SafePool

Seçkin Gokçe[1], Process Safety Superintendent, Ahmet Can Serfidan[2], Process Control Supervisor, Eyüp Azizoğlu[3] Operation Supervisor, Gökhan Gedik[4], Instrument Supervisor

TUPRAS Izmit Refinery, Kocaeli/TURKEY

Facilities have a large number and variety of equipment that provides process control and process safety according to risk assessments created for predetermined catastrophic scenarios. It is assumed that this equipment will always work correctly and be active; however, in practice these protections might be disabled for various reasons. Hereby, SafePool monitors and analyses the live data of the facility's predetermined critical equipment. Thus, it determines immediately whether the facility is at an acceptable risk level. SafePool is accessible by everyone and automatically creates a fault record for the faults it detects.

Keywords - Online Risk Monitoring, Reliability, Risk assessment, Digitalization, PSM

I. INTRODUCTION

Refineries need to own a good process safety management system in order to prevent unplanned events which might result in a major accident and to ensure asset integrity. Facilities want to be able to track plant-wide performance, track down bad actors no matter where they are, and maintain lower risk throughout the plant's lifespan. PSM necessitates a large number of resources with varying levels of internal and external knowledge, as well as a variety of manual functions for gathering important data and conducting safety-related research (HAZOP, LOPA, SIL, and so on). In addition, PSM incorporates numerous features to describe hazardous scenarios and manage hazardous materials in a safe and dependable manner. At that moment, the precautions for these dangerous scenarios become more critical, and SafePool is called in.

To identify their scenarios, each facility should do a process hazard study. Facilities learn about their critical and dangerous conditions as a result of these investigations, raising awareness and emphasizing the need of safety essential barriers. Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) will be performed after the HAZOP studies to determine the ALARP tolerance of the facilities. All safety barriers are judged healthy and in good operating order during this process. In fact, under typical operating conditions, these safety barriers may not always be this way. SafePool builds a digital transfer environment for the important situations and barriers identified in the studies undertaken here, and tests if these barriers work in the live system under various error modes.SafePool makes a new calculation over the PFD value of the equipment that shows malfunction over the FTA/ETA installed in the system if a malfunction is detected for any reason through this control, and it reflects the current risk status of the facility numerically and sends warning mail to related disciplines about malfunctioning equipment to put in use. SafePool also helps to validate design assumptions and improve risk-based decisions.

II. HOW IT WORKS

A- Infrastructure

The most important feature of SafePool is that SafePool can tell whether a critical preventive equipment is functional, i.e. whether it can help prevent the emergency as it is designed when it is needed. We will call this as “status” of the equipment. And SafePool can tell this based on the online data. In this section, we will tell more about which data SafePool use for this aim:

- Process Data: Process Historian Database collects and stores plant process data. Thanks to this database, we can access to process value, set value and manipulated value of controllers, and many more. Frequency between two subsequent data point can be configured but 1 min data is adequate for SafePool algorithm.
- Operator Action Database: When a control operator takes any action on DCS, it is collected and stored on Operator Action Database. For example, operator might change the alarm level of a controller, or changed the mode of controller to manual.
- System Alarm Database: When there are alarms related with system like IOP, channel alarms, then they are stored in Alarm Database.

Although process data is ready to use, there are some data preparation needed for Operator Action Data.

- In system alarm database, the message does not contain tag name. Instead it provides the NODE/SLOT/CHANNEL like NODE 05 SLOT 05 CH 02. This should be converted to Tag Name like FIC101 for coherence.
- In operator action database, the wording in messages can vary from vendor to vendor (even among versions in a same vendor). For example, one unit holds the ESD By-Pass information like “Tag is By-pass” and another unit holds like “By-Pass” one. Again, all of those variation has to be eliminated before SafePool algorithm.

Besides databases, SafePool is the next digital step of process hazard analysis and procedures. Therefore, related HAZOP studies, Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) has to be done before SafePool integration. Based on those analysis, all safety barriers, their related Tag Names, FTA and ETA structure should be listed and given to SafePool as input.

B-Monitoring

-Process Value Freeze

Measuring process value correctly plays a crucial role for safety. If there is any anomality in reading process value for critical preventive equipment, then it should be detected and fixed immediately. The following problem illustrates the process value freeze problem:

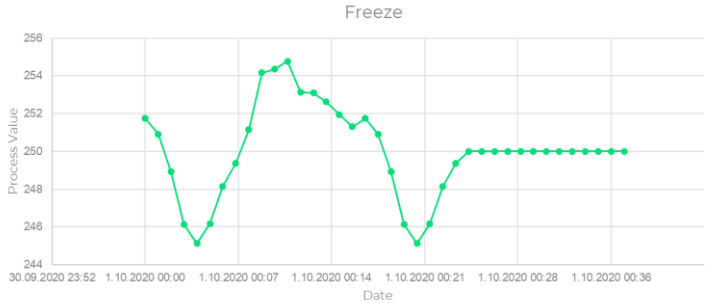

Figure 1. Process Value Freeze Chart

Since SafePool can access to process value database, the following formula detects whether there is process value problem or not:

$$\boldsymbol{a(t)_{Tag}} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{5}} \boldsymbol{abs(pv(t)_{Tag} - pv(t-i)_{Tag})}$$

$$\boldsymbol{pf(t)_{Tag}} = \begin{cases} \boldsymbol{0}, & \boldsymbol{a(t)_{Tag} = 0} \\ \boldsymbol{1}, & \boldsymbol{else}. \end{cases}$$

Where $\boldsymbol{pv(t)_{Tag}}$ is the process value of a certain tag at time t. We can think t-1 as the one period before process measurement. Therefore, we are checking all 5 previous process measurements and subtract them from the current process value and then sum them and store it inside $\boldsymbol{a(t)_{Tag}}$ variable. The summation should be 0 if there is a process freeze, 0 otherwise. We hold this information in $\boldsymbol{pf(t)_{Tag}}$. In other words, it is the process freeze status of a certain tag at time t. Finally, we store this information inside Process Freeze Table inside SafePool Database, which looks like this:

Table 1. Process Value Freeze Table in SafePool Database

Tag	FIC01	TIC15	LIC10
2021-08-01 00:00:00	1	0	0
2021-08-01 00:05:00	0	0	1
2021-08-01 00:10:00	0	0	0
…	…	…	..

- Process Anomaly Detection

Other than process value freeze, there might be some other anomalies in the process. Especially those anomalies are not related with the measurement malfunction, instead there is a significant change in the process condition. For example, the below figure tells that there is a significant standard deviation increase in the temperature measurement:

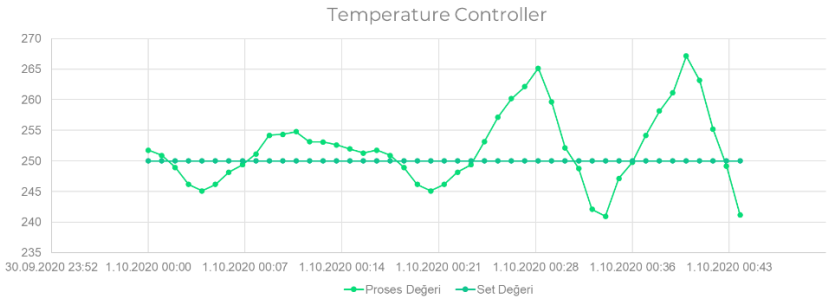

Figure 2. Temperature Controller Chart

SafePool checks following three information to catch anomaly:

- Standard Deviation of process value.
- Mean of process value.
- Mean of the difference between set value and process value for control loops.

To calculate of these statistics, we determine a time window. Although this time window can be changed from process to process, we took last 4 hours of data to describe the process condition. Then for each critical preventive equipment, we asked following questions to operation and process engineers:

1) What is the maximum allowable standard deviation for this process value?
2) What is the maximum and minimum values for this process value?
3) What is the maximum allowable difference between process value and set value?

Here is the final formula for calculating whether there is an anomaly or not:

$$\overline{pv_{Tag}} = \frac{1}{240}\sum_{i=0}^{239} pv(t-i)_{Tag}$$

$$std(t)_{Tag} = \sqrt{\frac{1}{240}\sum_{i=0}^{239}(pv(t-i)_{Tag} - \overline{pv_{Tag}})^2}$$

$$dev(t)_{Tag} = \frac{1}{240}(\sum_{i=0}^{239} abs(pv(t-i)_{Tag} - sv(t-i)_{Tag}))$$

Where $sv(t)_{Tag}$ is the set value of certain tag at time t.

$$anomaly(t)_{Tag} = \begin{cases} 0, & \overline{pv_{Tag}} < HighLimit_{Tag} \text{ and } \overline{pv_{Tag}} > LowLimit_{Tag} \\ & \text{and } std(t)_{Tag} < STDLimit_{Tag} \text{ and } dev(t)_{Tag} < DEVLimit_{Tag}; \\ 1, & else. \end{cases}$$

Finally, we store this information inside Anomaly State Table inside SafePool Database, similar to Process Freeze Table. Time interval between two rows are again 5 minutes. So, the above function is executed every 5 min.

- **Valve Position Limit**

Just like process value, we can access to valve openness of each control loop at given time from process database. This valve openness value should be between 10 and 90, otherwise it is accepted as valve is very close to out of control. Since loops we

are monitoring are the most critical preventive loops, it is not acceptable to be lower than 10 or higher than 90 in terms of valve openness. For example, in the below image, we see that valve openness is higher than 90 after certain point. It means that it cannot make corrective actions (especially when it needs to open valve) when needed.

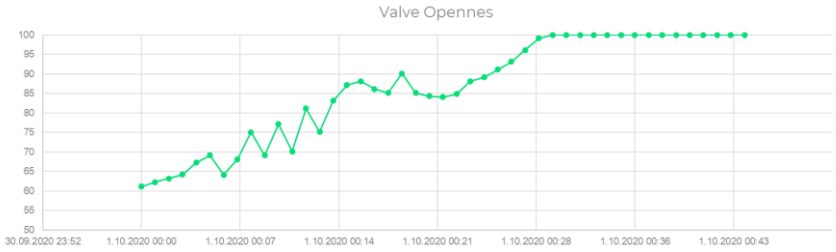

Figure 3. Valve Openness Checking

The formula for valve openness check is the following:

$$\boldsymbol{vop(t)_{Tag}} = \frac{\mathbf{1}}{\mathbf{5}} \sum_{\boldsymbol{i=0}}^{\mathbf{4}} \boldsymbol{mv(t-i)_{Tag}}$$

Again $\boldsymbol{mv(t)_{Tag}}$ is the valve position for the tag at time t. And SafePool calculates the last 5 samples and take the average and store this value in $\boldsymbol{vop(t)_{Tag}}$.

$$\boldsymbol{vcontrol(t)_{Tag}} = \begin{cases} \mathbf{0}, & \boldsymbol{vop(t)_{Tag} < 90 \; and \; vop(t)_{Tag} > 10} \\ \mathbf{1}, & \boldsymbol{else}. \end{cases}$$

Finally, we store this information inside Valve Openness Table inside SafePool Database, similar to Process Freeze Table. Time interval between two rows are again 5 minutes. So, the above function is executed every 5 min.

- **Control Mode Check**

Almost all control loops are designed to be in either auto or cascade mode. But when it comes to critical preventive control loops then their mode has to be auto/cascade, not manual definitely. This is crucial since if the control mode is manual, there will be no preventive action done by system. SafePool detects mode by monitoring operator action data. For the initial mode states, we provide the information manually, then SafePool tracks all mode changes in Operator Action Database. Then if there is a change, SafePool updates corresponding loop's mode condition accordingly. The following figure illustrates this process:

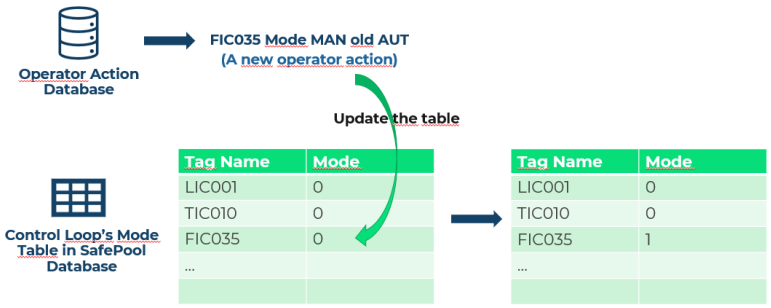

Figure 4. Control Loop Table

This function works since when the operator changes the mode, there is a pattern inside message. The first character displays tag name, and the third character tells the new mode status. This message changes from DCS vendor to vendor, but they have also consistent pattern too.

In contrast to other monitoring parameters, SafePool does not store Timestamp information in Control Loop Table.

- **ESD By-Pass**

Similar to control mode status, SafePool can track whether preventive equipment of Emergency Shutdown System (ESD) are active or not. For some reasons, control operators bypass these ESD systems. And those are the times that accidents and emergency situations occur frequently. When the operator bypasses an ESD system, this situation is stored inside Operator Action database, like this wording: "PT001A_BP Overridden". Again, the first character will be the tag, and if the message includes "overridden", the SafePool understand that this is a bypass situation and updated tag's corresponding By-pass value to 1. On the other hand, if the message contains "released", then SafePool updates the tag's value to 0 in By-pass Table.

- **System Alarm**

Very similar to control mode and ESD By-pass tracking, SafePool checks whether there is a system alarm on the critical preventive equipment. When there is a channel malfunction, or any input/output alarms on this critical equipment, operators have to take action quickly. SafePool detects this problem by applying the tracking message method. SafePool uses System Alarm database for this purpose. The only difference is that some of DCS vendors do not display tag name in system alarms. Instead they provide channel name like this one: Node 07 Slot 01 Channel 05. In that case, SafePool matches the corresponding Tag Name based on the pre-given channel – Tag Name link. Other than that, when there is any system alarm for a tag, then SafePool updates its value to 1 inside System Alarm Table.

All these six monitoring helps to identify whether this equipment is active or not. Namely, whether it can really prevent the accident by acting. Based on these six monitoring, we constructed a summary table and store it in Equipment Status table in SafePool Database:

Table 2. System Alarm Summary Table

Tag Name	Process Freeze	Anomaly	Valve	ControlMode	ESD	System
LIC001	0	0	0	1		0
LI002	1	0	0		1	1
LIC003	0	0	0	0		0
…	..	..	..	..	..	…

So, if there is a problem we assign 1 to corresponding cell. And if there is an at least one "1" for a tag, then SafePool concludes that that preventive equipment is out of service and should not be trustable.

Table 3. Out of Service Tag Table

Tag Name	Out of Service
LIC001	1
LI002	1
LIC003	0

In the following figure we summarize how does SafePool detect whether a critical equipment is out of service or not.

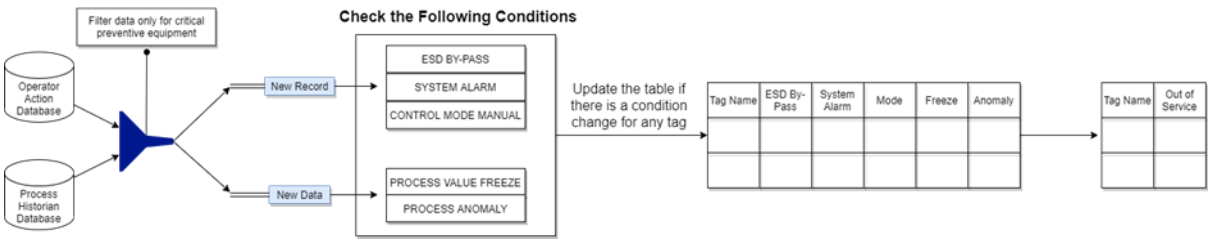

Figure 5. Critical Equipment Check Chart

C-Risk Assessment – PFD Value Calculation

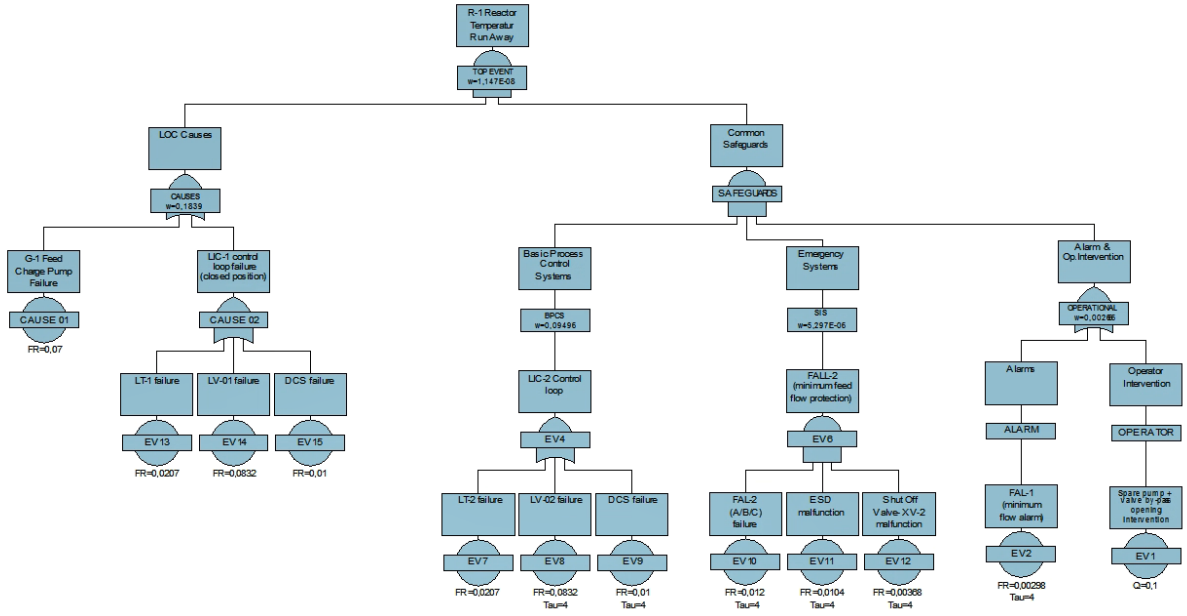

Figure 6. Fault Tree Analysis Graph

As you see on the Fault Tree Analysis (FTA) graph, major scenario is determined by during PHA studies. All loss of containment scenarios-initiator events and preventive safeguards are defined and put in analysis. Then top event frequency will be calculated. Normally, we assume that all defined effective safeguards work without any malfunctioning. If all safeguards run well top event frequency is 1,147E-8.

Let's assume that LT-2 was malfunctioned. After that all calculations should be calculated again because one of independent safeguard malfunctioned then top event frequency change as well.

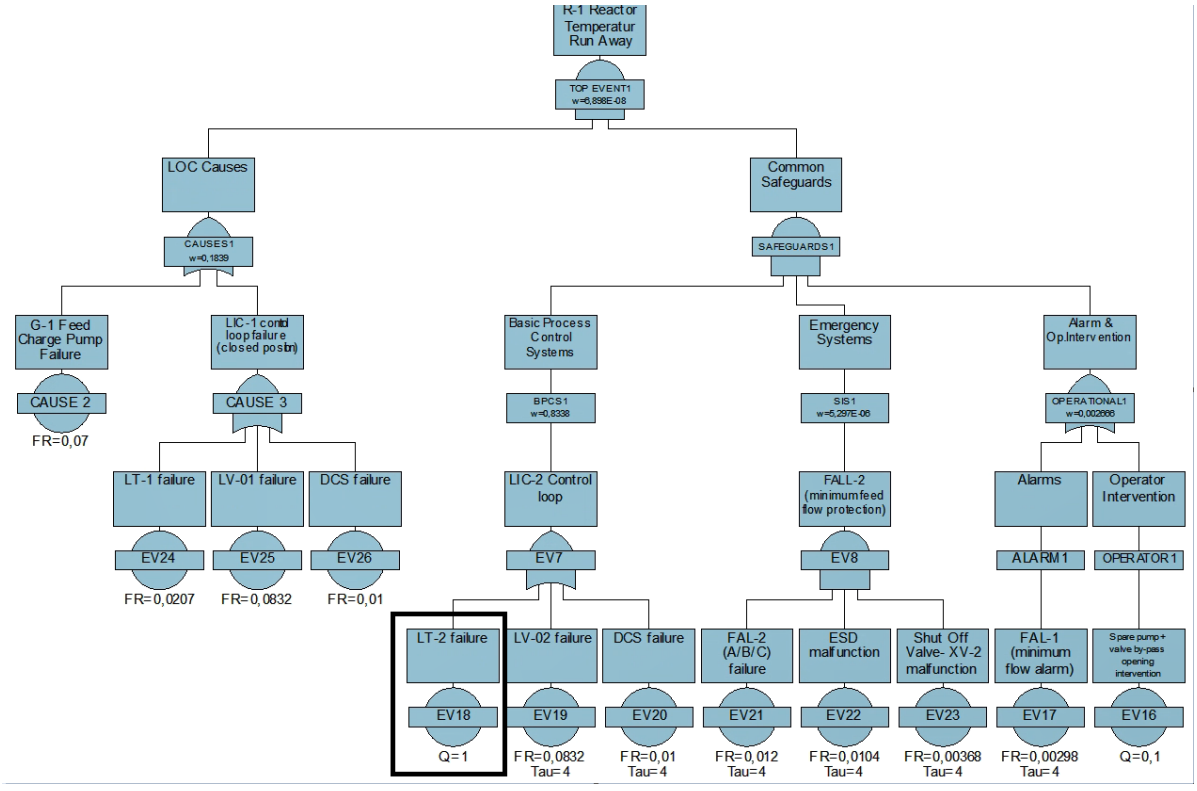

Figure 7. Event Tree Analysis

After malfunctioning of LT-2 Top event's new value is 6,88E-8. SafePool do the calculation again

After that Event Tree Analysis (ETA) will be done with mitigative barriers. Finally, top event's consequences types will be defined with Its final frequency. Final value compared with company's ALARP risk level.

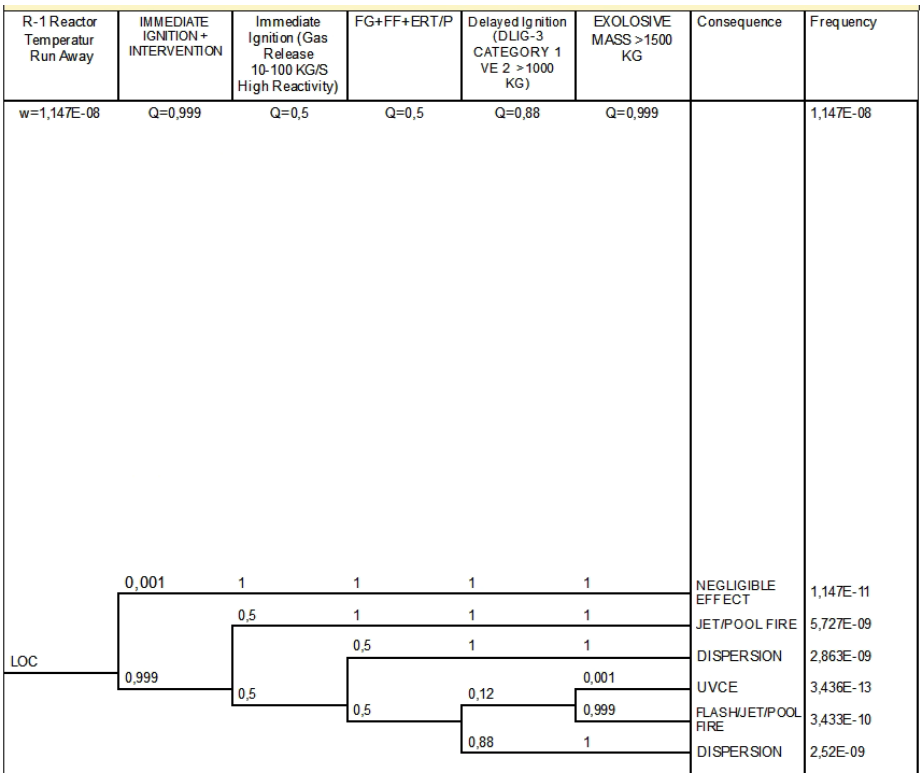

Figure 8. ALARP Risk Table

D - Notification

SafePool has the feature of not only calculating the live risk score, but also reporting the error that increases the risk score to the relevant units. It creates a maintenance request to the relevant maintenance unit so that the problem in the equipment, which is referred to as protection in the fault tree analyses (FTA), can be eliminated as soon as possible. It creates the maintenance request high priority by communicating with the maintenance coordination interface used by the facility. As a result, it calls the equipment responsible to take action on the malfunction and reduces the facility risk level back to an acceptable level.

E- Application Interface

In order to display results and make it accessible to all operators, engineers and managers in the refinery, we developed a basic web application. It has four categories:

1. Out of Service Equipment

In this tab, we show which tags are not active, ie which requires immediate attention. Otherwise they will not prevent accident in opposed to their design.

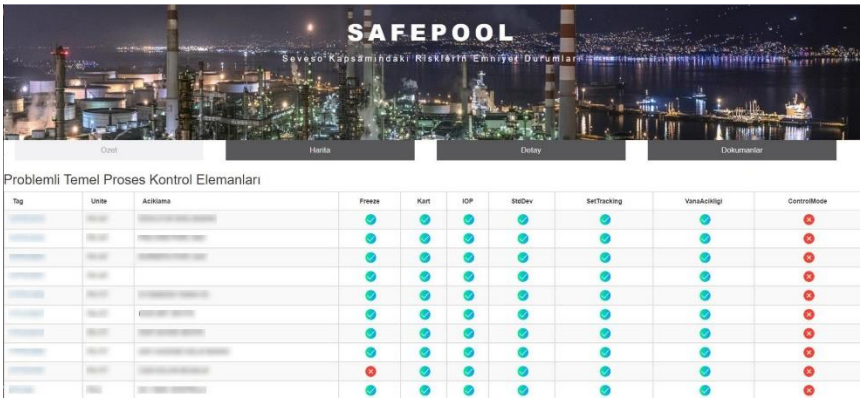

Figure 9. Refinery Map Risk Index Per Unit

In this tab, the user can see the current risk scores of all units. If the risk scores for all cases in unit are within acceptable rates, then it is coloured as green. If there is at least one high risk for a case, then it is coloured as red. Moreover, when the user clicks on the unit on the map, he/she can see the all cases and corresponding risk for the unit.

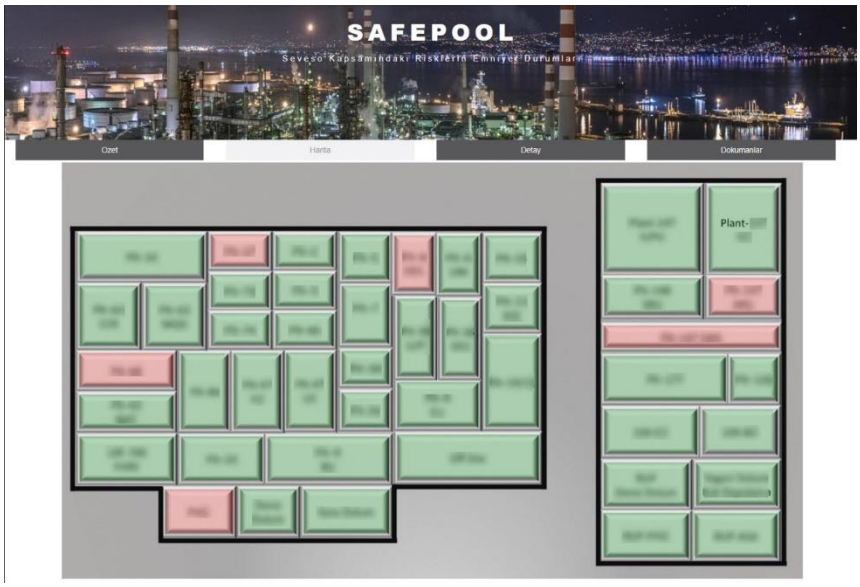

Figure 10. Detailed Case Review

We provide a detailed version of risk analysis of selected case. The user can see which equipment are in this case, and their current status.

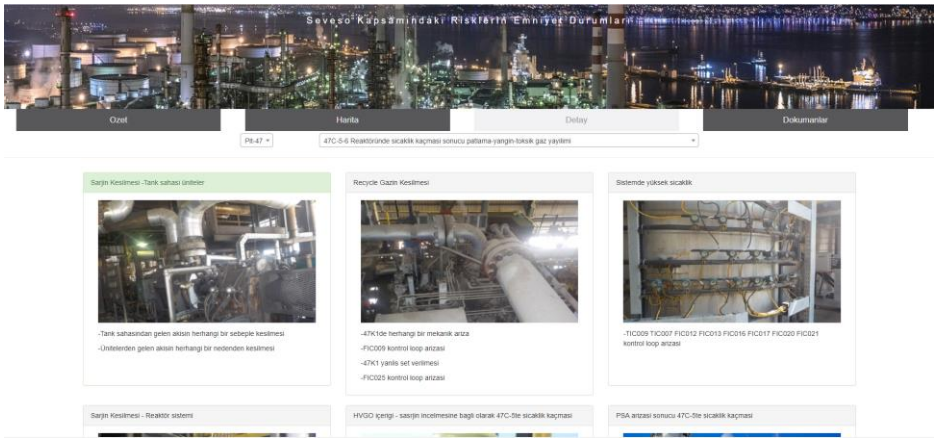

Figure 11. Documentation

This option is for to download desired FTA/ETA documents.

III. CONCLUSION

In the past, process safety was perceived as only the task of process safety experts. However, with the commissioning of the SafePool project, process safety became the priority of every employee. With the SafePool project, instant proses data transfer is provided by using digital communication infrastructures. So, The SafePool project has become a bridge in terms of digitalization in process safety. In this way, data is processed with logic algorithms without delay, making it possible to detect process safety risks much earlier and raise awareness.

Thanks to SafePool, Control room operators and engineers make sure that critical barriers in their system will work when needed.