An integrated framework for business continuity management of critical infrastructures

Jinduo Xing, Enrico Zio

An integrated framework for business continuity management of critical infrastructures

Jinduo Xing
Chair on Systems Science and the Energetic Challenge, Fondation EDF, Centrale-Supelec, Universite Pairs-Saclay, France

Enrico Zio
Chair on Systems Science and the Energetic Challenge, Fondation EDF, Centrale-Supelec, Universite Pairs-Saclay, France; Energy Department, Politecnico di Milano, Milano, Italy

ABSTRACT: Business continuity of critical infrastructures (CIs) is exposed to various hazards including random failures, malicious threats, natural disasters and human errors, which could generate accidents with serious consequences (fatality, injury, environmental damage, business interruption and company reputation loss). We conceptualize the business continuity management (BCM) process as the integration of four active stages: prevention, mitigation, emergency and recovery. Integrated assessment and management is needed on all stages. On the contrary, the current approaches of BCM have not considered all phases in an integrated manner. We propose a new framework, which stands on an extension of the Bow-Tie model, to efficiently and effectively prevent and mitigate the potential consequences of an accident by properly designing and strengthening safety barriers for preventing and mitigating accidents, and making safety decisions for emergency and recovery. The proposed framework allows considering safety barriers and decisions in an integrated way. For operationalization, we explore the use of two complementary quantitative methods, Bayesian Network (BN) and Constraint Goal Method. BN takes the "negative" viewpoint of failure to determine the causes which lead to the final damage. CGM employs the positive perspective of the goal achievement process. An oil pipeline system is considered to show the application of the proposed approaches.

1. INTRODUCTION

Critical infrastructures are exposed to various types of hazards, which could occur individually or concurrently. The consequent failures of CIs could generate serious damage (fatality, injury, environmental pollution, business interruption and company reputation loss). In this scenario, BCM (business continuity management) is crucial to provide confidence that the outputs of processes and operations can be delivered reliably through the CIs in the face of risks (Gibb and Buchanan 2006, Zio 2016). The international organization for standards gives a definition of BCM as "Holistic management process that identifies the potential threats to an organization and the impacts to business operations by those threats, if realized, might cause, which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities." (ISO 2012). Through identification and management of the risks leading to potential damage to business profit, one could improve the resilience of business activities. Several studies have proposed different methods for BCM. Rabbani et al. adopted the cost-benefit analysis for evaluating BCM strategies (Rabbani, Soufi et al. 2016). Satorabi et al. determined the maximum tolerable period of disruption for a minimum business continuity objective, within a framework for business impact analysis (Torabi, Rezaei Soufi et al. 2014). Bhamra et al. presented the relationship between business continuity and system resilience, and pointed out that those organizations that adopt BCM can have a higher level of resilience (Bhamra, Dani et al. 2011). Sahebjamnia et al. integrated BCM and disaster recovery planning to present a proactive approach for resilience of organization (Sahebjamnia, Torabi et al. 2015). A crucial part of

BCM is business impact analysis, to determine the latent probability and consequence of the events and the dependence between previous factors and subsequent events.

These previous studies on BCM have pointed out the benefit for crisis and recovery management. The hazards need to be considered over the whole business process. To this purpose, the business process can be divided into four phases along the event evolution process, as shown in Fig 1. Firstly, when the hazard attacks the targeted system, it could cross the preventive barriers (black rectangle) and affect the business of the system (S1). When the accident enters the crisis stage (S2), the mitigative barriers (gray rectangle) and the emergency decisions taken to control the accident, shape the resistance of the system in minimizing the damage. Then, external resources would be called upon to rescue the system, reducing the damage. During the emergency stage, additional emergency barriers (dark rectangle) and decisions of action shape the evolution of the accident. Eventually, a last step of recovery is undertaken to regain the site safety and reconstruct business, as soon as possible. The overall business loss and consequences depend on the preset barriers and decisions taken at the various stages of accident evolution.

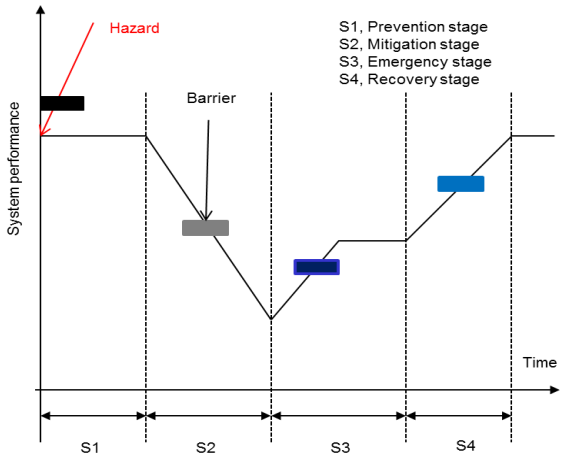

Fig 1.Systems performance evolution during the accident progression

The study reported in the present work aims at providing an integrated framework for BCM. We consider the Bayesian Network (BN) and Constraint Goal Method for a comprehensive analysis. The main contributions are:

(1) Conceptualization of the BCM of CIs.
(2) Presentation of an integrated framework for BCM of CIs, by an extended Bow-Tie diagram.
(3) Applying BN and CGM for BCM.

2. PROPOSED FRAMEWORK

2.1. Analysis framework

Risk management of CIs typically includes accident occurrence prevention and consequence mitigation. Emergency and recovery are usually considered outside this parameter, or at least separated. On the contrary, an integrated framework of risk analysis and management seems in order. For example, in the Huangdao petroleum transportation pipeline explosion accident of 2013, the reason for the accident escalation was a misoperation in the emergency phase, causing the explosion of the volatile gas. In 2015 Tianjin Port accident in China, 99 firefighters and 11 policemen died (among 165 casualties) during emergency operations.

The proposed integrated framework of BCM consists of four stages of a risk management process. The interface and dependence between different stages needs to be analyzed, for effective management decisions.

For business continuity throughout the different stages of risk management, the different safety barriers play an important role. Accident prevention involves technical aspects and organization decisions, concerning passive barriers, active barriers, human factors, etc. (Dianous and Fievez 2006). Once the hazard affects the system, an emergency situation arises, for which mitigation of consequences is the important aspect. Also for this, there exist passive or active barriers, detection and diagnosis instruments, and human actions. Then, when in the emergency stage, appropriate decisions and safety actions must be taken to safeguard the emergency activities. The principle is to control the hazardous consequences of the accident, for eliminating the site danger and provide suitable, safe recovery conditions of the system. Eventually, recovery starts.

2.2. Extended Bow-Tie model for BCM framework

Bow-Tie is a traditional method to model an accident process, coupling a fault tree and an event tree representation (Chevreau, Wybo et al. 2006). The use of Bow-Tie is common in many areas of risk management, hazard analysis, accident scenario analysis (Khakzad, Khan et al. 2011). Bow-Tie is capable of representing the logic relationships between the causes, intermediate events, possible consequences and safety barriers involved in an accident progression. Typically, the representation ends at the accident consequence, without considering emergency and recovery. Also, in traditional Bow-Tie the causes and consequences are assumed independent, which does not reflect the reality in some practical situations. We develop a Bow-Tie for the integrated framework of BCM, as illustrated in Fig 2.

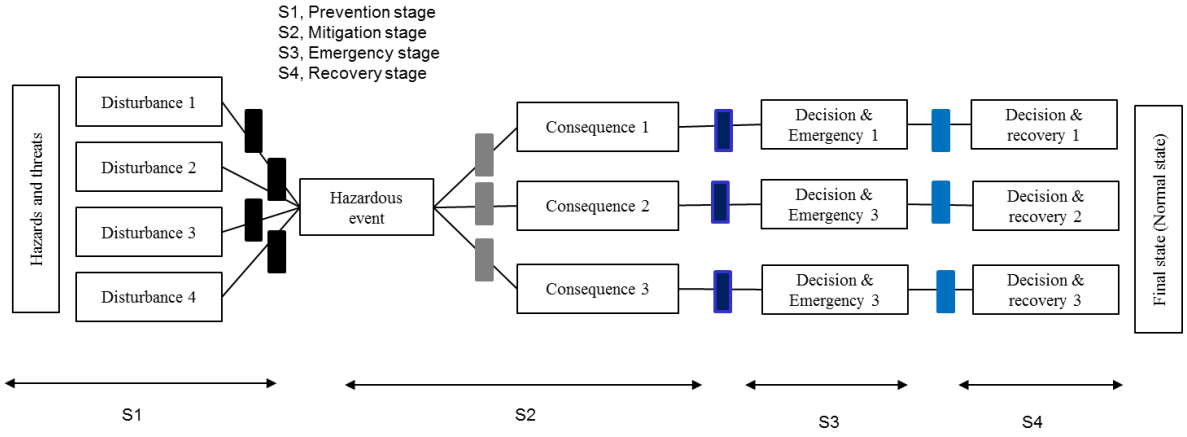

Fig 2 Extended Bow-Tie for the integrated framework of BCM

In stage S1, the hazards affect the system operation by generating business disturbance, which becomes a hazardous event if the disturbance goes through the safety barriers. As the accident progresses, it comes to the crisis stage, where consequences (e.g. materials waste, explosion, injuries, fatalities) are experienced to an extent which depends on the effectiveness of the mitigation barriers. Emergency decisions and actions are needed to prevent the accident to expand. Finally, decisions and actions are required to guide the recovery of the business to normal situation.

3. OPERATIONALIZATION OF THE INTEGRATED FRAMEWORK

To make sound application of the framework in practice, we consider the integration of quantitative methods, like CGM and BN. The former models the goal achievement process (a positive viewpoint), the latter models the failure logic to determine the causes of final damage (a negative perspective).

3.1 Bayesian network in BCM.

Bayesian network is a directed acyclic graphical representation method, where the nodes are random variables and dependencies are represented by the directed arcs between the nodes (Khakzad, Khan et al. 2014). Conditional probabilities are assigned to reflect the strength of dependencies. The root nodes are allocated marginal probabilities (Khakzad 2015). By applying the chain rule and the d-separation criteria (Khakzad, Khan et al. 2014), the joint probabilities of the parent node events are given from those of their children nodes:

$$P(\mathrm{X}) = \mathrm{P}(\mathrm{X}_1, \mathrm{X}_2, \cdots, \mathrm{X}_n) = \prod_{i=1}^{n} P(\mathrm{X}_i \left| Pa(\mathrm{X}_i)\right.) \qquad (1)$$

where $Pa\ (\mathrm{X}_i)$ is the parent set of X_i. $P(\mathrm{X})$ is the joint probability of its variables $\mathrm{X}=\{\mathrm{X}_1, \mathrm{X}_2, \cdots \mathrm{X}_n\}$. Bayes' theorem is used to update the probability (1), when there are new evidences E:

$$P(X \left| E\right.) = \frac{P(X)\,\mathrm{P}(E \left| X\right.)}{\sum_X P(X)\,\mathrm{P}(E \left| X\right.)} \qquad (2)$$

where $P(\mathrm{X} \left| E\right.)$ is the posterior joint probability updated based on the new evidence E.

We propose to use BN to represent the process of business impact analysis for BCM. By using BN, we can determine the probabilities of potential consequences and the importance for business continuity. Eventually, the probability updating of BN can improve BCM by adding evidences (measures) to control the critical factors during the different stages of the accident propagation.

3.2 Constrained goal modeling

CGM (http://www.cgm-tool.eu/) is used for requirement analysis in the computer science domain. The method aims to explain the requirement of stakeholders, and provide alternative designs for decision makers (Asnar, Giorgini et al. 2010). The CGM starts from the interests of the stakeholders and structures the process of goal achievement. The constrained goal model can be used to perform two types of analysis: (1) Given a CGM and assuming that certain leaf goals are fulfilled, one can infer the probability of the root goal; (2) given a CGM find a set of leaf goals that fulfill the root goal. To establish the CGM, the requirements of the stakeholders, resources, actions, tasks and data are needed. The probability $P(\mathrm{G})$ of the goal G of CGM is:

$$P(\mathrm{G}) = \sum_{i=1}^{n} R_i P(T_i) \qquad (3)$$

where R_i is the influence weight of the sub-goal (task) for the achievement of the goal in the upper layer, $P(T_i)$ is the probability of task T_i. Fig 3 presents the basic structure of CGM for BCM.

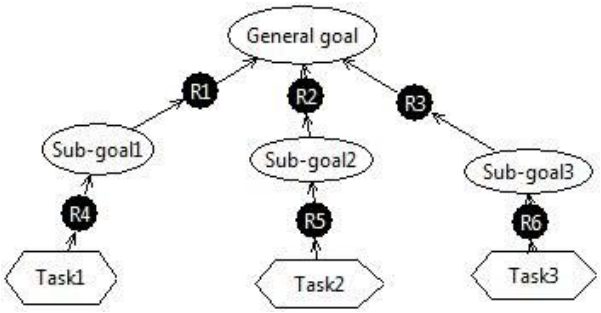

Fig 3 The basic structure of CGM. The round square represents different goal of the system; hexagon is the task or measure taken in the process. General goal means the overall goal of the system. Sub-goals are the different goals during the whole process. Task is the action in the process)

This work shows how to support the BCM through a goal achieving process structured by CGM for identifying critical aspects and actions.

4. CASE STUDY

The purpose of the case study is to illustrate the application of the framework described in section 2. The steps for the development of the integrated BCM framework are:
(1) Identify the BCM stages.
(2) Identify the potential business-impacting factors in the different stages.
(3) Determine the relationships between these factors.
(4) Calculate the business impact probabilities.
(5) Evaluate the importance index of every factor.
(6) Propose measures to reduce the probability of these critical factors.

4.1 Case description

On the morning of November 22, 2013, a severe oil pipeline accident occurred in Qingdao city, Shandong Province, P.R. China. Dong-Huang pipeline has been operating for 27 years. A leakage of explosive oil was discovered at 2:12 am and exploded at 10:25 am, China standard time (CST). The accident caused 62 fatalities, 132 injuries and a direct economic loss of 751.72 million RMB, including 2000 tons crude oil (Accident Investigation Team 2014). Liu et al described the propagation mechanism of the accident (Liu, He et al. 2015). The accident evolution is illustrated in Fig 4.

The direct cause of the leakage is the combination of transmission pipeline and drainage system corrosion and rupture. The spill entered into the drainage system and rushed to the pavement. During the emergency phase, the emergency personnel employed hydraulic hammers to punch, which unfortunately generated strike sparks. Consequently, the oil and gas in the drainage system was ignited and exploded.

In the whole process of accident propagation, there were various factors that contributed to the final outcome. The dependency relationship among them is presented in the following.

4.2 Case analysis

Based on the proposed framework of BCM, the whole accident analysis process can be divided into four stages. First comes the preventive stage, which must consider the possible hazards that may occur and the related influencing factors.

Corrosive environment and medium cause the pipeline becoming thinner. With high pressure and vibration, the corrosion situation becomes worse. Afterwards, the municipal city changed the road path, which resulted in the open drainage becoming covered drainage: during operation, there was then less checking and maintenance, which led to the final leakage. Inadequate supervision from related departments accelerated the progression of the leakage.

After the operator received the alarm signal, the emergency action started. Because of little emergency training and risk assessment ability, misoperation occurred. At the same time, wrong emergency decisions, where taken, with respect to no evacuation and safe guarding. Consequently, the accident generated severe fatality and injury consequences, environment pollution and economic loss. At the recovery stage, there still existed many threats including the spilled oil and fire, the offshore pipeline nearby, the chemical factory close-by and the polluted Jiaozhou bay of the Yellow Sea, North-West Pacific Ocean.

Note that this accident shows no distinction between the prevention and mitigation barriers. The inherent safety design is the first safety barrier. Periodical safety training is also included in the first safety barrier. Besides, safety decisions after disruption are included inside the barriers of the mitigation stage. Emergency training, knowledge of the site and risk assessment expertise are barriers for the emergency stage.

4.3 Bayesian network for pipeline BCM

The hazards and the safety barriers, and potential consequences need to be determined first. Based on literature review (OREDA participants 2002) and profes-

sional knowledge, the prior probabilities of the basic events are found (Table 1).

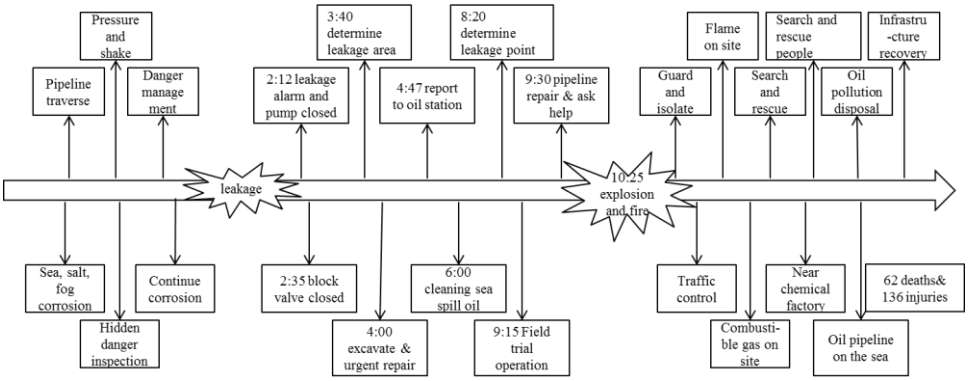

Fig 4 Timeline for Dong-Huang pipeline explosion accident

Table 1 Prior probabilities of basic events for pipeline accident

Number	Event	Symbol	Failure probability
1	No protection measures	N-prote	0.0749
2	Pipeline corrosion	Corrosion	—
3	Incomplete safety inspection	Is-ins	0.2506
4	Yet to repair	Yet-t	0.1345
5	Pipeline leakage	Leakage	—
6	Pipeline traverse	Traverse	0.2050
7	Combustible gas	Combu_gas	—
8	Emergency error	Emerg-error	0.3466
9	Combustible gas detection	Combu_det	0.2696
10	Fire and explosion	Fire_explosion	—
11	Weak safety awareness	W-sa	0.2132
12	Lack supervision	L-superv	0.1024
13	No emergency evacuation	N-ee	0.1365
14	Bearing and vibration	B-v	0.0902
15	No cordon off	N-co	0.1075
16	Detector failure	detectf	0.1915
17	Casualty and injury	Casualty-inj	—

A BN model for the accident was developed, covering the whole process of the BCM, as presented in Fig 5.

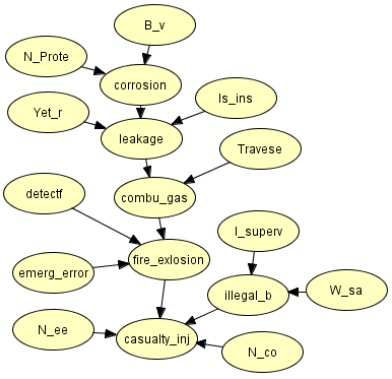

Fig 5 BN for the pipeline accident case

Combining the CPT (conditional probability Table) with the BN in Fig 5, we developed the probability of intermediate and top events of the accident. BN calculations were performed using HuGIN 7.3 package [1]. The results are shown in Table 2.

Table 2 Prior probabilities of intermediate and top events for the pipeline accident

Occurring event	Probability
Pipeline corrosion	0.1583
Pipeline leakage	0.0556
Combustible gas	0.0114
Fire and explosion	0.0896
Casualty and injury	0.0221

To analyze the contribution of each event to the final consequence of the accident progression, the improvement index was applied (Faisal I. Khan 2002), which indicates the contribution of the event. The importance index is:

$$I = \frac{P - P_{ui}}{P} \tag{4}$$

[1] http://www.hugin.com

where P is the probability of final event, in this case P equals to 0.0221, P_{ui} is the updating probability of final event under the condition of ith event does not occur. The higher the improvement index is, the more critical is the event for the consequence. Table 3 shows that the emergency error is the most important factor leading to the final accident.

Table 3 Consequence probability and improvement indices from BN analysis

Event not occurring	Probability	Improvement index (%)
Casualty and injury	0.0221	0.0
No protection measure	0.0218	1.3567
Bearing and vibration	0.0218	1.3567
Incomplete safety inspection	0.0217	1.81
Yet to repair	0.0219	0.09
Pipeline traverse	0.0215	2.715
Detector failure	0.0206	6.7
Emergency error	0.0005	97
No cordon off	0.0139	37
No emergency evacuation	0.0114	48.41
Lack supervision	0.0205	7.24
Weak safety awareness	0.0205	7.24

Then, to improve business continuity, measures could be taken to reduce the probability of emergency error. For this, emergency training and safety training can be developed. The probability updating of the final accident is shown in Fig 6, with two new evidences (no emergency drilling with probability 0.0765, no emergency training with probability 0.0625) added.

Fig 6 shows that the emergency and safety training help reducing the accident consequences. The posterior probability for casualty and injury is 0.0086 against the prior where of 0.0221. This shows that using BN in business impact analysis helps to allocate safety barriers.

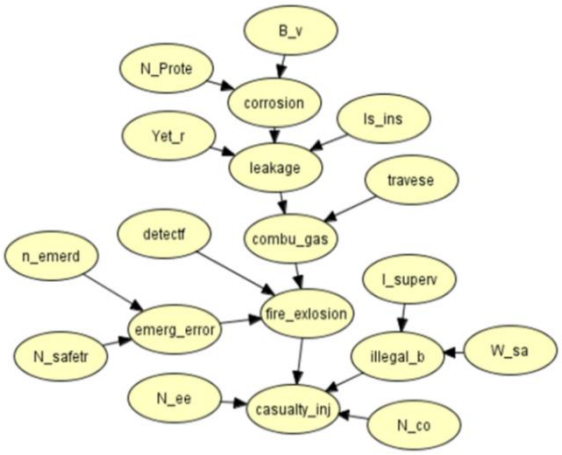

Fig 6 Probability updating for the top event of BN for the pipeline accident case

4.4 Constraint goal modeling of the accident

The constraint goal modeling for the pipeline accident is shown in Fig 7. The node name and the acronym is shown in Table 4.

Table 4 The node name and the acronym

Node name	Acronym	Node name	Acronym
Pipeline continuity operation	G1-PCO	Effective emergency	T7-EE
Reasonable pipe design	G2-RPD	Corrosion environment	G5-CE
Safety construction	G3-SC	Internal corrosion	G6-IC
Safety production	G4-SP	External corrosion	G7-EC
Reasonable planning	T1-RP	Around renovation	T8-AR
Suitable materials	T2-SM	Third-party damage	T9-TPD
Construction based on regulations	T3-CBR	Mis-operation	T10-MO
Safety supervision	T4-SS	Bearing and vibration	T11-BV
Operation based on regulations	T5-OBR	Salt-spry environment	T12-SPE
Periodic maintenance	T6-PM	No periodic emergency drilling	T13-NPED

The goal is keeping the pipeline continuity operation, which can be divided into three sub-goals. The first one is reasonable pipeline design and covers the reasonable planning and suitable materials. Next is safety construction for pipeline, which includes two tasks based on regulations and safety supervision during the construction process. The last one is safety production (operation), which could be attained by five actions corrosion resistant, obeying the regulations, periodic maintenance, effective emergency, and preventing third party damage. The influence weight of the sub-layers to the achievement of the upper layer

is given in Table 5. With the probability of each task given in section 3.2, the gradual goal achieved probability is,

$$P(\mathrm{G}) = \sum_{i=1}^{n} (R_{16} P_{\overline{G7}} R_{15} P_{\overline{G5}} + R_8 P_{T5} + \cdots + \mathrm{R_i} P_T) = 0.9440$$

where $\overline{G_i}$ means that the goal i has not occurred. The complement probability of system failure probability is 0.0560. Compared with the BN result, the accident evolution process is more visual. CGM gives the propagation weight of each sub-goal or task to the upper layer. However, such propagation weight depends on expert judgement, with inherent subjectivity.

Table 5 The value of each influence weight

R	Value	R	Value	R	Value	R	Value
R1	0.24	R5	0.35	R9	0.09	R13	0.75
R2	0.40	R6	0.50	R10	0.13	R14	0.05
R3	0.36	R7	0.50	R11	0.08	R15	0.50
R4	0.65	R8	0.65	R12	0.25	R16	0.50

5. DISCUSSION AND CONCLUSION

In this article, we have proposed an integrated framework for business continuity management based on an extended Bow-Tie model of the four stages, prevention, mitigation, emergency and recovery.

We have illustrated the proposed framework for the accident analysis of a severe oil and gas pipeline accident in 2013. BN and CGM have been used to quantitatively analyze the accident. Through the analysis process, the critical activities and factors have been identified.

REFERENCE

Accident Investigation Team (2014). The leakage and explosion accident investigation report of Sinopec Donghuang oil pipeline in Qingdao, Shandong. China, The State Council**:** 15.

Asnar, Y., P. Giorgini and J. Mylopoulos (2010). "Goal-driven risk assessment in requirements engineering." Requirements Engineering 16(2): 101-116.

Bhamra, R., S. Dani and K. Burnard (2011). "Resilience: the concept, a literature review and future directions." International Journal of Production Research 49(18): 5375-5393.

Chevreau, F. R., J. L. Wybo and D. Cauchois (2006). "Organizing learning processes on risks by using the bow-tie representation." Journal of Hazardous Materials 130(3): 276-283.

Dianous, V. and C. Fievez (2006). "ARAMIS project: a more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance." Journal of Hazardous Materials 130(3): 220-233.

Faisal I. Khan, R. S., Tahir Husain (2002). "Risk-based process safety assessment and control measures design for offshore process facilities." Journal of Hazardous Materials A94: 1-36.

Gibb, F. and S. Buchanan (2006). "A framework for business continuity management." International Journal of Information Management 26(2): 128-141.

ISO (2012). ISO 22301. Societal security- Business continuity management systems- Requirements. Switzerland, International Organization for Standardization.

Khakzad, N. (2015). "Application of dynamic Bayesian network to risk analysis of domino effects in chemical infrastructures." Reliability Engineering & System Safety 138: 263-272.

Khakzad, N., F. Khan and P. Amyotte (2011). "Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches." Reliability Engineering & System Safety 96(8): 925-932.

Khakzad, N., F. Khan, P. Amyotte and V. Cozzani (2014). "Risk management of domino effects considering dynamic consequence analysis." Risk Analysis 34(6): 1128-1138.

Liu, H., W. He, J. Guo and Q. Huang (2015). "Risk propagation mechanism: Qingdao Crude Oil Leaking and Explosion case study." Engineering Failure Analysis 56: 555-561.

OREDA participants (2002). OREDA. Offshore Reliability Data Handbook

Rabbani, M., H. R. Soufi and S. A. Torabi (2016). "Developing a two-step fuzzy cost–benefit analysis for strategies to continuity management and disaster recovery." Safety Science 85: 9-22.

Sahebjamnia, N., S. A. Torabi and S. A. Mansouri (2015). "Integrated business continuity and disaster recovery planning: Towards organizational resilience." European Journal of Operational Research 242(1): 261-273.

Torabi, S. A., H. Rezaei Soufi and N. Sahebjamnia (2014). "A new framework for business impact analysis in business continuity management (with a case study)." Safety Science 68: 309-323.

Zio, E. (2016). "Challenges in the vulnerability and risk analysis of critical infrastructures." Reliability Engineering & System Safety 152: 137-150.

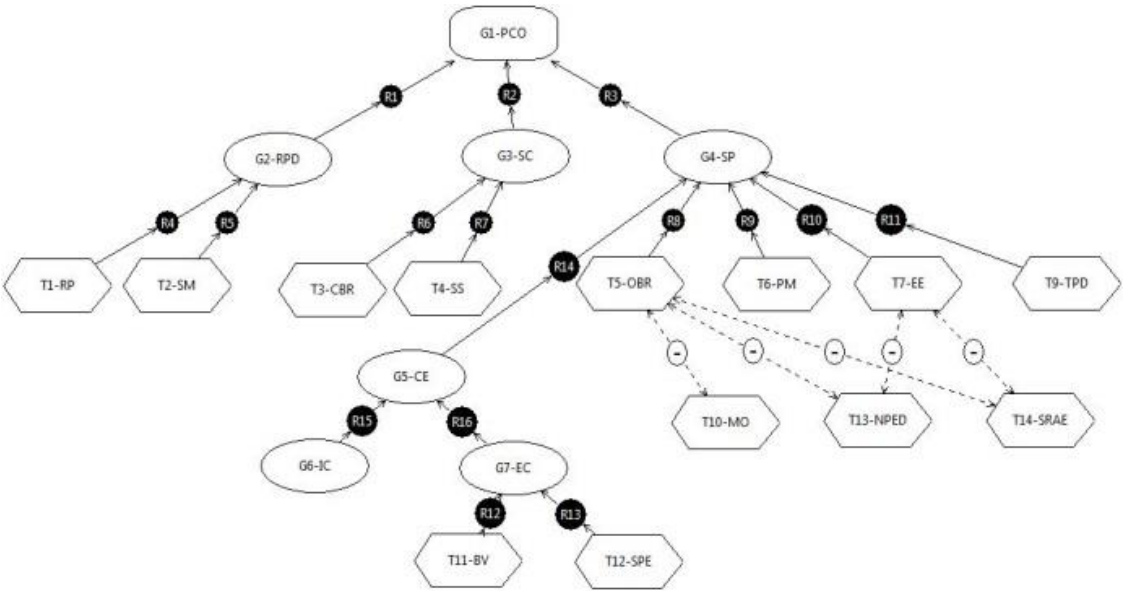

Fig 7 The CGM for the pipeline accident