CHEMICAL ENGINEERING TRANSACTIONS

VOL. 99, 2023

A publication of AIDIC

The Italian Association
of Chemical Engineering
Online at www.cetjournal.it

Guest Editors: Sauro Pierucci, Flavio Manenti
Copyright © 2023, AIDIC Servizi S.r.l.
ISBN 978-88-95608-98-3; **ISSN** 2283-9216

DOI: 10.3303/CET2399024

ALBATROS III: an Integrated Software to Obtain the Fault Tree, SIL Level and MCS from the Hazop

Fausto Zenier*, Franco Antonello

ARTES Analisi Rischi e Tecnologie di Ecologia e Sicurezza, Mirano, Italy
fausto.zenier@artes-srl.org

In the field of risk analysis regarding major accidents, the most commonly adopted techniques of analysis and evaluation are HazOp and Fault Tree Analysis (FTA), which have many application software and available established procedures to support risk analysts.Albatros III, developed on the basis of the experience gained with the previous software (Antonello et al. 2009, ref. [1]), aims to minimize wasted time by processing Fault Trees and Minimal Cut Sets (MCS) on the basis of the Hazop application.Basing the construction of the fault tree on the Hazop analysis also allows a more accurate and complete evaluation of the results.Fault trees are automatically obtained in graphical form and quantified. The MCS are also processed and displayed both by breaking down into categories associated with the different types of instrumentation, and by indicating the equations that compose them, with the level and incidence of the individual items. In this way it is also easy to obtain the SIL.A database containing reliability datasets is linked to the AlbatrosIII software, allowing the choice of individual data for the automatic calculation of the expected failure frequency or PFD of the system.

1. Introduction

Systems reliability and human errors are key elements in risk analysis. Many methods are available for their evaluation and there are also various software for calculating the expected frequency or probability of failure.
AlbatrosIII is the only software that implements the integration between HazOp and Fault Tree Analysis ensuring time saving and also allowing the development of Minimal Cut Sets (MCS).
This integration was conceptually presented back in the 80s (Lihou D.A. 1980, ref. [2]-[3]), but was developed with dedicated software only about ten years later and subsequently refined, also on the basis of further studies (Piccinini et al. 2002, ref. [4]), until the release of AlbatrosIII software. AlbatrosIII uses worksheets (MS Excel® type) for HazOp writing and Fault Trees with MCS development and reporting.The application of the HazOp methodology is done according to classical criteria, but using unique codes associated with elementary (primary) events descriptors.
The software allows the choice of predefined guide words for the hazop, which can also be integrated by the user, with the opportunity to further qualify the deviation, for example, specifying "+ FLOW feed" or "– FLOW water" etc. or "≠COMPOSITION +air" or "≠COMPOSITION -water", so as to describe the event as accurately as possible. The software includes a database with over 1700 cards containing reliability data taken from international databases related to mechanical, instrumental, electronic, electronic programmable, or human errors which may be automatically associated to the single primary event on the basis of a user choice, or which can be used by the experts as an aid in the choice of failure rate or error probability.
The representation of a typical HazOp worksheet is shown in Figure 1.

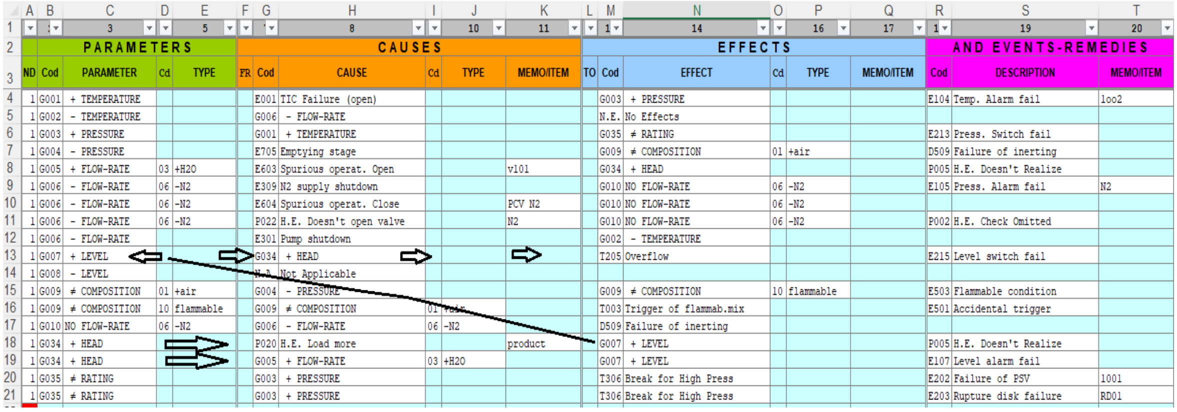
2. Application criteria

To ensure proper operation the software requires the application of some conventions, in order to limit users discretion. The main ones are:

- the use of mandatory parameters (temperature, pressure, flow rate, level, composition),
- the use of abbreviations to indicate the type of failure or event (e.g. H.E. = Human Error, etc.) with a series of predefined terms which can anyway be customized by the user,

Paper Received: 31 January 2023; Revised: 20 March 2023; Accepted: 24 April 2023
Please cite this article as: Zenier F., Antonello F., 2023, Albatros Iii: an Integrated Software to Obtain the Fault Tree, Sil Level and MCS from the Hazop, Chemical Engineering Transactions, 99, 139-144 DOI:10.3303/CET2399024

- the causes must correspond to elementary events, i.e. failures, anomalies, human errors, ..., which can be associated to an expected frequency,
- each event must be associated with the code reported in the P&I in order to obtain the list of critical components and allow MCS equations development,
- for each identified cause an effect or consequence is identified, which may consist of a deviation of another parameter in the same node or in another node, or an ultimate consequence (Top Event),
- the guide words can be used to describe a sequence of effects, each of which will become cause of a further effect, as exemplified in Figure 1



	PARAMETERS				CAUSES						EFFECTS						AND EVENTS-REMEDIES		
ND	Cod	PARAMETER	Cd	TYPE	FR	Cod	CAUSE	Cd	TYPE	MEMO/ITEM	TO	Cod	EFFECT	Cd	TYPE	MEMO/ITEM	Cod	DESCRIPTION	MEMO/ITEM
1	G001	+ TEMPERATURE				E001	TIC Failure (open)					G003	+ PRESSURE				E104	Temp. Alarm fail	1oo2
1	G002	- TEMPERATURE				G006	- FLOW-RATE					N.E.	No Effects						
1	G003	+ PRESSURE				G001	+ TEMPERATURE					G035	≠ RATING				E213	Press. Switch fail	
1	G004	- PRESSURE				E705	Emptying stage					G009	≠ COMPOSITION	01	+air		D509	Failure of inerting	
1	G005	+ FLOW-RATE	03	+H20		E603	Spurious operat. Open			v101		G034	+ HEAD				P005	H.E. Doesn't Realize	
1	G006	- FLOW-RATE	06	-N2		E309	N2 supply shutdown					G010	NO FLOW-RATE	06	-N2		E105	Press. Alarm fail	N2
1	G006	- FLOW-RATE	06	-N2		E604	Spurious operat. Close			PCV N2		G010	NO FLOW-RATE	06	-N2				
1	G006	- FLOW-RATE	06	-N2		P022	H.E. Doesn't open valve			N2		G010	NO FLOW-RATE	06	-N2		P002	H.E. Check Omitted	
1	G006	- FLOW-RATE				E301	Pump shutdown					G002	- TEMPERATURE						
1	G007	+ LEVEL				G034	+ HEAD					T205	Overflow				E215	Level switch fail	
1	G008	- LEVEL				N.A.	Not Applicable												
1	G009	≠ COMPOSITION	01	+air		G004	- PRESSURE					G009	≠ COMPOSITION	10	flammable		E503	Flammable condition	
1	G009	≠ COMPOSITION	10	flammable		G009	≠ COMPOSITION	01	+air			T003	Trigger of flammab.mix				E501	Accidental trigger	
1	G010	NO FLOW-RATE	06	-N2		G006	- FLOW-RATE	06	-N2			D509	Failure of inerting						
1	G034	+ HEAD				P020	H.E. Load more			product		G007	+ LEVEL				P005	H.E. Doesn't Realize	
1	G034	+ HEAD				G005	+ FLOW-RATE	03	+H20			G007	+ LEVEL				E107	Level alarm fail	
1	G035	≠ RATING				G003	+ PRESSURE					T306	Break for High Press				E202	Failure of PSV	1001
1	G035	≠ RATING				G003	+ PRESSURE					T306	Break for High Press				E203	Rupture disk failure	RD01

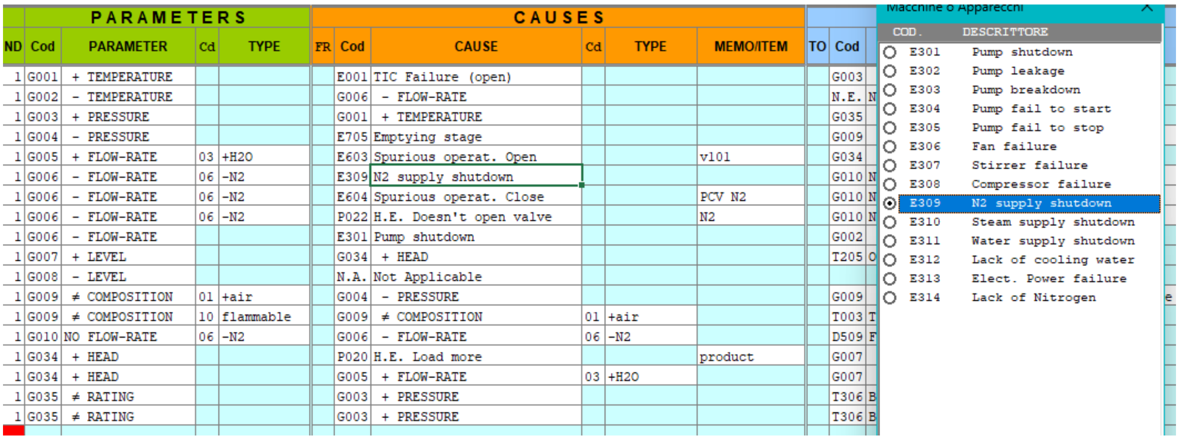
Figure 1: HazOp Worksheet

2.1 Articulation of the file containing the worksheets

The HazOp worksheet is divided into 4 sections: 1) parameters, 2) causes, 3) effects, 4) “And” events-remedies (these latter consisting of alarms or switches failure or human errors, or equipment unavailability).
All terms identifying these categories of events can be predefined by the user in an auxiliary worksheet (“Parameters”, “Initial”, “Intermediate”, “Finals”, “And”). Each category consists of 50 entries and the user can change terms or add new ones using MS Excel® rules.
The details and meaning of the abbreviations used in the worksheet are set out in the User Manual supplied with the software.

2.2 Working technique for the preparation of the HazOp worksheet

The user enters the details of the HazOp using the mouse keys (right key to open the menus as in Figure 2) taking care to report the complete sequence of events leading up to the Top Event.



	PARAMETERS				CAUSES						
ND	Cod	PARAMETER	Cd	TYPE	FR	Cod	CAUSE	Cd	TYPE	MEMO/ITEM	TO	Cod
1	G001	+ TEMPERATURE				E001	TIC Failure (open)					G003
1	G002	- TEMPERATURE				G006	- FLOW-RATE					N.E.
1	G003	+ PRESSURE				G001	+ TEMPERATURE					G035
1	G004	- PRESSURE				E705	Emptying stage					G009
1	G005	+ FLOW-RATE	03	+H20		E603	Spurious operat. Open			v101		G034
1	G006	- FLOW-RATE	06	-N2		E309	N2 supply shutdown					G010
1	G006	- FLOW-RATE	06	-N2		E604	Spurious operat. Close			PCV N2		G010
1	G006	- FLOW-RATE	06	-N2		P022	H.E. Doesn't open valve			N2		G010
1	G006	- FLOW-RATE				E301	Pump shutdown					G002
1	G007	+ LEVEL				G034	+ HEAD					T205
1	G008	- LEVEL				N.A.	Not Applicable					
1	G009	≠ COMPOSITION	01	+air		G004	- PRESSURE					G009
1	G009	≠ COMPOSITION	10	flammable		G009	≠ COMPOSITION	01	+air			T003
1	G010	NO FLOW-RATE	06	-N2		G006	- FLOW-RATE	06	-N2			D509
1	G034	+ HEAD				P020	H.E. Load more			product		G007
1	G034	+ HEAD				G005	+ FLOW-RATE	03	+H20			G007
1	G035	≠ RATING				G003	+ PRESSURE					T306
1	G035	≠ RATING				G003	+ PRESSURE					T306

Macchine o Apparecchi

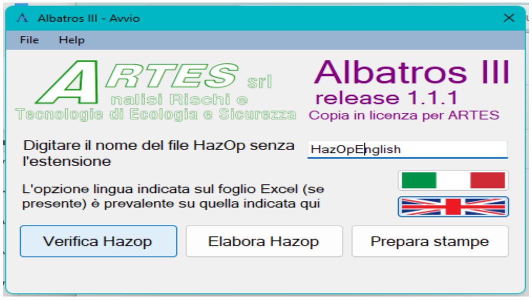
	COD.	DESCRITTORE
○	E301	Pump shutdown
○	E302	Pump leakage
○	E303	Pump breakdown
○	E304	Pump fail to start
○	E305	Pump fail to stop
○	E306	Fan failure
○	E307	Stirrer failure
○	E308	Compressor failure
●	E309	N2 supply shutdown
○	E310	Steam supply shutdown
○	E311	Water supply shutdown
○	E312	Lack of cooling water
○	E313	Elect. Power failure
○	E314	Lack of Nitrogen

Figure 2: example opening menu

It is possible to go back using the [Esc] key; the contents of the cells and rows can be copied following the rules of MS Excel® and the instruction provided with the User Manual. In the sequences of events that originate Top Events (also called final events), in addition to the causes, also the presence of safety barriers (elements or components that can prevent the occurrence of unwanted events or through which it is possible to minimize their impact) must be considered. These elements consist in alarms or switches systems or safety components such as PSV or rupture discs or also controlling measures and actions entrusted to man or computer systems. All of these safety barriers are able to timely detect the occurrence of events or failures and implement appropriate measures of prevention or protection.These elements are considered or expected as a result of the analysis and it’s possible to evaluate their unavailability and weigh the influence they may have towards the final result, that is, the expected frequency of the Top Event.

If a sequence of events affects several nodes, the columns "FR = from the node" and "TO = to the node" are used to indicate the source and destination nodes.

Once the HazOp has been edited and the file saved, AlbatrosIII is started and the preliminary checks are carried out. Indeed, one of the advantages provided by the software is the possibility of verifying the completeness and consistency of the analysis, especially in cases of complex analysis with many causes / effects sequences involving multiple nodes. The software allows to check if there are repetitions or duplications or interruptions of the sequences of events. The control is activated by clicking on the box "Verifica HazOp", as shown in the following figure.

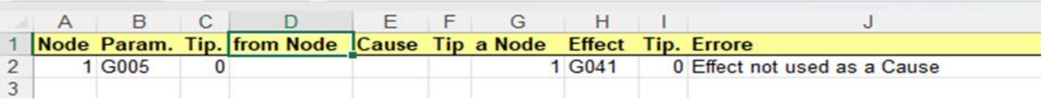


Digitare il nome del file HazOp senza l'estensione: HazOpEnglish

L'opzione lingua indicata sul foglio Excel (se presente) è prevalente su quella indicata qui

Figure 3: example of activation control

If there are errors, they are reported in the Errors sheet, as shown in the following figure



Node	Param.	Tip.	from Node	Cause	Tip	a Node	Effect	Tip.	Errore
1	G005	0				1	G041	0	Effect not used as a Cause

Figure 4: example of errors reporting

When the check is positive, one can go to process the Fault Trees using the "Processing" button.

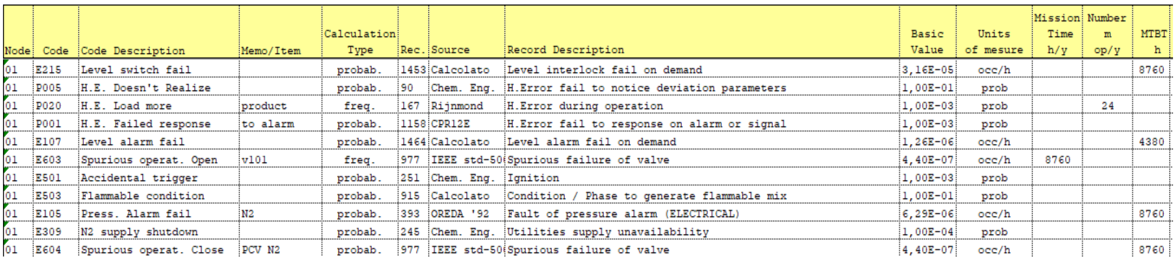
2.3 Fault Tree and Minimal Cut Set

Setting the analysis and respecting the conventions described above allows to obtain directly the Fault Trees from HazOp. It is possible to obtain only the Fault Tree graph (without any calculation) or the quantified Fault Tree graph (with the frequency/probability calculation).

To obtain the quantified fault trees it is necessary to open the database file and choose the failure rates or error probabilities for all the events involved in the accident sequence.

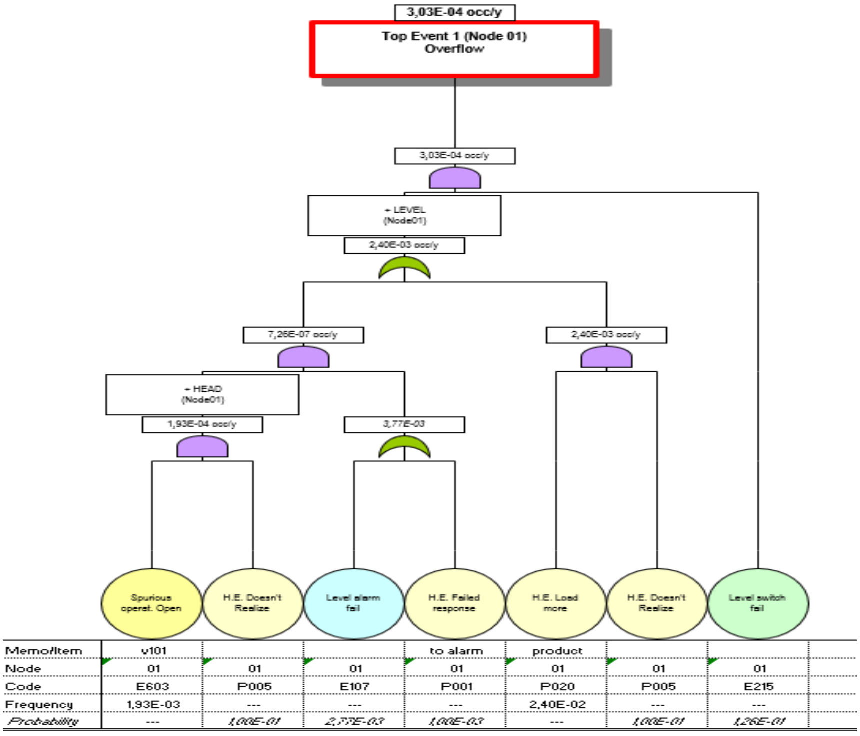
This operation is performed using the "Affidab" sheet, an example of which is shown in the Figure 5. To enter the failure rates, simply enter the card number of the database and click with the right mouse button: the program will automatically enter the average rates. You can choose between λ_D or λ_{DU}, in order to apply the appropriate reliability calculation relationships (SINTEF ref. [5] [6]). After entering the number of the selected dataset, using the right mouse button, the failure rate is loaded into the worksheet.

Once the entry of the reliability data and the other variables (mission time, MTBT, MTTR, etc) is completed, it will be possible to activate the processing of the Fault Trees. An example of the fault trees is shown in Figure 6. The MCS are visible both in detail, with highlighting of the sequences relating to the unavailability of components in stand-by, and as equations. The representation is shown in §3.2, Figures 7 and 8.



Node	Code	Code Description	Memo/Item	Calculation Type	Rec.	Source	Record Description	Basic Value	Units of mesure	Mission Time h/y	Number m op/y	MTBT h
01	E215	Level switch fail		probab.	1453	Calcolato	Level interlock fail on demand	3,16E-05	occ/h			8760
01	P005	H.E. Doesn't Realize		probab.	90	Chem. Eng.	H.Error fail to notice deviation parameters	1,00E-01	prob			
01	P020	H.E. Load more	product	freq.	167	Rijnmond	H.Error during operation	1,00E-03	prob		24	
01	P001	H.E. Failed response	to alarm	probab.	1158	CPR12E	H.Error fail to response on alarm or signal	1,00E-03	prob			
01	E107	Level alarm fail		probab.	1464	Calcolato	Level alarm fail on demand	1,26E-06	occ/h			4380
01	E603	Spurious operat. Open	v101	freq.	977	IEEE std-50	Spurious failure of valve	4,40E-07	occ/h	8760		
01	E501	Accidental trigger		probab.	251	Chem. Eng.	Ignition	1,00E-03	prob			
01	E503	Flammable condition		probab.	915	Calcolato	Condition / Phase to generate flammable mix	1,00E-01	prob			
01	E105	Press. Alarm fail	N2	probab.	393	OREDA '92	Fault of pressure alarm (ELECTRICAL)	6,29E-06	occ/h			8760
01	E309	N2 supply shutdown		probab.	245	Chem. Eng.	Utilities supply unavailability	1,00E-04	prob			
01	E604	Spurious operat. Close	PCV N2	probab.	977	IEEE std-50	Spurious failure of valve	4,40E-07	occ/h			8760

Figure 5: example of "Affidab" sheet



Memo/Item	v101			to alarm	product		
Node	01	01	01	01	01	01	01
Code	E603	P005	E107	P001	P020	P005	E215
Frequency	1,93E-03	---	---	---	2,40E-02	---	---
Probability	---	*1,00E-01*	*2,77E-03*	*1,00E-03*	---	*1,00E-01*	*1,26E-01*

Figure 6: Example of Fault Tree

3. Criteria for calculating reliability

3.1 Equations

Conceptually, the events sequence described in the HazOp can be represented by a set of equations of the following type.

$$E_{\lambda} = \sum_{i=1}^{L_{\lambda}} C_i \prod_{j=1}^{M_i} EA_{i,j} \qquad (1)$$

Where:

E_{λ} = λ-th effect

Ci = i-th cause of the λ-th effect

$EA_{i,j}$ = j-th event of the i-th cause.

Equation (1) should be read as: "the Event λ-th takes place by the L causes C_i if for each of them M_i concauses $EA_{i,j}$ occur, with an expected frequency equal to the sum of the expected frequencies of the L causes, each multiplied by the probability of the M_i contributing causes."

In other words the summations correspond to OR logic gates, while the multiplications correspond to AND logic gates.

The expression is thus both in terms of qualitative illustration and in quantitative terms of the phenomenon. Substituting the equations of the Effects into the Causes give rise to general equations of the type:

$$TE_{\mu} = \sum_{i=1}^{L\mu} EE_i \prod_{j=1}^{M_i} \left(\sum_{k=1}^{N_j} EE_{k,j} \prod_{l=1}^{O_k} EA_{l,k} \right)_{i,j} \tag{2}$$

Where EE$_i$ = i-th elementary event or C$_i$
Each term in the first sum of the equation (2), is a Minimal Cut Set (MCS), i.e. the contribution of each elementary cause to the final Top Event.
It should also be considered that the adopted HazOp drafting mode does not require a standard Boolean analysis of the Fault Tree. In fact, the elementary events (EE) appear only and always as expected frequency (unit of measure occ/year or event/year), while safety measures appear always as unavailability (unit of measure is dimensionless, i.e. probability).
The software is typically used for the estimation of frequencies derived from sequences of events, but may also represent single event resulting from a single cause such as, for example, the rupture of a pipe. Given the variability of the units of measure for the base failure rates in the various technical reference and given the multiplicity of possible situations, the convention to represent the Top Event with an annual frequency, and the unavailability as probability is assumed.
Given:
f = expected frequency [occ/y]
L = pipe length [m]
MT = Mission Time or working time in the year [h/y]
MTBT = Mean Time Between Test [h]
MTTR = Mean Time To Repair [h/occ]
N = occ/year or number of operations for each of which an error can potentially occur
P = probability [-]
PFD = probability of failure on demand [p]
λ = base failure rate [occ/h] or [occ/(h·m)]

$f = \lambda \cdot MT$ or, in case of pipes $f = \lambda \cdot MT \cdot L$ (3)

If the base failure rate is provided in probability or PFD then:

$$f = p \cdot \frac{MT}{MTTR} \tag{4}$$

For human errors frequency can be calculated considering the possibility of errors, so

$$f = p \cdot N \tag{5}$$

In case of unavailability or PFD a distinction has to be made between systems on stand-by mode and systems whose failure is autodetected (such as control loops whose failure automatically causes a deviation of controlled parameter or other parameters, or in the case of a pump stop, which results in the lack of flow).

In case of stand-by components (typically switch systems):

$PFD = \left[1 - \frac{(1-e^{-\lambda \cdot MTBT})}{\lambda \cdot MTBT}\right]$ which for λ·MTBT<0,1 approximates to $\lambda \frac{MTBT}{2}$ (6)

For events whose failure autodetects:

$$PFD = \frac{\lambda \cdot MT \cdot (MTTR + TR)}{8760} \tag{7}$$

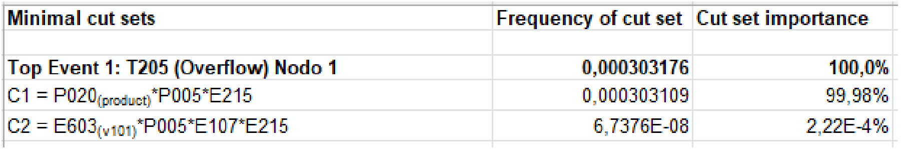
(here also time of detection TR – in hours – can be taken into consideration)
In case of redundant systems composed of identical items (no common causes of failure, to be considered separately) which failure doesn't auto detect, the calculation is performed by:

$$\mathrm{PFD} = \frac{\mathrm{n!}}{r! \cdot \mathrm{(n\text{-}r)!}} \cdot \frac{(\lambda \cdot MTBT)^r}{r+1} \tag{8}$$

Where:
m = number of components required for the operation, n = number of components existing in the system
r = n-m+1

3.2 Minimal Cut Set (MCS)

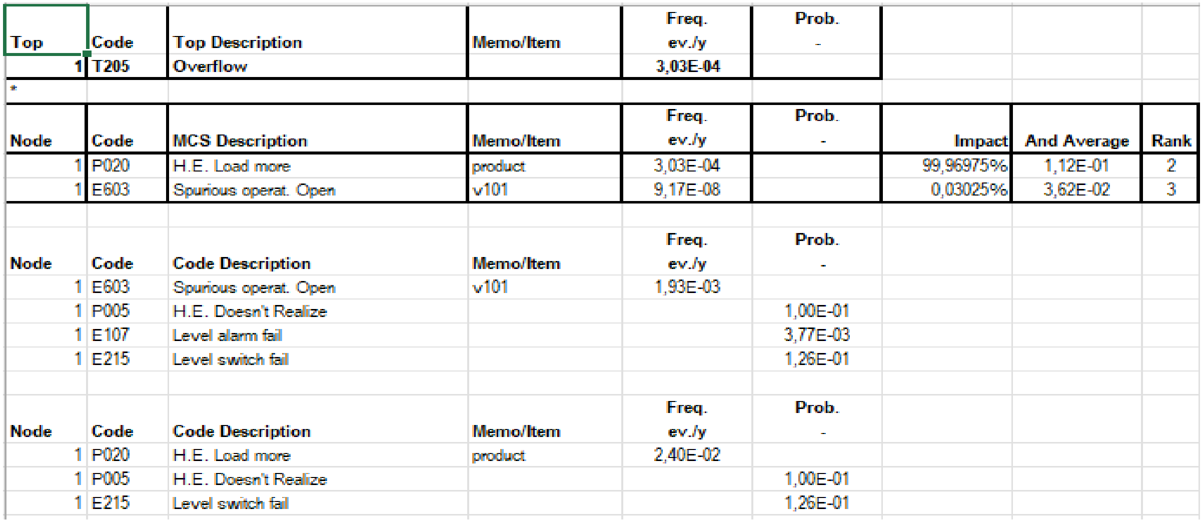
The user can choose whether to calculate the MCS as well or only the Fault Trees. AlbatrosIII allows to obtain the MCSs for each identified Top Event, by providing a summary of the causes (elementary events) with the percentage contribution of each MCS to the frequency of Top Event, as illustrated below.



Minimal cut sets	Frequency of cut set	Cut set importance
Top Event 1: T205 (Overflow) Nodo 1	**0,000303176**	**100,0%**
C1 = P020$_{(product)}$*P005*E215	0,000303109	99,98%
C2 = E603$_{(v101)}$*P005*E107*E215	6,7376E-08	2,22E-4%

Figure 7: MCS equation

It is possible to explain the contribution of each of the events that lead up to the Top Event, providing a useful tool for cost / benefit evaluation and ranking of combined events that can cause system failure.
Furthermore, in the detailed representation, AlbatrosIII supplies the average PFD of the "AND Events " (safety measures), and their number (corresponding to the number of barriers or components that must fail to cause the undesired occurrence). In this way there is also the representation of the safety level, i.e. of the barriers provided to stop the sequence of dangerous events. The example of the representation of MCS is reported in Figure 8.



Top	**Code**	**Top Description**	**Memo/Item**	**Freq.** **ev./y**	**Prob.** **-**			
1	**T205**	**Overflow**		**3,03E-04**				
*								
Node	**Code**	**MCS Description**	**Memo/Item**	**Freq.** **ev./y**	**Prob.** **-**	**Impact**	**And Average**	**Rank**
1	P020	H.E. Load more	product	3,03E-04		99,96975%	1,12E-01	2
1	E603	Spurious operat. Open	v101	9,17E-08		0,03025%	3,62E-02	3
Node	**Code**	**Code Description**	**Memo/Item**	**Freq.** **ev./y**	**Prob.** **-**			
1	E603	Spurious operat. Open	v101	1,93E-03				
1	P005	H.E. Doesn't Realize			1,00E-01			
1	E107	Level alarm fail			3,77E-03			
1	E215	Level switch fail			1,26E-01			
Node	**Code**	**Code Description**	**Memo/Item**	**Freq.** **ev./y**	**Prob.** **-**			
1	P020	H.E. Load more	product	2,40E-02				
1	P005	H.E. Doesn't Realize			1,00E-01			
1	E215	Level switch fail			1,26E-01			

Figure 8: Breakdown of the MCS

4. Conclusions

The AlbatrosIII software allows the drafting and development of the HazOp analysis from which, through the choice and input of failure rates or error probabilities collected in a dedicated database, it is possible to automatically obtain the Fault Trees for the identified Top Events.
With a detailed application of the HazOp, also considering the potential failure modes, the program allows the identification of the SIL (Safety Integrity Level - EN IEC 62061) or PL (Performance Level - EN ISO 13849-1) even of complex systems, such as DCS or PLC.
In the field of reliability and in the major accident risk analysis sector, this allows integration between risk analysis techniques with considerable time savings.

References

Antonello F., Buzzi G. (Bari 2009) Albatros II – un programma "user-friendly" per HazOp - Fault Tree quantificati e MCS. Convegno scientifico nazionale "Sicurezza nei Sistemi Complessi"

Lihou D.A. (1980) Efficient Use of Operability Studies. Safety Promotion and Loss Prevention in the Process Industries

Lihou D.A. (1980) Fault Trees from Operability Studies. Safety Promotion and Loss Prevention in the Process Industries

Piccinini N. et al. (2002) How to avoid the generation of loops in the construction of fault trees. Reliability and Maintainability Symposium Proceeding IEEE, vol. 2.

SINTEF PDS Method Handbook (2013) Reliability Prediction Methos for Safety Instrumented System.

SINTEF PDS Example collection (2010)