SAFE MACHINE LEARNING

Is Machine Learning safe for Critical Embedded Systems ?

CS

a Sopra Steria company

1

WHAT IS MACHINE LEARNING (ML) ?

Machine Learning is the ability of a system to learn from data and make predictions or decisions without being explicitly programmed.

✓ Effective for tasks like object detection and anomaly recognition.

✗ However, ML models can behave unpredictably, posing challenges in safety-critical environments

a Sopra Steria company

2

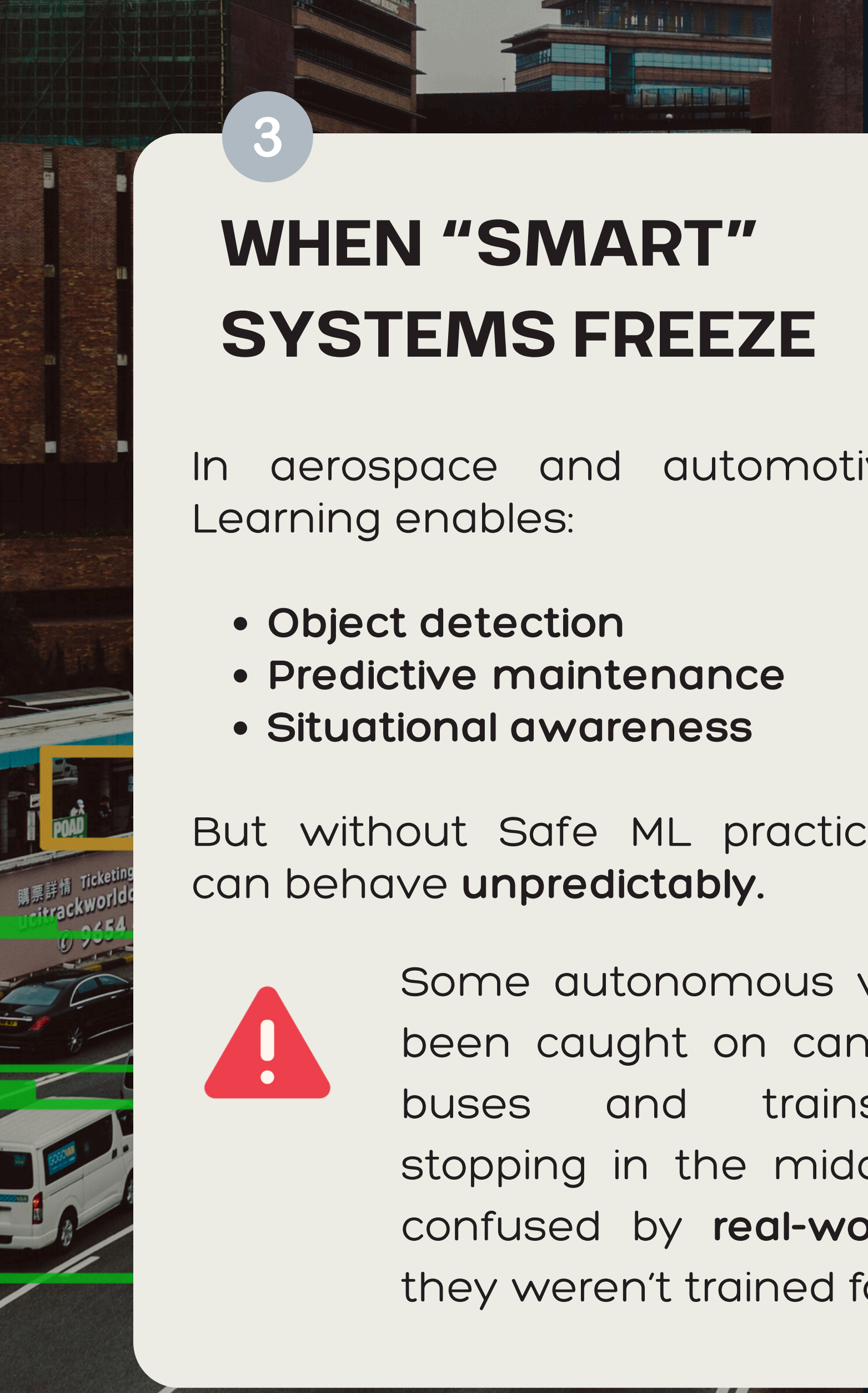
WHAT IS SAFE ML ?

Safe Machine Learning involves applying ML in a manner that ensures **safety, reliability, and compliance** in critical systems.

Key aspects include:

- 👉 Making ML behavior **explainable**
- 👉 Ensuring **robustness** under edge cases
- 👉 Complying with **functional safety standards** (e.g. ISO 26262, DO-178C....)

a Sopra Steria company



3

WHEN “SMART” SYSTEMS FREEZE

In aerospace and automotive, Machine Learning enables:

- **Object detection**
- **Predictive maintenance**
- **Situational awareness**

But without Safe ML practices, systems can behave **unpredictably**.

Some autonomous vehicles have been caught on camera blocking buses and trains, suddenly stopping in the middle of traffic– confused by **real-world scenarios** they weren’t trained for.

4

WHAT WE BRING AT CS NORTH AMERICA

Whether concerned with model training, model deployment, or integration into a complete product, we can help by :

- **Explaining your model** using industry-standard tools

- **Improving robustness** through data & model validation, and establishment of KPIs

- **Streamlining certification** by providing the framework and aligning your artifacts to the relevant standard

We specialize in safety-critical embedded software and are working to bring Safe ML to these systems, reliably.

a Sopra Steria company