Delft University of Technology

An Approach for Identification of Integrated Safety and Security Barriers in the Chemical Process Industries

Yuan, Shuaiqi; Yang, Ming; Reniers, Genserik; Chen, C.

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

An Approach for Identification of Integrated Safety and Security Barriers in the Chemical Process Industries

Shuaiqi Yuan, Ming Yang, Genserik Reniers[*], Chao Chen

Safety and Security Science Section, Faculty of Technology, Policy and Management, TU Delft, Delft, The Netherlands
G.L.L.M.E.Reniers@tudelft.nl

Chemical process industries are threatened with accidental and intentional adverse events because of the storage and operation of large quantities of hazardous substances. Safety and security barriers play important roles in protecting the chemical plants from safety and security-related undesired events and mitigating the potentially catastrophic consequences. Aiming to identify major accident scenarios in terms of both safety and security and determine the corresponding safety and security barriers, a novel approach based on MIMAH (methodology for identifying major accident hazards) and historical data analysis is proposed. In this approach, the MIMAH is extended to identify accident scenarios related to safety, physical security, and cyber security by using a combination of bow-tie analysis and attack tree analysis. Then, data analysis is conducted to supplement the identified major accident scenarios before the critical safety and security barriers can be identified and illustrated based on an integrated bow-tie and attack tree model. This study helps to identify major hazards considering both safety and security perspectives and supports the integrated assessment and management of safety and security barriers in the chemical process industries.

1. Introduction

Chemical process industries are subjected to important accidental and intentional risks due to the storage and usage of large quantities of hazardous substances. Notably, major accidents, such as toxic leakages, fires, and explosions triggered by safety hazards and security threats, can cause catastrophic damage to surrounding people, process facilities, and the environment. In terms of prevention and mitigation of major accidents, safety and security barriers are used in various forms to protect the chemical process industries from safety and security-related undesired events and mitigate the potentially catastrophic consequences (Villa & Cozzani, 2016). Moreover, practices in the field indicate the effectiveness and efficiency of integrating safety barrier management and security barrier management because security threats may lead to the same or even worse catastrophic scenarios as safety incidents. However, as an important part of barrier management, the identification of safety and security barriers is seldom investigated in previous studies, especially for security barriers. Generally, the identification of safety barriers should be conducted after the HAZard IDentification (HAZID). The reason is that barriers can always be linked to specific hazards or scenarios, and those linkages can be demonstrated by using bow-tie models. When a set of inclusive scenarios are identified, the corresponding barriers associated with the hazards or scenarios can be found. In previous studies, MIMAH (methodology for the identification of major accident hazards) was proposed in the Accidental Risk Assessment Methodology for Industries (ARAMIS) project, and it is able to identify all the potential safety-related major accident scenarios which can occur in the process industries (Delvosalle et al., 2006). However, some accident scenarios may not be identified by conventional HAZID techniques due to a lack of knowledge of atypical scenarios, a term defined by (Paltrinieri et al., 2012). To tackle this problem, retrieving information or knowledge from past accidents should be conducted. For example, the Dynamic Procedure for Atypical Scenarios Identification (DyPASI) methodology was proposed by Paltrinieri, et al. (2013) to identify atypical accident scenarios based on the information collected from literature and accident databases. In terms of barrier identification, bow-tie analysis usually is used as the baseline approach. For instance, the ARAMIS project recommended to identify safety functions and barriers with the help of bow-tie and proposed a checklist of safety functions and barriers on all the events of the bow-tie (Delvosalle & Fiévez, 2004). Moreno et al. (2018b) applied

DyPASI to identify critical safety barriers used for accident prevention and mitigation in biogas production and upgrading facilities.

Security threats are becoming an increasing concern for the chemical process industries due to the potential of intentional physical attacks and cyber-attacks (Moreno et al., 2018a). To protect the chemical plants from security-related undesired events, security barriers are used to achieve physical and cyber protections. Because the security-related threats and scenarios can not be captured using conventional HAZID techniques (e.g., MIMAH), identifying security barriers becomes difficult. The integration of security threats analysis and historical data analysis helps to identify complete accident scenarios and corresponding safety and security barriers, thus supporting safety and security risk management and barrier management. Therefore, this study proposed combining MIMAH with security threats analysis and historical data analysis to identify accident scenarios related to safety, physical security, and cyber security. Finally, the associated safety and security barriers can be determined according to the identified accident scenarios and can be illustrated on a model integrating bow-tie (BT) and attack tree (AT).

2. Methodology

This study proposes a systemic approach for identifying critical safety and security barriers for major accident scenarios in the chemical process industries. In the proposed approach, the MIMAH is extended by using attack tree analysis and historical data analysis. MIMAH mainly aims to identify potential major accident scenarios in a chemical plant without considering safety barriers/systems. The outcomes of the MIMAH are a series of complete bow-ties without safety barriers, which can be regarded as inputs for our proposed approach. To identify major accident scenarios considering both safety and security perspectives, attack tree analysis is employed to identify security scenarios that can be associated with the obtained bow-ties. By attaching the attack tree (AT) to the event in the bow-tie (BT), both safety-related and security-related accident scenarios can be presented by the AT-BT model (an example can be found in Figure 3). Because some atypical accident scenarios are hard to be identified by MIMAH and attack tree analysis, historical data analysis is employed to retrieve useful information from literature and accident databases and further generate atypical scenarios. The flow chart of the proposed approach that consists of four steps is shown in Figure 1. The elaborations of the four steps can be found in the following sub-sections.
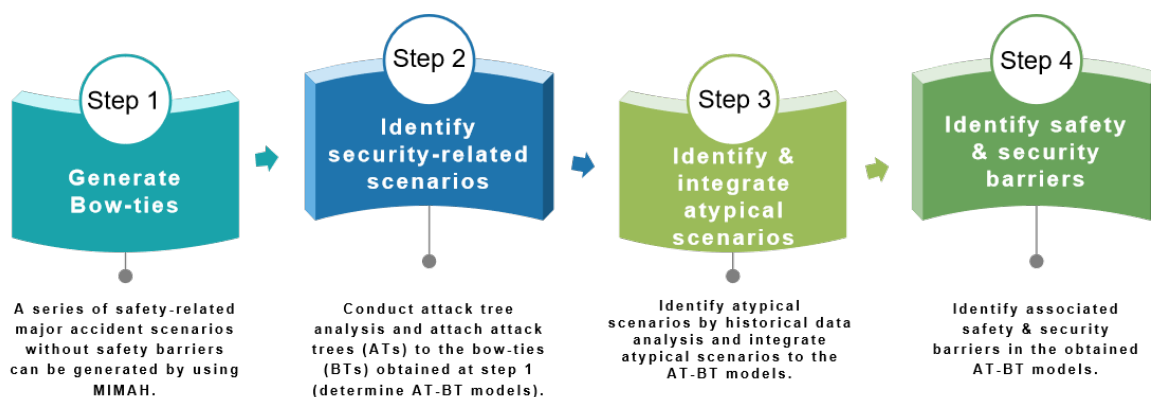

Figure 1: Flow chart of the proposed barrier identification approach

2.1 Generate Bow-ties by MIMAH (Step 1)

MIMAH aims to identify all the potential safety-related major accident scenarios within a process industry based on the bow-tie technique. MIMAH consists of nine steps, which can be found in Figure 2. The steps include: i) collect needed information, ii) identify potentially hazardous equipment, iii) select relevant hazardous equipment, iv) for each selected equipment, associate critical events, v) for each critical event, build a fault tree, vi) for each critical event, build an event tree, vii) for each selected equipment, build the complete bow-ties. Detailed elaboration on the MIMAH steps can refer to (Delvosalle et al., 2006). Finally, a series of complete bow-ties for each selected equipment can be constructed by the MIMAH methodology. These bow-ties demonstrate the identified major accident scenarios assuming that no interventions by safety barriers exist and they are the basis for the application of the barrier identification methodology.
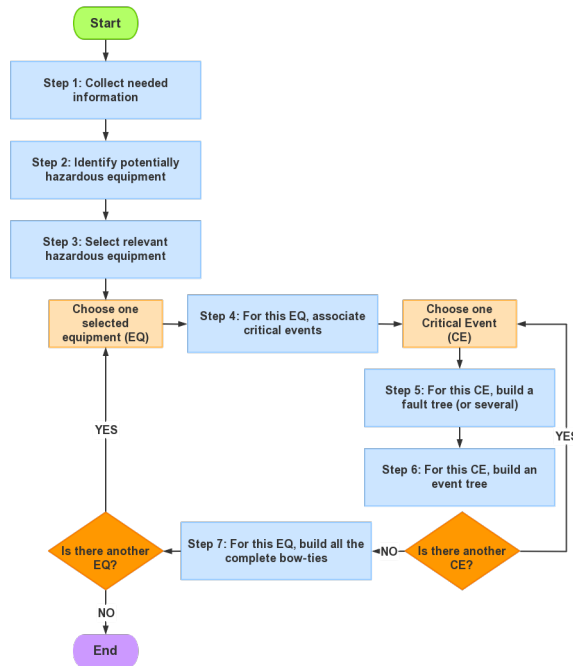
Figure 2: General overview of the MIMAH steps, adapted from (Delvosalle et al., 2006)

2.2 Security-related scenarios identification (Step 2)

Attack tree analysis is employed to identify security-related scenarios associated with the bow-ties obtained at step 1. Attack trees have been widely used to analyze risk scenarios related to cyber-security and identify threats to physical systems. The combination of bow-tie (BT) analysis and attack tree (AT) analysis can integrate safety and security risk assessment of critical systems. A combined AT-BT model was already employed to identify all safety and security threats that can lead to undesirable events and provide inclusive risk scenarios in terms of both safety and security (Abdo et al., 2018). A schematic example of the AT-BT model is presented in Figure 3. The definitions of the elements used in the AT-BT model are explained in Table 1. During step 2, the attack tree analysis is conducted to generate attack trees and attach attack trees to the associated bow-ties. The outcomes of step 2 are a set of AT-BT models, which can represent the major accident scenarios associated with both safety and security.
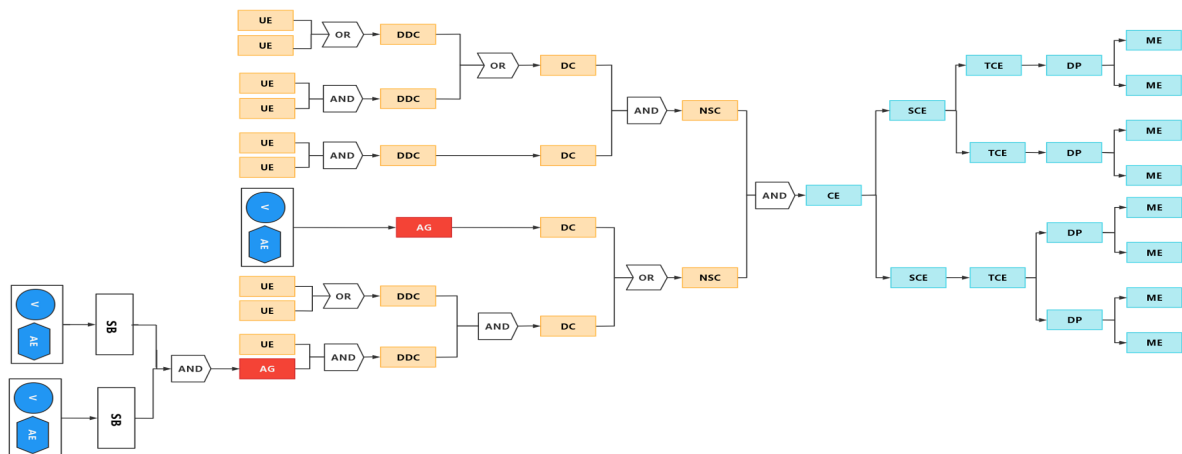

Figure 3: An example of the AT-BT model, adapted from (Delvosalle et al., 2006) and (Abdo et al., 2018)

2.3 Atypical scenarios identification (Step 3)

Atypical scenarios are the safety-and-security-related accident scenarios that cannot be captured by conventional HAZID techniques. The reason may be that the occurrence of atypical scenarios is very rare, and

the risk notions from past accidents were not considered in daily activities in terms of hazard identification. Additionally, new and emerging hazards may also comply with atypical scenarios due to the lack of operational experience.

Table 1: Abbreviations and definitions of the elements used in the AT-BT model, adapted from (Delvosalle et al., 2006) and (Abdo et al., 2018)

| Symbols	Elements	Definitions
UE	undesirable events (UE)	Undesirable events are very generic causes linked with human behavior and organizational deficiencies which are potential causes for a very large variety of events
DDC	detailed direct causes (DDC)	Detailed direct causes are the immediate causes of the direct causes
DC	direct causes (DC)	Direct causes could lead to the occurrence of NSC. The causes at this level can be erosion, corrosion, etc.
NSC	necessary and sufficient conditions (NSC)	The necessary and sufficient conditions that can provoke the critical event
AND , OR	logical gates	Describe the relationships between events
CE	critical event (CE)	A bow-tie is centred on a critical event. A critical event is generally defined as a loss of containment or a loss of physical integrity.
SCE	secondary critical events (SCE)	The critical event such as a pipe failure, leads to secondary critical events (for example, a pool formation, a jet, a cloud, etc.)
TCE	tertiary critical events (TCE)	A secondary critical event leads to tertiary critical events (for example, a pool ignited, a pool dispersion, a jet ignited, etc.)
DP	dangerous phenomena (DP)	Physical phenomena that can cause major accidents such as missiles ejection, overpressure generation, fireball, etc.
ME	major events (ME)	Major events are the significant effects from the dangerous phenomena on targets (human beings, structure, environment, etc.)
V	vulnerability (V)	Any step describing a vulnerability required in order to achieve the attack
AE	attack event (AE)	The attack process in order to exploit a system vulnerability
SB	security breach	A security breach can be caused by the occurrence of the input events
AG	attack goal/top security breach	The main goal of an attack generated from one or several security breaches
V AE	security basic event	Direct cause of a security breach resulting from exploiting a given vulnerability

Paltrinieri, *et al.* (2013) emphasized the importance of systematizing information/risk notions retrieved from past accidents, near-misses, and risk studies to atypical scenario identification. Therefore, the aims of step 3 include i) retrieving risk notions, ii) formulating atypical scenarios, iii) integrating atypical scenarios into the obtained AT-BT models of step 2. This study suggests conducting historical data analysis to retrieve safety and security risk notions. The risk notions can be retrieved from literature, safety-related accident databases, and also security-related accident databases such as IChemE's accident database (Bond, 2002) and the database targeting security-related accidents in the chemical and process industry (Moreno, *et al.,* 2018a). Then, cause-consequence chains of the risk notions can be identified by following the AT-BT model structure and applying the "Why Tree" technique (CCPS, 2003). After the atypical scenarios were formulated according to the cause-consequence chains, the integration of an atypical scenario in an AT-BT model can be conducted.

2.4 Safety & security barrier identification (Step 4)

The outcomes of step 3 are a set of AT-BT models, which can represent the major accident scenarios, including atypical scenarios. Based on the obtained AT-BT models, the associated safety and security barriers can be identified. In order to facilitate barrier identification, a typology of barrier functions should be determined. According to the ARAMIS project, safety barrier functions can be classified into "prevent", "control" and "limit" (De Dianous & Fievez, 2006). The safety barrier can be placed upstream of an event if it prevents this one, or it can be positioned downstream because it controls or limits this event. By contrast, security barriers (physical protection systems) can for instance be classified into "detection", "delay", and "response" (Garcia, 2007). The security barrier can be placed upstream of a security breach if it detects or delays this breach, or it can be placed downstream if it responses to the security breach. Several questions should be asked about each event/security breach in the AT-BT models during the barrier identification process. For instance, "Is there a barrier which

avoids, prevents, or controls this event?" or "Is there a barrier which detects, delays, or responses to this security breach/event?". If yes, the corresponding barriers that play functions as avoiding, preventing, or controlling (detecting, delaying, or responding in case of security barriers) must be placed on the branch in the AT-BT model. At the right-hand of the AT-BT model, which is an event tree, there are sometimes two branches after a barrier. One branch presents the barrier failing with a probability that can be the probability of failure on demand (PFD) of the barrier. Another presents the barrier succeeding with a probability (1-PFD) (De Dianous, & Fievez, 2006). Event/security breach per event/security breach must be examined to ensure a complete barrier identification, and the barrier identification can be done with the help of existing documents related to the production process, instrumentation, physical protection systems, and cyber security systems.

3. Application

In order to show the feasibility of the proposed approach, the safety and security barriers targeting "large breach on shell in liquid phase", which is one of the typical CEs in the MIMAH method, were investigated. The IChemE's accident database (Bond, 2002) and security-related accidents database (Moreno, et al., 2018a) were used to determine the atypical scenarios.

3.1 Investigated accident scenario

A generic fault tree and event tree associated with a large breach on the shell in the liquid phase was presented in the ARAMIS project (De Dianous, & Fievez, 2006), and can be adapted to generate a generic bow-tie with large breaches on the shell in the liquid phase as the critical event. The detailed instructions on how to construct a generic bow-tie can be found in the ARAMIS project report (Andersen et al., 2004). Then, an attack tree analysis was conducted to generate attack trees and attach attack trees to the generic bow-tie for a large breach on the shell in the liquid phase. Finally, an AT-BT model was developed to present the accident scenario associated with the CE and involving all safety and security threats.

3.2 Integrate atypical scenarios

A list of risk notions was retrieved with the help of the IChemE's accident database (Bond, 2002) and security-related accidents database (Moreno, et al., 2018a) as shown in Table 2. Then, cause-consequence chains of the risk notions were developed to present the atypical scenarios and the integration of the atypical scenarios in the AT-BT model was achieved.

Table 2: Risk notions used to identify atypical scenarios

Risk notions	Causes	Safety or security	Risk notions	Causes	Safety or security
fire/equipment damage	lightning strike	safety	explosion/machinery damage	vehicle-borne explosive device	security
leak/malicious operation of the valve	trespasser	security	damage to control system/shutdown failure	cyber attack	security

3.3 Identification of barriers

Based on the obtained AT-BT model with safety and security threats, barrier identification should be conducted for every event branch. The identified safety and security barriers are listed in Table 3 and the corresponding accident scenario is presented in *Figure 4, which is an* AT-BT model.

Table 3: Identified safety and security barriers

| Marks	Barriers	Safety or security	Safety functions	Marks	Barriers	Safety or security	Safety functions
B1	Design protected	Safety	Avoid	B8	Sensors and alarm	Security	Detect
B2	Training on workers	Safety	Prevent	B9	Fence/access delay	Security	Delay
B3	Fire walls	Safety	Prevent	B10	Response force	Security	Response
B4	Fire fighting	Safety	Control	B11	Network security system	Security	Detect/delay
B5	Manual inspection	Safety	Prevent	B12	Manual control	Security	Response
B6	Leak test	Safety	Prevent	B13	Pool bund	Safety	Control/limit
B7	Entry control	Security	Detect	B14	Foam injection	Safety	Control/limit

576
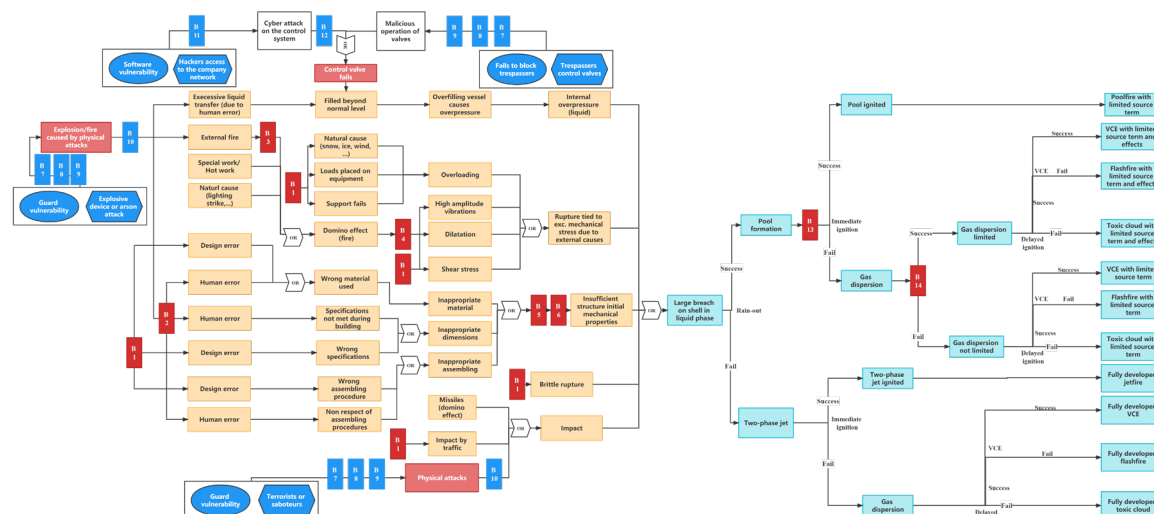
Figure 4: An illustrative AT-BT model with safety and security barriers concerning "large breach on shell in liquid phase"

4. Conclusions

The identification of integrated safety and security barriers in the chemical process industries was investigated in this study. The combination of bow-tie analysis and attack tree analysis has the potential to identify all the safety and security threats with respect to major accident scenarios. An accident database related to safety and security helps to determine risk notions and generate atypical scenarios. After accident scenarios were obtained, a more thorough identification of safety and security barriers can be achieved.

Acknowledgments

References

Abdo H., Kaouk M., Flaus J. M., Masse F., 2018, A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis, Computers & security, 72, 175-195.

Andersen H., Casal J., Dandrieux A., et al., 2004, ARAMIS User Guide. Retrieved from http://safetybarriermanager.com/files/aramis/ARAMIS_FINAL_USER_GUIDE.pdf.

Bond J., 2002, IChemE accidents database, IChemE, Rugby, UK.

Center for Chemical Process Safety (CCPS), Guidelines for investigating chemical process incidents, 2nd ed, New York, AIChE, 2003.

Delvosalle C., Fievez C., Pipart A., Debray B., 2006, ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries, Journal of Hazardous Materials, 130(3), 200-219.

De Dianous V., Fievez C., 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.

Garcia M. L., 2007, Design and evaluation of physical protection systems, Elsevier.

Moreno V. C., Reniers G., Salzano E., Cozzani V., 2018a, Analysis of physical and cyber security-related events in the chemical and process industry, Process Safety and Environmental Protection, 116, 621-631.

Moreno V. C., Guglielmi D., Cozzani V., 2018b, Identification of critical safety barriers in biogas facilities, Reliability Engineering & System Safety, 169, 81-94.

Paltrinieri N., Tugnoli A., Buston J., Wardman M., Cozzani V., 2013, Dynamic procedure for atypical scenarios identification (DyPASI): a new systematic HAZID tool, Journal of Loss Prevention in the Process Industries, 26(4), 683-695.

Villa V., Cozzani V., 2016, Application of Bayesian networks to quantitative assessment of safety barriers' performance in the prevention of major accidents, Chemical Engineering Transactions, 53, 151-156.