TPK4120
Fall 2012

Safety and Reliability Analysis

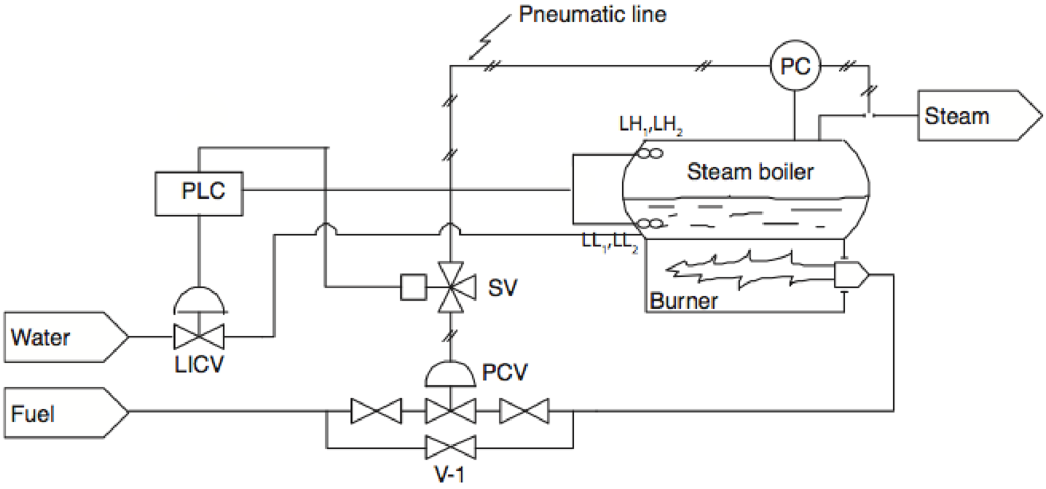
Kandidatnummer: 10037, 10054, 10043.

NTNU, IVT-fakultetet

TPK4120 Fall 2012

Table of Contents

1. Functional analysis and FMECA



Figur 1 - System schematic.

V-1: Bypass valve

LL: Low level transmitter

LH: High level transmitter

LICV: Level indicator controller valve

PC: Pressure controller

PCV: Pressure controller valve

PLC: Programmable logic controller

SV: Solenoid valve

1.1 System assumptions

1. We assume that the following components are operating on low-demand mode and are only active in a situation where the control system is not able to perform: PCV(open), SV(closed),LL- and LH-transmitters.
2. The following components, however also part of the safety function, are operating on high-demand mode and are active continuously: LICV, PLC and PC.

3. We assume that the given failure rate for component LL is the failure rate due to independent failures. To consider the dependency between the two LL transmitters we use the beta-factor model. We include the β-factor in the failure rates for the two low level transmitters by combining the following equations:

   Eq. 6.6[1]

   $$\lambda = \lambda^{(i)} + \lambda^{(c)}$$

   Eq. 6.7[1]

   $$\beta = \frac{\lambda^{(c)}}{\lambda}$$

   By inserting β = 0,9, we get

   $$\lambda = \frac{\lambda^{(i)}}{(1-\beta)} = \frac{\lambda^{(i)}}{0{,}9}$$

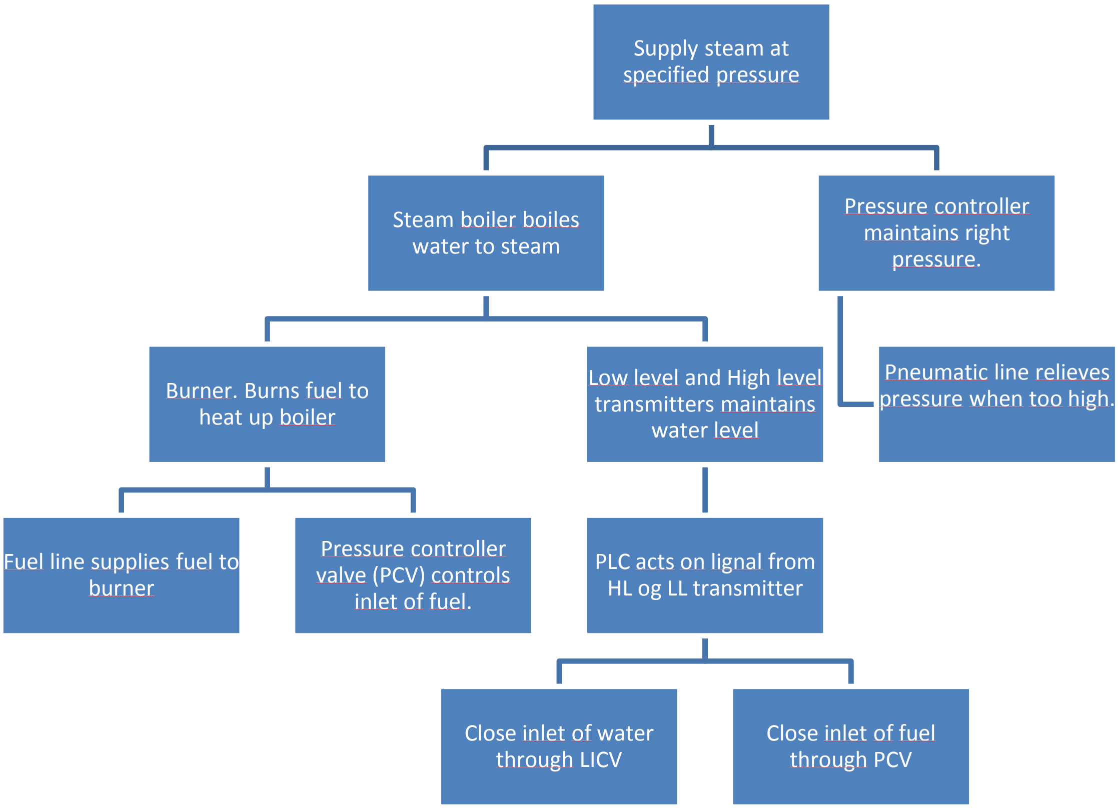
   The failure rate of the low level transmitters, adjusted for common cause failures is thus 2,222*10^{-6}.

4. We assume the PC is closing the PCV directly if it bleeds of pressure, meaning the PC does not depend on the SV. [2]

[1] Rausand/Høyland 2004 p. 217

[2] All assumptions have been discussed either with Professor Rausand, Maryam Rahimi or Jun Zhou.

1.2 Function tree


Supply steam at specified pressure
Steam boiler boiles water to steam
Pressure controller maintains right pressure.
Burner. Burns fuel to heat up boiler
Low level and High level transmitters maintains water level
Pneumatic line relieves pressure when too high.
Fuel line supplies fuel to burner
Pressure controller valve (PCV) controls inlet of fuel.
PLC acts on lignal from HL og LL transmitter
Close inlet of water through LICV
Close inlet of fuel through PCV

Figur 2 - Function tree for boiler system.

1.3 FMECA

The components we have chosen to look at in this part of the assignment are the bypass valve V-1, the solenoid valve and the low level transmitter. We have chosen to follow the procedure from the textbook, presented on page 89, although there was presented a slightly different one in class.

The first component is the bypass valve V-1. The main reasons are; it serves an important purpose when inspecting or maintaining the PCV, and is the component we perceive as the most likely to be influenced by human error in accordance with our assumptions. We assume the valve to be operated manually with a wheel handle, that it is a standard gate valve with rubber bushings, meaning it is possible for the valve to leak.

The second component is the solenoid valve. The reason we chose this component is its critical part in the system. If the solenoid valve does not open, thus activating the PCV to close the fuel supply, the system is in danger of overheating.

The third component is the low level transmitter. We chose this component because it is important in securing that the boiler does not run dry, which we define as our TOP event in our fault tree in task 2.

We wish to point out that the fact that there are two low level transmitters gives the system a fair degree of redundancy. Thus an FMECA is not perfectly suitable for analysis of this component[3]. However, for the purpose of the FMECA we regard the system as having only one low level transmitter.

1.4 The concept of failsafe in relation to this system.

The concept of fail-safe is "A design property of an item that prevents its failures from being critical failures. A design feature that ensures the system remains safe or, in the event of a failure, causes the system to revert to a state that will not cause a mishap"[4]

In relation to this system it means that in the event of low water level, there are two different security design features that cause a stop in fuel flow in the event of a failure.

The PCV is kept open by the pressure in the pneumatic line and if the pressure is relieved, PCV will close the fuel flow. If the pressure goes above a given *high level* the PC will bleeds of pressure such that the SV opens, relieving the pressure in the pneumatic line and closing the PCV. If the water level goes below the low level transmitters, they will signal to the PLC, which in turn signals the SV to open.

An additional feature of fail-safe is the redundancy of the level transmitters, for instance with a 1oo2-voting logic, the system will revert to a safe state in the event of a signal from one transmitter. This specific feature will be discussed later in the assignment to more detail.

2. Fault tree and reliability block diagram

2.1 Definition of TOP event

In this section we define various details of our Top event.

2.1.1 The what, where and when

We define the TOP event as "Vessel is boiled dry during normal operation". The reason for our choice is the severity of the consequences if the event occurs. If the vessel is boiled dry, it may be damaged to such a degree it has to be replaced, but more importantly it may lead to an explosion of the boiler or any of its connecting components, damaging equipment and endangering human lives.

[3] Rausand/Høyland 2004 p. 95

[4] Rausand/Høyland 2004 p. 600

2.1.2 Boundary conditions

To use both the method of reliability block diagram and the fault tree, we need to have clarity in the boundary conditions for the analysis. More specifically, we need to decide the level of resolution.

As for the physical boundaries of the system, we have quite simply decided to include all elements shown in the schematic. Furthermore, we have chosen the initial state to be operational and running at full speed at the time of our top event. We also neglect all external stresses such as sabotage or temperature changes.

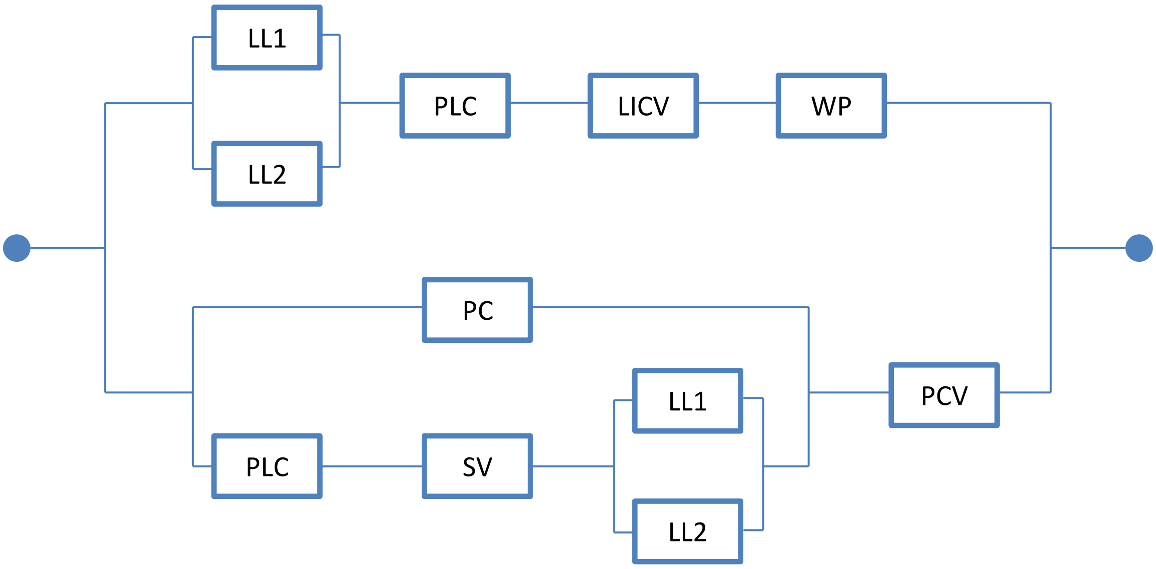
We choose a level of resolution corresponding to the information available. A more detailed analysis would require more data about the individual components.

2.2 Fault tree for top event

The fault tree is designed in CARA. See appendix 1 for the fault tree, in which we base our analysis for the rest of the assignment.

2.3 Reliability block diagram

We drew up a reliability block diagram based on our fault tree. The event “LICV” is defined as “fails in closed position”, if it were to fail in open position, the water supply would be sufficient. We can see the two paths from our fault tree*.* *The top path* represents components controlling water supply, and the *bottom path* represents components controlling and securing the fuel supply.



Figur 3 - RBD for Top event.

Component description:

LL1: Low level transmitter 1

LL2: Low level transmitter 2

LICV: Level indicator controller valve

PC: Pressure controller

PCV: Pressure controller valve

PLC: Programmable logic controller

SV: Solenoid valve

WP: Water pipe

2.3.1 Fault tree versus reliability block diagram

Choosing between fault tree or reliability block diagram is in most cases a matter of practicality. When the fault tree consists of only and-gates and or-gates, like in our case here, both methods may yield the same result. An and-gate is represented by a series-structure, and an or-gate is represented by a parallel-gate in a reliability block diagram.

The question is not only practicality, but also intuitiveness. In the case presented in this task, we view the reliability block diagram as faster and easier to understand.

Choosing method depends largely on how the system is structured, and how you are able to present the data. For some systems a fault tree might be easier to read, while for other the reliability block diagram looks simpler. In the case presented in this task, we view the reliability block diagram as faster and easier to understand.

2.4 Minimal cut sets

We used CARA to find the minimal cut sets from our fault tree. See Appendix 3 for output report. Below we present the minimal cut sets by order. Cut sets 1-4 is of order 2, and cut sets 5-8 is of order 3.

No.	Cut sets
1	{LICV, PCV}
2	{PLC, PCV}
3	{PLC, PC}
4	{WP, PCV}
5	{WP, SV, PC}
6	{LICV, SV, PC}
7	{LL1, LL2, PCV}
8	{LL1, LL2, PC}

Table 1 Cut sets from fault tree

Probability of Failure on Demand is only valid for hidden failures, thus we neglect WP as a failure when considering which cut set is the most important. We assume WP to be an evident failure which would be detected right away. Generally, we consider the cut sets of the lowest order to be the most important, when neglecting component failure rates.

Furthermore, we consider cut set 1 to be the most important, due to the fact that component LICV has the highest failure rate.

3. Statistics

3.1 SIS, PFD & voting method

In the following section we answer task 3 of the assignment.

3.1.1 Safety-instrumented systems

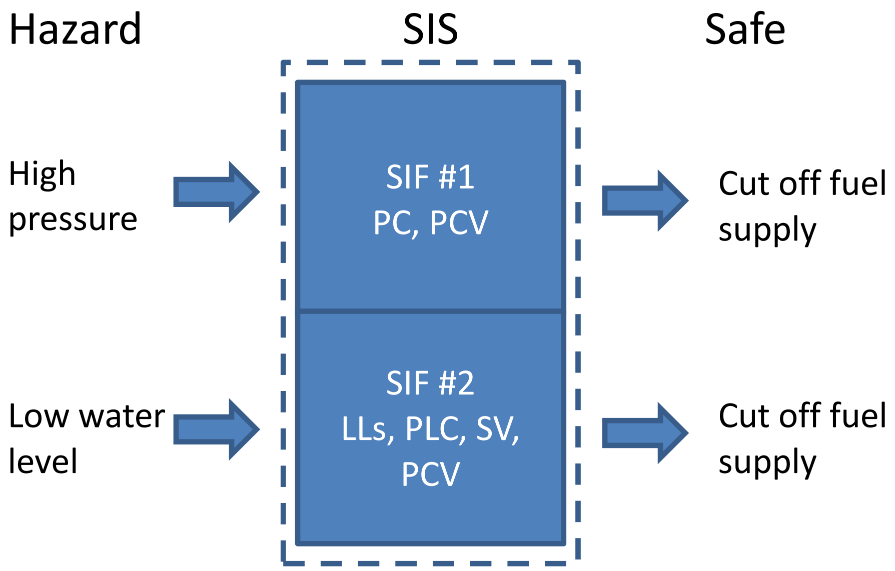
"According to IEC61511 a safety instrumented system (SIS) is made up of one or more safety instrumented functions (SIF)[5]. A SIF is a function that is (…) intended to achieve or maintain a safe state for the EUC with respect to a specified process demand" [6]

The SIS for the boiler system is presented in figure 4. The SIFs are:

- SIF #1; High pressure in the boiler cuts off fuel supply to burner chamber. The high pressure in is detected by the pressure controller (PC). The PC is also fills the role as a logic solver, and bleeds off pressure in the pneumatic line to close the PCV, which is the actuating item.
- SIF #2; Low water level in the boiler cuts off fuel supply to burner chamber. The low water level is detected by the low level transmitters, and the PLC unit opens the SV (actuating item) to bleed off the pressure in the pneumatic line, thus closing the PCV (actuating item).

[5] http://www2.emersonprocess.com/siteadmincenter/PM%20DeltaV%20Documents/Articles/ControlMagazine/The-Safety-Instrumented-Function-An-S-Word-Worth-Knowing.pdf

[6] Rausand/Høyland 2004 p. 421



Figur 4 - A safety instrumented system (SIS) in combination with two safety instrumented functions (SIFs)

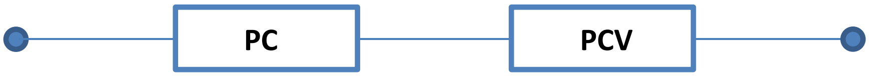
The water level is maintained by a control circuit connected to the regulator valve LICV. The logic unit PLC translates the signals from the level transmitters to a signal controlling the valve LICV. For SIF #2, the low level transmitters and the PLC is both part of the SIS and the control system.

3.1.2 Reliability block diagram

After having consulted with the student assistant[7] we decided to set up a reliability block diagram for each SIF respectively instead of one for the SIS, and calculate the PFD for each SIF individually.

3.1.2.1 SIF #1

This RBD is a simple series structure of two components. See figure 5.



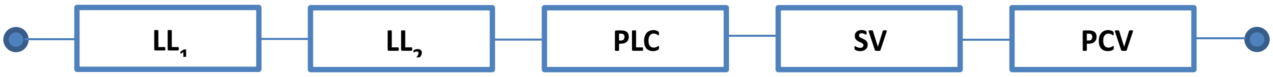
Figur 5. Reliability block diagram for SIF#1

3.1.2.2 SIF #2

We use two different RBDs to illustrate the different voting methods before discussing them in the next part of this task, see figure 6 and 7. We choose to not have the common cause failure illustrated in our RBDs, instead we have calculated with the combined failure rate in the PFDs.

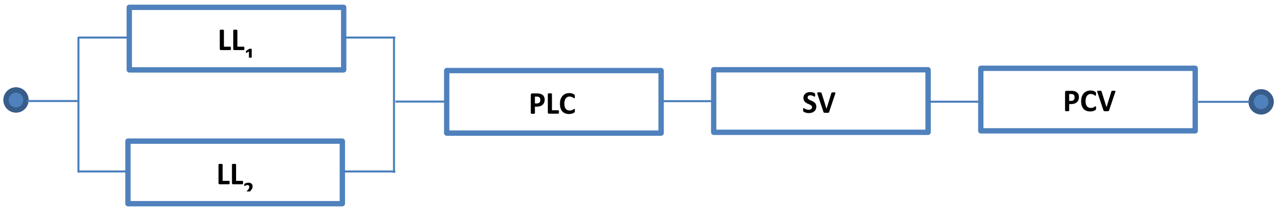
[7] The group spoke with Jun Zhou on Monday 19.11.2012 around noon.

With 2-out-of-2 voting method:



Figur 6. RBD for SIF#2 with a 2oo2 voting structure

With 1-out-of-2 voting method:



Figur4 - RBD for SIF #2 with a 1oo2 voting structure

3.1.3 PFD of the SIFs

To calculate the PFD of the SIFs, we have used the approximation formulas presented in table 10.1[8]. These formulas are often used in practical calculations.[9] The approximated values are conservative.

The items have different failure rates, and some have different test intervals. Thus, for each series of components, we calculate the PFD of each component and obtain the PFD of the series by adding these together.

3.1.3.1 PFD of SIF #1

$$PFD_{SIF\#1} = \frac{\lambda_{DU,PC}\tau_{PC}}{2} + \frac{\lambda_{DU,PCV}\tau_{PCV}}{2}$$

With $\lambda_{DU,PC} = 7 * 10^{-6}$, $\lambda_{DU,PCV} = 6 * 10^{-6}$ and $\tau_{PCV} = 2\tau_{PC} = 8640$ we get a PFD for SIF #1:

$$PFD_{SIF\#1} = 2{,}74\%$$

3.1.3.2 PFD of SIF #2

Reliability of the 2oo2 substructure

Since we have used the β-factor model to take into account common cause failures, we regard each component as independent and calculate the failure rate of each path through the structure in figure 3.1.3.

[8] Rausand/Høyland 2004 p. 432

[9] Rausand/Høyland 2004 p. 428

We observe that the 2oo2 structure is a simple series structure. We have included the β-factor in the failure rates for the low level sensors by combining the following equations:

When $\lambda_{DU,i}\tau$ is < 0,2 the PFD of the system is approximately the sum of the PFD of the individual components.[10] In our case, all of the components have small failure rates which would justify simply calculating the sum. Using the given failure rates for the components, this gives us a formula for the PFD of the whole 2oo2 system:

$$PFD_{2oo2} = \sum PFD_i = \frac{\lambda_{DU,LL}\tau_{LL}}{2} + \frac{\lambda_{DU,LL}\tau_{LL}}{2} + \frac{\lambda_{DU,PLC}\tau_{PLC}}{2} + \frac{\lambda_{DU,SV}\tau_{SV}}{2} + \frac{\lambda_{DU,PCV}\tau_{PCV}}{2}$$

$$PFD_{2oo2} = 3{,}16\%$$

Reliability of the 1oo2 substructure

The 1oo2 RBD has a slightly different configuration where the two low-level sensors are in parallel. Using the *koon* table from page 431 in Rausand/Høyland (2004), we get a slightly different formula for the combined PFD:

$$PFD_{1oo2} = \sum PFD_i = \frac{(\lambda_{DU,LL}\tau_{LL})^2}{3} + \frac{\lambda_{DU,PLC}\tau_{PLC}}{2} + \frac{\lambda_{DU,SV}\tau_{SV}}{2} + \frac{\lambda_{DU,PCV}\tau_{PCV}}{2}$$

$$PFD_{1oo2} = 2{,}21\%$$

3.1.4 Spurious trip rates of SIF #2

One of the disadvantages of a 1oo2 system is a shutdown of the fuel supply if one of the indicators is giving spurious signals. To be able to discuss which voting method is preferred we need to calculate the amount of shutdowns due to spurious signals. Formulas for calculating spurious trip rates[11]:

$$ST_{1oo2} = \sum \lambda_{ST,i} = \lambda_{ST,LL} + \lambda_{ST,PLC} + \lambda_{ST,SV} + \lambda_{ST,PCV}$$

$$ST_{1oo2} = 1{,}74 * 10^{-5}$$

$$ST_{2oo2} = \sum \lambda_{ST,i} = 2\lambda_{ST,LL} + \lambda_{ST,PLC} + \lambda_{ST,SV} + \lambda_{ST,PCV}$$

$$ST_{2oo2} = 2{,}34 * 10^{-5}$$

3.1.5 Discussion of voting method

Both voting's has its advantages and disadvantages. The 1-out-of-2 has the advantage that the signal is sent to close the fuel line even though only one of the low level transmitters are

[10] Rausand/Høyland 2004 p. 428-431

[11] Rausand/Høyland 2004 p. 440 Table 10.2

working. This however is also a disadvantage, assuming the operator cannot know whether one or both are sending the signal. Having a DU error in one of the indicators will severely increase the probability of our TOP-event happening.

Another notable disadvantage is that the 1-out-of-2 voting will lead to closure of the fuel inlet if one of the transmitters have failed and is giving spurious signals to the PLC, causing down time in the system. As shown in the previous calculation there is only a small change in the amount of spurious signals.

The 2oo2 has the advantage that the fuel line will not be closed down due to spurious behavior in one of the LL transmitters, but require them both to signal in order for the PCV to close the inlet of fuel.

However, many of the disadvantages in the two different voting's are secured by the fact that we have another safety cycle via the PC that will close down the fuel line if the pressure in the steam boiler gets too high. The 1oo2 voting is the preferred method when we take the severity of the consequences in account. We perceive the risk of having some unnecessary downtime as more acceptable than the risk of not closing the inlet of fuel when in fact the water level is low and we risk boiling the boiler dry.

3.2 TOP event probability

We have used CARA to compute the Top event probability. The probability of the top event is **0,08662%** (see appendix 4). This is the average probability that the system will boil dry within each test interval. CARA uses Upper bound approximation, which will yield a conservative result for the PFD, meaning the real PFD will always be lower than this approximation. Hence, we expect the true probability of the top event to be lower than that stated above.

3.3 Perfect proof-testing

The formulas used to calculate the PFD assume that all components are "as good as new" after testing, meaning that all hidden failures are detected, and that the failure rate of the item is constant. The formulas given in chapter 10 of the textbook assume that an item has an exponential life distribution, meaning that the failure rate function is independent of time. In our opinion this may be realistic for an item during its useful life period (at least for certain types of components).

Several of the the components in our system are simple valves, a function test of these would presumably reveal a lot of otherwise undetected errors. From the formulas we have that the failure rate must always "reset" after each test for the calculations to be correct.

All components are set to be tested on a regular interval, the PCV and LICV every year, and the rest every 6 months. The assumption that one could detect all DU errors during a simple test is wrong, but necessary for the calculations. There could be undetected cracks in the metal and the valves will be worn down over time.

3.4 Birnbaums measure of component importance

We had CARA calculate the importance of each component according to our fault tree. In general Birnbaums measure of component importance is calculated using the formula:

$$I^B(i|t) = \frac{\partial h(\boldsymbol{p}(t))}{\partial p_i(t)} = h(1_i, \boldsymbol{p}(t)) - h(0_i, \boldsymbol{p}(t))$$

The output from CARA is presented in the table below. See Appendix 5 for the data output from CARA.

No	Name	$I^B(i)$
1	PLC	$3{,}9301*10^{-2}$
2	PCV	$3{,}4287*10^{-2}$
3	LICV	$2{,}5646*10^{-2}$
4	WP	$2{,}4777*10^{-2}$
5	PC	$7{,}2878*10^{-4}$
6	SV	$4{,}9543*10^{-4}$
7	LL1	$1{,}8848*10^{-4}$
8	LL2	$1{,}8848*10^{-4}$

Table 2 Birnbaum's measure of component importance

The resulting number for each component is the probability that the system is in such a state that component i is critical for the system. After computing the measures for the different components, we see that PLC, PCV, LICV and WP all have a probability larger than 1% of becoming critical to the system. This is the same as the probability that the other components in the cut sets containing the component in question, have failed. The most important component is the PLC, which has got a 3,9% probability of becoming critical to the system.

3.5 Consideration of total system safety

There are, as the previous analysis have shown, ways the system could fail. However, the safety systems put in place and the low top event probability/ relatively even distributions of component importance (Table 2) also shows us that this is a sufficiently safe system.

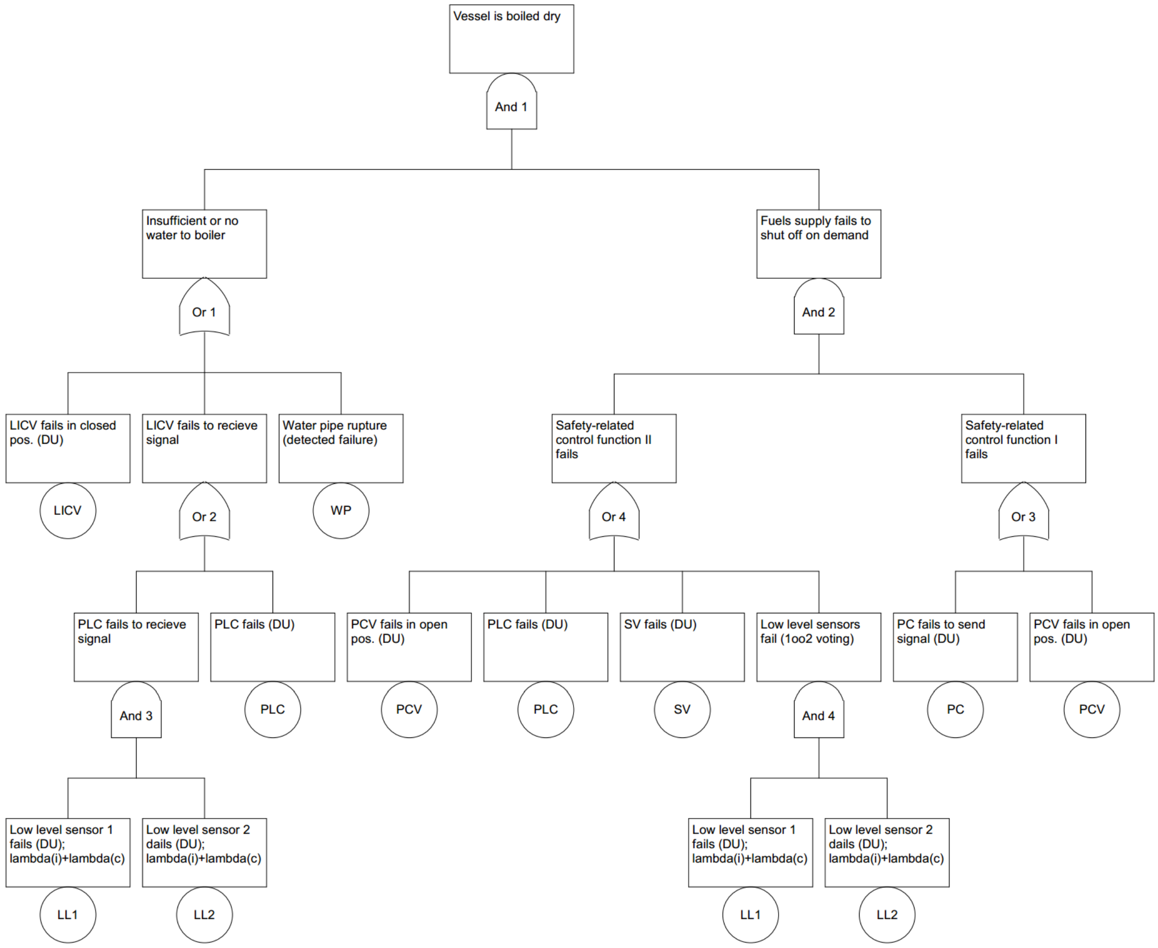
A way of improving the safety could be to use relative frequent testing routines to try to uncover possible hidden failures in the safety system. Meaning, that you allow the regular control system to let the water level come down towards the low level indicators in order to see how the system reacts. A possible scenario could be that one observed that the PC signaled the pressure to be above the allowed level, in addition to one of the LL transmitters giving a signal that the water level was too low. Then one could assume that one of the LL transmitters has failed, or that both the PC and the other LL transmitter gave spurious signals.

The negative side of doing this testing, is that if the safety system is working as it should, it will result in the fuel being cut off, thus creating some downtime for the system. We do not have sufficient knowledge on the frames of the bigger machinery in this case, to either be able to recommend this testing routine or not.

In reality the PLC and PC will most likely conduct diagnostic self-testing, meaning that several of the possible hidden failures will be detected once they occur. This way minimizing the risk of system failure, while still maintaining operation and minimizing downtime.

4. Appendices

Appendix 1 – Fault tree


Vessel is boiled dry
And 1
Insufficient or no water to boiler
Or 1
Fuels supply fails to shut off on demand
And 2
LICV fails in closed pos. (DU)
LICV
LICV fails to recieve signal
Or 2
Water pipe rupture (detected failure)
WP
Safety-related control function II fails
Or 4
Safety-related control function I fails
Or 3
PLC fails to recieve signal
And 3
PLC fails (DU)
PLC
PCV fails in open pos. (DU)
PCV
PLC fails (DU)
PLC
SV fails (DU)
SV
Low level sensors fail (1oo2 voting)
And 4
PC fails to send signal (DU)
PC
PCV fails in open pos. (DU)
PCV
Low level sensor 1 fails (DU); lambda(i)+lambda(c)
LL1
Low level sensor 2 dails (DU); lambda(i)+lambda(c)
LL2
Low level sensor 1 fails (DU); lambda(i)+lambda(c)
LL1
Low level sensor 2 dails (DU); lambda(i)+lambda(c)
LL2

Appendix 2 – Event overview

```
CARA Fault Tree version 4.0 (c) SINTEF 1996
University License - NTNU, Norway
Not for commercial use
Date: 22.11.2012        Time: 14:20:59

File:  Fault tree for steam boiler system

New fault tree

Basic events

Name          Type            Parameter    Value         Error factor   Shared
              Description
SV            Test intervall  Lambda       4,0000e-006   1,0000e+000    -          SV fails
(DU)
                              Tau          8,0000e+000   1,0000e+000
                              T*           4,3200e+003
PLC           Test intervall  Lambda       2,0000e-007   1,0000e+000    -          PLC fails
(DU)
                              Tau          6,0000e+000   1,0000e+000
                              T*           4,3200e+003
PC            Test intervall  Lambda       7,0000e-006   1,0000e+000    -          PC fails
to send signal (DU)
                              Tau          8,0000e+000   1,0000e+000
                              T*           4,3200e+003
WP            Non repairable  Lambda       0,0000e+000   1,0000e+000    -          Water
pipe rupture (detected failure)
PCV           Test intervall  Lambda       6,0000e-006   1,0000e+000    -          PCV fails
in open pos. (DU)
                              Tau          1,0000e+001   1,0000e+000
                              T*           8,6400e+003
LL1           Test intervall  Lambda       2,2222e-006   1,0000e+000    -          Low level
sensor 1 fails (DU); lambda(i)+lambda(c)
                              Tau          6,0000e+000   1,0000e+000
                              T*           4,3200e+003
LL2           Test intervall  Lambda       2,2222e-006   1,0000e+000    -          Low level
sensor 2 dails (DU); lambda(i)+lambda(c)
                              Tau          6,0000e+000   1,0000e+000
                              T*           4,3200e+003
LICV          Test intervall  Lambda       8,0000e-006   1,0000e+000    -          LICV fails
in closed pos. (DU)
                              Tau          1,2000e+001   1,0000e+000
                              T*           8,6400e+003
```

Appendix 3 – Cut sets

```
CARA Fault Tree version 4.0 (c) SINTEF 1996
University License - NTNU, Norway
Not for commercial use
Date: 22.11.2012          Time: 12:57:17

File:  Fault tree for steam boiler system

New fault tree

Cut set(s) with 1 component (None found)

Cut set(s) with 2 components (Total: 4)
   {PLC,PCV}
   {PLC,PC}
   {LICV,PCV}
   {WP,PCV}

Cut set(s) with 3 components (Total: 4)
   {LL1,LL2,PC}
   {LL1,LL2,PCV}
   {LICV,SV,PC}
   {WP,SV,PC}

Cut set(s) with 4 components (None found)
 Total number of cut sets up to order 4: 8
```

Appendix 4 – Top event probability

CARA Fault Tree version 4.0 (c) SINTEF 1996
University License - NTNU, Norway
Not for commercial use
Date: 22.11.2012 Time: 14:21:57

File: Fault tree for steam boiler system

New fault tree

Qo(t) - Unavailability

Method: Exact calculation (ERAC)

Maximum cut size: 4 Mod. level: 0 Top event: And 1

Unavailability [Qo(t)]:

	Est.
t	Value
0	8,8662e-004
876	8,8662e-004
1752	8,8662e-004
2628	8,8662e-004
3504	8,8662e-004
4380	8,8662e-004
5256	8,8662e-004
6132	8,8662e-004
7008	8,8662e-004
7884	8,8662e-004
8760	8,8662e-004

Appendix 5 – Birnbaum’s measure of reliability importance

```
CARA Fault Tree version 4.0 (c) SINTEF 1996
University License - NTNU, Norway
Not for commercial use
Date: 22.11.2012        Time: 14:22:43

File:  Fault tree for steam boiler system

New fault tree

Component importance

Method: Exact calculation (ERAC)

Maximum cut size: 4     Mod. level: 0     Top event: And 1

Mission time t=4320

                                                       Birnb.
     Event          Low             High               rel.
     PLC            8,6960E-004     4,0171E-002        3,9301E-002
     PCV            1,1235E-005     3,4298E-002        3,4287E-002
     LICV           1,8321E-005     2,5664E-002        2,5646E-002
     WP             8,8662E-004     2,5664E-002        2,4777E-002
     PC             8,7567E-004     1,6044E-003        7,2878E-004
     SV             8,8235E-004     1,3778E-003        4,9543E-004
     LL2            8,8571E-004     1,0742E-003        1,8848E-004
     LL1            8,8571E-004     1,0742E-003        1,8848E-004
```

Appendix 6 - FMECA

Description of unit				Description of failure			Effect of Failure		Failure rate	Severity ranking	Risk reducing measures	Comments
Ref. no	(Component Description)	Function	Operational Mode	Failure Mode	Failure cause or mechanism	Detection of failure	On the subsystem	On the system function				
V-1	Manually operated bypass valve	Remain closed and prevent fuel from passing through the valve when PCV is in operation	Closed	Not possible to close the valve (completely)	Insufficient lubrication	Evident failure; human perception	Fuel passing through the valve	No control on fuel flow	Low	High	Install an extra valve in series with the bypass valve; reduce time between inspection	
					Broken valve wheel/handle	Evident failure; human perception	Fuel passing through the valve	No control on fuel flow	Low	High		It is believed that the valve wheel may break when trying to close the valve
				Open when PCV is in operation	Human error, i.e. someone forgot to close the valve after	Hidden failure; inspection	Fuel passing through the valve	No control on fuel flow	Low	High	Reduce time between inspection	
				Leakage in closed position	Damaged/worn out valve bushing	Hidden failure; inspection	(Some) Fuel passing through the valve	Reduced control on fuel flow	Med	High	Reduce time between maintenance/inspection	
					Human error, not completely closed after maintenance on PCV	Hidden failure; inspection	(Some) Fuel passing through the valve	Reduced control on fuel flow	Med	High	Install flow meter on the line right after the valve	
		Remain open; provide flow to burner chamber while enableing maintenance of PCV	Open	Valve closed; fail to open the valve completely (manually)	Insufficient lubrication	Evident failure (manually operated), Scheduled maintenance, When the valve is in use	No/reduced flow through the valve	Whole system must be shut down to perform mainentance on PCV	Low	Low		
					Broken valve handle	Evident failure (manually operated)	No/reduced flow through the valve	Whole system must be shut down to perform mainentance on PCV	Low	Low		
SV	Electromechanic solenoid valve, normally closed (NC)	Open on signal from PLC/PC	Closed	Valve will not open when valve circuit is energized (direct-acting valve)	Low voltage or no voltage to solenoid coil	Hidden failure (?) Fuel remains cut off. If water is supplied, the boiler will be filled, and	Fuel to burner chamber not cut off	No control on fuel flow, LICV and PC rendered useless	na	High	Reduce time between maintenance/inspection	
					Burned out coil	Hidden failure, inspection						
					Excessive foreign matter jamming core in core tube	Hidden failure, inspection						
					Binding core or damaged core tube	Hidden failure, inspection						
					Excessive fluid pressure	Hidden failure, inspection						
				Spurious open		Evident failure (?)						
		Close when signal from PLC/PC is cut off	Open	Valve will not close or shift when valve circuit is de-energized (direct-acting valve)	Coil not de-energized	Hidden failure	No fuel to burner chamber	Not functioning; no steam generated	Med	Med	Reduce time between maintenance/inspection	
					Excessive foreign matter jamming core in core tube	Hidden failure			Med	Med		
					Damaged disc or seat causing internal leakage	Hidden failure			Med	Med		
					Binding core or damaged core tube	Hidden failure			Med	Med		
					Damaged spring	Hidden failure			Med	Med		
				Spurious close		Evident failure			Med	Med		
LL	Low level transmitter	Send signal to PLC when water level decreases below a said level	Passive (no signal when OK)	Spurious signal (false alarm)	Circuit malfunction, too high current	Detected failure	PLC recieves signal to cut off fuel supply	Not functioning; no steam generated, given PLC and PCV working	Low	Low	Reduce time between maintenance/inspection	
					Dirt covering transmitter	Detected failure			Low	Low		
				No signal when it is supposed to send signal	Circuit malfunction, no or too low current	Hidden failure	No signal sent to PLC	System does not shut down	Low	High		