

Proceeding Paper

Risk Assessment in a Petrochemical Plant Using Socio-Technical Approaches (STAMP-STPA) †

Mechhoud El-Arkam *, Bendib Riad , Aribi Aya and Zennir Youcef 

Laboratory of Automatic Skikda (LAS), Institut of Applied Sciences and Techniques, University 20 August 1955, Skikda 21000, Algeria

* Correspondence: el-arkam.mechhoud@univ-skikda.dz

† Presented at the 2nd International Conference on Computational Engineering and Intelligent Systems, Online, 18–20 November 2022.

Abstract: Major accidents continue to occur in chemical process industry, which may have serious consequences costing billion dollars and what is worse many human lives. That means the traditional Hazard analysis techniques are not becoming enough due to the increasing complexity of industrial plants. The main objective of this work is to present a new accident analysis technique based on system theory that has been developed lately changing the focus from reliability to system theory, in order to improve safety and for a better manage of risk. The considered is High Density Polyethylene plant which located in the Skikda industrial zone.

Keywords: STAMP; STPA; risk analysis; HDPE; petrochemical industries; safety; hazard

1. Introduction

There are many kinds of equipment in the petrochemical plants and petroleum refineries, usually presenting complex structures and several parameters. In such plants, it is important to consider different and critical types of risks, such as explosions, fire and toxic release which may cause serious damage either to human lives, equipment and plant or to the environment.

There are some traditional techniques developed during the last century employed to identify losses and hazards of chemical processes. The useful risk assessment methods are: HAZOP, FMEA, FTA, ETA . . . etc. [1], these methods are based on the component failures; they consider the risks as a chain of events and don't take in consideration the interaction between the components. Conventional methods have been used for a long time; they are not well-suited to handle modern systems with complex software, human-machine interactions, and decision-making procedures.

In order to conduct an automated risk assessment we are using another type of methodologies, as the socio-technical methods STAMP-STPA. In this paper we propose to implement the obtained results from STAMP-STPA, that is applied on the High Density Poly-Ethylene (HDPE) Reactor into a DCS to help the operator to take a good and safe decision.

2. Proposed Approach

The proposed approach is consist of four phases, the first one is the description of process, the second one is determining its position in the socio-technical system by STAMP method, the third phase is the application of System Theoretic Process Analysis (STPA) method and the fourth one is the implementation of the obtained results in the control system and display it in its HMI, to help operator in case of abnormal situation take a good and safe decision.



Citation: El-Arkam, M.; Riad, B.; Aya, A.; Youcef, Z. Risk Assessment in a Petrochemical Plant Using Socio-Technical Approaches (STAMP-STPA). *Eng. Proc.* **2023**, *29*, 8. <https://doi.org/10.3390/engproc2023029008>

Academic Editors:
Abdelmadjid Recioui,
Hamid Bentarzi and Fatma
Zohra Dekhandji

Published: 11 January 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

2.1. STAMP Systems Theoretic Accident Model and Processes

STAMP model is proposed by Leveson to model accident causation, it considers system theory as a useful way to analyze system accidents [2]. In STAMP safety is seen as a control problem, and it is managed by a control structure embedded in an adaptive socio-technical system, rather than in conventional methods, when accidents simply occur due to independent component failures, rather they occur when external disturbances, component failures, or dysfunctional interactions among system components are not adequately handled by the control system [2]. Safety management is defined as a continuous control task to impose the constraints necessary to limit system behavior to safe changes and adaptations. The main concepts in STAMP are: control loops, system model, constraints and levels of control. The cause of an accident, is viewed as the result of a lack of constraints imposed on the system design and on the operations, that is, by inadequate enforcement of constraints on behavior at each level of a socio-technical system, rather of a series of events [3].

2.2. STPA (System Theoretic Process Analysis)

STPA is a hazard analysis technique that embodies the STAMP accident causality model. It is based on control and system theory rather than the reliability theory underlying most existing hazard analysis techniques [4]. STPA does not generate a probability number related to the hazard. STPA is more powerful in terms of identifying more causal factors and hazardous scenarios, particularly those related to software, system design, and human behavior [5]. To apply STPA four steps should be followed:

1. Identify hazards and accidents: in this step we define the accidents and identify the hazards associated to those accidents.
2. Model the control structure: this step allow us to draw the feedback control system under study, from this model we can visualize actors involved, control actions and feedback information.
3. Identify unsafe control actions: Unsafe control actions UCAs are the wrong actions that lead to hazard. The UCAs are identified through four guide conditions taking advantage of control structure: (1) control action is not provided; (2) the UCA is provided; (3) control action is provided too late, too early or out of sequence; and (4) control action is stopped too soon or applied too long (applied only for continuous control). And Manuel et al added two UCAs (More and Less) because these two UCAs are adapted with petrochemical process, when we found the PID controllers [6].
4. Identify loss scenarios: this step is identified possible causes of UCAs causing hazards (losses). In this phase the information provided allows the engineers to change the design to eliminate or mitigate the causes of the hazards. This is the most important step of the analysis but also de most difficult one [5].

3. Case Study

In this section we study the HDPE reactor located in CP2K unit in polymed complex sonatrach-Skikda. The study consists of process description, the application of STPA method on this industrial process, in order to improve their safety and implement the obtained results in the control system in order to automated safety process [1].

3.1. Process Description

The HDPE reactor (Figure 1) is piping with length of 304 m and internal diameter of 560 mm in the form of loop, composed of four vertical sections, linked by horizontal sections. The vertical sections have Jacket insulated for heating in the phase of preparation and refrigeration in the phase of reaction. Those, made of carbon steel with external diameter 760 mm, are designed to the pressure and the temperature of 15 kg/cm²g and 142 °C respectively. The reactor can be decomposed into the four following parts:

- The reactor enclosure
- The reactor pump
- Refrigeration system

- Decantation legs.

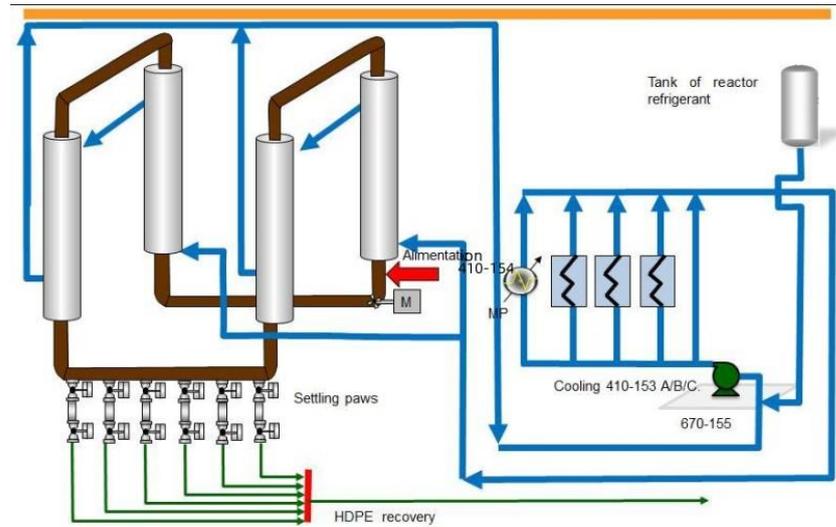


Figure 1. Polymerization process.

The reactor feed streams (ethylene, isobutane, hydrogen and 1-hexene, in the case of the production of copolymers) require a high degree of purity, for this; they are in advance treated to remove any catalyst poison (basically acetylene, oxygen, and water) until not harmful residual contents [7]. This is accomplished in suitable catalytic caterers, in the case of ethylene, degassing columns, isobutane and hexene-1, and specific dryers for all currents. The reactor is fed with the raw materials processed at the treatment area. Recycled isobutane, hydrogen, hexene-1 and ethylene arrive at the reactor through the main supply line to the reactor. Hexane and recycled isobutane are mixed in the static mixer isobutane/hexene. Hydrogen is mixed with the ethylene and it is added to the stream of recycled isobutane/hexene at the mixer output. The feed to reactor at different flows is adjusted based on certain variables. The isobutane-ethylene-polyethylene mixture flows into the reactor through the reactor pump [8].

3.2. Application of STAMP-STPA

Figure 2 shows the hierarchical control structure of polymerization plant, when we can identify the different unsafe control actions, the relation between each services and components and the nature of each information and order.

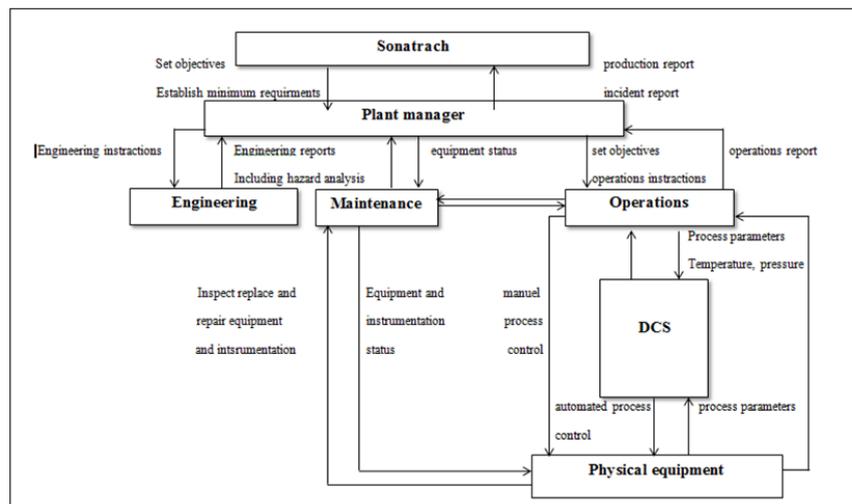


Figure 2. Hierarchical control structure of CP2K unit.

3.2.1. Hazards Identification

In our case study, we consider the variation of the temperature and pressure parameters, caused by the variation in the flow of the entering products (Ethylene, Hexene, and Isobutane), in addition the actions of cooling water valves and settling paws discharge valves. Table 1 shows the hazards identification and its constraints.

Table 1. Hazards identification.

Accident	Hazard	Safety Constraints
Explosion	H1: too high temperature H2: too high pressure	Temperature must never violate a maximum value Pressure must never violate a maximum value

3.2.2. Draw the Control Structure

In this step we draw the control structure of the HDPE reactor in order to identify all the unsafe control actions that can lead to the two hazards identified in the precedent section, which are caused the explosion (Figure 3).

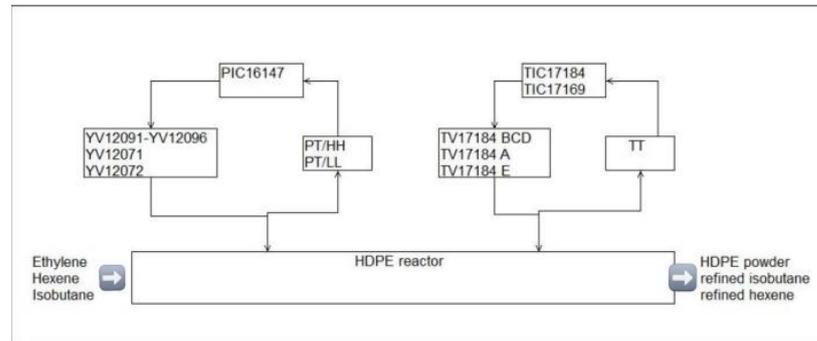


Figure 3. Control structure of HDPE reactor.

3.2.3. Identify Losse Scenarios

To determine the size of STPA table we use the following equasion:

$$STS = \prod_{i=0}^N \text{number of UCAs} \prod_{j=0}^M \text{Number of stats} \tag{1}$$

We choose (MORE (+), LESS (-), PROVIDED (1) and NOT PROVIDED (0)) as UCAs on each state. In this case, if we consider all the UCAs possible related to all states, we get:

$$STS = 4 \times 4 \times 4 \times 4 \times 4 = 4^5 = 1024 \tag{2}$$

So we get a big siize of the STPA table (Table 2) in term of rows number, in order to reduce the size of this table we consider only these UCAs: MORE, LESS, and NOT PROVIDED concerning the entering products (Ethylene and Hexane) and the cooling valve (for that it work continuously), PROVIDED (1) and NOT PROVIDED (0) concerning the flow of Isobutane and the opening of the discharging valves, in this case we get:

$$STS = 3 \times 3 \times 3 \times 2 \times 2 = 108 \tag{3}$$

From the STPA table we can see that the UCAs which lead to hazards are: more (+) concerning the entering flow of Ethylene and Hexene, and not provided (0) concerning the opening of the pressure valves (settling paws and safety valves). STPA analysis results not only in the detection of hazardous situations but also offer the technical solutions from the same table. In this case, it can be easily seen that all of those scenarios (colored green) corresponds to no hazards and the critical scenarios (colored red).

Table 2. STPA table.

ID	F _{ethylene}	F _{hexene}	Cooling Valve	F _{isobutane}	Settling Paw Valve	Hazard
1	+	+	+	0	0	H2
2	+	+	-	0	1	H1
3	+	+	0	1	0	H1, H2
4	+	-	+	1	1	No
5	+	-	-	0	0	No
6	+	-	0	0	1	H1
7	+	0	+	1	0	H2
8	+	0	-	1	1	H1
9	+	0	0	0	0	No
⋮	⋮	⋮	⋮	⋮	⋮	⋮
105	0	-	0	0	0	No
106	0	0	+	0	1	No
107	0	0	-	1	0	No
108	0	0	0	1	1	No

3.2.4. Recommendations

The recommendations have been offered to avoid the different hazardous situations are:

- Close the reactive flows when the cooling valves are not open.
- Open the pressure valves when the pressure in the reactor violate a maximum value because of the over flow of the reactives.
- Verify the timing settings concerning the opening of the discharging valves of the settling paws for that the high pressure could be easily discharged.
- Display textual messages on the HMI of DCS control room for that we ensure that the safety actions needed to be applied on the process can be easily done by any available operator in the control room in order to improve safety measures in the plant.

3.3. Implementation Results in Control System

In this stage we implement the obtained results from the STPA method into the control system to automate process safety, firstly we programme all cases in Tristation software (Triconnex PLC) (Figure 4), then we build the HDPE reactor HMI (Figure 5) into Intouch software to monitor our process and display the alarms and abnormal situations, all these operations are mad in order to help the operators to take good and safe decision.

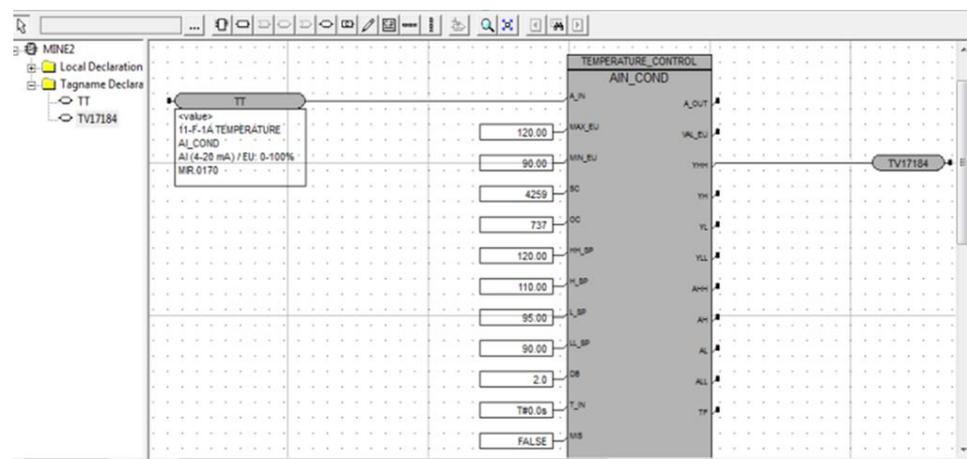


Figure 4. Temperature logic control in tristation software.

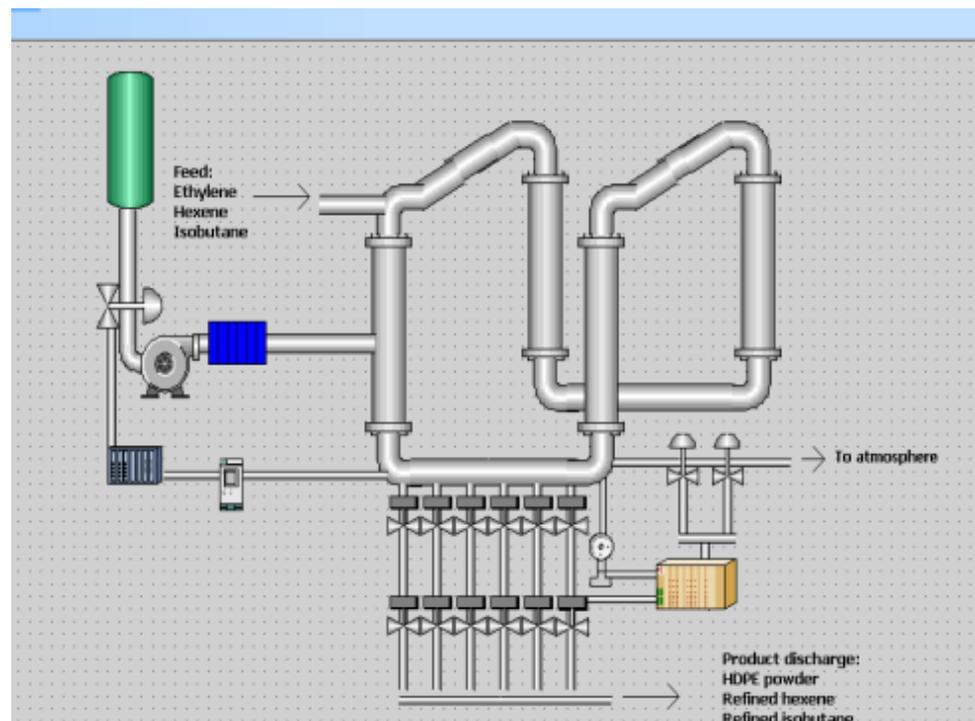


Figure 5. Build the HDPE reactor HMI.

3.4. Some Scenario Simulation

In this part we show some scenarios simulation as in Figure 6, when the temperature is increased the control system activate the cooling system to reduce the temperature. And so on in the case of high pressure or other parameters.

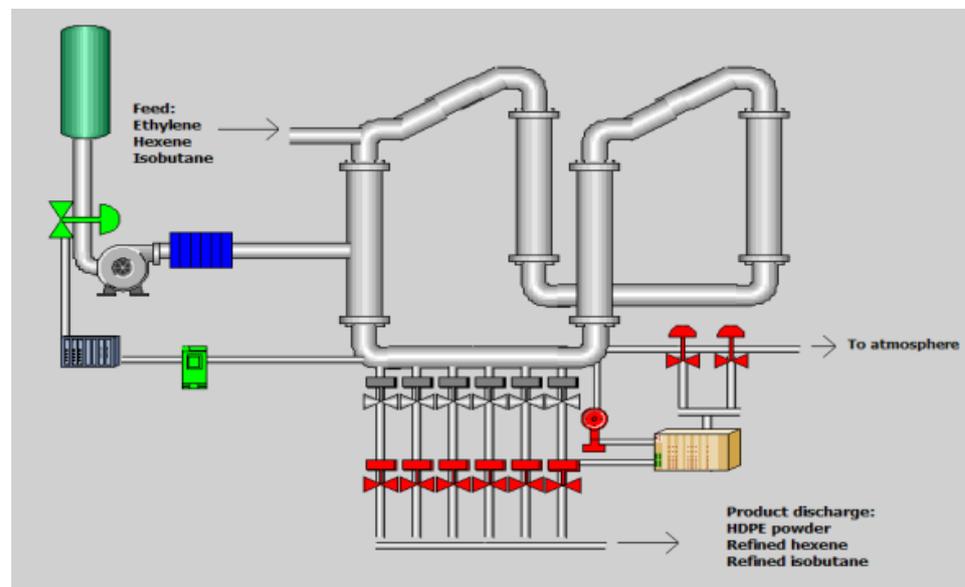


Figure 6. Scenario simulation High temperature.

4. Conclusions

In this paper, we have presented a system based theory that can deal with systemic failures when analyzing HDPE reactor. STPA has been applied to the lowest level of the HDPE plant. The methodology has been applied on the HDPE reactor showing that it can provide the same safety recommendations as other techniques (as HAZOP) but also

considering other factors out of the scope of those techniques. The case study shows how STPA could replace or at least complement HAZOP as the hazard analysis technique for chemical and oil & gas industries. The advantage of using STPA lies in its systemic nature and its application to the whole socio-technical hierarchy. Another advantage of STPA is that it can give a potential recommendations to eliminate hazards using the same analysis (the closest with less change in variables- safe scenario shown in the table). At the end we have implemented this analysis in the control system to improve safety process in term of time, cost and accuracy i.e., reduce the human errors by displaying textual messages and corrective actions.

Author Contributions: Conceptualization, M.E.-A. and B.R.; methodology, M.E.-A.; software, A.A.; validation, M.E.-A., B.R.; formal analysis, M.E.-A.; investigation, M.E.-A.; resources, A.A.; data curation, M.E.-A.; writing—original draft preparation, M.E.-A. and B.R.; writing—review and editing, M.E.-A. and Z.Y.; visualization, B.R.; supervision; project administration, M.E.-A. and B.R.; funding acquisition, M.E.-A. and B.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mechhoud, E.A.; Rouainia, M.; Rodriguez, M. A new tool for risk analysis and assessment in petrochemical plants. *Alex. Eng. J. (AEJ)* **2016**, *55*, 2919–2931. [[CrossRef](#)]
2. Leveson, N.G. *Engineering Safer World: Systems Thinking Applied to Safety*; MIT Press: Cambridge, MA, USA, 2011; ISBN 978-0-262-01662.
3. Yousefi, A.; Hernandez, M.R. A novel methodology to measure safety level of a process plant using a system theory based method (STAMP). *Process Saf. Environ. Prot.* **2020**, *136*, 296–309. [[CrossRef](#)]
4. Zhang, J.; Kim, H.; Liu, Y. Combining system-theoretic process analysis and availability assessment: A subsea case study. *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.* **2019**, *233*, 520–536.
5. Yousefi, A.; Hernandez, M.R. Using a system theory based method (STAMP) for hazard analysis in process industry. *J. Loss Prev. Process Ind.* **2019**, *61*, 305–324. [[CrossRef](#)]
6. Rodríguez, M.; Díaz, I. A systematic and integral hazards analysis technique applied to the process industry. *J. Loss Prev. Process Ind.* **2016**, *43*, 721–729. [[CrossRef](#)]
7. Mechhoud, E.A.; Rouainia, M. Automated dependability analysis of a HDPE reactor. In Proceedings of the 2014 IEEE International Carnahan Conference on Security Technology (ICCST), Rome, Italy, 13–16 October 2014; pp. 1–5.
8. Mechhoud, E.A.; Rouainia, M.; Rodriguez, M. Functional modeling of a HDPE reactor using dhigraphs for process hazard analysis. In Proceedings of the 2016 International Conference on Modelling, Identification and Control (ICMIC), Algiers, Algeria, 15–17 November 2016; pp. 1–6.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.