Risk analysis of a distillation unit

Forskningscenter Risø, Roskilde; Hansen, O.; Jensen, C.; Jacobsen, O.F.; Justesen, M.; Kjærgaard, S.

Publication date:
1982

Document Version
Publisher's PDF, also known as Version of record

RISØ-M-2319

RISK ANALYSIS OF A DISTILLATION UNIT

J. R. Taylor**, O. Hansen*, C. Jensen*,
O. F. Jacobsen*, M. Justesen**, S. Kjærgaard*

* Grindsted Products A/S
** Risø National Laboratory

Abstract. A risk analysis of a batch distillation unit is described. The analysis has been carried out at several stages during plant design, construction, and operation. The costs, quality, and benefits is using the methods are described.

UDC 614.8:66.048:661.721

March, 1982
Risø National Laboratory, DK 4000 Roskilde, Denmark

ISBN 87-550-0806-2
ISSN 0418-6435

Risø Repro 1982

CONTENTS Page

1.1 Introduction

This report gives an interim account of the risk analysis work carried out during the design and construction of a methanol-/organic product batch distillation unit. The report is made immediately after commissioning of the unit and must therefore be regarded as an interim report. The success or otherwise of the risk analysis can only really be judged after several years operation. Furthermore, there are some analyses which could not be carried out prior to commissioning (for lack of information) and also some comparison analyses outstanding. For these reasons, we have called this a "Half Term Report".

The results presented here cover the plant to be analyzed, the risk analysis methods used, experience of application of the methods, and a provisonal evaluation of the results.

1.2 Objectives and organisation

The objectives of this analysis were threefold

- to provide a "safe" design basis for a new organic product/methanol batch distillation unit of circa 5.000 l. capacity.

- To illustrate the use of risk analysis techniques and demonstrate their application throughout the design and construction of the plant.

- To investigate the effectiveness of various risk analysis methods in an industrial context, and gather basis information which would allow a cost/benefit optimisation of risk analysis procedures.

In order to fulfill the last of these objectives it was nescessary to use alternative methods and variations of methods. The analyses were also carried to a level of detail which would perhaps not be justified in normal industrial routine. The procedures to be used were rigidly defined (see 1) in order that the experiment should be well controlled.

The analyses were carried out as a close co-operation between Grindsted Products A/S and Risø National Laboratory. Orla Hansen was the project engineer for the distillation unit during the project having responsibility for overall design including safety design. The writer was project leader for the risk analysis, reporting in a consulting capacity to O. Hansen. C. Jensen was (and is) the plant safety officer. O. F. Jacobsen and M. Justesen were responsible for specific aspects of the risk analysis. S. Kjærsgaard was leader of the plant development department, and provided overall guidance during the risk analysis project.

In practice, a good deal of the work took place in closely working committees or "brainstorming groups". As a result it is difficult to say how the analysis work was apportioned, or "who did what". The result must be regarded as a group effort.

1.2.2. Philosophy and Approach

(This section represents the views of the editor, which are not nescessarily shared by other members of the project. The ideas presented here provided the basis for selection of the risk analysis methods used.)

The objective of risk analysis carried out during design is to produce a plant which is as safe as is practically possible. This may, in some instances, involve balancing the costs of safety equipment against the probability of failure. But for the most part, such questions are decided as a result of legal and standards requirements, such that an optimum safety level

for fitting of safety equipment is already achieved. The role of risk analysis then becomes one of finding risk sources, ensuring that for each risk source appropriate safety measures have been used and appropriate standards applied, and of finding errors in the design.

The approach taken has, then, been to use methods which give as thorough as possible an identification of possible design errors and sources of risk. The methods have been applied at as early a stage of design as possible, and different methods appropriate to each stage of the design have been applied.

Adopting this approach to risk analysis, a very important measure of success is that of completeness. Completeness can be defined either as

> "the proportion of potential risk sources found by the analysis" (measure 1)

or

> "the proportion of the actual risk, measured as expected loss, found by the analysis". (measure 2)

Calculating a measure of completeness directly to some extent begs the question, since it requires that the potential risk be known completely. There are several ways to get over this problem. One is to develop methods which, within certain well defined limits, perform a complete analysis. This can be done for example for plant disturbances recorded in terms of variations in thermodynamic variables describing the state of the plant. A complete analysis can then be built up automatically (See 1). Another example is operator error modes. A complete list of potential error modes can be built up, since the number of possible operator interactions with the plant is limited. Given a complete analysis derived by one method, completeness of another method can be determined by comparing the two.

Another way of determining completeness is to compare the results of the analysis with a set of case stories from similar

plant, and to then see if, on the basis of the case stories, the analysis can be extended.

A third way of checking completeness is to compare the results of an analysis with the actual experience in operating the plant.

All three approaches have been taken in this report.

Given a strong emphasis on completeness in identification of risks, another important parameter is discrimination. This can be defined as

> "The proportion of identified potential risk sources which subsequently proved to be actual risk sources".

The problem here is that it may be fairly easy to identify a large number of possible risk sources, if the only statement made is "this source of risk may be a threat". Considerable additional work may be required to confirm that "this source of risk is a threat". Methods for risk analysis should not only be complete, but should be reasonably discriminating.

The final aspect which is important when comparing risk analysis procedures is cost. Cost here has been measured in terms of engineer hours.

1.3.1. The distillation unit

The distillation unit itself consists of major parts

- a distillation kettle, heated by steam, and stirred (to improve heat transfer)
- a storage vessel, capable of supplying a continuous stream of feed to distillation unit

- a short packed column allowing separation of vapour.

- a condenser, with a proportioned reflux back to the column.

- a further cooler ensuring temperature control of condensed liquids.

- Four distillate receivers, for respectively methanol, impure methanol, impure urethane, and pure urethane.

- A vacuum pumping system, allowing the later stages of distillation to take place under vacuum. The vacuum system includes a condenser cooled by brine, as a vapour trap.

A sketch of the unit is shown in fig. 1.

The unit is controlled by a Texas Instruments PM 550, programmed logic controller, which implements both sequential and continous control. The sequential control principle used is that of a fixed sequence of control stages, with only limited sequence variations, and with operator control of the timing of the sequences. That is, the operator can signal the start of the next step in a procedure, and can also stop a procedure. Extensive safety interlocks are provided, preventing start of a procedure under unsafe conditions.

In use the distillation unit is first filled by pumping the product methanol mixture to the distillation kettle from a transportation tank. When the required level is reached, further filling of the storage vessel takes place, until a full charge of feed is contained.

Thereafter the distillation kettle is heated, and distillation begins, with heating controlled to maintain an appropriate pressure drop accross the distillation column. The distillation removes relatively pure methanol, which is transferred to the first distillate receiver.

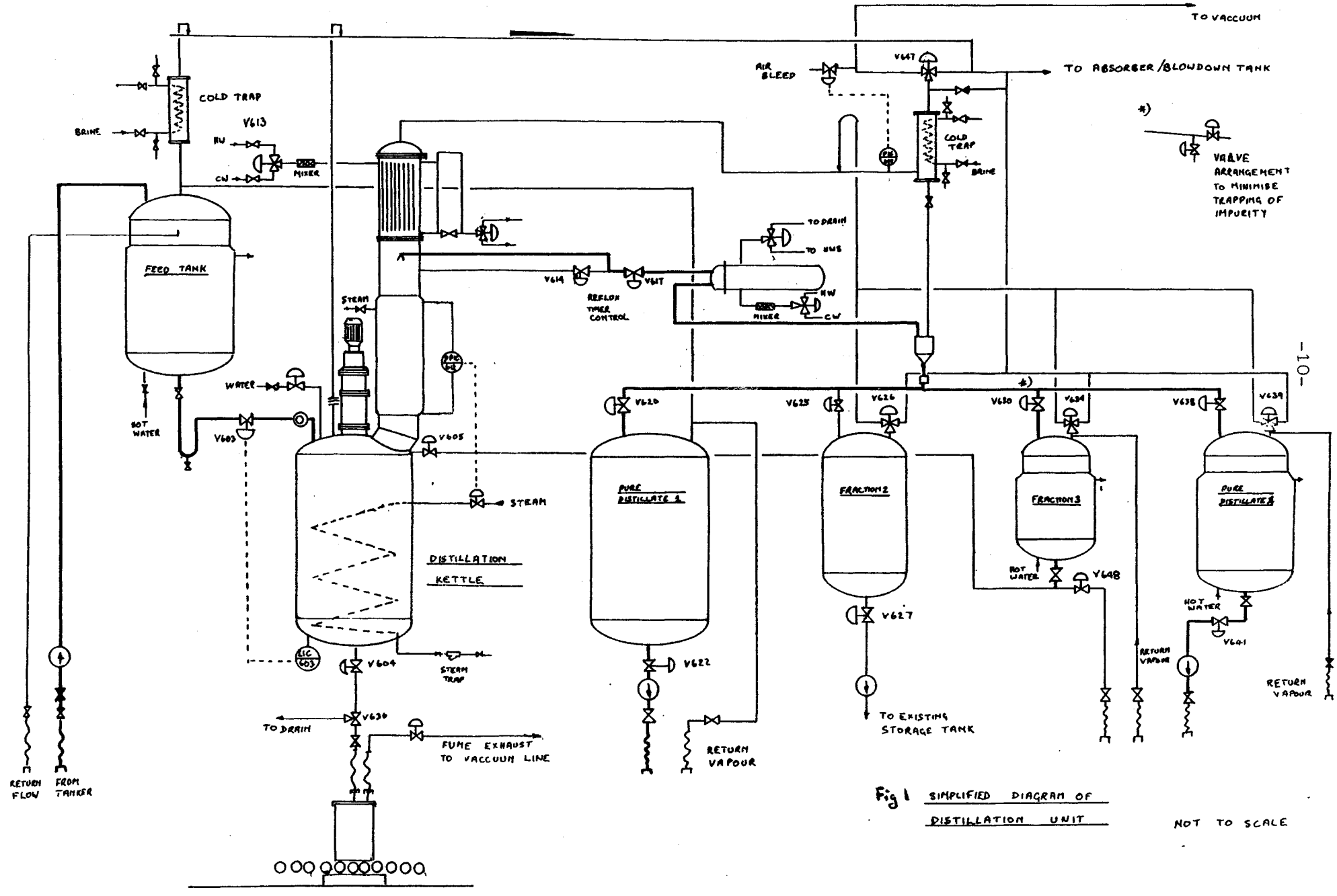


Fig 1 SIMPLIFIED DIAGRAM OF DISTILLATION UNIT

NOT TO SCALE

During the distillation, a flow of feed is maintained to the kettle from the storage vessel whenever the level falls below a desired point. The "pure methanol" distillation ceases when an appropriate distillation temperature has been reached.

Once the required limit temperature for pure methanol distillation has been reached, vacuum distillation is started manually, first of impure methanol, then of impure product finally of pure product. Switching between the different fractions takes place on the basis of temperature. The separate fractions are collected in separate receivers. Control of the temperature set point for the distillation is changed continuosly during urethane distillation, to ensure optimal distillation conditions.

On completion the various receivers can be emptied to transportation vessels. In the case of impure methanol, emptying is to an existing ground tank. In the case of impure product, this can be returned to the distillation kettle. (transfer by vacuum pumping).

Residue from the distillation, in the form of a thick readily freezing liquid, is emptied to drums after completion of the distillation, and is transported away to be burnt.

The entire distillation unit is rinsed and boiled out, after use, using water.

1.3.2. Boundaries for the analysis

The plant analysed is essentially that shown in fig. 1, extending from the intake coupling for distillate feed, through to the couplings to transport containers and to the ground tank. The analysis includes the vacuum pump. The analysis does not include the ventilation dump tank ("incident tank"), nor the transportation tanks.

The phases of plant operation analysed are all steps of normal production. Incidents occurring during repair or maintenance were not analysed.

No attempt was made to check the construction strength of vessels, supporting steelwork etc. during the risk analysis, since such checks are a normal part of the plant design procedure, and are already well standardised.

1.3.3. Safety Equipment fitted to the plant and plant safety features.

Safety equipment fitted to the plant is listed here. The list covers several items which are not normally considered under the title safety equipment, but which have a definite safety function. They are included in the list because of their impact on the safety analysis. An example is the overflow pipe on the distillation feed storage tank.

Some of the safety equipment was added to the plant as a result of the analysis. Some was added as standard safety features, following Grindsted Products normal design practice. Some of the safety equipment was added as a result of ad hoc checks during commissioning, that is, despite the need being overlooked during the initial safety analysis.

1) Pumps used are centrifugal pumps, with maximum delivery pressure less than plant design pressure.

2) The feed storage tank has an overflow back to the transportation tanker, to avoid overfilling.

3) "Cold trap" on all atmospheric vents, to prevent release of methanol vapour.

4) Venting to atmosphere on the feed storage tank.

5) Atmosphere venting on all other vessels, via a three way

valve, which also allows venting to the vacuum pump.

6) Atmosphere venting via an "accident tank"

7) "Swan neck" (U trap) on the feed tank to prevent blow back of methanol vapour.

8) Burst disk on the distillation kettle.

9) Double/triple activation required on the kettle drain valve, of diverse types (electronic and air).

10) Manual emergency valve on the kettle drain line.

11) Self closing valves in the coupling nozzles for emptying outlets for the methanol receivers.

12) Methanol vapour return lines for coupling to transport tanks.

13) A heavy lid and exhaust pump for vapour from the residue drum to prevent escape of vapour when emptying the distillation kettle of residue.

14) Weighing machine to control against overfilling residue drums.

15) Extensive interlocking to prevent unsafe action and to stop the plant in case of emergencies.

16) Safety showers.

17) Standard fire fighting equipment.

18) Bunds to prevent spread of liquids in case of release.

The use of a programmed logic controller for control of the plant made interlock design particularly easy and economic. Interlocks fitted include the following.

1) Emptying the feedtank must first be activated locally and then in the control room, ensuring that the operator has a chance to check that a receiving container is fitted.

   (Note that activation in the control rooom and then locally could be dangerous in the case of a switch failure).

2) The feed tank cannot be emptied while the distillation kettle is being filled.

3) The methanol receiver cannot be emptied if its level is already too low, or if the ground tank level is too high.

4) Item deleted.

5) Interlocks similar to 3 and 4 on the impure methanol receiver, and urethane reveivers.

6) The impure urethane receivers may not be emptied to the distillation kettle while the distillation or rinsing is being undertaken.

7) Interlocks similar to 1 on the impure urethane and pure urethane receivers.

8) Triple closure switches on the distillation kettle charging valve, to prevent overfilling.

9) Kettle charging cannot take place while the feed tank is being filled, or emptied, or while a vacuum distillation step is taking place.

10) Atmospheric distillation cannot be activated while the plant is activated for vacuum distillation.

11) Atmospheric distillation cannot be started, and stops, if the high level alarm or the high temperature alarm is received, or if the receiver is not empty. (This interlock was later removed)

12) Vacuum distillation cannot begin if the distillation apparatus is overfull, or if the receivers are not empty. (This interlock was later removed).

13) The agitator is stopped if the temperature falls unders $50^{o}C$ during urethane distillation.

14) Different distillation receivers may only be open one at a time, and distillation may not be activated during tank draining or rinsing.

15) Different trip temperatures for each of the distillation steps.

16) Prevention of emptying of the distillation kettle unless there is a receiving drum with less than 100 kg in it, or if the temperature is too high.

17) Rinsing of the distillation kettle can only take place if the other processes are inactive.

A lamp light behind the activating switch if and only if the corresponding operating step can be activated. Any operating step can be stopped by pressing the activating button once more.

1.4 Potential risks for the plant

The primary risks for the distillation unit is release of methanol or methanol-product mixtures. The risk is enhanced if the methanol is hot (at its boiling point). Methanol vapour is poisonous, but a much larger threat is ignition, which could cause af deflagration type explosion (more probably just a puff) and a fire.

Fighting methanol fires presents a problem in that ordinary foam is destroyed by the liquid. On the other hand dilution with water rapidly renders the methanol non-inflammable.

The product is itself non-poisonous, but contains, before distillation, in the present plant, dimethyl carbonate which is poisonous.

An additional potential risk in the plant is overpressuring, which could lead to a vessel rupture explosion.

The major threat from the plant is that of capital and production loss in the case of fire. Additionaly neibouring production units could be damaged. There is a possibility of harm to the operator of the plant, if a release of methanol, and subsequent fire, should occur while he was in the neighbourhood of the plant. The most probable circumstances for this is during movement of residue drums. Note that during filling of the drums, when the operator is immediately beneath the distillation unit, the distisllation unit itself is empty of methanol.

There is a risk that the operator could be splashed with residue, though extensive measures have been taken to prevent this. In particular, a heavy lid must be lowered over the drum before residue is emptied to it.

1.5.1. Safety constraints on the design (laws, standards, etc.)

The major safety constraints imposed on the design are from Grindsted Products A/S normal construction practice, which includes standards for arrangement of distillation units, steelwork, piping, etc.

1.5.2. Acceptance criteria

The main acceptance criterion adopted for the analysis was that

no single failure of equipment, and no single operating error, should result in release of liquids, overpressuring or similar extreme event.

The single failure criterion was extended to a double failure criterion, in some cases where failure probabilities were judged especially high.

2.1. Organisation of the analyses

Safety analysis as part of the plant design process

The safety analysis was carried out as part of the design process. What this meant in practice was that hazard and operability analyses were carried out at the flow sheet stage and at the piping and instrumentation diagram stage of the design. There was a qualitative analysis of possible procedural erros at the stage of initial procedure formulation. And prior to commissioning, checks were applied according to an outline check list of "safety officer checks".

The analysis was carried out by a team consisting of the plant design engineer in charge of the project, the plant safety officer and two risk analysts. With this composition of the team, a direct feedback of results was possible at each stage of the analysis. The benefit of the analysis was therefore an early recognition and correction of design problem and in some cases, recognition of problems which would otherwise have been overlooked.

The initial analysis was for a version of the plant including reactors and ammonia treatment. This plant was never in fact built, but hazards identified for this plant were relevant for the actual plant. In all about six days of analysis effort for a three man team, and an additional 10 man days of individual effort were expended for this original plant design, during 1979.

Fig. 2 Typical Action Sheets as completed during safety analysis meetings.

ACTION SHEET NO. 17

PROJEKT URETHAN PRODUKTIONS LINIET

PROBLEM Læk i ventil fra forlag (1) til autoklave (3)
årsags konsekvens analyse.

ANSVARLIG JRT CJ OH

LØSNING

Løst ved (a) udskiftning af 1000 l forlag
+ 3000 l. forlag.

(b) kontra ventil ved autoklave

(c) bundventiler (håndbetjent) ved forlagene.

(d) Lgr dimensioneret til 4½ atm.

ACTION SHEET

SYSTEM URETHAN PRODUKTION

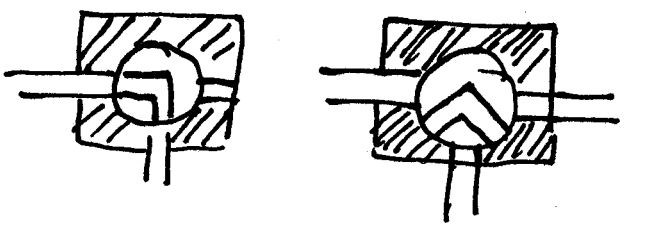
NO. 14 DATE

PROBLEM:

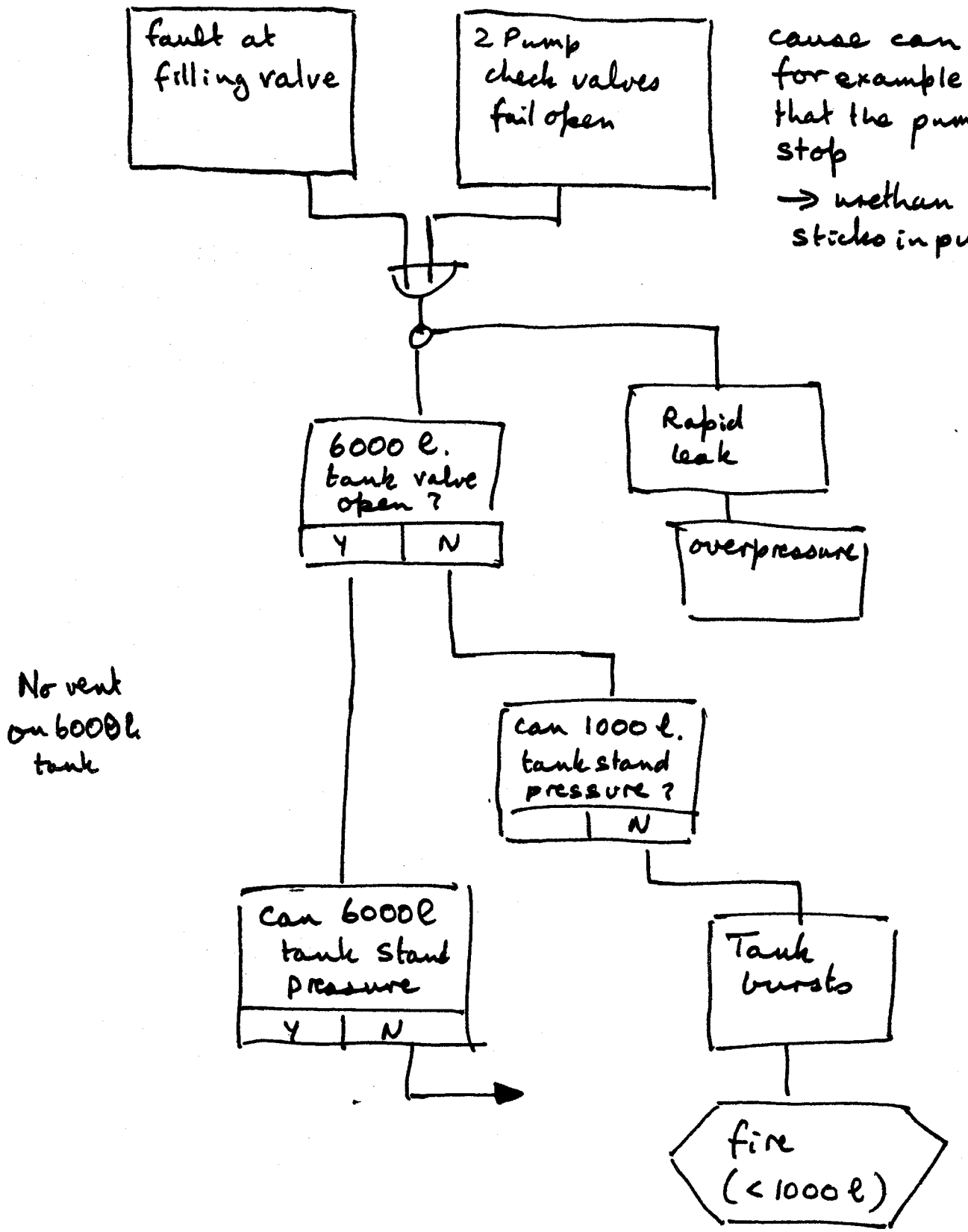
CHECK AT 3 VEJS VENTIL
IKKE LUKKE TOTAL, SAMT
KONSEKVENSER HVIS DEN GØRE
DET

RESPONSIBLE JRT H & OP SHEET NO

SOLUTION



3 VEJS VENTIL FJERNET VED KØLEREN ✓


fault at filling valve
2 Pump check valves fail open
cause can for example be that the pump stop → methan sticks in pump.
6000 ℓ. tank valve open ?
Y
N
Rapid leak
overpressure
No vent on 6000ℓ tank
can 1000 ℓ. tankstand pressure ?
N
can 6000ℓ tank stand pressure
Y
N
Tank bursts
fire (< 1000 ℓ)

The actual plant was analysed according to the following calender.

Jan	7	Initial planning meeting
Feb	22	first plant design analysis (Hazop)
April	27	Hazop analysis
May	27	Completion of Hazop Analysis
May	29 ff	Action error analysis of the plant
Nov		Begin commissioning/Safety Officer checks

The time taken was, in meetings, for Hazop analysis 2 days x 6 hrs. x 3 persons. For action error analysis, the analysis took 2 days x 6 hrs x 2 persons. The safety checks took 2 days for 2 persons.

Additionally, some 10 days were spent in evaluating problems outside safety analysis meetings.

A feature of the organisation of the analysis was that work was carried out by a team, as described above. For each meeting, a secretary was chosen, with the job of ensuring that a rigid analysis procedure was followed, and with the job of recording the results of the analysis. Any problems which arose during the analysis were discussed for a few minutes. If the problem proved too difficult, or if insufficient information were available, solution of the problem was postponed. A particular person was appointed to solve the problem, and this responsibility recorded. The problem was written down on an "action sheet". Some typical action sheets are shown in fig. 2.

Further analyses have been carried out for comparison purposes, but these have not yet reached a stage where reporting is appropriate.

An important aspect of the analysis was the need for repetition, at several stages, as the design altered.

4. Information basis for the analysis

The information on which the risk analysis was based consisted of

- Plant flow sheet and piping and instrumentation diagrams through all stages of design revision.
- The plant production/operating instructions which describe
    - The operators safety responsibilities (standard responsibilities for handling methanol, supervisory responsibilities for leaks and abnormalities in performance)
- Plant control programming tables (see fig. 2.5)
- Plant layout drawings
- Description of the PLC controller for the plant.

5. Analysis

5.1.1. Initial analyses

At the outset of the project a survey of litterature was carried out to determine the properties of substances used in the plant, and their potential reactions. A reaction matrix was built up (see fig. 3).

Experimental tests were performed on the reaction involved in producing the urethane, as a result of queries raised in the analysis. One result of this was the realisation that under

Fig. 2.5. Control Programming Tables.

HJÆLP: METHANOL- OG METANOLFRI DESTILLATION

PROCES NR. / NAVN: 3/ Vacuum destillation i destillatør 264 002, destillat til forlag 264.007

START BETINGELSER:

Se "Processer der ikke kan køre samtidig"

LIS-628 skal vise mindre end 60% fyldning.

LIS-635 og LIS-640 skal vise at forlagene er tomme.

SLUT BETINGELSER:

Afbrydes ved aktivering af proces nr. 10 eller af stop funktion.

BEMÆRKNINGER:

Reflux styres ved at V-617 og V-618 skiftevis åbnes og lukkes af to timere. Refluxforholdet er endnu ikke kendt.

Sætpunktet for vacuumregulering reduceres i løbet af 1/2 time fra 760 mm Hg til 20 mm Hg.

Hvis LSAH-628 aktiveres lukkes V-612, V-618 samt V-625 og V-617 åbner.

Hvis TSAH-616 aktiveres lukkes dampventil V-612 Sætpunktet er under proces nr. 9 40°C

HJÆLP : METHANOL - OG METHYLGLYKOL - DESTILLATION

PROCES NR. / NAVN : 9 / Vacuumdestillation, destillater

264.002 destillat til forlag 264.007

BEMÆRKNINGER :

Hvis TSAH-611 aktiveres afbrydes proces 9 ;
sætpunktet er 40°C under proces 9

Hvis TSAH-620 aktiveres afbrydes proces 9
sætpunktet for TSAH-620 er 40°C under proces 9.

FØLIEG : METHANOL- OG METHYLGLYKOL-DESTILLATION

PROCES NR. / NAVN : 9 / Vacuum destillation i destillator

264 002, destillat til forlag

FAIL OPEN

FAILCLOSED

FAIL LOCKED

VENTIL NR	FO	FC	FL	Tilbage melding	ÅBEN	LUKKET	AKTI-VERET	RÆKKE-FØLGE
603		x				x		
604		x		x		x		
605		x				x		
606		x				x		
612		x			x		x	
613	til VG*	til V65*c			til VG*	til V65		
(614)*					til VG*	til V65		
617	x				x ↔ x		(x)	
618		x			x ↔ x		(x)	
619	x					x	x	
621		x				x		
622		x						
625		x			x		x	
626	til atmos	til vacuum			til vacuum	til atmos	x	
627		x				x		
630		x				x		
632		x				x		
634	til atmos	til vacuum			til vacuum	til atmos	x	
636			x	x				
638		x				x		
639	til atmos	til vacuum			til vacuum	til atmos	x	
641		x				x		
642	til tank	til vogn		x				
644	til VG*	til V65*			til VG*	til V65		
(645)*					til VG*	til V65		
646		x				x		
647	til atmos	til vacuum			til vacuum	til atmos	x	
648		x				x		

MOTOR NR	Tilbage melding	KØRER	KØRER IKKE	RÆKKE-FØLGE
264-002	x	x		
264-012	x		x	
264-013	x	x		
264-014	x		x	
264-016	x			
264-017	x		x	

PROCES NR. - KAN IKKE KØRE SAMTIDIG MED FØLGENDE

PROCES NR.	
P 1	
P 2	x
P 3	x
P 4	x
P 5	x
P 6	x
P 7	x
P 8	x
P 9	-
P 10	x
P 11	x
P 12	x
P 13	x
P 14	x
P 15	x

* 614 og 645 er lokale regulatorer uafhængig af luft og el. svigt

STATE OF VALVE IN THIS STEP

Fig. 3. Reaction Matrix.

METHYLURETHAN - ANLEG

REAKTIONS MATRICE

20/3-1979 OH

	URINSTOF	METHANOL	METHYLURETHAN	NH_3	H_2O	CO_2	AMMONIUM-CARBAMAT	DIMETHYL-CARBONAT		
URINSTOF	POLYME-RISERER									
METHANOL	PRODUKT: METHYLURETHAN + NH_3	÷								
METHYLURETHAN	POLYME-RISERER ?	DIMETHYL-CARBONAT	POLYME-RISERER							
NH_3	÷	÷	URINSTOF + METHANOL	÷						
H_2O	$CO_2 + NH_3$	÷	÷	÷	÷					
CO_2	÷	÷	÷	AMMONIUM CARBAMAT	÷	÷				
AMMONIUM-CARBAMAT	÷	÷	÷	÷	$CO_2 + NH_3$	÷	÷			
DIMETHYL-CARBONAT	POLYME-RISERER ?	?	POLYME-RISERER ?	÷	÷	÷	÷	POLYME-RISERER ?		

failure conditions, pressure could be higher than originally thought (in the case of temperature control failure and burst disc failure to operate or blowdown line blockage). As a result, an additional pressure guage was added as part of the plant instrumentation.

The initial analyses took in all about 2 man days, apart from the time required for the reaction experiment.

5.1.2.1. Hazard and Operability analysis

METHOD

The method chosen for the first step of the risk anlysis was the hazard and operability method first developed by ICI Ltd. The method can be used in many versions. The version used for this plant was one based on systematic analysis of disturbances for each "volume" in the process plant.

The reason for the choice of this method was that, at least for steady state operation, of the plant, it provides a fairly complete analysis of hazards, and can be performed quite quickly.

In detail, the method involves the following stages.

1) A flow sheet on piping and instrumentation diagram for the plant is obtained.

2) Each "volume" on the diagram is numbered.

   A "volume" may be a tank or pressure vessel. It may equally be a pump, a section of pipe which can be closed off, a stand pipe, a drain pit, etc. A general definition would be "any volume in space which can be closed off from other volumes and in which mass or energy can accummulate.

3) For each "volume" a series of disturbances are proposed. These disturbances are drawn from the list

BREACH OF VESSEL BOUNDARY

TEMPERATURE	
PRESSURE	
LEVEL	TO HIGH
CONCENTRATION	TOO LOW
DEGREE OF MIXING	ZERO
pH	
REDOX	

4) For each disturbance, potential causes and potential consequences are described and written down in a table.

5) For any problems discovered either the solution is entered into the table, or an action is placed on one person to solve the problem at a later date.

6) If necessary, because of the degree of complication in a piping system, individual pipes may be subject to the disturbance cause - consequence - cure examination. Here the list of disturbances to the following.

MASS FLOW	TOO HIGH	NO FLOW
HEAT FLOW	TOO LOW	REVERSE FLOW
CONCENTRATION	TOO HIGH	TOO LOW
WRONG SUBSTANCE		
HIGH PRESSURE		

7) The procedure is repeated for each vessel, and, if nescessary, each pipe, turn.

For the analysis of the first plant, pre-printed tables containing the check lists given above were used (fig. 4). For the second analysis, of the distillation unit, new tables were used, with the most common causes of disturbances, and the most

Fig. 4. An example of the first version of the hazard and operability analysis tables - as completed in Hazop meetings.

VOLUME: 3

AUTOKLAVE

TANK PRESSURE VESSEL, STAND PIPE, PIPE SECTION,

VALVE DEAD SPACE.

DATE SHEET

VARIABLE	CHANGE	CAUSE	CONSEQUENCE	COMMENT, CURE, ACTION
TEMPERATURE	TOO HIGH	Temperatur control svigt (max 200 grade øvr høj tryk.)		stable reaction (40 års erfaring + eksperiment.) TIC 61A (170°C testet) tryk stiger til 21 atm. + Aktion 53.
	TOO LOW		forlænget reaktionstid, lav udbytte.	autoclave designed for 40 atm. Aktion 53 KT.
PRESSURE	TOO HIGH		~~Se~~ .	Se Aktion 15. (PI 618 lokal) (PIC 618 tryk reg.) Aktion 53.
	TOO LOW		—	
LEVEL	TOO HIGH		overtryk ved opvarmning	sikkerheds ventil på. Se Aktion 15 + sprængplade ved 6.
	TOO LOW			
VOLUME (CLOSED VESSEL, FULL)	TOO HIGH			
	TOO LOW			
PH	TOO HIGH			
	TOO LOW			
REDOX	TOO HIGH			
	TOO LOW			
INADEQUATE MIXING		omrøring fejl.	~~omrøring~~ darlig udbytte.	
HEATING	TOO HIGH		Se too high temperature.	
	TOO LOW			
COOLING	TOO HIGH		Størkner:	
	TOO LOW		Forlæng køle tiden	
SERVICES FAILURE ELECTRICITY, WATER, CONTROL, AIR NITROGEN, MIXING olie til omrører pakdåsen		Rører fejl Spærrevæske forsyning fejler	darlig udbytte. ethanol + ammoniak i olien. kostbart.	kun sjældent : kun økonomisk tab.

VOLUME: 3

PIPE TUBE, DRAIN, INSTRUMENT LINE

PORT: silurkedo vent:

DATE

SHEET NO.

VARIABLE	CHANGE	CAUSE	CONSEQUENCE	COMMENT, CURE, ACTION
MASS FLOW	TOO HIGH	fejl: ventilen, overtryk.	ammoniak + ethanol til vheldo tanke	TAH 616.
	TOO LOW			
	REVERSE FLOW			
	NO FLOW			
WRONG SUBSTANCE				
CONC. SUBSTANCE 1	TOO HIGH			
	TOO LOW			
CONC. SUBSTANCE 2	TOO HIGH			
	TOO LOW			
TEMP-ERATURE	TOO HIGH			
	TOO LOW			

VOLUME: 3

PORT: udtapning (urethan + alkohol)

PIPE, TUBE, DRAIN, INSTRUMENT LINE

DATE

SHEET NO.

VARIABLE	CHANGE	CAUSE	CONSEQUENCE	COMMENT, CURE, ACTION
MASS FLOW	TOO HIGH	læk: ventilen.	For tidligt — For meget ethanol til separation, dårlig udbytte.	Hand Ventil
	TOO LOW		—	
	REVERSE FLOW	Vand fra køler 13.	Vand: autoklave. (se senere) carbamat (bliver dedikeret af alligevel.)	
	NO FLOW		—	
WRONG SUBSTANCE			—	
CONC. SUBSTANCE 1	TOO HIGH			
	TOO LOW			
CONC. SUBSTANCE 2	TOO HIGH			
	TOO LOW			
TEMPERATURE	TOO HIGH	Ventilen & udtapning fejler.	Fuld ammoniak + ethanol tryk til 12. 12 har sprængplade på., og også udtag til luften via en ventil.	
	TOO LOW		tilstopning: aftapnings rør. Steam tracing på.	

VOLUME: 3

PORT: afluftning.

PIPE, TUBE, DRAIN, INSTRUMENT LINE

DATE

SHEET NO.

VARIABLE	CHANGE	CAUSE	CONSEQUENCE	COMMENT, CURE, ACTION
MASS FLOW	TOO HIGH	at wrong time : fejl i afluftningsventil.	ammoniak til absorber ingen problem. muligvis sprit i ammoniac.	belastning på rensningsanlæg.
	TOO LOW			
	REVERSE FLOW			
	NO FLOW			
WRONG SUBSTANCE				
CONC. SUBSTANCE 1	TOO HIGH			
	TOO LOW			
CONC. SUBSTANCE 2	TOO HIGH			
	TOO LOW			
TEMP-ERATURE	TOO HIGH	fejl i afluftnings ventil	— ethanol til absorptions form.	
	TOO LOW			

VOLUME: 3

PIPE, TUBE, DRAIN, INSTRUMENT LINE

PART: ethanol forlag, tilløb. og fra pumpe 10.

DATE

SHEET NO.

VARIABLE	CHANGE	CAUSE	CONSEQUENCE	COMMENT, CURE, ACTION
MASS FLOW	TOO HIGH		—	
	TOO LOW		—	
	REVERSE FLOW	Fejl i kontrol ventil (kuler)	Fuld ammoniac trykk i ethanol forlag. (170°c – 20 atm, 200°c – 40 atm) ammoniac → sikkerheds ventil. 3 vejs ventil.	ammoniac → lager tank. (350 L/6 minutter) AKTION 17 JRT CJ OH
	NO FLOW			
WRONG SUBSTANCE				
CONC. SUBSTANCE 1	TOO HIGH	VAND	CARBAMATE → TILSTOPPNIN VED TOPPEN AF DESTILLATION	
	TOO LOW			
CONC. SUBSTANCE 2	TOO HIGH			
	TOO LOW			
TEMP-ERATURE	TOO HIGH			
	TOO LOW			

VOLUME: 3 DATE SHEET

CONCENTRATION SUBSTANCE	CHANGE	CAUSE	CONSEQUENCE	COMMENT, CURE, ACTION
	TOO HIGH		darlig udbytte.	
	TOO LOW			
	TOO HIGH			
	TOO LOW			
	TOO HIGH			
	TOO LOW			

BREACH OF RETAINING BOUNDARY			

LEAK
omgiver
[illegible] med
som spaceraeske.
[illegible] ind → ~~[illegible]~~ bundrest.

OVERSTRESS

CORROSION
40 års erfaring.
) Lack i dæksel.

WEAR

MISSILE IMPACT, CRASH

HAMMER
ved stød kogning?
AKTION JRT 17

FIRE

OPENING BY MAN
disaster!
AKTION 16 JRT

COLLAPSE

Fig. 5. Hazop table examples for the second analysis.

MODULE [illegible] NO: forlag TANK, PRESSURE VESSEL, CLOSED PIPE SECTION, STAND PIPE SUMP (LEVEL)

STATE

SYSTEM: HUD

SHEET: 1 DATE:

VAR.	CHANGE	CAUSE		FT/CCD	CONSEQUENCE	CURE, COMMENT		ACTION	FOLLOW UP INSTR CHECK	PRE COMM	CUT SETS
LEVEL	TOO HIGH	TOO HIGH INFLOW	SEE LINE NO:		RELEASE POISON, FLAMMABLES, CORROSIVES. HIGH PRESS AT OUTFLOW	LEVEL CONTROL	X	LSAH 601			
		TOO LOW OUTFLOW	SEE LINE NO:		retter flow til container.	ALARM	X	LSAH 601			
		TEMP. EXPANSION			Hvis returlinien blokeret, flow til udeldstank + opløsning lag destillator springplade	TRIP, SHUTDOWN					
		VESSEL CONTRACTION, CRUSH				DUMP VALVE					
		SCUMMING, DEPRESSURISATION				OVERFLOW, DRAIN					
		BOILING				aendring i indløb til udeldstank linien. O.K.					
		Too long flows.			Ødelægge springpladens virkning.	ACTIONS					
	ZERO	SEE BELOW			BOIL DRY (BOILER).	ACTIONS					
	TOO LOW	TOO HIGH OUTFLOW	V603 sætter sig fast. Fejl		AIR, GAS IN OUTFLOW LINE, WRONG OUTFLOW IN DECANTING.	LEVEL CONTROL					
		TOO LOW INFLOW			hvis for lavt under destillation, damp kan komme ud under destillation.	ALARM					
		EVAPORATION				TRIP, SHUTDOWN					
		LEAK	SEE RUPTURE SHEET:		Hvis V603 sat fast - tab af Met.	el tracing på V603, Vasdske løs ~~på~~ for V603.					
		BOIL OVER, EFFERVESCE.			Hvis tilslutningsventil åben - retard damp ud.	ACTIONS					

VOLUME [illegible] NO.: | TANK, PRESSURE VESSEL, PIPE SECTION | SYSTEM: MUD

STATE: | STAND PIPE, DRAIN, SUMP (MISC.) | SHEET: 2 DATE:

VAR.	CHANGE	CAUSE			FT/CCD	CONSEQUENCE	COMMENT CURE			FOLLOW UP: MAKE CHECK		CUT SET
PH	TOO HIGH	INFLOW, OUTFLOW, REACTION, REMANENCE										
	TOO LOW	INFLOW OUTFLOW REACTION REMANENCE										
CONCENTRATION		TOO HIGH INFLOW		SEE LINE NO.		REACTION, STIFFENING, SOLIDIFICATION, CRUD, POISONING ON CLEANING	CONTROLLER					
		TOO LOW OUTFLOW		SEE LINE NO.		Problem med forhert levering af container.	PRE ADDITION ANALYSIS					
		REACTION		LONG STORAGE			LABELLING					
		REMANENCE CRUD		POOR CLEANING, CREVICES			AUTO WEIGHING					
		EVAPORATION		LONG STORAGE			CHECK VALVE					
		WRONG SUBSTANCE ADDED, IMPURITY					ALARM					
		REVERSE FLOW					DUMP TANK					
		WRONG SUBST IN FLOW					CLEANING LINE, STEAM					
		TOO HIGH INFLOW										
		TOO LOW OUTFLOW										
		REACTION					Sikres gennem general regler for levering af container.					
		EVAPORATION										
		WRONG SUBSTANCE ADDED, IMPURITY										
		REMANENCE CRUD		SUBSTANCE:			G. Instruks. 2.1.7		ACTIONS			
		REVERSE FLOW										
		WRONG SUBST. IN FLOW										
INADEQUATE MIXING		AGITATOR FAILURE, CREVICES, LAYERING, CAKING				ROLLOVER, UNEVEN REACTION HOT SPOTS, CLUMPS IN PROD.						

VOLUME: NO.: TANK, ESSURE VESSEL, CLOSED PIPE SECTION SYSTEM: MUD

STATE: STAND PIPE, SUMP (TEMPERATURE) SHEET: 3 DATE:

VARIABLE	CHANGE	CAUSE		CONSEQUENCE	FT/ CCC	CURE, COMMENT ACTION			FOLLOW UP INST. CHECK	FOLLOW UP PRE COMM	CUT SETS
TEMPERATURE	TOO HIGH	TOO HIGH HEATING FLOW	SEE LINES: SEE SERVICES:	OVERPRESSURE, METAL STRESS, METAL WEAKENING, REACTION FIRE.		TEMPERATURE CONTROLS					
		TOO LOW COOLING FLOW	SEE LINES:			ALARMS					
		TOO HIGH ELECTRICAL HEAT	SEE SERVICES:			TRIPS, SHUTDOWN,					
		CHEMICAL REACTION	SEE REACTION SHEET, NO: SEE CONCENTRATION SHEET NO:			DUMP VALVE					
		FIRE				RELIEF VALVE					
		STIRRING FAILS LOCAL HEATING									
		TOO HIGH FLUID IN FLOW	SEE LINES:								
		TOO HIGH INFLOW TEMP	SEE LINES:								
		FRICTION									
		COMPRESSION HEAT									
		HEAT RADIATION									
		BLANKETING									
		OTHER CAUSES									
	TOO LOW	TOO HIGH COOLING FLOW	SEE LINES: SEE SERVICES:	FREEZING (OVERPRESSURE), BLOCKAGE, REACTION (STOPPAGE) LOW PRESSURE		TEMPERATURE CONTROLS					
		TOO LOW HEATING FLOW	SEE LINES: SEE SERVICES			ALARMS					
		TOO LOW INFLOW TEMP	SEE LINES:			TRIPS, SHUT DOWN					
		TOO HIGH INFLOW	SEE LINES:								
		WEATHER									
		DEPRESSURISATION EVAPORATION									
		REACTION STOPS									
		OTHER CAUSES									

For høj temp → kogning metanol → dump til skadestank → tab af produkt

Hvis tilslutnings ventil åben — brand risiko.

Næsten umuligt at få overtemp. med selv regulerender el tracing.

ACTIONS

1 off bayonet tilslutnings ventil.

Vedsvigt af el tracing → Styrkning. → drift forstyrrelse

ACTIONS

- 24 -

ART Soft KRT

VOLUME: NO: TANI PRESSURE VESSEL, CLOSED PIPE SECTIC -. SYSTEM: MUD

STATE: STAND PIPE, SUMP (PRESSURE) SHEET: 4 DATE:

VARIABLE	CHANGE	CAUSE		FT/CCD	CONSEQUENCE	CURE	COMMENT / ACTION	FOLLOW UP INSTR. CHECK	FOLLOW UP PRE COMM.	CUT SETS
PRESSURE	TOO HIGH	TOO HIGH TEMP	SEE PREVIOUS SHEET NO.		Ved størkning af urethan (el.øvrigt) mulighed for overtryk hvis uheld tank linien og tilbageløb blokeres.	SAFETY VALVE				
		TOO HIGH INFLOW	SEE LINES NO:			RELIEF VALVE				
		TOO LOW OUTFLOW	SEE LINES NO:			TRIP, SHUTDOWN				
		GAS GENERATION				ALARM				
		REACTION	SEE REACTION SHEET NO SEE CONC. SHEET NO:			PRESSURE CONTROL				
		PRESSURE REDUCTION FAILS	SEE LINES NO:			COOLING				
		FULL OF LIQUID				BURST DISC				
		FREEZING								
							ACTIONS: 2 OH			
	TOO LOW	TOO LOW TEMP.	SEE PREVIOUS SHEET NO:		mulighed for undertryk ved blokering af linier og køling.	TRIP, SHUTDOWN				
		TOO LOW INFLOW	SEE LINE NO:			ALARM				
		TOO HIGH OUTFLOW	SEE LINE NO:			VACCUM BREAKER				
		COOLING + ISOLATION	SEE LINES NO:			PRESSURE CONTROL				
							ACTIONS: 3			

QRT Sept 1979

(Tring)

STORAGE OR PRODUCTION UNIT: 4000 L fol

SUBSTANCE :

RELEASE ROUTE AND BARRIER ANALYSIS

PLANT:

SHEET: 6

OF :

BREACH POSITION	PRODUCTION PHASE	CAUSE	TARGET	RELEASE ROUTE AND SECONDARY BARRIERS	BREACH PROBABILITY	RELEASE RATE	ALARMS	POSSIBILITY FOR STOPPING RELEASE	TIME TO STOPPING	EMERGENCY MEASURES
		LEAK		Ventil gevind						Forhindre ~~[illegible]~~ pøle ved overvagning; Nul teflon: gevind
		OPEN BY HAND								

CAUSES OF BREACH: OPENING VALVE, OPENING MANHOLE, OPENING FLANGE, RUPTURE / OVERPRESSURE / LEAK (HIGH INFLOW, LOW OUTFLOW, LIQUID EXPANSION, FREEZING)

HIGH TEMPERATURE, FIRE, CORROSION, CRACKING, FATIGUE, WATER HAMMER, STEAM HAMMER, CRASH (VEHICLE, CRANE, FALLING OBJECT, MISSILE) BIRD

FOUNDATION OR SUPPORT FAILURE, PIPE EXPANSION, JET REACTION, EARTHQUAKE, FLOOD, TORNADO, EXPLOSION, WELDING CUTTING REPAIR

common "cures" already printed. The list of causes and cures was obtained by examining the earlier tables. The intention was to increase the rate at which analyses could be performed (instead of writing, a cross could be set at the side of the appropriate cause, or a number for the relevant pipe, valve instrument (fig 5). Additionally it was hoped that the list of causes would improve the coverage or completeness of the analyses. Note that a space is left in the tables for "other causes".

The version of Hazards and Operability analysis used here should in principle provide a complete analysis of all plant disturbances. If it does not, then this may be because

- not all operating states have been considered (it is usual to concentrate on the normal operating state)

- Listing of causes is too complex (a fault tree or similar method should be used)

- Listing of consequences is too complex.

Comparison of different analyses later in this report enable omissions to be investigated.

5.1.2.2. Observations on the hazard Operability analysis process

The hazard and operability analysis was carried out within a "brain storming" group. Discussions in such a group tend to become long and detailed. It is nescessary for the meeting secretary to excercise a good degree of discipline if the time used is not to become excessive.

Recording of causes and consequences in the meeting can be difficult, because of the rate of discussion. As a result, the writing tends to be terse. It is important that a fair copy is written out later, if the results are required as plant docu-

mentation. (The primary result, though, can be regarded as the modifications added to diagrams, and the "actions" imposed on group members).

As the analysis progresses, there is a tendency for a disturbance which was originally studied as a "consequence" to reappear as a "cause". This is natural, because, for example a pressure disturbance can be transmitted from volume to volume. Time can be saved by cross referencing from table to table, but at each new volume, consequences should be considered.

5.1.2.3. Results of the hazard and operability analysis

Urethane reactor

The first analysis, on the product reactor, took in all three days, with about five hours working time each day. The team consisted of three persons. The work outside the meeting ("actions") required in all about four man-days.

The number of "volumes" in the plant was 34, giving an analysis time of about ½hr. per volume, or 1½ man hours per volume.

The number of modifications to the plant depends, of course, on how good the plant design is before the analysis takes place. Since the analysis took place when just the flow sheet, and later, when just an initial P & I D were completed, the scope for plant design improvement was in the present case relatively wide.

In all 14 modifications were made to the plant drawings on the basis of the hazard and operability analysis. Of these, perhaps half would have been made anyway during later design steps. (They would though have required some design review work, and may have required modification to already constructed equipment).

Detailed analysis of benefit is not possible, since the plant was not built as originally designed.

Modifications resulting from analysis of the product reactor.

1) One disturbance added to the alarm and evacuation plan

2) Modification of original flow sheet so that one reserve tank was replaced by two, in order to avoid the possibility of overfilling the reactor.

3) Replacement of a 3-way valve which could lead to blockage of a pipeway.

4) Addition of a pressure monitor on the reactor.

5) Design revision of the reactor charging lid arrangement, to allow interlocking.

6) Non return valves added to reactor feed lines.

7) Temperature alarm on safety valve outlet.

8) Addition of a temperature alarm on brine cooler.

9) Recess flanges specified for column.

10) Temperature and pressure trips added to reactor

11) Procedure points noted
    - emptying procedure
    - shutdown procedure in cold weather

12) Valves added to periodic test list.

13) Changes in ammonia pipework arrangement.

5.1.2.4 Results of the hazop analysis/methanol distillation

The analysis of the distillation plant (the plant subsequently built) took one day (with four man team including one novice). The day involved about five working hours. Work outside the meeting took about two man days.

The number of volumes in the plant was 7, giving an analysis time of about 1 hr. per volume in meetings, and a total analysis time including follow-up work of about 3 man hours per volume.

The number of modifications to the plant was in all 12. This gives an average of about 3-4 hrs. per modification. About half of the modifications would have been found anyway during later design steps, but would almost certainly have involved changes in construction or in ordering of components. One change resulted in a direct saving of equipment (ca. kr. 10.000 life cycle cost).

If the modifications were to have been required during commissioning, then there could have been perhaps a two to three day delay in plant start up. A capitalized value of such a delay is circa kr. 20.000, which puts a value on each man hour used of circa kr. 500 evaluated on this most conservative basis.

5.1.2.5. Modifications resulting from analysis of the distillation plant.

1) Safety valve blowdown lines enter into the top of the safety valve header, to prevent accumulation of liquid behind the safety valves (drain holes are also bored, as a standard practice).

2) Heat tracing added to one valve to prevent blockage

3) U-bend liquid trap added to prevent blowback of methanol vapour to feed tank.

4) Bayonet valve added to feed line to prevent blowback of vapour and resultant fire possibility.

5) Superfluous valve removed from drawing.

6) Temperature alarm added at top of condenser.

7) Pressure high trip added to distillation kettle

8) Brine traps added on methanol tanks.

9) Splash trap moved to before sight glass, rather than after.

10) Temperature alarm on brine trap.

11) Level alarms and switches on receivers.

12) Interlock required on shift between receivers.

Many of the modifications would have been uneconomic if delayed until the plant were built. An example of this is the interchange of a sight glass and splash trap in a condenser outlet. This may reduce the risk of a possible sight glass brekage, due to liquid or vapour hammer. The actual degree of risk is very uncertain probably none at all. But the cost of the change was less than a minutes effort with eraser and pencil. The change brought the design into agreement with GP's standard practices.

5.1.2.6. Comparision of the two hazard analyses

The main differences between the two analysis situations, for the reactor and the distillator were

- the potential risk is much higher for the reactor.

- the distillator analysis could already benefit from analysis of similar equipment on the reactor.

- the analysis tables used for the distillator included check lists for "causes" and "cures".

One might expect, with the use of preprinted lists of causes, that the analysis would go more quickly. In fact this was not the case, the distillator analysis took longer per volume.

One explanation of this could be that the second analysis has fewer "volumes". It is generally observed that later volumes in a plant are analysed more quickly. This is due to the fact that many problems repeat themselves, need not be solved twice. The longer a chain of vessels, the quicker the analysis per vessel.

Another explanation of the additional time taken to analyse the distillator could be that the analysis was more thorough. This could be a result of using a cause check list.

That the distillator cause analysis was more thorough is certainly true. For the volumes on the two plants which correspond to each other (distillation kettle, column, condenser, and two receivers) the following numbers of potential disturbances and problems were recorded.

For the reactor analysis 9 potential disturbances of the distillation unit were recorded, resulting in 2 modifications.

For the distillation analysis - 19 disturbances recorded, resulting in 12 modifications.

The cause check list seems to be a really worth while improvement in the hazard and operability method. Observation during the analysis indicated that it served as a stimulus to fantasy espescially towards the end of a long analysis series, when fantasy and patience are at at low ebb.

The comparison also suggests that what takes most time in an analysis is not the analysis itself, but the problems which arise and the modifications made.

5.1.2.7. Comparison with operating experience

This is discussed later, when experience from commissioning is described.

5.1.2.8. Action error analysis of the distillator operating procedure.

Method

The method chosen for analysis of operating procedures was action error analysis. This method involves.

1) listing each step in the operating procedure.

2) Describing the plant response for each step in the operating procedure. For this the technique of consequence analysis was used.

3) For each action, describing a range of possible error modes, and plant responses to these errors.

Actions and plant events are described using cause consequence diagram notation.

The error modes considered constitute a logically complete list, as follows

ACTION TOO EARLY
ACTION TOO LATE
ACTION OMITTED

ACTION TOO MUCH
ACTION TOO LITTLE
ACTION TOO LONG
ACTION TOO SHORT
ACTION IN WRONG DIRECTION
ACTION ON WRONG OBJECT
WRONG ACTION

For recording the plant consequences, the following consequence analysis procedure was used

1) Immediate consequence of the action on the directly affected component were described and recorded.

2) Effects of the changes in the first component on those components directly connected to it were described, taking account of alternative consequences which could occur because of different component states.

3) Step two is repeated tracing effects from component to component along pipes and cables, taking account of alternative components states at each stage

When using this technique, it is important to remember the full range of effects which a disturbance can cause. In particular if it is important to remember the effects which can arise as a result of flow reversal, and to remember that pressure effects can travel upstream, against the normal flow of a liquid. Fires, vibration, pipe whip, and escaping jets of liquid can transfer effects via routes which are not shown on flow sheets or piping diagrams.

Applying the action error procedure can be both time consuming and expensive. To reduce the effort involves, pre-printed action error analysis sheets were used. One sheet is used for each action in the normal operating procedure, and extension sheets are provided for those actions or errors with especially complex consequences.

Fig. 6. Examples of Action Error Sheets.

PROCEDURE: ______ STEP: 6

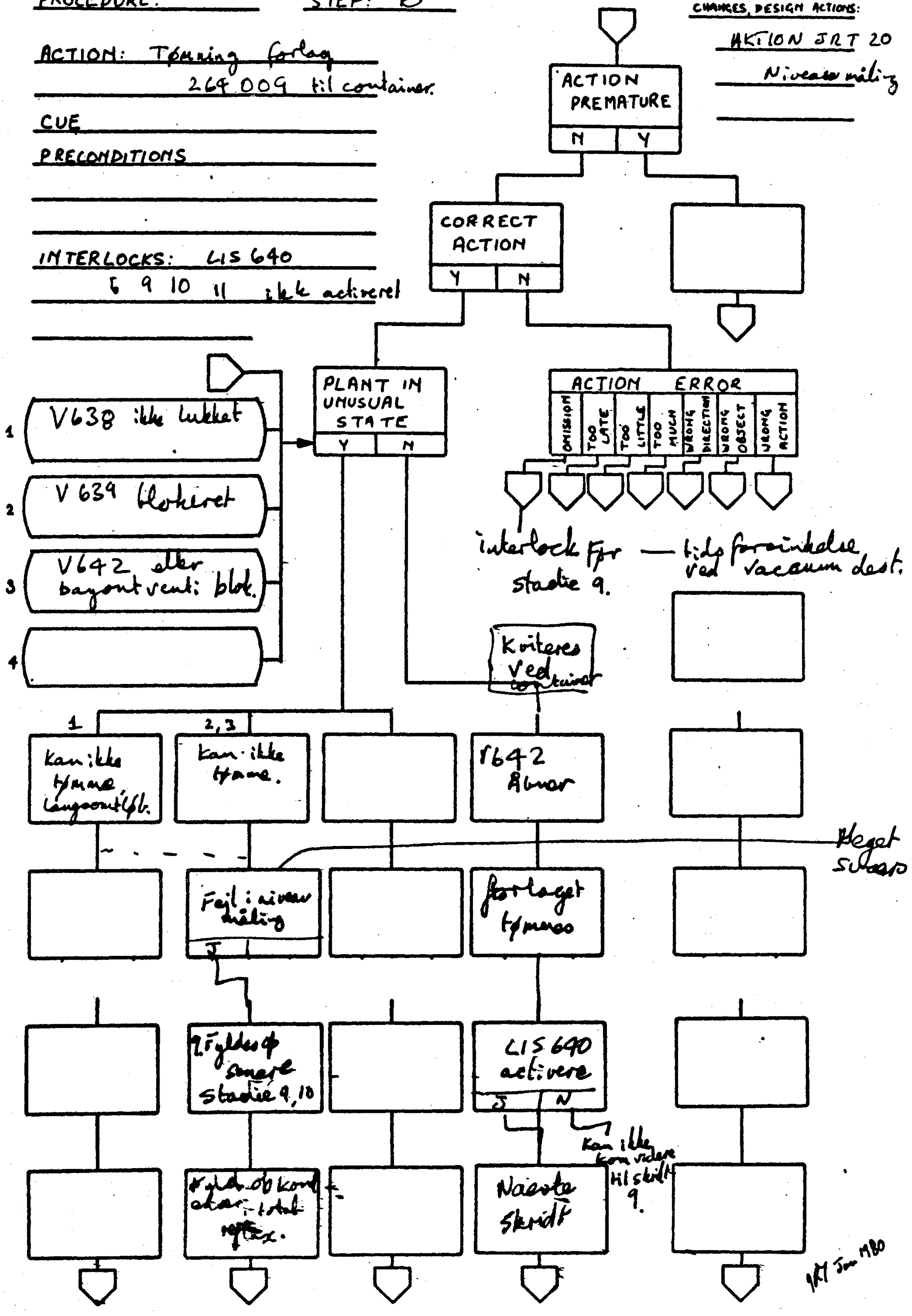
ACTION: Tømning forlag 264 009 til container.

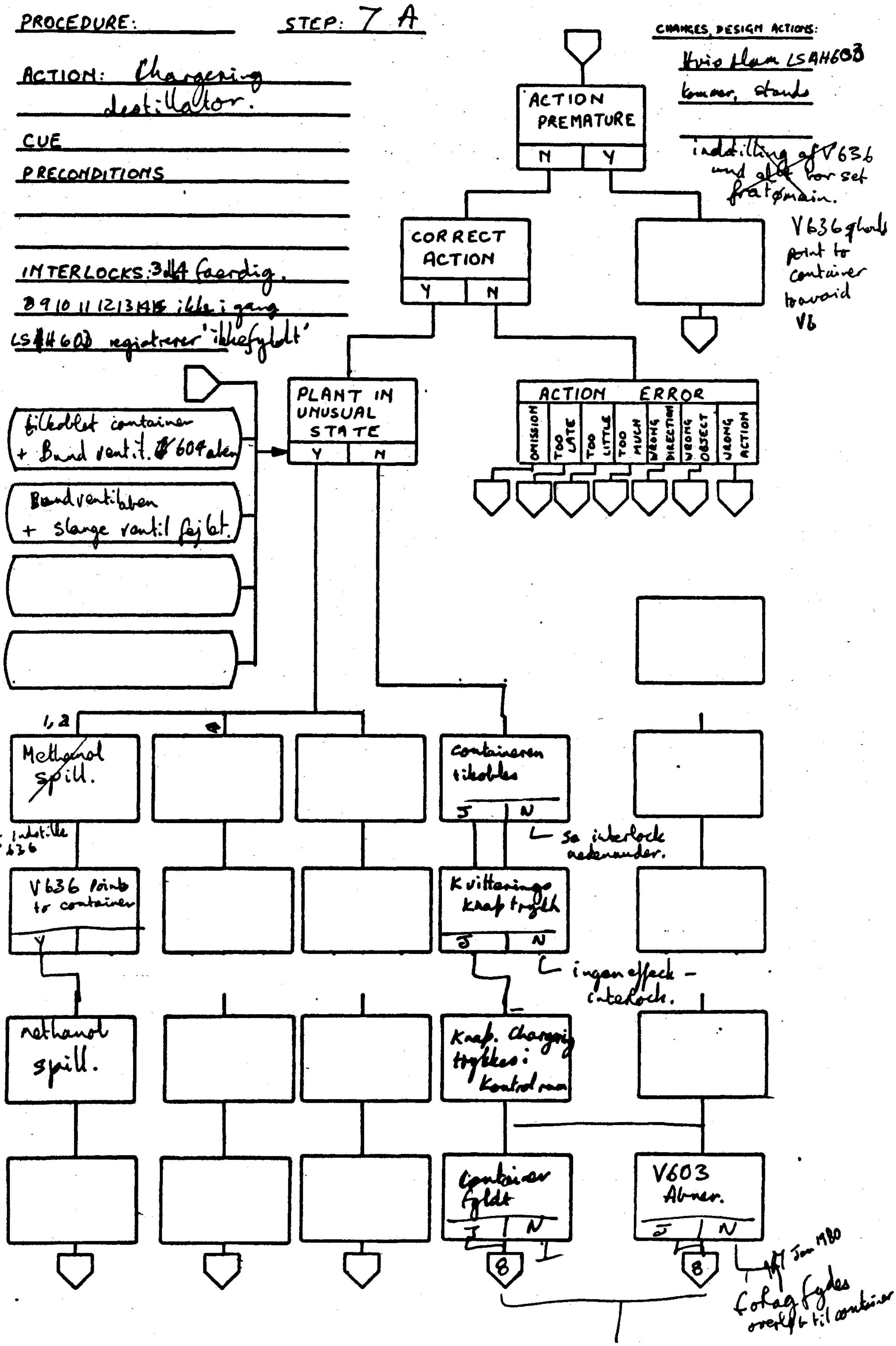
CUE

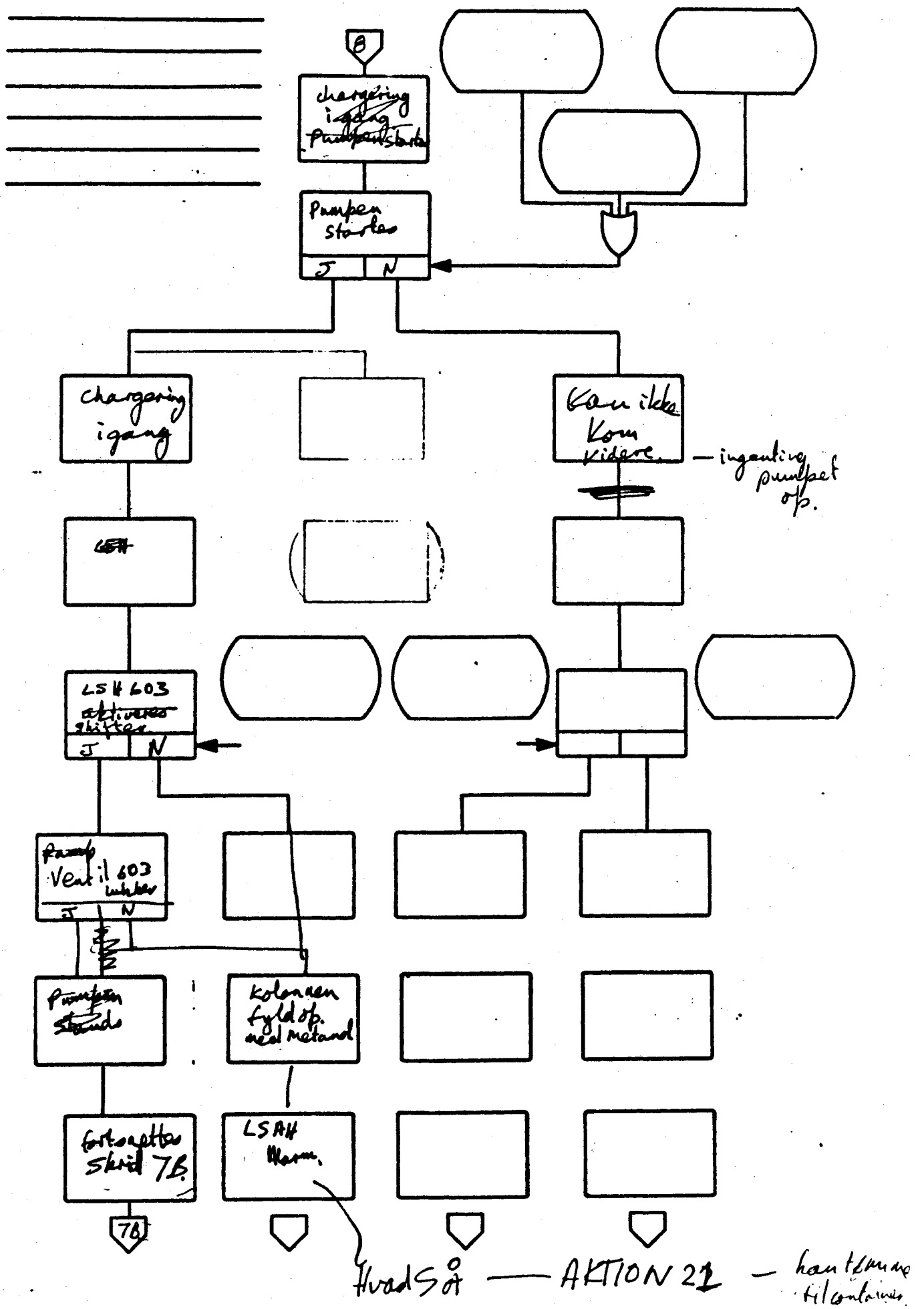
PRECONDITIONS

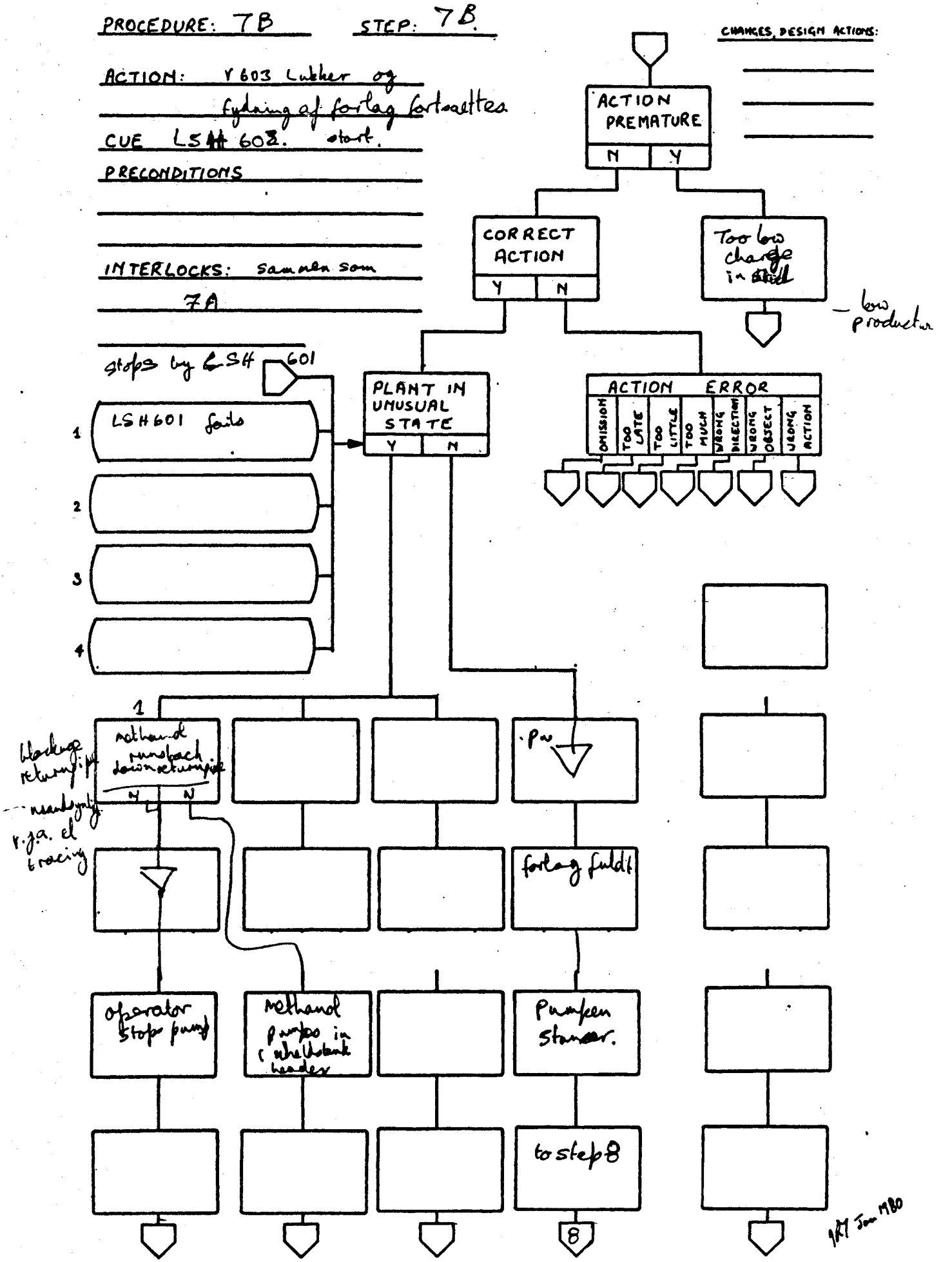
INTERLOCKS: LIS 640 6 9 10 11 ikke activeret

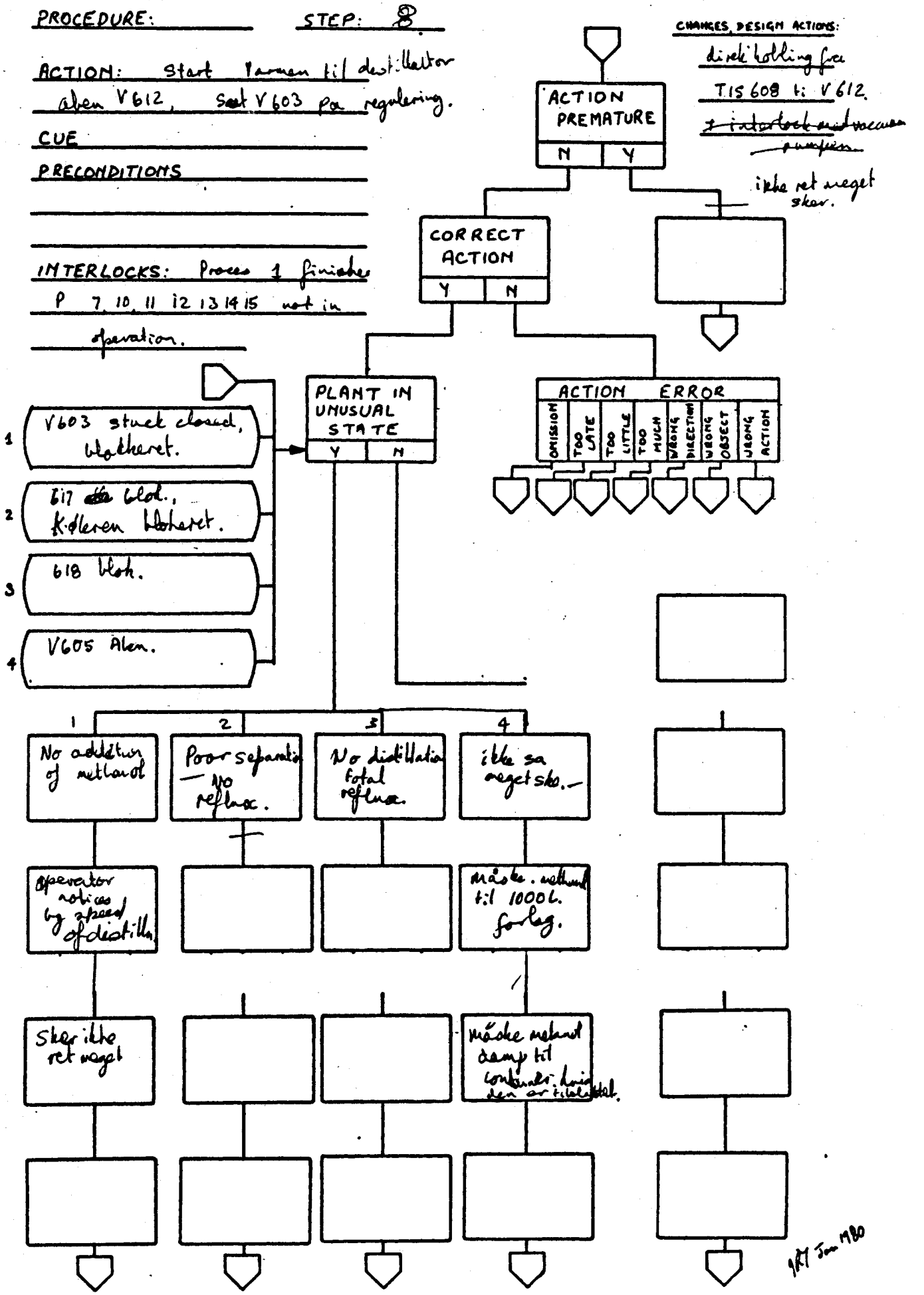
CHANGES, DESIGN ACTIONS: AKTION JRT 20 Niveau måling



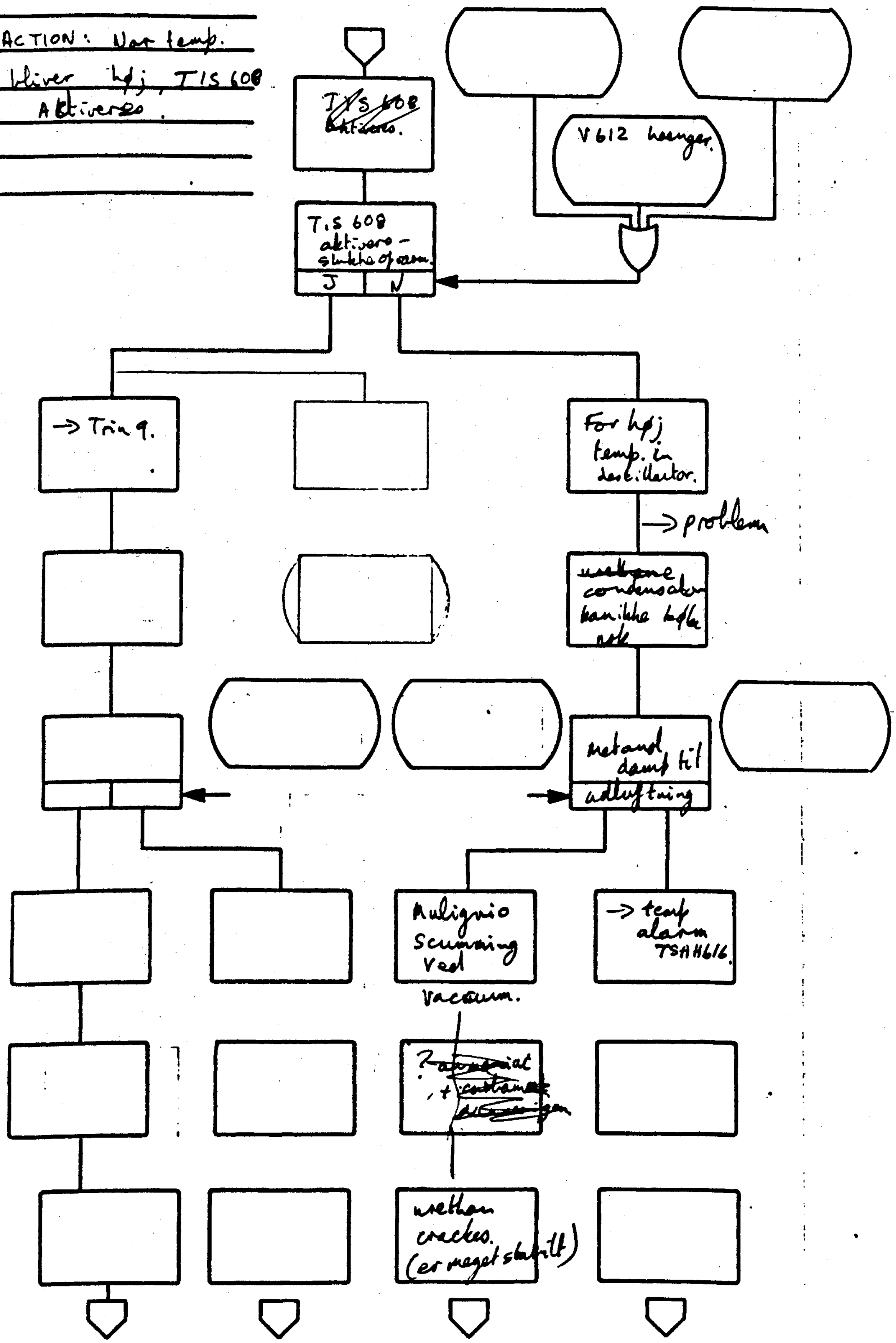

PROCEDURE:
STEP: 7 A
ACTION: Chargering destillator.
CUE
PRECONDITIONS
INTERLOCKS: 3 4 faerdig.
8 9 10 11 12 13 14 15 ikke i gang
LS 603 registrerer 'ikke fyldt'
CHANGES, DESIGN ACTIONS:
V636 should point to container toavoid V6
ACTION PREMATURE
N
Y
CORRECT ACTION
Y
N
PLANT IN UNUSUAL STATE
Y
N
ACTION ERROR
OMISSION
TOO LATE
TOO LITTLE
TOO MUCH
WRONG DIRECTION
WRONG OBJECT
WRONG ACTION
1
tilkoblet container
2
+ slange ventil fejlet.
3
4
1,2
Methanol spill.
No
V636 points to container
Y
methanol spill.
containeren tilkobles
J
N
se interlock nedenunder.
Kvitterings knap trykkes
J
N
ingen effekt - interlock.
Knap. Charging trykkes: Kontrolrum
Container fyldt
J
N
V603 åbner.
J
N
8
8


B
charging igang
Pumpen starter
J
N
charging igang
Kan ikke Kom videre.
— ingenting pumpet op.
LSH 603
J
N
Pumpen Vent. til 603 inhiber
J
N
Pumpen stoppes
kolonnen fyldt op. med metanol
LSAH Alarm.
forbrugeren Skrid 7B
7B
Hvad Så — AKTION 21 — hanteringen til containeren


PROCEDURE: 7B
STEP: 7B.
ACTION: V 603 Lukker og fyldning af forlag fortsættes
CUE LSH 603. start.
PRECONDITIONS
INTERLOCKS: samme som 7A
CHANGES, DESIGN ACTIONS:
ACTION PREMATURE
N
Y
CORRECT ACTION
Y
N
Too low charge in
low production
stops by LSH 601
PLANT IN UNUSUAL STATE
Y
N
ACTION ERROR
OMISSION
TOO LATE
TOO LITTLE
TOO MUCH
WRONG DIRECTION
WRONG OBJECT
WRONG ACTION
1
LSH 601 fails
2
3
4
1
methanol runback down return pipe
N
N
Pw
forlag fuldt
operator stops pump
methanol pumps in methanol header
Pumpen starter.
to step 8
8
IRT Jan 1980


PROCEDURE:
STEP: 8.
ACTION: Start Varmen til destillator Aben V612, Sæt V603 på regulering.
CUE
PRECONDITIONS
INTERLOCKS: Proces 1 finished P 7, 10, 11 12 13 14 15 not in operation.
CHANGES, DESIGN ACTIONS:
direkt kobling fra TIS 608 til V612.
ikke ret meget skær.
ACTION PREMATURE
N
Y
CORRECT ACTION
Y
N
PLANT IN UNUSUAL STATE
Y
N
ACTION ERROR
OMISSION
TOO LATE
TOO LITTLE
TOO MUCH
WRONG DIRECTION
WRONG OBJECT
WRONG ACTION
1 V603 stuck closed, blokeret.
2 617 blok., Køleren blokeret.
3 618 blok.
4 V605 Aben.
1
2
3
4
No addition of methanol
Poor separation — no reflux.
No distillation total reflux.
ikke så meget skø.-
operator notices by speed of distillation
måske. methanol til 1000 l. forlag.
Sker ikke ret noget
måske methanol damp til kondensator hvis den er tilstoppet.
JKT Jan 1980

ACTION: Nar temp. bliver høj, TIS 608 Aktiveres.



The sheets also provide space for alternative event sequences arising from unusual states or failure states in the plant hardware.

An important aspect in fixing probabilities of accidents arising from operator errors is whether the plant guides or "cues" the operator to perform the correct action, and whether there is a possibility for observing and correcting the results of an error. Although the sheets are intended primarily for finding possibilities rather than probabilities of error, cueing and correction aspects are included on the analysis sheets.

5.1.3.2. Observations during the analysis

The number of operator errors possible for this plant are quite limited, because of the extensive use of interlocks. No attempt was made to analyse double failures (interlock failure plus error) except in those cases which would lead directly to a dangerous state.

The parts of the consequence sheets treating hardware failures proved very valuable. The main emphasis of the analysis turned out in practice to deal with these.

Some interesting new principle could be observed in the analysis.

1) The list of "abnormal plant states" entered into the diagram could in principle be endless. But it is sufficient to limit the list to

   a) Abnormal states within the physical boundary normally affected by the action.

   b) Faults in equipment normally activated by the action.

c) Faults which change the boundary of the part of the plant normally affected. (eg. erroneously open valves on the boundary).

2) It is easier to derive the ultimate consequences of an error by following the erroneous event chain to its conclusion, than it is to remember a potentially hazardous state and take it up again for examination later, at the point in the procedure where danger becomes actual.

5.1.3.3. Results of the analysis

The analysis took three days, for a three man team. Since 15 operational steps were involved, that means that on average one hour (three man hours) were used per operation step.
In all 23 plant modifications were made on the basis of the analysis. This seems to indicate that in spite of the large amount of time used, the results made the analysis worthwhile. The changes are shown in Section 5.1.3.4. On the same basis as the calculation for the hazard and operability analysis, the capitalized value of the changes should be a minimum of about kr. 30.000.

Because of interlocks only three errors appeared initially dangerous, and when further interlocks were added, even these were irrelevant. An exception is an action which was overlooked in the analysis (see later) because "recovery actions" were not analysed.

5.1.3.4. Changes in the plant as a result of the action/error analysis.

1) Bayonet valves on charging and discharging hoses.

2) Change in sequence of interlock at discharge stations. -

the sequence now is - couple hoses, depress interlock button locally, depress activation button in control room.

3) Vacuum breaker on ground tank.

4) Flame arrester on ground tank.

5) Deleted

6) V636 removed.

7) Consequences of overflow in feed tank reduced.

8) Change from a positive displacement to centrifugal pump.

9) Temperature measurement re-sited.

10) Extra check of level measurement in the procedure.

11) New time delayed interlock on step 9.

12) LSAH 603 alarm replaced by trip

13) New instructions to prevent overfilling with methanol.

14) Deleted

15) Check valve on pump.

16) V647 fail open to atmosphere.

17) Change of layout for distillate distribution valves to preserve purity.

18) Interlock to prevent emptying 008,009 during distillation.

19) On alarm TSAH 616, V612 doses, V619 opens, and pump stops.

20) Position feedback from V636.

21) Regulation during boiling out for cleaning.

22) V 644, V 645 are in "warm" position except during distillation.

23) Weight interlock on drum filling.

5.1.3.5. Comparison of the action error analysis with the hazard and operability analysis.

Since the hazard and operability analysis is in principle a complete analysis of disturbances, one might reasonably ask why the action error analysis revealed new problems. An examination of the new problems found reveals the reason.

1) Need for bayonet valves.

   Breach of retaining boundary was not treated directly for all vessels in the hazard and operability analysis because operating procedures were unavailable at the Hazop stage. Otherwise, the possibility of a single operation error opening valves would presumably have been found.

2) V 622 remaining stuck open

   In the hazard analysis the possibility of V622 being opened was not really considered at all - again procedures were not available, and hence the problem of not closing did not arise. If breach of boundary had been considered, then presumably only "fails open" would have been considered. "Valve remains open from previous step" was added as an entry in the check list.

3) Vacuum breaker on the ground tank

The action error analysis was simply more thorough, since it traced consequences beyond the boundaries specified for the analysis.

4) Check that plant activities stop at the end of a procedure step. (This check was recommended but proved difficult to implement).

This is naturally related to procedural problems.

5) Of two valves 636, 605, one superfluous

Only when it came to checking the operation of the plant was the purpose of these two questioned.

6) Sequence change on interlock

Clearly a prcedural problem.

7) Placement of temperature measurement

This concerns correctness of measurement during a state change - a procedural problem. The measurement would probably work well on a continously operating plant.

8) Temperature trip bypasses the PLC
(This recommendation was not eventually adopted)

This is again a procedural problem - an action is required to be reliable at a particular stage of a procedure, but is irrelevant at other stages.

The general gist of these examples is that the "normal state" for a batch processing plant can be any one of a number of states. What these are becomes obvious when procedures are exami-

ned in detail. The hazard and operability analysis could for example examine why temperature was too high during a particular stage, and find that a trip had not occurred. But the effect would be something like making an action error analysis backwards. The first step would have to be to make a procedural analysis forwards, in order to discover what was "normal".

An important point is that purpose of control devices and instruments is largely overlooked in the hazard and operability analysis as performed here, whereas purpose is a clear aspect of the action error analysis. A major conclusion is that purpose of each volume, each control device, and each operation step should be documented.

5.1.4. Error cause analysis

More for illustrative purposes than for any other reason, a cause analyses of the error

"operator presses drum filling interlock buttom
at the wrong time".

was carried out.

The method was to use a check list in diagram form, based on an error data calssification by Rasmussen (2). Three cases are examined.

- Button is pushed while there is no residue drum present.
- Button is pushed while the resiue drum has already 100 kg of residue in it.
- Button is pushed while the residue is scrumming.

For illustrative purposes, weighing machine interlocks are assumed to have failed. The results are shown in fig. 7.

Fig. 7. Excerpt from the Error Cause Analysis.

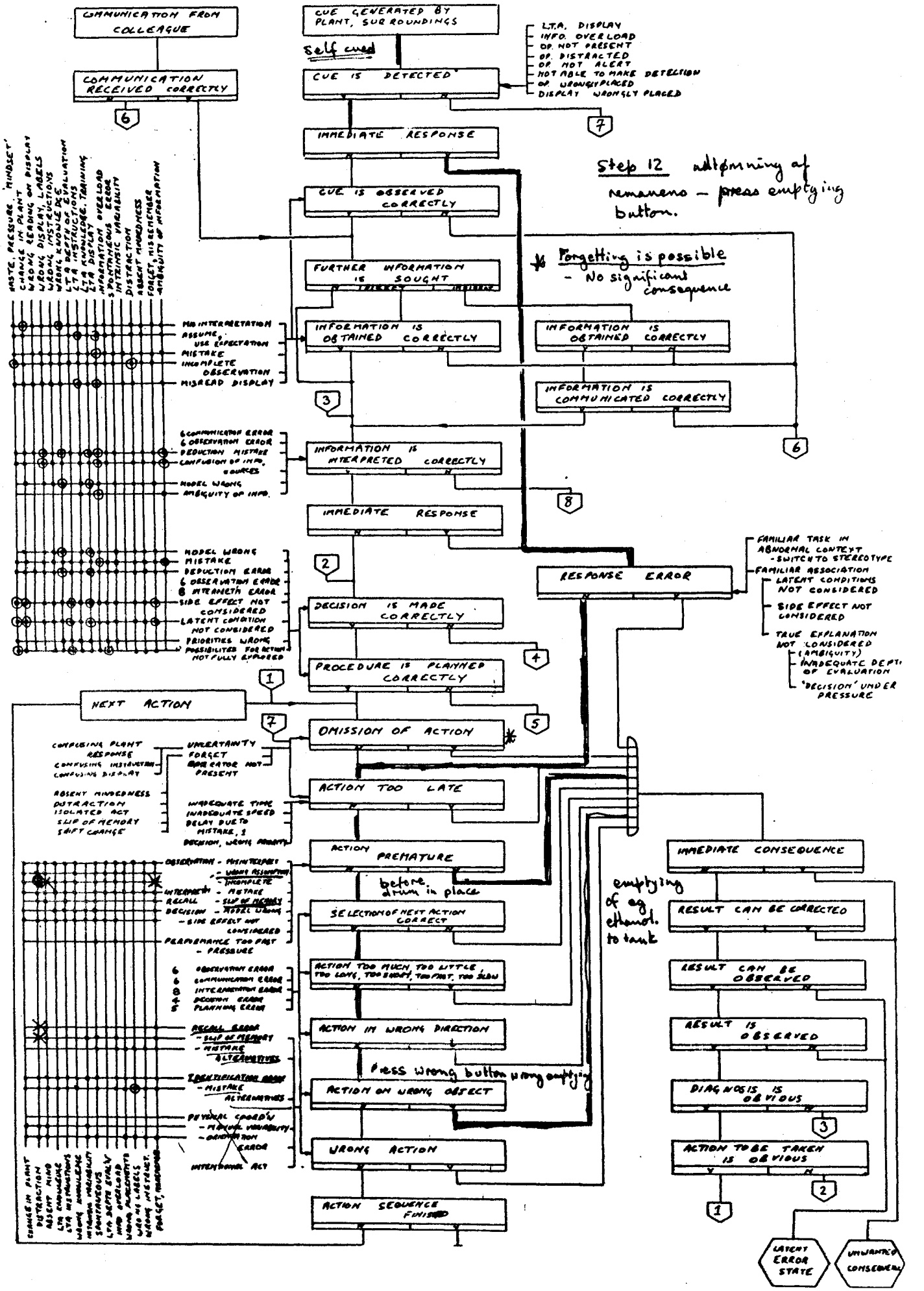
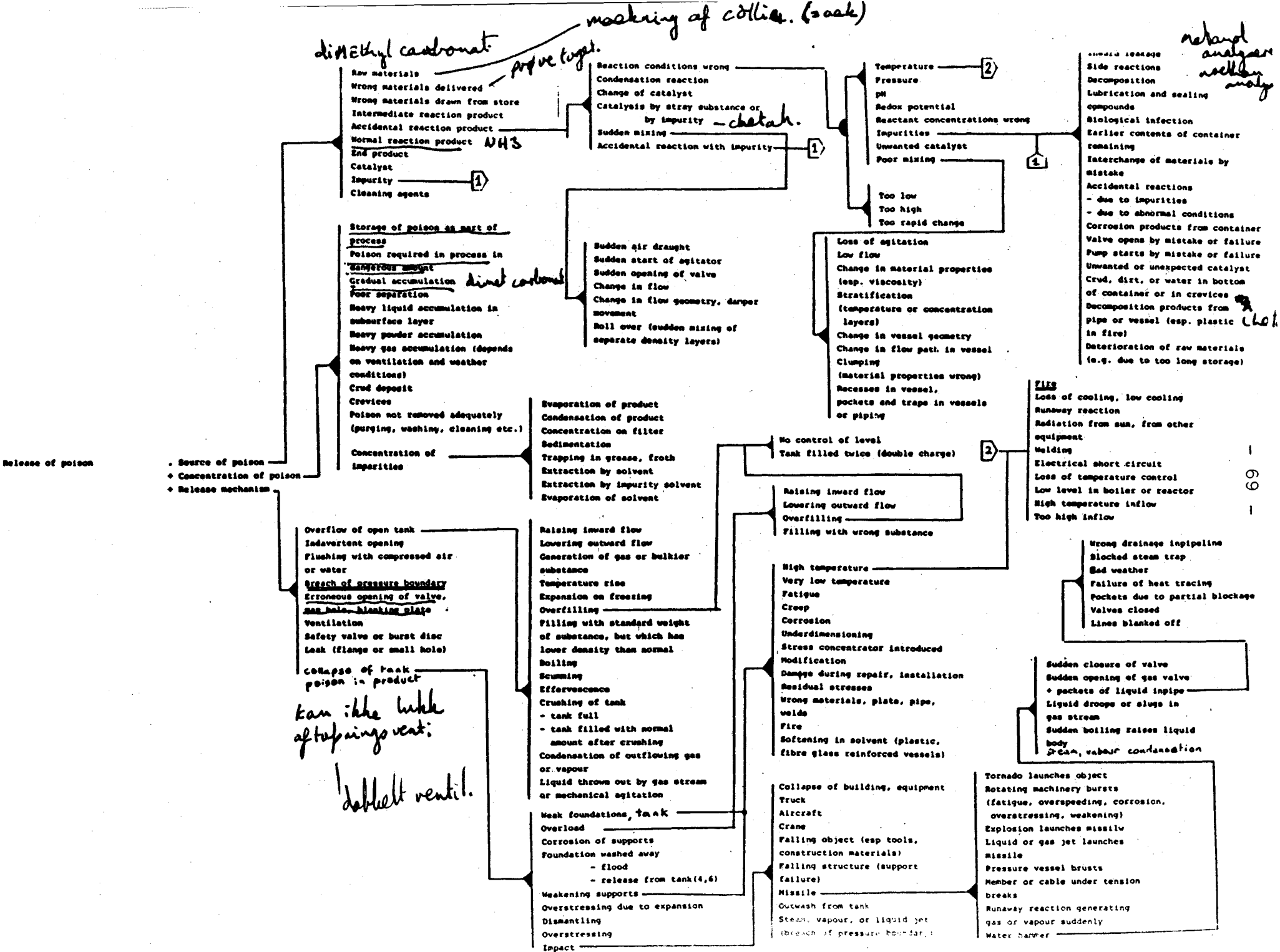
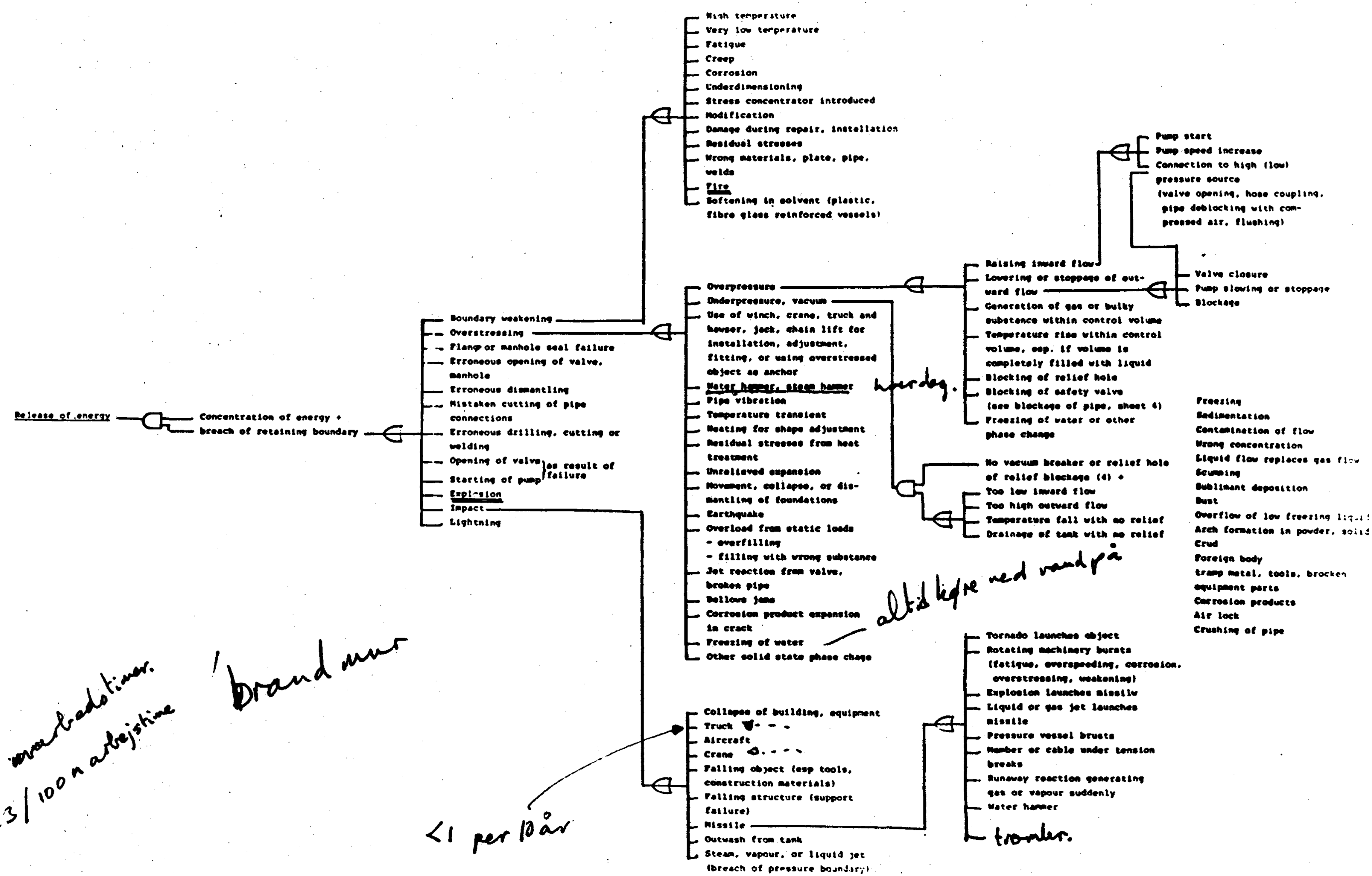
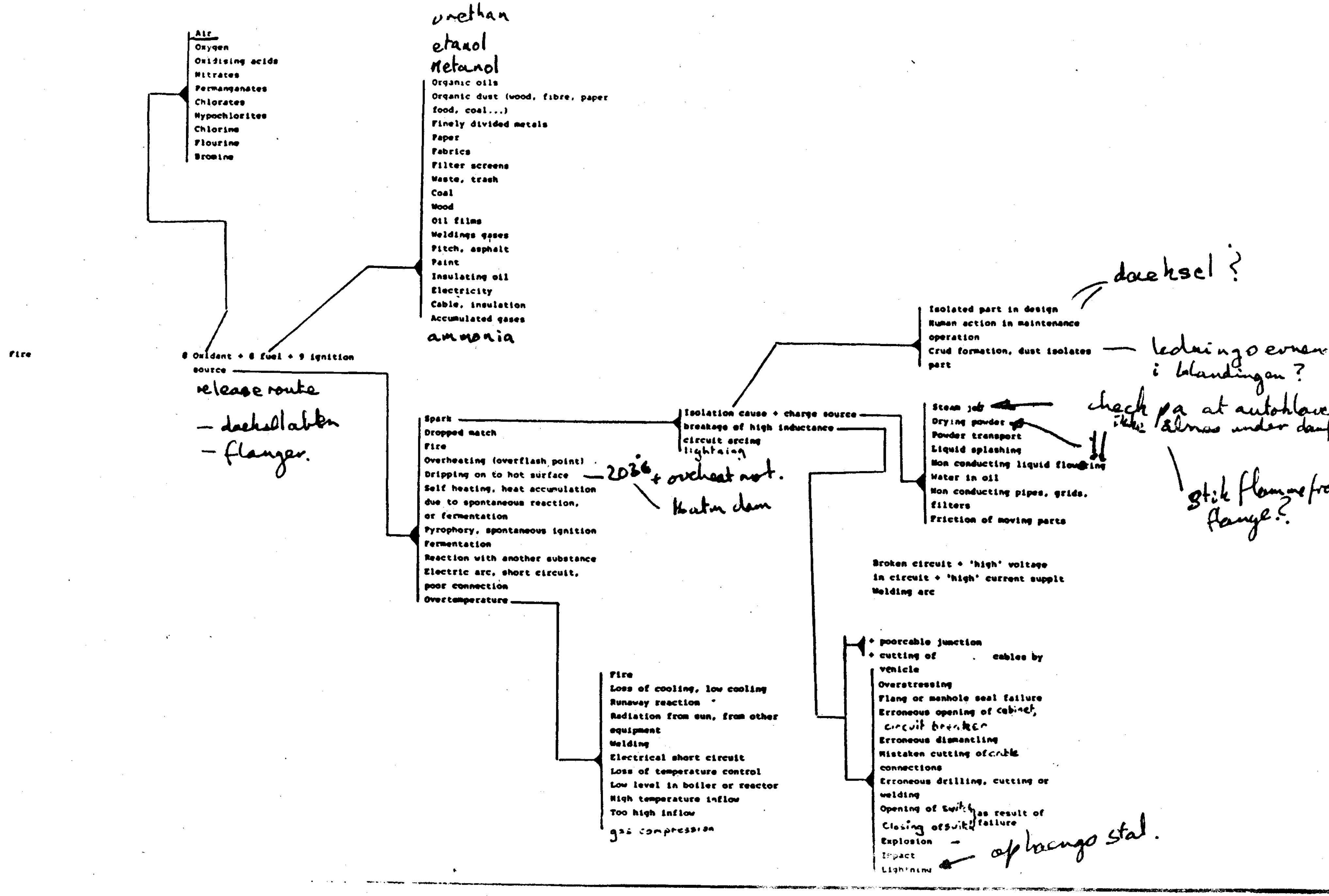

COMMUNICATION FROM COLLEAGUE
COMMUNICATION RECEIVED CORRECTLY
CUE GENERATED BY PLANT, SURROUNDINGS
Self cued
CUE IS DETECTED
L.T.A. DISPLAY
INFO. OVERLOAD
OP. NOT PRESENT
OP. DISTRACTED
OP. NOT ALERT
NOT ABLE TO MAKE DETECTION
OP. WRONGLY PLACED
DISPLAY WRONGLY PLACED
IMMEDIATE RESPONSE
Step 12 adjourning of remanence – press emptying button.
CUE IS OBSERVED CORRECTLY
FURTHER INFORMATION IS SOUGHT
Forgetting is possible
- No significant consequence
INFORMATION IS OBTAINED CORRECTLY
INFORMATION IS COMMUNICATED CORRECTLY
INFORMATION IS INTERPRETED CORRECTLY
IMMEDIATE RESPONSE
DECISION IS MADE CORRECTLY
PROCEDURE IS PLANNED CORRECTLY
NEXT ACTION
OMISSION OF ACTION
ACTION TOO LATE
ACTION PREMATURE
before drum in place
SELECTION OF NEXT ACTION CORRECT
ACTION TOO MUCH, TOO LITTLE, TOO LONG, TOO SHORT, TOO FAST, TOO SLOW
ACTION IN WRONG DIRECTION
Press wrong button wrong emptying
ACTION ON WRONG OBJECT
WRONG ACTION
ACTION SEQUENCE FINISHED
RESPONSE ERROR
FAMILIAR TASK IN ABNORMAL CONTEXT - SWITCH TO STEREOTYPE
FAMILIAR ASSOCIATION
LATENT CONDITIONS NOT CONSIDERED
SIDE EFFECT NOT CONSIDERED
TRUE EXPLANATION NOT CONSIDERED
(AMBIGUITY)
INADEQUATE DEPTH OF EVALUATION
'DECISION' UNDER PRESSURE
IMMEDIATE CONSEQUENCE
RESULT CAN BE CORRECTED
RESULT CAN BE OBSERVED
RESULT IS OBSERVED
DIAGNOSIS IS OBVIOUS
ACTION TO BE TAKEN IS OBVIOUS
emptying of eg. ethanol. to tank
LATENT ERROR STATE
UNWANTED CONSEQUENCE
HASTE, PRESSURE, 'MINDSET'
CHANGE IN PLANT
WRONG READING OR DISPLAY
WRONG DISPLAY LABELS
WRONG INSTRUCTIONS
MODEL DEPTH OF EVALUATION
L.T.A. INSTRUCTIONS
L.T.A. KNOWLEDGE, TRAINING
L.T.A. DISPLAY
INFORMATION OVERLOAD
SPONTANEOUS ERROR
INTRINSIC VARIABILITY
DISTRACTION
ABSENT MINDEDNESS
FORGET, MISREMEMBER
AMBIGUITY OF INFORMATION
MIS-INTERPRETATION
ASSUME, USE EXPECTATION
MISTAKE
INCOMPLETE OBSERVATION
MISREAD DISPLAY
COMMUNICATION ERROR
OBSERVATION ERROR
DEDUCTION MISTAKE
CONFUSION OF INFO. SOURCES
MODEL WRONG
AMBIGUITY OF INFO.
MODEL WRONG
MISTAKE
DEDUCTION ERROR
OBSERVATION ERROR
INTERPRETATION ERROR
SIDE EFFECT NOT CONSIDERED
LATENT CONDITION NOT CONSIDERED
PRIORITIES WRONG
POSSIBILITIES FOR ACTION NOT FULLY EXPLORED
CONFUSING PLANT RESPONSE
CONFUSING INSTRUCTION
CONFUSING DISPLAY
ABSENT MINDEDNESS
DISTRACTION
ISOLATED ACT
SLIP OF MEMORY
SHIFT CHANGE
UNCERTAINTY
FORGET
OPERATOR NOT PRESENT
INADEQUATE TIME
INADEQUATE SPEED
DELAY DUE TO MISTAKE, I DECISION, WRONG PRIORITY
OBSERVATION - MISINTERPRET
- WRONG ASSUMPTION
- INCOMPLETE
INTERPRETATION - MISTAKE
RECALL - SLIP OF MEMORY
DECISION - MODEL WRONG
- SIDE EFFECT NOT CONSIDERED
PERFORMANCE TOO FAST
- PRESSURE
6 OBSERVATION ERROR
6 COMMUNICATION ERROR
8 INTERPRETATION ERROR
4 DECISION ERROR
5 PLANNING ERROR
RECALL ERROR
- SLIP OF MEMORY
- MISTAKE
ALTERNATIVES
IDENTIFICATION ERROR
- MISTAKE
ALTERNATIVES
PERCEPTUAL CONFUSION
- PERCEPTUAL VARIABILITY
- ORIENTATION
ERROR
INTENTIONAL ACT
CHANGE IN PLANT
DISTRACTION
ABSENT MIND
LTA INSTRUCTIONS
LTA KNOWLEDGE
WRONG INTENTION
SPONTANEOUS
LTA DEPTH EVAL.
WRONG PRIORITY
WRONG LABELS
WRONG INTERPRET.
FORGET, MISREMEMB.

Fig. 8. Significant excerpts from the hazard tree analysis.


Release of poison
. Source of poison
+ Concentration of poison
+ Release mechanism
Raw materials
Wrong materials delivered
Wrong materials drawn from store
Intermediate reaction product
Accidental reaction product
Normal reaction product
End product
Catalyst
Impurity
Cleaning agents
Storage of poison as part of process
Poison required in process in dangerous amount
Gradual accumulation
Poor separation
Heavy liquid accumulation in subsurface layer
Heavy powder accumulation
Heavy gas accumulation (depends on ventilation and weather conditions)
Crud deposit
Crevices
Poison not removed adequately (purging, washing, cleaning etc.)
Concentration of impurities
Evaporation of product
Condensation of product
Concentration on filter
Sedimentation
Trapping in grease, froth
Extraction by solvent
Extraction by impurity solvent
Evaporation of solvent
Overflow of open tank
Inadvertent opening
Flushing with compressed air or water
Breach of pressure boundary
Erroneous opening of valve, man hole, blanking plate
Ventilation
Safety valve or burst disc
Leak (flange or small hole)
Collapse of tank
poison in product
Raising inward flow
Lowering outward flow
Generation of gas or bulkier substance
Temperature rise
Expansion on freezing
Overfilling
Filling with standard weight of substance, but which has lower density than normal
Boiling
Scumming
Effervescence
Crushing of tank
- tank full
- tank filled with normal amount after crushing
Condensation of outflowing gas or vapour
Liquid thrown out by gas stream or mechanical agitation
Weak foundations, tank
Overload
Corrosion of supports
Foundation washed away
- flood
- release from tank(4,6)
Weakening supports
Overstressing due to expansion
Dismantling
Overstressing
Impact
Reaction conditions wrong
Condensation reaction
Change of catalyst
Catalysis by stray substance or by impurity
Sudden mixing
Accidental reaction with impurity
Sudden air draught
Sudden start of agitator
Sudden opening of valve
Change in flow
Change in flow geometry, damper movement
Roll over (sudden mixing of separate density layers)
Temperature
Pressure
pH
Redox potential
Reactant concentrations wrong
Impurities
Unwanted catalyst
Poor mixing
Too low
Too high
Too rapid change
Loss of agitation
Low flow
Change in material properties (esp. viscosity)
Stratification (temperature or concentration layers)
Change in vessel geometry
Change in flow path in vessel
Clumping (material properties wrong)
Recesses in vessel, pockets and traps in vessels or piping
No control of level
Tank filled twice (double charge)
Raising inward flow
Lowering outward flow
Overfilling
Filling with wrong substance
High temperature
Very low temperature
Fatigue
Creep
Corrosion
Underdimensioning
Stress concentrator introduced
Modification
Damage during repair, installation
Residual stresses
Wrong materials, plate, pipe, welds
Fire
Softening in solvent (plastic, fibre glass reinforced vessels)
Collapse of building, equipment
Truck
Aircraft
Crane
Falling object (esp tools, construction materials)
Falling structure (support failure)
Missile
Outwash from tank
Steam, vapour, or liquid jet (breach of pressure boundary)
Tornado launches object
Rotating machinery bursts (fatigue, overspeeding, corrosion, overstressing, weakening)
Explosion launches missile
Liquid or gas jet launches missile
Pressure vessel bursts
Member or cable under tension breaks
Runaway reaction generating gas or vapour suddenly
Water hammer
Fire
Loss of cooling, low cooling
Runaway reaction
Radiation from sun, from other equipment
Welding
Electrical short circuit
Loss of temperature control
Low level in boiler or reactor
High temperature inflow
Too high inflow
Wrong drainage inpipeline
Blocked steam trap
Bad weather
Failure of heat tracing
Pockets due to partial blockage
Valves closed
Lines blanked off
Sudden closure of valve
Sudden opening of gas valve
+ packets of liquid inpipe
Liquid droops or slugs in gas stream
Sudden boiling raises liquid body
Steam, vapour condensation
Leakage
Side reactions
Decomposition
Lubrication and sealing compounds
Biological infection
Earlier contents of container remaining
Interchange of materials by mistake
Accidental reactions
- due to impurities
- due to abnormal conditions
Corrosion products from container
Valve opens by mistake or failure
Pump starts by mistake or failure
Unwanted or unexpected catalyst
Crud, dirt, or water in bottom of container or in crevices
Decomposition products from pipe or vessel (esp. plastic in fire)
Deterioration of raw materials (e.g. due to too long storage)
1
2
69
1


Release of energy
Concentration of energy +
breach of retaining boundary
Boundary weakening
Overstressing
Flange or manhole seal failure
Erroneous opening of valve, manhole
Erroneous dismantling
Mistaken cutting of pipe connections
Erroneous drilling, cutting or welding
Opening of valve
Starting of pump
as result of failure
Expl-sion
Impact
Lightning
High temperature
Very low temperature
Fatigue
Creep
Corrosion
Underdimensioning
Stress concentrator introduced
Modification
Damage during repair, installation
Residual stresses
Wrong materials, plate, pipe, welds
Fire
Softening in solvent (plastic, fibre glass reinforced vessels)
Overpressure
Underpressure, vacuum
Use of winch, crane, truck and hawser, jack, chain lift for installation, adjustment, fitting, or using overstressed object as anchor
Water hammer, steam hammer
Pipe vibration
Temperature transient
Heating for shape adjustment
Residual stresses from heat treatment
Unrelieved expansion
Movement, collapse, or dismantling of foundations
Earthquake
Overload from static loads
- overfilling
- filling with wrong substance
Jet reaction from valve, broken pipe
Bellows jams
Corrosion product expansion in crack
Freezing of water
Other solid state phase chage
Raising inward flow
Lowering or stoppage of outward flow
Generation of gas or bulky substance within control volume
Temperature rise within control volume, esp. if volume is completely filled with liquid
Blocking of relief hole
Blocking of safety valve (see blockage of pipe, sheet 4)
Freezing of water or other phase change
Pump start
Pump speed increase
Connection to high (low) pressure source (valve opening, hose coupling, pipe deblocking with compressed air, flushing)
Valve closure
Pump slowing or stoppage
Blockage
Freezing
Sedimentation
Contamination of flow
Wrong concentration
Liquid flow replaces gas flow
Scumming
Sublimant deposition
Dust
Overflow of low freezing liquid
Arch formation in powder, solid
Crud
Foreign body
tramp metal, tools, brocken equipment parts
Corrosion products
Air lock
Crushing of pipe
No vacuum breaker or relief hole of relief blockage (4) +
Too low inward flow
Too high outward flow
Temperature fall with no relief
Drainage of tank with no relief
Collapse of building, equipment
Truck
Aircraft
Crane
Falling object (esp tools, construction materials)
Falling structure (support failure)
Missile
Outwash from tank
Steam, vapour, or liquid jet (breach of pressure boundary)
Tornado launches object
Rotating machinery bursts (fatigue, overspeeding, corrosion, overstressing, weakening)
Explosion launches missilw
Liquid or gas jet launches missile
Pressure vessel brusts
Member or cable under tension breaks
Runaway reaction generating gas or vapour suddenly
Water hammer


Fire
8 Oxidant + 8 fuel + 9 ignition source
Air
Oxygen
Oxidising acids
Nitrates
Permanganates
Chlorates
Hypochlorites
Chlorine
Flourine
Bromine
Organic oils
Organic dust (wood, fibre, paper food, coal...)
Finely divided metals
Paper
Fabrics
Filter screens
Waste, trash
Coal
Wood
Oil films
Weldings gases
Pitch, asphalt
Paint
Insulating oil
Electricity
Cable, insulation
Accumulated gases
Spark
Dropped match
Fire
Overheating (overflash point)
Dripping on to hot surface
Self heating, heat accumulation due to spontaneous reaction, or fermentation
Pyrophory, spontaneous ignition
Fermentation
Reaction with another substance
Electric arc, short circuit, poor connection
Overtemperature
Isolation cause + charge source
breakage of high inductance circuit arcing
Isolated part in design
Human action in maintenance operation
Crud formation, dust isolates part
Steam jet
Drying powder
Powder transport
Liquid splashing
Non conducting liquid flowing
Water in oil
Non conducting pipes, grids, filters
Friction of moving parts
Broken circuit + 'high' voltage in circuit + 'high' current supplt
Welding arc
+ poorcable junction
+ cutting of cables by vehicle
Overstressing
Flang or manhole seal failure
Erroneous opening of
Erroneous dismantling
Mistaken cutting of
connections
Erroneous drilling, cutting or welding
Opening of
as result of failure
Explosion
Impact
Lightning
Fire
Loss of cooling, low cooling
Runaway reaction
Radiation from sun, from other equipment
Welding
Electrical short circuit
Loss of temperature control
Low level in boiler or reactor
High temperature inflow
Too high inflow

5.1.5. Hazard tree analysis

As a cross check on the other analyses, a hazard tree analysis of the plant was carried out. The purpose of such an analysis is to try to discover if there is some obscure failure or accident phenomenon in the plant which has been overlooked by the more standard analyses.

The method makes use of an extensive check list of accident phenomena, structured in the form of a fault tree. The list has been built up through examination of failure mechanism in some 2.000 accident case stories (see 1).

In use, relevant parts of the check list are marked with red ink. Because the list is structured, it is not generally necessary to examine and consider all failure possibilities - irrelevant parts can generally be discarded as the highest level of the hazard tree structure is considered.

The analysis took about 20 minutes, for a three man team. It revealed one potential hazard which had been overlooked and resulted in one modification to procedures.

5.1.6. Observations and analysis prior to and during commissioning

The plant was commissioned during November 1980. The commissioning itself took four days, with a precommissioning check out over a period of one week.

It is impossible to observe all possible failure problems by an analysis of drawings alone. Apart from any other reason, not all plant details appear on drawings. For this reason a further check of the plant was carried out during commissioning.

An attempt was made to use a check list of potential problems. However, at the time of the analysis the list was only partially developed. As a result, the plant was checked during commissioning by a combination of personal observation and formal check list checks. Consequently, the commissioning served as a help in developing check lists. (A formal trial of their effectiviness is planned later, on another part of the plant). This resulting lists are shown in appendix 1.

A list of the technical problems arising during the plant testing and commissioning is given below. Some of the problems are precisely those to be expected during commissioning, and can be regarded as "normal". some could perhaps have been prevented by a deeper or different form of risk analysis. These are discussed in more detail in later sections.

5.1.7. Problems arising during final check out and commissioning

Before listing the problems arising during commissioning it should be pointed out that by comparison with other plants, this plant was commissioned rapidly, and plant start up can be regarded as successful and relatively problem free.

A list of problems found is as follows.

1) Some flanges and valve sets leaked during the commissioning, after the vacuum testing had been completed successfully. As far as the flanges were concerned this was a consequence of heating the plant for the first time. For the valve seats, it appeared that these (teflon seated ball valves, 2" lines) became fouled with oxide deposits. As a result the seats became scratched, and would not seal properely. In some cases the seats had to be replaced twice.

This must be regarded as a normal commissioning problem, but illustrates the feet that reliability and risk analyses do not apply during the early stages of plant operation. An especially high standard of vacuum tightness should generally be the objective in a plant of this type, to reduce the period during which a flammable atmosphere exists inside plant vessels.

2) During plant check out, it was nescessary to exchange the PLC controller three times, until a correctly functioning controller was obtained. This is clearly an extreme "infant mortality" problem. It must be regarded, though, as a "normal" commissioning problem, and could hardly be prevented by risk analysis. Checking procedures ensured that the PLC failures did not present any safety problem.

3) Identical high level cut out set points had been fixed for both starting and stopping the charging pump. Waves (swash) in the feed tank ensured that the charging pump would start and stop several times as the tank became full.

A simple change, providing two set points, slightly different, for starting and stopping the pump solved this problem.

The problem solution is a standard one, and the cause of the problem must be regarded as a simple oversight. It is doubtful whether it is reasonable to try to treat problems at this level of detail in a risk analysis, but it is perhaps reasonable to add the problem to instrumentation review checklists.

Problems of this kind can potentially have some safety implications, since starting and stopping pumps rapidly can damage seats, and cause fluids to be released. (in this case flammable fluids).

4) One output circuit on a PLC interface was faulty. A reserve circuit was wired up instead.

This problem must be regarded as a normal commissioning problem. It illustrates though the flexibility of computer based instrumentation. The problem was corrected, including reprogramming, within 15 minutes.

5) One valve had been installed the wrong way round. The valve was a mixer for hot and cold water streams, and it was difficult to see externally which way round the valve should be fitted.

The result of the error was that only cold water could be sent to one condenser, and that cold water could be sent to the hot water system. This affected not only the plant unit under test but other nearly units. It took some time to identify what the problem was.

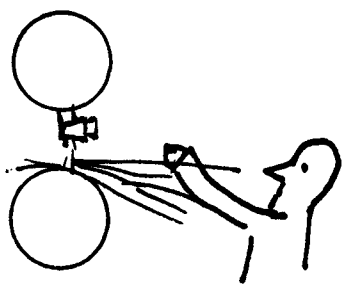
Valve installation errors are a typical problem in commissioning, and were not unexpected. The case illustrated though that even with careful checking the problem is hard to eliminate. The valve in question had been examined several times by several engineers before the wrong installation was identified because the installation "looked correct".

The case provides another potential cause to be added to the list of causes of water supply failure, and can be generalized.

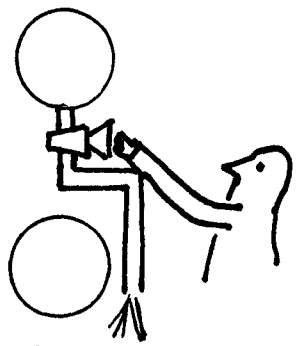
6) A number of instrument act point adjustments were required including resetting after the first operation of the plant.

This is a normal problem during commissioning.

7) Drain cocks for the steam jacket of the distillation kettle had been installed neatly, but in such a way that on opening, a hot water jet would strike the lagging on another pipe, and splash the operator. The problem was quickly cured by fitting a couple of short pipe sections and bends. This solution worked perfectly.



First arrangement



Revised arrangement

A problem of this kind is almost impossible to treat in a risk analysis during design, since, such detailed information on pipe and drain layout is rarely available on drawings.

If a layout and clearance check were made after drawings are completed, then perhaps such problems could be predicted. But such checks would only really be practical if computer aided design techniques were used. It would be possible to add such problems at design review or pre-start up inspection check lists, but even then it is difficult to "see" such detailed problems amid a mass of piping. A fairly direct solution to problems of this kind would be to provide standard drawings of such design details, with required clearances etc.

8) A "trap" was found in the sequence control program, such that a two way drain valve (tee valve) could only have its position changed at one stage in the

distillation sequence. This was at the step in the procedure at which changeover should normally be required. But the limitation proved inconvenient in commissioning, and prevented a potential safety action (direction of leaking methanol to a drain) It served no safety purpose.

The problem arises directly from what is otherwise a very good safety policy in sequential control design, that is "only allow actions which are explicitly known to be safe". But if such a policy is followed, it would be a good idea to add a further step to the sequential control design procedure, asking "What further freedom is desired, beyond normal operation". (An alternative is to design the sequential control to prevent only unsafe actions, but such a design procedure is much more complex, see (1) .

9) One valve was of the "fail steady" type. This meant that it could not follow the normal pattern of valve control in the PLC, since on shutdown problems could arise. If the PLC loses track of the valve position, it will switch the valve to the wrong position. The problem could be corrected by modifying the software.

Fail steady/Fail leave valves should have position sensors on them, and alarms to indicate when a valve is in the "wrong" position. Software should take account of possible changes is state not ordered by the computer.

In the present case, the valve was implemented with a selective "fail to safe position".

10) Sun shining on the PLC LED display obscures the LED display completely. Sun shades are required.

11) An interlock prevents restart after stop in step 7 of the PLC program - program changes were required.

12) If there are two active alarms on the PLC loop display only one can be seen at a time. This in unfortunate, but is a feature of the controller chosen.

13) As it turned out, there was an unexpectedly high water content in the feed. At first this was thought to be a problem of effectiveness in the distillation When the problem turned out to be more or less permanent, the distillation program was changed. The first fraction coming over was distilled to the "impure methanol" storage, followed by "pure methanol" to the first receiver tank, followed once again by "impure methanol".

14) It was found that a single failure in the PLC output circuits could open the bottom valve on the distillation kettle at any time!! This included the possibility of releasing boiling methanol!

This is a serious oversight, and was found on making a simple check of the boundary of the plant analysed. On checking the action sheets the problem had been found once before, as a general problem. It resulted in a change in the interlocks on emptying valves, and it resulted in fitting self closing nozzles to outlet and inlet lines on most receivers. But already at that time there was some question of the advisability of fitting a second valve to the kettle emptying line because of the problem that crude could gather in this valve. (The thick residue liquid could freeze).

Because the action sheet was phrased ambiguously, and because some safety changes <u>were</u> made to reduce the problem, a complete solution was not reached during the initial design.

This illustrates the need for careful review of actions, and also the value which should be obtained

from automatic analysis. It also illustrates the value of checks during commissioning.

A good general principle is

> "After finding a solution to a safety problem, reanalyse the solution".

In this case, because of the timing of the various analysis meetings, the reanalysis was delayed right up to the last days of plant testing.

15) When the plant stopped, one thermocouple ceased to be washed by the distillate flow. As a result, it measured the temperature of the heat tracing, rather than the distillate.

A simple rewiring solved the problem.

Instrument placement is a general problem espescially for thermocouples and pressure sensors on external lines which can be blocked - Questions concerning placement are included in commissioning check list, but it is not always easy to answer the questions correctly.

16) Drains were added to the pumps, so that they could be emptied of water during plant testing using water. Otherwise, freezing on a cold November night would have cracked them. The drains will probably not be needed later with the pumps filled with methanol, but they may prove convenient during maintenance. They do present a minor increase in risk since they can be left open but not nearly so much as a cracked pump would. This is typically a problem which should be solved by providing standard drawings.

17) A wrong sign in a temperature control loop was corrected (a question concerning this was already included in the checklist).

18) An interlock was specified during the initial risk analyses, such that on filling a residue drum, it would be weighed. As soon as the weight exceed 100 kg, the interlock would stop the filling.

Since the consequence of failure is not great in this step of the procedure (some cleaning would be needed if a failure occurred and the drum overfilled) this was, during the analysis judged to be adequate.

During trials of the plant, it was noticed that the amount of residue leaving the outlet pipe after the emptying valve closed was 5 - 10 kg. This represented the pipe volume after the valve, and was not unexpected. But the reading mechanism on the weighing machine was an inductive sensor placed to sense the weighing machine pointer. This stopped the filling perfectly as the 100 kg mark was reached, but the pointer travelled further, to 107 kg. If the filling buttom were pressed a second time, the same drum could be filled further, and this time, the interlock would not stop the filling.

The problem was "solved" by fitting a second interlock to prevent filling, unless an empty drum was in position. This required little effort, since there was already an interlock to ensure that a drum was in position. (Later the "solution" was removed, because an extra empty drum was needed to catch drips from the pipe).

This case illustrates a general problem in safety analysis. It is difficult to predict the failure behaviour of instruments and actuators which work with pulse signals. It is often difficult to see just which instruments do work with pulses. Special attention should be given to this point during instrumentation analysis.

19) A slow scumming effect in the residue meant that drums could not be filled to 100 kg immediately. They could be qaurter filled, then halffilled later.

This problem could hardly have been predicted during analysis, and even now is difficult to explain. Analyses cannot predict everything precisely, and particularly special substance properties and side reactions are difficult to predict.

20) During analysis, the problem of blocking in the condenser was considered. The possibility of blockage due to excessive cooling, and therefore freezing of the product was recognized. But the problem was not considered to be serious because it was thought that the condenser coling water should normally be above the freezing point of product and because the burst disc would relieve any overpressure resulting from blockage.

In practice the problem is more frequent than had been expected. Firstly, the warm water supply was cooler than expected, at some times. This means that flow must be controlled carefully to prevent freezing in the condenser. The second problem was not fully recognized in the original analysis probably because it was "masked". That is, in solving another problem (blockage due to lack of heat tracing) attention was drawn away from the heat exchanger. (The check list for "volumes" tends to hide some heat exchanger problems, and it would seem worthwhile to develop a hazard analysis sheet for heat exchangers alone).

When a condenser treats a vapour which can freeze, there are several potential problems. Too low a condenser temperature, coupled with too high cooling flow, too low vapour flow, or too low vapour temperature, will lead to blockage in the condenser. Too

high vapour flow, too high vapour temperature, too high cooling temperature or too low cooling flow, will result in reduced condensation. Vapour will pass through the condenser.

In the present case, it will pass through the condenser to the cold trap, and tend to condense and cause blockage there.

One disturbance has been noted which can cause this. If the plant is stopped during product distillation, under vacuum, pressure rises. On restarting the distillation, heating from the steam jacket can heat the product charge faster than the vacuum pump can establish a vacuum. The result is boiling at a higher temperature, since the partial pressure of urethane in the distillation kettle rapidly reaches the total pressure in the whole distillation apparatus. The result of this, in turn, is an excessively high vapour temperature to the condenser.

The problem can be solved by adapting the control system in any of a number of ways. The main problem is to ensure that the control adapts to all the likely disturbances.

This example illustrates a general problem in control system design for process plant. That is, that on a simple structural basis, one can, using for example risk analysis techniques, predict the possibility of disturbances. But to predict their size, their quantitative effect, and their importance, is difficult. The methods for control system design and for risk analysis are at present inadequate to treat this problem.

6. Information program

The objective of the analysis was to ensure a safe design. Since the plant designers were a part of the analysis team, transfer of information was direct (or unnecessary). All analysis information was immediately available throughout the design process.

7. Conclusions

The analysis can be said to have fulfilled its goal, both in providing a safe design basis and in illustrating and investigating the use of risk analysis. Moreover it has served as a basis for improving safety analysis techniques. Just how safe the resulting plant is will only be demonstrated after several years experience, but certainly many problems have been avoided as a result of the analysis. All of the recomendations arising from the analysis were directly included in the plant design. The anlysis method developed are currently in use by six groups, in a total of about ten projects.

The general conclusion can be drawn that no single analysis method would be adequate for a batch plant of this type (probably not for any chemical plant) but that the overall program of analyses was of benefit to the design and also very cost effective.

7.2. Future work

The planned future work for this plant is to continue with three further analyses for comparison purposes. These are

- a fault tree analysis (quantitative) making use of automatic analysis methods.

- an IFAL analysis
  (analysis of fire an explosion risk on a fairly approximate basis).

- a Dow Index Study
  (Indicates safety equipment level desired, but does not calculate risk).

Additionally further work is felt to be needed on the action error and Safety Officer check methods, since the plant studied was in some ways rather special (highly automated).

The study revealed an acute need for failure rate data for chemical plant components, and even more acute need for methods for analysis of computer control programs. It is hoped to be able to take up these topics later.

8.1. Lessons learned

Mechanical design

In analysis of plant hazards, the material used initially is the plant flow sheet and piping and instrumentation diagram. At these stage of analysis, several points concerning mechanical design are decided, and many assumptions are made implicitly, especially on the basis of layout of components on paper. But to take mechanical designers into the team is undesirable at an early analysis stage. The result of doing so is, for them, extensive boredom, since there are few problems which concern them, and many they cannot understand, not having the necessary background information.

But there are also many analysis problems which cannot be solved without taking plant layout into account.

1) Excessive head on tank drain lines can, if the tank does not have a vacuum breaker or vent, give a vacuum and such in the tank.

2) Tanks, especially those receiving distillate can often be placed high enough to allow emptying directly to transport containers, tankers etc. This avoids the need for pumps, and resulting risks.

3) Pumps can be placed directly over other equipment, depending on the character of the liquid pumped, can be a direct hazard.

4) Air locks can prevent or reduce flow from a tank

5) Liquid traps, not seen on flow sheets, can be introduced during layout, and others which appear to be a problem on the flow sheet, can be removed during layout (a case of this kind arose during the present plant design).

6) New flow routes can be established, and others removed, by changing the relative height of vessels.

There is a need for some way of communicating need and purpose to mechanical designers, which is better than that available at present.

There is also a strong need for an analysis procedure which takes direct account of problems arising during plant layout.

8.2. Lessons learned

Controller programming

Although a complete study of controller programming could not be made during this project, som points arose which should provide useful experience.

The procedure followed for controller programming was the following

1) The individual steps in the procedure written down.

2) The individual steps were described in more detail on sheets which provided for

   a) Step description

   b) Valve positions

   c) Listing of valves and motors activated

   d) Parallel processes

   e) Interlocks and start conditions

   f) End conditions for the step.

3) These conditions were transformed to statements for the PL 550 controller

Lessons learned were:

1) It would be useful to have purpose expressed for each step. (similarly on instrument list).

2) Before starting documentation, in detail for procedures the following questions should be posed.
   a) Which process steps may be stopped during their execution?

   b) What reasons can be envisioned for wanting to stop.

   c) Can the plant be shut down and drained from any step?

d) Can the plant be restarted after stopping?

3) Care should be taken with instruments giving pulse signals, and with actuators responding to pulses. For these the question should be posed

What will happen if the controller/operator forgets the current position?

4) Programmed controllers are very sensitive to errors in the manufactures software. These are always present, and give significant saftey problems.

8.3. Lessons learned

Completeness of existing procedures

Existing hazard and operability procedures are "internally complete", at least with respect to starting points. That is, they allow a complete analysis of disturbances within a plant model which is described by energy and mass balance equations and property equations. From a theoretical point of view, the "holes" in the procedure should then be

- omission of an energy or mass storage

Examples are oversights of pockets, low points in piping etc.

- Omission of a substance or a form of energy

In particular the current analysis forms ignore potential energy, in not accounting for component height. An example of this was escape of methanol by back flow from a riser through a charging pump.

- Oversight of a substance property

An example of this was scumming of residue

- Oversight of an energy or mass transfer.

In practice there is a potential for further omissions.

- Not all components are shown on drawings e.g. drain valves.

- Not all causes are identified in filling out hazard tables. Use of fault tree procedures would improve completeness, but generally would be very time consuming. Automation might reduce this problem.

- Not all problems identified are judged to be sufficiently serious to require in depth investigation, or solution.

- A potential problem may be identified, but its actual appearance may depend on numerical values in design of the plant. But insufficient information may be available to allow the magnitude of the problem, or even its actual existence, to be judged.

In particular it is almost impossible to predict magnitude of disturbances in control loops prior to plant construction.

No serious oversights in the action/error analysis could be found, but supplementary questions should be added to check list as follows.

"Stop of process step"

"Restart of process step after stopping"

"Shutdown of process step"

Especial problems were found to arise from omission of components and hazards on the boundary of the plant analysed. Choice of plant boundary should be made very carefully on the basis of

"What hazards are we omitting, and why". Also special procedures should be applied to check the boundary.

8.4. Improvements in procedures resulting from the study

As a result of the experience gained during this project a number of significant improvement in analysis procedures have been made.

First, standard analysis sheets have been prepared which greatly reduce the effort in Hazop and Action error analysis. Quality is also improved. These sheets are now used by six companies (at the time of writing).

Secondly, check lists have been derived for problems which can only be found after plant construction.

Thirdly, principles have been developed for steering the Hazop and Action Error analyses, to minimize effort without the risk of additional oversights.

Finally, the strength and weakness of individual procedures can now be documented.

9. Evaluation

A. Resources

The resources used for the analysis (engineer time) were (for the distillation unit)

Hazop analysis:	15 man hours (3 persons) in meetings + 10 man hours at desk

for 9 volume	
	3 man hours per volume
Action Error analysis	45 man hours (3 persons) in meetings
for 15 steps	
	3 man hours per step
Error cause analysis	½ hour per step
Hazard tree analysis	3 persons x ½ hr.
Safety officer checks	2 persons x 12 man hours

B Methods and criteria

a) Acceptance criteria

The single failure criterion used was very easy to apply and fulfill.

b) Data Collection

The data needed for the analysis were all either directly available, or required only a short visit to the company library.

c) Analysis methods.

The methods for hazard identification showed themselves to be logically complete when property applied within well defined classes of hazards. Omissions and oversights fall into two classes.

1) Lack of proper application

2) Problems which are systematically excluded from consideration by the method.

In general a method will be improperely applied because of lack of information. Both Hazop analyses as performed, and cause consequence analyses used to support action error analyses, suffer from oversights as follows.

- ommitted energy or mass storage
- omitted energy or mass transport
- overlooked or unknown chemical
- reactions or substance properties

All of these classes were observed in the present analysis.

Additionally Hazop analysis oversaw many hazards of the form

- Valve opens as a result of a misoperation
- Valve remains open as a result of a forgotten or failed operation

This seems to be natural since it is hard in a Hazop analysis to relate to required operations, there being no basis for such relations in the analysis procedure. Operating procedure information is not used..

Other systematic omissions (both methods) were to overlook pipes as potential storage vessels, and to overlook the properties of vessel height as a source of energy (such information was not readily available during the analysis.

Finally, some hazards were found, but were either not judged to be significant, or were overlooked during subsequent analyses of the plant.

On the assumption that all hazards have now been found, the degree of completeness resulting from the different analyses was then for hazards which could be identified from diagrams

Hazop	35 %
+ Action Error	99,0%
+ Hazard tree	99,5%
+ Safety officer checks	100 %

of total problems identified.

(Circa 200 significant hazard sources initially).

There were about twenty additional hazards which could not have been identified in inspection of diagram, but were identified during commissioning checks, which brings the overall completeness of the desk analyses down to about 90%.

The discrimination of the analysis, that is, the proportion of hazards identified which appear to be significant after completion of construction, is about 90%.

These figures apply to analysis at the component failure made and action error level, which was the level of the analysis performed. A more detailed analysis of component failure causes would be expected to be less complete.

The conclusion one can draw from this is that risk analysis methods should be combined if good coverage of hazards is to be achived.

SKj
OH
Bob Taylor

GRINDSTED PRODUCTS

04.06.81
OH/SKj/gam

C GP's erfaringer med sikkerhedsanalyse på en methanol/urethan-destillationsenhed.

Et af de problemer, man som kemiingeniør i Danmark står overfor, er, at ingen dansk kemisk virksomhed er stor nok til at besidde de erfaringer og standards med hensyn til sikkerhed, som man har brug for, når man er beskæftiget med potentielt farlige produktioner.

Problemet forstørres ved, at den undervisning ingeniører og teknikere modtager i sikkerhedsspørgsmål er af begrænset omfang, og for civilingeniørens vedkommende er den ikke engang obligatorisk.

Endelig kan man undre sig over, at den ellers kolosale kemisk-tekniske håndbogslitteratur ikke omfatter noget alment kendt standardværk om sikkerhed.

Slår man f.eks. op i den ellers fortræffelige Perry og Chilton CHEMICAL ENGINEERS HANDBOOK under ordene "flame arrestors", "lightning" eller "static electricity", finder man intet.

Vi mener derfor, at de af RISØ udarbejdede analysemetoder kan være til en betydelig hjælp. En sikkerhedsanalyse baseret på den metode og de skemaer, som J. R. Taylor, RISØ, har udviklet, sikrer en systematisk gennemgang af procesanlægget med hensyn til driftssikkerhed og farlige situationer, som kan opstå i anlægget.

Skemaerne med de mange check-spørgsmål danner en god basis for diskussion i en gruppe med deltagerne fra projektering/sikkerhedsafdelingen og drift. Sikkerhedsanalysens kvalitet vil dog afhænge af deltagernes erfaringer og kreativitet.

..2

GRINDSTED PRODUCTS

Skemaerne sikrer, at sikkerhedsanalysen bliver godt dokumenteret i takt med, at sikkerhedsanalysen udføres.

Tidsforbruget på ½-1½ time pr. apparat er rimeligt. Når man kender teknikken, kan sikkerhedsanalysen foretages hurtigere, dog med fare for at analysen bliver mere overfladisk, fordi gentagelsen af de samme kendte spørgsmål virker trættende.

Det er derfor vigtigt, at der ikke holdes for lange sikkerhedsmøder (højst 2-3 timer).

Det er svært at vurdere, hvad sikkerhedsanalysen af methanol/urethan-destillationsenheden har sparet Grindsted Products A/S i tid, penge og undgåede uheld, men vores erfaringer med metoden har bevirket, at vi har brugt den på andre anlæg uden deltagelse af medarbejdere fra RISØ.

Metoden bør beskrives i en let tilgængelig håndbog med forklaring af, hvordan skemaerne bruges og med et eksempel på skemaernes brug på et simpelt anlæg.

Håndbogen bør gøres tilgængelig for interesserede firmaer.

Grindsted, den 04.06.81

S. Kjærsgård Orla Hansen

D General Experience

The resources used for the analysis were about 3 man hours per vessel for the Hazop analysis and about the same per operational step for the action error analysis. It appears that the more people involved in an analysis, the longer it takes in absolute time, so that more people require more than proportionally more man time. It would be interesting to compare the quality of result and time taken for a single engineer to perform the analysis.

The brain storming group approach used in this project though, served two purposes beyond the direct one of completing the analysis. That is, it allowed a considerable amount of necessary communication to take place, and it served an educational purpose.

The later steps in this project should give a basis for comparing the purely qualitative analysis presented here with quantitative analysis methods.

References

1. J. R. Taylor: A Background to Risk Analysis, vol. 1 to 4. Risø National Laboratory, 1979.

2. J. Rasmussen: Human Errors. A Taxonomy for Describing Human Malfunction in Industrial Installations. Risø-M-2304, 1981.

TRYK: RISØ REPRO

Risø National Laboratory **Risø - M - 2319**

Risø - M - 2319

Title and author(s)

RISK ANALYSIS OF A DISTILLATION UNIT

J. R. Taylor**, O. Hansen*, C. Jensen*
O. F. Jacobsen**, M. Justesen**, S. Kjærgaard*

* Grindsted Products A/S
** Risø National Laboratory

Date: March 1982

Department or group: Electronics

Group's own registration number(s): R-14-81

JRT/AME

pages + tables + illustrations

Abstract

A risk analysis of a batch distillation unit is described. The analysis has been carried out at several stages during plant design, construction and operation. The costs, quality, and benefits in using the methods are described.

Copies to

Available on request from Risø Library, Risø National Laboratory (Risø Bibliotek), Forsøgsanlæg Risø), DK-4000 Roskilde, Denmark
Telephone: (03) 37 12 12, ext. 2262. Telex: 43116