FVMEARA : A NEW SYSTEMATIC APPROACH for SECURITY and SAFETY RISK Co-ASSESMENT BASED ON ICVSS METHODOLOGY

R Chemali, Blaise Conrard, M Bayart

13^{th} *International Conference on Modeling, Optimization and Simuation* - MOSIM*'20 - November 12-14, 2020*
Agadir - Morocco "New advances and challenges for sustainable and smart industries"

FVMEARA : A NEW SYSTEMATIC APPROACH for SECURITY and SAFETY RISK Co-ASSESMENT BASED ON ICVSS METHODOLOGY

R. CHEMALI, B. CONRARD, M. BAYART

CRIStAL (Centre de Recherche en Informatique, Signal et Automatique de Lille) University of Lille
Lille, France
riad.chemali@univ-lille.fr, Blaise.Conrard@polytech-lille.fr, Mireille.Bayart@univ-lille.fr

ABSTRACT : *The nowadays CPPS (Cyber Physical Production System) depends essentially on Operational Technologies (OTs) that have been acquired from a wide range of Information Technologies (ITs). In order to guarantee the CPPSs requirements, several of ITs have been adjusted or adapted. As a result, new issues appeared, in the design of this production system, such as the integration of safety, security and vulnerability risks. The greater part of CPPSs vulnerabilities have generally not been considered in the design phase. However, this dependence on ITs makes CPPSs increasingly vulnerable to cyber-attacks and security threats, which affect their global performance. The focus of this research is to address the cyber security challenges that these systems have to cope. It discusses the features of the CPPSs threat environment and align safety and security risk analysis. In fact, the first problem in security risk analyzes is determining the likelihood of the cyber-attacks. The use likelihood in security analysis is not practical and sometimes does not make sense. Therefore, this prevents the research community from using a panoply of methods that exist in the field of safety because they are based on the use of probabilities. In this paper it is introduced a new vulnerability scoring system for industrial systems, called ICVSS. The proposed approach based on the calculation of variety of metrics distributed into two groups of metrics inherited from the classical CVSS metrics. The ICVSS not only make possible to assess the vulnerability and to ease the communication between the safety and security teams, but also it is a good alternative to replace the likelihood in order to be able to use these safety methods. Next, a new approach to co-analysis and co-assessment of safety and security called FVMEARA (Failure and Vulnerability Modes, and Effect Analysis and Risk Assessment) is presented. Actually, FVMEARA is a use case that shows the effectiveness of our methodology in which we have been able to reuse the FMEA method, known as the most widely used in the field of safety, to carry out a co-analysis of hazards and threats and to assess their risks. Even more, the proposed solution complies with the standards IEC 60812 for safety and the standard IEC 62443 for security.*

KEYWORDS : *Cybersecurity, Risk assessment, Design, Risk management, CVSS, ICS, Cyber-Physical Production System, Vulnerability, ISA/IEC 62443, IEC 60812, FMEA.*

1 Introduction

Today, the emergence of the Industry 4.0 and the smart factories amplify the needs of communication systems and their cooperation with each other, but also with humans, to decentralize decision-making with a distribution of information in each of the entities making up the global system. In relation to smart factories, a cyber-physical production system (CPPS) can be created when multiple cyber-physical systems are connected and interact with one another Reinhart et al. (2013), Scholz-Reiter et al. (2013), Monostori et al. (2016). Moreover, there is a strong need to integrate numerous systems and to share data via a cloud into CPPSs. This integration has created many challenges for the safety and security research community. In fact, safety and security play a vital role as well as in the design phase than in the operational phase (Banerjee et al. (2011); Piètre-Cambacédès and Bouissou (2013)). The purpose of safety is to protect the System Under Consideration (SUC) from accidental faults in order to avoid hazards. However, the purpose of security is to protect the SUC from intentional faults, attacks, and malicious activities in order to avoid threats. Safety and security are very important when hazards or threats can cause loss of life or environmental loss. However, safety and security risk assessment must be aligned. A weak collaboration between safety and security activities could produce weakly or partially protected systems (Sabaliauskaite and Mathur (2015)) . In fact,

security countermeasures influence and sometimes even weaken safety. Similarly, safety countermeasures could impact the security (Piètre-Cambacédès and Bouissou (2010)). Aligning safety and security risk assessment enables to avoid a number of problems that affect the CPPS either in the design phase or in the operational phase. For many years, the research community addressed safety and security separately. The International Electrotechnical Commission (IEC) has proposed the standard IEC 60812 for instrumented systems safety and the standard ISA/IEC 62443 for ICS security (Sabaliauskaite and Mathur (2015)). International Society of Automation (ISA) has gone one step further and formed a working group called Work-Group 7 to align safety and security and to address the common issues.

In this paper it is introduced a new vulnerability scoring system for industrial systems, called ICVSS. The proposed approach based on the calculation of variety of metrics distributed into two groups of metrics inherited from the classical CVSS metrics. These metrics allow refining and adapt score results for CPPS. Thereafter, a new methodology to co-analysis and co-assessment which integrates safety and security lifecycle called FVMEARA (Failure and Vulnerability Modes, and Effect Analysis and Risk Assessment). This integration is achieved by using safety risk assessment method based on likelihood of faults and security risk assessment based on vulnerability scoring system in a unified methodology. The proposed solution must comply with the standards IEC 60812 for safety and the standard IEC 62443 for security.

This paper is organized as follows : Section 2 is a summary of the state of the art related to risk assessment methods in distributed digital systems and vulnerability scoring systems. Section 3 presents some preliminaries. Section 4 presents Hazards/Threats Impacts, vulnerability assessment, and risk analysis. Section 5 details the Industrial Control Vulnerability Scoring System (ICVSS). Sections 6 and 7 describe the proposed methodology, Failure and Vulnerability Modes, and Effect Analysis and Risk Assessment (FVMEARA). In last part, the conclusion and the future work are given.

2 Related works

Several articles were published that provide the main definitions of dependability in distributed digital systems such as safety and security, and their attributes such as faults, errors, failures, vulnerabilities and their causes have been well detailed in (Avizienis et al. (2004); Piètre-Cambacédès and Bouissou (2010)).

In (Nicol et al. (2004)), the authors present a classification of different approaches to combining safety and security. Several works were done to model the stochastic behavior to assess reliability of ICSs. Sallhammar et al. (2006) propose game theory to model to compute the probability of attacker behavior by state machine stochastic model while Chen et al. (2011) suggest the use of stochastic Petri nets to have more complete modeling to avoids the explosion of the state space. Game theory is also used to model human interactions and particularly the relationship between cyber attacks and operators (Backhaus et al. (2013)).

In recent years, some major IT security companies and organizations have provided rating systems to assess information system (IT) vulnerabilities. (A vulnerability is a weakness or bug in software or hardware application, systems, device or service that allows an attacker to potentially cause a loss of confidentiality, integrity and availability). Many companies such as IBM, Symantec, Microsoft and Secunia have created their own vulnerability rating systems called X Force, Symantec Security Response Threat Severity Assessment, Security Bulletin Severity Rating System respectively. The NVD (National Vulnerability Database) is a standards-based US government vulnerability management database (NIST (2019)). It provides basic CVSS (Common Vulnerability Scoring System) measures that give a quantitative and a score for each vulnerability. The first open vulnerability scoring system CVSS was realized, in 2005, by the U.S. government's National Infrastructure Assurance Council (NIAC) (*Complete CVSS v1 Guide* (2019)). Subsequently, several enhancements were released (Mell and Scarfone (2007); Scarfone and Mell (2009)). In addition, CVSS has been used in several studies to estimate the security parameters, such as MTTC (Mean Time To Compromise) (McQueen et al. (2006)).

In recent years, several researchers have attempted to adapt the CVSS to OT (Operation Technologies) systems (Qu and Chan (2016)). Next, the open Robot Vulnerability Scoring System (RVSS) is proposed for robotic systems (Vilches et al. (2018)). A few works focus on the relation between safety and security risk assessment, although safety/security risk co-analysis is very important to avoid any conflict of safety and security requirements (Piètre-Cambacédès et al. 2010). Chemali et al. (2019) introduce a first vulnerability scoring system for Industrial Control Systems called ICVSS (Industrial Control Vulnerability Scoring System). The methodology uses different approaches to score vulnerabilities, depending on characteristics of Industrial Control Systems to integrate the effects and the impacts of an attack on control loops in terms of loss of control,

Maximum Abbreviated Injury Scale	SIL reference [IEC61508]	Risk reduction factor (SIL)
S1	No injuries	10-100
S2	Light and moderate injuries	100-1000
S3	Severe and life-threatening ; injuries (survival probable).	1000-10000
S4	Life-threatening injuries (survival uncertain), fatal injuries	10000-100000

TABLE 1 – Safety integrity level metrics and corresponding proportions

loss of view, or denial of service that can impact safety and security

3 Preliminaries

The following sections provide some general information on the definition of risk, and the Security Integrity Levels (SIL) used in our methodology. These are methods from different computer disciplines, not only from the ICS field. However, they are then particularly adapted and interlinked to enable a good assessment security and safety risks.

3.1 Risk definition

Cybersecurity Risk is the potential that a given attacker will capture and exploit your critical information, which will have a negative impact on industrial facilities. Different organizations define risk in different ways. In general, risk in most engineering disciplines is defined as follows (e.g. [EN50126] (Wolf and Scheibel (2012))) :

$$Risk = Likelihood of an accident \times Impact \quad (1)$$

3.2 Safety Integrity Levels (SIL)

Safety Integrity Levels (SILs) are a discrete and systematic classification, varying from SIL 1 (for lowest reliability) to SIL 4 (for highest reliability). Depending on the standard applied, safety integrity (and thus SIL) is a concept applicable to safety-related electrical/electronic/programmable electronic (E/E/PE) systems (for IEC 61508 (61508 (2005))) or safety-related instrumented systems (SIS) (for IEC 61511 (61511 (2004)) [IEC, 2004]). In the table(1 the safety integrity level metrics and corresponding proportions(Wolf and Scheibel (2012).

4 Impacts, vulnerabilities assessment, and risk analysis

For CPPS security, the likelihood of an accident can be compared with the accessibility of the attacker to exploit a weakness in the system. In our case, attack potential describes the accumulated technical, and intellectual resources that are needed to successfully mount a certain attack. This approach is based on the significant hypothesis that the probability of an accident (which in our CPPS security scenario means a successful security attack) decreases with the increase in the required potential attack.

4.1 Impacts and Consequences Determination

We look at the direct impacts of the identified potential hazards/threats and faults/vulnerabilities and their consequences on the system as a whole and assess the resulting risks. In this work we present a new systematic approach to a quantified safety/security risk analysis based on risk matrix which takes the ICVSS rating system and impact (Collateral Potential Damage (CPD)) as inputs in order to better assess the risks of attacks on CPPS. The worst impact is when safety of staff is affected. In fact, staff safety is the first priority for all actors of the system. However, various events can endanger health and safety, not to mention the terrorist threats that must be taken into account when protecting production systems. The impacts identified may touch on one or more aspects. According to the area affected. We define three types of impact (Rekik et al. (2018)) : safety impact, financial impact and operational impact. For space limitations, we choose only to present the safety impact and the financial one. For each type, we define 3 levels of severity. For the assessment of the impact, we use the same in Rekik et al. (2018) but with some adaptations. The methodology Wolf and Scheibel (2012) assigns the consequences of each type of impact (Table 1), according to their level of severity. A decimal power scale was used to evaluate the severity according to the impacted area. The total impact is determined as :

$$Impact = Impact_{Safety} + Impact_{Financial} \quad (2)$$

We are using a qualitative scale (1,2 to assess the impact(Rekik et al. (2018); Wolf and Scheibel (2012)).

4.2 Identification of Security Objectives, Security Threats, and Attack Paths

Before we can evaluate any attack, we need to identify high-level security and safety objectives, sometimes

Severity level	Severity level	Risk reduction factor
S1	No or tolerable financial damage	1-10
S2	Undesirable financial damage and/or the incident may have an impact on the public image of the company	10-100
S3	Substantial financial damage, but yet not existence-threatening and/or the incident may have a serious impact on the public image of the company	100-1000
S4	Existence-threatening financial damage and/or the incident will incur people suing the company, severe impact to the public image of the company	1000-10000

TABLE 2 – Financial impact level

also referred to as security objectives or security goals. Security objectives include all relevant security assets (e.g., critical data, functionality, or resources) and security policies (e.g., "Only authorized personnel may change the operating parameters of this system component"), as well as potential use cases and issues that need to be addressed at a very high level.

4.3 Vulnerability assessment and likelihood determination

The calculation of probability of attacks is a big challenge, it is commonly carried out using the method for calculating the attack potential (AP) that is specified by the standardized method Common Criteria ISO (2017) which is also applied by the ETSI TVRA (2011-03) and in the risk analysis approach described in Wolf and Scheibel (2012); Rekik et al. (2018). In our approach, the likelihood of an attack is replaced by ICVSS (Chemali et al. (2019)) to calculate the accessibility of a potential attack to exploit any vulnerability.

Firstly, we assess the vulnerability by ICVSS. In fact, it can measure the effort necessary to mount a successful attack against the system under consideration. The factors taken into account in determining the score of ICVSS and their ranges and values are presented in the figure 1(Chemali et al. (2019)).

5 ICVSS Methodology

Despite the improvement which has been made compared to version 1, the conventional CVSS version 2 is not suited to assessing the vulnerability for the domain of industrial systems. Indeed, environmental metrics considered as optional metrics in CVSS, are essential in case of industrial system vulnerability. These metrics allow integrating the effects and the impacts of an attack on control loops in terms of loss of control, or loss of view, or denial of service that can impact safety and security. In the following section, we present an adaptation of CVSS for Industrial Control Systems called ICVSS (Industrial Control Vulnerability Scoring System) based on CVSS version 2. We propose to improve and refine each metric, keeping the same CVSS methodology (fig 1). The proposed scoring system based on the calculation of variety of metrics distributed into two groups of metrics inherited from the classical CVSS metrics. These metrics allow refining and adapt score results for CPPS. In the following we present these groups of metrics.

5.1 BASE metrics

5.1.1 Access Vector (AV)

This metric is divided into two sub-metrics :

(i) Physical Media (PM) :

This sub-metric measures the media that could be used to exploit the vulnerability. The possible values are : Physical device (0.2) when the intrusion can come through a USB key ; Wired (0.395) : this possible value is assigned when the attacker could exploit the vulnerability by a wired media. Lastly, Wireless (1.0) is assigned when the vulnerability can come through a wireless media.

(ii) Access Layer (AL) :

This sub-metric is designed to measure the layer where the vulnerability could be exploited. The possible values are : Network (1.0) when the attacker exploits a vulnerability that comes from the Internet ; Adjacent Network (0.646) when threat comes from Virtual Private Network (VPN) ; Local network (0.395) when threat comes from Local Area Network (LAN). The last possible value is the Physical (0.2), when the attacker needs physical contact with the ICS system components.

5.1.2 Access complexity (AC) :

This metric measures the complexity of the attack that exploits the vulnerability. The metric is divided into two sub-metrics :

(i) System complexity [SC] : Distributed system

(e.g., SCADA power distribution systems) is more vulnerable to attacks, because it is physically distributed over several sites. The coordination between the different sites is ensured by the communication networks (e.g., WAN (wide area networks) ; and NAN (Neighborhood Area Networks)(Zhang (2015)). Consequently, the attacker can use less sophisticated attacks to compromise the system compared to the system which is physically located on single and isolated site. The possible values are : Simple (0.35), when the facility located on a single isolated site ; Distributed (0.71), when the facility is distributed over several sites.
(ii) Attack complexity [ATC] : In this metric we keep the same definition of the CVSS which measures the complexity of the attack that required to exploit the vulnerability (Access Complexity (AC)). There are three possible values.
High (0.35) : This value is assigned when the attack requires a lot of time, several steps, knowledge, and skills to exploit the vulnerability. Usually these attacks are launched by terrorist and nation-state threats (group 1)(e.g., Stuxnet attack) ("ICS-CERT" 2019). Medium (0.61) : this value is assigned when the attacker needs for less knowledge and technical skills than group 1 to exploit the vulnerability. Usually, these attacks are launched by organized threats (group 2) where their motivation may be financial, or revenge, or theft of trade secrets, or to draw attention to a cause (hacktivists)(*ICS-CERT* (2019)).
Low (0.71) : this value is assigned when the attack requires less structured and sophisticated knowledge and technical skill than the group (2), which can be quite advanced. These attacks are launched by mainstream threats (group 3) where their motivations have been related to notoriety, fame, or attacking a system to attract attention to themselves(*ICS-CERT* (2019)).
Cryptography [C] : This sub-metric presents the encryption level of exchanged data (e.g., the communication protocol has an encryption system). The possible values are : Non (0.71), Encrypted (0.35).

5.1.3 Security Impact (C, I, A) :

The same definitions are used in the conventional CVSS version 2 to measure the Confidentiality (C), Integrity (I), and Availability (A) impacts.

5.1.4 Safety System (SS) :

This sub-metric measures the presence of safety systems in the facility that should protect the equipment and the people from harmful situations that may arise from operating. The possible values are : None (0.9), Safety System (0.01).

5.1.5 Authentication (Au) :

This metric describes the number of authentication required to perform the attack. The possible values are : Multiple (0.45), Single (0.56), and None (0.704).

5.2 Temporal metric :

5.2.1 Exploitability (E) :

this metric includes three sub-metrics :

(i) System Access [SA] : This sub-metric presents the degree of accessibility to useful information (about the hardware or about the software), when an attacker intends to launch cyberattack. The possible values are : Open Source (0.85), Proprietary (1.0).
(ii) Maturity [M] : We adopt the same definition of Exploitability (E) in CVSS version 2. The possible values are : High (1.0), Functional (0.95), Proof of concept (0.90), Unproven (0.85).

5.3 Remediation Level (RL) and Report Confidence (RC) :

The same definition is used in CVSS version 2 to measure Remediation Level (RL) and Report Confidence (RC)(for more details see Chemali et al. (2019)).

5.4 ICVSS Mathematical formula

With these metrics, the score (BS) and its sub-scores, exploitability (ES) and impact score (IS), can be calculated through the next formula (Chemali et al. (2019)] :

$$ES = 20 \times AV \times AC \times Au$$

$$IS = 10.41(1 - (1 - C)(1 - I)(1 - A))$$

$$F(IS) = \begin{cases} 0 & if \quad IS = 0 \\ 1.176 & if \quad IS \neq 0 \end{cases}$$

$$BS = RoundTo1Dec((0.6 \times IS + 0.4 \times ES - 1.5) \times f(IS))$$

$$TemporalScore = RoundToDecimal(BS \times E \times RL \times RC)$$

The score , defined between 0.0 and 10, expresses the overall severity of the vulnerability on the system (see the Table 3).

CVSS v 2.0	ICVSS
BASE Metric	
Exploitability Group	
Access Vector, AV	***Access Vector, AV***
Local (L); Adjacent Network (A); Network (N).	**SUB-METRICS GROUP**
	PHYSICAL MEDIA, PM
	USB key (USB); Wired (W); Wireless (WL);
	ACCESS LAYER , AL
	Physical (P); Local (L); Adjacent Network (A); Network (N).
Access Complexity, AC	***Access Complexity, AC***
Low (L); Medium (M); High (H).	**SUB-METRICS GROUP**
	SYSTEM COMPLEXITY, SC
	Simple (S); Distributed (D).
	ATTACK COMPLEXITY, ATC
	High (H); Medium (M); Low (L).
	CRYPTOGRAPHY, C
	Non (N); Encrypted (E).
Authentication, Au	***Authentication, Au***
Multiple (M), Single (S), None (N).	Multiple (M); Single (S); None (N).
Impact group	
Security Impact (C, I, A)	***Security Impact (C, I, A)***
None (N); Partial (P); Complete (C).	None (N); Partial (P); Complete (C).
	Safety System, SS
	None (N); Safety System (SS).
Temporal Metric	
Exploitability, E	***Exploitability, E***
Unproven (U); Proof-of-Concept (PoC); Functional (F); High (H); Not Defined (ND).	**SUB-METRIC GROUP**
	SYSTEM ACCESS, SA
	Open Source (OS); Proprietary (P).
	MATURITY, M
	Unproven; Proof-of-concept; Functional; Not Defined (ND).
Remediation level, RL	***Remediation level ,RL***
Official-fix (OF); Temporary-fix (TF); Workaround (W); Unavailable (U); Not Defined (ND);	Official-fix (OF); Temporary-fix (TF); Workaround (W); Unavailable (U); Not Defined (ND);
Report Confidence , RC	***Report Confidence , RC***
Unconfirmed (U); Uncorroborated (UC); Confirmed (C); Not Defined (ND).	Unconfirmed (U); Uncorroborated (UC); Confirmed (C); Not Defined (ND).

FIGURE 1 – Comparison of the indexes of the CVSS v 2.0 And ICVSS

Rating	CVSS Score
Very Low	0.0 - 1,9
Low	1.9 - 3.9
Medium	4.0 - 6.9
High	7.0 - 7,9
Very High	7.9 - 10

TABLE 3 – Qualitative severity rating scale

Likelihood	Risk Level			
Certain	Unacceptable	Unacceptable	Unacceptable	Unacceptable
Likely	Medium	Unacceptable	Unacceptable	Unacceptable
Possibly	Acceptable	Medium	Unacceptable	Unacceptable
Unlikely	Acceptable	Acceptable	Medium	Unacceptable
Remote	Acceptable	Acceptable	Acceptable	Medium
	Insignificant	Medium	Critical	Catastrophic
	Impact			

FIGURE 2 – Safety risk matrix

Scoring System	Risk Level			
Very hight	Unacceptable	Unacceptable	Unacceptable	Unacceptable
High	Meduim	Unacceptable	Unacceptable	Unacceptable
Meduim	Acceptable	Meduim	Unacceptable	Unacceptable
Low	Acceptable	Acceptable	Meduim	Unacceptable
Very low	Acceptable	Acceptable	Acceptable	Meduim
	Insignificant	Medium	Critical	Catastrophic
	Impact			

FIGURE 3 – Security risk matrix

5.5 Security and safety risk assessment

The risk matrices are used to determine the level of risk (Likelihood/Score x impact) and to decide whether or not it is acceptable. In industrial systems, a risk is considered as not acceptable when its value is high or critical, and acceptable if its value is low or negligible Rekik et al. (2018). In our case, we add the security risk matrix by replacing the likelihood by the ICVSS (2,3). The risk matrices will also be used to identify mitigation solutions. Actually, countermeasures will be applied in such way that to reduce the severity of the faults/vulnerabilities, but never the impact it could have on the system. Therefore, if a hazard/threat presents an unacceptable risk, we must push vertically through the matrix to the nearest acceptable cell (see figures 2,3). In a risk assessment, the impacts on the system have to be evaluated without any additional countermeasure in order to see the real consequences(Rekik et al. (2018)).

6 Annotated FVMEARA cause-effect chain

We are looking for a new method of safety/security co-analysis that starts with a system analysis similar to STPA-Sec (Security Theoretic Process Analysis (Young and Leveson (2013)), which identifies the functional control structure of a system, including

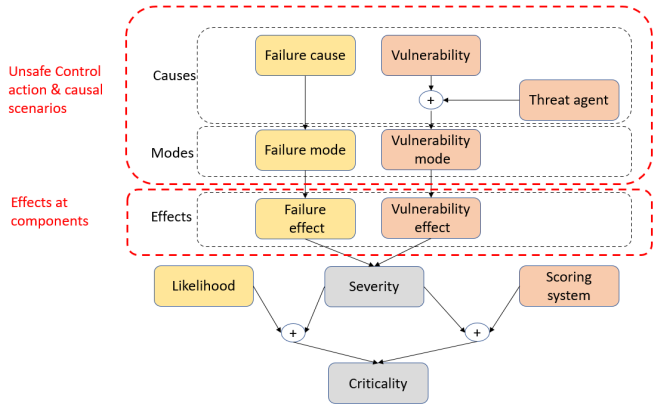

FIGURE 4 – Annotated FVMEARA cause-effect chain

the relationships between the system and the environment. This may include extensions or modifications to the original STPA-Sec to improve its coverage of safety topics, for example(Schmittner et al. (2016)). The resulting graphical model of the functional control structure will help stakeholders to identify potential risks to reliability, safety and security. Figure 4 shows the information flow in the FMVEA cause-effect chain (see Schmittner et al. (2014)).

7 Risk assessment methodology

We propose a safety and security integration methodology for the design of CPPS. This integration is achieved by merging safety and security methods (see Fig 5). In this section we present our unified methodology called FVMEARA (Failure and Vulnerability Modes, and Effect Analysis and Risk Assessment) that allows integrating safety and security risk assessment. Even more, the proposed solution must be compliant with safety and security standards for industrial systems. Consequently, we use the standard IEC 60812 for safety and the standard iSA/IEC 62443 for security.
In case of safety analysis, the basic approach to carry out an FMEA is described in IEC 60812. A system is divided into physical components, and failure modes for each component are identified. For each failure mode the effects, the severity of the final effect on the system and potential causes are examined. As far as possible, frequency or probability of the failure modes are estimated. However, in case of security analysis, the essential precondition for a successful security breach of a system is a vulnerability. In our methodology, a vulnerability is comparable to a failure cause and represents the basic prerequisite in security. For information security ISO/IEC 27005 divides vulnerabilities into categories : Network, Software, and Hardware vulnerabilities Schmittner et al. (2014). A vulnerability or threat mode is similar to the failure mode of safety and describes the manner in which the security fails. Threat mode is the effect by which the exploitation of vulnerability is observed. Next, for each mode, the detection procedures and the required corrective actions must be specified. The safety/security risk assessment methodology includes 23 phases. The first step identifies high-level safety/security objectives, sometimes also called safety/security objectives or goals. For example, the security objectives include all relevant security assets (e.g., critical data, functionality or resources) and security policies (e.g. "Only authorized personnel may change the operating parameters of ICS components"). Step 2 is the identification of the system that has need to be studied. It involves a functional specification and design phase, which looks at identifying the physical and IT equipment of the system. Step 3,4,12,13 and, 14 address the system threat landscape through hazards/threats and fault/vulnerability analysis. When potential hazards/threats or faults/vulnerabilities to the system are identified, then their direct impacts and consequences on the system must be assessed. Then, the likelihood/score of each identified hazard/threat should be determined in steps 5 and 14 respectively.

In the steps 6 and 7 for safety and steps 15 and 16 for security, the mode and effect are identified by identifying the effect by which the failure or the exploitation of vulnerability is observed. And for each mode, the detection procedures and the required corrective actions must be specified. Once failure/vulnerability mode and effect are identified, their direct impacts and cascading consequences on the whole system should be studied in steps 8 and 17. This procedure is taken from IEC 60812. The steps 9 and 18 are consisting of the calculation of the safety/security risk matrix using determined likelihood/score and impact levels. In steps 11 and 21, the countermeasures should be implemented to mitigate the intolerable risks. Next, the score or likelihood should be re-evaluated to measure the effectiveness of the proposed measures. If some risks are considered unacceptable, then a set of supplementary countermeasures must be proposed. In step 22, the alignment between safety and security is performed. Steps 3 until 22 should be repeated again until all risks become tolerable. Finally, the safety/security risk assessment process would have to conclude with a documentation phase.

8 Conclusion

In this paper we have proposed a methodology called FVMEARA for merging safety and security risk assessment CPPS at early development phases or in operation phases. We outline the vision for a hybrid method that combines elements of the

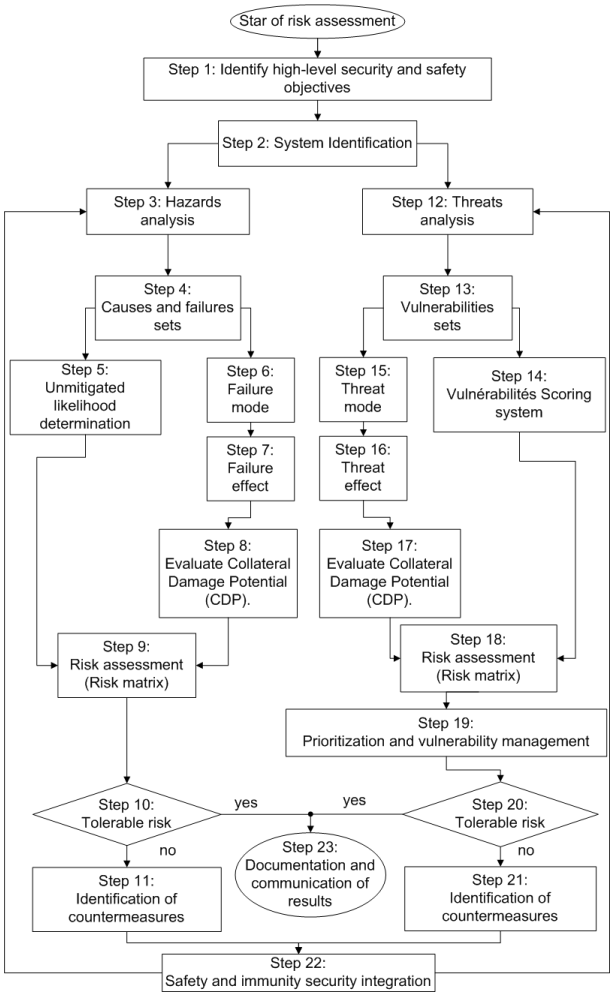

FIGURE 5 – Risk assessment methodology based on ISA/IEC-62443 and IEC60812

popular approaches from the systems and component side FMVEA and IEC/IEC 62443. Using this methodology engineers can align safety and security activities, by following the aligning 23 steps of safety and security life cycle methodology. The advantage of our methodology :

- we have used a very rich scoring system (ICVSS) that can assess vulnerabilities in a more accurate way.
- ICVSS is a language that facilitates communication between safety and cyber security engineers (because CVSS is the most used language in the security community).
- We have found a link between safety methods and security methods, this will allow us to use a lot of safety methods or methodologies, by replacing the likelihood by a score system to evaluate security.

In the future work, we will further develop the impact aspect by including other environmental metrics such as Target Distribution (TD). After we will apply our approach to a production system then to other industrial use cases such as railway systems. Some good practices and related techniques for the development of safer, more secure future industrial systems will be discussed.

Références

(2011-03), E. T. . .-. V. (2011). Part 1 : Method and proforma for threat, risk, vulnerability analysis, *Standard* .

61508, I. (2005). Functional safety of electrical/electronic/programmable electronic safety-related systems, *International Electrotechnical Commission* .

61511, I. (2004). Functional safety of electrical/electronic/programmable electronic safety-related systems, *International Electrotechnical Commission* .

Avizienis, A., Laprie, J.-C., Randell, B. and Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing, *IEEE transactions on dependable and secure computing* **1**(1) : 11–33.

Backhaus, S., Bent, R., Bono, J., Lee, R., Tracey, B., Wolpert, D., Xie, D. and Yildiz, Y. (2013). Cyber-physical security : A game theory model of humans interacting over control systems, **4**(4) : 2320–2327.
URL: *http ://ieeexplore.ieee.org/document/6665110/*

Banerjee, A., Venkatasubramanian, K. K., Mukherjee, T. and Gupta, S. K. S. (2011). Ensuring safety, security, and sustainability of mission-critical cyber–physical systems, *Proceedings of the IEEE* **100**(1) : 283–299.

Chemali, R., Conrard, B. and Bayart, M. (2019). ICVSS : A new methodology for scoring industrial control systems vulnerabilities, *Proceedings of the 29th European Safety and Reliability Conference*, European Safety and Reliability Association. OCLC : 8339510257.

Chen, T. M., Sanchez-Aarnoutse, J. C. and Buford, J. (2011). Petri net modeling of cyber-physical attacks on smart grid, **2**(4) : 741–749.
URL: *http ://ieeexplore.ieee.org/document/5967924/*

Complete CVSS v1 Guide (2019).
URL: *https ://www.first.org/cvss/v1/guide*

ICS-CERT (2019).
URL: *https ://ics-cert.us-cert.gov/*

ISO (2017). Common critera, common methodology for information technology security evaluation : Evaluation methodology, *Standard* .

McQueen, M., Boyer, W., Flynn, M. and Beitel, G. (2006). Quantitative cyber risk reduction estimation methodology for a small SCADA control system, *Proceedings of the 39th Annual*

Hawaii International Conference on System Sciences (HICSS'06), IEEE, pp. 226–226.
URL: *http ://ieeexplore.ieee.org/document/1579754/*

Mell, P. and Scarfone, K. (2007). Improving the common vulnerability scoring system, *IET Information Security* **1**(3) : 119–127.

Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Sihn, W. and Ueda, K. (2016). Cyber-physical systems in manufacturing, *Cirp Annals* **65**(2) : 621–641.

Nicol, D. M., Sanders, W. H. and Trivedi, K. S. (2004). Model-based evaluation : from dependability to security, *IEEE Transactions on dependable and secure computing* **1**(1) : 48–65.

NIST (2019). Nvd vulnerability metrics.
URL: *https ://nvd.nist.gov/vuln-metrics/cvss*

Pièrre-Cambacédès, L. and Bouissou, M. (2010). Modeling safety and security interdependencies with bdmp (boolean logic driven markov processes), *2010 IEEE International Conference on Systems, Man and Cybernetics*, IEEE, pp. 2852–2861.

Pièrre-Cambacédès, L. and Bouissou, M. (2013). Cross-fertilization between safety and security engineering, *Reliability Engineering & System Safety* **110** : 110–126.

Qu, Y. and Chan, P. (2016). Assessing vulnerabilities in bluetooth low energy (BLE) wireless network based IoT systems, IEEE, pp. 42–48.
URL: *http ://ieeexplore.ieee.org/document/7502262/*

Reinhart, G., Engelhardt, P., Geiger, F., Philipp, T., Wahlster, W., Zühlke, D., Schlick, J., Becker, T., Löckelt, M., Pirvu, B. et al. (2013). Cyber-physische produktionssysteme. produktivitäts-und flexibilitätssteigerung durch die vernetzung intelligenter systeme in der fabrik, *wt-online, Jg* **103**(2) : 84–89.

Rekik, M., Gransart, C. and Berbineau, M. (2018). Cyber-physical security risk assessment for train control and monitoring systems, *2018 IEEE Conference on Communications and Network Security (CNS)*, IEEE, pp. 1–9.

Sabaliauskaite, G. and Mathur, A. P. (2015). Aligning cyber-physical system safety and security, *Complex Systems Design & Management Asia*, Springer, pp. 41–53.

Sallhammar, K., Helvik, B. E. and Knapskog, S. J. (2006). On stochastic modeling for integrated security and dependability evaluation., *J. Networks* **1**(5) : 31–42.

Scarfone, K. and Mell, P. (2009). An analysis of CVSS version 2 vulnerability scoring, *2009 3rd International Symposium on Empirical Software Engineering and Measurement*, IEEE, pp. 516–525.
URL: *http ://ieeexplore.ieee.org/document/5314220/*

Schmittner, C., Gruber, T., Puschner, P. and Schoitsch, E. (2014). Security application of failure mode and effect analysis (fmea), *International Conference on Computer Safety, Reliability, and Security*, Springer, pp. 310–325.

Schmittner, C., Ma, Z. and Puschner, P. (2016). Limitation and improvement of stpa-sec for safety and security co-analysis, *International Conference on Computer Safety, Reliability, and Security*, Springer, pp. 195–209.

Scholz-Reiter, B., Veigt, M. and Lappe, D. (2013). Entwicklung eines cyber-physischen logistiksystems, *Industrie Management 1/2013-Vierte industrielle Revolution* p. 15.

Vilches, V. M., Gil-Uriarte, E., Ugarte, I. Z., Mendia, G. O., Pisón, R. I., Kirschgens, L. A., Calvo, A. B., Cordero, A. H., Apa, L. and Cerrudo, C. (2018). Towards an open standard for assessing the severity of robot security vulnerabilities, the robot vulnerability scoring system (RVSS).
URL: *http ://arxiv.org/abs/1807.10357*

Wolf, M. and Scheibel, M. (2012). A systematic approach to a qualified security risk analysis for vehicular it systems, *Automotive-Safety & Security 2012* .

Young, W. and Leveson, N. (2013). Systems thinking for safety and security, *Proceedings of the 29th Annual Computer Security Applications Conference*, pp. 1–8.

Zhang, Y. (2015). *Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment*, PhD thesis, University of Toledo.