# A fuzzy safety/cybersecurity risk analysis approach for more safe/secure industrial systems

Houssein Abdo, Jean-Marie Flaus, François Masse

# A fuzzy safety/cybersecurity risk analysis approach for more safe/secure industrial systems

# Une approche floue d'analyse des risques de sûreté/cybersécurité pour des systèmes industriels plus sûrs et sécurisés

H. ABDO. et J-M. FLAUS.
G-SCOP
Université Grenoble Alpes
Grenoble, France
houssein.abdo@grenoble-inp.fr
jean-marie.flaus@grenoble-inp.fr

F. MASSE.
INERIS
Verneuil-en-Halatte, France
Francois.masse@ineris.fr

**Résumé**

L'introduction de la technologie numérique dans les industries crée de nouvelles menaces de cybersécurité qui affecte la sûreté des systèmes industriels. De plus, nombreux experts du risque soulignent que la sûreté et la sécurité ne doivent pas être analysées séparément. Dans des études antérieures, les auteurs ont proposé une méthode d'analyse des risques qui considère la sûreté et la sécurité ensemble au cours de l'analyse des risques industriels. Le cyber-nœud proposé utilise une méthodologie qualitative d'analyse de la probabilité pour définir le niveau de risque. Cependant, cette approche peut sous-estimer les risques en raison de l'incertitude des données. Pour cette raison, cette recherche vise à remplacer la méthodologie qualitative par une approche semi-quantitative floue pour traiter cette incertitude.

**Summary**

The introduction of digital technology in process industries creates new cyber-security concerns that can affect the safety of industrial systems. Moreover, many risk experts highlight that safety and security should not be analyzed separately. In previous studies, the authors have proposed a risk analysis method that considers safety and security together during industrial risk analysis. The proposed cyber bow-tie uses a qualitative likelihood analysis methodology to define the level of risks. However, this approach may underestimate risks due to data uncertainty. For this reason, this research aims to replace the qualitative methodology by a more effective fuzzy semi-quantitative approach in order to define the level of safety/security risks under input data uncertainty. The effectiveness of the fuzzy approach is demonstrated using a real case study.

## Introduction

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. For this reason, concerns about approaches for industrial risk analysis that consider and analyze safety and security together become a primary need (Masse et al, 2017). Quantifying and analyzing these major risks contributes to better decision making and ensures that risks are managed according to defined acceptance criteria (Abdo and Flaus., 2016).

However, analyzing safety and security risks together is not simple. Safety and security risks are of different nature. In general, safety is associated with accidental risks caused by component failures, human errors or any non-deliberate source of hazard, and considered to be rare events with low frequency. While security is related to deliberate risks originating from malicious attacks and are classified as common events with high probability.

In previous studies, the authors have proposed a new method called cyber bow-tie analysis to model the safety and cybersecurity related causes and consequences of an undesirable dangerous event ((Abdo et al., 2018) and (Abdo et al., 2017a)). In the same study, we also developed a qualitative likelihood analysis methodology based on the proposed cyber bow-tie for evaluating the risk level based on two-term likelihood parts, one for safety and one for security.

Likelihood analysis is a very important step in risk analysis. Qualitative or quantitative likelihood analysis can be performed depending on the type of data available. This data is derived from different sources: historical accident data or expert judgments in terms of numerical values (quantitative such as $10^{-3}$ per year) or linguistic variables (qualitative such as low, high, etc.), respectively. Quantitative information for a quantitative analysis is expensive and not always provided. Qualitative analysis is subjective and may lead to loss of quantitative information if it exists. In addition, the accuracy of the analysis based on these two approaches still a major issue since uncertainty is not taken into consideration. However, qualitative and quantitative likelihood analysis approaches have drawbacks that can be eliminated by the use of a semi-quantitative one (please see (Abdo et al., 2017b) for more details about the drawbacks). That is why this study proposes a fuzzy-semi quantitative approach to overcome the drawbacks presented in the qualitative and quantitative approach. This approach relies on the available information from historical data or experts if the former is not available. It should be noted that here we deal with the uncertainty related to the likelihood of risk scenarios regarding the available data.

In order to present the possibilities offered by this study, the paper is structured as follows: Section 2 presents the cyber bow-tie analysis developed in (Abdo et al., 2018). In Section 3, we present the proposed methodology for likelihood analysis based on the cyber bow-tie. In Section 4, we present a case study where the proposed methodology is applied for a hazard scenario in a chemical facility. Finally, Section 5 draws a number of conclusions.

## Cyber-BowTie analysis

In this section, we will present the Cyber bow-tie methodology proposed in (Abdo et al., 2018) for a combined safety/security industrial risk analysis. This approach is located in the risk analysis part regarding the ISO 27001 and ISO 22301 standards.

The cyber bow-tie combines the bow-tie (BT) for safety analysis and the attack tree (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.

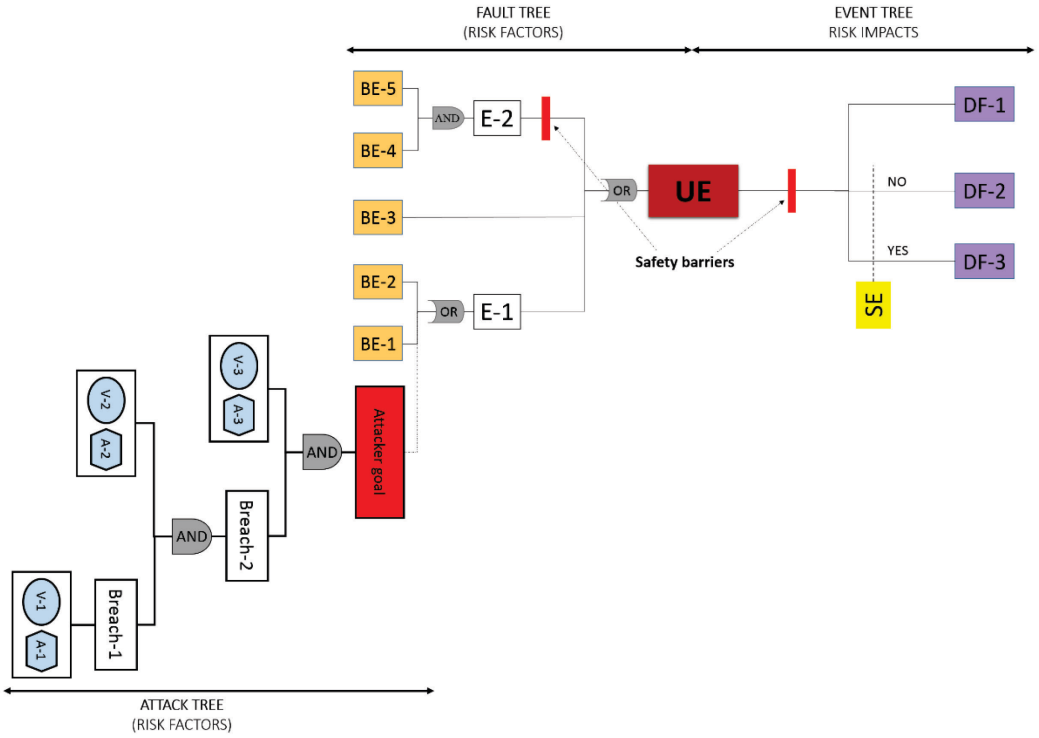



*Figure 1. Structure of the cyber bow-tie diagram as proposed by (Abdo et al., 2018)*

BT analysis 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 (Ferdous et al., 2012).

The AT describes the sequence of steps to perform an attack. It represents an attack against a system in a tree structure ((Schneier, 1998), (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. In the cyber BT, a new version of attack tree as proposed. This new version of AT covers the limits presented in traditional ATs. Traditional ATs do not present all the information needed to evaluate the likelihood of a successful attack on the target system. However the AT presented by (Abdo et a., 2018) allows the consideration of this 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.

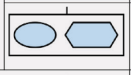
| | shape | Signification | Definition |
|---|---|---|---|
| Input events |  | Vulnerability | Any step describing a vulnerability required in order to realize the attack |
| |  | Attack | The attack process in order to exploit a system vulnerability |
| |  | Security basic event | Direct cause of a 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 1. Description of events used for representing an attack scenario.*

The relationships between trees' nodes in the ATBT are represented using the logical AND/OR gates. Figure 1 presents a schematic diagram of the cyber bowtie analysis, the definition of each event in the AT and BT are detailed in Table 1 and 2, respectively. In Figure 1, the event E1 can occur due to safety events (BE-1 or BE-2) or due to a cyber-attack as modelled by the AT.

Please refer to (Abdo et al., 2018) for more information about constructing the ATBT.

| 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. Abbreviations, significations and definitions of elements listed in the bowtie diagram.*

## Proposed approach: Fuzzy likelihood analysis for safety/security risk scenarios

In this section, we will outline the proposed fuzzy approach for likelihood analysis of combined safety/security industrial risk scenarios. The idea is to use the ATBT and provide a more precise likelihood analysis approach to evaluate risks by using the fuzzy semi-quantitative approach introduced in (Abdo et al., 2017b). The likelihood .Here this approach will be adjusted to suit the ATBT perspectives.

This likelihood analysis using the ATBT is made up of three main steps as presented in (Abdo et al., 2018):

1. Determining the minimal cut sets to identify the system weaknesses
2. Characterizing likelihoods of input events

3. Quantify the likelihood of each MC to prioritize the system's weaknesses

However, no changes have been made to step 1 as presented by (Abdo et al., 2018). The main contribution of this paper is presented in steps 2 and 3 as presented in Section 3.2 and 3.3, respectively.

### 3.1 Determining minimal cut sets

A minimal cut (MC) is the smallest combination of input events which causes the occurrence of the undesirable event being studied (Yuanhui, 1999).

In the ATBT, we can separate between three types of MCs:

- 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. The event causes of the MC are non-deliberate and due to components failures or human errors ;
- 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.

### 3.2 Characterizing likelihood analysis of input events

Likelihood analysis can be qualitative, quantitative or semi-quantitative. Qualitative and quantitative likelihood analysis have several disadvantages due to uncertainty of input data (please see (Abdo et al., 2015) for more information). To overcome the disadvantages of qualitative and quantitative likelihood analyses, a semi-quantitative approach can be used (INERIS, 2015). In this study, a fuzzy semi-quantitative approach is developed to quantify the likelihood of safety/cybersecurity risk scenarios using the ATBT.

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). In addition, there are different concepts to define likelihood related to safety and security. Due to the deviation in the likelihood translation, (Abdo et al., 2018) have proposed two different scales *Ls*: security and *Lf*: safety of respectively five and six levels to separately represent the likelihood of safety and security related events. 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 (*Ls*, *Lf*).

Based on this likelihood representation in terms of couples, we can differ between three different types of events in the ATBT:

- Events that are purely related to safety with likelihood *(N/A, Lf)* for each event. Characterizing the likelihood of this type of events using the fuzzy semi-quantitative approach is detailed in Section 5.2;
- Events that are purely related to cyber-security with likelihood *(Ls, N/A)* for each event. The representation of this type of events is detailed in Section 5.3;
- Events related to both safety and security with likelihood *(Ls, Lf)* for each event (see Section 5.3).

#### 3.2.1 Preliminary

Before going in detailing the proposed approach, it is important to introduce the concept of fuzzy numbers used for characterizing input data. The concept of fuzzy numbers was introduced by the pioneer Zadeh in 1965 as a tool to characterize imprecise variables as well as to represent experts' knowledge in a mathematical tool (Zadeh, 1965).

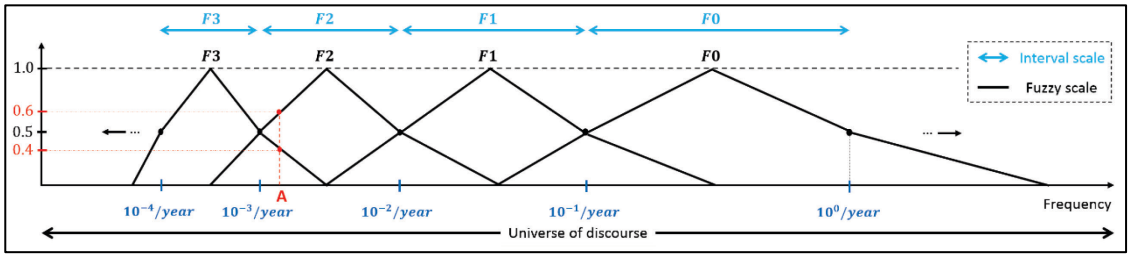



*Figure 2. Mapping event frequencies on fuzzy scale*

Fuzzy variable is associated with a possibility distribution or membership function in the same manner as random variable is associated with a probability distribution. A fuzzy number is the generalization of a regular, real number in the sense that it does not refer to one single value but rather to a connected set of possible values, where each possible value has its own weight between 0 and 1 (Dubois et Hanss, 2007).

Consider a fuzzy subset $F$ of the universal set X, thus the membership function is $\mu_F: X \rightarrow [0,1]$. Where, for a given $x \in X$, the weight or membership degree $\mu_{F,X}(x)$ represents the degree of compatibility of the value $x$ with the concept expressed by F.

Different fuzzy number shapes are used to represent uncertain data, triangular and trapezoidal fuzzy numbers are the most popular, and can be expressed as [a, b, c] and [a, b, c, d], respectively, see (Abdo and Flaus, 2016) for more details. In this study triangular, trapezoidal and a new shape of fuzzy number (proposed by the authors in (Abdo et al., 2017b) to fit the semi-quantitative approach) are used. A detailed description on the expression and membership functions of the used fuzzy numbers is presented in the next sections

#### 3.2.2 Characterizing likelihood for safety risk events

Likelihood characterization here aims to determine the likelihood of occurrences of safety input events according to a specific scale. The same scale proposed in (Abdo et al., 2017b) which is based on the INERIS approach (INERIS 2015) is used in this study and as detailed in the rest of this section.

The semi-quantitative method developed by the INERIS (INERIS 2015) characterizes the probabilities of safety basic events in terms of frequency classes. Each class is considered to cover a broad range (interval) of occurrence frequencies. Giving a frequency class to an input event is based on the process of asking experts, or by translating the quantitative data into a class. A class is

| | | |
|---|---|---|
| F-2 | $10^{+1}/year \leq frequency < 10^{+2}/year$ | 10 to 100 times/year |
| F-1 | $10^{0}/year \leq frequency < 10^{+1}/year$ | 1 to 10 times/year |
| F0 | $10^{-1}/year \leq frequency < 10^{0}/year$ | 1 time every 1 to 10 years |
| F1 | $10^{-2}/year \leq frequency < 10^{-1}/year$ | 1 time every 10 to 100 years |
| FX | $10^{-(X+1)}/year \leq frequency < 10^{-X}/year$ | |

*Table 3. Determining the frequency classes based on the semi-quantitative approach*

linguistically elicited from experts since they prefer linguistic judgments rather than precise value. This interval scale is presented in Table 3.

However, in (Abdo et al., 2017b), the authors have replaced the interval scale by a fuzzy scale to overcome the disadvantages presented in the interval scale. This fuzzy scale is used to characterize the frequency of occurrence of safety basic events as presented in Figure 2. In term of example, an event E with a frequency of occurrence equals $10^{-3}$ is of classes F2 and F3 with possibility degrees equal to 0.5 for the two classes.

| Quantitative scale | $10^{-5}$ | $10^{-4}$ | $10^{-3}$ | $10^{-2}$ | |
|---|---|---|---|---|---|
| Frequency classes | F5 | F4 | F3 | F2 | F1 |
| Probability levels | ***E*** | ***D*** | ***C*** | ***B*** | ***A*** |

*Table 4. Transforming of frequency classes into probability levels*

After calculating the frequency of the BT, this frequency is translated to probability levels defined by the French ministerial order of 29/09/2005 as presented in Table 4. Please refer to (Abdo et al., 2017b) for more information about the definition of each probability level where E is the lowest and A is the highest. The same article details performing likelihood analysis using BT based on the fuzzy semi-quantitative approach.

In the next section, the same fuzzy approach will be used to characterize the likelihood of security input events. Since safety and security events are of different nature, new fuzzy scales based on triangular and trapezoidal fuzzy numbers will be proposed to represent the likelihood of security related events.

### 3.2.3 Characterizing likelihood for security risk events

As presented in (Abdo et al., 2018), 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). In other words, the likelihood is a function of the difficulty of performing a needed attack to exploit a vulnerability, and the level of exploitability of a given vulnerability depending on the existing counter measures. In this section, two different fuzzy scales are constructed 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 5 and Figure 3 show the three different fuzzy levels proposed to evaluate this criterion with the associated fuzzy numbers. The qualitative terms proposed in (Abdo et al., 2018) are expressed in terms of fuzzy numbers as presented in the table and figure. Levels range from easy (E) to hard (H) depending on how difficult the vulnerability is to exploit. In case of uncertainty about the level, for example, an expert can suggest that a vulnerability is almost easy to exploit and give it a level 1 (E) with a possibility degree equals 0.6 and a level 2 (M) with a possibility degree equals 0.4. Thus, the vulnerability will be belong to two levels with two different membership degrees;

- Technical difficulty of conducting an attack: given to an attack event to show the needed level of expertise to conduct the attack. Table 6 and Figure 4 present the fuzzy levels of difficulty of an attack. Four levels T, M, D, VD are used and represented in terms of triangular and trapezoidal fuzzy numbers to describe the difficulty of executing an attack. The level (T) is the easiest while the level (VD) is the hardest. As discussed earlier, different levels with different membership degrees can be given to characterize an attack difficulty if uncertainty about the difficulty level is presented.

These two criteria are then combined in order to provide a likelihood characterization for the security initial (or basic) events. The difficulty of the attack is combined with the vulnerability levels as presented in Table 7. Four different security likelihood levels in addition to the N/A level are proposed to represent the combination. Please refer to (Abdo et al., 2018) for the definition of each security likelihood level in Table 5. Calculating this likelihood level in the case of uncertainty based on Table 7

| Qualitative scale | Vulnerability Level | Linguistic terms: Designation | Corresponding fuzzy numbers |
|---|---|---|---|
| exploitability (Level of difficulty to exploit a given vulnerability) | 1 | Easy (E): No countermeasures are presented | (0.0, 0.0, 0.2, 0.4) |
| | 2 | Medium (M): Countermeasures are presented | (0.2, 0.4, 0.6, 0.8) |
| | 3 | Hard (H): Countermeasures existed with continuous review and improvements. | (0.6, 0.8, 1.0, 1.0) |

*Table 5. Fuzzy scale to characterize the vulnerability level*

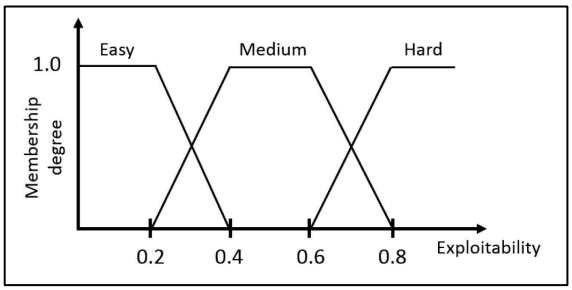



*Figure 3. Membership functions of the proposed fuzzy scale to represent the vulnerability level*

| Qualitative scale | Difficulty Level | Linguistic terms: Designation | Corresponding fuzzy numbers |
|---|---|---|---|
| Technical difficulty of an attack | 1 | Trivial (T): Little technical skill required | (0.0, 0.0, 0.2, 0.4) |
| | 2 | Moderate (M): Average cyber hacking skills required | (0.2, 0.4, 0.6) |
| | 3 | Difficult (D): Demands a high degree of technical expertise | (0.4, 0.6, 0.8) |
| | 4 | Very difficult (VD): Beyond the known capability of today's best hackers | (0.6, 0.8, 1.0, 1.0) |

*Table 6. Fuzzy scale to characterize the difficulty of conducting an attack*

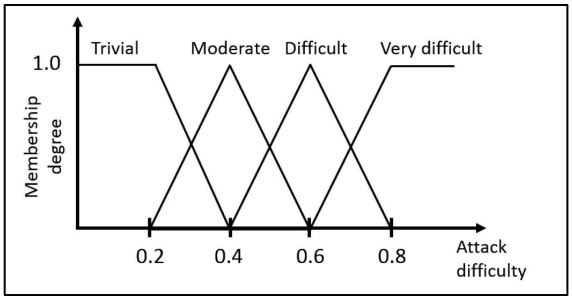



*Figure 4. Membership functions of the proposed fuzzy scale to represent the attack difficulty level*

will be explained in the next section using simple examples.

### 3.3 Calculating the likelihoods of MCs

| 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 7. Combining attack difficulty levels with the vulnerability levels to determine the likelihood of security input events (Abdo et al., 2018)*

This step aims to prioritize the system weaknesses by calculating the likelihood of each MC. 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

| 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 (Abdo et al., 2018)*

input events have occurred. Based on the fuzzy semi-quantitative scales proposed for safety and security likelihood characterization, the min rule is used to solve the AND gate and calculate the likelihood levels of the top event with their associated membership degrees.

Suppose an AND gate with n input events *EVi, i=1, ..., n*, the output likelihood is calculated as presented in Eq. 1. The membership degree of the output event is calculated based on Eq. 2.

$$L(ANDout) = min[L(EVi)] = (min[Lsecurity(EVi)], min[Lsafety(EVi)]) = (min[Lsecurity(EV1), \ldots, Lsecurity(EVn)], min[Lsafety(EV1), \ldots, Lsafety(EVn)]) \quad \{1\}$$

$$Degree(L(ANDout)) = min[Degree(L(EVi))] = (min[Degree(Lsecurity(EVi))], min[Degree(Lsafety(EVi))]) = (min[Degree(Lsecurity(EV1), \ldots, Lsecurity(EVn))], min[Degree(Lsafety(EV1), \ldots, Lsafety(EVn))] \quad \{2\}$$

Finally, for each MC, the two determined likelihoods for safety and security are taken together to provide an overall likelihood to be used for prioritizing MCs as presented in Table 8 (Abdo et al., 2018). This overall scale defines five different expressions from low (L) to very high (VH). This overall-likelihood can not replace the double part likelihoods *(Lsecurity, Lsafety)* which is important for decision-making and in choosing the right countermeasure.

Figure 5 presents an example on how to calculate the fuzzy likelihood of an MC. The MC in Figure 5 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 fuzzy 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 fuzzy likelihood levels security basic events are determined. For example, SBE-1 is of levels 4 and 3 with membership degrees equal to 0.6 and 0.4, respectively. This is because the vulnerability level is almost easy (E:0.6 and M:0.4) and the needed attacker skills are uncertain and elicited to be T:0.6 and M:0.4). The output likelihood of SBE-1 is calculated using the Cartesian product as shown in Figure 6. The output level and membership degree of each case in the Cartesian table is respectively determined based on Table 7 and Eq 2 as presented in Figure 6. Level 4 appears several times in the Cartesian table of Figure 6. In this case, the highest membership degree is taken (0.6). The dashed rectangle beside each event in the figure presents its likelihood. These likelihood are then propagated through the MC. The likelihood of events E-1 and E-2 and their membership degrees are calculated using the Cartesian product as in Figure 8 and based on Eqs 1 and 2, respectively. L(E-1) = min(L(BE-1), L(BE-2)) = (min(Lsecurity(BE-1), Lsecurity(BE-2)], min[Lsafety(BE-1), Lsafety(BE-2)]) = (N/A | F1:0.3, F2:0.7), where L(E-2) = min (L(SBE-1), L(SBE-2)) = (4:0.6, 3:0.4 | N/A). The likelihood of the top event is equal to min (L(E-1), L(E-2)) = (3:0.6, 2:0.4 | F1: 0.3, F2: 0.7) =(3:0.6, 2:0.4 | A: 0.3, B: 0.7) which is of level Moderate (M:0.4) and High (H:0.6) based on Table 8. From this example we can conclude that there is a high possibility that the risk is high.

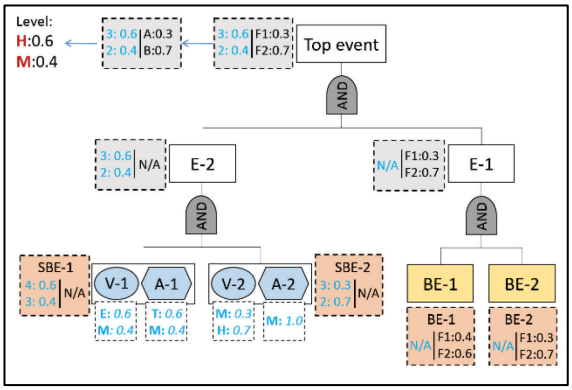
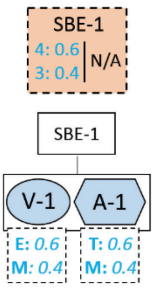



*Figure 5. Example of how calculating the likelihood of an MC*

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




| Event SBE-1 | | Attack difficulty | |
|---|---|---|---|
| | | T:0.6 | M:0.4 |
| | E:0.6 | ✓4:0.6 | 4:0.4 |
| | M:0.4 | 4:0.4 | ✓3:0.4 |

*Figure 6. Determining the likelihood of security basic event based on the fuzzy scale*

## Case study

The same case study presented by (Abdo et al., 2018) is presented in this section for comparison purposes. The case study concerns an industrial site of a propylene oxide polymerization reactor (Flaus, 2013). The reactor runs a high exothermic chemical reaction at high pressure. Risks

associated with the operation of the reactor are of high consequences.

cooling system after gaining unauthorized access to the SCADA system. SCADA system can be exploited by

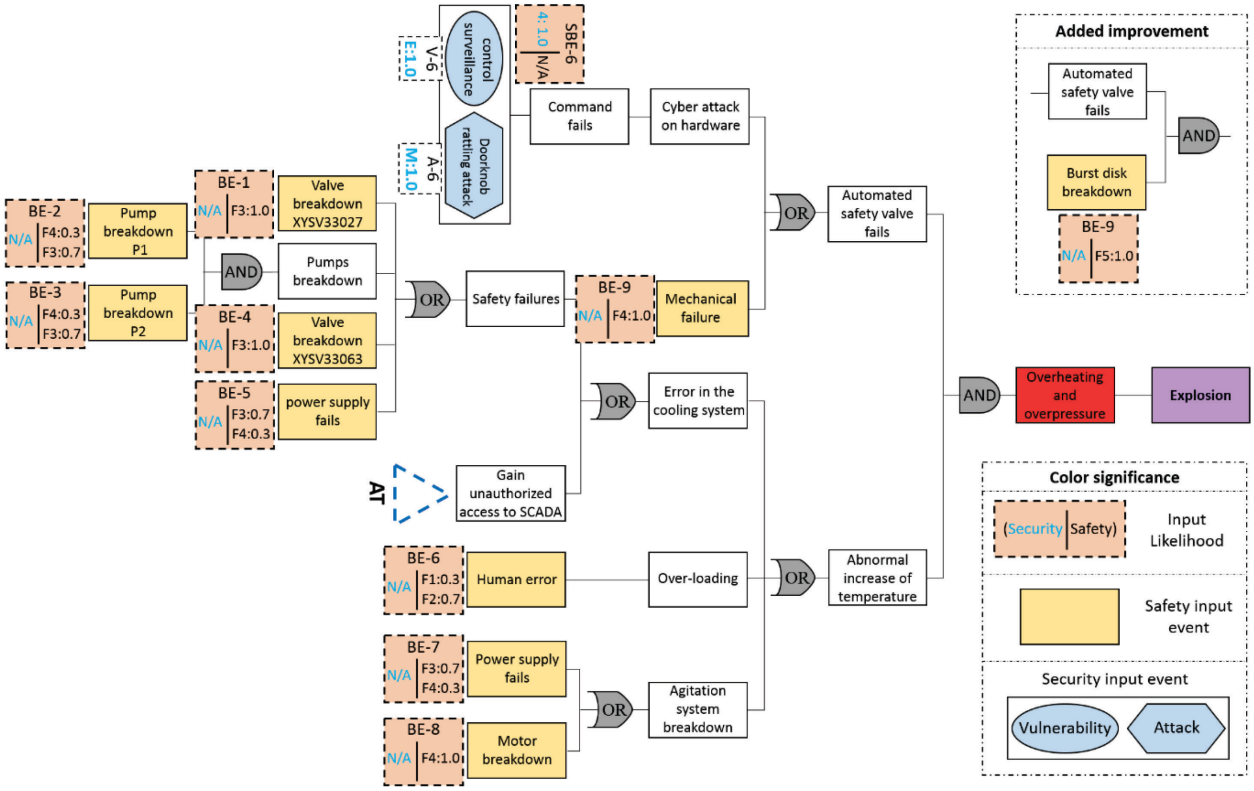



*Figure 7. Combined ATBT of the scenario under study*

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 the 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 10 shows the architecture of the system under study. The architecture of the system is taken from (Flaus 2013).

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 presented in the rest of this section.

**Step-1: constructing the ATBT for safety/security analysis. This step contains two sub-steps:**

Figure 7 presents the BT for the undesirable event under study, which is the overheating inside the reactor. Nine safety related basic events are investigated as causes of the overheating in the reactor. However, two events in the BT of Figure 7 can occur due to security breaches. The first event is the failure of the automated safety valve due to an attack on the hardware. The second is by sabotaging the attacking the computer software or the communication network as shown in Figure 8. Please refer to (Abdo et al., 2018) for more information about how we constructed the ATBT for this case study and details on each event.

**Step-2: Likelihood evaluation:**

The three steps explained in Section 4 for fuzzy likelihood analysis are conducted. The cyber bow-tie yields to 21 MCs as presented in Table 9. These MCs are divided into 7 that are purely related to security, 7 that are purely related to safety and 7 that are related to mixture safety/security. It should be noted that the same MCs obtained by (Abdo et al., 2018) are obtained here. For likelihood characterization, experts in the field are asked to characterize likelihoods of safety and security basic events. Uncertainty in the experts' elicitations are represented using the fuzzy scale as discussed in Section 4. The characterized likelihoods in terms of fuzzy couple (Lsecurity, Lsafety) are drawn beside the basic events in the ATBT (see figures 7 and 8). Then, the likelihood of each MC was calculated as shown in Table 9 (likelihood and level columns). However, if we compare the output likelihoods of MCs between the fuzzy approach and the qualitative approach of (Abdo et al., 2018), we notice that the qualitative approach may underestimate the risk. For example, MC number 2 in Table 6 is of level M (Moderate) based on the qualitative approach (Abdo et al., 2018). While, we can see that there is a high possibility to be of level H (high) based on the fuzzy semi-quantitative approach. This is because important non-qualitative information if existed can be ignored by using the qualitative approach. An almost easy elicitation from an expert is considered to be of level 1 using the qualitative approach, while it is of levels 1 and 2 with different membership degrees using the fuzzy approach.

**Discussion and improvement**

As shown in Table 9, the MCs ranked high (H) and (VH) are purely due to cybersecurity. The same improvement proposed by (Abdo et al., 2018) for the same case study is added here. The idea behind this improvement is to show the importance of analyzing safety and security together even under uncertainty. The improvement represents a burst disk that represents a mechanical component (no security breaches are related), see figure 7. The re-determination of MCs (see Table 10) shows that there is no MC that is related to pure security. The introduced improvement diminishes the likelihoods into the lowest level even with the presence of input data uncertainty.

Finally, in spite of all the uncertainties presented in the input data, we succeed to maintain the risk at the lowest level thanks to a combined safety/security risk analysis, and the only remaining risk is linked to the failure of the added improvement.

## Conclusion

Analyzing safety and security together is an urgent need for complete and effective risk analysis. In previous studies, the authors propose an approach called cyber BT that integrates ATs with BT analysis for a combined safety and security industrial risk analysis. However the qualitative likelihood analysis methodology developed for the cyber BT presents concerns due to data uncertainty. This is why this paper proposes a new likelihood analysis methodology that uses fuzzy theory to represent uncertainty.

The proposed methodology is applied to an undesirable safety/security risk scenario in a chemical facility. 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. The outputs of the approach show important results in terms of representation of risk scenarios as well as in likelihood quantification. The results show that the proposed fuzzy methodology provides more accuracy in the quantification, in addition to the consideration of uncertainty.

In the future, this work will be extended by using multiple sources of data in likelihood analysis. Different data bases or experts may provide different likelihood regarding the same event. Thus, rating and aggregating the data from different sources will lead to a more robust probability quantification approach using the cyber bow-tie analysis.

## 7 Acknowledgments

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

## 8 References

D. Dubois, M. Hanss, Applied fuzzy arithmetic: An introduction with engineering applications (2007).

Flaus, J. M. 2013. Fault tree analysis. Risk Analysis, 229-251.

F. Masse, H. Abdo and J-M. Flaus. (2017). Vers une approche integrant les exigences de cybersécurité à la maîtrise des risques d'accidents majeurs pour les ICPE). In 12ème Congrès International Pluridisciplinaire en Qualité, Sûreté de fonctionnement et Développement durable, Bourges, France.

Fovino IN, Masera M. Through the description of attacks: A multidimensional view. In: International Conference on Computer Safety, Reliability, and Security. Springer, pp. 15–28; 2006.

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

H. Abdo, M. Kaouk, J-M.Flaus, et F. Masse (2017a). Towards a better industrial risk analysis: Anew ap proach that combines cyber security within safety. Pages 179–187.

H. Abdo, J-M. Flaus et F. Masse (2017b). Fuzzy semi-quantitative approach for probability evaluation using bow-tie analysis. Pages 376–376.

H. Abdo, J-M. Flaus (2016). Uncertainty quantification in dynamic system risk assessment: a new approach with randomness and fuzzy theory. Int J Prod Res 2016; 1–24.

INERIS. F. N. I. for Industrial Environment, R. (2015), Aggregation semi-quantitative des probabilités dans les études de dangers des installations classées - Omega Probabilités.

Schneier B. Modeling security threats. In: Dr. Dobbs Journal; 1998.

Ferdous R, Khan F, Sadiq R, Amyotte P, Veitch B. Handling and updating uncertain information in bow-tie analysis. J Loss Prevent Proc Indust 2012;25(1):8–19.

Flaus, J. M. (2013). Risk analysis: socio-technical and industrial systems. John Wiley & Sons.

L. Zadeh, Fuzzy sets, Information and Control 8 (3) (1965) 338 - 353.

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

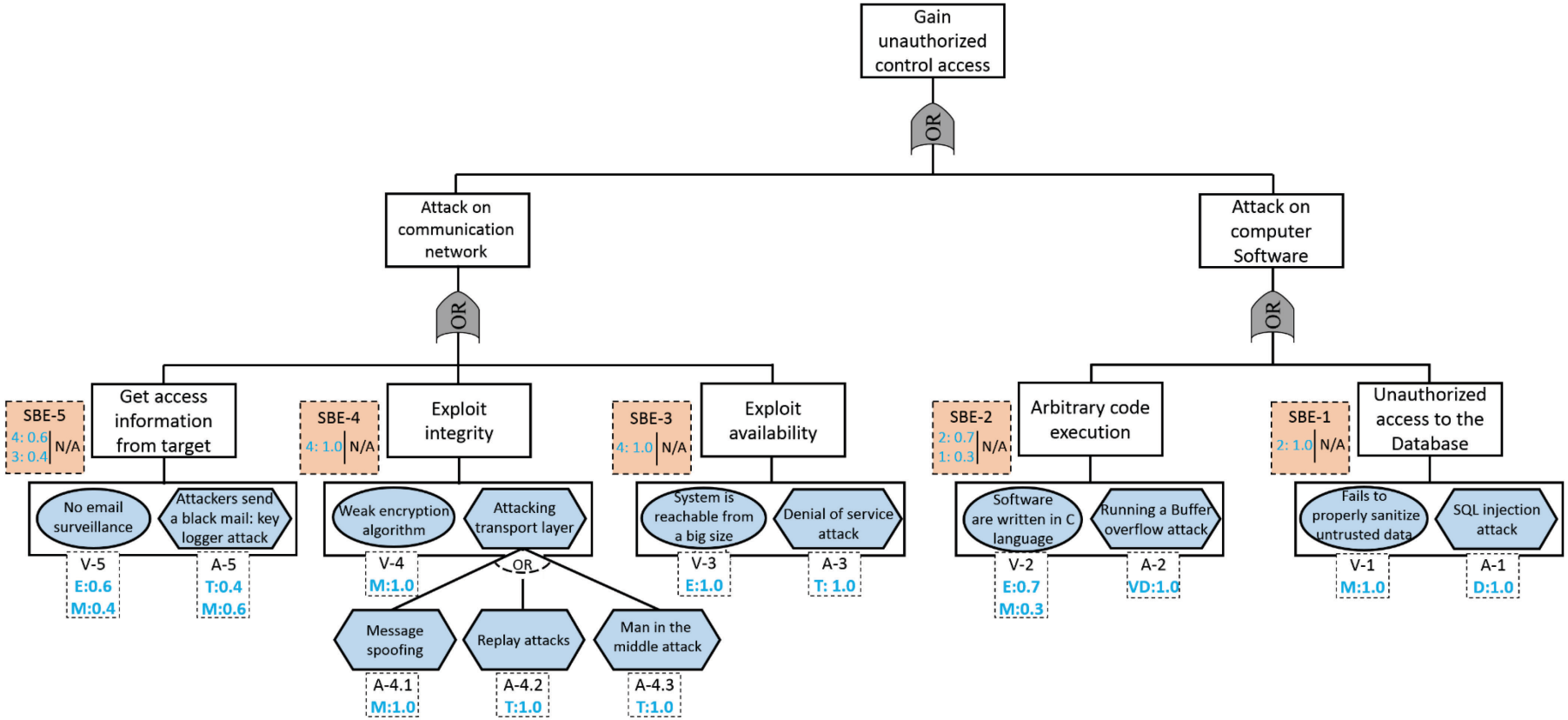



*Figure 8. AT for the goal: gain unauthorized access to SCADA*

| | MCS | Likelihood | Level | | MCS | Likelihood | Level |
|---|---|---|---|---|---|---|---|
| 1 | SBE-1; SBE-6 | 2: 1.0 \| N/A | H | 12 | BE-6, BE-9 | N/A \| F4:1.0 F4: | L: 1.0 |
| 2 | SBE-2; SBE-6 | 2: 0.7 1: 0.3 \| N/A | H: 0.7 M: 0.3 | 13 | BE-7, BE-9 | N/A \| F4:1.0 F4: | L: 1.0 |
| 3 | SBE-3; SBE-6 | 2: 1.0 \| N/A | H: 1.0 | 14 | BE-8, BE-9 | N/A \| F4:1.0 | L: 1.0 |
| 4 | SBE-4(V-4, A-4.1) ; SBE-6 | 3: 1.0 \| N/A | H: 1.0 | 15 | SBE-1; BE-9 | 2: 1.0 \| F4:1.0 | L: 1.0 |
| 5 | SBE-4(V-4, A-4.2) ; SBE-6 | 4: 1.0 \| N/A | VH: 1.0 | 16 | SBE-2; BE-9 | 2: 0.7 1: 0.3 \| F4:1.0 | L: 1.0 |
| 6 | SBE-4(V-4, A-4.3) ; SBE-6 | 3: 1.0 \| N/A | H: 1.0 | 17 | SBE-3; BE-9 | 4: 1.0 \| F4:1.0 | L: 1.0 |
| 7 | SBE-5; SBE-6 | 4: 0.6 3: 0.4 \| N/A | VH: 0.6 H: 0.4 | 18 | SBE-4(V-4, A-4.1) ; BE-9 | 3: 1.0 \| F4:1.0 | L: 1.0 |
| 8 | BE-1, BE-9 | N/A \| F4:1.0 | L: 1.0 | 19 | SBE-4(V-4, A-4.2) ; BE-9 | 4: 1.0 \| F4:1.0 | L: 1.0 |
| 9 | BE-2, BE-3, BE-9 | N/A \| F4:1.0 | L: 1.0 | 20 | SBE-4(V-4, A-4.3) ; BE-9 | 4: 1.0 \| F4:1.0 | L: 1.0 |
| 10 | BE-4, BE-9 | N/A \| F4:1.0 | L: 1.0 | 21 | SBE-5; BE-9 | 4: 0.6 3: 0.4 \| F4:1.0 | L: 1.0 |
| 11 | BE-5, BE-9 | N/A \| F4:1.0 | L: 1.0 | | | | |

Purely security related MC  Mix related MC  Purely safety related MC

*Table 9.The identified MCs for the scenario under study*

| | MCS | Likelihood | Level | | MCS | Likelihood | Level |
|---|---|---|---|---|---|---|---|
| 1 | SBE-1; SBE-6; BE-10 | 2: 1.0 \| F5:1.0 | VL:1.0 | 12 | BE-6, BE-9; BE-10 | N/A \| F4:1.0 F4: | VL:1.0 |
| 2 | SBE-2; SBE-6; BE-10 | 2: 0.7 1: 0.3 \| F5:1.0 | VL:1.0 | 13 | BE-7, BE-9; BE-10 | N/A \| F4:1.0 F4: | VL:1.0 |
| 3 | SBE-3; SBE-6; BE-10 | 2: 1.0 \| F5:1.0 | VL:1.0 | 14 | BE-8, BE-9; BE-10 | N/A \| F4:1.0 | VL:1.0 |
| 4 | SBE-4(V-4, A-4.1) ; SBE-6; BE-10 | 3: 1.0 \| F5:1.0 | VL:1.0 | 15 | SBE-1; BE-9; BE-10 | 2: 1.0 \| F4:1.0 | VL:1.0 |
| 5 | SBE-4(V-4, A-4.2) ; SBE-6; BE-10 | 4: 1.0 \| F5:1.0 | VL:1.0 | 16 | SBE-2; BE-9; BE-10 | 2: 0.7 1: 0.3 \| F4:1.0 | VL:1.0 |
| 6 | SBE-4(V-4, A-4.3) ; SBE-6; BE-10 | 3: 1.0 \| F5:1.0 | VL:1.0 | 17 | SBE-3; BE-9; BE-10 | 4: 1.0 \| F4:1.0 | VL:1.0 |
| 7 | SBE-5; SBE-6; BE-10 | 4: 0.6 3: 0.4 \| F5:1.0 | VL:1.0 | 18 | SBE-4(V-4, A-4.1) ; BE-9; BE-10 | 3: 1.0 \| F4:1.0 | VL:1.0 |
| 8 | BE-1, BE-9; BE-10 | N/A \| F5:1.0 | VL:1.0 | 19 | SBE-4(V-4, A-4.2) ; BE-9; BE-10 | 4: 1.0 \| F4:1.0 | VL:1.0 |
| 9 | BE-2, BE-3, BE-9; BE-10 | N/A \| F5:1.0 | VL:1.0 | 20 | SBE-4(V-4, A-4.3) ; BE-9; BE-10 | 4: 1.0 \| F4:1.0 | VL:1.0 |
| 10 | BE-4, BE-9; BE-10 | N/A \| F5:1.0 | VL:1.0 | 21 | SBE-5; BE-9; BE-10 | 4: 0.6 3: 0.4 \| F4:1.0 | VL:1.0 |
| 11 | BE-5, BE-9; BE-10 | N/A \| F5:1.0 | VL:1.0 | | | | |

Purely security related MC  Mix related MC  Purely safety related MC

*Table 10. The re-identified MCs after the added improvement*