



HAL
open science

Towards a better industrial risk analysis : A new approach that combines cyber security within safety

Houssein Abdo, M. Kaouk, Jean-Marie Flaus, François Masse

► **To cite this version:**

Houssein Abdo, M. Kaouk, Jean-Marie Flaus, François Masse. Towards a better industrial risk analysis : A new approach that combines cyber security within safety. 27th European Safety and Reliability annual conference (ESREL 2017), Jun 2017, Portoroz, Slovenia. pp.1215-1222. ineris-01853454

HAL Id: ineris-01853454

<https://ineris.hal.science/ineris-01853454>

Submitted on 7 Sep 2018

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

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

Towards a better industrial risk analysis: A new approach that combines cyber security within safety

H. Abdo, M. Kaouk & J.-M. Flaus

University Grenoble Alpes, CNRS, G-SCOP, F-38000, Grenoble, France

F. Masse

INERIS, Parc Technologique Alata BP 2 F-60 550 Verneuil-en-Halatte, France

ABSTRACT: The introduction of digital technology in industries creates new security threats that can lead to undesirable safety accidents. Thus, analyzing these threats during safety analysis becomes an important part for effective risk evaluation. However, nowadays, safety and security are assessed separately where they should not be. This is because a security threat can lead to the same dangerous phenomena as a safety accidental cause. In this paper, a new method that considers safety and security for probability evaluation during industrial risk analysis is proposed. This approach combines Bow-Tie Analysis (BTA), commonly used for safety analysis and the Attack Tree Analysis (ATA), recently introduced for security analysis of computer control systems. The combined use of BT and AT provides an exhaustive qualitative investigation of security and safety scenarios, and a qualitative evaluation of the likelihood of these scenarios. The definition of BT and AT combined, and the mathematical formulas for likelihood quantification are presented. The application of this approach is demonstrated using the case study of a risk scenario in a chemical facility.

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 & Flaus 2016). Quantifying and analyzing these risks contributes to better decision making and ensures that risks are presented according to defined acceptance criteria (Arunraj & Maiti 2007). A systematic safety risk analysis process is made up of three steps: (i) identification of risk scenarios, (ii) likelihood analysis and (iii) effect analysis ((Purdy 2010); (Kaplan & Garrick 1981)). Based on these steps, a level of risk will be given to each scenario to see if it is acceptable or not. If not, safety measures should be added to reduce the level of risk to an acceptable level by diminishing the likelihood or the effects. This work considers the first two steps. Identifying a risk scenario aims to explore how an undesirable hazard can be developed starting from causes and ending with the consequences. Likelihood analysis aims to estimate the likelihood of risk scenarios. This estimate can be qualitative or quantitative depending on the available data.

However, traditional industries were based on mechanical devices and closed systems (Kriaa, Pietre-Cambacedes, Bouissou, & Halgand 2015).

Today, industries are influenced by the development of digital technology related to instrumentation and control systems (SCADA: Supervisory Control And Data Acquisition). The shift from analog equipment towards technologies has a number of benefits concerning production, but it also presents challenges (Shin, Son, & Heo 2016). This introduction of technology increases the degree of complexity and communication among systems. The use of internet for remote controlling and supervising systems and facilities has generated a new type of risk related to 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 & Zalewski 2010)).

The differences and similarities between safety and security are studied by many authors ((Kriaa, Pietre-Cambacedes, Bouissou, & Halgand 2015); (Firesmith 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 malicious risks originating from attacks, which can be accomplished physically or by cyber means. In this study, physical attacks are excluded.

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

In this study, we propose a methodology that combines BT and AT for an exhaustive likelihood evaluation (see Figure 1). It aims to examine cyber-security attacks during likelihood analysis process. BT analysis is one of the most popular methodologies used in probabilistic safety assessment (Abdo & Flaus). 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 complex systems. This methodology identifies and considers all safety and security threats that can lead to the same undesirable phenomenon. The likelihood of a security related risk is analyzed based on the same process used in safety risk analysis (27005 2011). The proposed approach will provide a deep, exhaustive analysis on safety and security for a specific risk scenario in a given facility.

In this proposed approach, different likelihood scales, one for safety and another for security are defined to characterize the likelihood of input events. This differentiation helps in identifying

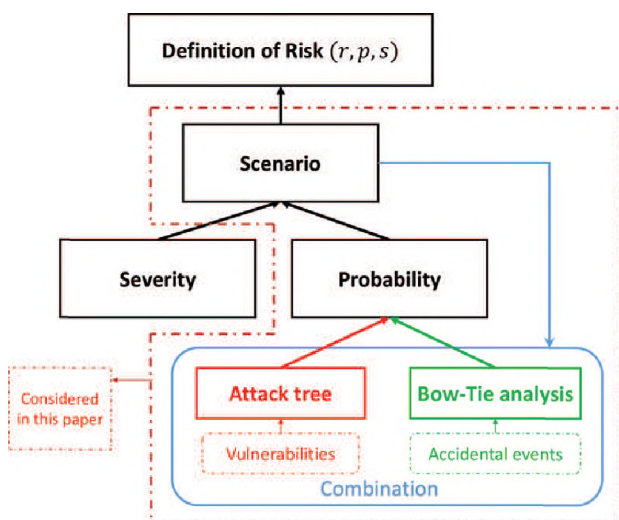


Figure 1. Definition of risk.

the sequences of events (minimal cut sets) that are purely related to safety, security or to both. The resulting output of different types of cut sets offers richer information for decision making. In the rest of this paper we are going to prove that purely security risk sequences should be treated firstly.

The second part of this paper introduces the concept of BT and AT analyses, and the mathematical rules to perform a likelihood analysis using these approaches. The third part presents how BT and AT can be used together for a safety/security analysis. Section four presents a case study where the proposed approach is applied for a hazard scenario in a chemical facility. Finally, section five draws a number of conclusions.

2 PRELIMINARY

In this section, we introduce the concepts of SCADA system, BT and AT analyses. Section 2.1 presents the role and architecture of the SCADA system. Steps and structures to analyze risks using BT and AT are highlighted in Sections 2.2 and 2.3, respectively.

2.1 SCADA: Supervisory Control & Data Acquisitions

SCADA system refers to an industrial computer system that monitors and controls a process. The principal function of SCADA is acquiring the data from devices such as valves, pumps, etc. and providing control of all these devices using a host software platform (Schneider Electric 2012). The system monitoring 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. SCADA system also provides more functions such as graphical display, alarming, tending and historical storage of data.

Figure 2 presents the structure of a SCADA system. There are four distinct levels within the

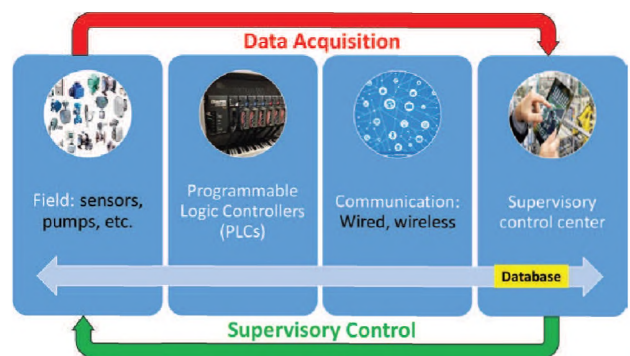


Figure 2. SCADA architecture.

SCADA system structure. These levels are presented as follows:

- Field instruments: refers 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;
- PLC (Programmable Logic Controller): 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;
- Communication network: the link that relays data from PLCs to the SCADA host software and the field instruments;
- SCADA host software: provides graphical displays in order to monitor, maintain and engineer processes and SCADA elements;

2.2 Bow-Tie analysis

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

Likelihood evaluation using BT is based on two main steps: (i) determining likelihood of occurrences of input events (BEs and SEs) and the likelihood of failures of risk barriers, (ii) propagating the likelihood through the BT in order to calculate the likelihood of outcomes. These two steps will be detailed in Section 3.

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









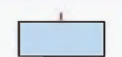


Shape	Signification	Definition
	Basic event	Direct cause of a physical integrity
	Event	Physical integrity caused by the occurrence of basic events
	Undesirable event	The unwanted event such as a loss of containment, etc.
	Secondary event	Characterize the source term of an accident, such as ignition
	Dangerous phenomenon	Physical phenomena 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		Operation	Any step representing an operation made by the attacker in order to perform the attack
		Vulnerability	Any step describing a vulnerability required in order to realize the attack
		Assertion	Any step representing assumptions, results, or requirements characterizing the attack process
		Intermediate/top event	A security breach caused by the occurrence of input events

2.3 Attack Tree

Attack tree is a graph that describes the sequence of steps in order to perform an attack (Fovino, Masera, & De Cian 2009). It represents an attack against a system in a tree structure. The root (top event) of the tree is the goal of an attack. This root is connected to intermediate and starting events (leaf nodes) in order to represent the different ways to achieve the attack (Schneier 1998).

In this study, we will adopt the extended version of attack tree proposed by (Fovino & Masera 2006), but with modifications where the concept of the intermediate event is added. This intermediate event aims to differentiate between the input events and the event generated by these inputs. This extended version allows the consideration of significant information such as attacker resources, motivations, etc. As in BT, different types of events and AND/OR gates are used to model an attack scenario. The term, shape and definition of each event are presented in Table 2.

An Operation node can have an input that presents a special structure regarding the other input events. However, for likelihood treatment, the Operation event and its input will be treated as an AND gate. The treatment of AND/OR gate will be presented in Section 3.

3 METHODOLOGY

In this section we present how ATs can be integrated within BTA for richer representations and precise evaluations of risks (see Section 3.1). Then, the different steps for conducting a qualitative likelihood evaluation will be presented. This evaluation is made up of three main steps: (i) determining the minimal cut sets, (ii) characterizing input data and (iii) propagating input data as highlighted in Sections 3.2, 3.3 and 3.4 respectively. Figure 3 shows the framework to apply the proposed approach.

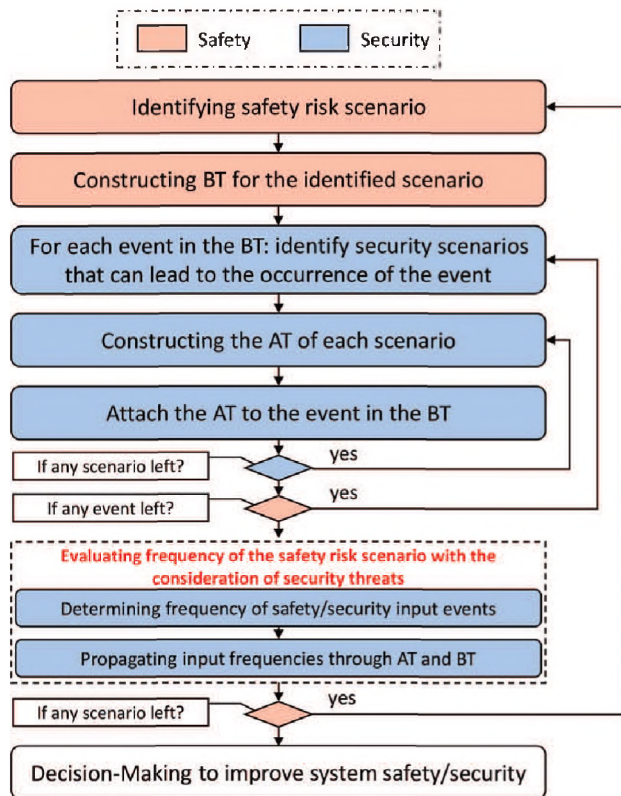


Figure 3. Framework to combine BT and AT for safety/security risk analysis.

3.1 Combining ATs with BT

Integrating ATs within BT analysis can help in understanding how attackers can take advantage of controlling systems' components in order to cause damages.

This combination aims to enrich the analysis by considering security risks modeled by attack trees that can lead to the same safety events modeled using BT. The top event of an AT tree coincides with an event contained in the BT. This means that an event in BT can occur due to accidental (safety) or deliberate (security) sequence of events.

3.2 Determining minimal cut sets

Finding out the minimal cut sets represents the first step of likelihood evaluation in our approach. A MC is the smallest combination of input events which causes the occurrence of the undesirable event. Determining the MCs is very useful to discover the weak point in our system and the different ways in which the top event can occur. In this study, the MCs are obtained using rules of boolean algebra (Yuanhui 1999).

This step aims to 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.

3.3 Characterizing likelihoods of input events

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. 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 null) in order to specify if an event is purely related to safety or security. Thus, each input 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 (basic events) related to safety with likelihood $(0, L_f)$ for each event;
- events (basic events) related to cyber-security with likelihood (L_s, NS) for each event;
- events (intermediate events) related to both safety and security with likelihood (L_s, L_f) for each event.

Tables 3 and 4 present the scales proposed for safety and security respectively. The same scale used by INERIS for safety analysis is used in this study (INERIS 2015). Different criteria are used to determine the likelihood of the cause of an attack (assertions, operations, vulnerabilities) based on the proposed scale (see (ANSSI 2014) for more details). These criteria are presented as follow:

- Attacker's level (individual, group of attackers, private organization, state organization, etc.);
- Installation's architecture: the level of technology used (if SCADA system is installed or less/high control technology is manipulated);
- Connectivity between systems (isolated, use of wireless technology, etc.);
- Resources of attackers;
- etc.;

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

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

Table 4. Qualitative scale to characterize the frequency of input security events.

Qualitative scale	Security Level	Designation
Likelihood	0	Not Significant: event is purely related to safety, not security
	1	Very Low: high unlikely to occur, never happened before even on a similar system
	2	Low: possibility to occur, but existed security measures reduce the likelihood of occurrence
	3	Moderate: somewhat is likely to occur, but system is not an attack target
	4	Strong: is almost certain to occur, system is an easy target

3.4 Propagating input frequencies through AT-BT combined

The propagation process aims to calculate the frequencies of the undesirable central event and its consequences. Propagating input frequencies through the AT-BT is achieved by setting the rules to solve the logical gates. Since qualitative scales are used for safety and security frequency characterization, the min-max rules are used to solve the gates (INERIS 2015). The output frequencies for OR/AND gates with n input events (E_1, \dots, E_n) are determined based on Eqs 1/2 respectively.

$$F(OR_{out}) = \max[F(E_1), \dots, F(E_n)] \quad (1)$$

$$F(AND_{out}) = \min[F(E_1), \dots, F(E_n)] \quad (2)$$

This approach will be illustrated in the next section and applied on an over-pressure scenario in a chemical reactor.

4 CASE STUDY

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 & Flaus 2015). The reactor runs a high exothermic chemical reaction at high pressure. Risks associated with the operation of the reactor are of high consequence. 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 4 shows the architecture of the system under study.

In this case, the most likely undesirable scenario with the highest consequences due to overheating/over-pressure is considered. This scenario is derived from an abnormal response of the cooling system after deliberate or accidental errors. The different steps of the proposed approach are applied to identify causes, consequences and the occurrence likelihood of this scenario. Figure 5 depicts

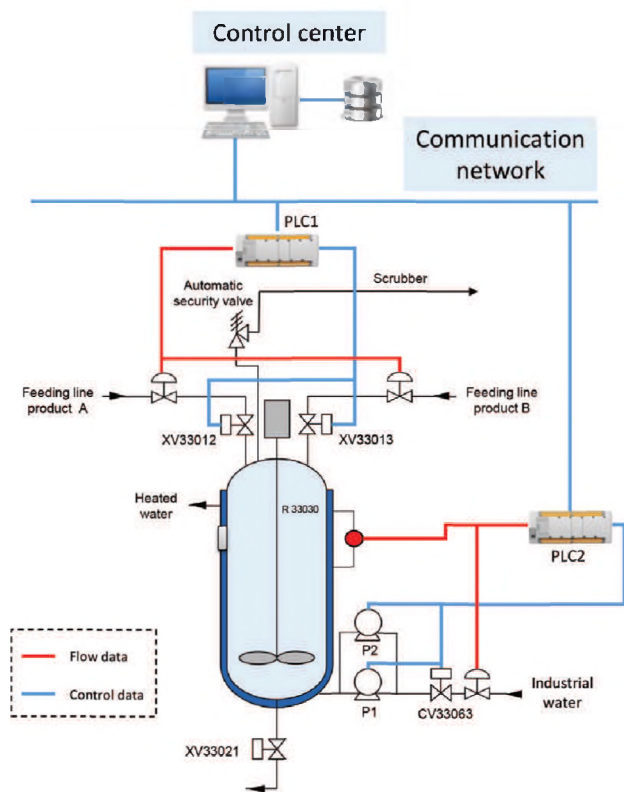


Figure 4. The chemical reactor with its SCADA system structure.

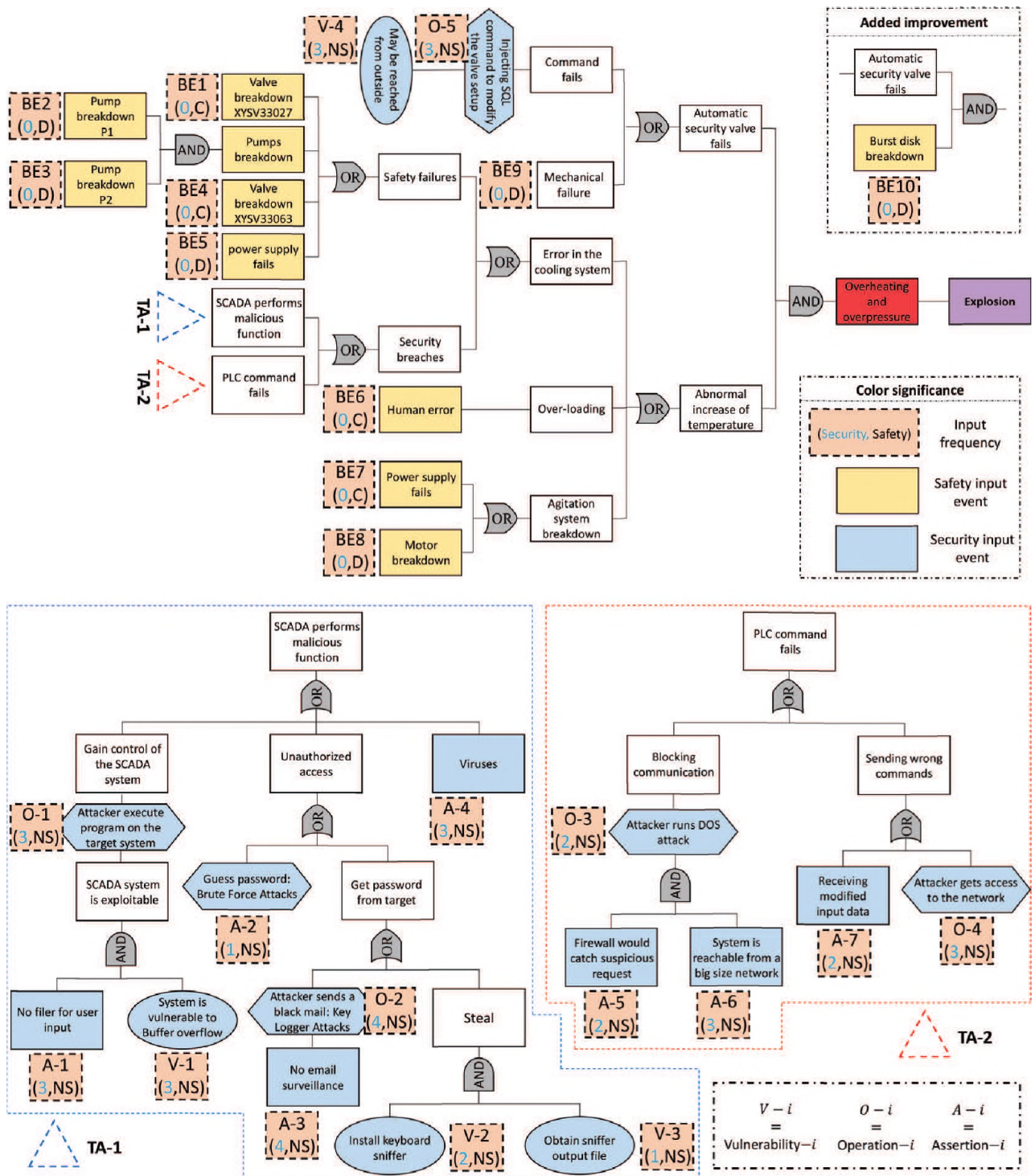


Figure 5. Combined AT-BT of the scenario under study.

the combined ATBT for this scenario. The ATBT shown in Figure 5 yields to 30 MCs. Table 5 presents the identified MCs with their estimated likelihoods.

As shown in Table 5, the MCs ranked high (H) are purely due to cybersecurity. This reveals the importance of considering security risks during safety risk analysis. However, the presence of a safety event in an MC will lead to less likelihood of occurrence. We can clearly see that between MC-1

and MC-16 where their attached likelihoods are equal to H and L respectively, MC-16 is of less likelihood because it contains the accidental event BE9.

For more details, a burst disk is added which represents a mechanical component (no security breaches are related). This burst disk will open for pressure relief in the event of excessive pressure build-up. The re-determining of MCs shows that there is no MC that is related to pure security.

Table 5. The identified MCs for the scenario under study.

	MCS	Likelihood	Level		MCS	Likelihood	Level
1	A-1, V-1, O-1, V-4, V-5	(3,NS)	H	16	A-1, V-1, O-1, BE9	(3,D)	L
2	A-2, V-4, V-5	(1,NS)	L	17	A-2, BE9	(1,D)	L
3	A-3, O-2, V-4, V-5	(3,NS)	H	18	A-3, O-2, BE9	(4,D)	L
4	V-2, V-3, V-4, V-5	(1,NS)	L	19	V-2, V-3, BE9	(1,D)	L
5	A-4, V-4, V-5	(3,NS)	H	20	A-4, BE9	(3,D)	L
6	A-5, A-6, O-3, V-4, V-5	(2,NS)	M	21	A-5, A-6, O-3, BE9	(2,D)	L
7	A-7, V-4, V-5	(2,NS)	M	22	A-7, BE9	(2,D)	L
8	O-4, V-4, V-5	(3,NS)	H	23	O-4, BE9	(3,D)	L
9	BE1, V-4, V-5	(3,C)	M	24	BE1, BE9	(0,D)	L
10	BE2, BE3, V-4, V-5	(3,D)	L	25	BE2, BE3, BE9	(0,D)	L
11	BE4, V-4, V-5	(3,C)	M	26	BE4, BE9	(0,D)	L
12	BE5, V-4, V-5	(3,D)	L	27	BE5, BE9	(0,D)	L
13	BE6, V-4, V-5	(3,C)	M	28	BE6, BE9	(0,D)	L
14	BE7, V-4, V-5	(3,C)	M	29	BE7, BE9	(0,D)	L
15	BE8, V-4, V-5	(3,D)	L	30	BE8, BE9	(0,D)	L

Pure security related MC
 Mix related MC
 Pure safety related MC

Table 6. The re-identified MCs after the added improvement.

	MCS	Likelihood	Level		MCS	Likelihood	Level
1	A-1, V-1, O-1, V-4, V-5, BE10	(3,D)	L	16	A-1, V-1, O-1, BE9, BE10	(3,D)	L
2	A-2, V-4, V-5, BE10	(1,D)	L	17	A-2, BE9, BE10	(1,D)	L
3	A-3, O-2, V-4, V-5, BE10	(3,D)	L	18	A-3, O-2, BE9, BE10	(4,D)	L
4	V-2, V-3, V-4, V-5, BE10	(1,D)	L	19	V-2, V-3, BE9, BE10	(1,D)	L
5	A-4, V-4, V-5, BE10	(3,D)	L	20	A-4, BE9, BE10	(3,D)	L
6	A-5, A-6, O-3, V-4, V-5, BE10	(2,D)	L	21	A-5, A-6, O-3, BE9, BE10	(2,D)	L
7	A-7, V-4, V-5, BE10	(2,D)	L	22	A-7, BE9, BE10	(2,D)	L
8	O-4, V-4, V-5, BE10	(3,D)	L	23	O-4, BE9, BE10	(3,D)	L
9	BE1, V-4, V-5, BE10	(3,D)	L	24	BE1, BE9, BE10	(0,D)	L
10	BE2, BE3, V-4, V-5, BE10	(3,D)	L	25	BE2, BE3, BE9, BE10	(0,D)	L
11	BE4, V-4, V-5, BE10	(3,D)	L	26	BE4, BE9, BE10	(0,D)	L
12	BE5, V-4, V-5, BE10	(3,D)	L	27	BE5, BE9, BE10	(0,D)	L
13	BE6, V-4, V-5, BE10	(3,D)	L	28	BE6, BE9, BE10	(0,D)	L
14	BE7, V-4, V-5, BE10	(3,D)	L	29	BE7, BE9, BE10	(0,D)	L
15	BE8, V-4, V-5, BE10	(3,D)	L	30	BE8, BE9, BE10	(0,D)	L

Pure security related MC
 Mix related MC
 Pure safety related MC

Table 6 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. For these reason, safety and security being treated together will lead to a better risk analysis and effective decision making.

5 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 risk analysis ignore cybersecurity. In light of security threats, there is an urgent need for complete and effective safety risk analysis. That is why this paper proposes an approach that integrates ATs with BT analysis for a combined safety and security risk analysis. Bow-Tie analysis is used for analyzing safety accidents. Attack Trees are introduced to consider potential malicious attacks that can affect the system's safety. The concepts of BT and AT are presented and the process for likelihood evaluation is explained.

Due to the complexity of quantifying likelihoods of attacks, and the no consistency in likelihood of occurrence between deliberate and accidental causes of risk. Two different qualitative scales are used for representing the likelihood of basic events related to safety and security. A different likelihood scales provides three different types of events sequences. Qualitative mathematical rules are used to propagate the input probabilities through the BT-AT combined.

The outputs of the approach show important results in terms of representation of risk scenarios as well as in likelihood evaluation. 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 result show that the moves from purely security MCs to mix safety/security MCs is the safest risk treatment.

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

ACKNOWLEDGMENTS

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

REFERENCES

27005, I. (2011). Information technology–security techniques information security risk management. *ISO/IEC 66*.

Abdo, H. & J. Flaus (2015). A mixed fuzzy probabilistic approach for risk assessment of dynamic systems. *IFAC Papers On Line* 48(3), 960–965.

Abdo, H. & J.-M. Flaus. Uncertainty quantification in bow-tie analysis: A mixed approach of fuzzy theory with dempstershafer theory of evidence. In *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016 (Glasgow, Scotland, 25–29 September 2016)*, pp. 2743–2750. Taylor & Francis.

Abdo, H. & J.-M. Flaus (2016). Uncertainty quantification in dynamic system risk assessment: a new approach with randomness and fuzzy theory. *International Journal of Production Research*, 1–24.

ANSSI (January 2014). *Classification Method and Key Measures*. ANSSI: Agence nationale de la sécurité des systèmes d'information.

Arunraj, N. & J. Maiti (2007). Risk-based maintenance techniques and applications. *Journal of Hazardous Materials* 142(3), 653–661.

De Dianous, V., C. Deust, C. Bouissou, R. Farret, & S. Chaumette (2007). Prise en compte de la probabilité dans les études de dangers. *Préventique Sécurité* (95), 32–37.

Dell, I. (2015, 01). Dell Security Annual Threat Report. Technical report.

Ferdous, R., F. Khan, R. Sadiq, P. Amyotte, & B. Veitch (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. Technical report, Software Engineering Institute.

Fovino, I.N. & M. Masera (2006). Through the description of attacks: A multidimensional view. In *International Conference on Computer Safety, Reliability, and Security*, pp. 15–28. Springer.

Fovino, I.N., M. Masera, & A. De Cian (2009). Integrating cyber attacks within fault trees. *Reliability Engineering & System Safety* 94(9), 1394–1402.

INERIS (2015). Agrégation semi-quantitative des probabilités dans les études de dangers des installations classées – omega probabilités.

Johnson, C. (2012). Cybersafety: on the interactions between cybersecurity and the software engineering of safety-critical systems. *Achieving System Safety*, 85–96.

Kaplan, S. & B.J. Garrick (1981). On the quantitative definition of risk. *Risk analysis* 1(1), 11–27.

Kornecki, A.J. & J. Zalewski (2010). Safety and security in industrial control. In *Proceedings of the Sixth Annual Workshop Cyber Security and Information Intelligence Research*, pp. 77. ACM.

Kriaa, S., L. Pietre-Cambacedes, M. Bouissou, & Y. Halgand (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety* 139, 156–178.

Purdy, G. (2010). Iso 31000: 2009 setting a new standard for risk management. *Risk analysis* 30(6), 881–886.

Schneider Electric, T. R.S.S. (2012). Scada systems. Technical report, Schneider Electric, Ontario K2 K 2 A9, Canada. Schneier, B. (1998). Modeling security threats. In *Dr. Dobbs Journal*.

Shin, J., H. Son, & G. Heo (2016). Cyber security risk evaluation of a nuclear i&c system using bayesian networks and event trees. *Nuclear Engineering and Technology*.

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