Modeling Cyberattacks Affecting Systems' Safety with AltaRica: Achievements and Future Works

Théo Serru, Nga Thi Viet Nguyen, Michel Batteux

Modeling Cyberattacks Affecting Systems' Safety with AltaRica: Achievements and Future Works

1st Théo Serru
ETIS UMR 8051
CY Cergy Paris University, ENSEA, CNRS
Airbus Protect, France
theo.serru@ensea.fr

2nd Nga Nguyen
Leonard de Vinci Pole Universitaire
Research Center
France
nga.nguyen@devinci.fr

3rd Michel Batteux
Systemic Intelligence
France
michel.batteux.pro@laposte.net

***Abstract*—Cyber-physical systems are safety and security-critical because of their close interactions with humans and the environment. For this reason, their failures may have effects on humans, making them safety-critical. On the other hand, the integration of computational capabilities brings the risks of cyberattacks that may have effects on confidentiality, integrity, availability, and also safety. In the industry, the cybersecurity risk analysis of cyber-physical systems is insufficiently automatized and error-prone. To tackle this open issue, we propose a model-based approach using the formal language AltaRica and the industrial tool SimfiaNeo, to model systems, their behaviors in case of cyberattacks, and automatically generate the full set of attack scenarios leading to a safety-critical situation. In addition to the modeling, we propose a heuristic cutoff to reduce the state-space explosion. We end this position paper by evoking the remaining issues and future challenges of this work.**

***Index Terms*—Cyberattacks, Safety, Sequences of Events, AltaRica, SimfiaNeo**

I. Introduction

Assessing safety and security risks for cyber-physical systems is of critical importance in modern industries. However, safety and security are mostly clustered fields with few communications between teams. As a result, advances in safety have poorly benefited cybersecurity engineers. Cybersecurity risk assessments are thus poorly automatized, difficultly maintainable, and error-prone.

To tackle these limitations, a large number of works developed model-based approaches. Among the most popular we can find attack graphs, attack trees, Markov chains, Petri nets, and more. Several surveys summarize the advances in this field [1]–[3]. However, to our knowledge, none of these have reached industrial maturity (unlike safety's fault trees). We believe these works should focus more on industrial needs to better integrate into their processes.

Our work proposes to tackle these limitations by integrating engineers' needs into the requirements and using an industrial tool already in use for safety assessments. Therefore, this approach is based on the formal language AltaRica and the tool SimfiaNeo and allows to: i) model the architecture of cyber-physical systems, ii) model attack propagation in the system, iii) generate all the sequences of attacks leading to a safety-critical situation, and iv) embed state-space reduction capabilities. Our model can be used as part of the risk assessment process found in regulations (e.g. ED-203A) as displayed in Figure 1. This position paper briefly presents our contributions and discusses some future perspectives that are meant to ease industrial adoption.

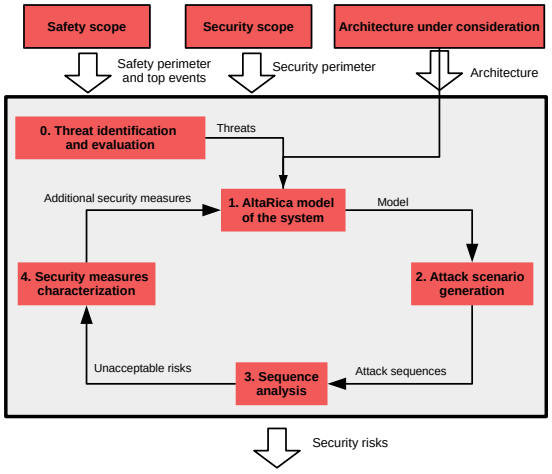

Fig. 1. Cybersecurity Risk Assessment Embedding AltaRica Model, Inspired from ED-203A

II. Modeling and Analyzing Cyber-Physical Systems

A. Modeling

Our approach relies on the AltaRica formal language and the SimfiaNeo platform. AltaRica can be seen as a sandbox allowing to model any component, attack, or reconfiguration using variables, transitions, and assertions. As part of the process depicted in Figure 1, we first need to model the system architecture. Components are modeled as AltaRica blocks, embedding variables encoding its state. Variables can be Booleans or take their values on a user-defined domain such as: *role*(none, user, root) that encodes the privilege of the attacker on a given component, or *CIA*(nominal, loss, partial loss) that encodes the state of confidentiality, availability, and integrity. We also model links to represent the data-flows circulating between components. In our models, links embed variables that represent data-flows, and the presence of the attacker.

Cyberattacks are modeled using AltaRica transitions. It corresponds to transitions from the state where the attack is available, to the state where the attack happened. The attack's pre-condition (called *guard*) is a Boolean formula that expresses all the conditions for the attacker to be able to launch the attack. The post-condition changes the variable's value to the desired one. For example, consider the following transition.

$$\begin{array}{c}(availability = nominal) and (role = root) | - \\ denial\ of\ service - > availability := loss;\end{array} \quad (1)$$

We model the fact that a denial of service will, for instance, change the value of availability from *nominal* to *loss* and may require a *root* privilege.

Countermeasures are also modeled with variables. However, as the model is dysfunctional, there is always a means to bypass or deactivate countermeasures. For example, a firewall will stop incoming infected data if active, but the attacker might exploit a vulnerability to deactivate or pass through.

B. Assessing

From a model, we aim to explore every sequence of actions leading to a safety top event. This top event is defined as a Boolean formula over the model's variables. The algorithm will explore the full state space and output the sequences leading to this top event. A sequence takes the form of a set of individual attacks on components from the initial state to the top event.

Unsurprisingly, this kind of sequence exploration is subject to state-space explosion. With a model of 14 components, 60 events, presented in [4] we ended up with more than 400000 sequences for one top event. Analyzing them is very time consuming and reduction methods must be applied. We applied minimality like in safety to reduce the number of sequences to 116. However, minimality is not enough to discard all the sequences that contain events happening in an irrelevant order.

Sequences of cyberattacks are different from sequences of failures. The former tends to be longer and probabilities are not sound as we do not benefit from industrial feedback. Consequently, thresholds on length and probabilities (used in safety) make little sense. However, the actions of the intruder are deliberately directed toward a goal. Against protected systems, attackers will often have to achieve several subgoals to achieve their main goal. Taking these into account allowed us to define a new cutoff dedicated to sequences of cyberattacks, called *footprint* and defined in [5]. This cutoff weights an event if it is independent of the previous one. With this cutoff, we can prioritize the analysis of sequences where the attacker focuses on one sub-goal at a time, and performs attacks in a more efficient/logical way. Finally, the cutoff allows to drastically reduce the computation time. For the example of article [4] we were able to reduce the number of sequences to 72, and the computation time from 14 minutes to 1 second.

III. Conclusion and Future Works

In this document, we briefly present a formal model to generate scenarios of cyberattacks affecting the safety of cyber-physical systems. This approach tackles some issues that we found in the literature: few models of the architecture, state-space explosion, and lack of industrial considerations. By using an industrial tool based on a formal language, and by proposing a heuristic cutoff to prioritize the analysis of the most relevant sequences, we focus on the usability of our model. However, the modeling can still be improved in order to ease the integration into industrial processes and deal with regulations.

We propose some future perspectives and wish to find new ones during the conference session.

- Joined safety and cybersecurity analyses are strongly limited by the use of probabilities. Safety assessments are probabilistic in nature which is not the case in cybersecurity. However, the use of a common model for safety and cybersecurity is of great interest to improve communication between both teams. One idea might be to inform failures and cyberattacks in the same model but only generate sequences of failures or cyberattacks. However, this will lead to complex models that might be difficult to build and maintain.
- Quantitative analyses are important in a risk assessment, and are often required by regulations. Even if current metrics are poorly validated, analysts might still want to use them in one way or another. One critical improvement will be to develop sound and validated metrics. This work needs a group of experts and some time to be developed. In the meantime, we plan to prove that the metrics from the literature can be handled with AltaRica, and we will study the use of importance factors in cybersecurity.
- Integration into a risk assessment process in the industry is also of critical importance. To stress the modeling and prove the scalability, we should model a real industrial system and compare the results with the results obtained by classical analyses.

We believe that this model-based approach will help engineers in their task of securing systems, but further improvements are required.

References

[1] J. Geismann and E. Bodden, "A systematic literature review of model-driven security engineering for cyber–physical systems," *Journal of Systems and Software*, vol. 169, p. 110697, Nov. 2020.

[2] H. S. Lallie, K. Debattista, and J. Bal, "A review of attack graph and attack tree visual syntax in cyber security," *Computer Science Review*, vol. 35, p. 100219, Feb. 2020.

[3] P. Nguyen, S. Wang, and T. Yue, "Model-Based Security Engineering for Cyber-Physical Systems: A Systematic Mapping Study," *Information and Software Technology*, vol. 83, Nov. 2016.

[4] 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 *Congrès Lambda Mu 23*, Paris-Saclay, France, oct 2022.

[5] T. Serru, N. Nguyen, M. Batteux, and A. Rauzy, "Minimal critical sequences in model-based safety and security analyses: Commonalities and differences," *ACM Trans. Cyber-Phys. Syst.*, may 2023.