Quantitative Security Metrics: Assessment of Cyberattack Scenarios for Cyber-Physical Systems

Mike Da Silva, Nga Nguyen

Quantitative Security Metrics: Assessment of Cyberattack Scenarios for Cyber-Physical Systems

1st Mike Da Silva
De Vinci Higher Education
De Vinci Research Center
Paris, France
mike.da_silva@devinci.fr

2nd Nga Nguyen
De Vinci Higher Education
De Vinci Research Center
Paris, France
nga.nguyen@devinci.fr

***Abstract*—Cyber-Physical Systems (CPS) are digitized infrastructures controlling physical processes. To improve their dependability, we propose in this paper CYBERSIM, a framework to jointly automate safety and cybersecurity risk assessments for CPS in a common tool by means of generating cyberattack scenarios compromising system safety. However, due to the state space size of these complex systems, the sequence generation is subject to combinatorial explosion leading to an unmanageable number of attack scenarios. We develop in CYBERSIM a flexible and multi-metrics cost function which enables us to filter out quantitatively sequences of lesser importance and concentrate analysts efforts on the system's most critical weaknesses. This cost model using CVSS scores computed for MITRE EMB3D threats has been applied to an automotive case study in order to prove its applicability and effectiveness in an industrial context.**

***Index Terms*—Quantitative Analysis, Security Metrics, Safety, Risk Assessment, Cyber-Physical System**

I. Introduction

Cyber-Physical Systems (CPS) are safety-critical infrastructures used in various fields such as industry, automotive, aeronautics, etc. which are increasingly computerized and thus exposed to cyberattacks. To improve the dependability of these complex systems, we developed in partnership with Airbus Protect CYBERSIM, a framework that aims to jointly automate the safety and cybersecurity risk assessment of CPS in a common tool called SimfiaNeo [1]. The last one uses the mathematical formalism of Discrete Event Systems (DES) for its capacity to model complex system behaviors. This formalism models the system in the form of a state transition system from which we can generate sequences of events leading to a critical state. These critical sequences can be used to identify weaknesses in the system under study, and to suggest ways of improving its architecture. The challenge of CYBERSIM is to adapt the DES formal framework initially dedicated to safety, which deals with random and unintentional events, to security, with intentional attacker actions.

A preliminary study [2] of the similarities and differences between critical sequences in the cybersecurity (cyberattacks) and safety (failures) domains revealed two major differences that require adaptation to apply the DES formalism to cybersecurity domain.

Firstly, the critical sequences representing cyberattacks tend to be longer than those representing failures, which compounds the state space explosion problem, characteristic of CPS models. To avoid an exhaustive state space exploration, safety approaches define cutoff criteria, similar to threshold, under which the probability of occurrence is considered acceptable. Due to the lack of reliable historical data in cybersecurity, no relevant probabilistic distributions representative of reality can be computed to match with a cutoff criterion.

Secondly, safety-critical sequences are combinations of independent failures whose order is unimportant, unlike cyberattacks, which are sequences of intentional actions aimed at achieving a defined objective. A first contribution was to take advantage of the dependencies between an attacker's actions to compute a cutoff criterion in the form of "Footprint" [2] that limits the exploration of the state space. This preliminary work allows us to generate a set of candidate cyberattack scenarios for which we want to quantify the risk they pose to system safety, so that risk analysts can prioritize and filter them appropriately.

Contributions: We present in this paper CYBERSIM, a theoretical framework based on a *Multi-Metrics Cost Function* that proposes a flexible quantitative assessment of cyberattack scenarios which can be adapted to available data. We apply this framework to build a cost function for MITRE EMB3D [3], a threat modeling framework dedicated to embedded systems, based on reliable data such as Common Vulnerability and Exposures (CVE) [4] and Common Vulnerability Scoring System (CVSS) [5] scores provided by the National Institute of Standards and Technology (NIST). Finally, we show the effectiveness of the EMB3D *Multi-Metrics Cost Function* in the industrial context by assessing attack scenarios identified by SimfiaNeo for an automotive case study based on the EVITA project [6].

The paper is organized as follows. We introduce in Section II some related work on quantitative model-based security analysis. Then, we detail the CYBERSIM *Multi-Metrics Cost Function* and its application to the MITRE EMB3D framework in Section III. Then we apply the EMB3D cost function to an automotive case study in Section IV. Finally, Section V gives some conclusions and directions for our future work.

II. Related Work

The generation of relevant attack sequences has been studied in various research works through for example the simulation of complex scenarios with cyber range platforms, the data model such as MITRE Attack Flow [7] to describe sequences of adversary behaviors, the use of reinforcement learning to dynamically evaluate the relevance of attack paths, etc. These approaches differ in a number of aspects such as the abstraction level, the mathematical foundation, the automatic or manual generation, and the qualitative or quantitative analysis.

This work is part of the field of quantitative model-based security analysis in which we retrieve two principal model types: attack graphs and stochastic models [8]. Attack graphs are models used to represent the set of possible paths an attacker can take to achieve a feared event [9], [10]. To build the attack graph, vulnerabilities are modeled according to *preconditions* and *postconditions*, respectively the requirements to exploit a vulnerability and the consequences of the exploitation (e.g. attacker privilege escalation or device denial of service). Once modeled, vulnerabilities are associated together to represent their relationships, based on theirs *preconditions* and *postconditions*, in a form of a graph, hence the name of attack graph.

Related work defines four main security metric types based on attack graphs. Path metrics define security metrics according to characteristics of paths such as the path length [11] or the number of paths [12], [13]. The second type of metrics belongs to the Non-Path metrics which measures more general information like the *Weakest Adversary* metric [14] which defines the security strength of a network as the strength of the initial conditions of the attack graph required to compromise it. Finally, Probabilistic metrics and Bayesian Network-Based metrics use respectively probabilities and Bayesian network formalism for their computation [15], [16]. The main limit of attack graphs is that they are not scalable for a real system and can not be used in the industrial context.

Stochastic models rely on finite state machines to represent the system behavior. The transition from one state to another is triggered by an event labeled with random variables whose distribution function permits to represent uncertainty in the occurrence of the event. Stochastic models use time-based or probability-based metric analyses, such as Monte-Carlo methods, to calculate statistical data like the mean time [17] or the probability (likelihood) [18] of a system to be compromised by an attacker. In CYBERSIM, we use another classical safety analysis method, called the minimal cutset [19], which defines a set of minimal sequences (minimal means, when any basic event is removed from the sequence, the remaining events collectively are no longer a sequence), in line with a cutoff criterion that fixes a threshold beyond which sequences are not considered as significant.

Regardless the model type used, stochastic or attack graph, security metrics are frequently based on unreliable data and data sources [17], [20], [21], [22], such as vulnerability exploitation probability provided by expert opinion, to determine input's values of the assessing function. Some other researches use ad-hoc methods that lack of a mathematically sound framework, to convert reliable data, such as those provided by the CVSS scores, into probabilities [9], [16], [23], [24], [25]. CYBERSIM proposes to aggregate scores from CVSS, a published standard and open framework, for MITRE EMB3D threats. These CVSS metrics are considered by [26] as sound security metrics with well-defined, progressive and reproducible properties.

III. CYBERSIM Quantitative Assessment of Cyberattack Scenarios

A. Quantitative Security Metrics Framework

We extract from [2] and extend here two important definitions about Discrete Event System (DES) and Critical Sequence.

Definition 1 (DES): A *discrete event system* is a five-tuple $\langle V, E, T, s_0, C\rangle$ where:

- V is a finite set of variables. The state s_i of the system is thus described by *valuations* of variables of V.
- E is a finite set of events e_i. These events represent threats that an attacker can use to attack the system.
- T is a finite set of transitions $\langle e, g, i\rangle$ where:
  - e is an event from E;
  - g is a Boolean condition on variables of V, called the *guard* of the transition;
  - i is an *instruction* that modifies the current values of variables, passing the system from a state s satisfying the guard g to the new state $s' = i(s)$ through the event e. We denote $s \xrightarrow{e} s'$.
- s_0 is the *initial state* of the system;
- C is a Boolean expression on the values of the variables of V representing the critical states.

Definition 2 (Critical Sequence): Let $M = \langle V, E, T, s_0, C\rangle$ be a DES and let $s_0 \xrightarrow{e_1} s_1 \cdots \xrightarrow{e_n} s_n$ be an execution of M. The sequence $e_1 \cdots e_n$ is a critical sequence if:

- s_n satisfies C;
- none of the s_i, $0 \leq i < n$ satisfies C.

In order to limit the number of generated critical sequences, we associate a cost to each event and compute the cost of a sequence as the aggregation of the costs of its events. The condition that a cost $Cost$ must verify is that:

- It associates events with values taken in a domain D equipped with an order relation $\sqsubseteq$, an aggregation function $\oplus$, and an identity element id;
- It is monotonically increasing, i.e. for all valid sequences we, where w is a, possibly empty ($\emptyset$), sequence and e is an event, the following condition holds:

$$Cost\,(w) \sqsubseteq Cost\,(we) = Cost\,(w) \oplus Cost\,(e)$$

$$Cost(\emptyset) = id$$

Costs can be defined over the domain $\langle \mathbb{R}^+, \leq, +, 0\rangle$ to associate a positive weight to each event and to set the weight of a sequence as the sum of the weight of its events. If the weight is set to 1 for all events, the weight of a sequence

is simply its length. The domain can also be $\langle [0,1], \geq, *, 1\rangle$ to associate a probability to each event and to define the probability of a sequence as the product of the probabilities of its events. Then a threshold on the cost of sequences could be used by the sequence generation algorithm implemented in SimfiaNeo to avoid state explosion.

Costs in cybersecurity can be combined of different criteria such as the complexity of an attack, the needed expertise of the attacker, etc. We then can define a generic and flexible multi-metrics cost function that can be adapted in different risk analysis context.

Definition 3 (Multi-Metrics Cost Function): Let $\langle D_i, \sqsubseteq_i, \oplus_i, id_i\rangle, 1 \leq i \leq n$ be a domain with an order relation $\sqsubseteq_i$, an aggregation function $\oplus_i$, and an identity element id_i. The combined cost domain $\langle D, \sqsubseteq, \oplus, id\rangle$ is defined as:

- D is the Cartesian product $D_1 \times D_2 \times \cdots D_n$, with identity element $id = (id_1, id_2, \cdots id_n)$ and elements such as $(c_{11}, c_{12}, \cdots c_{1n})$ and $(c_{21}, c_{22}, \cdots c_{2n})$;
- $(c_{11}, c_{12}, \cdots c_{1n}) \sqsubseteq (c_{21}, c_{22}, \cdots c_{2n})$ if and only if $c_{1i} \sqsubseteq_i c_{2i}, \forall 1 \leq i \leq n$.
- $(c_{11}, c_{12}, \cdots c_{1n}) \oplus (c_{21}, c_{22}, \cdots c_{2n}) = (c_{11} \oplus_1 c_{21}, c_{12} \oplus_2 c_{22}, \cdots, c_{1n} \oplus_n c_{2n})$.

We will apply this generic multi-metrics cost function to the MITRE EMB3D threat model in the next subsection to illustrate the flexibility of our framework.

B. A MITRE EMB3D Multi-Metrics Cost Function

To limit the state space of the system model, we use threats, an abstraction of vulnerabilities, as events (cyberattack steps) in SimfiaNeo in order to build the cyberattack scenarios as sequences of threats. For that purpose, we used a recent threat modeling framework called MITRE EMB3D, which provides a single repository of information for known threats to embedded device features/properties. EMB3D also provides information on weaknesses (Common Weakness Enumeration, CWE [27]) best associated with each threat, as well as examples of publicly disclosed vulnerabilities (Common Vulnerabilities and Exposures, CVE) exploited in embedded devices.

The application of the multi-metrics cost function to the MITRE EMB3D threats is composed of three following tasks.

1) Define Metrics of the Multi-Metrics Cost Function: The CVSS proposes a well-known and widely used vulnerability severity score called the base score. To apply the *Multi-Metrics Cost Function* to EMB3D, we rely on the security metrics used for calculating the CVSS base score. These metrics are split in two sets, those related to calculation of the vulnerability exploitability and those related to assessing the impacts of the vulnerability. In the context of this work, we are interested in impacts on the safety of the system whereas CVSS impact metrics assess cybersecurity consequences. Therefore, we choose to use only metrics belonging to the exploitability set which is define as follow:

- ***Exploitability Metrics:*** This set of metrics aims to reflect the ease and technical means by which a vulnerability can be exploited through 4 metrics:
  - ***Attack Vector (AV):*** measures how remote the attacker is.
  - ***Attack Complexity (AC):*** measures if an attacker can expect repeatable success in exploiting a vulnerability.
  - ***Privileges Required (PR):*** measures the level of privileges required before exploiting a vulnerability.
  - ***User Interaction (UI):*** measures the dependency of an attacker to another user to exploit a vulnerability.
- ***Scope:*** Scope is a specific metric belonging to both sets (exploitability and impact metrics sets) that captures if a vulnerability impacts components beyond its security scope. The base score and the *Privileges Required* metric are dependent of the Scope value. For sake of simplicity, we will not use *Scope* in calculation.

2) Define Metrics Value for EMB3D Threats: Each CVSS metric includes several metric values which are associated to a numerical value to be used in the scoring formula. For example, the *User Interaction* metric has two metric values, *None* and *Required*, which are respectively associated to the numerical values 0.85 and 0.62. Therefore, if an analyst evaluates the *User Interaction* as *Required*, the metric *User Interaction* will have a value of 0.62 in the scoring formula. Descriptions of the metric values and their corresponding numerical value are detailed in the CVSS V3.1 specification document [5].

Due to the level of abstraction of the threats, it is not trivial to assign a value to the metrics directly. We therefore propose to build up a set of CVEs representative of the threat, from which we calculate the average value of the set of CVEs for each of the metrics as the EMB3D threat metric value.

To this end, we use the National Vulnerability Database (NVD) [28], a reliable CVE database that systematically provides a detailed CVSS base score and a corresponding CWE for each CVE record. Since each threat in MITRE EMB3D may be associated with different CVEs and CWEs, and the last ones are mapped as a root cause of vulnerability to different CVEs found in NVD, we can collect a set of CVEs related to a threat. This set will be the union of direct CVEs and mapped CVEs as shown in Figure 1.

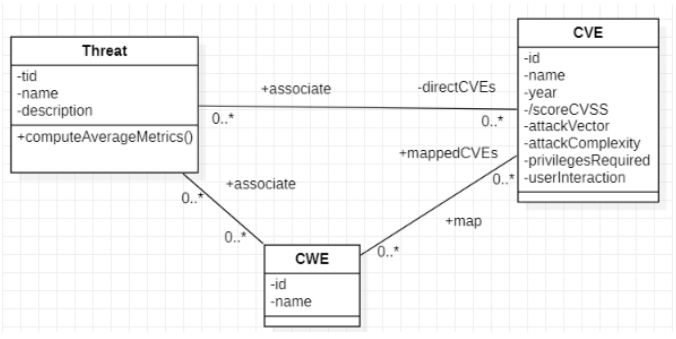

Fig. 1. The MITRE EMB3D™ Threat Model UML Class Diagram

Then, for each threat, we compute its exploitability metrics as an average value of those of its CVEs:

$$\frac{\sum_i number\_of\_CVEs\_in\_category_i * value_i}{total\_number\_of\_CVEs}$$

For example, for Attack Vector metric, the 4 categories are $\{Network, Adjacent, Local, Physical\}$ and the numerical values are respectively $\{0.85, 0.62, 0.55, 0.2\}$.

3) Apply the Multi-Metrics Cost Function: Applying the *the Multi-Metrics Cost Function* to EMB3D requires to define an aggregation function for each metrics. From our semantical interpretation of the metrics description in the context of an attack scenario (multi-step attack) and the assumption that, all other things being equal, the more steps an attack scenario comprises, the less critical it is. According to this hypothesis, metrics value should be monotonically decreasing according to the attack length (i.e. the number of steps). We therefore chose the multiplication ($*$) as aggregation function for all metrics, as the CVSS metrics values are all between 0 and 1. Furthermore, values 0 and 1 can be used respectively to provide an attacker ceil (value 0), i.e the attack step is not achievable by the attacker, or an architecture vulnerability (value 1) which does not require exploitation. These interpretations and assumptions are open to discussion as they depend on the risk analyst's point of view. Therefore, the combined cost domain for the MITRE EMB3D threat model is $AV \times AC \times PR \times UI$ and the domains are $\langle [0,1], \geq, *, 1 \rangle$. Then, we combine the cost function of threats belonging to the same attack scenario generated by SimfiaNeo by applying the aggregation function:

$$seq(av, ac, pr, ui) = (av_1 * av_2 * \cdots av_n, ac_1 * ac_2 * \cdots ac_n, pr_1 * pr_2 * \cdots pr_n, ui_1 * ui_2 * \cdots ui_n)$$

Once the combined cost function is established for the four exploitabiblity security metrics, we can compute the cost of a sequence by using a norm function in a 4-dimension vector space such as the Euclidean norm:

$$cost(seq(av, ac, pr, ui)) = \sqrt{av^2 + ac^2 + pr^2 + ui^2}$$

As with the choice of the aggregation function, another norm can be used in another modeling context. The weight of each security metric is equal here since it has already been taken into account by the numerical values proposed by CVSS.

Finally, we compare attack scenarios by considering their safety impacts severity. In SimfiaNeo, attack scenarios are generated according to an observer, i.e. a safety feared event. Therefore, attack scenarios generated for a same observer can be directly compared without safety impacts score because they share the same safety impacts. Otherwise, a safety expert assigns a severity impact score to each observer, which is integrated in form of attack scenarios weighting, to compare scenarios with different safety impacts. Although the formula to calculate this safety impact severity score is beyond the scope of this work, Process Hazard Analysis (PHA) can provide this kind of information.

IV. Application to an Automotive Case Study: EVITA

We extended a previous work [29] on a case study taken from the EVITA project in order to assess attack scenarios generated by SimfiaNeo with the EMB3D cost function introduced in Section III-B.

A. EVITA

EVITA, for E-safety Vehicle InTrusion protected Applications, is an European project that designed, verified, and prototyped a secure architecture for automotive on-board networks. The project proposes a set of 18 use cases from which they build dark-side scenarios, which we will call feared events in this paper, in order to identify requirements for the system. Figure 2 shows the graphical model of the EVITA case study, representing a classical on-board network architecture, in SimfiaNeo.

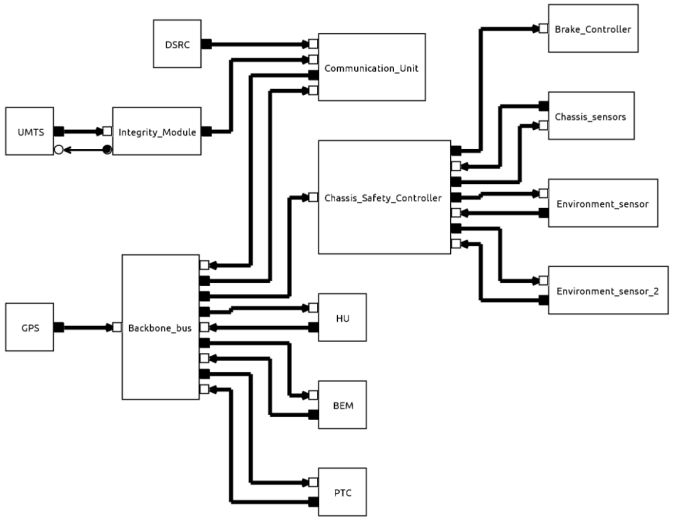

Fig. 2. EVITA Automotive Graphical Model on SimfiaNeo [29]

B. Generating and Assessing Attack Scenarios of the Case Study

Serru et al. [29] implemented two of EVITA project's feared events in SimfiaNeo which we propose to extend with a quantitative security assessment. The first feared event, called *Unauthorized brake*, aims to identify sequences leading to an unwanted activation of the brake function. The second one, *Attack active brake function*, determines sequences preventing the expected automated brake operation by delaying, inhibiting, or degrading the quality of a legitimate brake.

Sequence computation for these two feared events in SimfiaNeo generate respectively 14 *Unauthorized brake* and 26 *Attack active brake function* sequences for a Footprint equal to 1, i.e. each attack step is necessarily conditioned by the previous one. The same sequence computation without the Footprint criterion generate respectively 45 *Unauthorized brake* and 116 *Attack active brake function* sequences. An example of a sequence, as displayed by the graphical user interface of

SimfiaNeo, is shown in Figure 3. The sequence presents an attack scenario belonging to the *Unauthorized braking* where: an attacker (1) send an unauthorized replay message to *MyCar* impersonating another car; then (2) the *MyCar*'s communication module processes the replay message as a legitimate one and forwards it to the chassis safety controller; which finally (3) triggers an activation brake function event leading to the feared event (4) an unwanted activation of the brake function. For sake of simplicity, we will refer to this sequence as the "impersonate" attack scenario or sequence in the rest of this section.

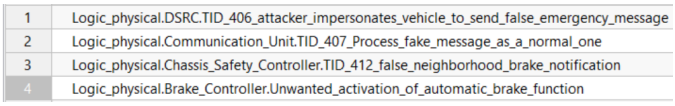

Fig. 3. Example of a SimfiaNeo Sequence for EVITA Case Study

SimfiaNeo allows to display internal system state in the sequences which are not attack steps, such as the feared events or corrupted data processing, to facilitate the remediation process. We increase readability of attack scenarios by identifying attack steps with the prefix *TID_XXX* where *XXX* is the ID of the corresponding EMB3D threat. Table I shows the 5 most costly sequences, according to the EMB3D cost function, for both feared events. A first observation of the sequences included in the top 5 shows that the attack scenarios' length seems to strongly impact the final score, in line with the design choice made when choosing the aggregation function.

TABLE I
TOP 5 SEQUENCES FOR EVITA CASE STUDY

Unauthorized brake

Rank	Sequence	Score
1	406, 407, 412	0.98
2	224, 205, 412, 412, 211, 406	0.45
3	224, 205, 412, 302, 406, 412	0.43
4	224, 205, 412, 412, 301, 406, 412	0.36
5	224, 205, 412, 302, 406, 202, 406	0.33

Attack active brake function

1	404	1.50
2	224, 405, 412, 405	0.63
3	224, 405, 412, 204	0.61
4	224, 205, 412, 302, 404	0.45
5	224, 205, 412, 302, 204	0.44

C. A Detailed Application of the EMB3D Cost Function

Continuing the example presented in Figure 3, we detail the calculation steps of the impersonate attack scenario which happens to be the best-scored scenario of the *Unauthorized brake*. In Table I, the impersonate scenario is defined as sequence (406, 407, 412) meaning that the scenario includes three steps, each of which refers to an EMB3D threat ID number: 406 refers to the threat *TID-406: Unauthorized Messages or Connections*[1], 407 refers to the threat *TID-407: Missing Message Replay Protection*[2] and 412 to the threat *TID-412: Network Routing Capability Abuse*[3]. To determine the cost of this sequence, we start by collecting CVEs related to the threats belonging to the sequence.

1) CVE collection: The impersonate sequence comprises three different threats, TID-406, TID-407 and TID-412. The TID-406 has 4 CVEs and 2 CWEs directly linked. We build the CVEs set by calculating the union of the CVEs directly linked to the threat (colone CVE in Table II) with the CVEs related to the CWE linked to the threat (colone CWE in Table II). CWE-related CVEs have been collected thanks to the NVD CVE/CWE mapping which respectively represent 1399 CVEs for CWE-306 and 3646 CVEs for CWE-287. This union provides a global pool of 4996 CVEs for TID-406. Then, TID-407 has 2 CVEs and 1 CWE assigned, which represents a set of 161 CVEs. Finally, TID-412 has no linked CVE and 2 CWEs, which include respectively a set of 1399 CVEs for CWE-306 and 35 CVEs for CWE-15, for a total of 1434 CVEs in the global CVE set. This information is summarized in Table II.

TABLE II
COMPONENTS OF THE CVE SET FOR EMB3D THREATS TID-406, TID-407 AND TID-412

Threat	CVE	CWE	CVE Pool
TID-406	CVE-2022-30266, CVE-2022-33139, CVE-2019-18250, CVE-2019-6533	CWE-306, CWE-287	4996
TID-407	CVE-2017-6034, CVE-2013-2820	CWE-294	161
TID-412		CWE-306, CWE-15	1434

2) Average CVSS score computing: The second step is to compute the average CVSS score of TID-406, TID-407 and TID-412. Table III shows the distribution of CVE according to their metrics values. For example, the TID-406 has 93% of its CVE set with an *Attack Complexity* metric equal to *Low*.

As a side note, the cost function uses metrics defined by the CVSS V3.1, thus CVEs that do not contain a CVSS V3.1 score in the NVD were removed from the set (1824 CVEs removed for TID-406, i.e. a set of 3172 remaining CVEs). This large cut in the set is explained by the fact that the CVSS V3.1 has been released in 2019 whereas NVD includes all CVEs since 1999.

We obtain the following average score for the threats TID-406, TID 407 and TID-412:

$$\begin{aligned} TID_{407}(av, ac, pr, ui) &= ((88 * 0.85 + 37 * 0.62 + 8 * 0.55 + 4 * 0.2)/137, \\ &\quad (91 * 0.77 + 46 * 0.44)/137, \\ &\quad (117 * 0.85 + 16 * 0.62 + 4 * 0.27)/137, \\ &\quad (121 * 0.85 + 16 * 0.62)/137) \\ &= (0.75, 0.66, 0.81, 0.82) \\ TID_{406}(av, ac, pr, ui) &= (0.78, 0.75, 0.79, 0.84) \\ TID_{412}(av, ac, pr, ui) &= (0.80, 0.76, 0.82, 0.84) \end{aligned}$$

[1]https://emb3d.mitre.org/threats/TID-406.html

[2]https://emb3d.mitre.org/threats/TID-407.html

[3]https://emb3d.mitre.org/threats/TID-412.html

TABLE III
METRICS VALUES DISTRIBUTION FOR IMPERSONATE SEQUENCE THREATS

Metrics	Values	TID-406	TID-407	TID-412
Attack Vector	Network	0.80	0.64	0.85
	Adjacent	0.06	0.27	0.06
	Local	0.08	0.06	0.06
	Physical	0.05	0.03	0.03
Attack Complexity	Low	0.93	0.66	0.96
	High	0.07	0.34	0.04
Privileges Required	None	0.79	0.85	0.84
	Low	0.18	0.12	0.12
	High	0.03	0.03	0.03
User Interaction	None	0.96	0.88	0.97
	Required	0.04	0.12	0.03

3) Threat score aggregation: Once the threat's metrics values have been computed, we aggregate them according to the *impersonate* sequence, i.e. (406, 407, 412) and the aggregation function $*$:

$$\begin{aligned} impersonate(av, ac, pr, ui) &= (av_{406}, av_{406}, pr_{406}, ui_{406}) \\ &\oplus (av_{407}, ac_{407}, pr_{407}, ui_{407}) \\ &\oplus (av_{412}, ac_{412}, pr_{412}, ui_{412}) \\ &= (av_{406} * av_{407} * av_{412}, \cdots, ui_{406} * ui_{407} * ui_{412}) \\ &= (0.78 * 0.75 * 0.80, \cdots, 0.84 * 0.82 * 0.84) \\ &= (0.47, 0.38, 0.52, 0.58) \end{aligned}$$

4) Sequence cost computation: Finally, we compute the sequence score by using the Euclidean norm function of the sequence vector:

$$\begin{aligned} cost(impersonate(av, ac, pr, ui)) &= \sqrt{av^2 + ac^2 + pr^2 + ui^2} \\ &= \sqrt{0.47^2 + 0.38^2 + 0.52^2 + 0.58^2} \\ &= 0.98 \end{aligned}$$

We therefore find the same cost (0.98) as that presented in Table I.

V. CONCLUSION

In order to automate cybersecurity risk analysis, we proposed in this paper CYBERSIM, a formal framework for the generation of attack scenarios that can have an impact on the safety of Cyber-Physical Systems (CPS), by focusing on the key problem of state-space explosion and handling the most relevant scenarios. Our model-based approach using discrete event systems considers the intentional actions of an attacker which are performed in a well-defined order to reach specific objectives. A multi-metric quantitative analysis based on the various security metrics such as the attack vector, the attack complexity, the required privileges and the need for a human user is proposed to filter the most probable scenarios. These exploitability metrics extracted from CVSS to compute the cost of MITRE EMB3D threats are applied to the EVITA case study to illustrate the approach.

Since our multi-metric framework is generic, we can adapt the approach to other metrics in cybersecurity risk quantification covering various points of view such as attacker motivation, financial cost [30], etc. The results will help risk analysts to automate tasks and optimize the time spent in assessing the most likely scenarios and identifying weaknesses in system architecture. System designers can then effectively choose compensatory or corrective measures to inhibit the consequences of the identified sequences or to attenuate their criticality. All this from the system design stage, by combining both safety and security analyses in the same tool.

Thanks to these quantitative assessments, the selection of the most plausible cyberattack paths can also be used in intrusion test to assist the auditor with a tool to assess a system's resilience. Knowledge of the most relevant attack scenarios without countermeasures will also enable the design of detection rules to raise a security alert when the presence of certain steps in the attack path is detected, which is very helpful for Security Operations Center (SOC) detection.

The implementation of the research results in SimfiaNeo, a tool developed by Airbus Protect for safety analyses is a major technical challenge for the company as well as a quite promising potential business asset, because it will improve the performance of its software in terms of cybersecurity disciplines and constitute a major advance in the effectiveness of the adaptation of "model-based" approaches to cybersecurity specificities.

Future work will delve deeper into the decision-making process for choosing metrics and functions (aggregation function and cost function) to explore their relevance and impact on the final score. In addition, we plan to reduce the uncertainty of metric value assignment for large and diverse CVEs sets by filtering CVEs based on component attributes. Finally, we will test the framework in different industry-derived use cases to assess the operational relevance of the simulated attack scenarios proposed by CYBERSIM.

VI. ACKNOWLEDGMENTS

This work was supported by a French government grant managed by the Agence Nationale de la Recherche under the France 2030 program, reference ANR-22-PTCC-0001.

This paper has been sponsored by the Innovation team of Airbus Protect, a subsidiary of the aerospace group Airbus specialised in risk management in the fields of cybersecurity, safety, and sustainability.

REFERENCES

[1] Airbus Protect, "SimfiaNeo software," last accessed 2025-03-20. [Online]. Available: https://www.protect.airbus.com/safety/simfianeo/

[2] T. Serru, N. Nguyen, M. Batteux, and A. Rauzy, "Minimal Critical Sequences in Model-based Safety and Security Analyses: Commonalities and Differences," *ACM Transactions on Cyber-Physical Systems*, vol. 7, no. 3, Jul. 2023.

[3] MITRE corporation, "The EMB3D™ Threat Model for Embedded Devices," last accessed 2025-03-18. [Online]. Available: https://emb3d.mitre.org/

[4] ——, "CVE® Program," last accessed 2025-03-18. [Online]. Available: https://www.cve.org/

[5] FIRST, "Common Vulnerability Scoring System SIG," last accessed 2025-03-20. [Online]. Available: https://www.first.org/cvss/

[6] EVITA Project, "Evita: E-safety vehicle intrusion protected applications," last accessed 2025-03-21. [Online]. Available: https://www.evita-project.org/

[7] MITRE, "Attack Flow," last accessed 2025-03-18. [Online]. Available: https://ctid.mitre.org/projects/attack-flow

[8] A. Ramos, M. Lazar, R. H. Filho, and J. J. P. C. Rodrigues, "Model-based quantitative network security metrics: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2704–2734, 2017.

[9] A. Singhal and X. Ou, *Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs*. Cham: Springer International Publishing, 2017, pp. 53–73. [Online]. Available: https://doi.org/10.1007/978-3-319-66505-4_3

[10] I. Semertzis, V. S. Rajkumar, A. Ştefanov, F. Fransen, and P. Palensky, "Quantitative risk assessment of cyber attacks on cyber-physical systems using attack graphs," in *2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, 2022, pp. 1–6.

[11] C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in *Proceedings of the 1998 Workshop on New Security Paradigms*, ser. NSPW '98. New York, NY, USA: Association for Computing Machinery, 1998, p. 71–79. [Online]. Available: https://doi.org/10.1145/310889.310919

[12] R. Ortalo, Y. Deswarte, and M. Kaaniche, "Experimenting with quantitative evaluation tools for monitoring operational security," *IEEE Transactions on Software Engineering*, vol. 25, no. 5, pp. 633–650, 1999.

[13] N. Idika and B. Bhargava, "Extending attack graph-based security metrics and aggregating their application," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 75–85, 2012.

[14] J. Pamula, S. Jajodia, P. Ammann, and V. Swarup, "A weakest-adversary security metric for network configuration security analysis," in *Proceedings of the 2nd ACM Workshop on Quality of Protection*, ser. QoP '06. New York, NY, USA: Association for Computing Machinery, 2006, p. 31–38.

[15] S. Noel, L. Wang, A. Singhal, and S. Jajodia, "Measuring security risk of networks using attack graphs." *International Journal of Next-Generation Computing*, vol. 1, 01 2010.

[16] M. Frigault and L. Wang, "Measuring network security using bayesian network-based attack graphs," in *2008 32nd Annual IEEE International Computer Software and Applications Conference*, 2008, pp. 698–703.

[17] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel, "Time-to-compromise model for cyber risk reduction estimation," in *Quality of Protection*, D. Gollmann, F. Massacci, and A. Yautsiukhin, Eds. Boston, MA: Springer US, 2006, pp. 49–64.

[18] K. Sallhammar, B. Helvik, and S. Knapskog, "Towards a stochastic model for integrated security and dependability evaluation," in *First International Conference on Availability, Reliability and Security (ARES'06)*, 2006, pp. 8 pp.–165.

[19] A. B. Rauzy, "Mathematical foundations of minimal cutsets," *IEEE Transactions on Reliability*, vol. 50, pp. 389–396, 2001. [Online]. Available: https://api.semanticscholar.org/CorpusID:323377

[20] T. Mahler, E. Shalom, A. Makori, Y. Elovici, and Y. Shahar, "A Cyber-Security Risk Assessment Methodology for Medical Imaging Devices: the Radiologists' Perspective," in *Journal of Digital Imaging 35*, 2022, p. 666–677.

[21] S. Yuan, M. Yang, and G. Reniers, "Integrated process safety and process security risk assessment of industrial cyber-physical systems in chemical plants," *Computers in Industry*, vol. 155, p. 104056, 2024.

[22] A. Sen and S. Madria, "Application design phase risk assessment framework using cloud security domains," *Journal of Information Security and Applications*, vol. 55, p. 102617, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212620307821

[23] Z. Luo, R. Xu, J. Wang, and W. Zhu, "A dynamic risk assessment method based on bayesian attack graph," *International Journal of Network Security*, vol. 24, no. 5, pp. 787–796, Sep 2022.

[24] A. Yousaf, A. Amro, P. T. H. Kwa, M. Li, and J. Zhou, "Cyber risk assessment of cyber-enabled autonomous cargo vessel," *International Journal of Critical Infrastructure Protection*, vol. 46, p. 100695, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548224000362

[25] O. Duman, M. Zhang, L. Wang, M. Debbabi, R. F. Atallah, and B. Lebel, "Factor of security (fos): Quantifying the security effectiveness of redundant smart grid subsystems," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1018–1035, 2022.

[26] G. Gori, L. Rinieri, A. Melis, A. Al Sadi, F. Callegati, and M. Prandini, "A systematic analysis of security metrics for industrial cyber–physical systems," *Electronics*, vol. 13, no. 7, 2024. [Online]. Available: https://www.mdpi.com/2079-9292/13/7/1208

[27] MITRE, "CWE - Common Weakness Enumeration," last accessed 2025-03-20. [Online]. Available: https://cwe.mitre.org/index.html

[28] NIST, "National Vulnerability Database," last accessed 2025-03-26. [Online]. Available: https://nvd.nist.gov/

[29] T. Serru, N. Nguyen, M. Batteux, A. Rauzy, R. Blaize, L. Sagaspe, and E. Arbaretier, "Generation of Cyberattacks Leading to Safety Top Event Using AltaRica: an Automotive Case Study," in *23e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Institut pour la Maîtrise des Risques (Lambda Mu 23)*, Paris-Saclay, France, Oct. 2022. [Online]. Available: https://hal.science/hal-03814648

[30] FAIR Institue, "Factor Analysis of Information Risk," last accessed 2025-03-18. [Online]. Available: https://www.fairinstitute.org/what-is-fair