Cybersecurity for critical embedded systems using AI

Céline Bellanger - Interactive Informatics Team
Supervisors: Pierre-Loïc Garoche[1], Matthieu Martel[2], Celia Picard[1]
[1]ENAC: LII, [2]UPVD

Context

Artificial intelligence is increasingly used in aeronautical embedded systems to perform various functions, such as:

⟶ GNC functions like stabilization or guidance

Example: autonomous rocket lander on mars [1]

⟶ Autonomous flight based on image recognition

Example: Autonomous Taxi, Take-Off and Landing project, by Airbus [2]

These methods are based on neural networks, imitating the functioning of human neurons to solve complex tasks. This leaves room for new types of cyberattacks.

Objectives:

⟶ Improve neural networks robustness: show that signals from neural networks always respect certain properties, whatever the input values.

⟶ Identify counter examples: use model checking to highlight potential situations that do not meet the requirements.

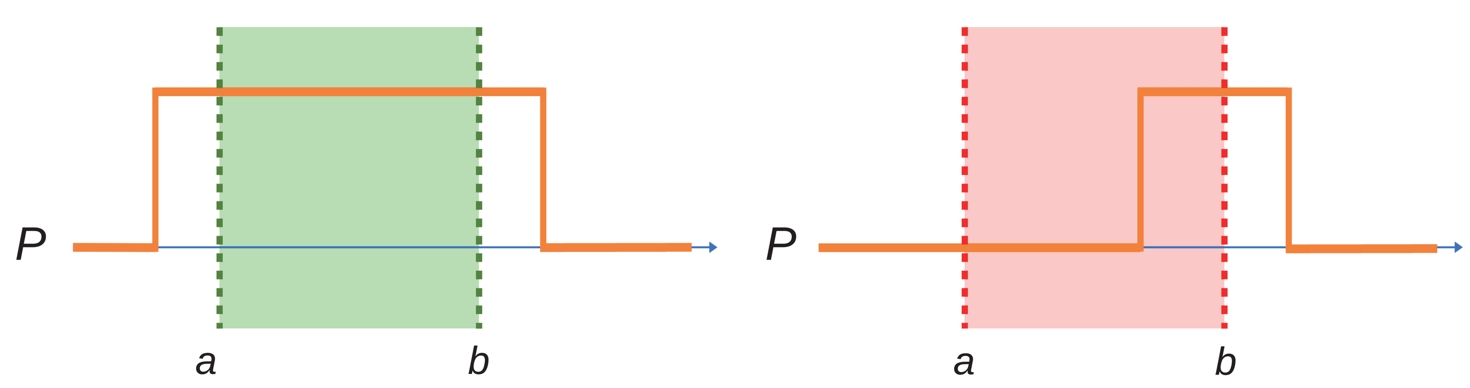
Signal temporal logic: a way to study signals behavior

Temporal logic is a form of logic involving temporal operators to verify properties as a function of time, such as *always* (□) - the property has to be satisfied at all times - or *eventually* (◊) - the property has to be satisfied at least one time.

Signal Temporal Logic (STL) evaluates these properties on a bounded horizon, as in the following example:

Property to verify: $\square_{[a,b]} P$

At any time between a and b, P must be true



Case 1: the STL property is satisfied

Case 2: the STL property is not satisfied

A first proposition to apply STL to dynamical systems has been made [3,4], subject to some limitations.

Our approach

We want to formally prove the operation of neural networks, using STL properties. This would ensure that neural networks are robust to external perturbations, and particularly to attacks based on input data alteration.

Next steps:

Step 1

Prove the operation of the existing STL modules

Step 2

Improve STL modules to adapt them to the embedded systems specificities

Step 3

Apply the STL modules to neural networks

References

[1] Airbus concludes ATTOL with fully autonomous flight tests—Airbus. https://www.airbus.com/en/newsroom/press-releases/2020-06-airbus-concludes-attol-with-fully-autonomous-flight-tests. Accessed 12 Dec 2022

[2] ESA - Next Generation Landing Technologies - ESA. https://www.esa.int/Science_Exploration/Human_and_Robotic_Exploration/Lunar_Lander/Next-generation_landing_technology. Accessed 20 Feb 2023

[3] Kapinski, James, Xiaoqing Jin, Jyotirmoy Deshmukh, Alexandre Donzé, Tomoya Yamaguchi, Hisahiro Ito, Tomoyuki Kaga, Shunsuke Kobuna, et Sanjit Seshia. « ST-Lib: A Library for Specifying and Classifying Model Behaviors », 2016. https://doi.org/10.4271/2016-01-0621.

[4] Balsini, Alessio, Marco Di Natale, Marco Celia, et Vassilios Tsachouridis. « Generation of simulink monitors for control applications from formal requirements ». In 2017 12th IEEE International Symposium on Industrial Embedded Systems (SIES), 1-9, 2017. https://doi.org/10.1109/SIES.2017.7993389.

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

ENAC