Comparative Study of STPA and Bowtie Methods: Case of Hazard Identification for Pipeline Transportation

Article *in* Journal of Failure Analysis and Prevention · October 2020

DOI: 10.1007/s11668-020-01010-9

CITATIONS
0

READS
277

1 author:

Wafia Benhamlaoui
Université Batna 2
5 PUBLICATIONS **0** CITATIONS

SEE PROFILE

J Fail. Anal. and Preven.
https://doi.org/10.1007/s11668-020-01010-9

TECHNICAL ARTICLE—PEER-REVIEWED

Comparative Study of STPA and Bowtie Methods: Case of Hazard Identification for Pipeline Transportation

Wafia Benhamlaoui · Mounira Rouainia · Yiliu Liu · Mohammed Salah Medjram

Submitted: 11 February 2020 / in revised form: 4 August 2020 / Accepted: 12 September 2020

Abstract In this research, two methods, the STPA and Bowtie, were applied to realize a hazard identification on pipeline transportation, more precisely a condensate pipeline, in SKIKDA region. This identification was followed by a comparison of the results obtained previously, with respect to some aspects; we compared all hazards identified by both methods and classified them into categories, also comparing consequences and losses; we also compared the different steps of each method used. The study performed allows us to determine the main differences using the STPA and Bowtie methods for hazard identification on pipeline transport and highlights a complementary while using them in order to identify in a more exhaustive way the hazards associated with the system being studied. Their combination may be more useful for a thorough hazard identification.

Keywords Hazard identification · STPA · Bowtie · Hazardous materials · Pipeline transportation

W. Benhamlaoui (✉) · M. Rouainia · Mohammed SalahMedjram
LGCES – Research Laboratory, Department of Petrochemistry and Process Engineering, University of 20 août 1955, Skikda, Algeria
e-mail: w.benhamlaoui@univ-skikda.dz; rofirof@me.com

M. Rouainia
e-mail: rouainia_m@yahoo.fr

Mohammed Salah Medjram
e-mail: medjram_ms@yahoo.fr

Y. Liu
Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology (NTNU), Trondheim, Norway
e-mail: yiliu.liu@ntnu.no

Introduction

The hazardous materials transportation, whether in a long or short distances mode, has several consequences, such as trucks/pipelines passage accidents in an urban area, pipeline leaks due to impacts and dig-ins, etc. These consequences affect people life safety, the environment and facilities.

Pipeline transportation includes a system of pipes with different diameters, which are used to move continuously and sequentially fluids, hydrocarbons (oil pipelines) or liquefied gases (gas pipelines), certain chemical products as ethylene, propylene, etc., under the appropriate pressure according to Safadi [1] works. In Bersani et al. [2] work's, the pipeline is considered a complex system, dispersed geographically over a wide area, requiring many technologies to support the identification, of high potential risks.

Several accidents were previously identified in gas and oil pipeline industry according to US Department of Transportation (DOT) Office of Pipeline Safety, in 1991 and CONCAWE 1996. Their causes are frequently classified into five categories:

- Damage caused by external operations in the pipeline vicinity and not related to its management;
- Corrosion, when pipeline is subjected to two types of corrosion: the first one is an inside corrosion, derived from water or other substances transported with hydrocarbons (viscosity and temperature are crucial information for the accident analysis) and the other is an outside corrosion related to the pipe coating and cathodic protection;
- Mechanical failures, which are fractures or cracks;

Published online: 09 October 2020

- Operational error, presented by excessive pressures or system malfunction;
- Natural events such as landslides, floods, erosion, subsidence, earthquakes, frost or lightning.

These causes can be identified using many types of risk analysis methods. In the context of hazardous materials transportation, some identified risks methods depend on the transportation mode used, the nature of the transported product and its physical/chemical properties, external activity (works near a pipe, state of the roadway, etc.) and weather conditions.

In our study, we proceed to compare between the STPA and the BOWTIE methods in order to identify pipeline hazardous materials transportation. We applied these two methods on a condensate pipeline system in the Arrival Terminal of Skikda, where the control and safety system for the entire pipeline are located.

Literature Review

Shahriar et al [3] conducted a sustainability assessment study using fuzzy-based Bowtie analysis in oil and gas pipelines, for deriving fuzzy probabilities of basic events in fault tree and estimate fuzzy probabilities of output event consequences. Han and Weng [4] have realized a comparison study on qualitative and quantitative risk methods for urban natural gas pipeline network, where the qualitative methods are selected according to several indexes (selection, classification, risk index, consequence index, etc.). The quantitative methods consist of probabilities assessment, consequence analysis and risk evaluation.

The Jo and Ahn [5] study takes into account pipeline transport and considers a model that intends to reduce the level of risk, as a key variable that should be exploited in the planning and building stages of a new pipeline. It does not only emphasize the importance of individual risk but also the social risk due to cumulative fatal length and failure rate. The dataset used in their study is based on data of European levels.

In Vianello and Maschio [6] study, they realized a quantitative risk assessment of the Italian gas distribution network. The main aim of this work is to analyze and assess the risk of the Italian high-pressure natural gas distribution network, and explain the methodology for quantitative risk assessment. Pontiggia and Al [7] conduct another research related to risk assessment of buried natural gas pipelines, where they focus on a novel Event Tree network and draw their conclusions about the effective application of the framework within risk assessment and related uncertainties in pipeline accident modeling.

On the other hand, the STPA method is a new hazard analysis method based on system theory rather than reliability theory [8]; in the field of risk assessment and risk analysis, the STPA method is used pretty much times. In some works, it was used as a qualitative risk analysis method and in the comparative studies.

Some of Leveson works [9] used the comparison study of STPA and APP4761 (a wheel brakes system) in aircraft, for providing evidence to support the hypothesis that it has a new accident causality model, where this latter are caused by component failures, system design (including software).

While in the work of J. Zhang et al. [10], the STPA approach is combined with availability assessment, the focus of this research is to place an interface between STPA and RAM analysis, where they proposed an approach named STPA-RAM. Others used the STPA to analyze and evaluate the feasibility hazard using it in process industry applications; they also conducted it in comparative study with HAZOP analysis to determine whether the STPA cam replace traditional HAZOP or not.

Sulaman et al. [11] applied STPA on a socio-technical system that has three controllers, which includes the system components because they contain some process models. The controller receives the inputs of all system components, such as sensors and actuators, and then, it carries out the internal calculations to produce the appropriate command. Also in 2017, Sulaman et al. [12] have realized a comparative study between the STPA method and FMEA, using case study research methodology, to compare the effectiveness of the methods and investigate the main differences between them.

Other works show the limitations and improvements of the STPA in safety and security; Schmittner et al. [13] have applied STPA-security using real cases for joint safety and security analysis, a battery management system for a hybrid vehicle, where they found several limitations of security extension, which motivated them to propose some improvements for addressing these limitations in safety and security analysis. Their improvements lead to a better identification of high-level security scenarios.

Our objective in this context is to compare the hazards analysis of natural gas pipeline transportations using STPA and Bowtie method, because the STPA includes in its analysis software and human operators, which is considered as an important part in several risk analysis procedures. However, the Bowtie method consists in the combination of causes using the fault tree analysis, and a tree of events to determine dangerous phenomena and their

consequences. These two analyses are achieved around a feared central event (which is the loss of containment).

To meet this objective, we:

- Identify all hazards using both methods and classify them into categories;
- Proceed to a the comparison of those hazards; investigate the effectiveness of both methods;
- Show the main differences between the risk assessment methodologies of each method;
- Focus on the importance of these methods complementarity, to have an exhaustive qualitative risk assessment.

Description of Pipeline Hazardous Materials Transportation in Skikda Region

Sonatrach—RTE (Eastern Transport Region)—manages pipeline transport in Skikda region. It transports crude oil, condensate and natural gas, respectively, from Haoud El Hamra and Hassi R'Mel and transports them to the oil and gas pipeline terminal in Skikda [14]; Fig. 1 shows the different pipes in the eastern region of the country.

Table 1 summarizes the different types of pipelines, the materials transported, as well as certain characteristics of the pipelines:

Fig. 1 Hydrocarbon transportation network map [15]

Table 1 Materials transported by the RTE-Skikda

Name of the pipe	Length (KM)	Length in Skikda (km)	Type of product transported	Characteristics
Pipeline NK1	645.5	40.880	Condensate	Start-up year: 2009 - Main line NK1 30″ - Place of departure: Haoud El Hamra - Arrival point: Skikda land terminal - Diameter: 30″ - Theoretical transport capacity: 11.4 million tons/year - Actual current transport capacity: 11.4 million tones/year
Pipeline OK1	645	109	Crude oil	- Date of entry into production (Date first loaded): 27 April 1972 - Main line OK.1 34″. - Place of departure: Haoud El Hamra - Arrival point: Skikda land terminal • Diameter: 34″ • Theoretical transport capacity: 30 million tons/year - Actual Transport Capacity: 30 million tons/year
GK1 40″	574.87	41	Natural gas	Date of commissioning: March 1971 - Departure point: CNDG Hassi R'mel - Arrival point: Arrival terminal Skikda - Diameter: 40″
GK2 42″	575,545	40.879	Natural gas	- Commissioning year: December 2001 - Departure point: CNDG Hassi R'mel - Arrival point: Arrival terminal Skikda - Diameter: 42″ - Theoretical capacity: In compression: 14.2 × 109 CM^3/year □ Free flowing: 7.2 × 109 CM^3/year - Actual capacity: In compression: 14.2 * 109 CM^3/year □ Free flowing: 7.2 * 109 CM^3/year
GK3 48″	785	55.198	Natural gas	- Start of construction year: 2010 - Year of production: 2012 - Place of departure: CNDG Hassi R'mel wilaya de Laghouat - Place of arrival: TASO Skikda (Terminal Skikda) and TA-KO El Kala (Arrival Terminal El Kala) - Diameter: 48″ - Theoretical Capacity: Free Flow: 8.34 × 109 CM^3/year - Actual production capacity/Product: Free flowing: 8.34 × 109 CM^3/an

Background

Presentation of the STPA Method

STPA (system-theoretic process analysis) is a hazard analysis based on an extended model of accident causation. It supposes that accidents can also be caused by unsafe interactions of system components [16]. Some of the advantages of STPA over traditional techniques hazard/risk analysis are:

- Very complex systems can be analyzed. "Unknown unknowns" that were previously only found in operations can be identified early in the development process and either eliminated or mitigated. Both intended and unintended functionality are handled;
- It can be started in early concept analysis to assist identifying safety requirements and constraints. These constraints can be used to design safety (and security) into the system architecture and design, eliminating the involved costly rework when design flaws are identified in development or during operations;
- It includes software and human operators in the analysis, ensuring that the hazard analysis contains all potential causal factors in losses;

- It provides documentation of functionality system that is often missing or difficult to find in large, complex systems;
- It can be easily integrated into your system engineering process and into model-based system engineering.

The steps in basic STPA are shown in Fig. 2 with a graphical representation:

- *In the first step,* it is necessary to define the purpose of the analysis. What kinds of losses will the analysis aims to prevent? What is the analyzed system and what is the boundary system?
- *The second step* is to build a model of the system called a control structure. A control structure captures functional relationships and interactions by modeling the system as a set of feedback control loops.
- *The third step* is to analyze control actions in the control structure to examine how they could lead to the losses defined in the first step. These unsafe control actions are used to create functional requirements and constraints of system.
- *The fourth step* identifies the reasons why unsafe control might occur in the system. Scenarios are created to explain:
- How incorrect feedback, inadequate requirements, design errors, component failures, and other factors could cause unsafe control actions and ultimately lead to losses;
- How safe control actions might be provided but not followed or executed properly, leading to a loss.

Presentation of the Bowtie Method

The BOWTIE method was commonly used in nuclear safety studies; today, its use extends even into the industry sector. The ARAMIS research program puts the advantages of this method, which aims to identify and quantify major accident phenomena and represents them in the form of a bowtie.

The principle of this method is to put together a fault tree and a tree of events around a feared central event.

- The cause tree: allows an analysis of the combinations of causes;
- The event tree: allows the determination of dangerous phenomena and their consequences;
- The feared central event: it is an event resulting from the drifts of operating parameters or element failures, which can have many consequences on human life, environment and facilities. This central event is generally designated by a loss of containment.

The main interest of this method is to allow the visualization of all paths leading to feared events, where each path represents an accident scenario. It can be used for:

- A qualitative risk analysis.
- A quantitative risk analysis.

In our study, we opted for a qualitative risk analysis to determine the loss causes of containment in a condensate pipeline, as well as their possible consequences.

Case Study

Our study concerns the hazards identification of a condensate pipe, its starting point is HAOUD EL HAMRA, and the arrival point is the arrived terminal Skikda, over a distance of 645.5 KM [17]. Figure 3 shows the different pipes in the Skikda region. Figure 4 represents a brief schematization of the studied system "a condensate pipeline transportation".

Results

Through our study, we applied the STPA and BOWTIE methods on a condensate pipe to identify all the hazards and accident scenarios; the result is summarized in 2 parts: Part A (6.1.) related to the STPA hazard analysis and Part B (6.2.) related to the Bowtie hazard analysis.

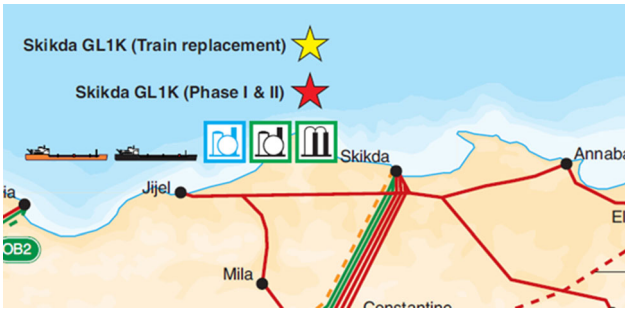

Fig. 3 Hydrocarbon transportation network in the Skikda region [15]

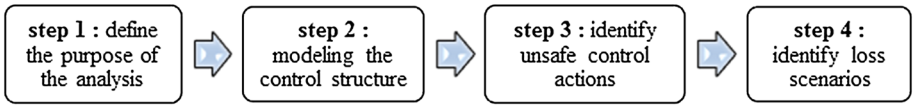

Fig. 2 The STPA steps diagram [16]

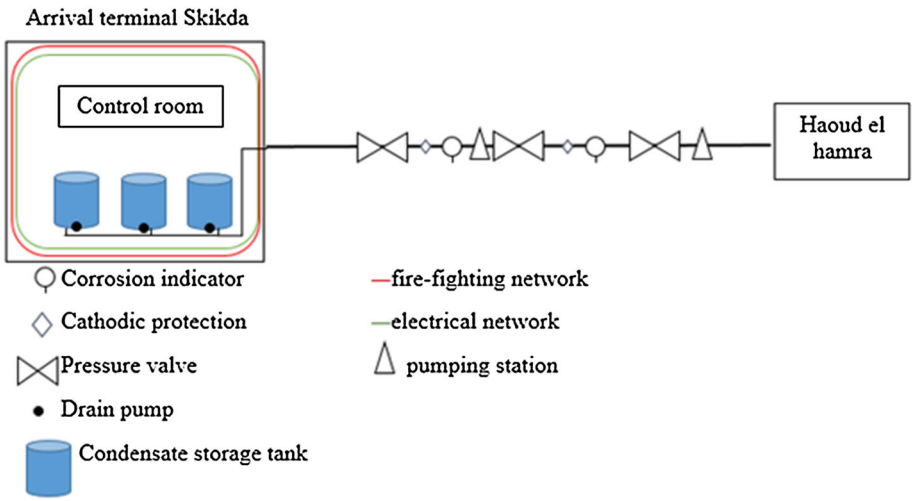

Fig. 4 Description condensate pipeline system

Hazard Identification Using STPA Method

The hazard identification based on the STPA method was employed in 4 steps; the results are summarized below:

Step 1: Define the purpose of the analysis

Identification of losses:

L-1: Loss of transportation (mission).
L-2: Loss of material being transported.
L-3: Loss of the pipe.
L-4: Environmental loss.
L-5: Loss of life.

Identification of system-level hazards:

H1: Impact/shocks due to external activities nearly to the pipeline [L1–L5].
H2: Mechanical failure of the pipe L1/L2/L3/L4.
H3: Pipe corrosion L1/L2/L3/L4.
H4: Overpressure in the pipe L2/L3/L3.
H5: Operating errors: maintenance operations L1–L5.
H6: Failure of the control system in the control room L1/L2/L3/L4.
H7: Overfilling tank in arrival station L2/L4.
H8: Electrical issues in the arrival station L2/L4/L5.
H9: Fire in facilities of the arrival terminal L4/L5.

Defining system-level constraints:

SC-1 places of the pipeline should be always marked H1.
SC-2 regular inspection of the state of the pipe should be presented H2/H3.
SC-3 the level of corrosion must be detected by periodic checks H3.
SC-4 constant pressure level must be maintained H4.
SC-5 the safety procedures must be followed during a maintenance operation H5.
SC-6 have a redundancy system in the case of control system which shows a failure H6.
SC-7 supervision of operators in the control room H7.
SC-8 level detector must be always in good working order H7.
SC-9 periodic inspection of the electrical network H8.
SC-10 fire/gas detectors must always be in good working order H9.

Step 2: Modeling the control structure

Figure 5 represents the modeling of control structure of our system, followed by explanations of the arrows shown in Fig. 5 that represent feedback/information:

a1: Alarm/signals/states of physical parameters information.
a2: manual safety control.
b1: Launch Cathodic protection.
b2: Physical parameters related to level of corrosion.
c1: Open/close the pressure valve.
c2: Flow/pressure flow.
d1: Trigger the fire prevention network.
d2: Level of the water in the water storage tank.
e1: Controlling the different safety action in all stations (ESD).
e2: Start the drain pump.
f1: State of level of condensate in the tank.
f2: The data of physical parameters/safety controls of the different stations.
g1: Shut down the system in case of major accident.
g2: Security management in the arrival terminal.
h1: Activation of automatic security systems.

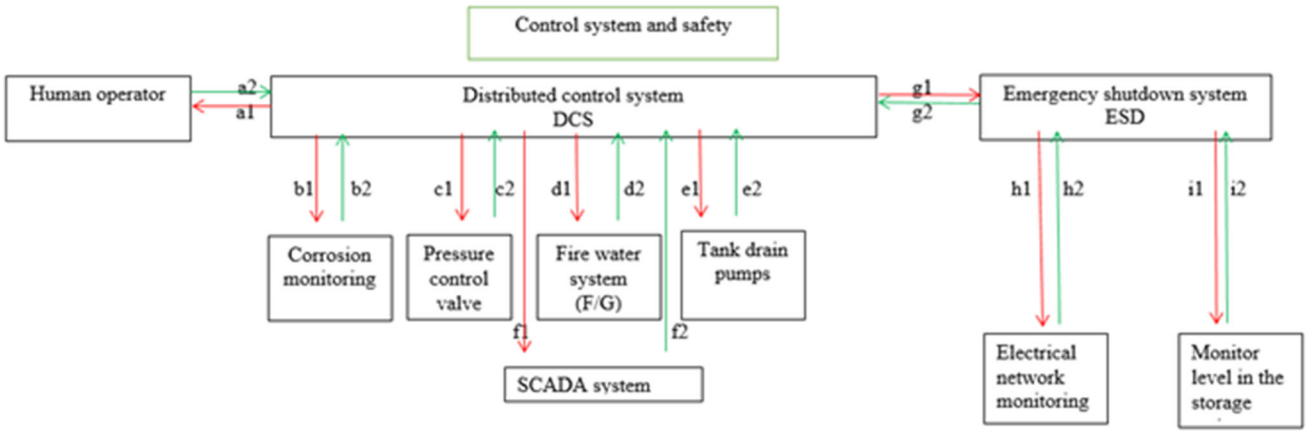

Fig. 5 The control structure

h2: State of electrical network.
i1: Opening / closing of the inlet valve of the arrival terminal (if HL).
i2: Level of the condensate in the tank.

Step 3: Identify Unsafe Control Actions

Table 2 summarizes the step's 3 results, all unsafe control actions identified and their hazards. Table 3 is about controller constraints, which are related to the unsafe control actions.

Step 4: Identify loss scenarios

Table 4 recaps all scenarios of the unsafe control actions identified previously in step 3.

Hazard Identification Using BOWTIE

The hazard identifications using the BOWTIE method, allowed us to find all the possible causes to the central feared event (loss of containment), and all the consequences that can occur.

Table 5 is related to critical feared events options that can be found in a pipeline risk assessment:

According to the QRA [18], we note that the selected risk event is 'breakage of a pipe: loss of containment.' The following step applies the Bowtie Method on this feared event; the interest in this step is to allow the visualization of all paths, going from basic events to damages. Figure 6 shows the results of Bowtie method application in our system.

Methods Performances Analysis and Results Comparison

This section presents the analysis of the results that encompasses the main comparison results of both methods, STPA and BOWTIE.

Table 6 summarizes the identified hazards by STPA and BOWTIE:

- From Table 6, we can notice that the hazards identified are the common hazards identified by both methods;
- The hazards identified by the Bowtie methods are only related the pipeline;
- The hazards identified by the STPA methods are related to the pipeline and safety control system (control room);
- The STPA method identifies the dangers both upstream and downstream.

Table 7 shows the all hazards identified by both methods by appearance order; we notice that there are four hazards not identified in each method, and nine common hazards.

The hazards that are not identified by the STPA method are related to:

- External events: evilness, natural events, impacts/shocks;
- Internal events correspond to the pipe physical state.

The hazards that are not identified by the BOWTIE method are mainly linked to:

- Software for control, electrical systems and fire in the arrival station.

Classification of possible causes

From Table 8 that shows the classification of all risks identified by both methods, we can notice that the type "physical components error" has the highest number of the hazards with both methods. We note also that BOWTIE method has not any hazards related to system error unlike the STPA method, which has identified 3 hazards.

Table 2 Unsafe control actions

Control action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Manual safety control by the operator	UCA1—Operator does not make the correct actions to activate safety controls **H4** UCA4—The operator does not activate all safety controls **H4**	Operator makes the correct action to activate safety controls	UCA 2—Operator activates the safety controls too late **H4**	UCA 3—Operator stops the safety controls too soon **H4**
Launching cathodic protection	UCA5—DCS does not start the cathodic protection **H2 H3**	Dcs starts the cathodic protection	UCA6—Dcs starts the cathodic protection too late **H2 H3**	UCA7—Dcs starts the cathodic protection too soon **H3**
Open/close the pressure control valve	Dcs does not close the pressure valve	UCA8—Dcs orders to close the pressure valve **H4**	UCA9—Dcs closes the pressure valve too early **H4** Dcs closes the pressure valve too late	N/A
	UCA10—Dcs does not open the pressure valve **H4**	Dcs orders to open the pressure valve	Dcs opens the pressure valve too early UCA11—Dcs open the pressure valve too late **H4**	N/A
Trigger the fire-fighting system	UCA12—Dcs does not trigger the fire-fighting system **H9**	Dcs triggers the fire-fighting system	The dcs triggers the fire-fighting system too early UCA13—The dcs triggers fire-fighting system too late **H9**	UCA14—The dcs stops the fire-fighting system too soon **H9**
Start the drain pumps	UCA15—Dcs does not order to start the drain pumps **H7**	Dcs orders to start drain pumps	UCA16—Dcs orders to start drain pumps too late **H7**	UCA17—Dcs orders to stop drain pumps too soon **H7**
Controlling safety action in the other stations (SCADA system)	UCA18—The SCADA system does not control safety actions **H3 H4**	The SCADA system controls safety actions	UCA19—The SCADA system is out of order **H3 H4**	N/A
Emergency shutdown system	UCA20—ESD system does not trigger **H4 H7**	ESD system starts	UCA21—ESD system does trigger too late **H4 H7**	N/A
Open/close the inlet valve in the arrival terminal	UCA22—Dcs does not close the inlet valve of the arrival terminal **H7**	Dcs orders to close the inlet valve of the arrival terminal	UCA23—Dcs closes the inlet valve of the arrival terminal too late **H7**	N/A
	UCA24—Dcs does not open the inlet valve of the arrival terminal **H4**	Dcs orders to open the inlet valve of the arrival terminal	UCA25—Dcs orders to open the inlet valve of the arrival terminal too late **H4**	UCA26—Dcs orders to open the inlet valve of the arrival terminal too long **H7**

Figure 7 shows a diagram by column of the possible causes identified by the two methods, like we say previously.

Both methods identified the same number of hazards for physical components, and human error. The BOWTIE method did not identify any hazard in relation to system error. For external aggressions, the STPA identified only 1 linked to impact/shock from external activities, while the BOWTIE method identified 3 hazards related to evilness, natural events and impact/shocks.

Table 3 Identifying controller constraints

Unsafe control actions	Controller constraints
UCA1—Operator does not make the correct actions to activate safety controls. H4	C1—The operator should do the correct actions to activate safety controls UCA1
UCA 2—Operator activates the safety controls too late. **H4**	C2—The Operator mustn't activate the safety controls too late UCA2
UCA 3—Operator stops the safety controls too soon. **H4**	C3—Operator must not stop the safety controls too soon UCA3
UCA4—The operator does not activate all safety controls **H4**	C4—The operator must activate all safety controls UCA4
UCA5—Dcs does not start the cathodic protection **H2 H3**	C5—Dcs must start the cathodic protection UCA5
UCA6—Dcs starts the cathodic protection too late **H2 H3**	C6—Dcs must not start the cathodic protection too late UCA6
UCA7—Dcs starts the cathodic protection too soon **H3**	C7—Dcs must not start the cathodic protection too soon UCA7
UCA8—Dcs orders to close the pressure valve **H4**	C8—Dcs must not order to close the pressure valve UCA8
UCA9—Dcs closes the pressure valve too early **H4**	C9—Dcs must not close the pressure valve too early UCA9
UCA10—Dcs does not open the pressure valve **H4**	C10—Dcs must open the pressure valve UCA10
UCA11—Dcs opens the pressure valve too late **H4**	C11—Dcs must not open the pressure valve too late UCA11
UCA12—Dcs does not trigger the fire-fighting system **H9**	C12—Dcs must trigger the fire-fighting system UCA12
UCA13—The dcs triggers fire-fighting system too late **H9**	C13—Dcs must not trigger the fire-fighting system too late UCA13
UCA14—The dcs stops the fire-fighting system too soon **H9**	C14—The Dcs must not stop the fire-fighting system too soon UCA14
UCA15—Dcs does not order to start the drain pumps **H7**	C15—Dcs must order to start the drain pumps UCA15
UCA16—Dcs orders to start drain pumps too late **H7**	C16—Dcs must not order to start the drain pumps too late UCA16
UCA17—Dcs orders to stop drain pumps too soon **H7**	C17—Dcs must not order to stop drain pumps too soon H7 UCA17
UCA18—The SCADA system does not control safety actions **H3 H4**	C18—The SCADA system must control safety actions UCA18
UCA19—The SCADA system is out of order **H3 H4**	C19—The SCADA system must not be out of order UCA19
UCA20—ESD system does not trigger **H4 H7**	C20—ESD system must trigger UCA20
UCA21—ESD system does trigger too late **H4 H7**	C21—ESD system must not trigger too late UCA21
UCA22—Dcs does not close the inlet valve of the arrival terminal **H7**	C22—Dcs must close the inlet valve of the arrival terminal UCA22
UCA23—Dcs closes the t inlet valve of the arrival terminal too late **H7**	C23—Dcs must not close the inlet valve of the arrival terminal too late UCA23
UCA24—Dcs does not open the inlet valve of the arrival terminal **H4**	C24—Dcs does not open the inlet valve of the arrival terminal UCA24
UCA25—Dcs orders to open the inlet valve of the arrival terminal too late **H4**	C25—Dcs must not order to open the inlet valve of the arrival terminal too late UCA25
UCA26—Dcs orders to open the inlet valve of the arrival terminal too long **H7**	C26—Dcs must not order to open the inlet valve of the arrival terminal too long UCA26

Comparison of the identified consequences

The different losses identified by the STPA method in the first stage cover several aspects, such as the main function of our system; the transportation of condensate, environmental damage, loss of the product transported and eventual loss of humans, if they are present there at the time of accident.

While the BOWTIE method identifies the consequences directly related to flash fire and jet fire accidents, the triggering of these fires is conditioned by the presence of an ignition source; if the latter is not present, we will end up with an explosive atmosphere.

The comparison of these two methods indicates that the STPA method determines the losses/consequences in a general way, while the BOWTIE method specifies the nature of the dangerous events.

Comparison of the methodology of each method

In this section, we compare the steps of each method used in this analysis.

In Table 9, we notice that all steps in the both methods are not matching, except for step 2 and step 3 in the STPA method which matches with second step of BOWTIE method; it is in relation to defining potential causes of the accident, and how they might lead to an accident.

The STPA method analyzes hazards principally related to software and system controls, while the BOWTIE performs a hazard identification in direct relation with the pipe and its components; this resumes the major difference between them.

Table 4 Scenarios identified

Unsafe control action	Scenarios	Hazards
UCA1—Operator does not make the correct actions to activate safety controls	**Scenario 1**: the operator does not make the correct manual actions to activate safety controls because he does not receive the feedback/information when he need them, due to flawed control algorithm	H4
	Scenario 2: the operator does not use the correct manual actions to activate safety controls because he does a wrong interpretation of the feedback/information received, due to lack of experience, personal issues	
UCA 2—Operator activates the safety controls too late	**Scenario 1**: the operator activates safety controls too late, because he does not receive the feedback/information when he need them, due to flawed control algorithm	H4
	Scenario 2: the operator activates safety controls too late, because he has multiple tasks to do, due to a lot of work to do and lack of workers	
	Scenario 3: the operator activates safety controls too late, because he was absent, break-time	
UCA 3—Operator stops the safety controls too soon.	**Scenario 1**: Operator stops the safety controls too soon, due to an inadvertence from him	H4
UCA4—The operator does not activate all safety controls	**Scenario 1**: The operator does not activate all safety controls, because he does not receive all feedback/information when needed; due to a flawed control algorithm	H4
	Scenario 2: The operator does not activate all safety controls, because he does a wrong interpretation of the feedback/information received, due to lack of experience	
UCA5—DCS does not start the cathodic protection	**Scenario 1**: DCS does not start the cathodic protection, because the controller receive wrong feedback/information, due to flawed control algorithm	H2 H3
	Scenario 2: DCS does not start the cathodic protection, because of a wrong value send by the corrosion indicator, due to a failure in the corrosion indicator	
UCA6—Dcs starts the cathodic protection too late	**Scenario 1**: Dcs starts the cathodic protection too late, because the feedback/information is not received when needed (too late), due to a flawed control algorithm	H2 H3
UCA7—Dcs starts the cathodic protection too soon	**Scenario 1**: Dcs starts the cathodic protection too soon, because the controller does a wrong interpretation of the feedback/information received, so it starts the cathodic protection too soon, when it's not needed	H3
UCA8—Dcs orders to close the pressure valve	**Scenario 1**: Dcs orders to close the pressure valve, because the dcs does a wrong interpretation of the feedback/information received, due a flawed control algorithm	H4
	Scenario 2: Dcs orders to close the pressure valve, because the dcs receives a wrong feedback/information (pressure indicator); so the interpretation will be wrong, due to a flawed control algorithm	
UCA9—Dcs closes the pressure valve too soon	**Scenario 1**: Dcs closes the pressure valve too early, because the dcs does a wrong interpretation of the feedback/information received, due a flawed control algorithm	H4
	Scenario 2: Dcs closes the pressure valve too soon, because the dcs receives a wrong feedback/information (pressure indicator), due a flawed control algorithm	
UCA10—Dcs does not open the pressure valve	**Scenario 1**: Dcs does not open the pressure valve, because the dcs does a wrong interpretation of the feedback/information received, due a flawed control algorithm	H4
	Scenario 2: Dcs does not open the pressure valve, because the dcs receives a wrong feedback/information (pressure indicator), due a flawed control algorithm	
UCA11—Dcs open the pressure valve too late	**Scenario 1**: Dcs open the pressure valve too late, because the dcs does not receive feedback/information in time, due a flawed control algorithm	H4
	Scenario 2: Dcs open the pressure valve too late, because the dcs receives a wrong feedback/information (pressure indicator), due a flawed control algorithm	
UCA12—Dcs does not trigger the fire-fighting system	**Scenario 1**: Dcs does not trigger the fire-fighting system, because the dcs does not receive feedback/information, due a flawed control algorithm	H9
	Scenario 2: Dcs does not trigger the fire-fighting system, because the dcs does a wrong interpretation of the feedback/information received, due a flawed control algorithm	
UCA13—The dcs triggers fire-fighting system too late	**Scenario 1**: The dcs triggers fire-fighting system too late, because the dcs does not receive feedback/information in time, due a flawed control algorithm	H9
UCA14—The dcs stops the fire-fighting sys too soon	**Scenario 1**: The dcs stops the fire-fighting sys too soon, because the dcs does a wrong interpretation of the feedback/information received, due a flawed control algorithm	H9
UCA15—Dcs does not order to start the drain pumps	**Scenario 1**: Dcs does not order to start the drain pumps, because the dcs does a wrong interpretation of the feedback/information received, due a flawed control algorithm	H7
UCA16—Dcs orders to start drain pumps too late	**Scenario 1**: Dcs orders to start drain pumps too late, because the dcs does not receive feedback/information in time, due a flawed control algorithm	H7
UCA17—Dcs orders to stop drain pumps too soon	**Scenario 1**: Dcs orders to stop drain pumps too soon, because the dcs does a wrong interpretation of the feedback/information received, due a flawed control algorithm	H7

Table 4 continued

Unsafe control action	Scenarios	Hazards
UCA18—The SCADA system does not control safety actions	**Scenario 1**: The SCADA system does not control safety actions, because the SCADA system receives a wrong feedback/information, due to an inadequate process model	H3 H4
	Scenario 2: The SCADA system does not control safety actions, because the SCADA system does a wrong interpretation of the feedback/information received	
	Scenario 3: The SCADA system does not control safety actions, because the SCADA system does not receive feedback/information, due to a flawed algorithm	
UCA19—The SCADA system is out of order	**Scenario 1**: The SCADA system is out of order, because of a flawed control algorithm	H3 H4
	Scenario 2: The SCADA system is out of order, because of a failure related to physical controllers	
UCA20—ESD system does not trigger	**Scenario 1**: ESD system does not trigger, because the ESD system does a wrong interpretation of feedback/information received	H4 H7
	Scenario 2: ESD system does not trigger, because the ESD system receive a wrong feedback/information	
UCA21—ESD system does trigger too late	**Scenario 1**: ESD system does trigger too late, because the ESD system does not receive feedback/information in time	H4 H7
UCA22—Dcs does not close the inlet valve of the arrival terminal	**Scenario 1**: Dcs does not close the inlet valve of the arrival terminal, because the Dcs receives wrong feedback/information, due to a flawed control algorithm	H7
	Scenario 2: Dcs does not close the inlet valve of the arrival terminal, because the Dcs do a wrong interpretation of feedback/information received	
UCA23—Dcs closes the t inlet valve of the arrival terminal too late	**Scenario 1**: Dcs closes the inlet valve of the arrival terminal too late, because the Dcs does not receive feedback/information when needed, due to a flawed control algorithm	H7
UCA24—Dcs does not open the inlet valve of the arrival terminal	**Scenario 1**: Dcs does not open the inlet valve of the arrival terminal, because the Dcs receives wrong Feedback/information, due to a flawed control algorithm	H4
	Scenario 2: Dcs does not open the inlet valve of the arrival terminal, because the dcs does a wrong interpretation of the feedback/information received	
UCA25—Dcs orders to open the inlet valve of the arrival terminal too late	**Scenario 1**: Dcs orders to open the inlet valve of the arrival terminal too late, because the dcs does not receive feedback/information when needed, due to a flawed control algorithm	H4
UCA26—Dcs orders to open the inlet valve of the arrival terminal too long	**Scenario 1**: Dcs orders to open the inlet valve of the arrival terminal too long, because the dcs receives a wrong feedback/information, due a flawed control algorithm	H7
	Scenario 2: Dcs orders to open the inlet valve of the arrival terminal too long, because the dcs does a wrong interpretation of the feedback/information received, due a flawed control algorithm	

Table 5 Feared events

Feared events	Commentaries
1 Pipeline leak in liquid phase	Corresponds to a hole of diameter equal to a certain percentage of the nominal diameter of a pipe carrying a flammable liquid. It can be a "functional" opening on the pipeline: leaks from seals on pumps, on valves…
2 Pipeline leak in gas phase	Corresponds to a hole of diameter equal to a certain percentage of the nominal diameter of a pipe carrying a gas. The feared event can be a "functional" opening on the pipeline: leaks from seals on pumps, on valves…
3 Breakage of a pipe	The rupture is the loss of equipment leading to a significant and instantaneous release of the substance. In most cases, the catastrophic rupture, can lead to the ejection of missiles, thermal flows and a surge wave
4 Collapse of the pipe	Reservoir collapse is the complete loss of equipment, leading to a complete and instantaneous release of the substance. It is due to a reduction of the capacity pressure leading to its collapse by action of the atmospheric pressure

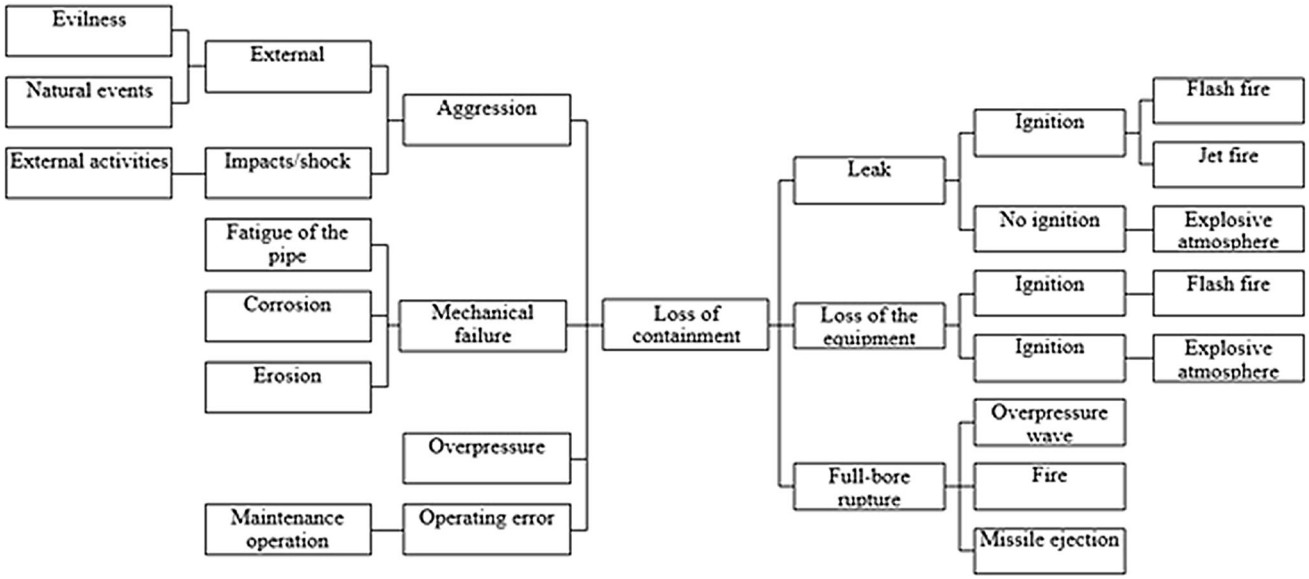

Fig. 6 Hazards identification in condensate pipeline using the Bowtie method

Table 6 Summary of identified hazards

Hazards identified by STPA	Hazards identified by Bowtie
Impact/shocks due to external activities nearly to the pipe	External impacts/shocks
Mechanical failure of the pipe	Corrosion
Corrosion	Overpressure
Overpressure in the pipe	Erosion
Operating errors: maintenance operations	Operating error: maintenance
Failure of the control system in the control room	Mechanical failure of the pipe: fatigue of the pipe
Overfilling tank at arrival station	Natural events
Electrical issues in the arrival station	Evilness
Fire in facilities of the arrival terminal	/

Table 7 Mapping of the hazards identification

No	STPA	BOWTIE
1	*Not identified*	Evilness
2	*Not identified*	Natural events
3	H1	Impacts/shocks
4	*Not identified*	Fatigue of the pipe
5	H2	*Not identified*
6	H3	Corrosion
7	*Not identified*	Erosion
8	H4	Overpressure
9	H5	Operating error
10	H6	*Not identified*
11	H7	*Not identified*
12	H8	*Not identified*
13	H9	*Not identified*

Conclusion

In this paper, we realized a hazard identification of pipeline hazardous materials transportation, in Skikda region, using two different methods: the STPA and Bowtie methods. The identification was followed by a comparison study of the two approaches performances. Through this comparison, we can mention that the hazards identified by the Bowtie method are essentially linked to the pipeline and its internal characteristics, while the STPA results are related to safety control system of the pipe. We noticed also that some hazards related to evilness, natural events and internal events are linked to physical state of the pipe, they are only identified by the Bowtie method. We were also able to identify some differences in the steps of these two methods.

Table 8 Classification of the possible causes

Possible causes	STPA	BOWTIE
Physical components error	H2: mechanical failure of the pipe	Fatigue of the pipe
	H3: pipe corrosion	Corrosion
	H4: overpressure in the pipe	Overpressure
	H9: fire in facilities of the arrival terminal	Erosion
Human error	H5: Operating errors: maintenance operations	Operating error
System error	H6: failure of the control system in the control room	/
	H7: overfilling tank in arrival station	
	H8: electrical issues in the arrival station	
External aggression (natural events, external activities)	H1: impact/shocks due to external activities nearly to the pipe	Natural events
		Evilness
		Impacts/shocks

Fig. 7 Classification of the hazards identified by both methods

At the end of our study, it was also found that the step of hazards identification using these two methods highlighted a complementarity of the latter in order to identify in a more exhaustive way the hazards associated with the studied system; their combination may be useful for a more exhaustive study. As a conclusion, for more thorough hazards identification associated with the studied systems, the complementarity between these two methods explored STPA and Bowtie, inciting the development of a hybridization or a combination of these methods, as a research avenue to be explored.

Table 9 Comparison between the steps of each method

STPA steps	BOWTIE steps
/	Determine the feared event that is the center of our bowtie, which is preselect in the preliminary risk analysis stage that allows risk hierarchization
Steps 1: define the purpose of analysis, system, system's environment, potential losses, system level hazards, system level constraints	/
Step 2: modeling the control structure of the system being studied, functional relationships and interactions between the different components of the whole system	Constitution of the fault tree which defines causes leading to feared event
Step 3: analyze control actions in the control structure to examine how they might lead to level hazards system previously identified	
Step 4: identify the reasons why unsafe control might occur, different scenarios are created	/
/	Construction of the event tree to determine the nature of the consequences

References

1. E.L.A.E.L. Safadi, Contribution to the risk assessment of transport of hazardous materials taking into account uncertainties. Automatic/Robotic. University Grenoble Alpes (2015)
2. C. Bersani, L. Citro, R.V. Gagliardi, R. Sacile, A.M. Tomasoni, Accident occurence evaluation in the pipeline transport dangerous goods. Chem. Eng. Trans. **19**, 249–254 (2010)
3. A. Shahriar, R. Sadiq, S. Tesfamariam, Risk analysis for oil & gas pipelines: a sustainability assessment approach using fuzzy based Bowtie analysis. J. Loss Prev. Process Ind. **25**(3), 505–523 (2012). https://doi.org/10.1016/j.jlp.2011.12.007
4. Z.Y. Han, W.G. Weng, Comparison study on qualitative and quantitative risk assessment methods for urban natural gas pipeline network. J. Hazard. Mater. **189**(1–2), 509–518 (2011)
5. Y.-D. Jo, B.J. Ahn, A method of quantitative risk assessment for transmission pipeline carrying natural gas. J. Hazard. Mater. **A123**, 1–12 (2005)
6. C. Vianello, G. Maschio, Quantitative risk assessment of the Italian gas distribution network. J. Loss Prev. Process Ind. **32**, 5–17 (2014). https://doi.org/10.1016/j.jlp.2014.07.004
7. M. Pontiggia, T. Vairo, B. Fabiano, Risk assessment of buried natural gas pipelines. Critical aspects of event tree analysis. Chem. Eng. Trans. **77**, 613–618 (2019)
8. N.G. Leveson, C.H. Fleming, M. Spencer, J. Thomas, C. Wilkinson, Safety assessment of complex, software-intensive systems. SAE Int. J. Aerosp. **5**(1), 233–244 (2012)
9. N. Leveson, C. Wilkinson, C. Fleming, J. Thomas, I. Tracy, A comparison of STPA and the ARP 4761 safety assessment process, MIT PSAS Technical Report Rev. 1, October 2014
10. J. Zhang, H. Kim, Y. Liu, M.A. Lundteigen, Combining system-theoretic process analysis and availability assessment: a subsea case study. Proc. Inst. Mech. Eng. Part O J. Risk Reliab. (2019). https://doi.org/10.1177/1748006X18822224
11. S.M. Sulaman, T. Abbas, K. Wnuk, M. Höst, Hazard analysis of collision avoidance system using STPA, in *International Conference on Information Systems for Crisis Response and Management (ISCRAM)* (2014), pp. 424–428
12. S.M. Sulaman, A. Beer, M. Felderer et al., Comparison of the FMEA and STPA safety analysis methods—a case study. Softw. Qual. J. (2017). https://doi.org/10.1007/s11219-017-9396-0
13. C. Schmittner, Z. Ma, P. Puschner, Limitation and improvement of STPA-Sec for safety and security co-analysis, in *International Conference on Computer Safety, Reliability, and Security* (Springer, Cham, September 2016), pp. 195–209
14. Data Sheets: OK1/NK1/GK1/GK2/GK3, RTE-Skikda documents
15. Hydrocarbons transport network map, TRC 2013, Sonatrach documents
16. N. Leveson, J. Thomas, *STPA Handbook* (MIT, Cambridge, 2018)
17. Data sheets NK1, RTE Skikda documents, Sonatrach—Algeria
18. Guideline for quantitative risk assessment 'Purple book', CPR 18E, The Netherlands Organisation of applied Scientific Research (2005)