

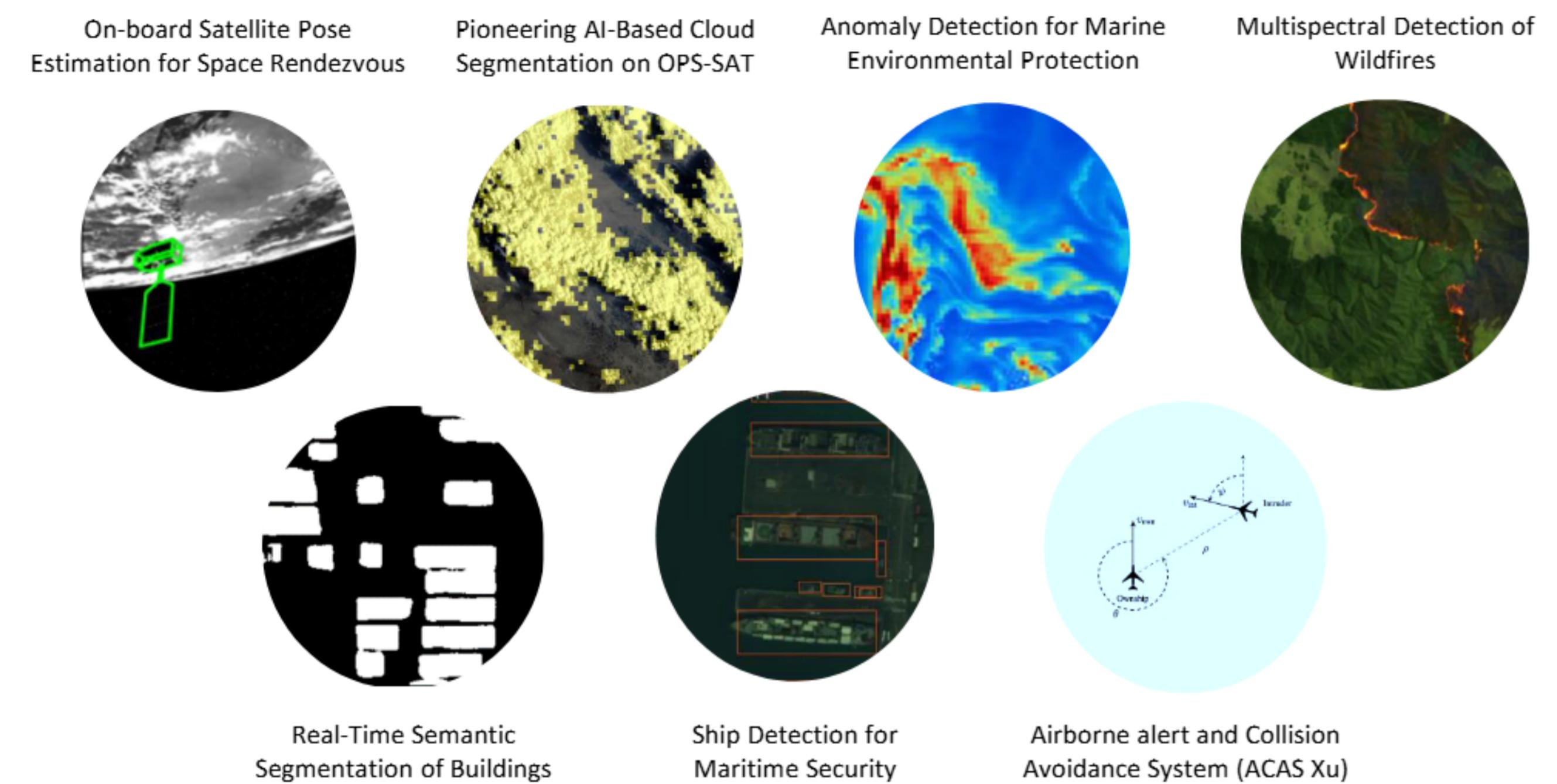
On-board AI for Critical Applications

Christophe Marabotto¹

¹Institute of Research and Technology Saint Exupéry

Aerospace Use-cases

We are involved in a wide diversity of aeronautics and space projects based on Deep Learning techniques.



AI Development Workflow for Critical Applications

This work is divided into different stages:

- **Operational Design Domain:** How do you specify the operational scenarios to be resolved ?
- **Data Management:** What characterises a high quality dataset ?
- **ML Constituent Design:** What should be taken into account during the model design phase in critical context ?
- **ML Deployment:** How to carry out an ML deployment pipeline in accordance with safety standards ?
- **On-board constituent requirements verifications:** What attributes should be checked once the model is deployed and how should they be measured ?

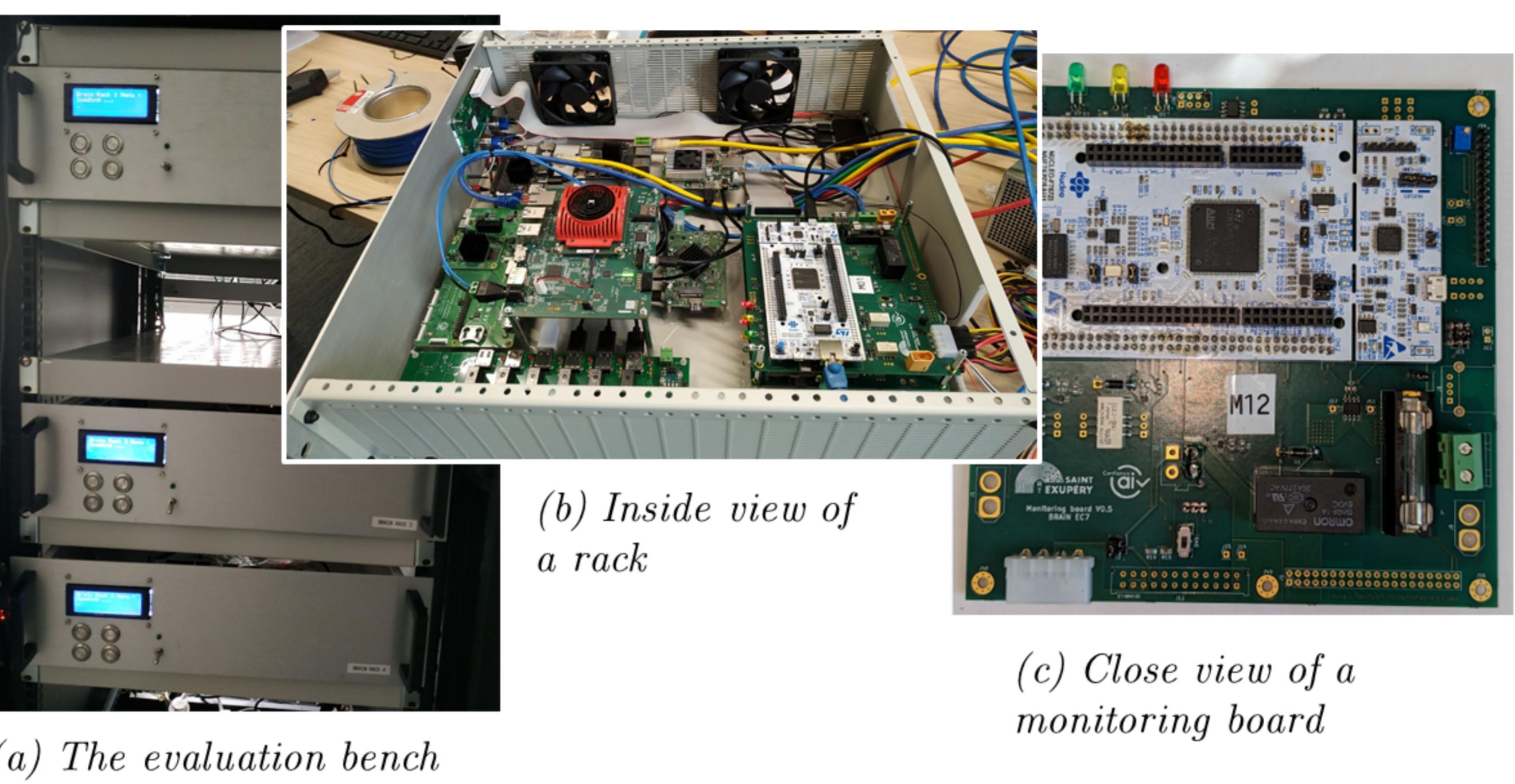
AI Certification

In order to meet aeronautical (EASA / DO) and space (ECSS) certification standards, several projects are working to improve the operational safety of AI-based systems.

- SONNX: Safe Open Neural Network Exchange (ONNX)
- AlxA: Artificial Intelligence for Interference Analysis
- DEEL (see respective section)

Evaluating AI Model for On-Board Applications

We propose an evaluation bench (mltestbench [4]) that (i) integrates the necessary software and hardware resources (tools, boards) to deploy a variety of ML models, and (ii) provides a uniform and abstract API to exercise and evaluate multiple deployment solutions.



(b) Inside view of a rack

(c) Close view of a monitoring board

(a) The evaluation bench

BIRD Project

BIRD is the name of a small two-wheeled robot that serves as a demonstrator of some of the technologies developed at IRT. The technological building blocks in development include:

- Robust Reinforcement Learning for Object Grasping using myArm C650 from Elephant Robotics
- IHM: Text-to-Speech, LLM and Speech-to-Text on NVIDIA Jetson AGX Orin
- Object Detection

DEEL Project

Dependable, Certifiable & Explainable Artificial Intelligence for Critical Systems

Explainability

Xplique [1] is a Python toolkit dedicated to explainability. The goal of this library is to gather the state of the art of Explainable AI to help you understand your complex neural network models. Originally built for Tensorflow's model it also works for PyTorch models partially.

Conformal Prediction

Punc [6] (short for Predictive uncertainty calibration and conformalization) is an open-source Python library. It seamlessly integrates a collection of state-of-the-art conformal prediction algorithms

Lipschitz Neural Network

deel-lip [7] provides an efficient implementation of k-Lipschitz layers for keras. It has many applications ranging from adversarial robustness to Wasserstein distance estimation.

$$\|f(x_1) - f(x_2)\| \leq L\|x_1 - x_2\|$$

Open questions

1. What future challenges in robotics can AI address?
2. How can we ensure the dependability of robots based on foundation models?
3. How to deal with autonomy (local vs remote computing) ?

References

- [1] Thomas Fel, Lucas Hervier, David Vigouroux, Antonin Poche, Justin Plakoo, Remi Cadene, Mathieu Chalvidal, Julien Colin, Thibaut Boissin, Louis Bethune, Agustin Picard, Claire Nicodeme, Laurent Gardes, Gregory Flandin, and Thomas Serre. Xplique: A deep learning explainability toolbox. In *Workshop on Explainable Artificial Intelligence for Computer Vision (CVPR)*, 2022.
- [2] Fabien Gallet, Christophe Marabotto, and Thomas Chambon. Exploring ai-based satellite pose estimation: from novel synthetic dataset to in-depth performance evaluation. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 6770–6778, 2024.
- [3] Thomas Goudement, Benjamin Francesconi, Michelle Aubrun, Erwann Kervennic, Ingrid Grenet, Yves Bobichon, and Marjorie Bellizzi. Onboard anomaly detection for marine environmental protection. In *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 2024.
- [4] Eric Jenn, Floris Thiant, Theo Allouche, Halima Bouzidi, Ramon Conejo-Laguna, Omar Hlimi, Cyril Louis-Stanislas, Christophe Marabotto, Smail Niar, Serge Romaric Tembo Mouaf, et al. An evaluation bench for the exploration of machine learning deployment solutions on embedded platforms. In *12th European Congress Embedded Real Time Systems-ERTS 2024*, 2024.
- [5] Erwann Kervennic, Thomas Louis, Michael Benguigui, Yves Bobichon, Nicolas Avaro, Ingrid Grenet, Frédéric Féresin, and Adrien Girard. Embedded cloud segmentation using ai: Back on years of experiments in orbit on ops-sat. In *2023 European Data Handling & Data Processing Conference (EDHPC)*, pages 1–8. IEEE, 2023.
- [6] Mouhcine Mendil, Luca Mossina, and David Vigouroux. Punc: a python library for predictive uncertainty calibration and conformalization. In *Conformal and Probabilistic Prediction with Applications*, pages 582–601. PMLR, 2023.
- [7] Mathieu Serrurier, Franck Mamalet, Alberto González-Sanz, Thibaut Boissin, Jean-Michel Loubes, and Eustasio del Barrio. Achieving robustness in classification using optimal transport with hinge regularization, 2020.