APPENDIX 7

Frequencies and probabilities data for the fault tree

Debray B., Piatyszek E., Cauffet F., Londiche H.

Armines, Ecole Nationale Supérieure de Mines de Saint Etienne (France)

TABLE OF CONTENTS

1. Introduction 4

2. Data sources available 6

2.1 Reliability databases 6

2.2 Human reliability data 16

2.3 Accident databases 21

2.4 Other relative distribution of causes 28

2.5 Frequency of the critical events 31

2.6 Other absolute frequencies 32

2.7 Synthesis of the data sources analysis 41

3. Some comments inspired by the Assurance Project 42

4. Proposal of a method for evaluating the frequency of the critical event 45

5. Conclusion 47

6. References 49

6.1 ARAMIS Documents 49

6.2 Other documents 49

7. Additional data 51

7.1 HSE reference failure frequencies 51

7.2 I-Risk 52

Summary

One of the main step of the ARAMIS methodology for the identification of reference accident scenarios is **the calculation of the frequency (per year) of the critical event**. It is shown in the main report that the frequency (per year) of the critical event can be estimated in two ways: either by estimating the frequency (probability) of the initiating events in the fault tree, and combining these frequencies (probabilities) with the actions of safety barriers to calculate the critical event frequency, or by choosing a generic frequency for the critical event, issued from published database.

This appendix aims to give information to the reader in order to be able to put frequencies in the fault tree part of the bow-tie. Other appendices give information on how to take barriers into consideration in order to calculate the frequency of the critical event.

First of all, this document gives an **overview of the different data sources available**. Chapter 2 gives information and figures about reliability databases, human reliability data, accidents databases and other data. Paragraph 2.7 presents a synthesis of data collected for this report, clearly showing that available data are sparse and scattered in the various levels of the fault tree.

Chapter 3 recalls the conclusion of the European project "Assurance", during which it has been shown that the estimation of failure frequencies is a topic in which a great discrepancy exists among experts.

Having in mind these limitations, **ARAMIS proposes to calculate the frequency of the critical event starting from the frequency (probability) of the initiating events, combining them in a fault tree and taking into account the influence of safety barriers in the calculation**.

In the previous steps of the analysis (see main report), the generic fault trees have been built for the equipment analysed.

Plant specific data should be preferred for the failure frequencies of these trees, if available. If not, chapter 4 and tables in chapter 7 give indications about what kind of figures should be used in what circumstances.

1. Introduction

The aim of this step of the ARAMIS project is to provide the user with the maximum number of elements to evaluate the frequency of the critical events resulting from the fault tree analysis of the plant. Once this frequency is evaluated, it should contribute to the selection of the reference scenarios, the definition of the requirements in terms of safety barriers and safety functions, the assessment of the safety barriers efficiency.

The elements that would be needed by the user of the ARAMIS methodology are a method for evaluating the frequency of the critical event and data to apply the method. **This document provides an analysis of the available data and their possible use in the framework of the ARAMIS methodology**.

Along this document different possibilities will be discussed, as they correspond to different trends in the probabilistic approach. For each of them, its applicability within the framework of ARAMIS with the available data will be discussed. Three different approaches have been considered :

a. Evaluate **specific frequencies** from a fault tree and event tree analysis : this corresponds to the most classical approach in the QRA. The frequency of the critical event attempts to take into account all the possible failure of the components and of their barriers. It is used as an input for the downstream evaluation of the consequences and their probabilities (societal risk).

b. Provide **generic frequencies** for the critical events. This approach is used in the Netherlands where the frequency of the critical event is not calculated on the basis of the actual plant configuration but is assumed on the basis of generic figures. In this country, frequencies have been assessed for standard configurations of plants and serve as references in the QRA (Quantitative Risk Assessment). These values implicitly take the presence of safety barriers into account.

c. Provide **initial data which will serve as reference for the barrier approach**. This possibility was discussed in Maastricht (ARAMIS meeting June 2003) as an alternative way to evaluate frequencies (probabilities). It is compatible with the approach developed by INERIS and adapted in the framework of WP3 for the assessment of barrier efficiency. The idea is to decrease an initially high reference frequency (probability) by factors which correspond to the efficiency of the barriers. This initial frequency (probability) would correspond to the frequency of the critical event without any barrier.

A first feeling about accident data would be that there are plenty of them and that their use is obvious. Many reference books about risk analysis simply expose the basics of fault tree and event tree analysis and leave aside the problem of finding or producing data to do the quantitative assessment. Some of them however warn the reader with the difficulty of this task.

The first part of this report lists and analyses the different categories of data available, which are of four main types :

- Reliability databases
- Human reliability data
- Accident databases
- Event frequencies available in the literature

The difficulties with the use of these data in the framework of the ARAMIS methodology is discussed. It lays mainly in the fact that the fault trees build in the first ARAMIS work package are not classical fault trees similar to those used for reliability analysis but generic fault trees with a limited number of levels and a large number of minimal cut sets.

After a short synthesis of the data source and their applicability, a brief comment is made about the result of the European project ASSURANCE, which brings enlightenment about the relativity of the QRA. This project shows that even with a rather complete description of an industrial site and process, very large deviations can be observed. This is a fortiori true for a generic approach.

From these preliminary conclusions, a series of recommendations is given on how the frequencies (probabilities) should be calculated within the framework of the ARAMIS methodology in an actual industrial site. An attempt is then made to provide indicative reference data which can be used as initial references for the barrier approach.

To conclude this introduction it seems interesting to quote the following sentence from the HSE risk assessment guide.

“Base event failure rate data are essential components of risk assessments, but they must be relevant and applicable to site circumstances. Simply taking a number from the literature without consideration of whether it applies to the site in question is unlikely to be acceptable. On the other hand, use of a failure rate that is not consistent with historical or relevant generic industry data must be justified. The origin of all probabilities quoted in a safety report should be given so that, where necessary, Assessors can make a judgement on their appropriateness.” (HSE assessment criteria)

2. Data sources available

2.1 Reliability databases

Fault tree analysis is now a well known and used method to evaluate the reliability of equipment and systems. FTA has been recommended as one of the main components of the QRA (Quantitative Risk assessment) analysis. It is designed to provide an evaluation of the overall probability of an accident scenario, knowing the failure rates of the individual components involved in the scenario.

In this purpose, reliability databases have been developed by groups of industrial companies. Several of them have been inventoried by the RISO [Akhmetjanov]. The first part of this document makes an extensive use of this inventory. It first analyses the industrial field to which these data apply to eliminate those which are not adapted to the process industry concerned by the SEVESO II directive. The content of the databases is then be discussed to evaluate how it can be used in he context of ARAMIS.

The application fields of the databases identified by Risoe are the following :

- Nuclear industry
- Military industry
- Automotive industry
- Aeronautic industry
- Process industry
- Offshore industry
- Electronic components of technical systems

Among these, the only databases applicable to the process industry are the following :

- OREDA : Offshore reliability database. [OREDA]
- GIDEP (only available to companies having a contract with the US government)
- AIChe/CCPS reliability database

The reliability databases provide information about component failures. The main information is the failure rate for different types of failure modes. Usually the failure rate is given as a range with upper, lower and mean value. The distinction is made between failure rates during operation which indicates a number of failure by unit time of functioning and failure on demand, which designates the number of failures per number of solicitation of the component. The components are standard components in the chemical industry. For example the OREDA database contains information about the following components :

- Machinery
  - Gas turbines
  - Compressors
  - Pumps
- Electric equipment
  - Electric generators
- Mechanical equipment
  - Heat exchangers
  - Vessels
  - Control logic units
  - Process sensors
- Control and safety equipment
  - Fire and gas detectors
  - Valves
  - Control systems
- Sub sea equipment
  - Well completions
  - Drilling equipment
  - Miscellaneous utility systems
- Other
  - Electric power systems
  -

Table 1: list of the components for which data are available in the OREDA Database

For each of these components, various sub types are proposed. For examples compressors are divided into :

- Centrifugal
- Electric motor driven
- 100-1000 kW
- 1000 – 3000 kW
- 3000 – 10000 kW
- Turbine driven
- Reciprocating
- Electric motor driven
- 1000-3000 kW
- 3000-10000 k W

For each component, various failure modes are proposed with very different failure rates for each. For example, the failure modes envisaged for **compressors** are given in Table 2.

• Critical	• External leakage
• Failed to start	• Fail while running
• High gas flow	• Overheated
• Other	• Overhaul
• Unknown	• Vibration
• Degraded	• External leakage
• Fail while running	• High gas flow
• Low gas flow	• Overheated
• Other	• Overhaul
• Unknown	• Vibration
• Incipient	•

Table 2: failure modes for compressors in the OREDA database

Detailed are also given in OREDA handbook of the repartition of the failures among the different components constituting the equipment. The following table is an example of an OREDA table.

Taxonomy no 1.1.1.1.1		Item Machinery Compressors Centrifugal Electric Motor Driven (100-1000) kW							
Population	**Installations**	**Aggregated time in service (10^6 hours)**					**No of demands**		
5	2	**Calendar time *** 0.1248		**Operational time †** 0.0832					
Failure mode		**No of**	**Failure rate (per 10^6 hours)**				**Active**	**Repair (manhours)**	
		fail.	**Lower**	**Upper**	**SD**	**MLE**	**rep. hrs**	**Min**	**Mean**	**Max**
Critical		**23*** **23†**	**1.31** **2.02**	**827.93** **1806.90**	**304.49** **665.33**	**184.33** **276.36**	**10.0**	**0.5**	**24.3**	**186.3**
Failed to start		1* 1†	0.94 0.29	22.20 61.58	7.02 22.41	8.01 12.02	-	13.0	13.0	13.0
Fail while running		14* 14†	0.97 1.28	499.13 1093.54	183.39 402.61	112.20 168.22	10.0	0.5	24.0	186.3
Unknown		1* 1†	0.94 0.29	22.20 61.58	7.02 22.41	8.01 12.02	-	11.4	11.4	11.4
Vibration		7* 7†	0.71 0.70	243.34 538.64	89.14 198.24	56.10 84.11	-	0.5	28.5	117.5
Degraded		**6*** **6†**	**0.67** **0.62**	**206.78** **459.35**	**75.67** **169.04**	**48.09** **72.09**	-	**9.7**	**27.4**	**75.4**
Other		6* 6†	0.67 0.62	206.78 459.35	75.67 169.04	48.09 72.09	-	9.7	27.4	75.4
Incipient		**29*** **29†**	**1.54** **2.51**	**1047.12** **2282.45**	**385.22** **840.47**	**232.42** **348.45**	**4.1**	**2.0**	**16.2**	**173.6**
External leakage		4* 4†	0.60 0.46	133.63 300.70	48.67 110.60	32.06 48.06	2.5	3.0	21.3	51.7
Overheated		1* 1†	0.94 0.29	22.20 61.58	7.02 22.41	8.01 12.02	-	173.6	173.6	173.6
Other		21* 21†	1.23 1.85	754.87 1648.38	277.58 606.95	168.30 252.33	4.4	2.0	9.0	62.3
Overhaul		1* 1†	0.94 0.29	22.20 61.58	7.02 22.41	8.01 12.02	2.0	3.0	3.0	3.0
Vibration		2* 2†	0.54 0.32	60.26 141.78	21.46 52.04	16.03 24.03	-	4.9	9.4	14.0
All modes		**58*** **58†**	**2.64** **4.90**	**2106.50** **4580.93**	**775.38** **1686.97**	**464.83** **696.91**	**4.4**	**0.5**	**20.6**	**186.3**
Comments										

Figure 1: example of OREDA data

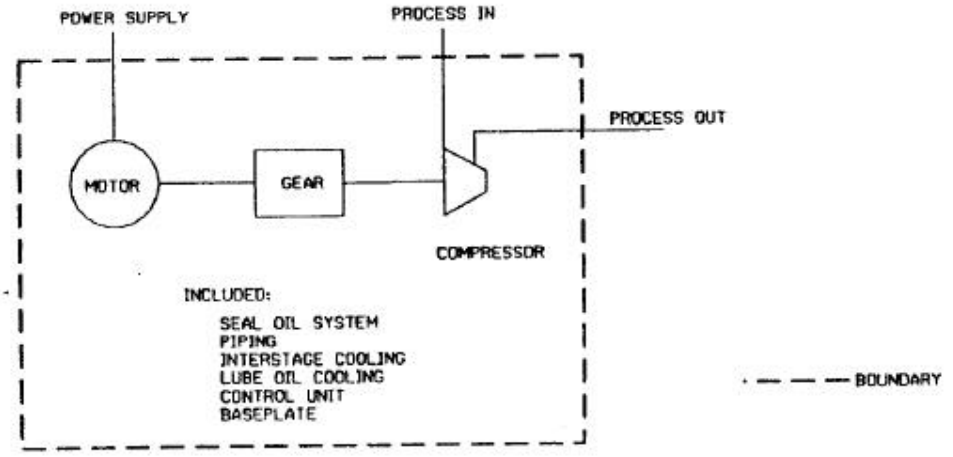
DATA ON SELECTED PROCESS SYSTEMS AND EQUIPMENT

Taxonomy No. 3.3.2.f	**Equipment Description** ROTATING EQUIPMENT-COMPRESSOR ELECTRIC MOTOR DRIVEN
Operating Mode	**Process Severity** UNKNOWN

Population	**Samples**	**Aggregated time in service (10^6 hrs)**		**No. of Demands**
		Calendar time	**Operating time**	

Failure mode	**Failures (per 10^6 hrs)**			**Failures (per 10^3 demands)**		
	Lower	**Mean**	**Upper**	**Lower**	**Mean**	**Upper**
CATASTROPHIC a. Fails While Running b. Rupture c. Spurious Start/Command Fault d. Fails to Start on Demand e. Fails to Stop on Demand DEGRADED a. External Leakage	27.9	2470.0	9690.0			

Equipment Boundary



Data Reference No. (Table 5.1): 8.4

Figure 2: Example of CCPS reliability data

Other databases are build by industrial groups. For example the French UIC (union of the chemical industries) has been developing a database for 20 years by collecting incident data from chemical plants of the Rhône-Alpes region.

The following tables are examples of the data that can be obtained from this database.

	First step of database development		Second step of database development	
EQUIPMENTS	**Year of introduction in the database**	**Number of equipment**	**Year of introduction in the database**	**Number of equipment**
Stirrers	1988	2 550	1999	1 863
Analysers	1988	8		
Sensors	1988	14 107	2002	24 944
Regulators	1988	7 470		
Compressors	1988	78		
Heat exchangers	1988	640		
Spinning Dryer	1988	129	2002	86
Electric motors	1988	5 572		
Pumps	1988	1 720	1996	5 276
Regulation valves	1988	13 374		
Transformers	1988	76		
Inverters	1988	8	2002	209
Reducer multiplier	1988	1 247		
Safety valves	1988	460	2003	4 691
Automated systems			2002	333

Table 3: components inventoried in the UIC Database

Table 4 provides an example of data collected for pumps.

Failure rate of different types of pumps with 80% confidence interval (failure/hour).

	Number de pumps	Number of failures	inferior borne	Middle	Superior borne
Centrifugal	3186	1390	$1{,}25.10^{-4}$	$1{,}30.10^{-4}$	$1{,}34.10^{-4}$
Horizontal centrifugal	2398	1113	$1{,}39.10^{-4}$	$1{,}45.10^{-4}$	$1{,}50.10^{-4}$
Vertical centrifugal	219	78	$9{,}44.10^{-5}$	$1{,}10.10^{-4}$	$1{,}28.10^{-4}$
Vacuum	373	177	$1{,}11.10^{-4}$	$1{,}23.10^{-4}$	$1{,}36.10^{-4}$
Multicell	362	98	$6{,}35.10^{-5}$	$7{,}27.10^{-5}$	$8{,}30.10^{-5}$
Volumetric	796	496	$1{,}90.10^{-4}$	$2{,}02.10^{-4}$	$2{,}14.10^{-4}$
Volumetric with piston	246	101	$1{,}40.10^{-4}$	$1{,}60.10^{-4}$	$1{,}83.10^{-4}$
Volumetric with gears	135	56	$1{,}03.10^{-4}$	$1{,}23.10^{-4}$	$1{,}47.10^{-4}$
Volumetric with membrane	366	254	$2{,}39.10^{-4}$	$2{,}59.10^{-4}$	$2{,}81.10^{-4}$
Vacuum extraction	175	43	$6{,}53.10^{-5}$	$8{,}06.10^{-5}$	$9{,}88.10^{-5}$
Complete set : all pumps	5276	2328	$1{,}24.10^{-4}$	$1{,}27.10^{-4}$	$1{,}30.10^{-4}$

Table 4: example of failure rates for pumps in the UIC database

A correction factor has been introduced to take the environment, failure mode and conditions of use into account. For each component, the correction factor to be used in an environment "e" is calculated as follows.

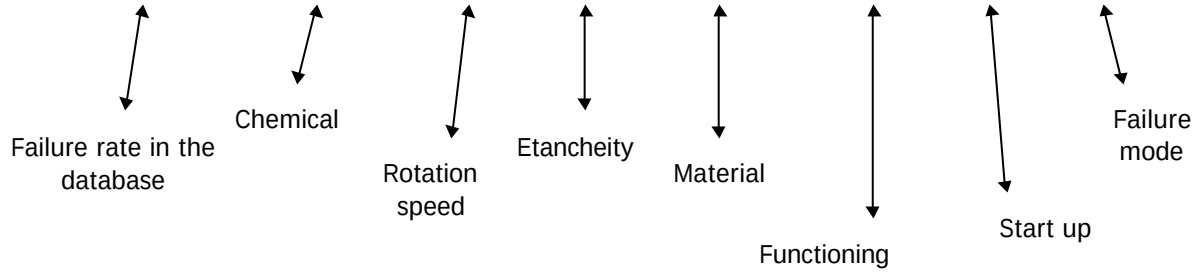
$$C_e = \frac{l_e}{l_{global}}$$

where λ_e is the failure rate measured in the environment "e" and λ_{global}, the failure rate given by the database.

The overall failure rate is then the product of the initial failure rate by the series of correction factors.

The following expression is an example of the calculation of the failure rate for a pump :

$$\lambda_k = 1{,}445.10^{-4} \times 1{,}283 \times 0{,}962 \times 1{,}146 \times 0{,}713 \times 1{,}551 \times 1{,}249 \times 0{,}337$$



$$\lambda_k = 0{,}951.10^{-4} \text{ failure / hour}$$

Correction factors function of the environment of the pump with 68% confidence interval.

		Number of pumps	Number of failures	Inferior borne	Middle	Superior borne
Product	Water	398	135	0,75	1,06	1,36
	Chemical	2613	823	0,84	1,28	1,73
	Corrosive	1785	441	0,51	0,89	1,26
	Loaded	580	195	0,69	1,27	1,84
	Hot	382	154	0,84	1,14	1,45
	Viscous	127	39	0,40	1,21	2,02
Rotation speed	from 0 to 1100 rev/min	261	182	1,77	2,96	4,16
	from 1100 to 1800 rev/min	1682	664	0,63	0,85	1,06
	from 1800 to 3500 rev/min	2189	982	0,68	0,96	1,25
	> 3500 rev/min	7	21	1,88	11,27	20,66
Water tightness	Braids	1084	406	1,01	1,05	1,09
	G.M.S.	2150	732	0,72	0,74	0,75
	G.M.D.	495	217	1,07	1,15	1,22
	Immerged pump	163	50	0,48	0,57	0,67
	Magnetic stirring	40	20	1,18	1,42	1,66

Material	Cast iron	993	553	0,61	1,58	2,55
	Stainless steel	1942	716	0,45	0,71	0,98
	Teflon	57	24	0,49	1,49	2,48
	PVDF	109	47	1,09	2,43	3,77
	Ceramic	10	24	7,85	17,07	26,30
	Graphite	80	57	0,32	2,02	3,73
Type of functioning	Continuous > 5000 h/y	2215	1324	0,53	0,74	0,95
	500 < Discontinuous < 5000 h/y	2006	662	0,95	1,55	2,15
	Occasional < 500 h/an	173	89	4,84	12,23	19,61
Frequency of starting	< 1 / week	1863	1161	0,38	0,70	1,01
	> 1 / week	2151	742	0,83	1,25	1,67

Table 5: examples of correction factors in the UIC database

	95 % lower bound	Average	95 % upper bound
Tightness	0,146	0,338	0,529
Mechanical part	0,099	0,281	0,463
Coupling part	0,001	0,086	0,170

Table 6: examples of correction factors according to the failure mode

This example shows that failure rates are highly dependent on the environment, on the conditions of use and on the failure mode.

The same approach is presented in the CCPS guidelines [CCPS], inspired by the methods recommended by du Pont in their *Process Safety Management Reference Manual*.

	Adjustment factors	
Equipment failure rate influences	Instruments	Valves
Process medium factors		
Corrosion	1.07	1.14
Erosion	1.14	1.28
Fouling, plugging	1.07	1.14
Pulsating flow	1.14	1.07
Temperature extremes	1.07	1.07
External environmental factors		
Vibration	1.42	1.21
Corrosive atmosphere	1.21	1.21
Dirty atmosphere	1.07	1.07
High temperature and/or humidity	1.07	1.07
Location factors		
Exposed mechanical damage	1.07	1.07
Inaccessible for inspection	1.07	1.07

Table 7: Generic failure rate data adjustment factors in the Du Pont's *Process Safety Management Reference Manual*

Using data from reliability databases to assess the frequency of critical events:

The use of reliability databases will now be discussed with respect to the objectives defined in the introduction.

a. **Evaluate specific frequencies from a fault tree and event tree analysis**.

Even if reliability databases are often used for maintenance purposes, their use for evaluating the specific frequency of critical events is widespread. It would therefore seem obvious that they can be used to assess the frequencies of critical events during an ARAMIS analysis. It is unfortunately not so simple. The fault trees build during WP1A of ARAMIS are generic fault trees. As such they present several characteristics which make them difficult to use with reliability databases :

- They are limited in depth to five levels (even four, as the first one is the critical event), which has the consequence that **the failure of plant components often does not explicitly appear in the tree**.

- When it does, the precise **type of component involved is not given**, which makes impossible the selection of a failure rate in the database.
- In the same way, the **failure mode is not given**, which again has an enormous importance on the definition of the failure rate. Especially, the distinction is not made between failure in use and failure on demand.
- The **number of components involved is not provided**. Depending on the type of components and the failure mode, the number of components can have diverse influence on the overall failure rate. The duplication of one component can be considered as a way to reduce the failure rate by introducing a redundancy if only one component is necessary (and provided that the configuration of the equipment really permits the second component to relieve the first one in case of failure) or it can be considered as an increase of the probability of failure if two components are necessary. The failure rate would be doubled in such a configuration. This is particularly true for pipes, for which the probability of failure is directly linked to the length of the pipe.

For all these reasons it is not possible to use directly the reliability databases with the generic fault trees to calculate the frequency of the critical event. Yet, this would be possible if the fault trees were used as a base for the definition of scenarios and the elaboration of specific and detailed fault trees. In such a case, it would be possible to make the specific components appear with their dread failure mode and environmental information.

b. **Provide generic frequency for the critical events**.

The reliability databases do not contain critical events frequencies but rather frequencies of component failure. To calculate a generic frequency for the critical event using reliability database it would be necessary to use the generic fault trees with the reliability data. This has been discussed above, and is not possible.

c. **Provide initial data which will serve as reference for the barrier approach**.

Here again, the configuration of the generic fault trees makes difficult using the reliability data to calculate an initial value corresponding to the frequency of the critical event without safety barriers. Yet, assumptions could be made to obtain a rough estimate of the upper bound of the critical event frequencies as will be proposed in the last section of this document.

2.2 Human reliability data

"Data tells us that human failures contribute up to 80% of industrial accidents. Even in oil refineries, which are highly capitalised and automated, the figure is 50%." (HSE safety report assessment guidelines)

Human error is a root cause for all the direct causes identified at the origin of the critical events. Therefore, an evaluation of the critical event frequency should use an evaluation of human error frequency (probability). The following paragraphs examine the possibility of using human reliability analysis to assess the overall frequency of the critical events.

HR (human reliability) is influenced by many factors among which the design of man-machine interface, the environment, the management, the pace of activity. In fact, human reliability analysis distinguishes different situations in which the human action is required and subject to errors.

A parallel can be made with equipment failure for which the failure mode is of extreme importance to determine the failure rate. The following tables provides examples of common human error failure rates (on demand).

Failure event	HEP (Human error probability)
Omitting step in procedure	0.003
Fail to use test or calibration procedure	0.05
Omission in procedure, with checkoff, <10 items	0.001
Omission in procedure, with checkoff, >10 items	0.003
Omission in procedure, without checkoff, <10 items	0.003
Omission in procedure, without checkoff, >10 items	0.01
Commission in reading digital meter	0.001
Commission in reading analogue meter	0.003
Commission in reading chat recorder	0.006
Inadvertent operation of manual control	Plant Specific
Select wrong controls, controls labelled only	0.003
Select wrong controls, controls in functional grouping	0.001
Select wrong controls, mimic	0.0005
Turn 2 position, control wrong way	0.0005
Turn 2 position, population stereotype violated	0.05
Select wrong circuit breaker, densely packed labels	0.005
Select wrong local valve, similar items clear labels	0.001
Select wrong local valve, similar items unclear labels	0.005
Checker fails to find error, routine with procedure	0.1
Checker fails to find error, routine, special activity	0.01
Checker fails to find error, routine, safety import	0.001

Table 8: Examples of HEP (human error probabilities) [Fragola]

Other authors provide data for human error probabilities which are more generic and, therefore, more easy to use in the framework of ARAMIS. However, some though has to be made about the meaning of these data and their use.

Type of Activity	**Probability of Error per Task**
Critical Routine Task (tank isolation)	0.001
Non-Critical Routine Task (misreading temperature data)	0.003
Non Routine Operations (start up, maintenance)	0.01
Check List Inspection	0.1
Walk Around Inspection	0.5
High Stress Operations; Responding after major accident	
- first five minutes	1
- after five minutes	0.9
- after thirty minutes	0.1
- after several hours	0.01

Table 9: Human Error Rates **(Source: US Atomic Energy Commission Reactor Safety Study, 1975)**

Type of Activity	**Probability of Error per Task**
Simplest Possible Task	
Overfill Bath	0.00001
Fail to isolate supply (electrical work)	0.0001
Fail to notice major cross roads	0.0005
Routine Simple Task	
Read checklist or digital display wrongly	0.001
Set switch (multiposition) wrongly	0.001
Routine Task with Care Needed	
Fail to reset valve after some related task	0.01
Dial 10 digits wrongly	0.06
Complicated Non-routine Task	
Fail to recognise incorrect status in roving inspection	0.1
Fail to notice wrong position on valves	0.5

Table 10: **Human Error Rates (Source: Smith DJ 1993)**

Practically, the failure rate depends a lot on the type of activity performed by the operator and on the time available to do it. The following figures illustrates this dependency. The more time is available to the operator to perform a given task the lower is the probability of error.

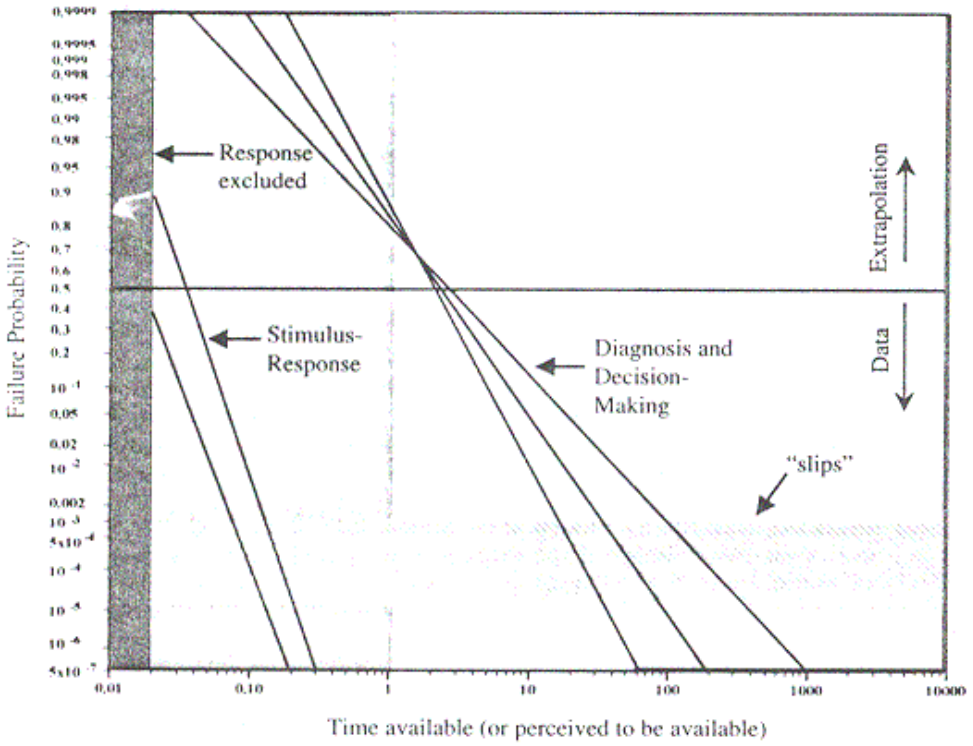


Figure 3: TRCs (time reliability curves) based on Human response Time Regime (Dougherty and Fragola cited in [Fragola])

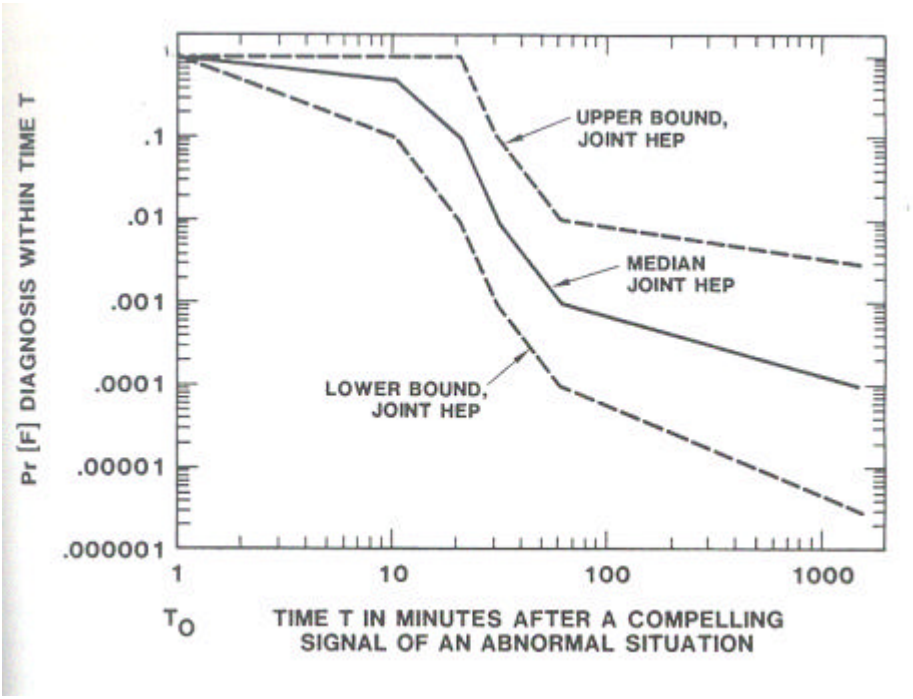


Figure 4: Human error probability of diagnosis of one abnormal event by control room personnel (after Swain and Guttmann, 1983) reproduced in [Lees]

Here again, it seems obvious that the generic nature of the fault trees prevents from using directly the human reliability data to evaluate the frequency of the critical event. Most of the time, the human failure modes are not specified, the number of tasks is not known. The latest is a problem because the human failure rates concern mostly failures on demand. The global failure rate to be applied is therefore the product of the failure rate by the number of tasks.

Any way, if human reliability data cannot be used directly in the generic fault trees to evaluate the frequencies of critical events, they can be used as references to produce basic frequencies which will be reduced by the application of prevention barriers.

2.3 Accident databases

The accident databases provide general and detailed information about past accidents in various types of industries and transport activities. These databases are build from the accident declarations by plant operators. The database structure varies from one database to another. Some databases have very detailed fields (MARS), others only provide textual descriptions of accidents (ARIA). The number of accidents accessible also varies a lot as well as the scope and reference territory.

For all these reasons, the results obtained by analysing the databases have to be taken cautiously.

An extensive analysis of MARS, HADES and MHIDAS has been made by FPMs, JRC and UPC [Delvosalle MOOA]. The aim of the present document is not to reproduce the results obtained by this analysis but rather to discuss their applicability in the objective of producing probability figures which could be used to evaluate the risk in a process plant.

The analysis of accident databases provides information about the relative distribution of causes.

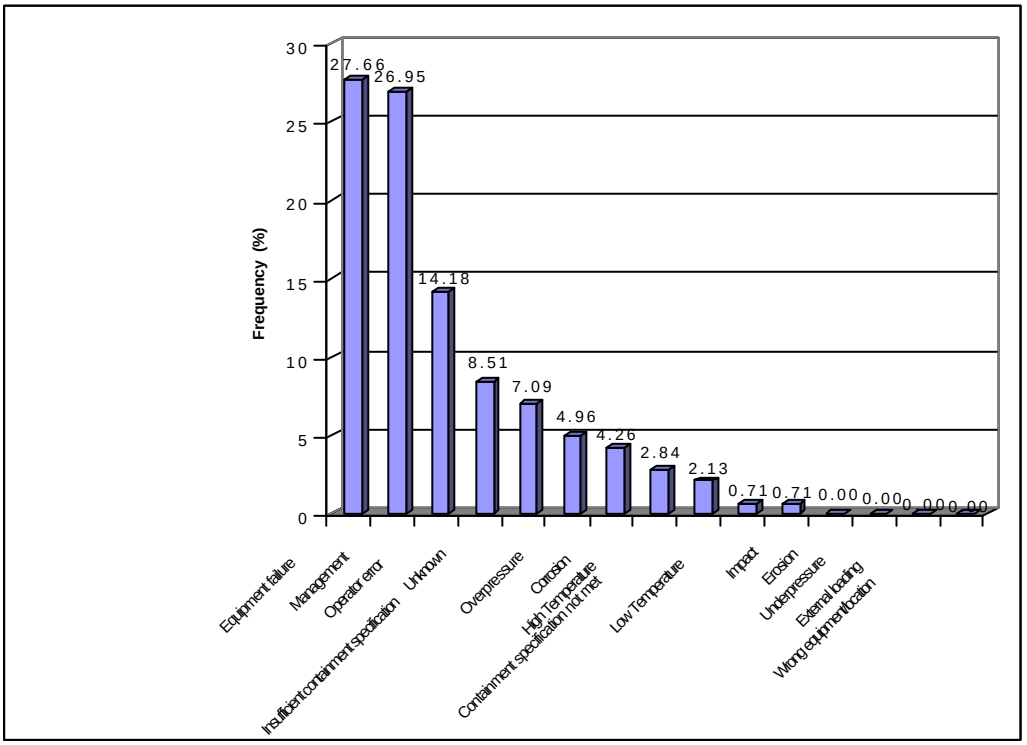


Figure 5: Causes distribution in MARS (141 accidents) [Delvosalle MOOA]

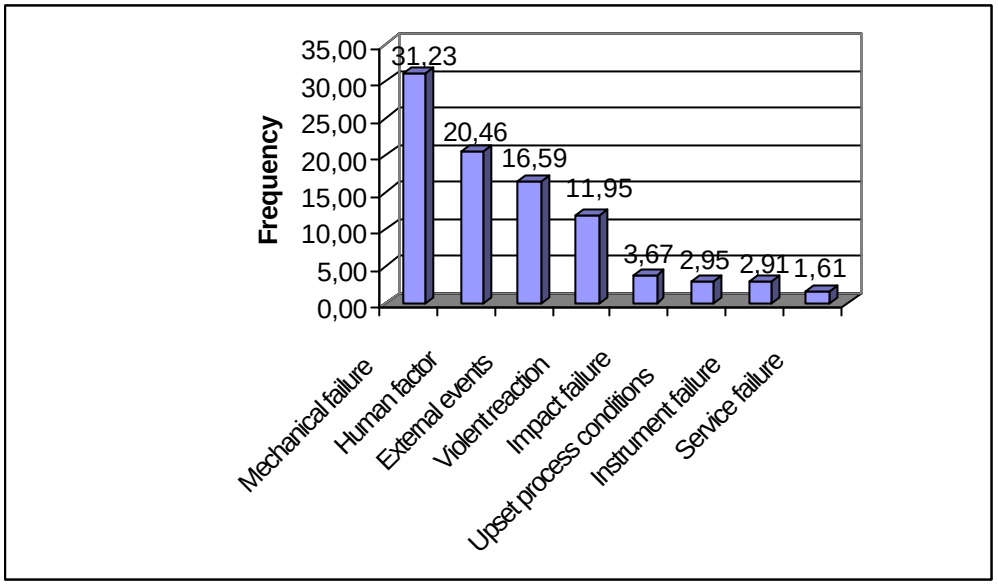


Figure 6: distribution of causes in MHIDAS [Delvosalle MOOA]

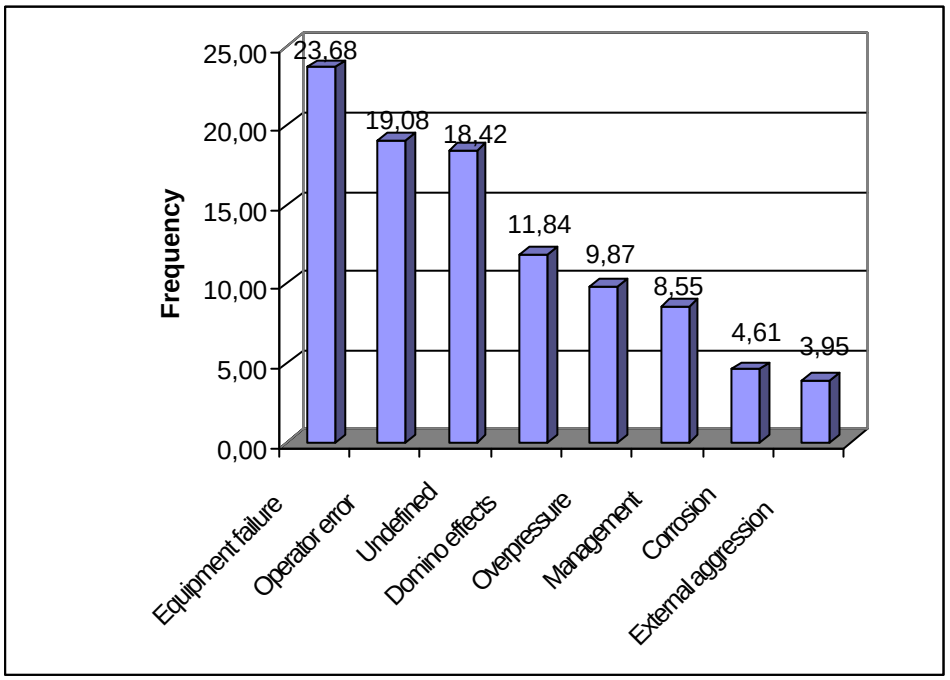


Figure 7 : Repartition of causes in HADES [Delvosalle MOOA]

A first analysis of these data shows that, even if they bring some information about the most observed accidents, they remain difficult to exploit to derive failure probabilities.

Differences can be observed between the databases in terms of cause classification, and values of the relative distribution. The types of cause are different from one base to another and are different

from the causes retained in the ARAMIS fault trees. The category "equipment failure" contains events which could be attributed to other categories of causes if a deeper analysis was made. Table 11 provides a rough analysis of the IChemE Accident database [IchmE]. Among the causes identified in this database, many can be found in the ARAMIS fault trees. Others were not identified. This shows that ARAMIS fault trees should not be considered as exhaustive but rather as a base for an initial risk analysis, which should be completed according to the local context.

	number of accidents	%
chemical causes		
additional chemical present		
accidental mixing	39	0,73
contamination		
cleaning inadequate	38	0,71
solids deposition	18	0,33
oxygen enrichment	4	0,07
residue	2	0,04
channelling in catalyst bed	0	0,00
chemical missing		
lack of stabiliser/inhibitor	3	0,06
low level of catalyst	3	0,06
chemicals added incorrectly	24	0,45
incorrect chemical present		
incorrect chemical concentration	4	0,07
incorrect material of construction	36	0,67
unwanted chemical reaction		
auto ignition	57	1,06
decomposition		
auto decomposition	10	0,19
polymerisation	38	0,71
runaway reaction	75	1,39
spontaneous combustion	37	0,69
thermic reaction	8	0,15
uncontrolled reaction	10	0,19
equipment causes		
control failure		
computer failure	9	0,17
electrical equipment failure		
arcing	32	0,59
flashover	8	0,15
generator failure	1	0,02
lack of earthling	33	0,61
Short circuit	50	0,93
Spark	232	4,31
Equipment missing	5	0,09
incorrect equipment installed	37	0,69
instrumentation failure	99	1,84
material of construction failure		
brittle fracture	22	0,41

						number of accidents	%
				corrosion		295	5,48
				crack		100	1,86
				creep		12	0,22
				embrittlement		10	0,19
				erosion		8	0,15
				fracture		61	1,13
				hydrogen embrittlement		2	0,04
				metal fatigue		19	0,35
				rusting		9	0,17
				Stress		27	0,50
				stress corrosion cracking		9	0,17
				weld failure		86	1,60
			mechanical equipment failure				
				agitation failure		5	0,09
				bearing failure		38	0,71
				blower failure		1	0,02
				bolt failure			
					bolts incorrectly tightened	9	0,17
				connector failure		5	0,09
				cooling tower collapse		1	0,02
				dam failure		1	0,02
				elbow failure		0	0,00
				equipment misalignment		4	0,07
				expansion joint failure		3	0,06
				flange failure		18	0,33
				flexible coupling failure		5	0,09
				floating roof failure		9	0,17
				gasket failure		43	0,80
				gauge glass failure		9	0,17
				hose failure		45	0,84
				joint failure		29	0,54
				lining failure		4	0,07
				pipeline failure		75	1,39
				pump failure		47	0,87
				refractory failure		3	0,06
				seal failure		62	1,15
				shaft failure		1	0,02
				tank failure		28	0,52
				tube failure		63	1,17
				valve failure		156	2,90
				vessel failure		9	0,17
			safety equipment failure				
				alarm failure		14	0,26
				bursting disk failure			
					bursting disk fails prematurely	1	0,02
				safety relief valve failure		9	0,17

	number of accidents	%
external causes		
deliberate acts		
arson	8	0,15
bomb	3	0,06
civil war	1	0,02
missile	1	0,02
sabotage	76	1,41
terrorism	31	0,58
vandalism	16	0,30
excessive vibration	55	1,02
fire/explosion		
lagging fire	22	0,41
friction heat	11	0,20
hot surface	155	2,88
mechanical spark	15	0,28
natural disaster		
avalanche	1	0,02
earth movement		
earth tremor	2	0,04
earthquake	20	0,37
excavation damage	52	0,97
landslide	3	0,06
settlement	2	0,04
subsidence	6	0,11
weather effects		
cold weather	54	1,00
flood	17	0,32
fog	25	0,46
lightning	140	2,60
rain	16	0,30
storm damage		
strong winds		
hurricane	46	0,86
typhoon	0	
sunlight	4	0,07
thermal expansion		
hot weather	6	0,11
human causes		
Additional incorrect operation	3	0,06
Cigarette	31	0,58
Contractor error	44	0,82
design fault	14	0,26
design or procedure error		
cleaning procedure incorrect	11	0,20
design inadequate	202	3,76
faulty instructions	12	0,22

	number of accidents	%
inadequate guarding	13	0,24
maintenance procedure error	28	0,52
safety procedure inadequate	286	5,32
standards inadequate	5	0,09
Document errors	5	0,09
drug misuse	1	0,02
operation inadequate		
competency lacking	16	0,30
draining of line insufficient	7	0,13
identification inadequate	10	0,19
inspection inadequate	68	1,26
installation inadequate	35	0,65
isolation inadequate	51	0,95
labelling incorrect	34	0,63
maintenance inadequate	59	1,10
pipe laying inadequate	1	0,02
testing inadequate	33	0,61
operation omitted		
atmosphere not tested	8	0,15
operator error	256	4,76
operator/crew fatigue	1	0,02
shift change	5	0,09
management system inadequate		
Manning levels inadequate	1	0,02
modification procedures inadequate	22	0,41
permit to work system inadequate	29	0,54
training inadequate	27	0,50
Process causes		
Backflow	24	0,45
exothermic reaction		
thermal instability	5	0,09
flameout	10	0,19
Friction spark	0	0,00
frothing	1	0,02
incorrect flow rate		
flow rate too high		
high loading rate	2	0,04
Inadequate venting	4	0,07
flow rate too low		
flow restriction		
vent blocked	9	0,17
no flow	12	0,22
incorrect pressure		
high pressure		
hydraulic pressure	6	0,11
internal explosion	3	0,06

						number of accidents	%
				overpressurisation		192	3,57
				pressure surge		16	0,30
				pump dead heated		3	0,06
				water hammer		12	0,22
			low pressure				
				implosion		7	0,13
				vacuum		23	0,43
		incorrect Temperature					
			high temperature				
				overheating		188	3,50
				thermal degradation		5	0,09
			low temperature				
				cold brittleness		1	0,02
				freezing		11	0,20
				inadequate insulation		2	0,04
		leak					
			air leaking into system			2	0,04
			flange leak			47	0,87
			gasket leak			1	0,02
			joint leak			6	0,11
		Offloading				20	0,37
		Overflow					
		tank overflow				2	0,04
		Overspeed				5	0,09
		reverse flow				20	0,37
		rollover				1	0,02
		static				192	3,57
		under filling of vessel				1	0,02
		water slug				2	0,04
		unidentified cause				77	1,43
		utility failure					
			air system failure			10	0,19
			fuel supply failure			1	0,02
			hydraulic failure			1	0,02
			inert gas failure			2	0,04
			lubrication failure			6	0,11
			power supply failure			70	1,30
			steam failure			3	0,06

Table 11: relative distribution of causes in the IchemE accident database (all types of activities excluding transportation). This relative frequency is only aimed at illustrating the diversity of causes.

2.4 Other relative distribution of causes

Apart from accident databases, different bibliographical sources provide tables with relative repartition of causes. The most interesting are those which cross the immediate cause, such as erosion or corrosion, with the root cause, human error, poor management,… In the framework of ARAMIS, the immediate causes could correspond to the direct causes and the root causes correspond to the undesirable events.

An interesting complement to this classification was brought by a contract research report by the HSE executive [Bellamy], which proposes a three entry classification of accident causes : direct cause, origin of failure and recovery failure. The following figure exposes the principle of such a classification applied to pipework failures. What is interesting in this approach is that it implicitly states that the recovery failure is part of the global failure scenario. This should be compared with the barrier approach introduced in ARAMIS.

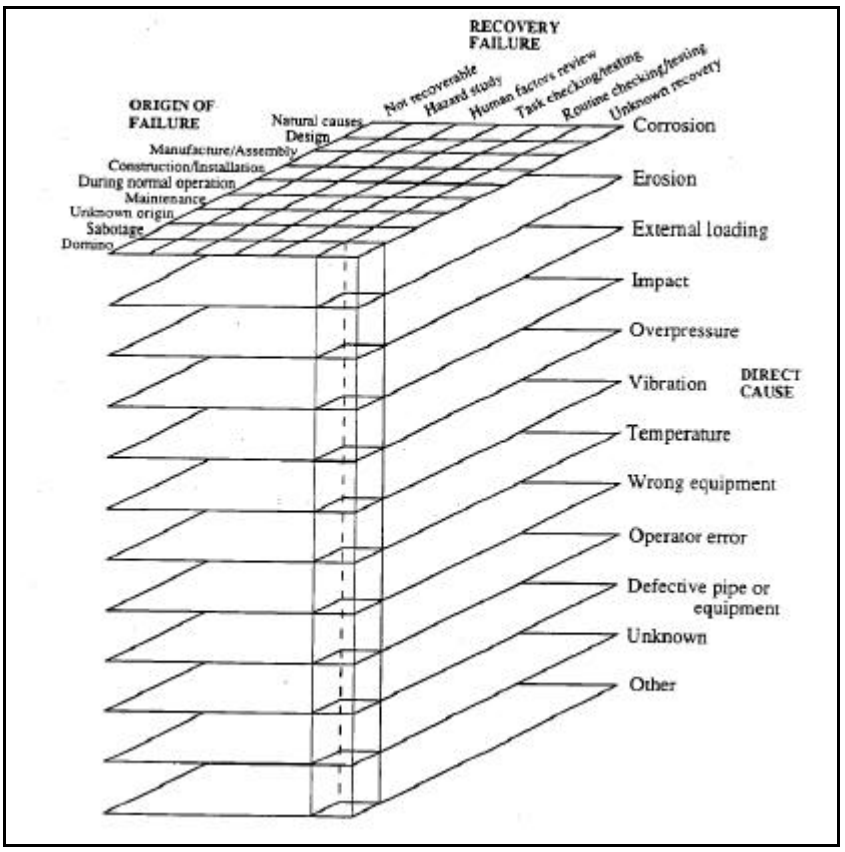


Figure 8: Structure of classification scheme showing direct cause, origin of failure and recovery failure. Bellamy et al, 1989

	N° of incidents to which cause contributed	Total contribution	% contribution (overall) (n=921)	% contribution (excluding unknowns) (n=543.5)
Defective pipe or equipment (unknown cause)	303	293.5	31.9	-
Operator error	190	167.83	18.2	30.9
Overpressure	129	111.83	12.1	20.5
Corrosion	92	85.5	9.3	15.6
Unknown	84	84	9.1	-
Impact	49	43.83	4.8	8.1
Wrong in-line equipment or location	44	36.83	4	6.7
Temperature (high or low)	44	34.83	3.8	6.4
External loading	35	27.5	3	5
Vibration	16	14	1.5	2.5
Other	17	14	1.5	2.5
Erosion	11	7.33	0.8	1.3
Total	1014	921	100	100

Table 12: Breakdown of level 1 direct causes of incidents [Bellamy]

	%
A. Incident modes	
Unknown exothermic decomposition	15.1
Incorrect charging	17.2
Inadequate cooling	13.1
Excessive heating	9.6
Incorrect agitation	10.1
Inadequate batch control	9.1
Undesired catalyst	2.5
Exothermic from impurity	10.6
B. Incorrect charging	
Excess of reactant	29.4
Deficiency of reactant	26.5
Too fast addition of reactant	23.5
Modification of reactant	11.8
Incorrect order of reactant addition	5.9
C. Inadequate cooling	
Coolant source/power failure	0
Coolant pump set failure	3.8
Coolant turned off	11.5
Automatic control failure	11.5
Condenser fault	11.5
D. Excessive heating	
Initial overheating	15.8
Heating / cooling changeover fault	15.8
Undesired heating	10.5
Automatic control failure	10.5
Manual control failure	10.5
E. Incorrect batch control	
Initial temperature too low	11.1
Initial temperature too high	0
Too fast addition of reactant relative to the temperature	22.2
Incorrect cycle	16.6
Excessive holding	22.2

Table 13: analysis of reactor overpressure [Lees] (Table 11.11)

Causes of service failure by corrosion	%	Causes of service failure by mechanical failure	
Cavitation	0.3	Abrasion, erosion or wear	5.4
Cold wall	0.4	Blisters, plating	0.1
Cracking, corrosion fatigue	1.5	Brinelling	0.1
Cracking, stress corrosion	13.1	Brittle fracture	1.2
Crevice	0.9	Cracking, heat treatment	1.9
Demetallification	0.6	Cracking, liquid metal pen	0.1
End grain	0.4	Cracking, plating	0.6
Erosion-Corrosion	3.8	Cracking, thermal	3.1
Fretting	0.3	Cracking, weld	0.6
Galvanic	0.4	Creep or stress rupture	1.9
General	15.2	Defective material	1.6
Graphitization	0.1	Embrittlement, sigma	0.3
High temperature	1.3	Embrittlement, strain age	0.4
Hot wall	0.1	Fatigue	14.8
Hydrogen blistering	0.1	Galling	0.1
Hydrogen embrittlement	0.4	Impact	0.1
Hydrogen grooving	0.3	Leaking through defects	0.4
Intergranular	5.6	Overheating	1.9
Pitting	7.9	Overload	5.4
Weld corrosion	2.5	Poor welds	4.4
		Warpage	0.4
Sub-total	55.2	Sub-Total	44,8

Table 14: Causes of service failure in metal equipment and piping in chemical plants (Collins and Monack, 1973) [Lees] (Table 12.26)

These relative distribution tables bring useful information about the most frequent causes, but, again, cannot be used directly to evaluate absolute frequencies. Yet, if the absolute frequency of one event is known, they can be used to derive the order of magnitude of other causes in the same family. This will be used in the last section of the present document to produce the initial data to be used for the barrier approach.

2.5 Frequency of the critical events

Diverse bibliographical sources provide generic frequencies for the critical events. Most of these are issued from countries where QRA serves as a decision support for land use planning. An analysis of these data sources is more deeply presented in appendix 10.

2.6 Other absolute frequencies

Lees and other authors propose a series of data from a large literature review. However, many of these data are relatively old. Most of them are from the seventies. A large proportion is issued from the nuclear industry and can therefore not be applied to the process industry. Many of these data are reliability data concerning different types of equipment used in the process industry. Others are frequencies of events such as pipe leaks or causes such as overfilling. Such data always apply to a particular industrial activity and are the result of a limited data collection process, or, often an expert judgement, which makes difficult their extrapolation to other activities. When secondary failures are considered, the data always apply to plants where the safety standards of the time were applied, which makes difficult their use as reference data in a "no barrier" context as required by the MIMAH methodology.

The following four tables (Table 15 to Table 18) provide useful reliability data, some of which can be used directly in the generic fault trees. Critical event frequencies are shown to allow the reader to compare his own calculations and some published data.

	Failure rate (failure/10^6 h)
Electric motor	10
Transformer (<15kV)	0.6
(132-400 kV)	7
Circuit breakers (general <33kV)	2
(400kV)	10
Pressure vessels (general)	3
(high standard)	0.3
Pipes	0.2
Pipe joints	0.5
Ducts	1
Gaskets	0.5
Bellows	5
Diaphragm (metal)	5
(rubber)	8
Unions and junctions	0.4
Hoses (heavily stressed)	40
(Lightly stressed)	4
Ball bearings (heavy duty)	20
(Light duty)	10
Roller bearings	5
Sleeve bearings	5
Shafts (heavily stressed)	0.2
(lightly stressed)	0.02

	Failure rate (failure/10^6 h)
Relief valves : leakage	2
Blockage	0.5
Hand-operated valves	15
Control valves	30
Ball valves	0.5
Solenoid valves	30
Rotating seals	7
Sliding seals	3
‘o’ring seals	0.2
Couplings	5
Belt drives	40
Spur gears	10
Helical gears	1
Friction clutches	3
Magnetic clutches	6
Fixed orifice	1
Variable orifices	5
Nozzle and flapper assemblies : blockage	6
Breakage	0.2
Filters : blockage	1
Leakage	1
Rack-and-pinion assemblies	2
Knife-edge fulcrum : wear	10
Springs (heavily stressed)	1
(lightly stressed)	0.2
Hair springs	1
Calibration springs : creep	2
Breakage	0.2
Vibration mounts	9
Mechanical joints	0.2
Grub screws	0.5
Pins	15
Pivots	1
Nuts	0.02
Bolts	0.02
Boilers (all types)	1.1
Boiler feed pump	1012.5
Cranes	7.8

Table 15: Some data on equipment failure rates published by the UKAEA 1972 from nuclear and non nuclear industry [LEES] (Table A14.2)

Equipment		Failure rate (failures/10^6h)	
Compressor			
Centrifugal turbine driven	150		
Reciprocating, turbine driven	500		
Electric motor driven	100	300	
Diesel generator	125	4000	
Electricity supply	110		
Gaskets	0.02	1	
Heat exchanger	1	40	
Pipe joint	0.5		
Pumps			
• Centrifugal	10	30	80
• Boiler	100	500	
• Fire	100		
• Fuel	6	50	
• Oil lubrication	10	30	100
• Vacuum	20		
Turbine, steam	30	80	
Valves			
• Ball	1	3.5	
Butterfly	**1**	**20**	**30**
• Gate	1.5	15	
• Relief	4	9	
• Non return	2	5	
• Slam shut	10	30	
• Solenoid	1.5	10	30
Valve actuator			
• Fail open	0.1	4	
• Spurious close	5	40	

Table 16: [Lees] Table A14.4 D.J.Smith 1985

Instrument	Failure (fault/year)
Control valve	0.6
Power cylinder	0.78
Valve positioner	0.44
Solenoid valve	0.42

Instrument	Failure (fault/year)
Current/pressure transducer	0.49
Pressure measurement	1.41
Flow measurement(fluids)	1.14
Differential pressure transducer	1.73
Transmitting variable area flowmeter	1.01
Indicating variable area flowmeter	0.34
Magnetic flowmeter	2.18
Flow measurement (solids)	
Load cell	3.75
Belt speed measurement and control	15.3
Level measurement (liquids)	1.70
Differential pressure transducer	1.71
Float type level transducer	1.64
Capacitance type level transducer	0.22
Electrical conductivity probes	2.36
Level measurement (solids)	6.86
Temperature measurement (excluding pyrometers)	0.35
Thermocouple	0.52
Resistance thermometer	0.41
Mercury-in-steel thermometer	0.027
Vapour pressure bulb	0.37
Temperature transducer	0.88
Radiation pyrometer	2.17
Optical pyrometer	9.70
Controller	0.29
Pressure switch	0.34
Flow switch	1.12
Speed switch	
Monitor switch	
Flame failure detector	1.69
Millivolt-current transducer	1.67
Analyser	8.49
PH meter	5.88
Gas-liquid chromatograph	30.6
O2 analyser	5.65
CO2 analyser	10.5
H2 analyser	0.99
H2O analyser (in gases)	8

Instrument	Failure (fault/year)
Infrared liquid analyser	1.4
Electrical conductivity meter (for liquids)	16.7
Electrical conductivity meter (for water in solid)	14.2
Water hardness meter	10.9
Impulse lines	0.77
Controller settings	0.14

Table 17: Example of instrument failure rates from three chemical works (1971) [Lees] p13/20 table 13.6 (extract)

Instrument	Failure rate (faults/year)
Instrument in contact with process fluid	1.15
Pressure measurement	0.97
Level measurement	1.55
Flow measurement	1.09
Flame failure device	1.37
Instrument not in contact with process fluids	0.31
Valve positioner	0.41
Solenoid valve	0.30
Current-pressure transducer	0.54
controller	0.26
Pressure switch	0.30
Control valve	0.57
Temperature measurement	0.29

Table 18: effect of environment on instrument reliability: instrument in contact with or not in contact with process fluids. [Lees] table 13.7

The following two tables (Table 19 and Table 20) are interesting as they illustrate the importance of the working conditions of the equipment. They concern process pressure vessel failure rates for different types of industries.

As can be seen, the frequencies can vary greatly with the type of vessel, the type of process and the type of chemical environment. It is interesting to compare these values with those given for the critical events (appendix 10). Frequencies in Table 19 and Table 20 are several (two or three) orders of magnitude higher, which shows the difficulty of choosing the appropriate data for risk assessment.

Vessel	Sample size		Number of failures	Failure rate (failures/year)
	Vessels	**Vessel-years**		
Process pressure vessel	415	5535	15	2.7×10^{-3}
Pressure storage vessel	129	2220	4	1.8×10^{-3}
Heat exchanger	446	5950	10	1.7×10^{-3}
Fired heaters	36	447	181	405×10^{-3}
High temperature vessel, except fired heater	58	809	6	7.4×10^{-3}
Low temperature vessel	147	1941	3	1.5×10^{-3}

Table 19: Arulanantham and Lees 1981 (olefins plants, data gathered between 1960 and 1981) [Lees] p. 12/97

Vessel	Sample size		Number of failures	Failure rate (failure/year)
	Vessels	**Vessel-years**		
Process pressure vessel	131	1572	15	26×10^{-3}
High temperature vessels, except fired heater	16	192	7	36×10^{-3}
Vessel in corrosive duty	45	540	21	39×10^{-3}
Vessel subject to stress corrosion	49	588	12	20×10^{-3}

Table 20: same study: toxic plants [Lees] p.12/97

The following series of data concerns pipeworks failure. They perfectly well illustrate this sentence by Lees: [Lees] p.12/98: "There is a considerable amount of data available on pipework failures, but the range of values quoted tends to be confusing." They also illustrate the necessity of knowing the precise configuration of the plant, as most of these data are given in number of failures per meter and vary a lot with the diameter of the pipes.

Frequency of guillotine rupture	$= 3 \times 10^{-7}$ failure/m.year
Frequency of lesser failure	$= 3 \times 10^{-6}$ failure/m.year
Frequency of gasket failure	
Gasket 0.6 mm thick	$= 3 \times 10^{-6}$ failure/year
Gaskets 3 mm thick	$= 5 \times 10^{-6}$ failure/year
These data include valve leaks.	

Table 21: Pape and Nussey for chlorine plant [Lees] p.12/105

Purple book data on pipes [CPR]

Type of pipe	failure frequency
Diameter <=50mm	$1x10^{-10}m^{-1}h^{-1}=8.8x10^{-7}m\text{-}1y\text{-}1$
50<diameter<150mm	$3x10^{-11}m\text{-}1h\text{-}1=2.6x10\text{-}7m\text{-}1y\text{-}1$
Diameter>150mm	$1x10^{-11}m^{-1}h^{-1}=8.8x10^{-8}$

Table 22: COVO Study catastrophic rupture [CPR]

[Hu92] pipe rupture frequency

Log(failure rate per meter per year)=-(0.0064x(pipe diameter in mm)+5.56)

Diameter <=50mm	failure frequency leak=10 x rupture failure frequency
50<diameter<150mm	failure frequency leak=20 x rupture failure frequency
Diameter>150mm	failure frequency leak=30 x rupture failure frequency

Table 23: COVO study for significant leaks

[Hu92] leak failure frequency

Log(failure rate per meter per year)=-(0.026x(pipe diameter in mm)+5.32)

Pumps

Catastrophic failure of pumps : the purple book proposes the following values :

Installation (part)	Catastrophic failure	Leak
Pumps without additional provisions	1x10-4y-1	5x10-4y1
Pumps with a wrought steel containment	5x10-5y-1	2.5x10-4y-1
Canned pumps	1x10-5y-1	5x10-5y-1

Table 24: Catastrophic failure of pumps

These figures should not be mistaken with the other pumps failure rates corresponding to other failure modes.

A : Pressure storage sphere (Drysdale and David)	**Frequency/probability (per year)**
Crack in pipe	$10^{-4}/y$
Gasket failure	$5x10^{-5}/y$
Flange failure	$4x10^{-5}/y$
Valve seating failure	$3x10^{-2}/y$
Draining/sampling valve not properly shut	$10^{-4}/y$
Pipe rupture due to	

Vehicle impact	10^{-5}/y
Vibration	10^{-2}/y
Corrosion	10^{-4}/y
Repair whilst operating	10^{-4}/y
Excess pressure (blockage)	10^{-7}/y
Fatigue	10^{-4}/y
Creep	10^{-5}/y
Sabotage	$2x10^{-3}$/y
During Filling operation	
Operator fails to stop filling when correct level is reached	0.1
Operator fails to pump quickly enough when release occurs	10^{-2}
Fixed water spray inoperative because :	
Water shut off	10^{-2}
Activation fails	$2x10^{-2}$
Water frozen	$5x10^{-4}$
Pipes completely blocked	10^{-4}
Low main pressure	$3x10^{-4}$
Sprinkler system damaged	10^{-5}
Fixed water spray system ineffective because :	
Pipe partially blocked	$3x10^{-4}$
Low mains pressure	$2x10^{-3}$
Some heads blocked	$8x10^{-4}$
B : Pressure storage (Considine, Grint and Holden)	
Catastrophic failure of vessel :	
Complete failure	$3x10^{-6}$/vessel-year
Failure equivalent to 6 in nozzle	$7x10^{-6}$/vessel-year
Fracture of a 6 in. liquid line	
Pipework	$3x10^{-7}$/m-year
Equivalent failure of fittings	$5x10^{-6}$/item-year
Release due to overfilling	10^{-4}/vessel-year
Fracture of 2 in. vapour line	$3x10^{-6}$/m.year
Serious leak from equipment or pipeworks (1 kg/s)	
6 in. pipework	$6x10^{-6}$/m.year
2 in. pipework	$6x10^{-5}$/m.year
Flange	$3x10^{-4}$/flange.year
Pump seal	$5x10^{-3}$/seal.year
Release in course of draining or sampling (1.5 kg/s)	
Release per operation	10^{-4}
Draining operations	50/year

Sampling operations	100/year
Failure to recover during draining	10^{-1}
Failure to recover during sampling	10^{-2}
C : Refrigerated atmospheric storage (Considine, Grint and Holden)	
Catastrophic failure of tank	$5x10^{-6}$/tank-year
Rollover	10^{-5}/tank-year
Overfilling	10^{-4}/tank-year
Overfilling with tank failure	10^{-5}/tank-year
Overfilling without tank failure	$9x10^{-5}$/year
Fracture of a 6 in. liquid line	As section B
Leak from pipework	As section B

Table 25: Event Frequency/probability estimates given in two LPG hazard assessments (after Drysdale and David 1979/80; Considine, Grint and Holden, 1982) [Lees] (table 22.16)

Table 25 illustrates the necessity of knowing the plant configuration to be able to calculate the frequency of a critical event. In this table several frequencies are given in number of occurrence per year and per equipment (flange.year or seal.year). Depending on the number of equipment, the overall probability can change considerably.

A. Estimates used	
Coolant source/power failure	
Frequency of coolant source/power failure	0.1 failure/year
Probability that failure is sufficiently serious to give total loss of power	0.1
Probability that reactor is in critical condition	0.2
Frequency of excursion due to this cause	$0.1 \times 0.1 \times 0.2 = 2.10^{-3}$/year
Coolant pump set failure	
Frequency of pump failure (complete failure to pump)	0.1 failure/year
Assume one pump operating and one on standby	
Length of batch cycle	16h=0.00183 year
Probability of successful pump changeover	0.95
Probability of failure during batch	$1-\exp(-0.1 \times 0.00183)(1+0.95x0.1x0.00183)=9x10^{-6}$
Probability that the reactor is in critical condition	0.2
Number of cycles	250/year
Frequency of excursion due to pump set failure	$250 \times 0.2x9x10^{-6}=2.5 \times 10^{-4}$/year
Coolant turned off	
Frequency of manual isolation valve wrongly directed closed	0.05/year
Probability that operator fails to detect lack of cooling	0.01

Probability that reactor is in critical condition	0.5
Frequency of excursion due to coolant turned off	$0.05x0.01x0.5=2.5x10^{-4}$/year
Automatic control failure	
Frequency of failure of control loop in fail to danger mode	0.25 failure/year
Probability that operator fails to detect loss of control	0.01
Probability that reactor is in critical condition	0.2
Frequency of excursion due to automatic control failure	$0.25x0.01x0.2=5x10^{-4}$/year
Inadequate agitation	
Frequency of agitator failure	0.5 failure/year
Frequency of operator failure to start agitator	0.5 failure/year
Probability that agitator failure is critical	0.01
Frequency of excursion due to inadequate agitation	$(0.5+0.5)x0.01=10^{-2}$/year

Table 26: Analysis of reactor overpressure : frequency of inadequate cooling (Marrs and Lees, 1989) [Lees] (Table 11.13)

Table 26 illustrates how different frequencies and probability combine to lead to the final probability of an event (here, a reactor overpressure). These last data show the difficulty of working with the limited generic fault trees, as it clearly appears that the number of combined causes which must be taken into account to assess the probability of the events can be high.

System	Operating time	No of failures	Downtime		Availability
			Failure (h)	Planned (h)	%
Single computer system with analogue standby	66528	13	65	300	99.9
Twin computer system with analogue standby	35040	8	30.5	38	99.91
Twin computer system with shared critical loops - 1	78 888	21	172	48	99.78
Twin computer system with shares critical loops -2	78 888	37	388	73	99.5
Twin computer system with analogue standby	13 848	6	54	17	99.61

Table 27: Failure data for some process computer systems in the chemical industry [Lees] (Table A14.18)

2.7 Synthesis of the data sources analysis

Figure 9 illustrates the position of the available data on the fault tree. The red circles represent the position of absolute frequencies in the fault trees. Equipment reliability data mostly apply to specific fault trees that would be further developed from the initial generic fault trees. However, some data can be applied in the generic trees (doted circle) at the DDC (detailed direct causes) or DC level, when an equipment is explicitly involved (pumps or compressors in the overpressure scenarios).

The human reliability data could be applied at the undesirable events level as these correspond mostly to human or organisational deficiencies. In many situations it also possible to apply them directly to the DCs or DDCs when these events correspond already to human error situations.

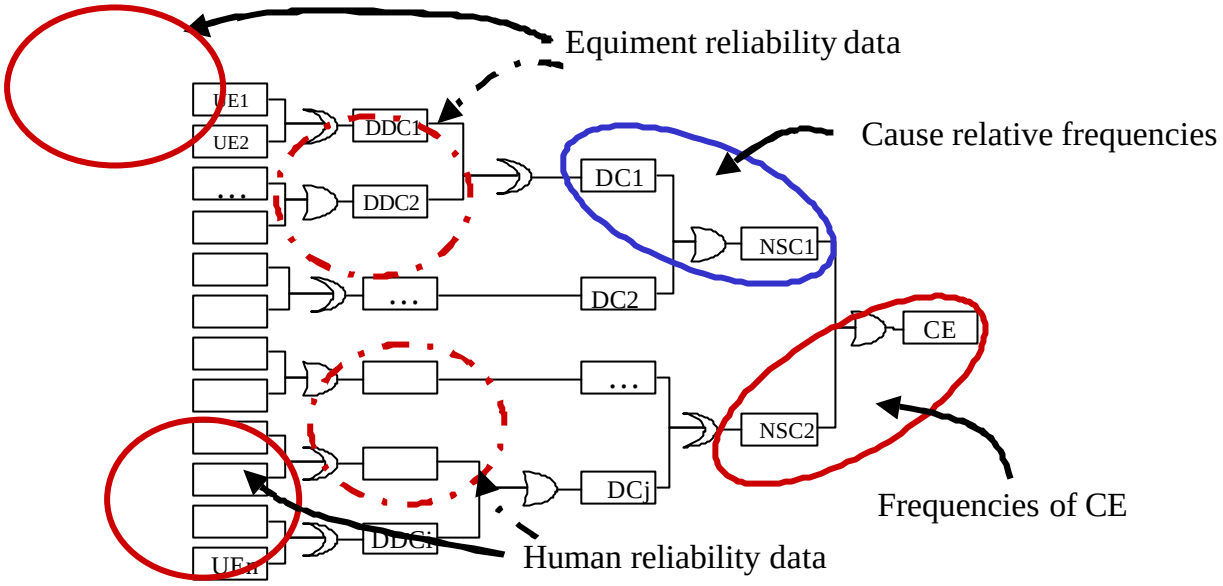


Figure 9: Position of the available data on the fault tree. Plain circles correspond to the most logical position of the data. Doted ones are alternative possibilities.

3. Some comments inspired by the Assurance Project

The ASSURANCE project [Lauridsen] was a benchmark operation aimed at comparing the risk analysis methodologies used by seven European Partners. The assurance project involved the calculation of event frequencies for a same ammonia plant using the methodologies in use in the partner countries.

The plant was originally described rather precisely with information about quantities stored and used in the process, the size and configuration of equipment. Yet, large differences were observed in the results of the frequencies of critical events. For some of the scenarios, the values calculated by the partners were varying initially by up to four orders of magnitude (Table 28).

Table 1 Frequencies of the top events of the common scenarios used by the partners (events per year)

#	Top Event*	Partner number 3	4	1	5	7	2	6	Range of deviation
1	Major ammonia leak from 8" feeding pipe	$2.1\ 10^{-4}$	$5.0\ 10^{-6}$	$9.5\ 10^{-5}$	$1.6\ 10^{-5}$	$2.0\ 10^{-5}$	$7.7\ 10^{-6}$	3	$5.0\ 10^{-6}$ - $2.1\ 10^{-4}$
2	Breakage of 4" pipe 241P-067-P1349	$3.9\ 10^{-4}$	$1.0\ 10^{-4}$	$2.0\ 10^{-4}$	$5.9\ 10^{-5}$	$7.3\ 10^{-4}$	$4.5\ 10^{-4}$	2	$5.9\ 10^{-5}$ - $7.3\ 10^{-4}$
4	Rupture or disconnection between ammonia ship and unloading arm 241-ME1	$5.8\ 10^{-4}$	$5.0\ 10^{-5}$	$4.8\ 10^{-4}$	$4.1\ 10^{-6}$	$1.0\ 10^{-5}$	$4.8\ 10^{-4}$	4	$4.1\ 10^{-6}$ - $5.8\ 10^{-4}$
7	Rupture of 10" pipe 241P-089-P1283	$4.0\ 10^{-4}$	$2.0\ 10^{-8}$	$3.9\ 10^{-8}$	$7.0\ 10^{-5}$	$1.7\ 10^{-4}$	-------	2	$2.0\ 10^{-8}$ - $4.0\ 10^{-4}$
7*	Rupture of a ship tank	$5.7\ 10^{-5}$	------	$2.3\ 10^{-7}$	$2.3\ 10^{-6}$	$4.9\ 10^{-6}$	$2.3\ 10^{-7}$	-------	$2.3\ 10^{-7}$ - $5.7\ 10^{-5}$
9	Rupture of cryogenic tank 241-S1	Contained leak: $1.0\ 10^{-6}$ Uncontain leak: $4.0\ 10^{-8}$	------	$5.0\ 10^{-7}$	$5.0\ 10^{-6}$	$5.0\ 10^{-7}$	$1.0\ 10^{-8}$	4	$1.0\ 10^{-8}$ - $1.0\ 10^{-6}$
10	Rupture of 20" pipe 241P-015-P1284	$9.0\ 10^{-4}$	$1.0\ 10^{-6}$	$7.6\ 10^{-6}$	$8.8\ 10^{-7}$	$9.7\ 10^{-7}$	$1.0\ 10^{-6}$	2	$8.7\ 10^{-7}$ - $9.0\ 10^{-5}$
14	Rupture of one of the ten pressurised tanks	$2.5\ 10^{-5}$	$5.0\ 10^{-7}$	$1.6\ 10^{-6}$	$1.3\ 10^{-5}$	$2.0\ 10^{-6}$	$5.0\ 10^{-7}$	3	$5.0\ 10^{-7}$ - $1.3\ 10^{-5}$
15	Rupture of 4" pipe on the distribution line of tank 241-V1	$2.3\ 10^{-4}$	$2.0\ 10^{-5}$	$6.0\ 10^{-5}$	$1.1\ 10^{-5}$	$4.9\ 10^{-5}$	$3.4\ 10^{-8}$	2	$3.4\ 10^{-8}$ - $2.3\ 10^{-4}$
17	Rupture or disconnection between ammonia truck and unloading arm	$3.7\ 10^{-4}$	$6.0\ 10^{-5}$	$4.7\ 10^{-6}$	$6.8\ 10^{-5}$	$1.0\ 10^{-6}$	$1.5\ 10^{-7}$	1	$1.5\ 10^{-7}$ - $3.7\ 10^{-4}$
18	Catastrophic rupture of a truck tank	$2.3\ 10^{-7}$	$1.2\ 10^{-7}$	$1.1\ 10^{-8}$	$7.4\ 10^{-10}$	$2.7\ 10^{-8}$	$1.5\ 10^{-10}$	1-2	$1.5\ 10^{-10}$ - $2.3\ 10^{-7}$

* Grey tanned cells contain the lower assessments. Black tanned cells contain the upper assessments

Table 28: Frequencies of the top events of the common scenarios used by the partners (events per year) in the ASSURANCE project

An analysis was made of the causes of deviation. For this purpose, the scenarios were grouped into three sets: scenarios related to (1) pipelines, (2) loading arms, and (3) tanks.

The following possible causes of uncertainty have been considered:

(1) scenarios related to pipelines

1. Length of a pipeline to be analysed
2. Utilisation factor (fraction of time when a pipeline is in use)
3. Including piping-related components (flanges, valves and pumps)
4. Failure causes considered:
    1. Mechanical
    2. Overpressure
    3. External impact

(2) scenarios related to loading arms

1. Number of transhipments
2. Failure causes considered:
    1. Mechanical
    2. Overpressure
    3. Other (e.g. "excessive movement of the arm, leading to its rupture")

(3) scenarios related to tanks

1. Failure causes considered:

    1. Mechanical

    2. Overpressure

    3. Other (e.g. fires and explosions)

After this analysis, characteristics common for all the partners were defined such as the length of the pipes to be analysed, the utilisation factor or the number of transhipments.

Once these precision were incorporated to the initial data, the calculation were performed again. The results were closer, even if the deviation could still reach three orders of magnitude for various top events (Table 29).

Table 5 Recalculated frequencies according to the assumptions common for all research teams

		Partner number							
#	Top Event*	3	4	1	5	7	2	6	Range of deviation
1	Major ammonia leak from 8" feeding pipe	$4.6\ 10^{-6}$	$9.0\ 10^{-7}$	$9.0\ 10^{-7}$	$1.0\ 10^{-6}$	$1.8\ 10^{-7}$	$9.0\ 10^{-7}$	3	$1.8\ 10^{-7}$ - 4.6×10^{-6}
2	Breakage of 4" pipe 241P-067-P1349	$1.4\ 10^{-5}$	$9.0\ 10^{-7}$	$1.0\ 10^{-5}$	$7.3\ 10^{-7}$	$4.6\ 10^{-6}$	$2.7\ 10^{-6}$	2	$7.3\ 10^{-7}$ - $1.4\ 10^{-5}$
4	Rupture or disconnection between ammonia ship and unloading arm 241-ME1	$8.0\ 10^{-3}$	$5.0\ 10^{-3}$	$4.8\ 10^{-4}$	$5.4\ 10^{-1}$	$1.3\ 10^{-5}$	$4.8\ 10^{-4}$	4	$1.3\ 10^{-5}$ - $8.0\ 10^{-3}$
7	Rupture of 10" pipe 241P-089-P1283	$4.6\ 10^{-6}$	$9.0\ 10^{-7}$	$1.0\ 10^{-6}$	$8.0\ 10^{-7}$	$1.8\ 10^{-6}$	-------	2	$8.0\ 10^{-7}$ - $4.6\ 10^{-6}$
7*	Rupture of a ship tank	$5.7\ 10^{-3}$	------	$2.3\ 10^{-7}$	$2.3\ 10^{-6}$	$4.9\ 10^{-6}$	$2.3\ 10^{-7}$	------	$2.3\ 10^{-7}$ - $5.7\ 10^{-3}$
9	Rupture of cryogenic tank 241-S1	$4.0\ 10^{-8}$	------	$5.0\ 10^{-7}$	$5.0\ 10^{-8}$	$5.0\ 10^{-7}$	$1.0\ 10^{-8}$	4	$1.0\ 10^{-8}$ - $5.0\ 10^{-7}$
10	Rupture of 20" pipe 241P-015-P1284	$5.0\ 10^{-6}$	$9.0\ 10^{-7}$	$6.0\ 10^{-6}$	$4.0\ 10^{-1}$	$4.0\ 10^{-7}$	$1.0\ 10^{-6}$	2	$4.0\ 10^{-7}$ - $6.0\ 10^{-6}$
14	Rupture of one of the ten pressurised tanks	$1.0\ 10^{-6}$	$4.5\ 10^{-7}$	$1.0\ 10^{-6}$	$1.3\ 10^{-6}$	$4.0\ 10^{-7}$	$1.0\ 10^{-6}$	3	$4.5\ 10^{-7}$ - $1.3\ 10^{-6}$
15	Rupture of 4" pipe on the distribution line of tank 241-V1	$1.5\ 10^{-5}$	$9.0\ 10^{-7}$	$5.0\ 10^{-6}$	$2.2\ 10^{-6}$	$8.0\ 10^{-7}$	$3.4\ 10^{-7}$	2	$3.4\ 10^{-7}$ - $1.5\ 10^{-5}$
17	Rupture or disconnection between ammonia truck and unloading arm	$2.1\ 10^{-3}$	$2.7\ 10^{-6}$	$2.4\ 10^{-6}$	$6.0\ 10^{-6}$	$5.0\ 10^{-3}$	$1.5\ 10^{-7}$	1	$1.5\ 10^{-7}$ - $2.1\ 10^{-3}$
18	Catastrophic rupture of a truck tank	$1.2\ 10^{-3}$	$1.2\ 10^{-3}$	$5.5\ 10^{-4}$	$4.7\ 10^{-6}$	$1.4\ 10^{-8}$	$1.5\ 10^{-8}$	1-2	$1.5\ 10^{-8}$ - $4.7\ 10^{-6}$

• Grey tanned cells contain the lower assessments. Black tanned cells contain the upper assessments
* More detailed definition of top events for the common scenarios can be found in ANNEX 1

Table 29: recalculated frequencies according to the assumptions common to all research teams in the ASSURANCE project

This project shows the difficulty of getting significant and reliable values when evaluating frequencies. It also shows the importance of the precise description of the plant, of its components and of its functioning. It is clear that using short generic fault trees with generic data is a major difficulty and that the results which could be obtained this way would probably not have much meaning. Yet, the following section attempts to propose some solution for the calculation of probabilities.

4. Proposal of a method for evaluating the frequency of the critical event

The method retained by the ARAMIS project is based on the barrier approach. In other words, the scenarios are quantified by applying the barrier failure rates to an initial failure probability. This approach should reduce the stress on the frequency evaluation. Yet, it is necessary to provide some type of initial evaluation of the frequency (probability) to be able to calculate the final critical event frequency. As the preceding considerations have shown it is not easy to derive frequency (probability) values from the data source available. Yet, some type of quantification is desired. The following solutions can be proposed.

As was already discussed, the main difficulty resides in the generic character of the fault trees and the appropriateness and validity of the failure data.

- Generic fault trees do not make a sufficient description of the failure modes and do not allow to take explicitly the number of components, the time of use, the number of demands into account.
- The failure data do not correspond to the events described in the event tree. They were derived from ancient studies and may not reflect the present state of the art.

To overcome these difficulties the following recommendations can be made.

- Detailed specific fault trees should always be preferred to generic fault trees as they allow a more precise description of the equipment and the failure modes. These detailed specific fault trees should be build, when possible, by developing the generic fault trees provided by MIMAH. In many plants, reliability analysis have been made and could be used as a reliable source to implement the probability analysis.
- When possible, plant specific data should be preferred to generic frequencies as the later reflect average behaviour of components which can be fairly different from those observed in the plant concerned by the study. The next section provides some useful data. When these cannot be used, the very coarse generic data given bellow can be adopted for an initial study.

	Plant specific data	Generic data
Detailed fault trees	Use plant specific data and detailed fault trees	Use generic data with detailed fault trees
Generic fault trees	Use plant specific data with generic fault trees	Use generic data with generic fault trees

Table 30: preferred data sources and methods for risk analysis

Chapter 7 of the present document proposes some failure rates for different types of components which could be used for the calculation of the failure probabilities provided that the fault trees be developed further sufficiently to make these components appear.

Table 31 and Figure 10 provide even more generic data. Whatever the data used, it is also necessary to apply them to the number of components susceptible to fail.

Item	Failure Rates (on demand)
People	10^{-2} per operation
Mechanical systems	10^{-3} per operation
Electrical systems	10^{-4} per operation

Table 31: Generic Failure Rates

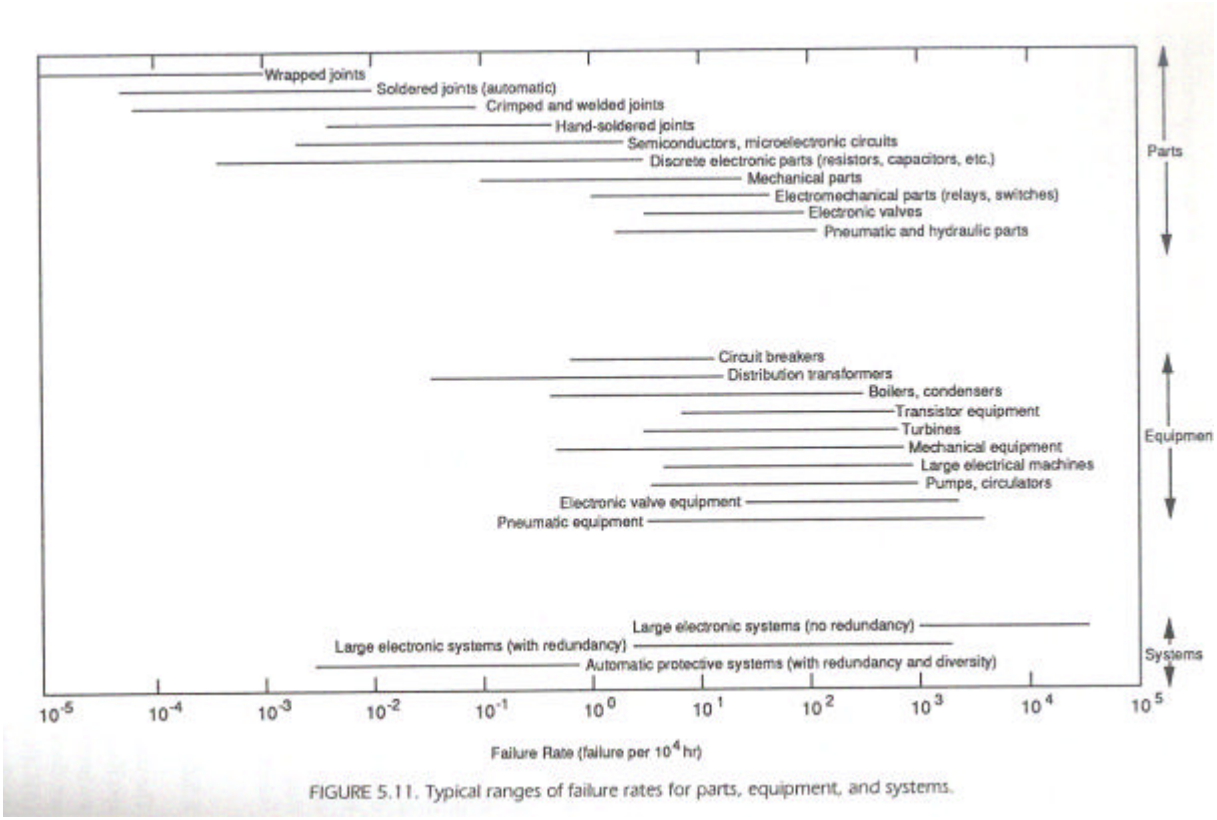


Figure 10: Typical ranges of failure rates for parts, equipment and systems (CCPS guidelines)

An attempt was made to introduce data into the generic fault trees (see tables at the end of chapter 7). The data correspond as much as possible to a "no barrier" situation, even if this criterion is not always easy to warrant.

In fact different situations were distinguished :

- **Component failure** : In such a situation, the component failure rate should be applied, if it can be found in the reliability databases. Of course, this failure rate can be increased by local conditions (corrosive environment,…). Distinction has to be made between failure in time and failure on demand. In this second situation, the number of component solicitation must be known. In any case, the number of components susceptible to fail and their configuration (series or parallel) should be known and taken into account to calculate the resulting frequency. **As it is not possible to reproduce entire databases such as the OREDA**

handbook, the CCPS guideline ranges given by Figure 10 were used in the fault trees.

- **Hazardous operation** : these are operations which should always result into a hazardous phenomenon, such as manipulating hazardous chemicals. In such situations, the frequency of hazardous event is that of the operations reduced by the provisions taken to reduce the risk. **In other words, the frequency without barriers is that of the operations. No data was introduced in the fault trees in this case. The value to be used is the plant specific frequency of operation.**

- **Human error** : the general comments about human reliability given above show that it is not recommendable to use single generic data to estimate the human error failure rate. Human reliability depends a lot on the context and the type of operations performed by the operators. **But, in a first approximation, conservative values can be used such as 10^{-1}/operation (it should be reminded that this value is taken before taking into account the safety barriers, this means that no training or work procedures are considered).** The frequency of the dread event (resulting from the error) is given by the product of the probability of human error by the frequency of the considered human operation (opening of a valve, for example).

- **External hazard** : such as earthquake, domino effects or weather conditions. In this case, the local data should be obtained from the competent authorities and used directly. Earthquake and lightening data issued from the HSE safety report assessment guide were introduced in the tree but they should be used very carefully as they correspond to the situation in England.

- **Continuous degradation leading to failure** : these include corrosion, erosion, and other mechanical failure. Whereas many absolute failure data are available for equipment failure, much less are available for these direct causes which appear in accident databases with high relative frequencies. In this case, the very few available data ($8x10^{-7}$ to 10^{-4}/h for corrosion in the I-Risk project database) were used as reference data and the other figures were derived from this initial data by applying relative distribution figures. However, the meaning of these is not clear, as it seems obvious that the probability of failure by corrosion or erosion must be somehow related with the length or surface of the concerned equipment. No figures could be found linking the different failure modes (corrosion, erosion, fatigue…) and the length of pipes, for example.

5. Conclusion

The objectives of this ARAMIS step was to produce a method and data to calculate the critical event frequencies which would be compatible with the elements of the method already developed, the generic fault trees, and those being developed by other partners, the safety barrier requirements approach.

For this purpose, a typology of data sources was made. These can mostly be divided into

- Reliability databases concerning mostly equipment failures

- Human reliability data
- Accident databases (relative distributions of causes)
- Scattered absolute and relative frequencies which can be found in very diverse literature references. These include frequencies of the critical events and some more scarce frequencies of intermediate events (NSC, DC or DDC in the fault trees).

The limits of each data type were underlined with respect to the ARAMIS methodology. These limits concern both the data themselves and their applicability to the structure of the generic fault trees.

As far as the data are concerned, and excluding, maybe, the reliability databases which are updated regularly, but are not easily accessible, it is difficult to know how accurate and reliable they are. The conditions and time of the initial collection are seldom known, which makes their use as generic data delicate.

But it is also the generic nature of the fault trees which makes the assessment of the critical events frequencies difficult. For many events it is necessary to have more information on the plant configuration and operating conditions to calculate their frequency (probability). This is particularly true when on demand failure rates are involved.

Yet, it was necessary to provide some guidelines for the assessment of the frequencies (probabilities). This was done by making some recommendations which include the development of specific fault trees on the basis of the generic fault trees provided in the ARAMIS methodology and the use of plant specific data when available. When such data are not available, generic ones must be used. Orders of magnitude of such data were introduced in the fault trees. Most of them are based on a combined use of absolute frequencies, when available and relative distribution of causes.

Even if some results were obtained, this part of ARAMIS shows that the lack of reliable data and coupling between the data and the generic fault trees is a major difficulty. This should suggest to the project partners to propose an European data collection program which would result into a truly ARAMIS compatible database.

6. References

6.1 ARAMIS Documents

[Delvosalle MOOA] C. Delvosalle, C. Fiévez, A. Pipart, C. Kirchsteiger, F. Mushtaq, J. Casal Fabrega, Dr. E. Planas, PART 2 OF DELIVERABLE D.1.A. MOOA - MOST OFTEN OBSERVED ACCIDENTS WP 1/A

[Delvosalle WP1D] C. Delvosalle, C. Fiévez, A. Pipart, Methodology for the Identification of Reference Accident Scenarios, WP1D

[Delvosalle WP1C] C. Delvosalle, C. Fiévez, A. Pipart, Frequencies and probabilities on the event tree, Characteristics of critical events, WP 1C

[Fiévez WP1C] C. Fievez, A.Pipart, Intermediate report on the WP1C, ARAMIS

6.2 Other documents

[Akhmetjanov] Farit M. Akhmetjanov, Reliability databases : state of the art and perspectives : Risoe report Risoe –R- 1235 EN

[Bellamy] L.J. Bellamy, T.A.W. Geyer and J.A. Astley, Evaluation of the human contribution to pipework and in-line equipment failure frequencies, HSE contract research report n°15/1989

[Barton] J. Barton, R. Rogers, Chemical reaction hazards, Ichem E, Rugby, 1993,184 p.

[CCPS] Guidelines for Chemical Process Quantitative Risk Analysis, Second Edition, Center for Chemical Process Safety, American institute of chemical engineers, New-York, 2000

[CPR] Guidelines for quantitative risk assessment, purple book, CPR 18E, Committee for the prevention of disasters, Sdu Uitgevers, Den Haag, 1999

[Fragola] J.R. Fragola Human reliability analysis procedure, ESREL 2001, Safety and reliability, proceedings of the european conference on safety and reliability, ESREL 2001, tutorial notes, ed: Politecnico di Torino, 2001, pp.107-142

[Giovannini] Création d'un pôle de compétences sur l'évaluation de la sécurité des procédés chimiques (DRA-005) RAPPORT INTERMEDIAIRE D'OPERATION, Guide méthodologique d'évaluation des dangers liés à la mise en oeuvre de réactions chimiques *B. GIOVANNINI* Juin 2001, available at www.ineris.fr

[HOURTOLOU] *D. HOURTOLOU,* Analyse des risques et prévention des accidents majeurs (DRA-007), Rapport final – Opération ASSURANCE, ASSessment of the Uncertainties in Risk Analysis of Chemical Establishments, Projet U.E. ENV4-CT97-0627 available on (www.ineris.fr)

[HSE] HID - SAFETY REPORT ASSESSMENT GUIDES :

http://www.hse.gov.uk/comah/index.htm, **links to**

- Safety Report Assessment Guide : Chlorine
- Safety Report Assessment Guide : Chemical Warehouses
- Safety Report Assessment Guide : LPG
- Safety Report Assessment Guide : HFL
- Safety Report Assessment Guide : Methane Gas Bullets
- Safety Report Assessment Guide : Methane Gas Holders
- Safety Report Assessment Guide : Whiskey Maturation Warehouse

[IchmE] The Accident Database Version 4.1, Institution of Chemical Engineers, Rugby, UK

[I-RISK] I-RISK Project : ANNEX IV.1, QUANTIFICATION: DATABASE MAY 1999

[Lauridsen] Assessing the uncertainties in the process of risk analysis of chemical establishments: part I, *Kurt Lauridsen, Michalis Christou, Aniello Amendola, Frank Markert, Igor Kozine, Monica Fiori available at : http://mahbsrv.jrc.it/antwerp/docs%5CLauridsen.pdf*

[Lees] Franck P. Lees, *Loss prevention in the process industry*, London: Butterworths, 1986

[OREDA] Offshore Reliability Data Handbook, 1997, *Det Norske Veritas*

[Piccini] Human Factors In The Design Process Of Advanced Supervisory And Control Systems**,** Piccini M. and Carpignano A., Politecnico di Torino – Dipartimento di Energetica, C.so Duca degli Abruzzi 24, 10129 Torino, Italy,

[R2A] http://www.r2a.com.au/publications/4th_Edition/4th_edition.html

[RIVM 1] RIVM Report 610066015 Benchmark risk analysis models

[RIVM 2] Report 610066014 A method to judge the internal risk of establishments with dangerous substances

[Tucci] Human reliability analysis to high-risk industries: the case of process chemical industry for the polyethylene production. Prof. Mario Tucci, Ing. Lorenzo Giagnoni, Ing. Irene Cappelli

[Villemeur] Alain Villemeur, "Sureté de fonctionnement des systèmes industriels, fiabilité, facteurs humains, informatisation », Eyrolles, PARIS, 1988, 798 p.

7. Additional data

7.1 HSE reference failure frequencies

Event	**Probability/Frequency**
High pressurise gas transmission line rupture	5×10^{-4}/km.yr
Lightning strike	1×10^{-7}/yr
Severe earthquake capable of rupturing pipework	1×10^{-6}/yr - 1×10^{-7}/yr
Seal Fire	approx. 2×10^{-4}/holder.yr
Failure of a ROSOV on demand	$3 \times 10^{-2/yr}$
Failure of an excess flow control valve on demand	1.3×10^{-2}/yr
Failure of an automatic shutoff valve to close	1×10^{-2}/demand
Failure of a level sensor (sticking)	50 per 10^{-6} hrs
Split Crown (without ignition)	Approx. 3×10^{-4}/holder.yr
Split crown explosions	< 3 x 10-5/holder.yr
Rupture of pipe on a pressurised storage system	1×10^{-5}/yr
Sudden catastrophic failure of vessels	3×10^{-6}/yr
Failure of a flow sensor	40 per 10^{-6} hrs
Export/Import line failure	5×10^{-4}/km.yr
High pressurise gas transmission line rupture	5×10^{-4}/km.yr
Failure rate of small bore gas pipework	6×10^{-5}/m
Frequency of sparking of zone 1 equipment	1×10^{-4}/item
Seal Fire	approx. 2×10^{-4}/holder.yr
Split Crown (without ignition)	Approx. 3×10^{-4}/holder.yr
Split crown explosions	< 3 x 10-5/holder.yr

Table 32: General summary of HSE data from HID - safety report assessment guides : [HSE]

7.2 I-Risk

The failure rates are expressed as number of failures per hour or per demand [I-Risk]

Table 33: database developed in the framework of the I-Risk project

	EQUIPMENT	PARAMETER	Good Management	Generic Plant	Poor Management	Comments	Use for I-Risk Technical Model?
1	Safety valves, remote control valves	Time for repair (Tr) (hr)	1	1,5	8	OREDA data.Does not include: isolation time, waiting time, detection time	NO
2	Safety valves, remote control valves	Time for repair (Tr) and Time for maintenance (Tm) (hrs)	24	168	1176	DEMOKRITOS judgement.	YES
3	Safety valves, remote control valves	T (inspection interval)	Plant data x 0.9	Plant data	Plant data x 5	DEMOKRITOS judgement.	YES
4	Safety valves, remote control valves	Lambda (failure rate)	1,71E-06	1,25E-05	3,15E-05	OREDA, page 492	YES
5	Safety valves, remote control valves	Qm1 (error in maintenance)	1,00E-03	0,01	0,1	Expert judgement based on generic data according to SAVE's suggestions	YES
6	Safety valves, remote control valves	Qm2 (error recovery failure by independent check)	0,05	1,00E-01	1	SAVE/RIVM judgement based on generic data	YES
7	Safety valves fail in open position	Lambda (failure rate)	8,50E-07	1,17E-05	3,40E-05	OREDA, p. 492	
8	Manual valves	Lambda (failure rate)	2,736E-07	1,9952E-06	5,0416E-06	OREDA page 493 All caused by seals (x 0.16 of safety valve failure values)	YES
9	Manual valves	Qm1	1,00E-03	1,00E-02	0,1	DEMOKRITOS judgement.	YES
10	Manual valves	Other parameters = Tr, Tm, T, Qm2 (not failure rate or Qm1)	Same as for safety valves	Same as for safety valves	Same as for safety valves	Same as for safety valves	YES
11	Flow instruments	Lambda(failure rate)	8,30E-07	2,76E-06	5,59E-06	OREDA page 325	YES

	EQUIPMENT	PARAMETER	Good Management	Generic Plant	Poor Management	Comments	Use for I-Risk Technical Model?
12	Flow instruments	Time for repair (Tr) (hr)	0,2	0,6	2	OREDA data page 325 Does not include: isolation time, waiting time, detection time	NO
13	Flow instruments	Time for repair (Tr) and Time for maintenance (Tm) (hrs)	24	168	336	SAVE/RIVM expert judgement to account for what OREDA leaves out and using Test Case B as benchmark for good.	YES
14	Instruments where have to take equipment apart for repair	Time for repair (Tr) and Time for maintenance (Tm) (hrs)	24	168	720	DEMOKRITOS judgement.	YES
15	Level instrument	l (failure rate)	2,50E-06	6,09E-06	1,10E-05	OREDA page 329	YES
16	Pressure instrument	l (failure rate)	2,50E-07	1,27E-06	2,94E-06	OREDA page 332	YES
17	Temperature instrument	l (failure rate)	3,00E-08	7,73E-06	2,97E-05	OREDA page 338	YES
18	Instruments easy maintenance	Qm1	5,00E-04	5,00E-03	5,00E-02	DEMOKRITOS judgement.	YES
19	Process pump (666 lb)	l (failure rate)	4,50E-05	1,21E-04	2,28E-04	OREDA page 115	YES
20	Process pump	Tr Time for repair (hrs)	2	24	168	OREDA data, page 115 Does not include: isolation time, waiting time, detection time	NO
21	Process pump	Time for repair (Tr) and Time for maintenance (Tm) (hrs)	24	168	720	DEMOKRITOS judgement.	YES
22	Human Error	Qo1	1,00E-03	1,00E-02	1,00E-01	DEMOKRITOS judgement.	YES
23	Human Error	Qo2	5,00E-02	1,00E-01	1,00E+00	DEMOKRITOS judgement.	YES
22	Compressor fails while running (reciprocating)	l (failure rate)	6,40E-05	6,10E-04	1,63E-03	OREDA p.65	YES

	EQUIPMENT	PARAMETER	Good Management	Generic Plant	Poor Management	Comments	Use for I-Risk Technical Model?
23	Compressor fails (critical, reciprocating)	l (failure rate)	1,56E-04	1,44E-03	3,82E-03	OREDA p.65	YES
24	Compressor fails owing to vibration (reciprocating)	l (failure rate)	9,00E-08	2,30E-05	8,70E-05	OREDA p.65	YES
25	Compressor fails, low gas flow (reciprocating)	l (failure rate)	2,00E-06	1,01E-04	3,60E-04	OREDA p.65	YES
26	Compressor fails, low gas flow (reciprocating)	Tr Time for repair	4	32	98	OREDA p.65	YES
27	Compressor fails (centifugal)	l (failure rate)	6,70E-05	3,93E-04	9,41E-04	OREDA, p.52	YES
28	Compressor (reciprocating)	Tr Time for repair	1	70	5462	OREDA p.65	YES
29	Compressor fails (centrifugal)	Tr Time for repair	0,5	47	1749	OREDA, p.52	YES
30	Ammonia pump (critical)	l (failure rate)	1,21E-05	1,06E-04	2,77E-04	OREDA, p.107	YES
31	Ammonia pump (vibration)	l (failure rate)	4,60E-07	6,00E-06	1,60E-05	OREDA, p.107	YES
32	Ammonia pump	Tr Time for repair	0,5	41	537	OREDA, p.107	YES
33	Ammonia pump, other modes	l (failure rate)	3,00E-08	6,00E-06	2,40E-05	OREDA, p.107	YES
34	Oil pump (critical)	l (failure rate)	2,10E-05	1,27E-04	3,07E-04	OREDA, p.125	YES
35	Oil pump (fail while running)	l (failure rate)	8,00E-06	8,20E-05	2,24E-04	OREDA, p.125	YES
36	Leak of Oil pump	l (failure rate)	3,00E-06	1,00E-05	2,10E-05	OREDA, p.125	YES
37	Oil pump	Tr Time for repair	0,5	39	502	OREDA, p.125	YES
38	Spurious operation of control valve	l (failure rate)	4,00E-08	1,52E-06	5,26E-06	OREDA, p.345	YES
39	Spurious operation of control valve	Tr Time for repair	0,2	1,9	8	OREDA, p.345	YES
40	Control valve fails to open	l (failure rate)	1,10E-07	1,96E-06	4,79E-06	OREDA, p.345	YES
41	Control valve fails to open	Tr Time for repair	2	14	58	OREDA, p.345	YES

	EQUIPMENT	PARAMETER	Good Management	Generic Plant	Poor Management	Comments	Use for I-Risk Technical Model?
42	Control valve fails to close	l (failure rate)	4,00E-07	2,90E-06	7,40E-06	OREDA, p.345	YES
43	Control valve fails to close	Tr Time for repair	2	18	96	OREDA, p.345	YES
44	Other process sensors	l (failure rate)	8,70E-07	2,43E-06	4,62E-06	OREDA, p.322	YES
45	Other process sensors	Tr Time for repair	2	7	36	OREDA, p.322	YES
46	Controller	l (failure rate)	4,10E-05	1,29E-04	2,55E-04	OREDA, p.266	YES
47	Controller	Tr Time for repair	0,2	3,4	42	OREDA, p.266	YES
48	Electric generators	l (failure rate)	1,20E-05	1,44E-04	4,07E-04	OREDA, p.155	YES
49	Electric generators	Tr Time for repair	0,5	15	1404	OREDA, p.155	YES
50	Fire fighting system	l (failure rate)	1,20E-05	2,10E-05	3,10E-05	OREDA 92, p.441	YES
51	Fire fighting system	Tr Time for repair		8,5		OREDA 92, p.441	YES
52	BATTERY CHARGER FAILS	l (failure rate)	3,00E-07	6,00E-07	4,00E-06	IAEA (BCAFB)	YES
53	RECTIFIER MECH. FAILURE	l (failure rate)	3,20E-07	1,30E-06	3,60E-06	IAEA (EREFE)	YES
54	FUSE FAILS OPEN	l (failure rate)	6,00E-08	3,00E-06	2,00E-05	IAEA (KTAKB)	YES
55	SWITCH FAILS OPEN	l (failure rate)	2,00E-10	1,80E-07	4,20E-07	IAEA (KDCDO)	YES
56	SHORT CIRCUIT IN BUS	l (failure rate)	1,00E-09	1,00E-08	1,00E-07	DEMOKRITOS judgement	YES
57	TRANSFORMER FAILS OPEN	l (failure rate)	3,00E-07	6,00E-07	4,00E-06	IAEA (TAAAB)	YES
58	STRAINER IN COMPRESSOR BLOCKS	l (failure rate)	6,00E-07	3,00E-05	3,00E-05	IAEA (YSFQB)	YES
59	LOSS OF OFFSITE POWER	Fi	1,00E-07	1,40E-06	1,00E-05	DEMOKRITOS judgement	YES
60	EXTERNAL FIRE	fi	6,00E-07	6,3E-06	1,00E-05	DEMOKRITOS judgement	YES
61	LOSS OF OFFSITE WATER	fi	1,00E-08	1,0E-07	1,00E-06	judgement	YES

	EQUIPMENT	PARAMETER	Good Management	Generic Plant	Poor Management	Comments	Use for I-Risk Technical Model?
62	LEVEL RISE	fi	1,00E-05	3,7E-04	1,00E-04	DEMOKRITOS judgement	YES
63	TEMPERATURE RISE, LOADING	fi	1,00E-06	6,3E-06	1,00E-05	DEMOKRITOS judgement	YES
64	TEMPERATURE RISE, UNLOADING	fi	1,00E-06	1,0E-05	1,00E-04	DEMOKRITOS judgement	YES
65	LOW LEVEL IN TANK	fi	1,00E-06	1,0E-05	1,00E-04	DEMOKRITOS judgement	YES
66	HOT AMMONIA ENTERS THE TANK	fi	1,00E-06	1,9E-05	1,00E-04	DEMOKRITOS judgement	YES
67	CORROSION IN PIPING	fi	1,00E-06	1,9E-05	1,00E-04	DEMOKRITOS judgement	YES
68	BATTERY UNAVAILABLE	l (failure rate)	8,00E-07	2,00E-06	1,00E-05	IAEA (BTWFB)	YES
69	BATTERY UNAVAILABLE	Tr Time for repair	4		7	IAEA (BTABN)	YES
70	NO SYCHRG	l (failure rate)	8,00E-07	2,00E-06	1,00E-05	DEMOKRITOS judgement	YES
71	NO SYCHRG	Tr Time for repair	4	5	7	DEMOKRITOS judgement	YES
72	Water fire fighting pump	l (failure rate)	2,00E-04	3,17E-04	4,70E-04	OREDA, p.119	YES
73	Water fire fighting pump	Tr Time for repair	1	18	60	OREDA, p.119	NO
74	Water fire fighting pump	Tr Time for repair	24	168	8760	DEMOKRITOS judgement	YES
75	Electric ignition failure	l (failure rate)	3,00E-07	1,00E-06	3,00E-06	IAEA (KTAKW)	YES
76	IGNITION FAILURE OF FLARE	Tr Time for repair	24	168	8760	DEMOKRITOS judgement	YES
77	FLARE UNAVAILABLE	Tr Time for repair	24	168	8760	DEMOKRITOS judgement	YES
78	Flare fails to start	l (failure rate)	2,00E-07	1,00E-06	5,00E-05	IAEA (QDAFB)	YES
79	All comps	fm		1,16E-03		ACTUAL DATA FROM INDUSTRY	YES
80	All comps	Tm		8		ACTUAL DATA FROM INDUSTRY	YES