MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

18th Annual International Symposium
October 27-29, 2015 • College Station, Texas

Application of Human Factors Evaluation in Engineering Design and Safe Operation of Dense Phase Ethylene Treaters

W.R. Banick and C. Wei
Genesis
11750 Katy Freeway, Houston, TX 77079
Email address: bill.banick@genesisoilandgas.com; cindy.wei@genesisoilandgas.com

Abstract

Ethylene treaters are widely used in the petrochemical industry to remove impurities from ethylene feedstock imported from pipeline networks or storage caverns. The safety concerns of dense phase ethylene treaters due to the reactive and highly flammable nature of ethylene are well known and studied. Under certain conditions, ethylene may self-polymerize and decompose violently with heat release. If vented too fast, ethylene will auto-refrigerate generating cold liquids that may cause potential brittle fracture hazards. Due to these safety concerns, it is a challenge to select the appropriate engineering design options for dense phase ethylene treaters and the associated regeneration facilities. Totally automated treater regeneration systems add complexity and instrument maintenance requirements and manually operated systems rely heavily on operator training and procedures. This paper presents a risk assessment method to evaluate the engineering design and safe operation options for dense phase ethylene treaters. The proposed risk assessment method integrates human factor analysis into the traditional HAZOP, LOPA and fault tree analysis to allow evaluation of automated, manual and hybrid approaches with a goal of selecting and optimizing design options to ensure plant safety.

Introduction

Ethylene treaters or purification beds are widely used in the petrochemical industry to remove trace impurities such as water, oxygenates, nitrogen compounds and acid gases (CO_2, H_2S, COS) from ethylene feedstock. Ethylene is an inherently unstable molecule and in particular, under dense phase operating conditions, presents special hazards. Under the right conditions, ethylene can decompose with significant heat release causing temperature increases above 1500°F. Many serious incidents have occurred in industry due to ethylene decomposition resulting from a variety of causes (e.g., catalytic molecular sieves, uncontrolled adsorption in purification beds, sudden compression involving nitrogen, oxygen contamination, excess heating in stagnant systems) [1].

Many ethylene treaters are operated under dense phase ethylene conditions at high pressures and ambient temperatures associated with cavern storage and pipeline delivery. Besides the highly flammable and reactive nature of ethylene, dense phase ethylene presents two special challenges:

1. Pressure is well within the region where self-polymerization and decomposition is possible if temperatures are elevated, which can lead to equipment failure due to excessive heating.
   a. Where high pressure treaters are connected to low pressure regeneration systems, hazardous conditions can occur during operating transitions, where introduction of the high pressure dense phase stream into the low pressure piping system can cause heat-up due to vapor compression.
   b. Some adsorbents exhibit moderate reactivity with olefin streams, such as ethylene, and also may require special pre-loading procedures to limit temperature rise due to heat of adsorption upon introduction of the feed stream after regeneration. If feed is introduced prior to pre-loading or into a hot bed, exothermic polymerization can cause further heat-up and potentially trigger ethylene decomposition. (It should be noted that proper selection of adsorbent type is an important design consideration which can reduce this risk, however, this topic is not specifically addressed in this paper.)
2. As ethylene pressure is reduced, a frequent occurrence in cyclic services such as treaters, ethylene enters the two-phase envelope resulting in liquid formation and auto-refrigeration. Uncontrolled depressurization can lead to shock chilling and brittle fracture concerns.

Due to these unique safety concerns, selection of appropriate engineering design options for cyclic regeneration of dense phase ethylene treaters is a challenge. Common options have significant advantages and disadvantages:

- Totally automated treater regeneration systems reduce operator error likelihood, but add complexity and instrument maintenance requirements;
- Manually operated systems are simpler, but rely heavily on operator training and procedures and usually cannot meet typical risk acceptance criteria;
- Hybrid approaches require detailed risk and cost benefit analysis to justify modifications from conventional systems.

In this paper, a risk assessment method is proposed to evaluate the engineering design and safe operation options for dense phase ethylene treaters by integrating human factors analysis into the traditional HAZOP, LOPA and fault tree analysis. The objective is to allow evaluation of automated, manual and hybrid approaches with a goal of selecting and optimizing design options to ensure plant safety.

Figure 1 provides a basic illustration of a dense phase ethylene treater with process and regeneration system connections. Ethylene supply from the process flows downwards in the treater during the purification/drying cycle, which typically lasts about one month. At the completion of the purification/drying cycle, treaters are switched, the spent treater is drained and depressured, and then heated regeneration nitrogen flows upwards through the treater bed in a purge, heating and cooling sequence. Once the regenerated treater is cooled, it is placed in standby or back in service by slowly pressurizing and filling. As noted earlier, this may involve a pre-loading step, however, for clarity pre-loading facilities are not shown in the figure. The valve manifolds illustrated in the figure are critical to providing positive isolation between the process and the regeneration systems.

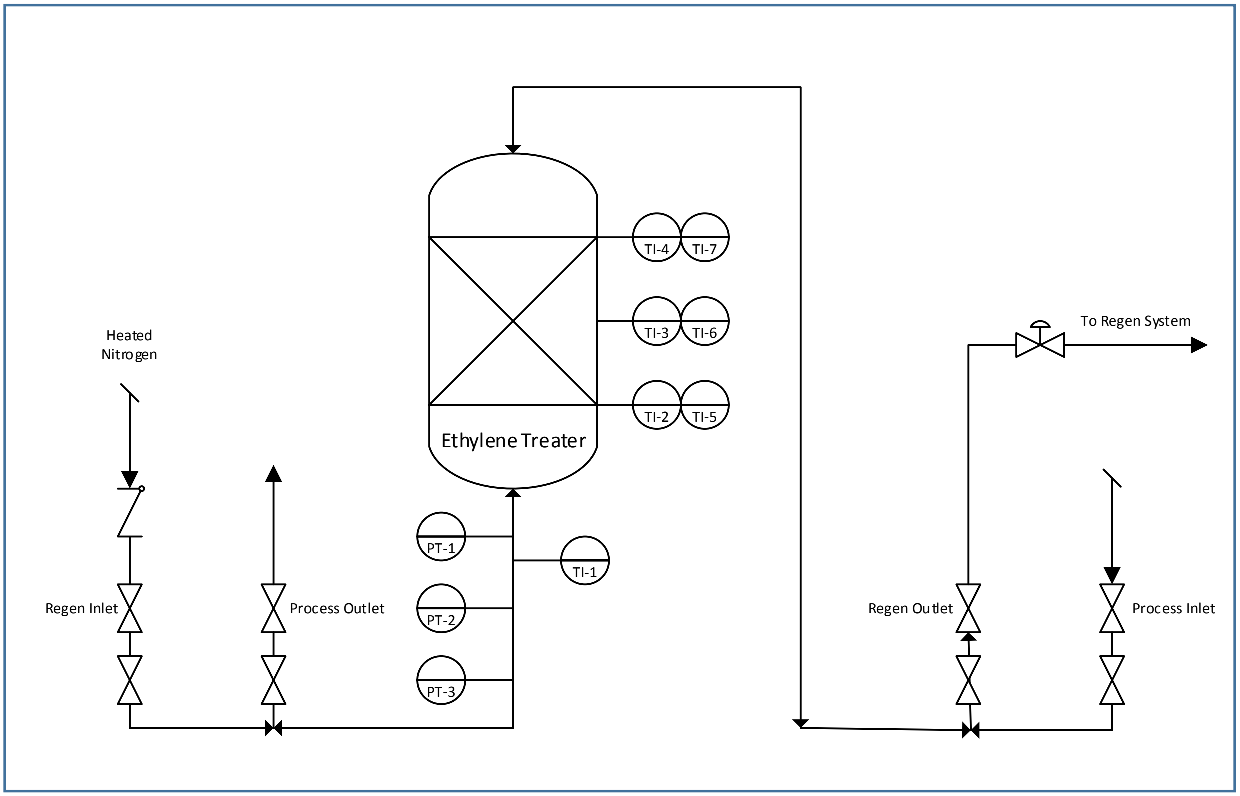


Figure 1: Schematic of Ethylene Treater

Risk Assessment Results

A risk assessment approach incorporating human factors task analysis and fault tree analysis was conducted following the traditional HAZOP/LOPA analysis. This approach allowed for a more complete evaluation of the engineering design and safe operation options for dense phase ethylene treaters. While the HAZOP method, conducted with experienced process engineers, design engineers and operators, is a good tool for team identification and evaluation of potential ethylene treater regeneration system hazard scenarios, use of LOPA alone can lead to complex solutions to meet the relatively conservative requirements for independent protection layers. This is especially true for routine operations with a high degree of human/machine interface.

To illustrate the risk assessment process, six representative ethylene treater HAZOP scenarios were selected and are shown in Table 1, along with the associated LOPA analysis results. The plan was to evaluate these scenarios using three proposed industrial practices - automated, manual and hybrid approaches, with the goal of selecting and optimizing design options to ensure plant safety.

Table 1: Ethylene Treater HAZOP Scenarios and LOPA Analysis

HAZOP/LOPA Guide Word	Cause	Freq. (/yr)	Consequence	Severity	Target Freq.(3) (/yr)	IPLs Req'd	Safeguards (Independent Protection Layers)	IPL Type	IPLs	Total IPLs	Comment
1. Misdirected Flow	1.1 Inadvertent opening of the block valves on the ethylene treater regeneration inlet or outlet line on the online treater.	0.1 (1)	1.1.1 Ethylene flows into the regeneration system resulting in compression of nitrogen with potential for decomposition, leading to overheating of the piping and loss of containment.	Fire, explosion with potential loss of life	Less than 1E-04	4	1. Blinding procedure	Procedure	1	4-5	Required risk reduction is achieved. .
							2. Trapped key interlock system on treater process and regeneration valves.	Mechanical Interlock	2(2)		
							3. Double check valves on regeneration inlet line and rupture disk on regeneration outlet line.	Other IPL	1-2		
			1.1.2 Ethylene flows into the low pressure regeneration system with potential for overchilling of piping and equipment leading to brittle fracture and loss of containment.	Fire, explosion with potential loss of life	Less than 1E-04	4	1. Blinding procedure	Procedure	1	4	
							2. Trapped key interlock system on treater process and regeneration valves.	Mechanical Interlock	2(2)		
							4. Low temperature alarm	DCS Alarm	1		
2. Missed Step	2.1 Ethylene treater is not drained and	0.1(1)	2.1.1 Ethylene flows into the regeneration system resulting in compression of nitrogen with potential for decomposition,	Fire, explosion with potential loss of life	Less than 1E-04	4	3. Double check valves on regeneration inlet line and rupture disk on regeneration outlet line.	Other IPL	1-2	4-5	Required risk reduction is achieved.

HAZOP/LOPA Guide Word	Cause	Freq. (/yr)	Consequence	Severity	Target Freq.(3) (/yr)	IPLs Req'd	Safeguards (Independent Protection Layers)	IPL Type	IPLs	Total IPLs	Comment
	depressured before the regeneration inlet or outlet line is opened. (This step is done after blinding/un-blinding.)		leading to overheating of the piping and loss of containment.				5. DCS Treater Regeneration Sequence	DCS Control	1		
							6. Automatic SIL-2 isolation valves on the treater regeneration lines with permissives for opening based on treater pressure.	SIF	2		
			2.1.2 Ethylene flows into the low pressure regeneration system with potential for overchilling of piping and equipment leading to brittle fracture and loss of containment.	Fire, explosion with potential loss of life	Less than 1E-04	4	4. Low temperature alarm	DCS Alarm	1	4	
							5. DCS Treater Regeneration Sequence	DCS Control	1		
							6. Automatic SIL-2 isolation valves on the treater regeneration lines with permissives for opening based on treater pressure.	SIF	2		
2. Missed Step	2.2 After regeneration,	0.1(1)	2.2.1 Ethylene polymerization on the hot bed which causes	Fire, explosion with	Less than 1E-	4	5. DCS Treater Regeneration Sequence	DCS Control	1	4	Required risk reduction is

HAZOP/LOPA Guide Word	Cause	Freq. (/yr)	Consequence	Severity	Target Freq.(3) (/yr)	IPLs Req'd	Safeguards (Independent Protection Layers)	IPL Type	IPLs	Total IPLs	Comment
	ethylene feed is re-introduced into the treater prior to cool-down.		further heating and triggers decomposition, leading to overheating and loss of containment.	potential loss of life	04		7. Automatic SIL-3 isolation valves on the treater process lines which close on high treater temperature.	SIF	3		achieved. However, SIL-3 protection with automatic valves and permissives will be very expensive and may not be practical to achieve over the plant life cycle. Additional analysis is warranted.
	2.3 After regeneration, ethylene feed is re-introduced into the treater prior to pre-loading.	0.1(1)	2.3.1 Heat-up of treater bed due to heat of adsorption resulting in ethylene polymerization which causes further heating and triggers decomposition, leading to overheating and loss of containment.	Fire, explosion with potential loss of life	Less than 1E-04	4	5. DCS Treater Regeneration Sequence	DCS Control	1	4	
							7. Automatic SIL-3 isolation valves on the treater process lines which close on high treater temperature.	SIF	3		

HAZOP/LOPA notes:

1) Operator failure rate is based on treater regenerations once per month. [2]
2) 2 IPLs are taken for a trapped key interlock system that requires that both process inlet and outlet valves are closed prior to allowing opening of the regeneration valves, and vice versa. [2]
3) Target frequency is based on a typical industry risk matrix, which requires the likelihood of any scenario with potential loss of life to be reduced to less than once in 10,000 years.

Discussion:

HAZOP Scenarios:

Ethylene treaters in dense phase service that are connected to low pressure nitrogen regeneration systems present a unique challenge. Low pressure closed loop or once through regeneration systems are commonly used in industry and are often connected to multiple treater systems in a plant or unit. Design of these systems for high pressure and brittle fracture resistance (e.g., stainless steel) is cost prohibitive; and therefore, protection schemes are employed to prevent inadvertent cross-connection of the process and regeneration streams. The hazardous nature of this arrangement is captured in multiple HAZOP scenarios involving mis-lineups during treater switching operations. Scenarios are often complicated by the fact that plants or units often have multiple sets of treaters that may be located next to each other in an effort to optimize the regeneration system piping layout. Operator confusion, or shift-to-shift mis-communication, can result in opening the wrong valves and/or missed steps in the sequence of isolation, draining and depressuring a treater in preparation for regeneration.

Table 1 includes a description of four such scenarios and the potential consequences. In the event of a regeneration or process valve mis-alignment or skipped steps allowing ethylene into the regeneration system, one of two consequences can occur:

1. If the regeneration outlet is closed, sudden compression of nitrogen in the regeneration piping system can trigger ethylene decomposition, leading to overheating of the piping. (Scenarios 1.1.1 and 2.1.1)
2. If the regeneration outlet is open (typically through a back pressure control valve to a flare or VOC destruction device), then auto-refrigeration of the dense phase ethylene, which becomes flashing liquid as pressure is reduced, can result in brittle fracture of the carbon steel regeneration system. (Scenarios 1.1.2 and 2.1.2)

Both consequences can result in loss of containment with a fire, explosion and potential impact to plant personnel.

Table 1 also includes two scenarios (2.2.1 and 2.3.1), which involve a missed step during the sequence of placing a treater back in service following a regeneration. Once again, this could be caused by operator confusion, or shift-to-shift mis-communication, especially in the case where the plant has multiple sets of treaters, some of which require a pre-loading procedure and others that do not.

For some adsorbent types, skipping the treater cool-down step following a regeneration in Scenario 2.2.1 could lead to exothermic polymerization when ethylene feed is re-introduced onto the hot bed, causing further bed heat-up and triggering decomposition as the treater pressure increases. Similarly in Scenario 2.3.1, for some adsorbent types, skipping the pre-load step, where a small flow of ethylene diluted with nitrogen is slowly added to the bed to control heat of adsorption, could result in a sharp bed temperature rise when ethylene feed is re-introduced. This could lead to the same consequence with exothermic polymerization causing further heat-up and triggering ethylene decomposition, ultimately leading to vessel over-temperature and failure with loss of containment.

Layers of Protection Analysis (LOPA) Discussion:

As shown in Table 1, LOPA analysis for scenarios 1.1.1 and 1.1.2 indicates the need for both a blinding procedure (for 1 IPL) and a mechanical interlock system (such as a trapped key interlock, for 2 IPLs) to prevent inadvertent valve mis-alignments. In scenarios 2.1.1 and 2.1.2, a SIL-2 protective system involving automatic valves on the regeneration lines, with permissives for opening based on treater pressure, is suggested. This is required to supplement the 1 IPL that can be taken for the treater regeneration sequence logic, which is implemented in the DCS. SIL-2 integrity is required since the large treater vessel contains enough mass to cause decomposition or brittle fracture if it is not drained and depressurized before either one of the regeneration valves is opened. In these scenarios, the blinding procedure and mechanical interlock system do not provide protection since the process valves are already closed and blinding/un-blinding of appropriate lines in preparation for a regeneration would be completed prior to the draining operation.

In the LOPA analysis for the last two scenarios, 2.2.1 and 2.3.1, a SIL-3 protective system with automated valves is suggested to prevent the operator from inadvertently placing the treater back in service prior to completing the cool-down or pre-load steps. This system would supplement the single IPL taken for the DCS sequence logic. The protective system would either prevent opening or would re-close the process inlet and outlet valves in the event of high bed temperature in order to stop the flow of the ethylene reactant and thereby limit the exothermic heating of the bed to below the point at which decomposition could be triggered. SIL-3 integrity is required since the temperature rise in either scenario would be too fast to allow alarms and operator response to be used as an effective IPL.

Together these results suggest that an automatic SIL-3 protective system may be the best solution since both the regeneration and process valves require automated action to cover all six scenarios. However, a SIL-3 system would be expensive, and as with any high integrity system, it would be a challenge to maintain this level of performance over the life cycle of the treater system. Total automation of the regeneration sequence may provide some advantages, however, since two valves are required on each process and regeneration line for isolation purposes, total automation would involve even more cost and complexity and would not typically be justified for a monthly operation.

Finally, LOPA is a conservative analysis tool often used for screening purposes, and therefore it is prudent to conduct additional analysis when LOPA is driving the user towards a complex solution. For this case, a human factors analysis of the treater regeneration procedure was conducted and incorporated into a fault tree analysis for the safeguards identified in the HAZOP.

Fault Tree Analysis Discussion:

Fault tree analysis was conducted for the six identified HAZOP/LOPA scenarios:

- Scenarios 1.1.1 and 1.1.2 - Mis-alignment of the regeneration valve on the on-line treater, as shown in Figure 2.
- Scenarios 2.1.1 and 2.1.2 - Opening the regeneration valve before the treater is drained and depressurized, as shown in Figure 3.
- Scenario 2.2.1 - Re-introducing feed into a treater prior to cool-down, as shown in Figure 4.

– Scenario 2.3.1 - Re-introducing feed into a treater prior to pre-loading, as shown in Figure 5.

The following data and assumptions were utilized for this analysis:

- The design ethylene treater regeneration frequency is once per month.
- Tables 14.15 and 14.16 in Lee's Loss Prevention Handbook [3] were used as the basis for the human error rates. Error multiplication factors of 3 to 5 were used to account for the upper limit of data uncertainty.
- Based on the human factors task analysis, credit was taken for immediate operator recognition and correction of the regeneration valve mis-alignment on an on-line treater in 3 out of 4 instances. This was based on the fact that opening the valve with excessive pressure drop would be more difficult, and the vibration and noise associated with sudden flow would be noticeable.
- For the trapped key interlock mechanism, which would be attached to the manual block valves, a generic failure rate of 750 cycles with 10% failure probability was used based on the mechanical failure of the spring inside the interlock. Using the regeneration frequency of the treaters (one regeneration involving 2 cycles/month/valve), the mean time to failure (MTTF) was estimated to be 300 years. [4]
- Supplemental safeguards, such as DCS sequence logic, alarms, double dissimilar check valves and pressure relief devices are included in the fault trees with nominal IPL failure rates assigned, consistent with those used in the LOPA analysis.
- In order to maintain a reasonable level of conservatism, the top event was assumed to be the process condition (high or low temperature) that could lead to piping or vessel failure. No credit was taken for probability of failure, or for post-release conditional modifiers, such as likelihood of ignition, presence of the operator or likelihood of injury.

Fault tree analysis for Scenarios 1.1.1 and 1.1.2 indicated that the trapped key interlock and the supplemental safeguard reduced the loss of containment frequency to an acceptable level, 3.7E-5/yr. This was achieved even without the use of the blinding safeguard. As such, for these scenarios, blinding would not be a required step in the regeneration procedure and this has the advantage of eliminating the need to opening up equipment to install or remove blinds.

Given the risk reduction achieved by the trapped key interlock in Scenarios 1.1.1 and 1.1.2, use of this safeguard in a hybrid approach to address the other scenarios was suggested. This will maintain a simpler system utilizing manual block valves for the process and regeneration system isolation. A fault tree analysis was developed for utilizing the trapped key interlock with a pressure and/or temperature permissive for Scenarios 2.1.1, 2.1.2, 2.2.1 and 2.3.1 in lieu of the SIL-2 or SIL-3 automated isolation valves. The concept was to design the trapped key interlock system with appropriate process variable inputs to create a permissive using a key release solenoid.

For example, in Scenarios 2.1.1 and 2.1.2, the key utilized to open the first regeneration valve can be trapped in a key exchange box, until the closed process valve keys are inserted <u>and</u> the treater pressure input meets a pre-determined low setpoint. The key required to open the first regeneration valve cannot be obtained, until both conditions are satisfied. If this hybrid arrangement achieves the required risk reduction factor, it would greatly simplify the overall design and avoid the need for a complex and costly SIL-3 instrumented system.

Similarly for Scenario 2.2.1, the key utilized to open the first process valve can be trapped in a key exchange box, until both closed regeneration valve keys are inserted and the treater temperature meets a pre-determined low setpoint (confirming completion of the cool-down step). For Scenario 2.3.1, the key utilized to open the first process valve can be trapped in a key exchange box, until both closed regeneration valve keys are inserted and the treater pressure meets a pre-determined high setpoint (confirming that pre-loading has been completed).

For the fault tree analysis of Scenarios 2.1.1, 2.1.2, 2.2.1 and 2.3.1, the following additional data and assumptions for utilizing the trapped key interlock with a pressure and/or temperature permissive were utilized:

- Generic equipment data from SERH (Safety Equipment Reliability Handbook) was used for failure rates of the pressure and temperature sensors a logic solver and the key release solenoid to be utilized as part of the pressure and temperature permissives.
- Each ethylene treater will require multiple independent pressure and temperature transmitters, with one set providing input to a DCS treater regeneration sequence, another providing alarm inputs and a third providing input to an SIS as part of the key release solenoid pressure and temperature permissives.

Fault tree analysis for Scenarios 2.1.1 and 2.1.2 confirmed that the trapped key interlock with the integrated low pressure permissive provides the required risk reduction, with a loss of containment frequency of 8.1E-5/yr. Likewise for Scenario 2.2.1 the trapped key interlock with the low temperature permissive reduced the loss of containment frequency to 9.3E-5/yr and for Scenario 2.3.1 the trapped key interlock with the high pressure permissive reduced the frequency to 8.1E-5/yr. Fault tree analysis results for all six scenarios are summarized in Table 2.

Table 2: Ethylene Treater Scenario Fault Tree Analysis Results

Scenario	Top Event Description	Top Event Frequency (/yr)
1.1.1, 1.1.2	Mis-alignment of the regeneration valve on the on-line treater resulting in gross flow of ethylene into the regeneration system with potential loss of containment due to decomposition or brittle fracture	3.7 E-5
2.1.1, 2.1.2	Opening the regeneration valve before the ethylene treater is drained and depressurized resulting in sudden emptying of the treater contents into the regeneration system with potential loss of containment due to decomposition or brittle fracture	8.1 E-5
2.2.1	Lining up ethylene feed to the treater before the cool-down step is completed after a regeneration with potential loss of containment due to overheating from polymerization and decomposition	9.3 E-5
2.3.1	Lining up ethylene feed to the treater before the pre-loading step is	8.1 E-5

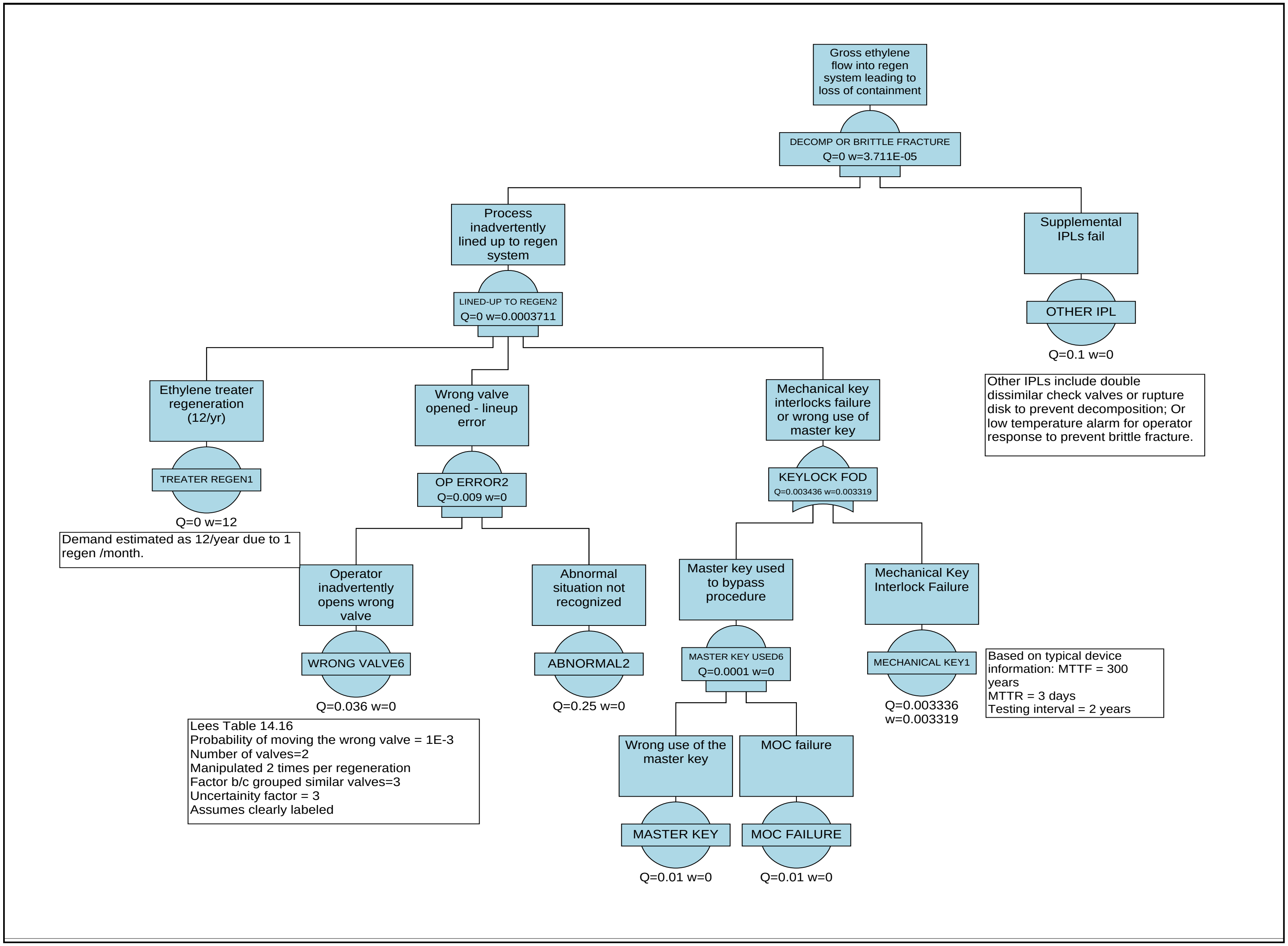
	completed after a regeneration with potential loss of containment due to overheating from heat of adsorption, polymerization and decomposition	

Conclusions:

Using a combination of HAZOP scenario identification, LOPA, human factors task analysis and fault tree analysis, a cost effective design solution was developed to manage the unique risks associated with dense phase ethylene treater and regeneration systems. The hybrid solution maintained a simpler system utilizing manual block valves for process and regeneration system isolation. A trapped key interlock system on the block valves, with treater vessel pressure and temperature permissives, provided fit-for-purpose risk reduction. These techniques not only avoided the cost and complexity of implementing a SIL-3 instrumented safety system, they also identified that the risks associated with routine opening of process equipment for blinding and un-blinding could be avoided as well.

References:

1. L. G. Britton, Loss Case Histories in High Pressurized Ethylene Systems, Process Safety Progress, Vol. 13, No. 3, July, 1994.
2. 2015 CCPS Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis.
3. Lee’s Loss Prevention Handbook, Rev. 4, Chapter 14, Human Factors and Human Error, Table 14.15, HRA Handbook; Human Error Probability (HEP) estimates and Error Factors (EFs) for Written Procedures, and Table 14.16, HRA Handbook; Human Error Probability (HEP) and Error Factors (EFs) for Manipulation and Checking of Locally Operated Valves.
4. CEN ISO 13849-1, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design, 2006



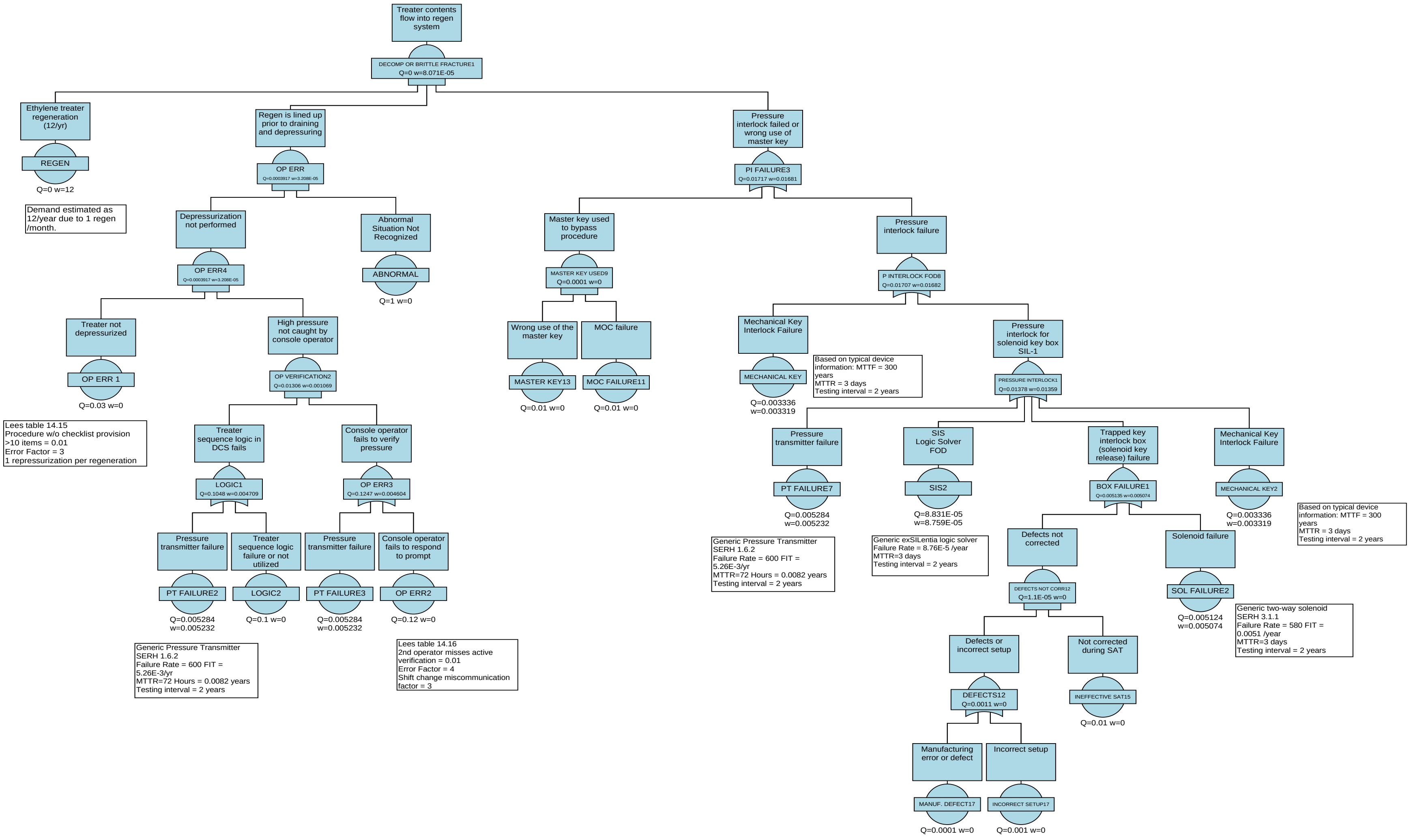
Other IPLs include double dissimilar check valves or rupture disk to prevent decomposition; Or low temperature alarm for operator response to prevent brittle fracture.

Demand estimated as 12/year due to 1 regen /month.

Lees Table 14.16
Probability of moving the wrong valve = 1E-3
Number of valves=2
Manipulated 2 times per regeneration
Factor b/c grouped similar valves=3
Uncertainity factor = 3
Assumes clearly labeled

Based on typical device information: MTTF = 300 years
MTTR = 3 days
Testing interval = 2 years

Figure 2: Fault Tree Diagram – Scenarios 1.1.1 and 1.1.2



Demand estimated as 12/year due to 1 regen /month.

Lees table 14.15
Procedure w/o checklist provision >10 items = 0.01
Error Factor = 3
1 repressurization per regeneration

Generic Pressure Transmitter SERH 1.6.2
Failure Rate = 600 FIT = 5.26E-3/yr
MTTR=72 Hours = 0.0082 years
Testing interval = 2 years

Lees table 14.16
2nd operator misses active verification = 0.01
Error Factor = 4
Shift change miscommunication factor = 3

Based on typical device information: MTTF = 300 years
MTTR = 3 days
Testing interval = 2 years

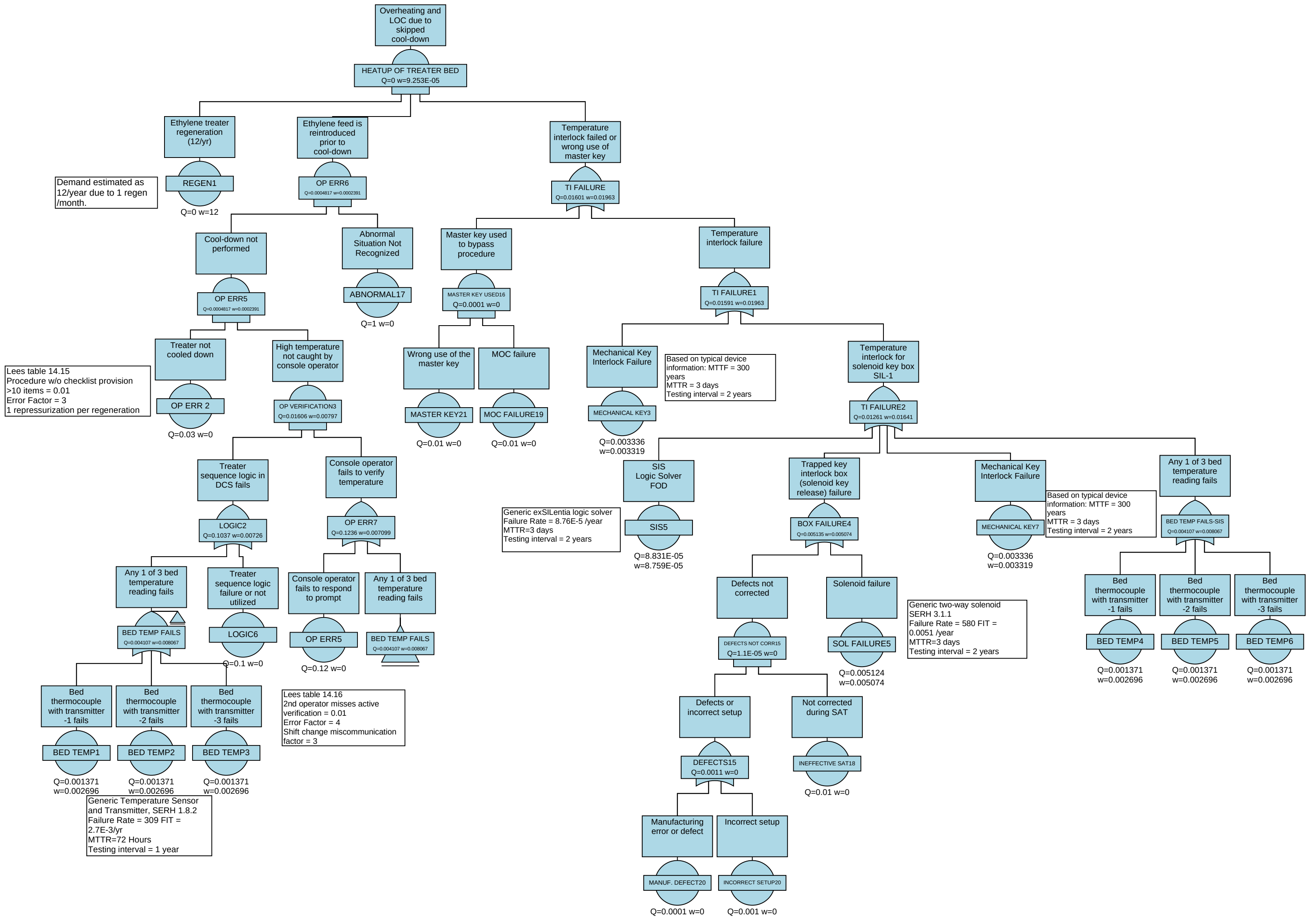
Generic Pressure Transmitter SERH 1.6.2
Failure Rate = 600 FIT = 5.26E-3/yr
MTTR=72 Hours = 0.0082 years
Testing interval = 2 years

Generic exSILentia logic solver
Failure Rate = 8.76E-5 /year
MTTR=3 days
Testing interval = 2 years

Based on typical device information: MTTF = 300 years
MTTR = 3 days
Testing interval = 2 years

Generic two-way solenoid SERH 3.1.1
Failure Rate = 580 FIT = 0.0051 /year
MTTR=3 days
Testing interval = 2 years

Figure 3: Fault Tree Diagram – Scenarios 2.1.1 and 2.1.2



Demand estimated as 12/year due to 1 regen /month.

Lees table 14.15
Procedure w/o checklist provision
>10 items = 0.01
Error Factor = 3
1 repressurization per regeneration

Based on typical device information: MTTF = 300 years
MTTR = 3 days
Testing interval = 2 years

Generic exSILentia logic solver
Failure Rate = 8.76E-5 /year
MTTR=3 days
Testing interval = 2 years

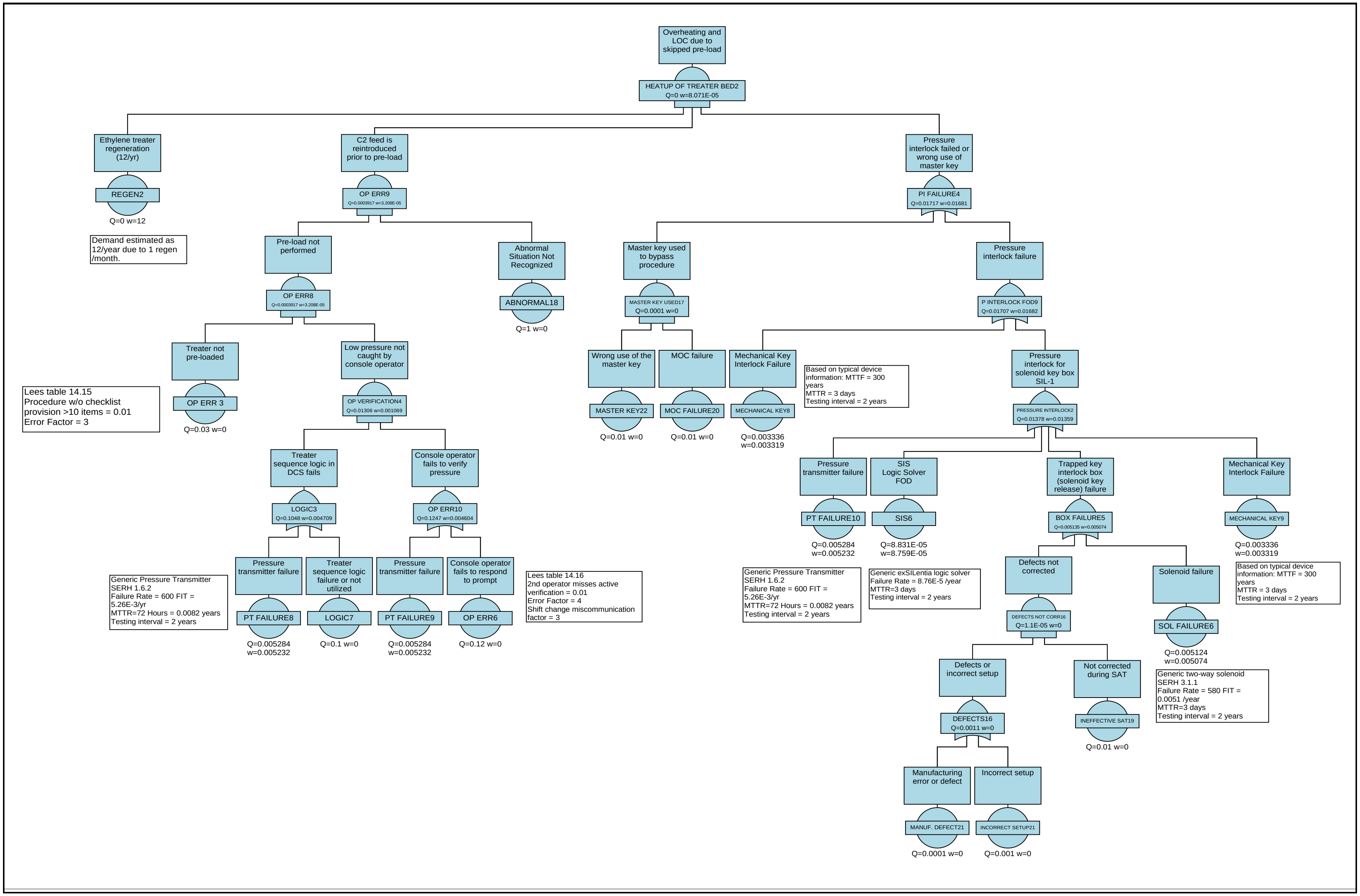
Based on typical device information: MTTF = 300 years
MTTR = 3 days
Testing interval = 2 years

Generic two-way solenoid
SERH 3.1.1
Failure Rate = 580 FIT = 0.0051 /year
MTTR=3 days
Testing interval = 2 years

Lees table 14.16
2nd operator misses active verification = 0.01
Error Factor = 4
Shift change miscommunication factor = 3

Generic Temperature Sensor and Transmitter, SERH 1.8.2
Failure Rate = 309 FIT = 2.7E-3/yr
MTTR=72 Hours
Testing interval = 1 year

Figure 4: Fault Tree Diagram – Scenario 2.2.1



Demand estimated as 12/year due to 1 regen /month.

Lees table 14.15
Procedure w/o checklist
provision >10 items = 0.01
Error Factor = 3

Generic Pressure Transmitter
SERH 1.6.2
Failure Rate = 600 FIT = 5.26E-3/yr
MTTR=72 Hours = 0.0082 years
Testing interval = 2 years

Lees table 14.16
2nd operator misses active verification = 0.01
Error Factor = 4
Shift change miscommunication factor = 3

Based on typical device information: MTTF = 300 years
MTTR = 3 days
Testing interval = 2 years

Generic Pressure Transmitter
SERH 1.6.2
Failure Rate = 600 FIT = 5.26E-3/yr
MTTR=72 Hours = 0.0082 years
Testing interval = 2 years

Generic exSILentia logic solver
Failure Rate = 8.76E-5 /year
MTTR=3 days
Testing interval = 2 years

Based on typical device information: MTTF = 300 years
MTTR = 3 days
Testing interval = 2 years

Generic two-way solenoid
SERH 3.1.1
Failure Rate = 580 FIT = 0.0051 /year
MTTR=3 days
Testing interval = 2 years

Figure 5: Fault Tree Diagram – Scenario 2.3.1