A New Way to Generate Automatically the Attacks Scenarios and Combine them with Safety Risks

Tamara Oueidat, Jean-Marie Flaus, François Massé

A new way to generate automatically the attacks 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

Industrial systems have undergone a transformation with the introduction of connected systems and digital technology into their control systems, making them open to new cybersecurity threats that affect the safety of the system with the accidental situations. Therefore, analysing these new threats becomes crucial during risk analysis. A significant number of risk analysis approaches have been proposed to treat independently the safety and cybersecurity issues. There is a strong interest in developing risk analysis approaches that combine safety and cybersecurity, particularly in the critical process industry, which poses a significant risk to local populations and the environment. The goal of this article is to present a new developed risk analysis approach that aims to generate the possible attacks scenarios that can occur in industrial systems systematically in new models, and generate these scenarios automatically using a computerized code to simplify the risk analysis process; especially for users who are not experts in the domain of cybersecurity.

Keywords: Cybersecurity, Attack scenarios, Risk analysis, Safety, Industrial systems, meta-models.

1. Introduction

In industrial systems, safety and cybersecurity are two different concepts that refer to different types of risks. In terms of risk analysis, they differ, but they also have similarities and interdependencies (Piètre-Cambacédès 2010). Traditional industrial systems relied on mechanical and electrotechnical devices, closed systems, and human resources, and they focus in risk analysis solely on the safety issues. In recent years, industrial systems have increasingly integrated digital and communication technologies into their automated control systems, such as the internet connectivity and the remote access to control systems (Flaus 2019), the convergence between the Information Technology (IT) and the Operational Technology (OT), and so on. This digitization makes industrial systems more vulnerable to cyberattacks and exposes them to new cybersecurity threats that could affect the system safety. Many security incidents affecting the industrial systems, such as NotPeya, TRITON, and others (Hemsley, Fisher, and others 2018), have been observed around the world.

Cybersecurity has become a significant issue for critical industrial systems, and it should be treated as part of the risk analysis process. Thus, industrial systems should be more conscious of cybersecurity and raise awareness about the risks related to cybersecurity. For risk analysis, a wide variety of approaches have been proposed, the majority of them evaluate the risks associated to safety and cybersecurity independently, despite the similar outcomes consequences. HAZOP (Wei, Matsubara, and Takada 2016), FMEA (Schmittner et al. 2014), Bow-Tie (Ferdous et al. 2012), PHA (Mohr 2002) are some risk analysis approaches for safety, and Attack Tree (Fovino and Masera 2006), EBIOS (Flaus 2019), CORAS (Lund, Solhaug, and Stølen 2010) are some risk analysis approaches cybersecurity. In recent years, it has been recognized as vital to joint safety and cybersecurity together, and a large number of safety and cybersecurity risk analysis approaches have been proposed. In section 2 of the related work, several of these developed approaches are shown. Each of these approaches has limits in terms of the system modelling, the generation of attack scenarios, and the risk evaluation. The purpose of this paper is to present a new model-based risk analysis approach that provides a new way to automatically generate the attack scenarios that may exist on a case study when using the proposed approach, and then integrate them with safety risks in the same Bow-Tie. Section 3 outlines the overall concept of our approach, as well as the steps for automatically generating the attack scenarios. Section 4 summarizes and concludes this article with future work.

2. Related work

Since the relevance of merging safety and cybersecurity in risk analysis for critical industrial systems has grown, a shift has occurred by developing risk analysis approaches that include processes that address both safety and cybersecurity concerns. There are several approaches that aim to extend traditional safety risk analysis approaches to include cybersecurity risks, such as FMVEA (adaptation of FMEA) (Schmittner, Ma, and Smith 2014), Cyber HAZOP (Wei, Matsubara, and Takada 2016), SECFT (adaptation CFT) (Steiner and Liggesmeyer 2014), or to extend cybersecurity risk analysis approaches to include safety risks, such as the extension of TVRA (Reichenbach et al. 2012). Other approaches are attempting to merge existing safety and cybersecurity approaches, such as SAHARA (Macher et al. 2015), ATBT (Abdo et al. 2017), and others. Other approaches were created from scratch to incorporate safety and cybersecurity concerns in the same analysis, such as S-cube (Kriaa, Bouissou, and Laarouchi 2015), CHASSIS (Schmittner et al. 2015), Integrating security in BDMP (Piètre-Cambacédès and Bouissou 2010). Other approaches have been offered and based on the STPA process, which treats accidents and losses as a dynamic control problem, with an accident occurring as a result of a behaviour fault on the control, not as a consequence of a failure (Young and Leveson 2013). Examples of some approaches in this category: STPA-SafeSec (Friedberg et al. 2017), STPA and STRIDE (de Souza et al. 2020), Combination of STPA-Sec with FMVEA (Temple et al. 2017).

Despite the existence of various limits, such as in the system modelling which represents an important step before starting the risk analysis, the technique to define the attack scenarios in a no formal and systematic way, the amount of complexity, and detail when using the approach, each developed risk analysis approach has advantages and is good to implement. In this paper, we propose a new model-based risk analysis approaches that considers the links between safety and cybersecurity during the risk analysis process, with the main goals of covering the limits of the existing approaches and making the steps of defining the attack scenarios easier and simpler to apply with a sufficient level of detail by taking into account the level of cybersecurity expertise of users. The following section illustrates our proposed approach, which includes the contribution of the automatic generation of attack scenarios.

3. The proposed risk analysis approach

In this section, our new proposed risk analysis approach is provided, it tries to generate the attacks and integrate them with the safety risks, and it simplifies the risk analysis process phases. The following are main steps of our approach:

- The construction of a model that explains the industrial installation.
- The proposition of a guide to help defining and searching for possible vulnerabilities.
- The proposition of new meta-models for defining the attack scenarios.
- The automatic generation of cyberattacks.
- The combination of the generated attacks with the safety risks in the same meta-model.

We will focus in this article on the steps for generating the attack scenarios in meta-models and generating them automatically for a case study. To carry out these steps, some data from the industrial installation is required, such as the components of the system architecture and their attributes (physical access, internet connection, remote access, removable media, email reception, software), which can reveal important vulnerabilities in the industrial system and are gathered from the system mapping and cartography; The list of vulnerabilities generated from a check-list and guide for the vulnerabilities that may be found on industrial systems, these data of vulnerabilities are gathered from the organisational policies and security barriers that are used and applied on an industrial system. The data gathered aids in the generation of the attack scenarios. In the next section, the principle of the proposed risk analysis approach is provided. Then, there is the way to generate the attack scenarios in meta-models, as well as how to do it automatically.

3.1. Principle of the proposed approach

The risk analysis approach is based on a Knowledge Base KB, which contains the defined generic list of vulnerabilities as well as the generic attack scenarios developed after by meta- models. The generic data and the meta-models of the KB, along with the system architecture (components and attributes), provide the inputs for automatically generating the attack scenarios, which are considered the output of the approach.

Figure 1 depicts the principle of the approach. The processing of an algorithm using data produced from the meta-models of attack scenarios and the other inputs leads in the automatic generation of the existing attack scenarios on a case study. Therefore, the contribution here is the automatic generation of attack scenarios with the generation of the data in the KB. In the following section, the way to generate the different attack scenarios that can exist on an industrial system is discussed, along with the automatic generation of these scenarios.

3.2. Generation of attack scenarios in meta- models

To execute a cyberattack, the attacker must go through one or more steps to achieve its goal. A starting point for a cyberattack is the attack surface exiting on the component or any level of an Industrial Control System. Based on the attributes of the components, five attack surfaces are established, and they can be sources of vulnerability leading to the execution of cyberattacks.

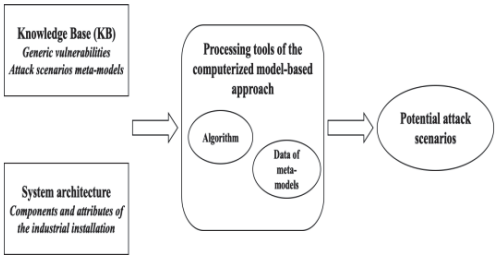

Fig. 1.The principle of the proposed risk analysis approach

- Physical access: an attacker can use uncontrolled physical access to gain unauthorized physical access and carry out his or her attack.
- Email reception: a component that receives emails from outside the industry can be used to carry out cyberattacks via phishing emails.
- Remote access: if a component can be accessed remotely, it can become a target for cyberattacks, if the access is unprotected and unregulated.
- Internet connection: if a component is connected to the internet, it can become a target for cyberattacks if the connection is insecure and unregulated.
- Unsecured implemented software can be used to launch cyberattacks.

The possible attack scenarios are generated into meta-models; each meta-model contains the existing attack surface on each zone of the Industrial Control System (ICS) level, as well as the different steps to conduct an attack through this surface. We work on the three levels of ICS listed below: Field level (zone of physical components), Control level (two zones: PLC zone and station zones), and Supervision level (zone of SCADA system and zone of computer stations). We decompose the ICS levels into zones since at the same level, each zone can have different attack surfaces with different levels of vulnerabilities. The output of this part is the catalog of cyberattack scenarios that can be experienced on any industrial site. This meta- model is depicted in Figure 2.

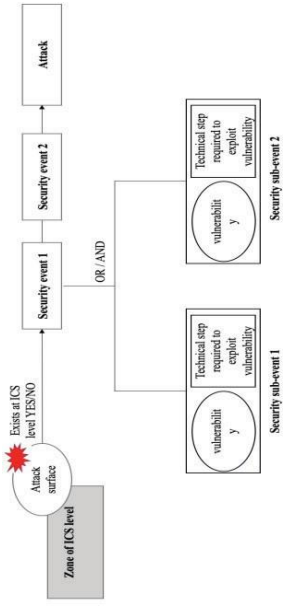

Fig. 2.The meta-model representing the sequence of an attack scenario

- One or more security events may occur during the execution of an attack. The security event can occur as a result of the occurrence of one or more security sub-events linked by the gates OR/AND, or it can occur as an initiating event of an attack or as a complimentary event.
- The security sub-event in this meta- model is a combination of the vulnerability and the technical step required to exploit the vulnerability.

The possible attacks scenarios for each attack surface and each ICS level zone are generated using this meta-model. In order to cover as many scenarios as possible, our research was built on the MITRE ATTACK framework (ATT&CK 2020). Figure 3 depicts an example of an attack scenario on the zone of physical components from the field level through the surface of physical access. Figure 4 depicts another attack scenario via the surface or receiving email on the station's zone of control level.

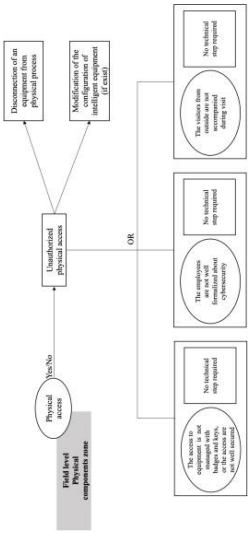

Fig. 3.The attack scenarios on the field level through a physical access

To execute the attack of disconnecting a physical component through physical access (figure 3), an attacker must first get an unauthorized physical access through one of the following security sub- events:

- The attacker can exploit a vulnerability that exists on the access to physical components locals, the access can be without badges or keys without any technical step required.
- The attacker can exploit the vulnerability during an unsupervised external visitor's visit, and he can gain unauthorized access without any technical steps.
- The internal staff who are not well formalised about cybersecurity and its risks can be a significant source of vulnerability for gaining unauthorized access without requiring any technical steps.

Figure 4 shows how the attacker can change the configuration or the functionality of a PLC by sending an email to the appropriate station. The attacker sends an email with malicious content without taking any technical steps in the first step, by exploiting these two possible vulnerabilities:

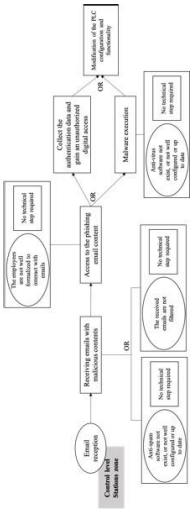

Fig. 4. The attack scenarios on the control level through the email reception

- There is no anti-spam software installed on the station that can prevent these types of emails from being received.
- The received emails to the configuration station are not filtered.

When a station receives a phishing email, an untrained employee in cybersecurity has access the content of the email (virus, malicious websites, etc.). After gaining access to the content, an attacker can steal the authentication data and use it to get an unauthorized digital access to the station, or the attacker can install a malware on the station and use a vulnerability in the anti-virus software implemented to prevent the malware from being executed. The algorithm of automatically generating the attack scenarios is provided in the following section.

3.3. Algorithm for the automatic generation of attack scenarios

When using the proposed approach to a case study, the major goal of the automatic generation of attack scenarios is to make the step of searching for the possible attack scenarios easier, especially for users who are not experts in the field of cybersecurity. This generation enables a simple application of the analysis process with a sufficient level of detail for the attack scenarios while limiting the complexity and time cost of the risk analysis. To carry out this step, some input data (from the KB) is required in order to run an algorithm and obtain the potential attack scenarios as outputs. There are two categories of inputs to consider:

- &The data of meta-models from the generated attack scenarios from the previous step, which is fixed data and identical across all cases studies. These data comprise the different zones of ICS levels, the generated list of vulnerabilities, the different attack surfaces, all the sequences and schemas of security events and sub-events, and all the relationships between them in order to carry out the attack.
- The second type of data is that which the user must enter in while using the risk analysis approach. The user must fill in the policies that are implemented at each zone of ICS level with their levels of applicability, as well as the attack surface that exists at each zone of ICS levels, depending on the case study.

These two types of input data are converted into data interchange format files, which are then used in a developed code to automatically generate the existing attack scenarios as output data in the same format

as the input data.

Until this phase of the approach, the undesirable events that can occur on an industrial site are listed with their accidental situations representing the safety risks from a traditional risk analysis approach, and the list of possible attacks that can occur is formed. In the rest of the approach, these two types of risks that lead to the same physical undesirable event are merged in a single Bow-Tie, called Cyber Bow-Tie, the likelihood of occurrence of the combined risks is evaluated, and lastly, the combined risks are treated by proposing new safety and cybersecurity measures in order to minimise the criticality of the unacceptable combined risk.

3.4. Example and results

This section includes an example to demonstrate the steps of the proposed risk analysis approach. The example shows a case study of a polymerization system. The field level of this system is composed of different sensors, valves for running a chemical reaction, and they are physically accessible. These components are controlled by a PLC at the control level that can be accessed remotely from outside the industry and is configured on a configuration station at the control level. This station is physically accessible, has remote access from outside, and is implemented by software such as an operating system and an anti-virus. The field and control levels are supervised by a SCADA system that containing a server with a database, and a supervision station. These components can be physically accessed. Furthermore, at the supervision level, many computer stations are connected to the internet, can be accessed remotely, and they receive emails from outside the industry and are implemented by a variety of software.

In this case study, a Bow-Tie is used to depicts the different scenarios of safety risks that can result in the occurrence of a critical undesirable event, such as the toxic release into the atmosphere. In addition to the safety risks, cybersecurity issues must be examined for this case study. The components are correctly modelled with their attributes into tables, and the generated list of vulnerabilities is validated for the existing ones. For the step of searching the possible attack scenarios, we define for each zone of ICS level the existing attack surfaces before executing the automatic generation.

- Physical components zone (field level): physical access.
- PLC zone (control level): physical access, remote access.
- Stations zone (control level): physical access, remote access, software.
- Supervision zone (supervision level): physical access.
- Computer stations zones (supervision level): physical access, remote access, internet connection, email reception, software.

The developed algorithm uses the data from the defined attack surfaces, as well as the data from the generated meta-models of attack scenarios, to define the possible attack scenarios on each zone. The configuration station, for example, is not connected to the internet, thus there are no attacks possibilities on this zone via the internet connection. The output is all the sequences of security events for each zone and each attack surface in this case study, as well as all of the attacks that can occur as a result of these sequences of security events, as well all of the combinations between the vulnerabilities and technical steps of the security sub-events for each security event at each zone and attack surface.

4. Conclusion and future work

The need of incorporating of safety and cybersecurity into risk analysis for critical industrial systems grew. These industries have been subject to new cybersecurity threats as a result of the integration of new technologies into their control systems, which can harm the safety of their systems. Therefore, in addition to the safety issues, industries should raise awareness about the risks associated with cybersecurity. Several authors proposed and developed approaches for including safety and cybersecurity into risk analysis. However, to identify and analyse the critical attack scenarios from the perspective of safety for people and the environment, a risk analysis strategy based on the best characteristics and analysis process picked from the existing approaches (Oueidat, Flaus, and Massé 2020) is needed.

In this article, our proposed model-based risk analysis approach is provided. It focuses on merging safety and cybersecurity risks analysis in a clear and straightforward manner, with as many attack

scenarios as possible. Its process for generating the list of vulnerabilities and the attack scenarios differs from that of other existing approaches. The attack scenarios are automatically generated based on the KB as inputs, which includes the meta-model of attacks scenarios as well as some data collected from the industrial installation. We discussed in this article the processing for generating the attack scenarios in meta-models, as well as how to generate them automatically. The remaining steps represent the integration of safety and cybersecurity risk into a single bow-Tie, the evaluation of the likelihood of the combined risks, as well as their evaluation. The objective of introducing a new risk analysis approach is to simplify the steps of the risk analysis process, thus we will enhance future research about the integration of the likelihood evaluation of each attack scenario in the same algorithm of attack scenarios generation.

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."

ATT&CK, MITRE. 2020. "Mitre Att&ck." *URL: Https://Attack. Mitre. Org*.

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).

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.

Macher, Georg, Harald Sporer, Reinhard Berlach, Eric Armengaud, and Christian Kreiner. 2015. "SAHARA: A Security-Aware Hazard and Risk Analysis Method." In *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*, 621–24. EDA Consortium.

Mohr, R. 2002. "Preliminary Hazard Analysis." *Jacobs Sverdrup. February*.

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.

Piètre-Cambacédès, Ludovic. 2010. "Des Relations Entre Sûreté et Sécurité." PhD Thesis, Télécom ParisTech.

Piètre-Cambacédès, Ludovic, and Marc Bouissou. 2010. "Modeling Safety and Security Interdependencies with BDMP (Boolean Logic Driven Markov Processes)." In *2010 IEEE International Conference on Systems, Man and Cybernetics*, 2852–61. IEEE.

Reichenbach, Frank, Jan Endresen, Mohammad MR Chowdhury, and Judith Rossebø. 2012. "A Pragmatic Approach on Combined Safety and Security Risk Analysis." In *2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops*, 239–44. 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.

Schmittner, Christoph, Zhendong Ma, and Paul Smith. 2014. "FMVEA for Safety and Security Analysis of Intelligent and Cooperative Vehicles." In *International Conference on Computer Safety, Reliability, and Security*, 282–88. Springer.

Souza, Nivio Paula de, Cecília de Azevedo Castro César, Juliana de Melo Bezerra, and Celso Massaki Hirata. 2020. "Extending STPA with STRIDE to Identify Cybersecurity Loss Scenarios." *Journal of Information Security and Applications* 55: 102620.

Steiner, Max, and Peter Liggesmeyer. 2014. "Qualitative and Quantitative Analysis of CFTs Taking Security Causes into Account." In *International Conference on Computer Safety, Reliability, and Security*, 109–20. Springer.

Temple, William G, Yue Wu, Binbin Chen, and bigniew Kalbarczyk. 2017. "Systems-

Theoretic Likelihood and Severity Analysis for Safety and Security Co-Engineering." In *International Conference on Reliability, Safety and Security of Railway Systems*, 51–67. Springer.

Wei, Jingxuan, Yutaka Matsubara, and Hiroaki Takada. 2016. "HAZOP-Based Security Analysis for Embedded Systems: Case Study of Open Source Immobilizer Protocol Stack." In *Recent Advances in Systems Safety and Security*, 79–96. Springer.

Young, William, and Nancy Leveson. 2013. "Systems Thinking for Safety and Security." In *Proceedings of the 29th Annual Computer Security Applications Conference*, 1–8. ACM.