A new model-based risk analysis approach that generate cyberattacks scenarios and combine them with safety risks

Tamara Oueidat, Jean-Marie Flaus, François Massé

A new model-based risk analysis approach that generate cyberattacks scenarios and combine them with safety risks

Tamara Oueidat

G-SCOP laboratory, Grenoble Alpes University, France. E-mail: tamara.oueidat@grenoble-inp.fr

Jean-Marie Flaus

G-SCOP laboratory, Grenoble Alpes University, France. E-mail: jean-marie.flaus@grenoble-inp.fr

François Massé

INERIS, Direction des Risques Accidentels, France. E-mail: francois.masse@ineris.fr

For many years, the introduction of connected systems and digital technology in critical industries worldwide makes them vulnerable to cyberattacks that can lead to undesirable safety accidents. Thus, analysing these attacks becomes an important matter during risk analysis. In most proposed risk analysis approaches applied in the industries, the safety subjects are taking into consideration without analysing the cyberattack that can lead to the same dangerous phenomenon as a safety incident, the safety and security subjects are treated separately, despite the common consequences and the interdependencies between them. Therefore, there is a strong interest in the development of risk analysis approaches combining safety and security, particularly in the process industry, which is a major potential hazard for local populations and the environment. In this article, a new model-based risk analysis approach is proposed, it presents a new way to generate the cyberattacks systematically based on the modelling system architecture and a list of generic vulnerabilities encountered on industrial systems. A likelihood evaluation for these attacks is presented with their combination with the safety risks.

Keywords: Safety, Cybersecurity, Cyberattack, Accidental situation, Undesirable event, Risk analysis.

1. Introduction

The risks related to safety in this article are associated with internal accidents caused by a system failure or some combination of accidental conditions, external accidents or any non-deliberate source of hazards that can harm people and the environment. While, the cybersecurity discipline in this article is related to internal or external deliberate threats caused by malicious cyberattacks which can be accomplished physically or by cyber means.

Recently, industrial systems worldwide are integrated by automated systems with communicating and digital technologies, like the use of connected objects (Industrial Internet of Things IIoT), the connection to the internet or the remote access, the interconnection between IT (Information Technology) and OT (Operation Technology) (Flaus 2019). This shift increases the industrial infrastructures attack surface and makes them more vulnerable to cyberattacks, which can affect system safety. Therefore, cybersecurity became an important matter of the critical industries and their risk analysis (ISA 2020). Most industries focused on safety subjects without necessarily taking into consideration that a cyberattack can compromise the safety of a system. Recently, many security incidents that affect the industrial systems have been observed such as NotPeya or TRITON (Hemsley, Fisher, and others 2018). These critical automated industries should raise awareness about the risks related to cybersecurity.

For risk analysis, a large number of methods have been proposed, most of them evaluate separately the risks related to safety and security, despite the common consequences. Some risk analysis approaches for safety are HAZOP (Ericson and others 2015), FMEA (Schmittner et al. 2014), Bow-Tie (Ferdous et al. 2012), PHA (Flaus 2019), and for security are Attack Tree (Fovino and Masera 2006), EBIOS (Flaus 2019), CORAS (Lund, Solhaug, and Stølen 2010). In recent years, the joint treatment of safety and security has been seen as necessary and a large number of safety and security risk analysis approaches have been proposed, like Combined ATBT (Abdo et al. 2017), S-Cube (Kriaa, Bouissou, and Laarouchi 2015), FMVEA (Schmittner et al. 2015), STPA-SafeSec (Friedberg et al. 2017), etc. Each of these approaches presents limits, in the system modelling, or the generation of attack scenarios, or the risk evaluation. This article aims to propose a model-based risk analysis approach that provides a new way to generate the cyberattacks scenarios encountered on industrial systems, with an evaluation of their likelihood, and their combination with the safety risks leading to the same physical undesirable events. This generation will be based on data collected from industries like the physical undesirable events, the system architecture, and the organizational policies applied. In this article, section 2 presents a motivation example to combine safety and security in risk analysis. Section 3 highlights the global idea of our model-based approach and its steps illustrated with an example:

Proceedings of the 31th European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud and Christophe Berenguer
 Published by Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2021-paper

Data collection, generation of cyberattacks scenarios with a likelihood evaluation, and their combination with the safety risks. Section 4 summarises and concludes this article.

2. Motivation example

The problem in critical automated industries is that a cyberattack can impact the whole system's safety, and these cyberattacks are not taken into consideration in risk analysis in most industries. Along this article, we focus on critical automated industrial systems. An example is illustrated to present the importance to integrate safety and security in risk analysis, and Figure 1 presents the different levels of Industrial Control Systems (ICS) and the interconnection between levels.

- Field level: the lowest level of ICS which includes the sensors, valves, actuators, etc. that are directly connected to the plant. They generate and collect data used in the other levels to control the industrial process (Abdo et al. 2017).
- Control level: this level includes PLCs (Programmable Logic Controller), that are linked to the field and supervision levels. It can contain stations for the programming and configuration for the PLC.
- Supervision level: this level presents the SCADA system, it includes supervision stations, servers, workstations, etc. It aims to monitor and maintain the process and the equipment.

The example concerns a simplification of a polymerization process. It is composed of two reactors worked in series and with similar instrumentation and operation. A runway reaction in these reactors can lead to a pressure increase and a toxic release to the atmosphere. Sensors and actuators (valves, pumps) are used for the regulation and safety of the chemical process. These components are controlled by two standard PLC for the regulation and a safety PLC to control the safety barriers (inhibitor system to control the pressure in the two reactors), and they are supervised by the SCADA system. There are a physical access to sensors and actuators for the local operation. At the control level, a station for the configuration of the PLC has remote access, and at the supervision level, an office workstation connected to the SCADA system has a connection to the internet and can receives emails from outside the site.

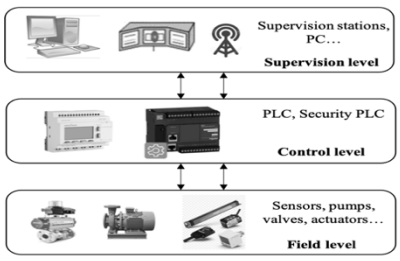

Fig. 1. Industrial Control System.

Different physical undesirable events can occur and have a critical impact on the system, for example, the increasing of pressure in one of the reactors leading to an explosion. This event is caused by an accidental situation such as the failure of a sensor, valve, or PLC, or by a cyberattack through for instance a no secure remote access to change the configuration and the functionality of the PLC, or a cyberattack on the workstation through the internet connection to change the functionality of physical components. Therefore, there is a strong interest in the development of risk analysis approaches combining the risks related to safety and security, particularly in the critical process industry.

In the following, the global idea of our proposed risk analysis approach combining safety and security is presented, with the detailed process to generate the cyberattacks scenarios and their likelihood evaluation.

3. Proposed risk analysis approach

In this section, we will outline the steps of the proposed model-based risk analysis approach and the new way to generate the cyberattacks scenarios which can be found on any industrial site. These attacks will be combined with the safety risks leading to the same physical undesirable events.

This model-based approach responds to the needs of risk analysis on industrial installations, it aims at identifying and evaluating the critical cyberattack scenarios from the perspective of the people's and environment safety to control them over time and organize the response. This proposed approach integrates the best characteristics and analysis process sorted from the existing approaches presented and classified in a review (Oueidat, Flaus, and Massé 2020).

The global idea of our approach is to define a formal, systematic, and guided process that allows to reach a sufficient level of detail to be relevant while being simple, to implement on an industrial site. The analysis has to be time and cost effective and applicable by that employees which are not experts on the cybersecurity field (Dürrwang, Beckers, and Kriesten 2017).

The risk analysis process is based on existing data from the industrial site, including the physical undesirable events to be analysed, the system mapping and cartography to model its physical and IT architecture at each ICS level, the vulnerabilities, the policy and barriers applied to be used in the generation of the attack scenarios. This generation aims to present the generic attack scenarios in a guided meta-model at each ICS level.

The approach is divided into two parts; the first part is to collect the needed data from the industry, including the physical undesirable events, the system architecture, and the

vulnerabilities at each level of the industrial system. The second part is to generate the cyberattack scenarios with an evaluation of their likelihoods and their combination with the accidental situations. This part includes also the estimation of the risks level and their treatments by proposing new safety and security measures.

3.1. *Part 1: Collect data*

This part of the approach aims to collect data needed to generate the cyberattacks scenarios and to combine them with the safety risks. These data are collected form historical databases and existing data on an industrial site. This part aims to collect the undesirable events from existing risk analysis, the system components and their interactions, and the list of vulnerabilities. This part is composed of three steps:

3.1.1. *Listing the physical undesirable events*

The objective of this step is to identify the list of physical undesirable events that must be analysed, with their initiating events that can accidental, malicious (cyberattacks), or a combination of both. These events are identified from the existing classical safety risk analysis approach used in the industry such as Bow Tie, HAZOP, FMEA, PHA, etc. In this step, the undesirable events that may occur following only a cyberattack and which are not presented in the safety risk analysis are defined. Each undesirable event is listed with its impact level chosen from these values: Disastrous, Catastrophic, Important, Serious, and Moderate. The events which have an impact level more or equal to Serious must be analysed.

3.1.2. Modelling the *system architecture*

Based on the industry cartography, the physical and IT system architecture is modelled as well as the components, and the interconnection between them. This step is necessary to describe the system functionalities, to identify the vulnerabilities existing on the component attributes and possibly targeted of attacks, and to generate the attack scenarios from attack surfaces existing on the component attributes. This modelling includes the critical components involved in the occurrence of undesirable events or the components that must have high availability for the process. These components with their attributes are modelled into tables. The attributes for the components are presenting below:

- Physical access: if the components have protected physical access (Yes/No);
- Contributor: the persons who have physical access to the components;
- Critical software implemented on a component (anti-virus, anti-spam, operating system, automates…);
- External interaction: if a component has remote access or connection to the internet;
- Removable media: if they can be branched on a component (Yes/No);
- Receipt of emails: If a component receives emails from outside (Yes/No);
- Other attributes can be defined: the type of the internal connection (wireless or wired connection), the communication protocols used (Fieldbus, Modbus, Ethernet, TCP/IP).

3.1.3. *Identification of the vulnerabilities*

This step aims to define the generic vulnerabilities at each level of the industrial system, which will be used in the generation of the attack scenarios. It is based on a list of generic organizational policies applied to the industry with a level of applicability. The list is presented by ICS levels since at each level the policies can be applied in different ways. A qualitative scale for the applicability levels is defined and presented in Table 1. These policies with their applicability levels are considered generic vulnerabilities. Some examples of these policies: the policies for using the removable media on the workstations, for the anti-virus implemented, for the physical access, for the connection to the internet, etc. In this step, if there are other specific policies applied, they can be added to the list and they can be considered as specific vulnerabilities.

Table 1. The scale of the applicability level of organizational policies

Level of applicability	Designation
4	No existing rule and dispositive
3	Rule and dispositive partially applied
2	Sufficient rule and dispositive applied systematically almost everywhere
1	Sufficient rule and dispositive and well applied systematically (complete and well-adapted)
N/A	Not Applicable

Once the physical undesirable events are identified, the system architecture is modelled, and the generic vulnerabilities are defined, the generic attack scenarios can be generated and combined to safety risks in the next part.

3.2. *Part 2: Generation of attacks scenarios and the combination with the safety risks*

Based on the data collected, the generic cyberattacks scenarios that can be encountered on industrial sites and leading to the undesirable events with the accidental situations are generated with a likelihood evaluation at each level of ICS separately, since at each level it can exist different attacks with different likelihoods. These scenarios are combined with accidental situations, with an estimation of the risk levels and their treatments.

3.2.1. *Generation of attack scenarios*

The generation of these cyberattack scenarios is based on the data collected before: the attributes of the components modelled and the vulnerabilities. To execute an attack, the attacker needs to go through one or more steps to reach its objective. As a starting point for the attack execution, the five principles attack surfaces existing on the components of each industrial level. These surfaces are the following:

- Physical access: if there is unprotected physical access to the components of each level;
- Phishing email: if there are components that receive emails from outside at different ICS levels;
- Remote access: if there are components that have remote access from outside the industry;
- Internet connection: if there are components which are connected to the internet;
- No secure software or software with a backdoor: if there are components that are implemented by vulnerable and no-secure software.

This generation of attack scenarios is performed using a meta-model representing the sequence of events to execute the objective attack with an evaluation of its likelihood. This meta-model is presented in Figure 2. For each ICS level, each attack surface is taken into account, if the attack surface exists at an ICS level, the attack scenarios will be defined. Otherwise, the next attack surface for the same ICS level will be taken to define the existing attack scenarios, and so on to define all the attack scenarios of all the attack surfaces at all ICS levels. If on an ICS level, exists different zones of components with different attributes and organisational policies, the meta-model to generate the cyberattacks will be applied separately to each zone.

If the attack surface exists on a given ICS level, the scenarios are defined in this way: For the execution of the attack, a sequence of one or more security events can occur. The occurrence of security events is due either to the occurrence of one or more security sub-events connected by the gates AND/OR, or just because of the need for a secondary security event. Each sub-event is a combination of two factors vulnerabilities (organisational policies) and the technical step required to exploit the vulnerability.

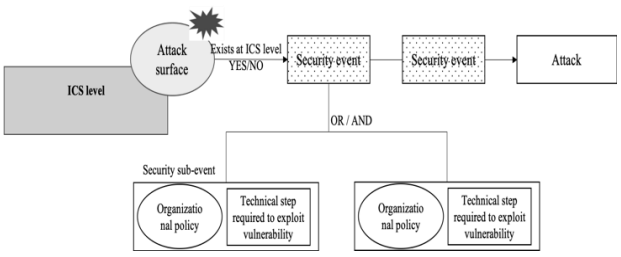

Fig. 2. The meta-model for attack scenarios

From this meta-model, for each attack surface and ICS level, the generic attack scenarios that can be encountered on any industrial site are generated. All the generated scenarios will be considered as a guide to applying this step on a real case study, by taking the scenarios that may exist on the ICS level of each site. An evaluation of these attack scenarios likelihoods will be presented in the next subsection.

3.2.2. *Likelihood evaluation*

To evaluate the occurrence likelihood of the attack, the first step is to assess the likelihood of the security sub-events, then that of the security events. Figure 3 presents the data added to the meta-model to evaluate the likelihoods. First, the security sub-events likelihoods (likelihood 1) evaluation requires for each vulnerability to specify the applicability level of the policies from the list of vulnerabilities, and to specify for each technical step its difficulty level to be executed, this value is defined from the scale in Table 2 (Abdo et al. 2017). A combination of these two values (vulnerability and difficulty levels) is presented in the scale in Table 3, and the combined values are assigned to designations in Table 4 to determine the likelihoods of security sub-events. Second, to evaluate the likelihood of occurrence for security security events (likelihood 2), if the occurrence of a security event is due the occurrence of security sub-events connected with the gate OR, the Maximal value of the different values of likelihood of security sub-events is taken and given to the security event, or if the security sub-events are connected with the gate AND, the Minimal value of the different values of likelihood is taken and given to the security event. Finally, to determine the likelihood of the attacks (likelihood 3), for the sequence of security events, the minimal value of likelihoods is taken.

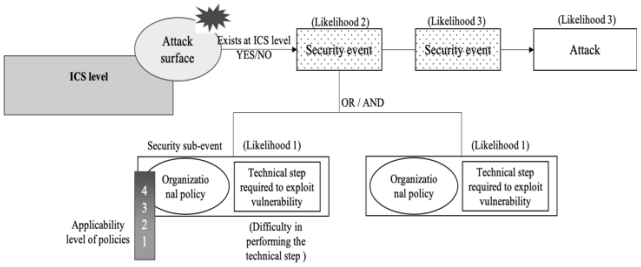

Fig. 3. The meta-model with evaluation the likelihood

Table 2. The scale of the difficulty levels to execute the technical step

Difficulty level	Designation
1	Trivial (T): Little technical skill required
2	Moderate (M): Average cyber hacking skills required
3	Difficult (D): Demands a high degree of technical expertise systematically almost everywhere

Table 2. Continued

4	Very Difficult (VD): Beyond the known capability of today's best hackers

Table 3. Combination of applicability and difficulty levels

Likelihood levels		Difficulty levels T	M	D	VD
Applicability levels	4	4	4	3	2
	3	4	3	3	1
	2	3	2	2	1
	1	2	2	1	1

Therefore, to apply this meta-model to a real case study, the analysts must take the existing attack scenarios in a given industrial system and must fill the applicability levels of the policies and the difficulty levels to execute the technical step, in order to evaluate the security sub-events, the security events, and the attacks likelihoods. Once the attack scenarios are generated with their occurrence likelihood, they will be combined with the accidental situations leading to the same undesirable physical event in the next subsection.

Table 4. Likelihood levels designation

Likelihood level	Designation
1	Low: High unlikely to occur, an attack is hard to perform
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, the system in an easy target

3.2.3. *Combination of the attacks with the safety risks*

The attack scenarios with their likelihoods are ready, and they will be combined with the accidental situations leading to the same initiating events of the physical undesirable event. Figure 4 presents a systematic diagram of the cyber Bow-Tie to combine safety and security events, it is based on the Bow-Tie concept (Ferdous et al. 2012) by integrating the attacks. Bow-Tie is a very prominent method to identify and analyse safety risks. The occurrence of the undesirable events is started by the occurrence of one or more initiating events, which can be from safety events (searched from the classical safety risk analysis), or security events (searched from the attack scenarios), or from a combination of these two types of events. Secondary events occur after the occurrence of the initiating events, it can exist a sequence of many secondary events for reaching the undesirable events. In this combination schema, the safety and security barriers applied to the industrial system are presented, and following them, many undesirable events can happen with different impact levels. The dysfunction of the barriers can happen also due to an attack or failure situation.

Once the combination of safety and security events is ready, the occurrence likelihood of undesirable events is evaluated. To evaluate the likelihood of undesirable events, the notion of Minimal Cut sets (MCs) is used, which represents the smallest combinations of safety and security events leading to the undesirable events. The MCs will be determined, then the likelihood of each input event will be characterized using two different scales (L_s, L_f) representing respectively the likelihood of security events (searched from the step before) and the likelihood of safety events (searched from the existing classical safety risk analysis approach). A double quotation is used since there is a difference between the likelihood of safety and security events (Abdo et al. 2017). Finally, the likelihood of each MC will be quantified by taking the minimum value of the likelihood of the input events (INERIS 2015). The next step is to estimate the risk level of the undesirable events analysed from these scales: unacceptable risk, risk to be reduced, acceptable risk. The risk level is defined depending on the likelihood and the impacts based on a predefined risk matrix, which is used by the French authorities. To reduce the criticality of unacceptable risks and the risks to be reduced, safety and security measures will be proposed, or some of the organisational policies applied will be updated or modified.

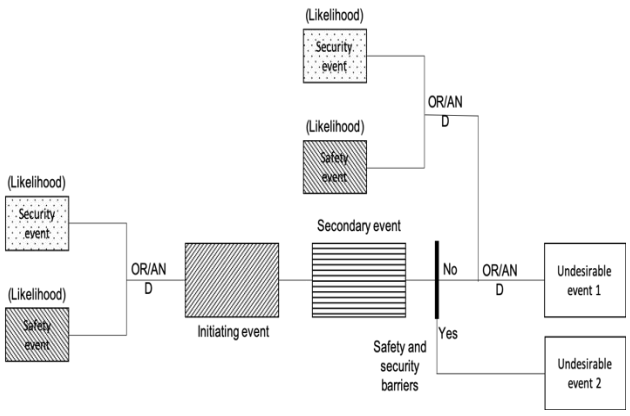

Fig. 4. The combination of safety and security events

3.3. *Example and results*

To illustrate the steps of the proposed approach, an example is presented in this section. The physical undesirable event from the case study of the polymerisation system is analysed here, which is the explosion of the reactors, and its impact is catastrophic. Based on an existing Bow-Tie for this case study, the initiating and secondary events of this undesirable event are defined. One of these initiating events is analysed here, which is the excess of the catalyst in the reactor, that can occur due to an accidental situation or to a cyberattack. The components responsible for the occurrence of the initiating event and that must be modelled are two sensors used to regulate the introduction of the catalyst in the reactors, a regulation valve, and a TOR valve to control the injection of the catalyst. Also, the components responsible for the inhibitor system are modelled. These components of the field level are connected to the standard PLC for the regulation component at the control level and to the safety PLC for the inhibitor system. The PLC is connected to a configuration station used for maintenance, programming and configuration. All the physical components have physical access by technicians, operators, visitors, and external sub-contractors. Once the components are modelled with their attributes, the list of vulnerabilities that can be exploited is defined, the organisational policies applied with their applicability levels are defined. At the PLC zone of the control level: Employees security awareness (level: 3), Access to room with keys or badges (level: 2), Visitors accompaniment (level: 4). At the configuration station of the control level: Policy to generate the passwords for logical access (level: 3), Passwords readable and clear (level:3), Policy for account management (level: 2), Policy to use removable media (level: N/A). In this example, the data collected are only from the field and control levels.

The data needed for the identification of attack scenarios are ready. Some attack scenario examples with their likelihood evaluation existing in this case study are presented. Figure 5 presents the attack scenarios on the control level (PLC zone) that can be encountered through the physical access on the PLC which has uncontrolled physical access by external visitors, service company and operators. The attacker gains unauthorized physical access through one of these three security sub-events, to disconnect the PLC from the physical process. Figure 6 presents the attack scenarios through the physical access on the PLC configuration station of the control level. The attacker gains unauthorized physical access, and he can modify the PLC configuration and functionality, by having unauthorized logical access through access to authentication data or through the user accounts without restrictions, or by plugging in removable media with malicious content in order to execute malware on the station. Now, the attack scenarios are ready and will be combined with the safety events.

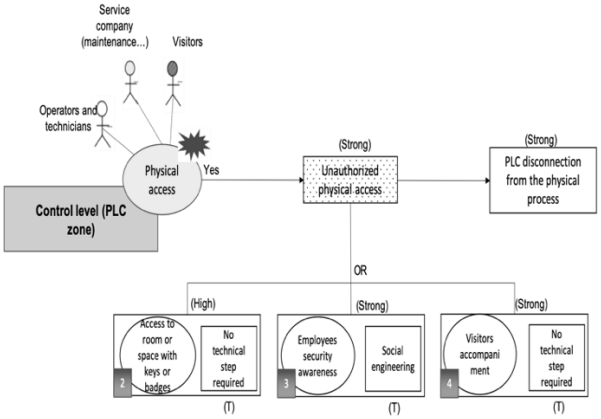

Fig. 5. Attack scenarios on PLCs zone

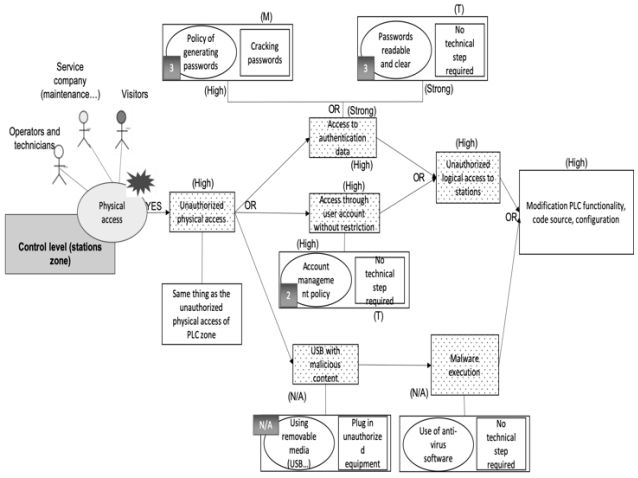

Fig. 6. Attack scenarios on stations zone

Due to the attack to the PLC, its disconnection from the physical process, or due to the attack of modification of the PLC configuration and functionality through the physical access surface, or due to the safety event the technical failure of the PLC, the excess of the catalyst can occur and cause the runway of reactors. The dysfunction of the inhibitor system can occur due to the attack of changing the safety PLC configuration or due to the safety event of technical failure of the safety PLC, causing the occurrence of the overpressure in reactors and then an explosion. These safety and security events are combined together in the same graphical model, with their likelihoods (Figure 7). The likelihoods of the safety and security events are evaluated with the two scales. After the MCs causing the occurrence of the undesirable event are listed in table 5, in this example, MC1 is composed only of safety events; MC5, MC6 are

composed only of security events; MC2, MC3, MC4 are composed from a combination of safety and security events, and the likelihood for each MC is evaluated. This likelihood evaluation is done with a double scale, by taking the minimum value of the safety or security events likelihoods. The likelihood level for each MC is defined from the scale in Table 6. The level risk of the undesirable event (impact catastrophic) is estimated through each defined MC, and it is unacceptable (Table 5). To treat this risk, an update for the policy to secure the component local, or termly maintenance for the equipment, or more security formations for employees can be solutions to make the risks acceptable.

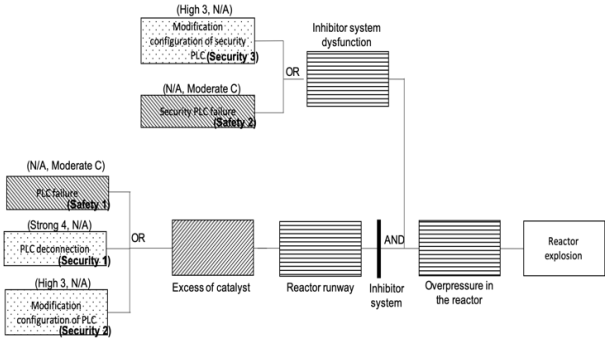

Fig. 7. Bow-Tie with the attacks

Table 5. Minimal Cut sets with their likelihoods

MCs	Likelihood	Level	Risk level
MC1: Safety 1, Safety 2	(N/A, C)	M	Unacceptable
MC2: Safety 1, Security 3	(3, C)	M	Unacceptable
MC3: Security 1, Safety 2	(4, C)	M	Unacceptable
MC4: Security 2, Safety 2	(3, C)	M	Unacceptable
MC5: Security 1, Security 3	(3, N/A)	H	Unacceptable
MC6: Security 2, Security 3	(3, N/A)	H	Unacceptable

After applying the proposed approach on a case study, the risk analysis process of our approach is guided and systematic, and easy to be applied on any industrial system. The process aims to model the system architecture, to generate the attack scenarios systematically based on the system modelling and the vulnerabilities. Its process can cover all the system lifecycle phases (development, deployment, and exploitation). This risk analysis process also covers the three main steps of the standard ISO 31000 (Flaus 2019): Risk identification, risk analysis, and risk evaluation. It can evaluate the risks related to safety and security qualitatively, and quantitatively depending on the analysed industrial system, if exist historical databases for the likelihood and impact values. All these criteria are presented in (Oueidat, Flaus, and Massé 2020). This approach will be applied in a real case study for a chemical critical industry.

Table 6. Overall likelihood scale

Likelihood levels		Likelihood of safety events E	D	C	B	A	N/A
Likelihood of security events	N/A	VL	L	M	H	VH	[redacted]
	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

VL: Very Low; **L**: Low; **M**: Moderate; **H**: High; **VH**: Very High

4. Conclusion and perspectives

The integration of safety and security in risk analysis for critical industrial systems became important. Due to the integration of new technologies in their automated systems, these critical industries became vulnerable to cyberattacks. These attacks can harm the system's safety. Safety and security have many differences, but also have similarities, interactions, and interdependencies. For these reasons, many authors proposed and developed approaches to integrate safety and security in risk analysis. But, there is a need to propose a risk analysis approach based on the best characteristics and analysis process sorted from the existing approaches (Oueidat, Flaus, and Massé 2020), to identify and evaluate the critical cyberattack scenarios from the perspective of the safety of people and the environment. In this article, our new model-based risk analysis approach is proposed, it aims to model the physical and IT architecture of the industrial system, identify the vulnerabilities, generate the attacks scenarios in a systematic way based on the system architecture and the vulnerabilities, also evaluate the likelihood of these attacks, and then to integrate them to the bow-tie that representing the accidental situations, leading to the same undesirable events. This approach to be improved, it will be applied to a real case study of a chemical industry that can have risks with serious consequences on the installation and the environment.

References

Abdo, H, Mohamad Kaouk, Jean-Marie Flaus, and François Masse. 2017. “A New Approach That Considers Cyber Security within Industrial Risk Analysis Using a Cyber Bow-Tie Analysis.”

Dürrwang, Jürgen, Kristian Beckers, and Reiner Kriesten. 2017. “A Lightweight Threat Analysis Approach Intertwining Safety and Security for the Automotive Domain.” In *International Conference on Computer Safety, Reliability, and Security*, 305–19. Springer.

Ericson, Clifton A and others. 2015. *Hazard Analysis Techniques for System Safety*. John Wiley & Sons.

Ferdous, Refaul, Faisal Khan, Rehan Sadiq, Paul Amyotte, and Brian Veitch. 2012. “Handling and Updating Uncertain Information in Bow-Tie Analysis.” *Journal of Loss Prevention in the Process Industries* 25 (1): 8–19.

Flaus, Jean-Marie. 2019. *Cybersécurité Des Systèmes Industriels*. ISTE Editions.

Fovino, Igor Nai, and Marcelo Masera. 2006. “Through the Description of Attacks: A Multidimensional View.” In *International Conference on Computer Safety, Reliability, and Security*, 15–28. Springer.

Friedberg, Ivo, Kieran McLaughlin, Paul Smith, David Laverty, and Sakir Sezer. 2017. “STPA-SafeSec: Safety and Security Analysis for Cyber-Physical Systems.” *Journal of Information Security and Applications* 34: 183–96.

Hemsley, Kevin E, E Fisher, and others. 2018. “History of Industrial Control System Cyber Incidents.” Idaho National Lab.(INL), Idaho Falls, ID (United States).

INERIS. 2015. “Agrégation Semi-Quantitative Des Probabilits Dans Les Études de Dangers Des Installations Classées - Omega Probabilités.”

ISA. 2020. “ISA-62443-3-3 Security for Industrial Automation and Control Systems - Security Risk Assessment for System Design.”

Kriaa, S, M Bouissou, and Y Laarouchi. 2015. “A Model Based Approach for SCADA Safety and Security Joint Modelling: S-Cube.”

Lund, Mass Soldal, Bjørnar Solhaug, and Ketil Stølen. 2010. *Model-Driven Risk Analysis: The CORAS Approach*. Springer Science & Business Media.

Oueidat, Tamara, Jean-Marie Flaus, and François Massé. 2020. “A Review of Combined Safety and Security Risk Analysis Approaches: Application and Classification.” In *2020 International Conference on Control, Automation and Diagnosis (ICCAD)*, 1–7. IEEE.

Schmittner, Christoph, Thomas Gruber, Peter Puschner, and Erwin Schoitsch. 2014. “Security Application of Failure Mode and Effect Analysis (FMEA).” In *International Conference on Computer Safety, Reliability, and Security*, 310–25. Springer.

Schmittner, Christoph, Zhendong Ma, Erwin Schoitsch, and Thomas Gruber. 2015. “A Case Study of Fmvea and Chassis as Safety and Security Co-Analysis Method for Automotive Cyber-Physical Systems.” In *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, 69–80. ACM.