A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie - combining new version of attack tree with bowtie 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 vulnerabilities that can be exploited by sophisticated threats and lead to undesirable safety accidents. Thus, identifying these vulnerabilities during risk analysis becomes an important part for effective industrial risk evaluation. However, nowadays, safety and security are analyzed 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 bowtie analysis, commonly used for safety analysis, with a new extended version of attack tree analysis, introduced for security analysis of industrial control systems. The combined use of bowtie and attack tree 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, bowtie 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 occurrence 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 are 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 Dell's 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 Attack tree (AT) for security analysis within bowtie (BT) for safety analysis in order to provide a complete 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.

In order to present the possibilities offered by this study, the paper is structured as follows: Section 2 introduces the concepts of safety risks, security risks and the industrial automation and control system IACS. In Section 3, we highlight the global idea behind this study. In Section 4, we present the proposed methodology for a combined safety/security industrial risk analysis. In Section 5, we present a case study where the proposed methodology is applied for a hazard scenario in a chemical facility. Finally, section 6 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 defined or defined as follows (Kaplan and Garrick, 1981):

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

where

- R_{safety} - safety related risk which is defined as a set of {};
- S_e - scenario representation 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 defined in terms of likelihood and effects of a given threat exploiting a potential vulnerability (Stouffer et al. (2011); Henrie (2013)):

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

where

- $R_{security}$ - security related risk which is defined as a set of {};;
- tv - scenario representation 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 Controld 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 limited or 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 (Li et al. (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.

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. In the safety domain, risk is described as a set of undesirable events scenarios S_e with their related likelihoods and impacts (see Section 2.1). In the security domain, risk is described as a set of scenarios that consist of threats exploiting vulnerabilities with the attached likelihoods and impacts (2.2). However, undesirable safety events can occur due to cyber threats after exploiting specific vulnerabilities. Thus, safety/security risk is defined in terms of a triplet as follows:

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

where

- $S_{(tv,e)}$ - Scenario description of the undesirable event (e) that can result from safety incidents (safety causes) or/and security breaches (tv: threats exploit vulnerabilities - 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 the likelihoods 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.

To represent and evaluate the likelihood of a risk scenario, in the domain of safety, a bowtie analysis is constructed and then we use this bowtie to calculate the likelihood. In the domain of security, the chain of a security breach is represented by a graph called attack tree. The structures of the trees are close, here we propose a common representation by combining them as presented in Figure 2.

In both cases (safety and security), the risk is measured by a pair Likelihood/severity. However, we realized that it is not possible to use a common qualitative scale for likelihood analysis. Indeed, if we consider an undesired event that can be generated from a component failure (safety) or a cyber attack (security), it is preferable to keep a double measure of likelihood

(safety, security) rather than aggregating the two likelihood information into one. This gives a better idea on the importance of the two aspects and eventually, the use of the common model to detect an attack.

Let us take the example of a door lock which is controlled via the Internet. If the IT protection mechanism is moderate reliable, and the lock is difficult to break, then the risk is moderate (it needs a mechanical attack or a cyber attack). In comparison to a purely mechanical lock that is a little less resistant, this will present the same level of risk. The two systems appear to be similar whereas only the first one presents a residual cyber risk.

Thus, the proposed methodology to analyze safety/security risks is 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 event 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 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 and provides inputs for intrusion detection systems. 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. Here,

the severity of an individual scenario is considered to be the same whatever the causes are related to safety or security. 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 terms 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.

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 bowtie analysis

bowtie 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. Figure 4 presents a schematic diagram of the bowtie analysis, the definition of each is detailed in Table 1.

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 in the proposed AT.

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 and exploit three different vulnerabilities in order to achieve their goal. This attack can be modeled by the proposed 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.

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 7. If we take the WannaCry ransomware attack as an example, the attack event is

sending an unsolicited email that contains a link to exploit two different vulnerabilities: (1) the computer runs Windows operating system that is a not updated and (2) the unawareness of the user (if he/she clicks on the link). The security event will be as presented in Figure 8.

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 complete 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;

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 9). 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 safety/security 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.

4.3.1. Determining minimal cut sets

Finding out the MCs represents the first step of likelihood evaluation in our approach. An 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). In this study, the MCs are obtained using rules of boolean algebra (Yuanhui, 1999). Each MC set is a combinations of AND gates containing a set of basic inputs necessary and sufficient to cause the top event (see Grossel (2001), appendix D for more details).

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.

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, while safety incidents are rare). 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 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 Es 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.

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. In this article, 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 10(a) shows the three different levels proposed to evaluate this criterion. Level 1 (E) means that the vulnerability is easy to be exploited (for example, a password that should be a number of four digit represents an easy vulnerability). Vulnerabilities of level 2 (M) or 3 (H) are harder to be exploited due to the presence of security measures. If we take the same example, a password that should be a number of eight digit would be of level 2. While an eight digit password that should contains lower and upper case letters in addition to numbers would be of level 3;

• 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 10(b) presents the levels of difficulty of an attack inspired from (Byres et al., 2004). Four levels $\{T, M, D, VD\}$ are used to describe the difficulty of executing an attack. (T) is the easiest to conduct where normal computer skills are required (for example, running a Denial Of Service Attack). (M) demands some programming and security skills (running an SQL injection). (D) needs a hacking expert (man in the middle attack). (VD) is the hardest where a team of competent hackers are needed to conduct the attack (implementing a sophisticated warm).

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 10(c). 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 4. From Table 4, we can note that likelihood levels of security events are different from those of safety events (Table 3).

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. Suppose an AND gate with *n* input events EV_i, $i = 1,...,n$, the output likelihood is calculated as presented in Eq 4 (INERIS, 2015).

$$\begin{aligned} L(AND_{out}) &= min[L(EV_i)] = \left(min[L_{security}(EV_i)], min[L_{safety}(EV_i)]\right) \\ &= (min[L_{security}(EV_1),...,L_{security}(EV_n)], min[L_{safety}(EV_1),...,L_{safety}(EV_n)]) \end{aligned} \quad (4)$$

where $L(EV_1),...,L(EV_n)$ are the likelihoods of occurrence attached to $EV_1,...,EV_n$, 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 5 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 in choosing the right countermeasure, because decision makers should know if the high likelihood is related to safety, security or to both.

Figure 11 presents an example on how to calculate the likelihood of an MC. The MC in Figure 11 presents four basic events, two are related to safety ($BE-1$ and $BE2$) and the other two are security related ($SBE-1$ and $SBE-2$). Based on the proposed approach, experts are asked to characterize the likelihood of safety basic events, and (i) difficulty of attacks and (ii) exploitability of vulnerabilities for security basic events. From (i) and (ii), the likelihood security basic events are determined based on Table 10 (For example, $SBE-1$ is of level 4 since the vulnerability level is E and the needed attacker skills are T). The dashed rectangle beside each event in the figure presents its likelihood. These likelihood are then propagated through the MC. The likelihood of events SE-1 and E-1 are calculated based on Eq 4.

$L(E-1) = min(L(BE-1), L(BE-2)) =$
$(min[L_{security}(BE-1), L_{security}(BE-2)], min[L_{safety}(BE-1), L_{safety}(BE-2)]) = (min[N/A, N/A], min[A, C]) = (N/A, C)$, where

$L(E-2) = min(L(SBE-1), L(SBE-2)) = (min[4,3], min[N/A, N/A]) = (3, N/A)$. The likelihood of the top event is equal to

$min(L(E-1), L(E-2)) = (min[N/a; 3], min[C; N/A]) = (3, C)$ which is of level Moderate (M) based on Table 5.

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 12 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.

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.

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 13 presents the BT for the undesirable event under study. The undesirable main event is an overheating and increase in pressure inside the reactor. This event occurs after an abnormal increasing of the temperature and pressure which is due to:

(a) an error in the cooling system: this event can be generated from accidental failures if the valve XYSV33027 breaks down (BE-1), pumps P1 or P2 breakdown (BE-2 or BE-3), the valve XYSV33063 breaks down (BE-4), or failure in the power supply (BE-5). It can also be initiated by deliberate attacks on the control system (as detailed in the next paragraph: constructing ATs);

(b) over loading: an excessive loading of the reactor due to a human error (BE-6);

(c) agitation system breakdown: if the power supply or the motor of the system breaks down (BE-7 or BE-8).

However, this rise in pressure is limited by an automated safety valve. If this does not accomplish its purpose due to mechanical failure (BE-9) or cyber-attack (see next paragraph), it would result in the explosion of the reactor. Thus, nine safety related basic events are investigated as causes of the overheating in the reactor.

2. constructing ATs for security analysis: two events in the BT of Figure 13 can occur due to security breaches. The first event is the failure of the automated safety valve due to an attack on the hardware (SBE-19 in Figure 13: exploiting the control surveillance vulnerability by running a Doorknob rattling attack). The second is by sabotaging the cooling system after gaining unauthorized access to the SCADA system. SCADA system can be exploited by attacking the computer software or the communication network as shown in Figure 14 and detailed below:

• attacking the communication network: this can be achieved by sending a malicious email to steal access information from an authorized target (employees inside the facility) to exploit the no existence of email surveillance (exploit confidentiality), see SBE-18 in Figure 14. Or, exploiting the weakness of the encryption algorithm (integrity of information) used for communication between the SCADA and the control level. Different attacks can be performed to exploit integrity: message spoofing, replay attack or man in the middle attack

(SBE-17). The communication network can also be hacked by running a Denial Of Service attack where the system is vulnerable and reached from a big sized network (SBE-16).

• attacking the computer software: variety of applications software are implemented to complete the functionality of the control system. Furthermore, their are large databases that save confidential information and data about the process. SACDA applications software are susceptible to be hacked by sophisticated threats. Most of these applications are written in C programming language which make them vulnerable to the Buffer Overflow attack (SBE-15). This attack aims to insert lines of assembly codes such that can result in corrupting the memory. A successful Buffer Overflow attack can corrupt data, crash the program, or cause the execution of malicious codes. SQL injection also represents a threat to the computer software (SBE-14). SQL injection is one of the top Web attacks that affects the security of SCADA systems. It occurs when an adversary is able to manipulate a malicious SQL query into a Web application that fails to properly sanitize the query. In addition to these two attacks, computer worms represent the biggest threat for computer software. For this purpose, we also modeled the Stuxnet warm to examine the impact of computer worms on industrial control systems and to present the utility of the approach. Stuxnet is chosen because it represents the most sophisticated virus that can affect ICS. In the rest of this section, we detail how stuxnet operates to sabotage the control system.

The different operations (attacks) and vulnerabilities Stuxnet exploits are modeled in Figures 15, 16, 17.

Stuxnet is one of the most sophisticated worm that was designed to target a specific Siemens PLC (Falliere et al. (2011); McMillan (2010)). The main goal of Stuxnet is to gain unauthorized access to this PLC in order to attack and sabotage the industrial system Karnouskos (2011). To do so, Stuxnet shall install itself after being injected into the facility, spread via the network to find the PLC and lastly run the attack as respectively presented in Figures 17, 16 and 15. From Figure 17, Stuxnet can infect a computer inside using different paths. Injecting an infected removable drives and open it. The virus will spread to the computer by exploiting the Auto-run or the LNK vulnerabilities. Or via internet by sending a malicious email as modeled by SBE-3. After infecting a computer inside the facility, Stuxnet installs itself by stealing a digital certificate (exploiting the Realtek vulnerability) and loading a dropper (.ddl) file (exploiting the Windows vulnerabilities) as represented by SBE-4 and SBE-5, respectively.

The second step of Stuxnet is to spread inside the facility searching for its target (Siemens PLC). Stuxnet can spread using different ways as shown in Figure 16 and presented below (Mueller and Yadegari (2012)):

• spread via WinCC vulnerability: Stuxnet searches for computers running the SCADA interface Simatic WinCC and connects into WinCC using a password hard-coded (SBE-6). Then attacks using SQL injection (SBE-7). If these two have been done successfully, Stuxnet uploads and copies itself on the WinCC computer.

• spread via Network shares (SBE-8): Stuxnet can exploit the existing of shared folders to spread throughout the local network. It places a Trojan.dropper file to install the virus on the target computers that share the same folders.

• spread via the MS10-061 print spooler 0-day vulnerability (SBE-9): Stuxnet uploads copies of itself on remote computers by exploiting this vulnerability. By executing these copies, Stuxnet infects the remote machines.

• spread via the MS08-067 SMB vulnerability (SBE-10): if a remote computer has this vulnerability, Stuxnet can send a malformed path over SMB (a protocol for sharing files and other resources between computers) to execute arbitrary code on the remote machine, thereby propagating itself to it.

The last step for Stuxnet represents the attack phase to compromise and sabotage the SCADA system (see Figure 15). After spreading and finding its target, Stuxnet checks the connection to PLC as well as other specific configuration (PLC model, Profibus configuration, speed regulators number). Stuxnet sends this information to its senders in order to get updated (SBE-11). Once it is updated, Stuxnet looks for WinCC/Step7 software on the control PC used to configure the PLC in order to proceeds infecting and modifying PLC function blocks. If found, it installs a rootkit: it loads a library file (s7otbxdx.dll) used for the communication between the control PC and the PLC, renames it (s7otbxsx.dll) and inserts malicious codes into the new file (SBE-12). Beside this step, Stuxnet conceals the attack activities (SBE-13): it collects data for a period of 13 to 90 days before conducting the attack and sending modified control data. Thus, the malware operates without being detected. As result, Stuxnet sends wrong control data and displays to the operator that the system is under normal conditions.

5.2.2. Step-2: Likelihood evaluation

1. determining minimal cut sets: The ATBT shown in Figure 13 yields to 61 MCs. All minimal combinations of basic events that result in the occurrence of the main event are identified. Figure 18 shows an example of the MC number 59. The MC in Figure 18 is related to mixture safety/security because safety and security basic events (respectively BE-9 and SBE-17 in the Figure) should occur together to cause the occurrence of the undesirable event. 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.

2. characterizing likelihood of occurrence of input events: 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).

3. calculating likelihood of MCs: safety/security likelihood of each MC is calculated using Eq 4 as shown in Table 6. Then the overall likelihood of each MC is determined based on Table 5. As an example, Figure 18 presents calculating the likelihood of MC number 59. MC number 59 contains two basic events BE-9 and SBE-17 with likelihoods equal to (*N*/*A*, *D*) and (4, *N*/*A*) (derived based on Table 10(c)), respectively. After propagating these likelihoods, the likelihood of the explosion event is equal to (4, *D*) which is of level *L*.

5.3. Discussion and improvement

As shown in Table 6, the MCs ranked high (H) and (VH) are purely due to cyber-security. 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.

To show the importance of analyzing safety and security together, a burst disk is added which represents a mechanical component (no security breaches are related) as improvement for the process. The re-determination of MCs shows that there is no MC that is related to pure security. Table 7 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.

The methodology in this paper focuses on introducing cyber-security related threats within industrial risk analysis. Beside the advantages this methodology presents, it hides some limits:

• the step of characterizing likelihood for security related events (Section 4.3.2.2) could be improved. Many other criteria could be taken into account to evaluate the likelihood of security related events: connectivity of systems, control of internal and external stakeholders, technology and communication protocols used, organization set up to monitor and patch vulnerabilities, etc.;

• the approach presented for likelihood analysis is qualitative. The advantage of this qualitative approach is its simplicity of applying and understanding by the relevant personnel. But, this qualitative approach is subjective and heavily dependent on the experience of experts who are performing the analysis and it can be influenced by personal idiosyncrasies. Consequently, it can lead to inaccurate and imprecise risk predictions. Therefore, moving towards a quantitative approach by using statistical data for likelihood analysis is a focus of interest for future work;

• in general, each dangerous phenomenon is analyzed a part in terms of likelihood/severity. Nevertheless, in case of security, it can be imagined that several scenarios can occur at the same time. An attacker could try to cause several phenomena at the same time to maximize the effects. For example, if there are several tanks of dangerous materials, in traditional risk analysis, the fire of each tank is assessed separately. But, if there are several simultaneous fires, the severity would be greater and the the intervention to reduce accidents would be more difficult.

These limits will be considered for future work.

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 cyber-security. On the other hand, cyber-security analysis ignore the benefits of non-digital systems in decreasing the likelihood of security scenarios. 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. Bowtie 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 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).

Houssein ABDO holds a master's degree in computer security and risk management. He is currently a PhD student at G-SCOP laboratory, Grenoble Alpes University, France. His research focus is safety, security and uncertainty analysis in industrial risk management of critical facilities.

Mohamad KAOUK received his master's degree in networks and telecommunications in France in 2016 from Paul Sabatier University. He is currently a research Engineer at the GSCOP

laboratory, Grenoble Alpes University, France. His research concerns cyber security of control systems.

Jean-Marie FLAUS has more than 20 years of experience in industrial engineering, computer engineering and safety/security risk analysis. He is a professor at G-SCOP laboratory, Grenoble Alpes University, France.

François MASSE is a reliability and functional safety engineer at the French National Institute for Industrial Environment and Risks (INERIS). He is currently managing a project on cyber security in critical facilities run by the French ministry.

References

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 maintenance techniques 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.

Falliere, N., Murchu, L. O., Chien, E., 2011. W32. stuxnet dossier. White paper, Symantec Corp., Security Response 5 (6).

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.

Grossel, S. S., 2001. Guidelines for chemical process quantitative risk analysis: ; by center for chemical process safety; american institute of chemical engineers, new york, ny, 2000, pp. 750.

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 probabilits 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.

Karnouskos, S., 2011. Stuxnet worm impact on industrial cyber-physical system security. In: IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society. IEEE, pp. 4490–4494.

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.

Li, W., Xie, L., Deng, Z., Wang, Z., 2016. False sequential logic attack on scada system and its physical impact analysis. Computers & Security 58, 149 – 159.

McMillan, R., 2010. Siemens: Stuxnet worm hit industrial systems. Computerworld 14.

Mueller, P., Yadegari, B., 2012. The stuxnet worm. Département des sciences de linformatique, Université de lArizona, http://www. cs. arizona. edu/˜collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report. pdf.

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: 2009setting 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.

Table 1: Abbreviations, significations and definitions of elements listed in the bowtie diagram

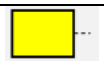
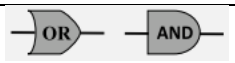
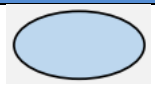
Shape	Signification	Definition
	Basic event (BE)	Direct cause of a physical integrity
	Event (E)	Physical integrity caused by the occurrence of basic events
	Undesirable event (UE)	The unwanted event such as a loss of containment, etc.
	Secondary event (SE)	Characterizes the source term of an accident, such as ignition
	Dangerous phenomenon (DP)	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 2: Description of events used for representing an attack scenario

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

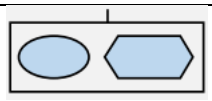
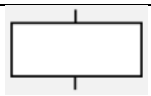
		Security basic event	Direct cause of a security breach resulting from exploiting a given vulnerability
		Intermediate	A security breach caused by the occurrence of input events
		Top event	The main goal of an attack generated from one or several security breaches

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

Qualitative scale	**Safety Level**	**Designation**	**Quantitative meaning**
Likelihood	N/A	**Not Applicable**: event is purely related to security, not safety	
	E	**Very unlikely:** event that is practically impossible, very low chance of happening	0
	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^{-5}
	C	**Moderate:** may	10^{-4}

		occur during total operational life if considering several systems of the same type	
	B	**Likely event:** may occur during total operational life of a system	10^{-3}
	A	**Very likely event**: can frequently occur (several times) during operational life	10^{-2}

Table 4: Qualitative scale to characterize the likelihood of input security 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 5: Analysis scale - Overall likelihood

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 6: The identified MCs for the scenario under study

	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,	(1, N/A)	L	**34**	BE-8, BE-9	(N/A, D)	L

	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							
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; SBE8; 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;	(3, N/A)	H		**37**	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4;	(1, D)	L

	SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; SBE-19					SBE-5; SBE-6; SBE-7; SBE-11; SBE-12; SBE-13; BE-9		
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; SBE8; 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;	(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

	SBE-13; SBE-19							
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,	(2, N/A)	M		**44**	SBE-1(V1,	(3, D)	L

	A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; SBE-19					A-1.2); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-9; SBE-11;SBE-12; SBE-13; BE-9		
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;	(2, N/A)	M		**47**	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-10;	(2, D)	L

	SBE-10; SBE-11; SBE-12; SBE-13; SBE-19					SBE-11; SBE-12; SBE-13; BE-9		
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	3	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;	(2, N/A)	M		**51**	SBE-3; SBE-4; SBE-5; SBE-6; SBE-7; SBE-11;	(1, D)	L

	SBE-10; SBE-11; SBE-12; SBE-13; SBE-19					SBE-12; SBE-13; BE-9		
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 7: The re-identified MCs after the added improvement

	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);	(1, E)	VL		**34**	BE-8, BE-9; BE-10	(N/A, E)	VL

	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							
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; SBE8; 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);	(3, E)	VL		**37**	SBE-1(V1, A-1.1);	(1, E)	VL

	SBE-2(V-2.1, A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; SBE-19; BE-10					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		
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; SBE8; 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,	(3, E)	VL		**40**	SBE-1(V1, A-1.2); SBE-2(V-2.1,	(3, E)	VL

	A-2); SBE-4; SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; SBE-19; BE-10					A-2); SBE-4; SBE-5; SBE-8; SBE-11; SBE-12; SBE-13; BE-9; BE-10		
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;	(3, E)	VL		**43**	SBE-1(V1, A-1.1); SBE-2(V-2.1, A-2); SBE-4;	(3, E)	VL

	SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; SBE-19; BE-10					SBE-5; SBE-9; SBE-11; SBE-12; SBE-13; BE-9; BE-10		
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;	(2, E)	VL		**46**	SBE-1(V1, A-1.2); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-9;	(3, E)	VL

	SBE-10; SBE-11; SBE-12; SBE-13; SBE-19; BE-10					SBE-11;SBE-12; SBE-13; BE-9; BE-10		
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;	(2, E)	VL	3	49	SBE-1(V1, A-1.1); SBE-2(V-2.2, A-2); SBE-4; SBE-5; SBE-10; SBE-11; SBE-12;	(2, E)	VL

	SBE-19; BE-10					SBE-13; BE-9; BE-10		
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;	(4, E)	VL		**54**	SBE-3; SBE-4;	(2, E)	VL

	SBE-19; BE-10					SBE-5; SBE-10; SBE-11; SBE-12; SBE-13; BE-9; BE-10		
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