



HAL
open science

A new approach that considers cyber security within industrial risk analysis using a cyber bow-tie analysis

H Abdo, Mohamad Kaouk, Jean-Marie Flaus, François Masse

► To cite this version:

H Abdo, Mohamad Kaouk, Jean-Marie Flaus, François Masse. A new approach that considers cyber security within industrial risk analysis using a cyber bow-tie analysis. 2017. hal-01521762

HAL Id: hal-01521762

<https://hal.science/hal-01521762v1>

Preprint submitted on 9 Jun 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A new approach that considers cyber security within industrial risk analysis using a cyber bow-tie analysis

H. ABDO^a, M. KAOUK^a, J-M. FLAUS^a, F. MASSE^b,

^a*Univ. Grenoble Alpes, CNRS, Grenoble INP*, G-SCOP, F-38000 Grenoble, France*

^b*INERIS, Parc technologique Alata BP 2 F-60 550 Verneuil-en-Halatte, France*

Abstract

The introduction of connected systems and digital technology in process industries creates new cyber-security threats that can lead to undesirable safety accidents. Thus, analyzing these threats during risk analysis becomes an important part for effective industrial risk evaluation. However, nowadays, safety and security are assessed separately when they should not be. This is because a security threat can lead to the same dangerous phenomenon as a safety incident. In this paper, a new method that considers safety and security together during industrial risk analysis is proposed. This approach combines Bow-Tie Analysis (BTA), commonly used for safety analysis, with a new extended version of Attack Tree Analysis (ATA), introduced for security analysis of industrial control systems. The combined use of BT and AT provides an exhaustive representation of risk scenarios in terms of safety and security. We then propose an approach for evaluating the risk level based on two-term likelihood parts, one for safety and one for security. The application of this approach is demonstrated using the case study of a risk scenario in a chemical facility.

Keywords: Risk analysis, safety, cyber security, Bow-Tie analysis, Attack-Tree analysis, SCADA.

1. INTRODUCTION

Analyzing risks of industrial and complex systems such as those found in nuclear plants, chemical factories, etc., is of crucial importance given the hazards linked to these systems (explosion, dispersion, etc.) (Abdo and Flaus, 2016b). Quantifying and analyzing these major risks contributes to better

decision making and ensures that risks are managed according to defined acceptance criteria (Arunraj and Maiti, 2007).

Industrial safety risk analysis aims to evaluate undesirable risk scenarios that can lead to major accidents that affect human and the environment. Traditionally, a systematic risk analysis process is made up of three steps: (i) identification of risk scenarios, (ii) likelihood analysis, (iii) effect analysis (Purdy, 2010). Based on these steps, a level of risk will be given to each scenario to see if it is acceptable or not. If not, safety measures should be added to reduce the level of risk to an acceptable level by diminishing the likelihood or the effects. This work considers the first two steps. Identifying a risk scenario aims to explore how an undesirable hazard can be developed starting from causes and ending with the consequences. Likelihood analysis aims to estimate the likelihood of risk scenarios. This estimate can be qualitative or quantitative depending on the available data.

Traditional industries were based on mechanical devices and closed systems (Kriaa et al., 2015). Only safety related risks generated from accidental component failures and human errors need to be addressed during risk analysis of these industries. However, today, industries are influenced by the development of digital technology related to instrumentation and industrial automation (IA). Supervisory Control And Data Acquisition (SCADA) systems are introduced to monitor and control equipment that deals with critical and time-sensitive materials or events. The shift from analog equipment towards technologies has a number of benefits concerning production, but it also presents challenges (Shin et al., 2016). This introduction of automation technology increases the degree of complexity and communication among systems. The use of internet for connecting, remote controlling and supervising systems and facilities has generated a new type of risk causes that related to cyber security. These systems and facilities have become more vulnerable to external cyber attacks. These new security threats can affect the safety of systems and their surrounding environments in terms of people, property, etc. (Johnson (2012); Kornecki and Zalewski (2010)).

The differences and similarities between safety and security are studied by many authors (Kriaa et al. (2015); Firesmith (December 2003)). In general, safety is associated with accidental risks caused by component failures, human errors or any non-deliberate source of hazard, while security is related to deliberate risks originating from malicious attacks which can be accomplished physically (which are excluded in this study) or by cyber means. In addition, causes of accidents related to safety are internal and considered to

be rare events with low frequency. Causes of security accidents can be internal or external (attacks via insider agents or outsiders) and are classified as common events.

Until today, industrial risk analysis does not take into consideration the cyber-security related risks that can affect the safety of the system and lead to major accidents. Systems are designed to be reliable and safe, rather than cyber secure. In recent years, there has been an increasing number of cyber attacks that target critical facilities (e.g., Stuxnet in 2010 and Flame in 2012). According to Dells annual threat report (Dell, 2015), cyber attacks against SCADA systems doubled in 2014. Dell SonicWALL saw global SCADA attacks increase against its customer base from 91,676 in January 2012 to 163,228 in January 2013, and 675,186 in January 2014. Many authors have studied the potential impact of security related threats on the safety of critical facilities and highlight the importance of analyzing safety and security risks together (Kornecki and Zalewski, 2010). Thus, concerns about approaches for industrial risk analysis that consider safety and security together are a primary need.

In this paper we aim to analyze and consider the effect of cyber-security on safety risk scenarios that lead to major accidents. As a result, we propose a new global definition of industrial risk and a risk analysis methodology that covers security and safety. The proposed methodology combines AT for security analysis within BT for safety analysis for an exhaustive representation of a risk scenario. Then, a likelihood analysis approach with two different scales, one for security and another for safety, is introduced. The likelihood of an event is represented in terms of couples (security, safety) in order to see if higher likelihood is related to either security or safety.

It should be noted that in this study we are interested in cyber-security breaches that can lead to major hazards that have effects on human life and the environment and not on confidentiality, integrity or availability of information.

The second part of this paper introduces the concepts of safety risks, security risks and the industrial automation and control system IACS. The third part highlights the global idea behind this study. The fourth part presents the proposed methodology for a combined safety/security industrial risk analysis. Section five presents a case study where the proposed methodology is applied for a hazard scenario in a chemical facility. Finally, section six draws a number of conclusions.

2. Preliminary

In this section, we present the definitions of safety and security related risks (Sections 2.1 and 2.2, respectively). These two definitions will be used to generate a new global definition of industrial risk that covers safety and cyber-security related risks. Section 2.3 introduces the concept and design of the industrial automation system.

2.1. Definition of risks related to safety

In general, safety related risk is described or analyzed as follows (Kaplan and Garrick, 1981):

$$R_{safety} = (S_{e_i}, P_{e_i}, X_{e_i}); i = 1, 2, \dots, N; \quad (1)$$

where

- R_{safety} - safety related risks;
- S_e - scenario description of the undesirable event under study (e) by identifying safety causes of e and its related consequences;
- P_e - likelihood of occurrence of S_e ;
- X_e - severity of consequences of S_e ;
- N - is the number of possible scenarios or undesirable events that can cause damages.

2.2. Definition of risks related to security

In the context of cyber security, risk is analyzed in terms of likelihood and effects of a given threat exploiting a potential vulnerability, and described as follows (Stouffer et al. (2011); Henrie (2013)):

$$R_{security} = ((tv)_j, P_{(tv)_j}, X_{(tv)_j}); j = 1, 2, \dots, M; \quad (2)$$

where

- $R_{security}$ - security related risks;
- tv - scenario description of a security breach: threat or attack (t) exploits a vulnerability v ;

- P_{tv} - likelihood of t exploits v ;
- X_{tv} - severity of consequences if t exploits v ;
- M - is the number of possible attacks.

2.3. Industrial Automation and Control System - IACS

Industrial automation is the use of Industrial Control System (ICS), such as computers and information technologies for handling different processes in an industry. The use of ICS helps in increasing productivity, quality and flexibility in the manufacturing process (Almalawi et al., 2014).

The SCADA system is one of the most important parts of IACS, which refers to an industrial computer system that monitors and controls processes and systems distributed over large geographical areas (Nicholson et al. (2012); Cherdantseva et al. (2016)). The principal function of SCADA is acquiring the data from devices such as valves, pumps, etc. and providing control of all of these devices using a host software platform (Li2 (2016); Schneider Electric (2012)). The monitoring of the process is provided using a remote method of capturing data and alarm events, where instruments can be regulated and turned on and off at the right time. The SCADA system also provides more functions such as displaying graphics, alarming facilities and storing data. Malfunctions of SCADA may cause undesirable consequences ranging from financial loss to environmental damages (Patel et al., 2005).

SCADA systems throughout the world supervise and control electric grids, power plants, water systems, chemical plants, pipelines, manufacturing, transportation, and other physical processes (Weiss, 2016). Figure 1 shows the basic hierarchy and architecture of an IACS, which is classified into five distinct levels. SCADA operates on levels 1 and 2. The different levels of IACS are presented as follows:

- level 0 - field instruments: the lowest level of the control hierarchy which includes to sensors, pumps, actuators, etc. that are directly connected to the plant or equipment. They generate the data that will be used by the other levels to supervise and control the process;
- level 1 - control level using Programmable Logic Controller (PLC): PLC is an adapted industrial digital computer that controls the manufacturing processes. It is linked to the field instruments, and to the SCADA host software using a communication network;

- level 2 - SCADA: monitor, maintain and engineer processes and instruments;
- level 3 - MES: this level is responsible for process scheduling, material handling, maintenance, inventory, etc;
- level 4 - ERP: the top level of the industrial automation which manages the whole control or automation system. This level deals with commercial activities including production planning, customer and market analysis, orders and sales, etc.

Industrial communication networks are most prominent in IAS which represents the link that relays data from one level to the other in order to provide continuous flow of information. This communication network can be different from one level to another.

The SCADA system represents the most sensitive and targeted part of the industrial automation in terms of cyber security. Cyber attacks on the SCADA system are classified into three different categories: (i) hardware, (ii) software, (iii) communication network.

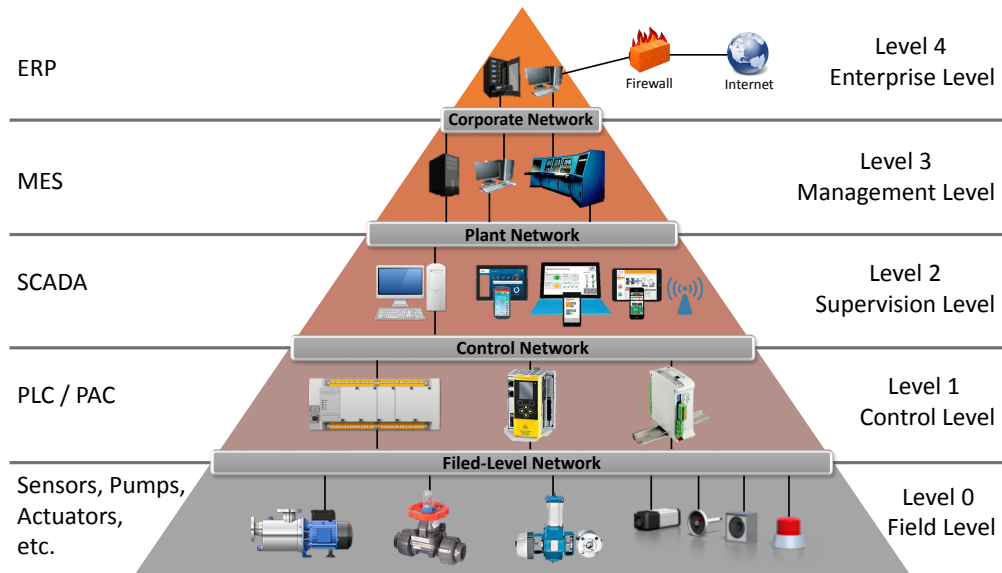


Figure 1: Components and architecture of IAS

3. General idea

This section generalizes the global idea behind the methodology proposed in this paper. This study first contributes a new global definition of industrial risk that covers safety and security as presented in Figure 2. Risk is described in terms of a triplet as follows:

$$R = (S_{(tv,e)_i}, P(se, sa)_i, X_{(tv,e)_i}); i = 1, 2, \dots, N; \quad (3)$$

where

- $S_{(tv,e)}$ - Scenario description of the undesirable event (e) that can result from safety incidents or/and security breaches (tv: see the definition of security risk in Section 2.2);
- $P(se, sa)$ - likelihood of occurrence of $S_{(tv,e)}$, where se and sa are respectively related to security and safety;
- $X_{(tv,e)}$ - Severity of consequences of $S_{(tv,e)}$;
- N - is the number of possible scenarios or undesirable events that can cause damages.

This paper proposes a methodology to analyze risk based on three main steps:

- ✓ identifying risk scenarios: we propose a methodology that combines BT with adjusted AT to identify the safety and security related causes and consequences of the undesirables events being studied. BT analysis is one of the most popular methodologies used in probabilistic safety analysis (Abdo and Flaus, 2016a). AT is widely used to represent and analyze risk scenarios related to cyber security. However, combining BT and AT analyses can be effectively used for an integrated safety/security assessment of critical systems. This methodology identifies and considers all safety incidents and security threats that can lead to the same undesirable phenomenon generating damages.
- ✓ likelihood evaluation: as BT and AT offer likelihood evaluation for safety and security risk scenarios, respectively, then the combined ATBT offers the same option for a safety/security risk scenario. But, as we

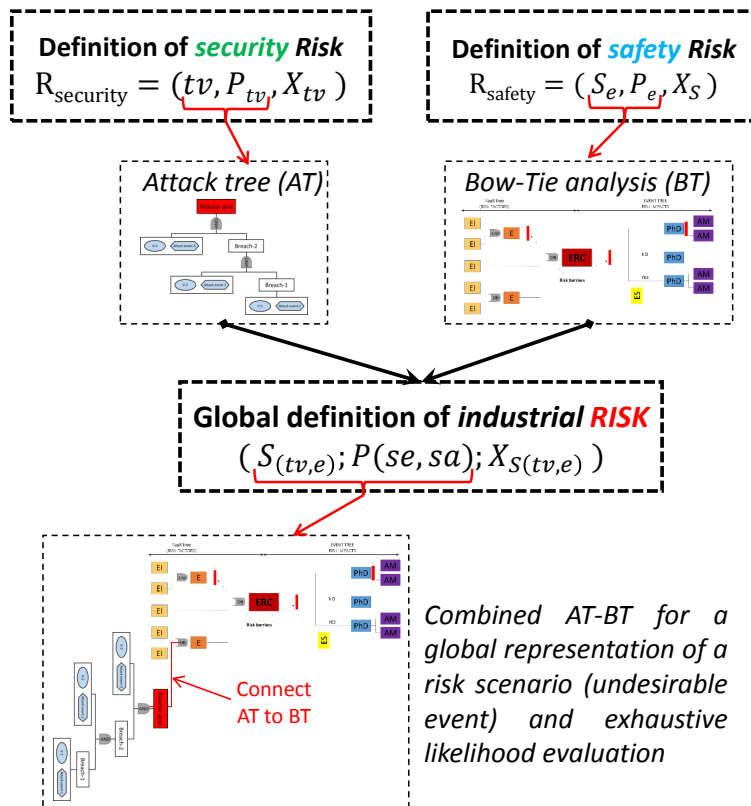


Figure 2: Global definition of risk

said, sources of risk for safety and security are of different nature. Usually the likelihood of cause events related to safety are very low in comparison to the likelihood of security related cause events. For this reason, different likelihood scales, one for safety and another for security are defined to characterize the likelihood of input events. This differentiation helps in identifying the sequences of events (minimal cut sets) that are purely related to safety, security or to both. The resulting output of different types of cut sets offers richer information for decision making. In the rest of this paper we are going to prove the importance of considering safety and security together and show that purely security risk sequences should be treated first.

- ✓ severity of consequences evaluation: this step aims to quantify the loss in terms of system assets, human life and environmental damage if the undesirable event has occurred. This part is not considered in this paper.

The proposed approach will provide a deep, exhaustive analysis on safety/security for industrial risk scenarios in a given facility.

4. Methodology for combined safety/security risk analysis

4.1. Introduction

In this section, we will outline the proposed methodology for a combined safety/security industrial risk analysis. As we are going to prove that the occurrence of safety related events, security related events or both together can lead to the same undesirable accident, the idea then is to combine the BT for safety analysis and the AT for security analysis in order to provide a complete modeling of a risk scenario. A risk scenario will be a combination of all expected security and safety events that can result in the undesirable event being studied. This modeling will be the first step in our methodology and it is conducted as presented in Section 4.2.

Next, we explain the second step that aims to evaluate a risk scenario in term of likelihood as presented in Section 4.3. But, due to the difference in nature between safety and security related events, they will be characterized separately for likelihood analysis.

Figure 3 shows the framework to apply the proposed methodology.

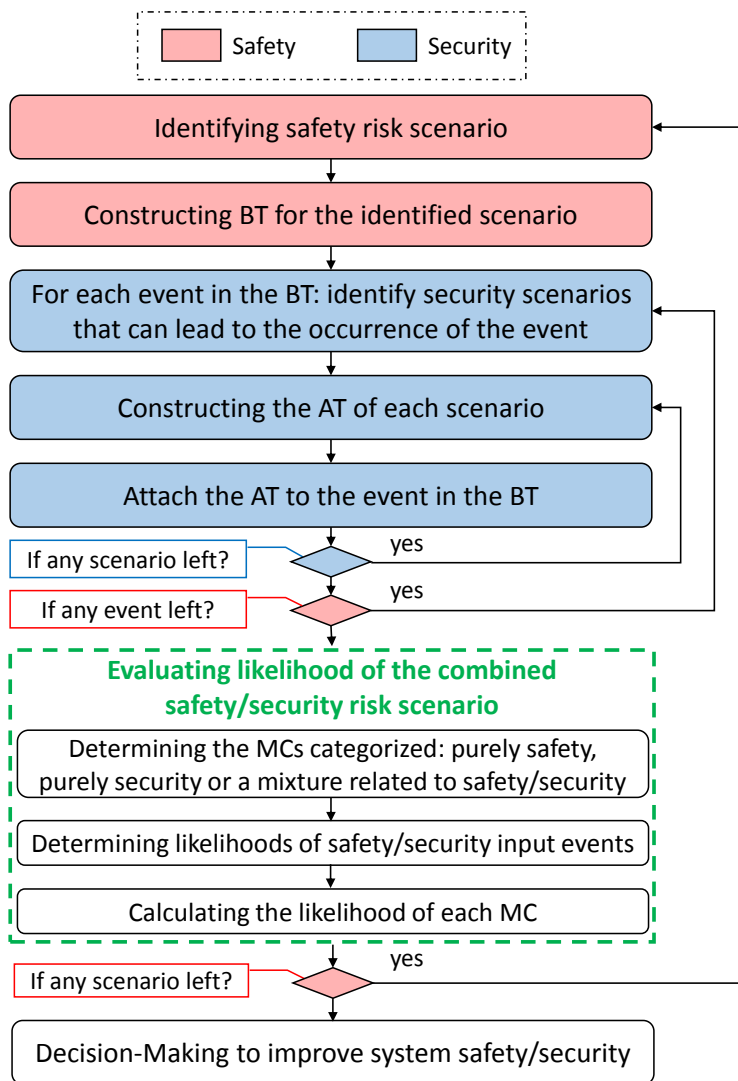


Figure 3: Framework of the proposed approach for safety/security risk analysis

4.2. Step-1: representation of a risk scenario

In this section, first we will present the concept of BT analysis and introduce a new extended AT as depicted in Sections 4.2.1 and 4.2.2, respectively. Then, we show how ATs can be integrated within BT for richer combined safety/security representation of a risk scenario (see Section 4.2.3).

4.2.1. Safety risk analysis using Bow-Tie analysis

Bow-Tie analysis is a very prominent method to identify and analyze the likelihood of risk (Ferdous et al., 2012). It presents a combination between fault tree analysis (FTA) and event tree analysis (ETA). FTA and ETA respectively describe the relationships between the undesirable event, its causes and its consequences for a systematic representation of hazard. These relationships between trees' nodes are represented using the logical AND/OR gates. BT uses different types of nodes to model a risk scenario. The definition of each is detailed in Table 1.








Shape	Signification	Definition
	Basic event (BE)	Direct cause of a physical integrity
	Event	Physical integrity caused by the occurrence of basic events
	Undesirable event	The unwanted event such as a loss of containment, etc.
	Secondary event (SE)	Characterizes the source term of an accident, such as ignition
	Dangerous phenomenon	Physical phenomenon that can cause major accidents, explosion, dispersion, fire
	Risk barrier	Measures taken place to reduce the likelihood of undesirable event and the effects of accidents
 	Logical gates	Describe the relationships between events

Table 1: Abbreviations, significations and definitions of elements listed in the Bow-Tie diagram

4.2.2. Security risk analysis using a new extended Attack Tree

The “Attack Tree” technique as initially presented by Schneier (1998) is a graph that describes the sequence of steps in order to perform an attack. It represents an attack against a system in a tree structure (Fovino and

Masera, 2006). The root (main event) of the tree is the goal of an attack. This root is connected to intermediate and starting (leaf nodes) events in order to represent the different ways to achieve the attack.

Traditional AT presents some limitations to be used for risk analysis. Showing just the steps that an attacker or a team of attackers follow to achieve a particular goal is not enough to understand the system's weaknesses. On the other hand, traditional AT does not present all the information needed to evaluate the likelihood of a successful attack on the target system. Thus, mapping information on the target system such as vulnerabilities in addition to attack steps is essential for an effective security risk analysis using AT.

In this study, we will propose an extended version of attack tree with new modeling in order to characterize a security risk scenario. This extended version allows the consideration of significant information such as the target system vulnerabilities to suit the security risk analysis perspective. The AT's leaf nodes (security input events) are represented by a combination of attack events and vulnerabilities. This representation help the decision makers understanding the system's vulnerabilities (or weaknesses) and the different types of attacks that can be contacted in order to provide the right countermeasures.

As in BT, the AND/OR gates are used to link the tree's events and define the relationship between them. Table 2 presents the term, shape and definition of each event used to model a security scenario.

It should be noted that different attack events may be needed to exploit a specific vulnerability and vice versa. In these cases, the forms of the basic security events are presented in Figure 4.

The goal of this new AT is to model how attackers can exploit system vulnerabilities in order to cause damage. Figure 5 shows in a schematic way the reality behind how attackers target a system by exploiting its vulnerabilities. Here, attackers should run three different attacks to exploit three different vulnerabilities in order to achieve their goal. This attack can be modeled by the proposed extended AT as shown in Figure 6. Figure 6 shows the breach layers to attain the attack goal. This concept of layers would help propose the right countermeasure in the right place.

4.2.3. Combined ATBT analysis

This step aims to combine AT and BT analyses for a combined safety/security industrial risk analysis. The goal of this combination is to provide a com-

	shape	Signification	Definition
Input events		Vulnerability	Any step describing a vulnerability required in order to realize the attack
		Attack	The attack process in order to exploit a system vulnerability
		Security basic event	Direct cause of a security breach resulting from exploiting a given vulnerability
		Intermediate/top event	A security breach caused by the occurrence of input events

Table 2: Description of events used for representing an attack scenario

plete representation of risk scenarios by plotting on the same scheme safety and security events that can lead to the same undesirable events. Additionally, integrating ATs within BT analysis can help in understanding how attackers can exploit systems' weaknesses in order to cause damages besides non-deliberate incidents.

This step is conducted as follows:

1. construct BT for the chosen undesirable event being analyzed;

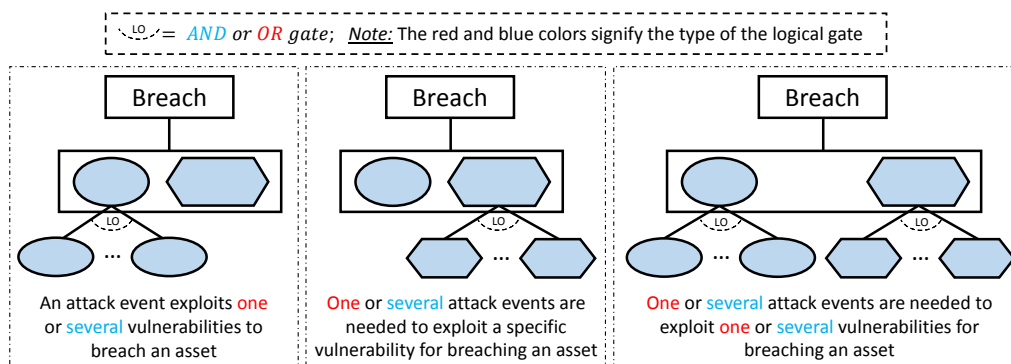


Figure 4: The different form of a security basic event

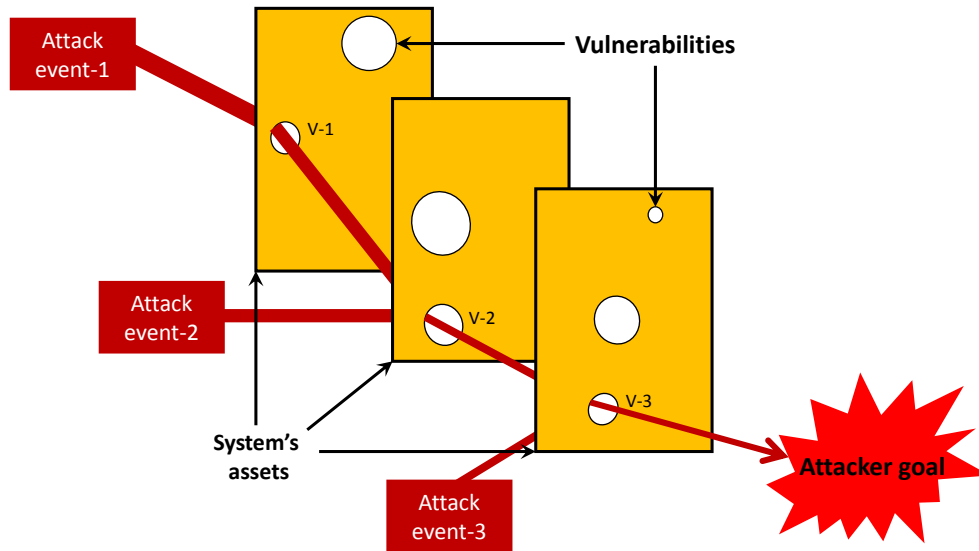


Figure 5: How attackers exploit system vulnerabilities in order to cause damages

2. for each safety event in BT, identify if there are security incidents that can lead to the occurrence of this event. If yes, construct the AT and attach its goal to the corresponding event (see Figure 7). This means that this event can occur due to accidental (safety) or deliberate (security) incidents.

Finally, a cyber security BT (ATBT) is obtained for the undesirable event being studied.

4.3. Step-2: likelihood evaluation

This section proposes an approach for conducting a qualitative likelihood analysis of a risk scenario. This likelihood analysis methodology is made up of three main steps: (i) determining the minimal cut sets to understand the structural weaknesses of a system, (ii) characterizing likelihoods of input events using a two-levels representation and (iii) quantify the likelihood of each MC to prioritize the system's weaknesses (see Sections 4.3.1, 4.3.2 and 4.3.3, respectively).

It should be noted that we are required to characterize likelihood of safety and security events separately because they are intrinsically different and the control in terms of safety or security barriers should be managed independently of the two safety and security aspects.

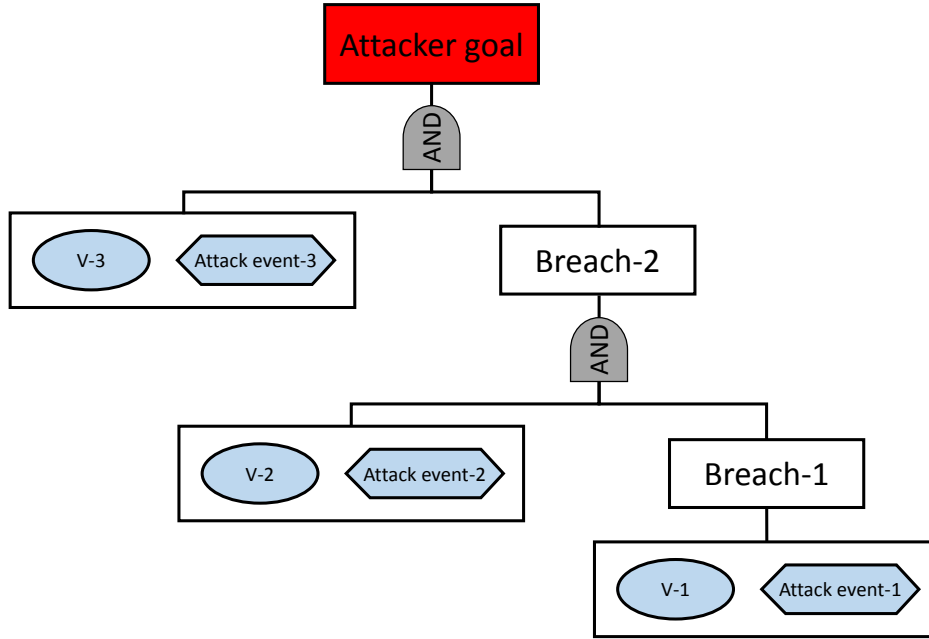


Figure 6: Example of the structure of the proposed attack tree

4.3.1. Determining minimal cut sets

Finding out the MCs represents the first step of likelihood evaluation in our approach. A MC is the smallest combination of input events which causes the occurrence of the undesirable event. MCs present the different ways in which component failures or events alone or in combination with others make the occurrence of the top event (minimal cut sets with one or several components or events). Determining the MCs is very useful to discover the weak point in our system. In this study, the MCs are obtained using rules of boolean algebra (Yuanhui, 1999).

We separate between three types of minimal cuts:

- purely related to security: all events of the MC are due to deliberate attacks;
- purely related to safety: the MC does not contain any security related event;
- related to a mixture of both security and safety: accidental and deliberate causes exist in the MC.

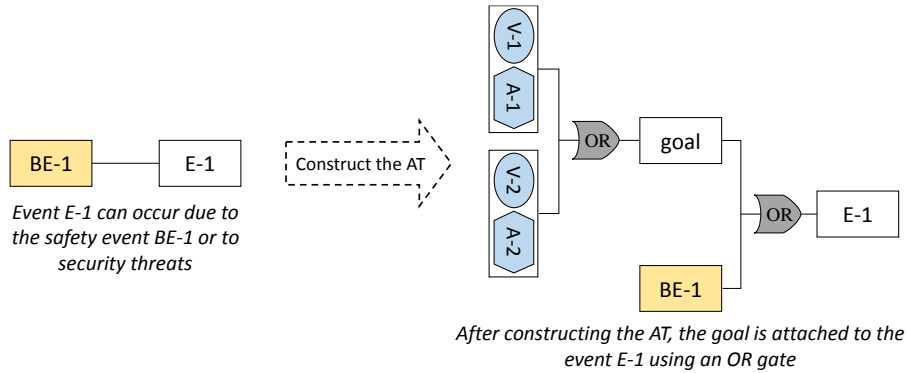


Figure 7: Example of how we attach an AT to its corresponding event in BT

The importance of this differentiation between types of MCs is to discover the system’s weaknesses where a pure security MC represents a weak point due to the high likelihood of occurrence of security causes. This reasoning will be detailed and demonstrated in the rest of this paper.

4.3.2. Characterizing likelihoods of occurrence of input events

In safety, the likelihood of occurrence is the probability (expected frequency) or possibility of something happening. But when we talk about security, the likelihood of occurrence is the probability that a given threat is capable of exploiting a vulnerability (or set of vulnerabilities).

Likelihood analysis can be qualitative or quantitative depending on the type of available data. This data is either quantitative derived from historical incident or qualitative based on experts’ elicitations. Because of the difficulties in estimating quantitative likelihood of occurrence of an attack or an accidental cause, a qualitative scale is used. The advantage of the qualitative methodology is its simplicity of applying and understanding by the relevant personnel.

As we presented in the beginning of this section, there are different concepts to define likelihood related to safety and security. Due to the deviation in the likelihood translation, high likelihood in safety is different than high likelihood in security regarding the number of observed safety and security incidents (we see cyber attacks on critical facilities every day). Two different scales L_s : *security* and L_f : *safety* of respectively five and six levels are proposed. The first level of each scale represents an undefined value (likelihood equals zero) in order to specify if an event is purely related to safety or

Qualitative scale	Safety Level	Designation	Quantitative meaning
Likelihood	N/A	Not Applicable: event is purely related to security, not safety	0
	E	Very unlikely: event that is practically impossible, very low chance of happening	10^{-5}
	D	Unlikely: Low chance of occurrence even if we consider several systems of the same type, but has to be considered as a possibility	10^{-4}
	C	Moderate: may occur during total operational life if considering several systems of the same type	10^{-3}
	B	Likely event: may occur during total operational life of a system	10^{-2}
	A	Very likely event: can frequently occur (several times) during operational life	

Table 3: Qualitative scale to characterize the frequency of input safety events

security. Thus, each event is characterized by couples (L_s, L_f) .

Based on this likelihood representation in terms of couples, we can differ between three different types of events presented as follows:

- events that are purely related to safety with likelihood $(N/A, L_f)$ for each event;
- events that are purely related to cyber-security with likelihood $(L_s, N/A)$ for each event. If the event is a security cause (basic event in terms of two parts), L_s will depend on the vulnerability level and the technical difficulties of conducting the attack as we will detail in Section 4.3.2.2;
- events (intermediate events) related to both safety and security with likelihood (L_s, L_f) for each event.

4.3.2.1 Characterizing likelihood for safety risk events

Likelihood characterization here aims to determine the likelihood of occurrences of input events (BEs and SEs in BT) and the likelihood of failures of risk barriers according to a specific scale. The same scale used by INERIS for safety analysis is used in this study (INERIS, 2015) as presented in Table 3.


Qualitative scale	Vulnerability Level	Designation
exploitability 	1	Easy (E): No countermeasures are presented
	2	Medium (M): Countermeasures are presented
	3	Hard (H): Countermeasures existed with continuous review and improvements.

Table 4: Qualitative scale to characterize the vulnerability levels

4.3.2.2 Characterizing likelihood for security risk events

In the context of a security risk analysis, the likelihood of occurrence depends on the capability that a given threat (or set of threats) exploiting a potential vulnerability (or set of vulnerabilities). Thus, the likelihood is a function of the difficulty of performing a needed attack to exploit a vulnerability, and the level of vulnerability depending on the existing counter measures. Two different criteria are considered to determine the likelihood of a security initial event presented as follow:

- Vulnerability level: given to a vulnerability in the ATBT to represent how easy or hard exploiting this vulnerability depending on the existing countermeasures. Table 4 shows the three different levels proposed to evaluate this criterion;
- Technical difficulty of conducting an attack: given to an attack event to show the needed level of expertise or difficulty to conduct the attack. Table 5 presents the levels of difficulty of an attack inspired from (Byres et al., 2004).

These two criteria should then be combined in order to provide a likelihood for the security initial (or basic) events. The difficulty of the attack is combined with the vulnerability levels as presented in Table 6. Four different security likelihood levels in addition to the N/A level are proposed to represent the combination. The definition of each security likelihood level is presented in Table 7. From Table 7, we can note that likelihood levels of security events are different from those of safety events (Table 3).

Qualitative scale	Difficulty Level	Designation
Technical difficulty of an attack	1	Trivial (T): Little technical skill required
	2	Moderate (M): Average cyber hacking skills required
	3	Difficult (D): Demands a high degree of technical expertise
	4	Very difficult (VD): Beyond the known capability of today's best hackers

Table 5: Qualitative scale to characterize the difficulty of conducting an attack

Likelihood levels		Technical difficulty of an attack			
		T	M	D	VD
Exploitability	E	4	4	3	2
	M	4	3	2	1
	H	2	2	1	1

Table 6: Combining attack difficulty levels with the vulnerability levels to determine the likelihood of security input events

Qualitative scale	Security Level	Designation
Likelihood	N/A	Not Applicable: Event is purely related to safety, not security
	1	Low: High unlikely to occur, attack is hard to perform, existence of effective security measures
	2	Moderate: Possibility to occur, but existed security measures reduce the likelihood of occurrence
	3	High: Likely to occur, limited countermeasures are presented
	4	Strong: Is almost certain to occur, system is an easy target

Table 7: Qualitative scale to characterize the likelihood of input security events

4.3.3. Calculating the likelihoods of MCs

This step aims to prioritize the system weaknesses by calculating the likelihood of each MC in order to help decision makers propose the right countermeasure where MCs with highest likelihood should be treated first.

Calculating the likelihood of an MC only needs the AND gate to be solved. AND gate signifies that the output event occurs if all its input events have occurred. Since qualitative scales are used for safety and security likelihood characterization, the min rule is used to solve the AND gate as presented in Eq 4 (INERIS, 2015).

$$L(AND_{out}) = \min[L(E_1), \dots, L(E_n)] \quad (4)$$

where $L(E_1), \dots, L(E_n)$ are the likelihoods of occurrence attached to E_1, \dots, E_n , respectively.

Finally, for each MC, the two determined likelihoods for safety and security should be taken together to provide one meaningful likelihood to be used for prioritizing MCs and for risk evaluation using the likelihood-consequence risk matrix (which is not discussed in this paper). Table 8 presents the overall scale regarding the proposed safety and security scales. This overall scale defines five different qualitative expressions from low (L) to very high (VH).

It should be noted that this overall-likelihood can not replace the double part likelihoods ($L_{security}, L_{safety}$) which is important for decision-making and

Likelihood levels		Likelihood of safety events					
		E	D	C	B	A	N/A
Likelihood of security events	N/A	VL	L	M	H	VH	
	4	VL	L	M	H	VH	VH
	3	VL	L	M	H	H	H
	2	VL	L	M	M	M	H
	1	VL	L	L	L	L	M

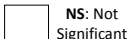
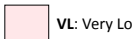

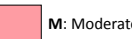
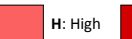
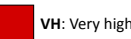
 NS: Not Significant	 VL: Very Low	 L: Low	 M: Moderate	 H: High	 VH: Very high
---	--	--	---	--	---

Table 8: Analysis scale - Overall likelihood

in choosing the right countermeasure, because decision makers should know if the high likelihood is related to safety, security or to both.

This approach will be illustrated in the next section and applied to an overheating scenario in a chemical reactor.

5. Case study

5.1. Description

This case study illustrates the implementation of the proposed approach, which can be applied in any industrial context. The case study concerns an industrial site of a propylene oxide polymerisation reactor (Abdo and Flaus, 2015). The reactor runs a high exothermic chemical reaction at high pressure. It is located in a manufacturing site located south of a small town. Risks associated with the operation of the reactor are of high consequences.

In a systematic representation of the reactor, a production system, a cooling system and a power supply are interacting in order to perform the operation under normal conditions (regulated temperature and pressure). Components of these systems (valves, pumps, etc.) are controlled by PLCs and supervised by a SCADA system. The information collected by the SCADA system is accessible by all the site managers from their offices using wireless remote control. The manager of the utility can control the facility using its tablet or smart phone via internet. Controlling the process via internet would

allow the manager to handle the situation from where he/she is before it is too late, rather than waking up at midnight racing to the plant to handle the situation. Figure 8 shows the architecture of the system under study.

The reactor is used in batch mode to run a chemical reaction in order to produce a product C from two reactives A and B. The temperature of the reaction is regulated with industrial water. At the end of the reaction, after the mixture A,B is completely transformed. The output C is transferred toward another unit in the facility by opening the valve XV33021. This process is controlled by PLC1.

The cooling system E33040 receives cold industrial water as input which is used to cool down the content of reactor R33030 using a double jacket. The temperature of the cooling system and the water flow rate are measured by the sensor TI33061 and TI33062, respectively. The data collected by these two sensors is sent to PLC2 which regulates the water flow rate by controlling P1, P2, CV33063 and XYSV33027. Under normal conditions, the pressure in the reactor is less than six bars when the temperature is controlled under 120 °C. An automated safety valve PSV33009 opens in the case of over-pressure to limit the pressure to 10 bars. After PSV33009 opened, the exhausted gases are cleaned by scrubber.

5.2. Application

In this case study, the most likely undesirable scenario with the highest consequences due to overheating/overpressure is considered for risk analysis. This scenario can be generated after the occurrence of deliberate attacks or accidental errors. Overheating occurs if the temperature and pressure exceed the threshold. Abnormal increase in temperature can be due to (1) an abnormal response of the cooling system, or (2) when the agitator breaks down, or (3) an excessive loading of the reactor. (1) and (3) can be initiated by deliberate attacks on the control system, or by accidental accidents due to mechanical breakdowns or human errors. The rise in pressure is limited by an automated safety valve. If this does not accomplish its mission, it would entail the explosion of the reactor.

The two first steps for risk analysis (risk identification and likelihood evaluation) using the proposed methodology are applied on the overheating scenario as depicted in Sections 5.2.1 and 5.2.2, respectively.

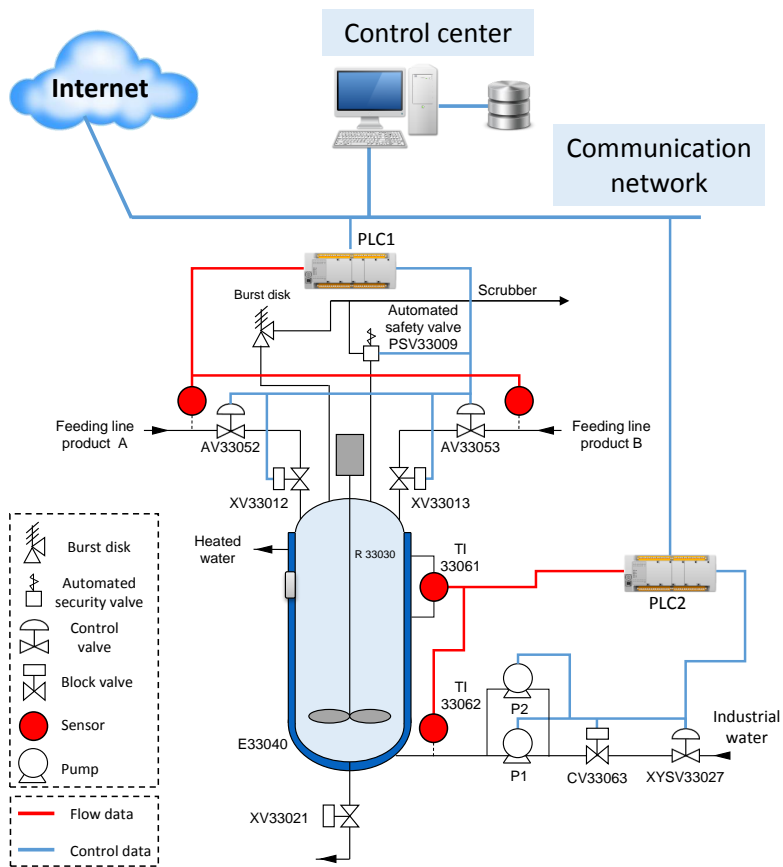


Figure 8: The chemical reactor with its SCADA system structure

5.2.1. Step-1: Constructing ATBT for safety/security analysis

This step contains two sub-steps as presented in the proposed methodology:

1. constructing the BT for safety analysis: Figure 9 presents the BT for the undesirable event under study. We investigated nine safety related basic events that are the causes of the overheating in the reactor.
2. constructing ATs for security analysis: two events in BT can occur due to security breaches. The first is the failure of the automated safety valve due to an attack on the hardware. The second is error in the cooling system after gaining unauthorized access on the SCADA system by attacking computer software or the communication network as shown in Figure 10. We also modeled the Stuxnet virus to examine the impact of computer worms on industrial control systems and to present the utility of the approach. The different operations (attacks) and vulnerabilities Stuxnet exploits are modeled in Figures 11, 12, 13.

5.2.2. Step-2: Likelihood evaluation

The ATBT shown in Figure 9 yields to 61 MCs. These MCs are divided into 27 that are purely related to security, 7 that are purely related to safety and 27 that are related to mixture safety/security.

Experts in the field are asked to characterize likelihoods of safety and security basic events. The characterized likelihoods in terms of couple $(L_{security}, L_{safety})$ are drawn beside the basic events in the ATBT (see figures). Then, we estimate the safety/security likelihood of each MC with the overall likelihood as shown in Table 9.

5.3. Discussion and improvement

As shown in Table 9, the MCs ranked high (H) and (VH) are purely due to cybersecurity. This reveals the importance of considering security risks during safety risk analysis. However, the presence of a safety event in an MC will lead to less likelihood of occurrence. We can clearly see that between MC-25 and MC-59 where their attached likelihoods are equal to VH and L respectively, MC-59 is of less likelihood because it contains the accidental event BE-9.

For more details, a burst disk is added which represents a mechanical component (no security breaches are related) as improvement for the process.

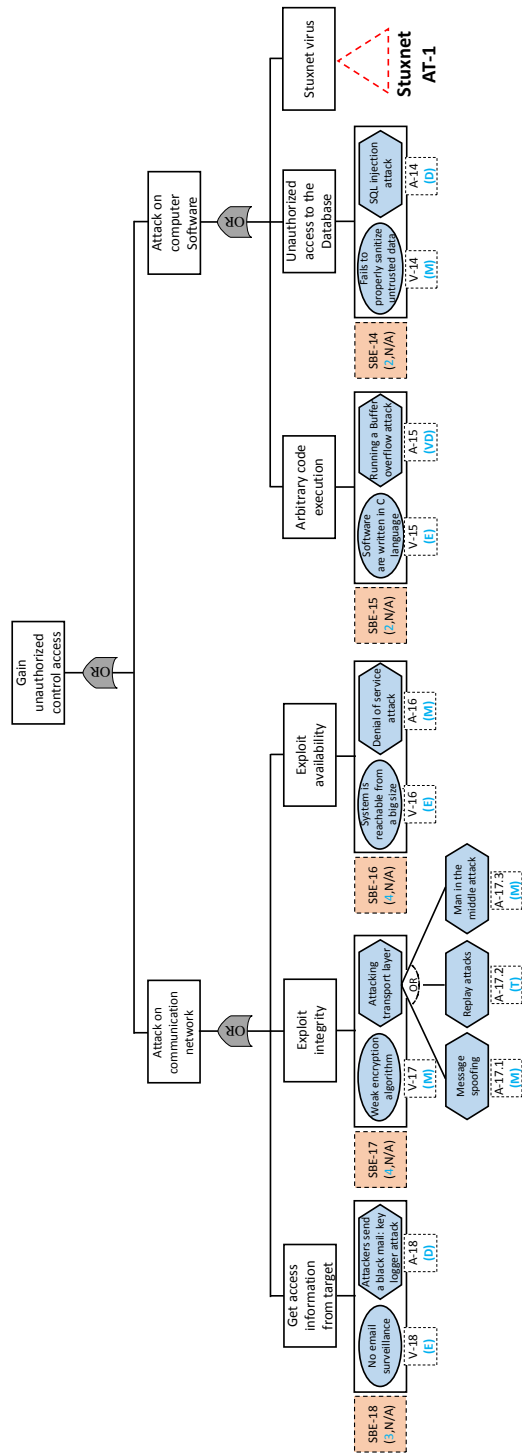


Figure 10: AT for the goal: gain unauthorized access to SCADA
26

	MCS	Likelihood	Level		MCS	Likelihood	Level
1	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; SBE-19	(1, N/A)	L	32	BE-6, BE-9	(N/A, D)	L
2	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; SBE-19	(1, N/A)	L	33	BE-7, BE-9	(N/A, D)	L
3	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; SBE-19	(1, N/A)	L	34	BE-8, BE-9	(N/A, D)	L
4	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; SBE-19	(1, N/A)	L	35	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; BE-9	(1, D)	L
5	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; SBE-19	(3, N/A)	H	36	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; BE-9	(1, D)	L
6	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; SBE-19	(3, N/A)	H	37	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; BE-9	(1, D)	L
7	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; SBE-19	(3, N/A)	H	38	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; BE-9	(1, D)	L
8	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; SBE-19	(3, N/A)	H	39	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; BE-9	(3, D)	L
9	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; SBE-19	(3, N/A)	H	40	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; BE-9	(3, D)	L
10	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; SBE-19	(3, N/A)	H	41	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; BE-9	(3, D)	L
11	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; SBE-19	(3, N/A)	H	42	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; BE-9	(3, D)	L
12	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; SBE-19	(3, N/A)	H	43	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; BE-9	(3, D)	L
13	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; SBE-19	(2, N/A)	M	44	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; BE-9	(3, D)	L
14	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; SBE-19	(2, N/A)	M	45	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; BE-9	(3, D)	L
15	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; SBE-19	(2, N/A)	M	46	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; BE-9	(3, D)	L
16	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; SBE-19	(2, N/A)	M	47	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; BE-9	(2, D)	L
17	SBE-3; SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; SBE-19	(1, N/A)	L	48	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; BE-9	(2, D)	L
18	SBE-3; SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; SBE-19	(2, N/A)	M	49	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; BE-9	(2, D)	L
19	SBE-3; SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; SBE-19	(2, N/A)	M	50	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; BE-9	(2, D)	L
20	SBE-3; SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; SBE-19	(2, N/A)	M	51	SBE-3; SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; BE-9	(1, D)	L
21	SBE-14; SBE-19	(2, N/A)	M	52	SBE-3; SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; BE-9	(2, D)	L
22	SBE-15; SBE-19	(2, N/A)	M	53	SBE-3; SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; BE-9	(2, D)	L
23	SBE-16; SBE-19	(4, N/A)	VH	54	SBE-3; SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; BE-9	(2, D)	L
24	SBE-17(V-17, A-17.1); SBE-19	(3, N/A)	H	55	SBE-14; BE-9	(2, D)	L
25	SBE-17(V-17, A-17.2); SBE-19	(4, N/A)	VH	56	SBE-15; BE-9	(2, D)	L
26	SBE-17(V-17, A-17.3); SBE-19	(3, N/A)	H	57	SBE-16; BE-9	(4, D)	L
27	SBE-18; SBE-19	(4, N/A)	VH	58	SBE-17(V-17, A-17.1); BE-9	(3, D)	L
28	BE-1, BE-9	(N/A, D)	L	59	SBE-17(V-17, A-17.2); BE-9	(4, D)	L
29	BE-2, BE-3, BE-9	(N/A, D)	L	60	SBE-17(V-17, A-17.3); BE-9	(3, D)	L
30	BE-4, BE-9	(N/A, D)	L	61	SBE-18; BE-9	(4, D)	L
31	BE-5, BE-9	(N/A, D)	L				

Purely security related MC
Mix related MC
Purely safety related MC

Table 9: The identified MCs for the scenario under study

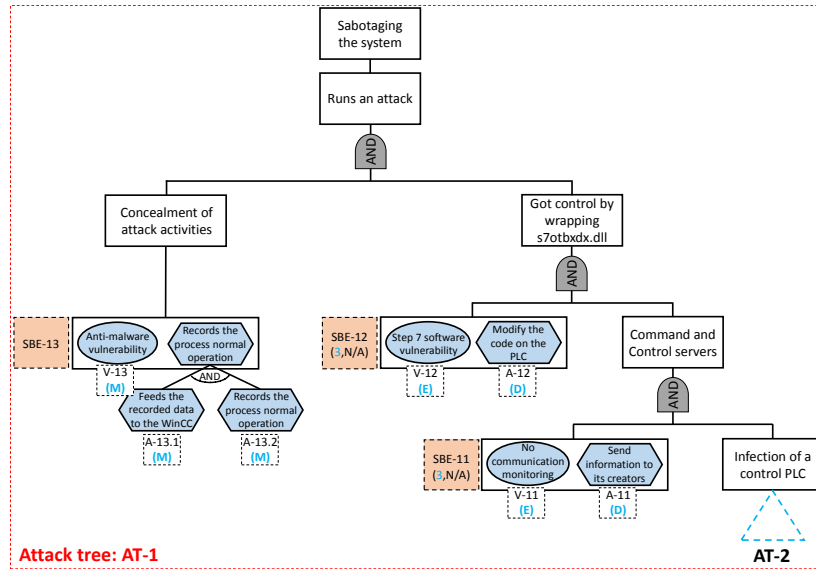


Figure 11: The top objective of Stuxnet

The re-determination of MCs shows that there is no MC that is related to pure security. Table 10 shows the re-determined MCs with their re-estimated likelihoods. The introduced improvement diminishes the likelihoods into the lowest level. Thus, the presence of a mechanical failure (safety event) in a cut set will insure the prevention of malicious attacks and vice versa. For these reason, safety and security being treated together will lead to a better risk analysis and effective decision making.

6. Conclusion

The use of technology in critical facilities exposes systems' safety to security related threats. These threats are due the use of internet, standardized protocols and electronic components for connectivity and remote controls.

Nowadays, existing approaches for industrial risk analysis ignore cybersecurity. In light of security threats, there is an urgent need for complete and effective safety risk analysis. That is why this paper proposes an approach that integrates ATs with BT analysis for a combined safety and security industrial risk analysis. Bow-Tie analysis is used for analyzing safety accidents. A new concept of Attack Tree is introduced to consider potential malicious attacks that can affect the system's safety. The steps of combining AT within

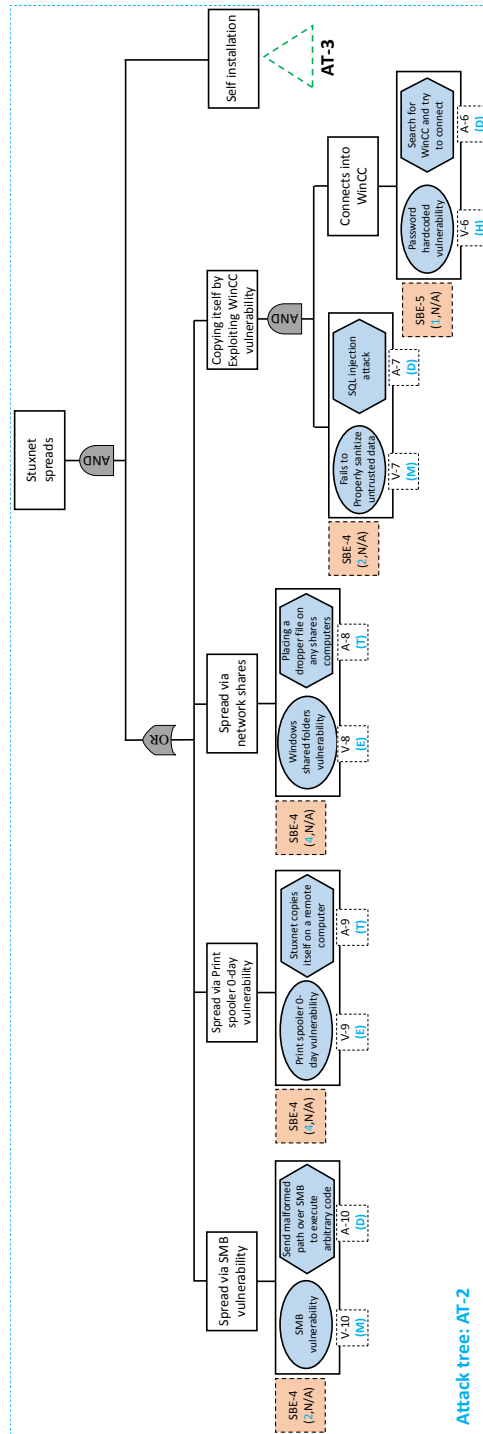


Figure 12: Attack tree of the “spreading of Stuxnet”

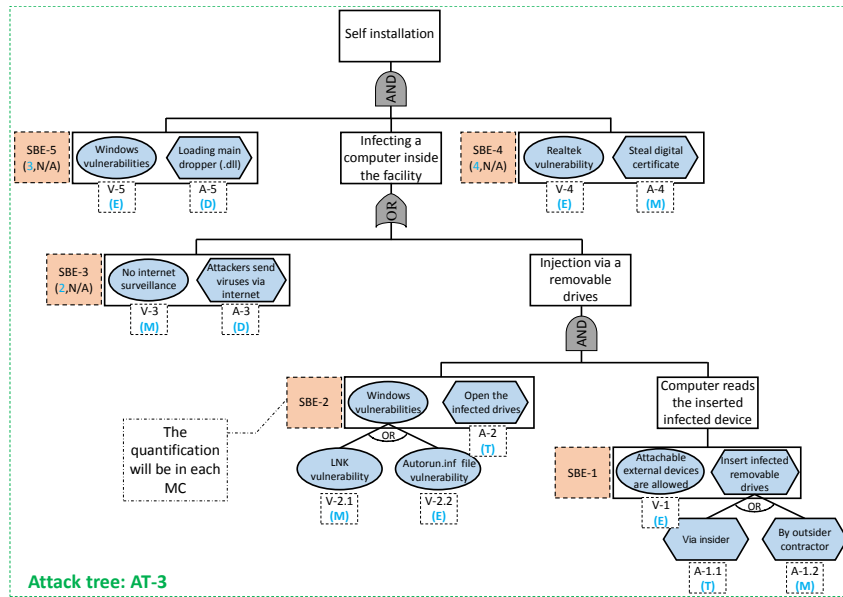


Figure 13: Attack tree of “Stuxnet self installation”

Scenario number 59: SBE-17(V-17, A-17.2); BE-9

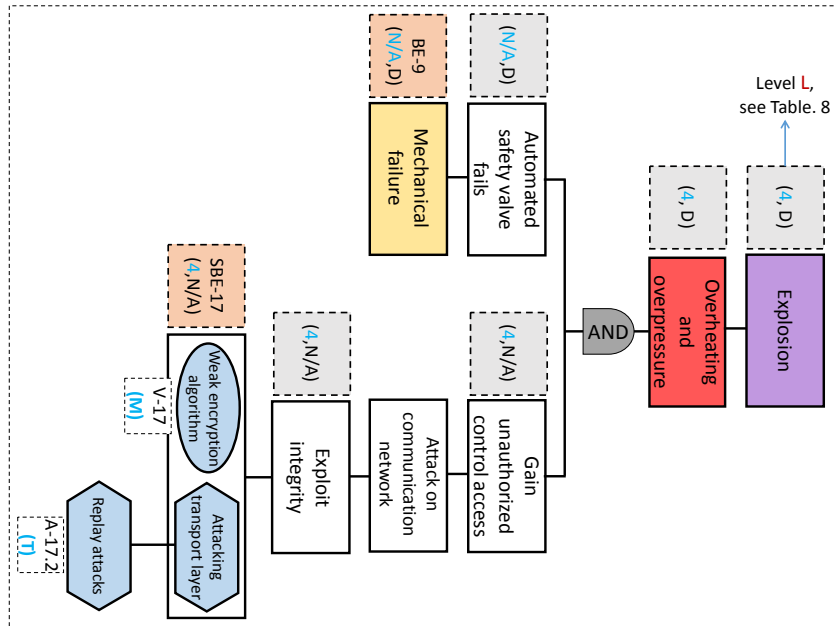


Figure 14: Calculating the likelihood of MC number 59

	MCS	Likelihood	Level		MCS	Likelihood	Level
1	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(1, E)	VL	32	BE-6, BE-9; BE-10	(N/A, E)	VL
2	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(1, E)	VL	33	BE-7, BE-9; BE-10	(N/A, E)	VL
3	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(1, E)	VL	34	BE-8, BE-9; BE-10	(N/A, E)	VL
4	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(1, E)	VL	35	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(1, E)	VL
5	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(3, E)	VL	36	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(1, E)	VL
6	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(3, E)	VL	37	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(1, E)	VL
7	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(3, E)	VL	38	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(1, E)	VL
8	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(3, E)	VL	39	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(3, E)	VL
9	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(3, E)	VL	40	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(3, E)	VL
10	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(3, E)	VL	41	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(3, E)	VL
11	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(3, E)	VL	42	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(3, E)	VL
12	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(3, E)	VL	43	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(3, E)	VL
13	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(2, E)	VL	44	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(3, E)	VL
14	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(2, E)	VL	45	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(3, E)	VL
15	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(2, E)	VL	46	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(3, E)	VL
16	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(2, E)	VL	47	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(2, E)	VL
17	SBE-3; SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(1, E)	VL	48	SBE-1(V1, A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(2, E)	VL
18	SBE-3; SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(2, E)	VL	49	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(2, E)	VL
19	SBE-3; SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(2, E)	VL	50	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(2, E)	VL
20	SBE-3; SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; SBE-19; BE-10	(2, E)	VL	51	SBE-3; SBE-4; SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(1, E)	VL
21	SBE-14; SBE-19; BE-10	(2, E)	VL	52	SBE-3; SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(2, E)	VL
22	SBE-15; SBE-19; BE-10	(2, E)	VL	53	SBE-3; SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(2, E)	VL
23	SBE-16; SBE-19; BE-10	(4, E)	VL	54	SBE-3; SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; BE-9; BE-10	(2, E)	VL
24	SBE-17(V-17, A-17.1); SBE-19; BE-10	(3, E)	VL	55	SBE-14; BE-9; BE-10	(2, E)	VL
25	SBE-17(V-17, A-17.2); SBE-19; BE-10	(4, E)	VL	56	SBE-15; BE-9; BE-10	(2, E)	VL
26	SBE-17(V-17, A-17.3); SBE-19; BE-10	(3, E)	VL	57	SBE-16; BE-9; BE-10	(4, E)	VL
27	SBE-18; SBE-19; BE-10	(4, E)	VL	58	SBE-17(V-17, A-17.1); BE-9; BE-10	(3, E)	VL
28	BE-1, BE-9; BE-10	(N/A, E)	VL	59	SBE-17(V-17, A-17.2); BE-9; BE-10	(4, E)	VL
29	BE-2, BE-3, BE-9; BE-10	(N/A, E)	VL	60	SBE-17(V-17, A-17.3); BE-9; BE-10	(3, E)	VL
30	BE-4, BE-9; BE-10	(N/A, E)	VL	61	SBE-18; BE-9; BE-10	(4, E)	VL
31	BE-5, BE-9; BE-10	(N/A, E)	VL				

Purely security related MC
Mix related MC
Purely safety related MC

Table 10: The re-identified MCs after the added improvement

BT is presented and the process for likelihood evaluation is explained.

There is complexity in quantifying likelihoods of attacks and a lack of consistency in the likelihood of occurrence between deliberate and accidental causes of risk. For these reasons, two different qualitative likelihood scales one for safety and another for security are proposed for representing the likelihood of basic events related to safety and security. The different likelihood scales lead to three different types of events sequences (MCs). A qualitative mathematical rule is used to calculate the likelihoods of MCs.

The outputs of the approach show important results in terms of representation of risk scenarios as well as in likelihood quantification. MCs due to purely safety, security or both can be separately extracted. This separation between MCs helps understand the origins of risk and provide the right control measures.

The application of the proposed approach on an undesirable scenario in a chemical reactor shows that the highly likelihood MCs are purely related to security. The added improvement diminishes the unacceptable likelihood to an acceptable level. The results show that the moves from purely security MCs to mix safety/security MCs is the safest risk treatment.

In the future, this work will be extended by proposing a more robust likelihood evaluation technique. Quantitative data, if available, will be used for more accurate analysis. In addition, uncertainty due to imprecision, vagueness and the lack of consensus (if multiple sources of data are used) will be considered.

Acknowledgments

This work is based on research supported and funded by the French National Institute for Industrial Environment and Risks (INERIS).

References

- , 2016. False sequential logic attack on {SCADA} system and its physical impact analysis. *Computers & Security* 58, 149 – 159.
- Abdo, H., Flaus, J., 2015. A mixed fuzzy probabilistic approach for risk assessment of dynamic systems. *IFAC-PapersOnLine* 48 (3), 960–965.
- Abdo, H., Flaus, J.-M., 2016a. Uncertainty quantification in bow-tie analysis: A mixed approach of fuzzy theory with dempster-shafer theory of

- evidence. In: *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL (Glasgow, Scotland)*. Taylor & Francis, pp. 2743–2750.
- Abdo, H., Flaus, J.-M., 2016b. Uncertainty quantification in dynamic system risk assessment: a new approach with randomness and fuzzy theory. *International Journal of Production Research*, 1–24.
- Almalawi, A., Yu, X., Tari, Z., Fahad, A., Khalil, I., 2014. An unsupervised anomaly-based detection approach for integrity attacks on {SCADA} systems. *Computers & Security* 46, 94 – 110.
- Arunraj, N., Maiti, J., 2007. Risk-based maintenancetechniques and applications. *Journal of Hazardous Materials* 142 (3), 653–661.
- Byres, E. J., Franz, M., Miller, D., 2004. The use of attack trees in assessing vulnerabilities in scada systems. In: *Proceedings of the international infrastructure survivability workshop*.
- Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K., 2016. A review of cyber security risk assessment methods for {SCADA} systems. *Computers & Security* 56, 1 – 27.
- Dell, I., 01 2015. Dell Security Annual Threat Report. Tech. rep.
- Ferdous, R., Khan, F., Sadiq, R., Amyotte, P., Veitch, B., 2012. Handling and updating uncertain information in bow-tie analysis. *Journal of Loss Prevention in the Process Industries* 25 (1), 8–19.
- Firesmith, D. G., December 2003. Common concepts underlying safety security and survivability engineering. Tech. rep., Software Engineering Institute.
- Fovino, I. N., Masera, M., 2006. Through the description of attacks: A multidimensional view. In: *International Conference on Computer Safety, Reliability, and Security*. Springer, pp. 15–28.
- Henrie, M., 2013. Cyber security risk management in the scada critical infrastructure environment. *Engineering Management Journal* 25 (2), 38–45.
- INERIS, 2015. Agrégation semi-quantitative des probabilités dans les études de dangers des installations classées - omega probabilités.

- Johnson, C., 2012. Cybersafety: on the interactions between cybersecurity and the software engineering of safety-critical systems. *Achieving System Safety*, 85–96.
- Kaplan, S., Garrick, B. J., 1981. On the quantitative definition of risk. *Risk analysis* 1 (1), 11–27.
- Kornecki, A. J., Zalewski, J., 2010. Safety and security in industrial control. In: *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*. ACM, p. 77.
- Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y., 2015. A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety* 139, 156–178.
- Nicholson, A., Webber, S., Dyer, S., Patel, T., Janicke, H., 2012. {SCADA} security in the light of cyber-warfare. *Computers & Security* 31 (4), 418 – 436.
- Patel, S., Tantalean, R., Ralston, P., Graham, J., 2005. Supervisory control and data acquisition remote terminal unit testbed. *Intelligent Systems Research Laboratory technical report TR-ISRL-05-01*, Department of Computer Engineering and Computer Science. Louisville, Kentucky: University of Louisville.
- Purdy, G., 2010. Iso 31000: 2009 setting a new standard for risk management. *Risk analysis* 30 (6), 881–886.
- Schneider Electric, T. . R. S. S., 2012. Scada systems. Tech. rep., Schneider Electric, Ontario K2K 2A9, Canada.
- Schneier, B., 1998. Modeling security threats. In: *Dr. Dobbs Journal*.
- Shin, J., Son, H., Heo, G., 2016. Cyber security risk evaluation of a nuclear i&c system using bayesian networks and event trees. *Nuclear Engineering and Technology*.
- Stouffer, K., Falco, J., Scarfone, K., 2011. Guide to industrial control systems (ics) security. *NIST special publication 800 (82)*, 16–16.
- Weiss, J., 2016. Industrial control system cyber security and the critical infrastructures. *INSIGHT* 19 (4), 33–36.

Yuanhui, W., 1999. Safety system engineering. Tianjin: Tianjin University Publishing House.