World Journal of Environmental Biosciences
All Rights Reserved WJES © 2014
Available Online at: www.environmentaljournals.org

Volume 6, Supplementary: 12-22

ISSN 2277- 8047

Analyzing the Effectiveness of Organizational Processes on Health, Safety and Environment Risk of the Oil Industry Operations Based STAMP Model and STPA Method
(Case Study: F&G system implementation project in the Lavan oil district)

Mohammad Kazemi speily[1], Ziaeddin Almassi[2], Mahnaz Nasrabadi[1]

[1]*Department of Environment Management (HSE), Faculty of Engineering, Zahedan Branch, Islamic Azad University, Iran.*
[2]*Department of Sustainable Development, Faculty of Environment, Karaj, Iran.*

Abstract

Background and Purposed: *Nowadays, with regard to the major industries, we are faced with this question that why, despite a comprehensive risk assessment, still many incidents occur in line with the implementation of industrial projects. The main objective of this study is to identify the causes of conventional risk assessment procedures failures in line with event controlling processes and provide a suitable test and model for risk assessment in large organizations such as oil industries.*

Analysis method: *In order to find an appropriate answer, a comparative study of conventional risk assessment methods was done in industrial projects, and by this research we can identify the reasons for these method failures. After recognizing the weakness of the existing risk assessment methods, the newly formed attitude in the accident investigation, STAMP causal logic was investigated and finally, by using the risk assessment based on this model (STPA), the case study was assessed.*
Findings*: Results of this study show that most of the conventional risk assessment methods have been built based on the Cartesian logic. According to the Cartesian logic "To fully understand a system, it should be divided into smaller components and by studying these components we can got a full knowledge of that system". This is the same logic that has been taken into consideration in the scientific safety engineering disciplines and reliability and most of the conventional risk assessment methods have emerged from this factor. However, there is another view against Cartesian logic that is called Pascal logic. According to this logic, "there are governing relations in a system that by dividing the system into smaller components these relations will be destroyed and the system cannot be identified". The same reason can be a source of industrial accidents and crises in the world today. Based on this theory, newer scientific disciplines have emerged, including safety management. Therefore, by studying and understanding one of the event logics causality, called STAMP which is based on the logic of Pascal; one risk assessment approach can be identified and used that is called STPA that the results of this assessment procedure was identifying defects and the main reasons for the accident.*
Results: *Based on the findings of this study, the main causes of accidents are: existence of authority-oriented organizational structure, importing non-standard equipment and material, old and dependent on people organizational structure.*

Keywords*: Risk Assessment, Technical and social complex systems, Safety restraints, and the hierarchical structure.*

Corresponding Author: Ziaeddin Almassi

INTRODUCTION

in this study, following the fourth generation incident models, which are known as system incident models, it is attempted to discuss the causes of gradual inefficiency of control layers in oil projects by applying a holistic and systemic view and by using public tools of system theory, such as cybernetics, control systems and dynamic of system. Based on the research hypothesis, many of the risks inherent in the system, are related to the structural defect of hierarchical control and inventory management systems within the organization. In this study, by approaching the language of safety, health and environment engineering to the organizational management and literature new vision of STAMP (System Theoretic Accident Modeling and

Process) model incident, and risk identification method presented in this model as STPA (System Theoretic Process Analysis), we try to deal with modeling and analyzing management control structures in the organizations that complexity and ambiguity is of their main characteristics.

Method

STAMP Pattern

STAMP is rooted in the theory of systems; therefore, before say anything it is necessary to note that according to this theory, there are features in the system that are caused by interactions between system components; these special features that are called emergent properties must be controlled by imposing constraints on behavior and interaction with the system components in order to kept the totality of the system under control and the system move to achieve the targets. Based on this theory, system safety and risk features are among these emergent properties, thus it should be controlled by applying suitable safety constraints in the system. According to this theory "Safety" is the challenge of "control" and the aim of control is imposing safety constraints. So from this perspective, incident is the result of inadequate control or inappropriate imposing of safety constraint in line with designing, development or operation of the system. STAMP model that is based on systems and control theory, tries to focus on the system control structure, pays attention to the safety challenge in the complex socio-technical systems. This model is based on three concepts of safety constraints, hierarchical control structure and process models based.

STAMP - as a tool for analyzing accidents - by finding those safety provisions that have been violated and determining why the controls failed to properly apply these restrictions, can identify the basic causes of accidents. On the other hand, STAMP - as a tool to analyze the system risks- Not only beyond models that focus on the deficiency of the system components, can find more reasons to the risks and probable disasters, but focus more on the Deficiency components with more accuracy and details; Because deficiency of system components is the result of safety constraints failure that will lead to the incident and STAMP is well focused on these provisions.

STAMP method for analyzing accidents and system risks acts in a way that by using general theory of system, control theory and control structure modeling **[Figure 1]** can list the main causes of accidents and provide multi-step instructions to compare what is and what ought to be, in order to be able find holes in the structure of the hierarchical control and provide suggestions for it.

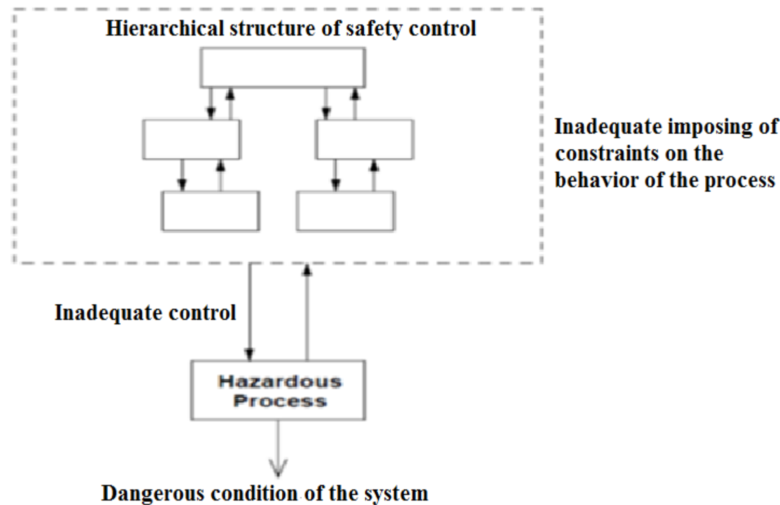


Figure 1: Example of control structure graphical model (Samadi, 2012)

STPA Risk Assessment Method

STPA can be used at each stage of the system life cycle; this technique similar to any other method of risk assessment follows a general purpose and that purpose is:

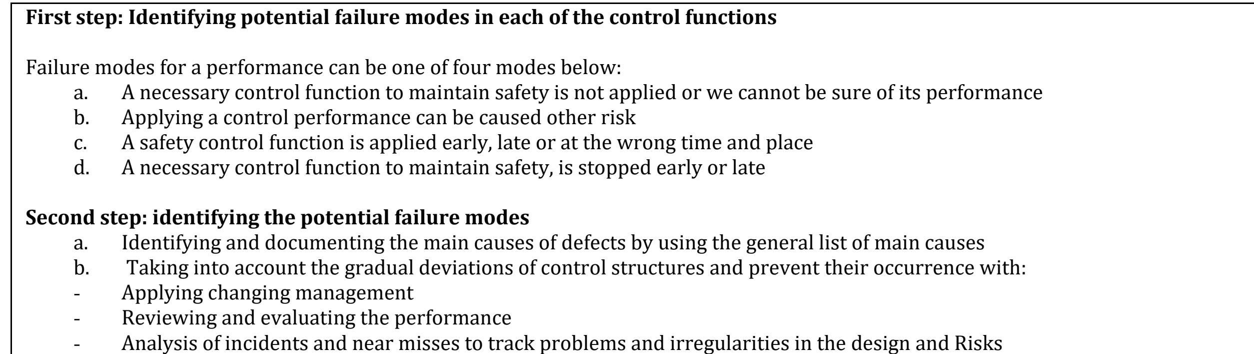
"Collecting necessary data about this issue how the safety imposed restrictions that are used to control system risks will be violated."

The data used as inputs in the STPA implementation process include:

- Operational control diagram
- System safety requirements

- System risks
- Constraints and limitations of the safety system.

STPA risk assessment method consists of two main stages and several subsidiary steps that they have been referred in **[Figure 2]**:



First step: Identifying potential failure modes in each of the control functions

Failure modes for a performance can be one of four modes below:

a. A necessary control function to maintain safety is not applied or we cannot be sure of its performance
b. Applying a control performance can be caused other risk
c. A safety control function is applied early, late or at the wrong time and place
d. A necessary control function to maintain safety, is stopped early or late

Second step: identifying the potential failure modes

a. Identifying and documenting the main causes of defects by using the general list of main causes
b. Taking into account the gradual deviations of control structures and prevent their occurrence with:

- Applying changing management
- Reviewing and evaluating the performance
- Analysis of incidents and near misses to track problems and irregularities in the design and Risks

Figure 2: STPA implementation steps

The introduction under study project

To test the model that was presented, F&G (Fire and Gas System) System Implementation Project will be studied in the operational area of Offshore Oil Company in Lavan Island of Iran. The purpose of doing F&G plan in the Lavan Island is following the international requirements and standards of security.F&G project is generally separated into three distinct parts - fire alarm, fire extinguishing and office buildings- which are located on the island in [**Table 1]**.

Table 1: Brief specifications of F&G plan

Subject of the contract	Project of completing engineering, procurement and implementation of fire safety and F&G in the Lavan district
Employer	Iranian Offshore Oil Company
Contractor	Payandan Company
Contract number	2-92-4575 F&G
Start date	2014-08-03
Finish Date	2016-02-01
Duration of contract	18 months
The initial cost of the contract	350000000000 Rials 12400000 €

The safety of this system is dependent on several components; but what will be discussed in this is study is the effect of the implementation, construction and operation of facilities and equipment on F&G system safety and reliability during operation.

Research findings:

First stage) Identifying the components of organizational control

A wide variety of control components such as the employer's corporate structure, contractor, third party consulting firms, contractors and other companies and governmental and private sector organizations such as Department of Environment, Employment and Social Affairs etc. are involved in controlling the safety system of this projects. Due to the expansion and distribution of all components involved and the enlargement of the study area, in this plan, the range of study will be limited to the Payandan corporate management layers as the contractor and Offshore Oil Company as the employer. Also important control elements of these two companies that were directly involved with system safety have been selected for limiting the scope of work.

hose organizational units that have certain duties in the control structure of organization are as follows in **[Figure 3]** :

A) The contractor's control components:
1. Engineering and project designing unit
2. Construction and project implementation unit
3. System test and failures eliminating unit
4. System launch and project delivery unit

B) The employer's control components:
5. Technical Monitoring and Project Engineering Unit
6. Repair And Maintenance Unit
7. Production Unit

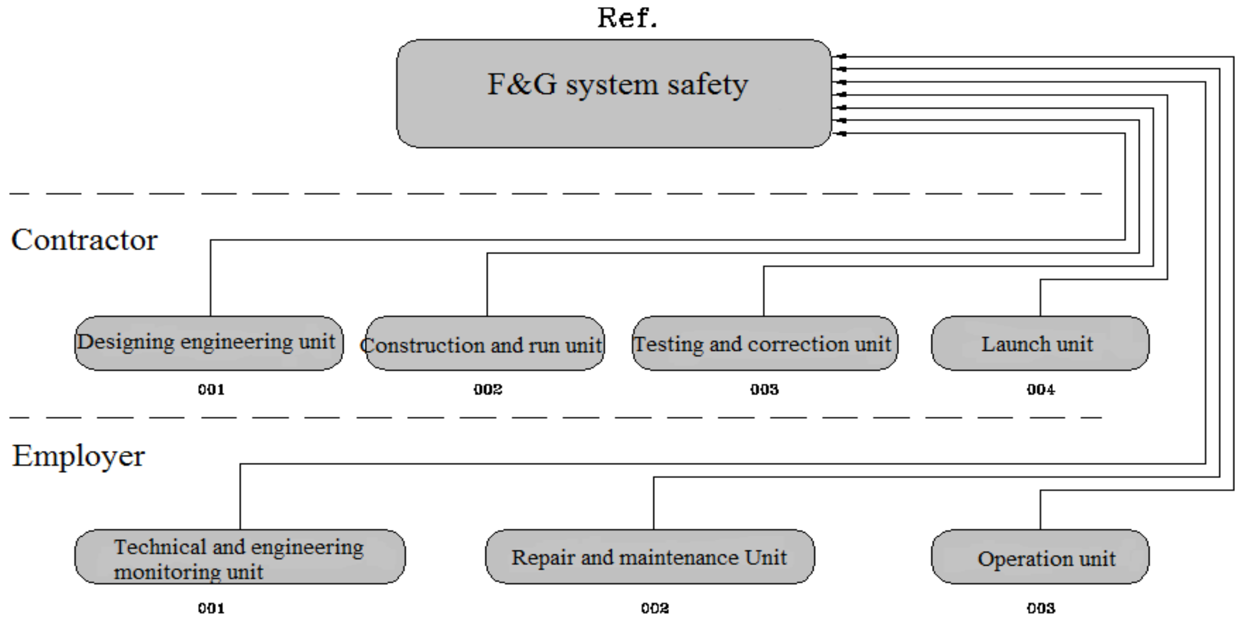


Figure 3: Components affecting the safety of F&G system,

Second Stage) identifying the functions of control components

Based on Flodiagrams depicted below, working processes of each unit and goal of every process in accordance with the number of units, are numbered and identified in the first phase in **[Figure 4 , 5 , 6 , 7 , 8 , 9 , 10]**.

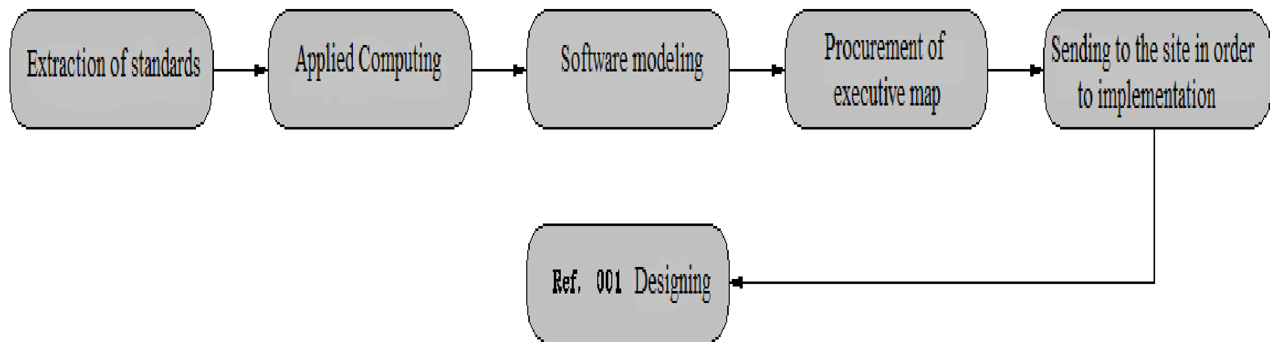


Figure 4: Diagram of executive process of contractor's designing and engineering unit

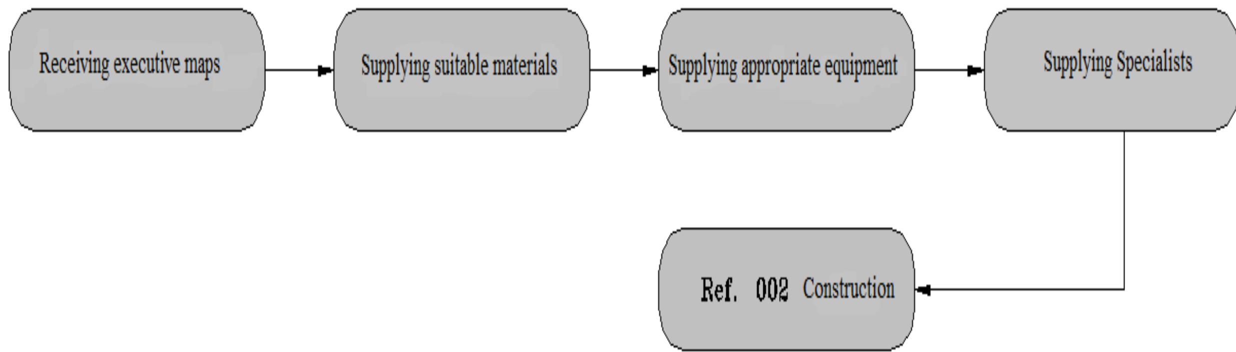


Figure 5: Executive process diagram of contractor's execution unit

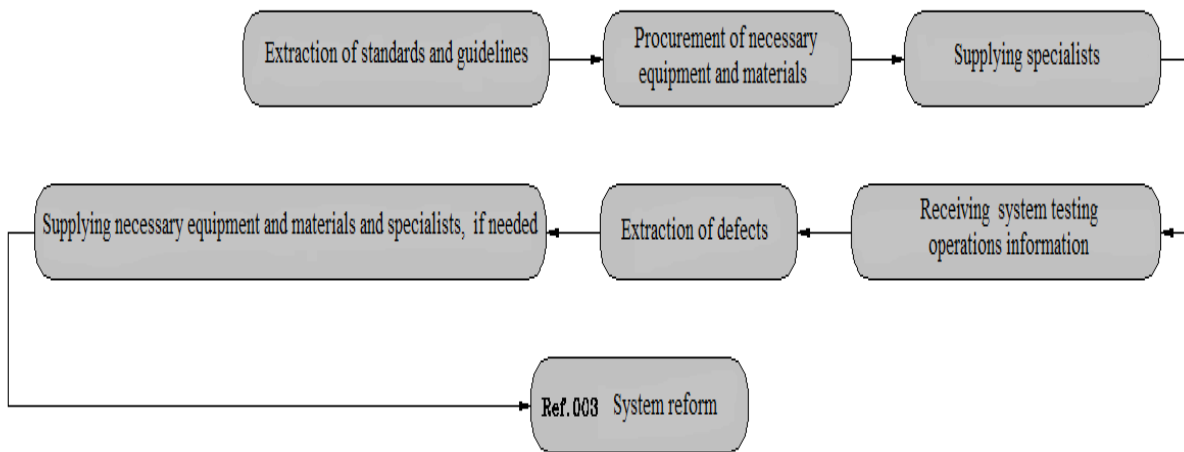


Figure 6: Executive process diagram of contractor's testing Unit

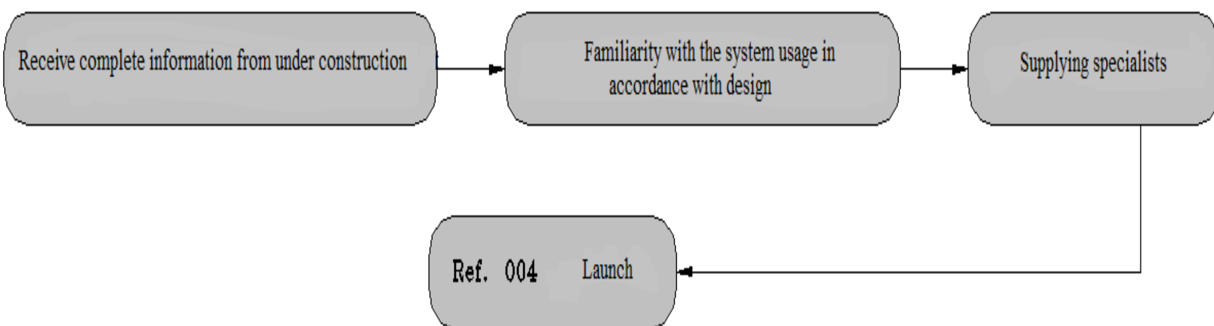


Figure 7: Executive process diagram of contractor's Launch Unit

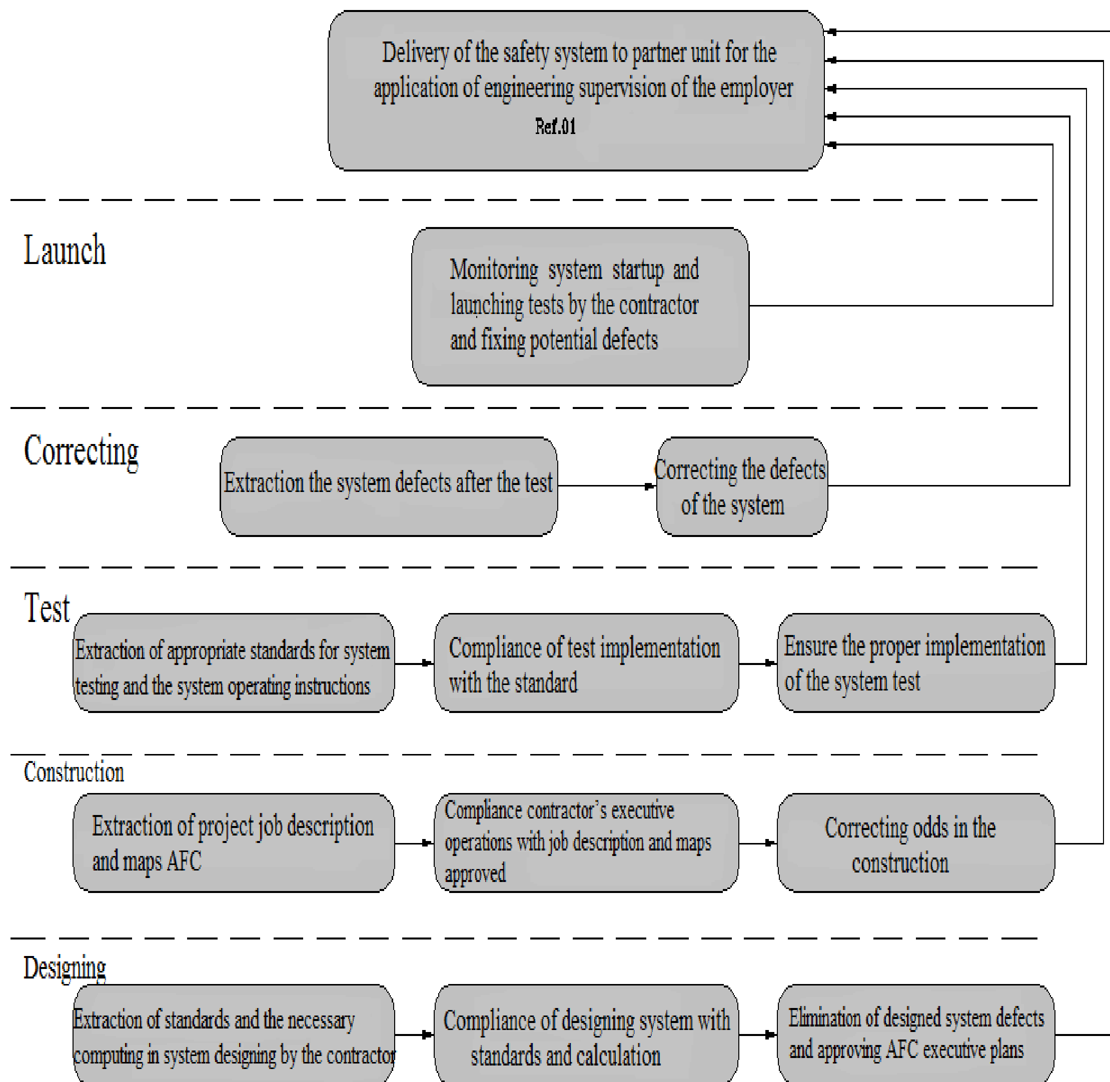


Figure 8: Executive process diagram of employer's engineering supervision unit

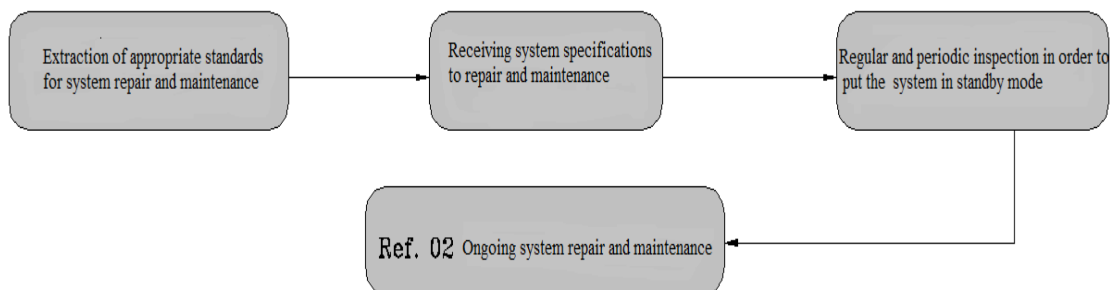


Figure 9: Executive process diagram of employer's repair and maintenance unit

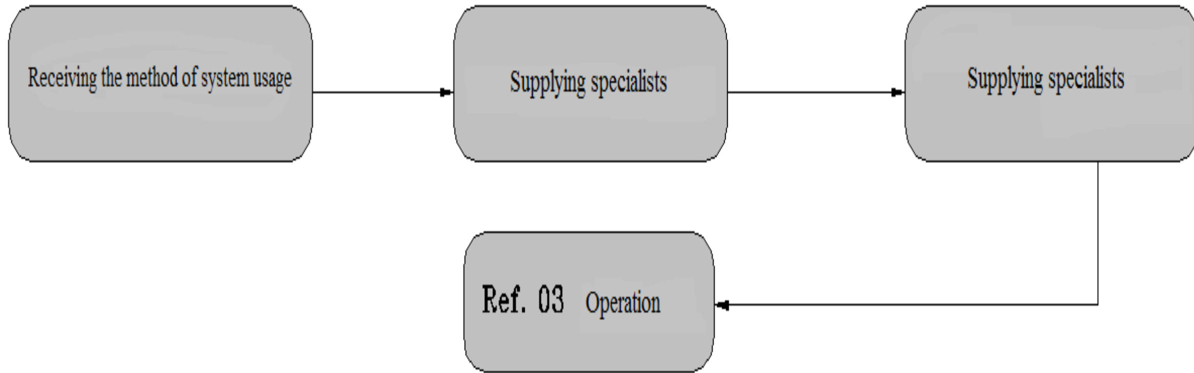


Figure 10: executive process diagram of employer's operation Unit

The third phase) determining the communication channel and relationships between system components

In this stage to pinpoint what occurs in different layers of the system, order of business processes and relationships between functional components in the implementation, construction and commissioning process, were extracted through studying the documented resources and interviews with experts in [**Table 2**].

Table 2: F&G Project Communication channels

Row	From **unit** to **unit**	Communication channel	Communication time
1	001 to 002	Presenting approved plans and technical maps for execution	Immediate
2	001 to 01	Presenting technical plans and maps for AFC approval	Immediate
3	01 to 001	Delivery of approved designs and technical maps	About 7 days
4	002 to 01	Presenting description of the work (methods, materials and equipment) for the implementation of regional plans in accordance with operating conditions	About 10 days
5	01 to 002	Correspondence of job description with the standard and operating conditions of approval and permission to carry out construction operations (issuance of Permit)	About 10 days
6	01 to 003	Presenting job description of test operation and reform system	About 10 days
7	01 to 003	Correspondence of job description with the standard and operating conditions of approval and permission to carry out construction operations (issuance of Permit)	About 10 days
8	01 to 004	Providing method of system startup operation	About 10 days

9	01 to 004	Job description correspondence with the standard and operating conditions of approval and permission to carry out construction operations (issuance of Permit)	About 10 days
10	01 to 02	System delivery training and providing technical documents of the project to the Repair And Maintenance Unit	30 days
11	01 to 03	System delivery training and providing technical documents of the project to the Repair And Maintenance Unit	30days
12	02 to 03	Delivery of sound and ready to work system in order to operation	Immediate

The fourth stage) system targets, the scenario of accident, risks and safety related constraints

the purpose of the studied system is construction and installation of F & G system in order to be ready to work, fire prevention and control in the oil and gas operations district of Lavan.Possible accident scenarios with the letter A, the high level risks with the letter H and safety constraints imposed on the system by the letter C are listed in the [**Table 3]**. It is noteworthy that in this study only the first scenario that is shown with A_1 will be examined.

Table 3: Incident scenarios, the high-level risks and system constraints

A1: Thunder and fire incidence in a one-million barrels oil reservoir and F&G system malfunction
H1: Delivery of system that has problem to the beneficiary by contractor
C1: Full compliance of F & G system construction and lunching operations with valid work methods
H2: Using defective equipment in the F&G system
C2: Compliance of the operating equipment status with the latest technical requirements

It should be noted that due to limitations in the existing plan scenario one was just checked out.

The fifth stage) control feedback loop and outlining the PML (Process Model Log) process model

In the final step, PML evaluation procedure [**Table 4]** was prepared based on STAMP model and organizational mapped Flodiagrams information and communication channels [**Tables 4 , 5]**, and by offering to experts in each of the control units, it was revised several times. Finally, what is shown in the following [**Tables 4 , 5]** is provided as final diagram of the F&G safety control system structure.

Table 4: PML process model for the purpose of C1safety control

Row	control layers	Control objectives and safety constraints	Under the control variable	Data and control feedbacks	Means of control exercising	Potential detected errors
1	001 Contractor's engineering and designing unit	C1	Compliance of operational maps with existing standards and guidelines	Related international and regional standards and guidelines, rules and regulations	Maps and duty description	Error in pipeline design and lack of appropriate extinguishers in the roof of reservoir
2	002 Contractor's manufacturing and implementation unit	C1	Compliance of operational maps with existing standards and guidelines	Related international and regional standards and guidelines, rules and regulations, AFC maps	Requesting a work construction operations permit	Improper pipeline execution and non-compliance of pipe size of with designed maps
3	003 Contractor's testing and system modification unit	C1	Compliance of operational maps with existing standards and guidelines	Related international and regional standards and guidelines, rules and regulations, system technical and operational documents	Requesting permission for testing procedure	Using inappropriate test pressure with system operating pressure

4	004 Contractor's launching Unit	C1	Compliance of operational maps with existing standards and guidelines	Related international and regional standards and guidelines, rules and regulations, system technical and operational documents	Requesting permission for launching procedure	Not enough time in the initial system launch
5	01 Employer's Technical and engineering supervision Unit	C1	Compliance of operational maps with standards and existing guidelines	Related international and regional standards and guidelines, rules and regulations, AFC maps	Permit	Issuing permit for Improper pipeline operation and lack of stopping and reforming the operation
6	02 Employer's repair and maintenance unit	C1	Compliance of operational maps with existing standards and guidelines	Related international and regional standards and guidelines, rules and regulations, system technical and operational documents	Operational Checklists	Lack of checking critical system components such as connecting pipelines
7	03 Employer's Operation Unit	C1	Full compliance of operation with the working methods valid	Related international and regional standards and guidelines, rules and regulations, system technical and operational documents	The periodic use of system and failure reports	The misuse of the system due to the lack of operator's familiarity

Table 5: PML process model for the purpose of C2safety control

Row	Control layers	Control objectives and safety constraints	Under the control variable	Data and control feedbacks	Means of control exercising	Potential detected errors
1	001 Contractor's engineering unit and design	C1	Operational maps compliance with existing standards and guidelines	Related standards and guidelines, technical specifications of equipment	Commercial and technical documents duty description	Error in equipment design and dysfunction of pumps
2	002 Contractor's manufacturing and implementation unit	C1	Compliance of operational maps with existing standards and guidelines	Technical Specifications of equipment	Requesting permission to buy equipment	Poor implementation of equipment and pumps destruction
3	003 Contractor's testing and system modification unit	C1	Compliance of operational maps with existing standards and guidelines	Technical Specifications of equipment	requesting permission for equipment testing	using disproportionate Pressure test to the system operating pressure
4	004 Contractor's launching unit	C1	Launch operations compliance with approved maps and available standards and guidelines	Technical Specifications of equipment	Request permission for equipment installation	Not enough time in the initial system launch

5	01 Employer's technical and engineering supervision unit	C1	Compliance of duty regulations, executive operations, testing and commissioning of with approved plans, available standards and guidelines	Related standards and guidelines, technical specifications of equipment	Issuing purchase permission	Issuing inferior equipment purchase permission
6	02 Employer's Repair And Maintenance Unit	C1	Compliance of service operation and maintenance with existing standards and guidelines	Technical Specifications of equipment	Equipment monitoring checklists	Lack of checking critical components of equipment
7	03 Employer's operation unit	C1	Full Compliance of operation practices with valid working methods	Technical Specifications of equipment	The periodic use of the equipment and shortcomings report	The misuse of the system due to the lack of operator's familiarity

Discussion and conclusion

After performing the STPA risk assessment procedure in the case study it was identified that this method is very comprehensive requires an extensive research team in all scientific trends and also this method requires open and unambiguous space and availability of all resources, facilities, records, managerial layers of decision-making and clear communication channels and in the security and information agencies which have hidden technologies; due to the unavailability of information its implementation would be extremely difficult and also in the structures that has a so-called behind the scenes and undetectable management will have major flaw.

Identified defects in this structure that are of the main causes of industrial accidents in the country are as follows:

1. Authoritarian organizational structure rather than consultative organizational structure
2. Importing non-standard material and equipment due to the country's macro-management issues
3. Old and dependent on the person organizational structure and the lack of a systematic structure
4. direct entry of non-specialized agencies and agents to the plans and projects
5. The lack of stable management in the control layers and continuous changing in the organizational structures

Based on the obtained results, the main cause of many risks of industry safety, health and environment in the hierarchical structure and management systems and the research hypothesis is confirmed.

References

1) Andersen S, 2012, Risk analysis and risk management approaches applied to the petroleum industry and their applicability to IO concepts.
2) Dulac N, 2007, A Framework for Dynamic Safety and Risk Management Modeling in Complex Engineering Systems, Ph.D. dissertation, Dept. of Astronautics Eng, MIT.
3) Hollnagel E, 2010, Safer complex Industrial Environment. United States: Taylor & Francis Group.
4) Khanzode V, 2012, Occupational injury and accident research: A comprehensive review. Safety Science
5) Khawaji IA, 2012, Developing System-Based Leading Indicators for Proactive Risk Management in the Chemical Processing Industry. MSc dissertation. MIT.
6) Leveson N. G. 2011, ENGINEERING A SAFER WORLD: Systems Thinking Applied to Safety. United States: MIT Press.
7) Mohaghegh Z, 2009, Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: A hybrid technique formalization. Reliability Engineering and System Safety.
8) Roberts K. H. 1990, Managing high reliability organizations. California Management Review.
9) Samadi J. 2012, Development of a Systemic Risk Management Approach for CO2 Capture, Transport and Storage Projects. Ph.D. dissertation, Centre for Research on Risk and Crises, MINES ParisTech.
10) Snowden D. 2002 , Complex acts of knowing: paradox and descriptive self-awareness. Journal of Knowledge Management.
11) Schonbeck M ,2010, Human and organizational factor in the operational phase of safety instrumented system: Anew approach. Safety Science
12) Stringfllow M.V. 2010, Accident analysis and hazard analysis for human Factors. Ph.D. dissertation, Department of aeronautical and engineering, MIT.
13) Teng B. 2010, Assessing Risk and prevent Accident in Complex system, Norwegian university of science and technology.
14) Vatn J. 2010, assess risk related to system characteristics relevant . SINTEF report.