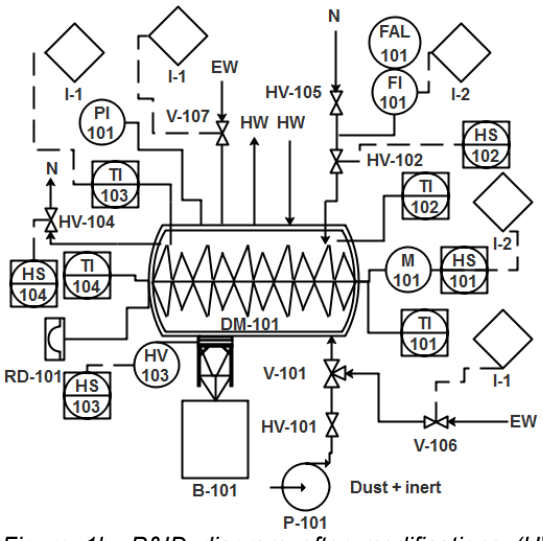

Figure 1b: P&ID diagram after modifications (HW: Hot water, EW: Emergency water, N: Nitrogen)

All the components involved are presented in Figure 1a. Since process safety is mostly left to operators, it was decided to upgrade the current process by adding a nitrogen flow indicator FI-101, which is also connected to a new interlock I-2 which stops M-101 to prevent dust lifting in case of low nitrogen flow. A low flow alarm FAL-101 was also installed as a warning for operators. An additional interlock L-1 opens V-106 and V-107 in case of high pressure or temperature, which are now automatized valves. The updated P&ID is shown in Figure 1b.

2.2 HazOp

HazOp (HAZard OPerability) is a technique for the systematic and detailed examination of a process plant (Dunjò et al., 2010). The technique is applied in accordance with IEC 61882, with the tool pf PHA Pro 8, and involves a multidisciplinary team which examines all the parts of a project or a system. Deviations from design intentions/parameters are identified using a set of guide words: in this case deviations of nitrogen flow (F), temperature (T) were analyzed in order to understand the causes and the circumstantial events leading to the explosion of a mixer. Hazard were considered not credible when they were characterized by very low frequency of occurrence or when two independent initiating events happening at the same time lead to an hazardous event (double jeopardy). Having examined the deviations by HAZOP, the analysis is carried on by estimating probabilities of occurrence throughout FTA. The trees are built in accordance with IEC 61025 using Logan Version 7.5.7 (2018) software.

2.3 ROA

The application of the ROA requires the correct compilation of records, which starts from the identification of nodes, deviations and variables (Barozzi et al., 2020), similar to HazOp. From any record, it is possible to deduce an Incidental Sequence Diagram, from which fault trees are created. The whole process can be assigned to a single node (1). Variables in account are oxygen/nitrogen concentrations (C), nitrogen flow (F), temperature (T), and pressure (P). Among these, only temperature and pressure are read from the system, so the analysis starts from deviations with respect to their setpoints. With the introduction of a flow indicator and the interlock, nitrogen flux can also be properly considered in the analysis. For what concerns deviations, high temperature (hT) is referred to mild deviations from setpoints (>10%), and it may trigger decomposition. A very high temperature (hhT) indicates a strong deviation from setpoint (>40%), and it suggests the presence of a dust fire. High pressure (hP) can be caused by either nitrogen pressurization during pre-inertization or the accumulation of gas from dust decomposition inside DM-101 during regular operation. In this case, probabilities have been estimated by solving the fault trees with OpenFTA 1.0 software (Formal software ltd.)

3. Results

Only results related to the analyses of both dust loading and maturation are reported, as they represent the most critical phases. All probabilities shown are referred to a mission time of 1 year.

3.1 HazOp

Table 1 shows the results of HazOp analysis on the system before process changes are implemented. The accidental scenario that was decided to be analyzed was the explosion of the mixer. Explosion can occur mainly for two reasons: the presence of an ignition source with oxygen in the mixer (due to incomplete inertization) and a thermal decomposition following an increase of temperature. Before the implementation of modifications on the plant, safety was mainly delegated to the operator intervention. In general, the nodes of the study were chosen in accordance with the three distinct phases of the process, i.e. vacuum pre-inertization (0), powder loading (1) and maturation (2) in a nitrogen stream and discharge in an inertized big-bag.

Table 1: HazOp before process changed (numbers in brackets are probabilities)

Node	Deviation	Cause	Consequences	Contingencies	Safeguards
1/2	No/low Flow	Human error: closing HV-102 ($5 \cdot 10^{-3}$)	No inertization in DM-101, ignition, fire	Internal ignition ($1 \cdot 10^{-2}$) Waxy product + silica inert ($1 \cdot 10^{-1}$)	Double signature operating procedure (SOP 1) ($1 \cdot 10^{-2}$)
2	High Temperature	Heat exchanger failure ($2.74 \cdot 10^{-5}$)	High T in the jacket, and in the mixer, possible decomposition	Kinetic factor (High T must persist over 3 hours) ($1 \cdot 10^{-1}$)	TI 102/103/104 alarm at DCS + operator intervention ($1 \cdot 10^{-1}$) RD 101 ($5 \cdot 10^{-4}$)

Table 2 reports instead the analysis after new protections were implemented. It is notable that safeguards improved remarkably, with the introduction of new automatic protection layers.

Table 2: HazOp after process changes (numbers in brackets are probabilities)

Node	Deviation	Cause	Consequences	Contingencies	Safeguards
1/2	No/low Flow	Human error: closing HV-102 ($5 \cdot 10^{-3}$)	No inertization in DM-101, ignition, fire	Internal ignition ($1 \cdot 10^{-2}$) Waxy product + silica inert ($1 \cdot 10^{-1}$)	Double signature operating procedure (SOP 1) ($1 \cdot 10^{-2}$) FI-101 at DCS stops the mixer ($1 \cdot 10^{-2}$)
2	High Temperature	Heat exchanger failure ($2.74 \cdot 10^{-5}$)	High T in the jacket, high T in the mixer, possible decomposition	Kinetic factor (High T must persist over 3 hours) ($1 \cdot 10^{-1}$)	TI 102/103/104 interlock at DCS opening EW valve ($1 \cdot 10^{-2}$) RD 101 ($5 \cdot 10^{-4}$)

From Tables 1 and 2, fault trees were drawn and elaborated with Logan Version 7.5.7 (2018) software. Figure 2 provides a summary of the tree developed, giving an immediate insight into the causes of failure and barriers within the two systems. Ignition was represented with the probability associated with a worn bearing.

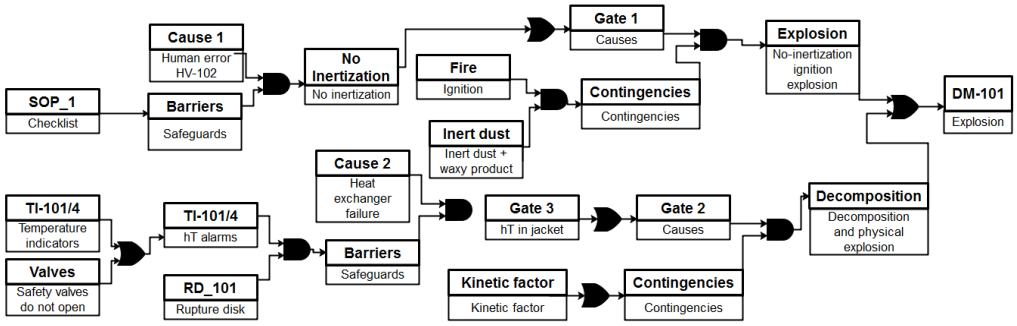

Figure 2: Fault tree from HazOp before process modifications (from Logan 7.5.7)

Figure 3 reports the fault tree for dust loading and maturation phase after process modifications are implemented.

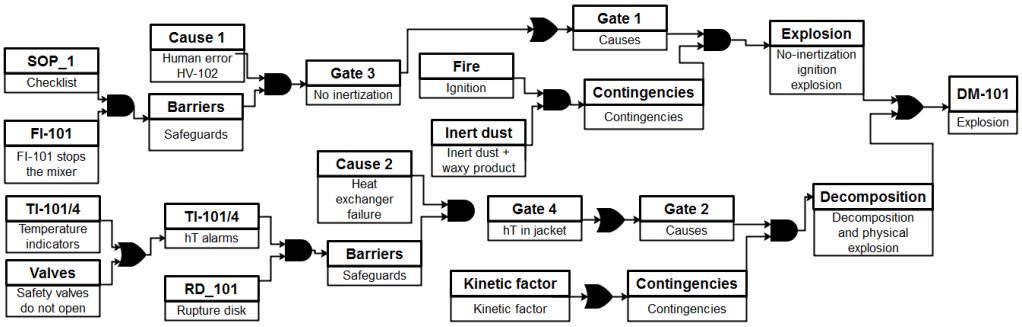

Figure 3: Fault tree from HazOp phases 1-2 after process modifications (from Logan 7.5.7)

It is worth to notice that, while trees seem very similar, automatization from new interlocks is updated through the association of barriers failure probabilities (HV-106 and HV-107 became automatized). For the first scenario, a probability of $5 \cdot 10^{-8}$ over a time mission of a year was estimated. After process modifications, such probabilities lowered to $1.25 \cdot 10^{-10}$, due to introduction of new protective barriers and new safety layers.

3.2 ROA

During dust loading and maturation, two top events are identified: a dust fire (TE2), triggered by the presence of ignition (most likely a worn mixer bearing) and oxygen, related to incomplete inertization, and a physical explosion (TE3) due to dust thermal decomposition. Table 3 reports results for the analysis before changes. It is easy to notice that process safety is highly lent to operators. Table 4 reports the analysis carried out for the updated system. Table structure instantly highlights the increase in safety due to the introduction of new barriers.

Table 3: ROA for the dust loading and maturation phase

Rec	NDV	Causes	Cons.	Plant state with protections working	Protections			Notes	TE
					Manual		Automatic safety means		
					Alarm	Operator actions			
1.1	1hC (O_2)	HV-102 OR HV-105	1hhT (in case of ignition)	-	-	Checklist	-	No control on oxygen content	
1.2	1hhT	1hC(O_2) AND Ignition	Fire	System shutdown	-	HV-106 HV-107	-	Valve unavailability ($1.84 \cdot 10^{-3}$)	TE2
1.3	1hT	hT (Hot water)	1hhP	System shutdown	-	HV-106 HV-107 HV-101		Valve unavailability ($1.84 \cdot 10^{-3}$)	
1.4	1hhP	1hT	Explosion of DM-101	System shutdown		RD-101	-	Unavailability ($5 \cdot 10^{-4}$)	TE3

From the analysis, fault trees are automatically generated by the union of the Cause-Consequence-Diagrams which can be deducted from each ROA record.

Table 4: ROA for the dust loading and maturation phase after process modifications

Rec	NDV	Causes	Cons.	Plant state with protections working	Protections			Notes	TE
					Manual		Automatic safety means		
					Alarm	Operator actions			
2.1	1hC (O_2)	1IF	1hhT	-	-	Checklist	-	-	
2.2	1IF	HV-102 OR HV-105	1hC	-	FAL-101	-	L-2 (M-101)	Valve unavailability ($1.84 \cdot 10^{-3}$)	
2.3	1hhT	1hC(O_2) AND Ignition	Fire	System shutdown	-	HV-101 ($1.84 \cdot 10^{-3}$)	L-1 (V-106 V-107)	L-1 unavailability ($2.74 \cdot 10^{-5}$)	TE2
2.4	1hT	hT (Hot water)	1hhP	System shutdown			L-1 (V-106 V-107)	L-1 unavailability ($2.74 \cdot 10^{-5}$)	
2.5	1hhP	1hhT	Explosion of DM-101	System shutdown	-		RD-101	Unavailability ($5 \cdot 10^{-4}$)	TE3

Figures 4 and 5 show the fault trees generated for the process before and after modifications have been implemented, respectively.

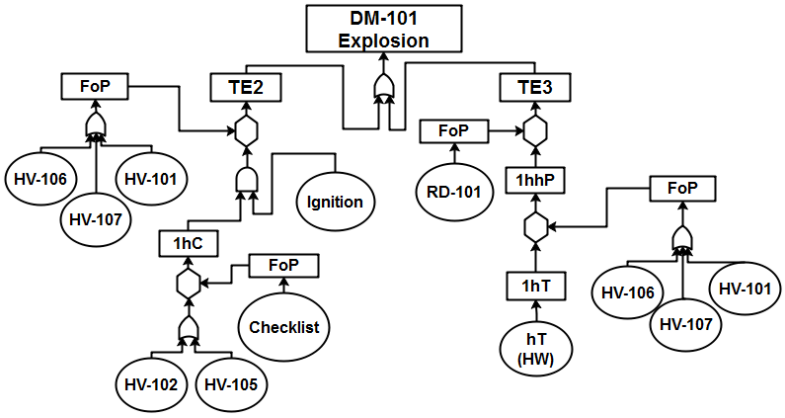

Figure 4: Fault tree from ROA before process modifications (FoP: Failure of Protections)

From the structure of fault trees, several levels of protection have been implemented.

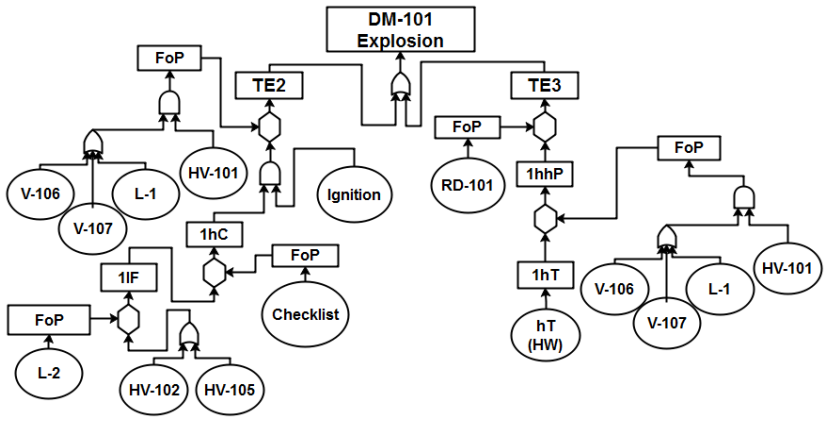

Figure 5: Fault tree from ROA after process modifications (FoP: Failure of Protections)

From numerical results, top event probability from Figure 4 is equal to $6 \cdot 10^{-9}$, and it is composed of 9 minimal cut sets (3 of 3-rd order and 6 of order 4). This result is very similar to the one proposed by HazOp, despite considering different aspects. For the second scenario, probability lowers to $1 \cdot 10^{-13}$, and minimal cut sets are increased of one order, highlighting the addition of new safety levels.

4. Conclusions

HazOp and ROA both proved effective methods to update a risk assessment following important process modifications. Accidental scenarios are very similar, despite accounting for different factors. Indeed, probabilities from ROA are lower compared to results from HazOp, and this can be due to considering in a different way how protections are connected. HazOp highlights some aspect, such as the presence of contingencies which can affect the accidental scenario. ROA advantages are the automatic construction of fault trees, which highly optimizes the analysis execution, making it a faster method.

References

Barozzi, M., Contini, S., Raboni, M., Torretta, V., Casson Moreno, V., Copelli, S.,2021, Integration of Recursive Operability Analysis, FMECA and FTA for the Quantitative Risk Assessment in biogas plants: Role of procedural errors and components failures, Journal of Loss Prevention in the Process Industries, 71,104468

Barozzi, M., Copelli, S., Scotton, M.S., Torretta, V., 2020, Application of an enhanced version of recursive operability analysis for combustible dusts risk assessment, International Journal of Environmental Research and Public Health, 17 (9), 3078

Chemical Safety Board, Investigation Report, T2 Laboratories Inc. Runaway reaction, 2009 <csb.gov/t2-laboratories-inc-reactive-chemical-explosion>, accessed 28.11.2021.

Dunjó J., Fthenakis V., Vílchez J. A., Arnaldos J., 2010, Hazard and operability (HAZOP) analysis. A literature review, Journal of Hazardous Materials, 173 (1–3), 19-32.

European Commission, Accident at Work Statistics, <ec.europa.eu/eurostat/statistics-explained/index.php?title=Accidents_at_work_statistics>, accessed 28.11.2021.

Jung S., Woo J., Kang C., 2020, Analysis of severe industrial accidents caused by hazardous chemicals in South Korea from January 2008 to June 2018, Safety Science, 124, 104580.

Nolan P. F., Barton J. A., Some lessons from thermal-runaway incidents, 1987, Journal of Hazardous Materials, 14(2), 233-239.

Piccinini N., Ciarambino I., 1997, Operability analysis devoted to the development of logic trees, Reliability Engineering & System Safety, 55 (3), 227-241.