



AI Roadblock

Risk management



Regulatory compliance



Performance



Trust

We Believe

That AI has numerous applications that can benefit the most,
but it's facing **trust** challenges **preventing** its **adoption**...



**In critical applications,
“probably” safe is unacceptable**

Our Mission

Help all industries confidently deploy
trustworthy & regulatory compliant AI systems

To do so Numalis endorses two key roles:

Establish rigorous framework by writing
international standards on AI robustness



Scale & streamline formal validation techniques
with state-of-the-art tools



Our Partners and Clients

Aeronautics



Industry



Institutions



Defence










Standardisation



pumalis

High-Level Structuring Projects

Prime	Name	Objective
	MLEAP	Applicability of the EASA guideline for certification of AI avionic models
	NoLeFa	Developing the framework for notified bodies regarding the AI Act
	JEY CUAS	Specification of anti-drone systems
	AI4DEF	Methodology and tool for an AI for Defence platform
	CONVOY & GENIUS	Detection & neutralization of IED
	TELLi	Self piloting trains
	AITIVE	Validation of embedded AI system for space exploration

We are *numalis*

Trustworthy company you can rely on

French Deeptech founded in 2015

- 23 FTE with $\frac{3}{4}$ of engineers and PhD
- 10 innovation awards
- Editor of the static analyzer for AI: Saimple®

Experts in formal methods

- More than 2 decades of R&D
- More than 40 published scientific articles

Experts in AI standardization

- Active member of standardization bodies: ISO/IEC, CEN-CENELEC, AFNOR...
- Major contributor to ISO/IEC 24029 series on robustness assessment of AI systems

High-level experts team



- Standardization expert
- R&D team expanding the state of the art
- Scale up technology team
- Industrialization team
- Use case support team

Our Added Value



ISO/IEC 24029-2
process applied



Artificial Intelligence
Trustworthiness Framework



Streamline AI development

- Improve neural network design
- Improve neural network training

Build trust & Manage risks

- Explain model behavior
- Validate model robustness

Ensure regulatory compliance

- Enable certification
- Capture new business opportunities & unlock regulated markets

Standardization & EU Regulatory Landscape

The EU AI Act, a Risk Based Approach



Prohibited AI practices:
Unacceptable risk Art. 5

High-risk:
High-risk AI systems Art. 6

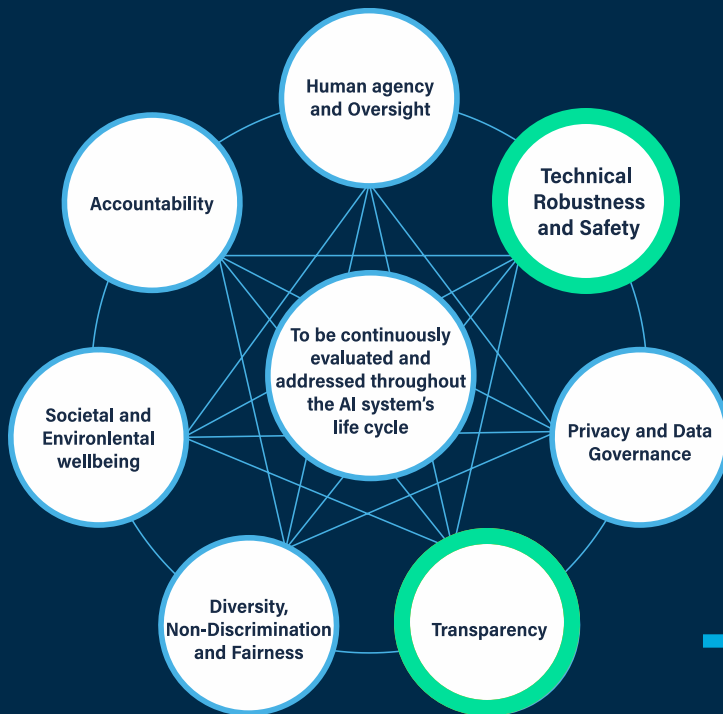
Transparency:
Limited-risk AI systems Art. 52

No obligations:
Low or minimal-risk AI systems Art. 69



Trustworthy AI
Source: HLEG, EU

Key Challenges we Address



We help prove AI model readiness for real world applications

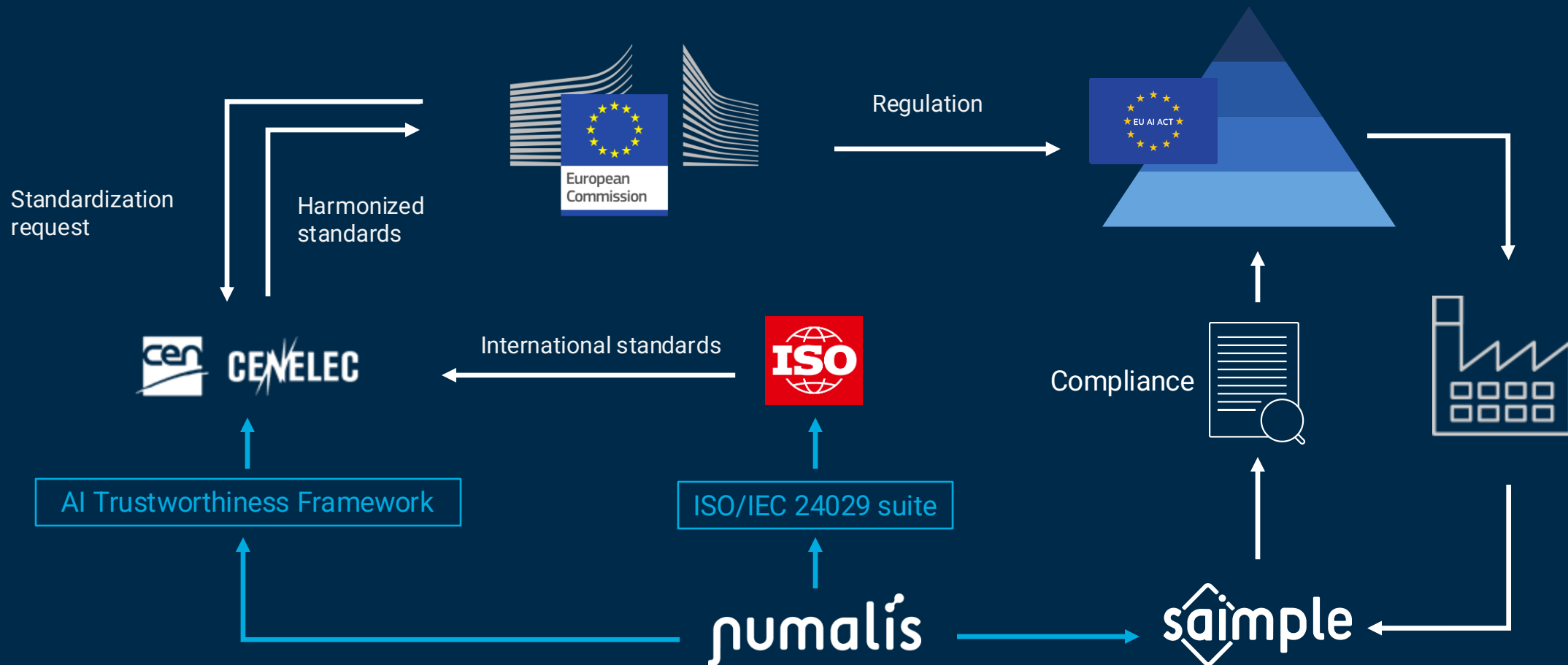
Using state-of-the-art techniques described in the standards, based on formal methods and abstract interpretation, we help demonstrate model ability to maintain stable decisions despite perturbations on inputs.

We help explain AI model decisions in human-understandable way

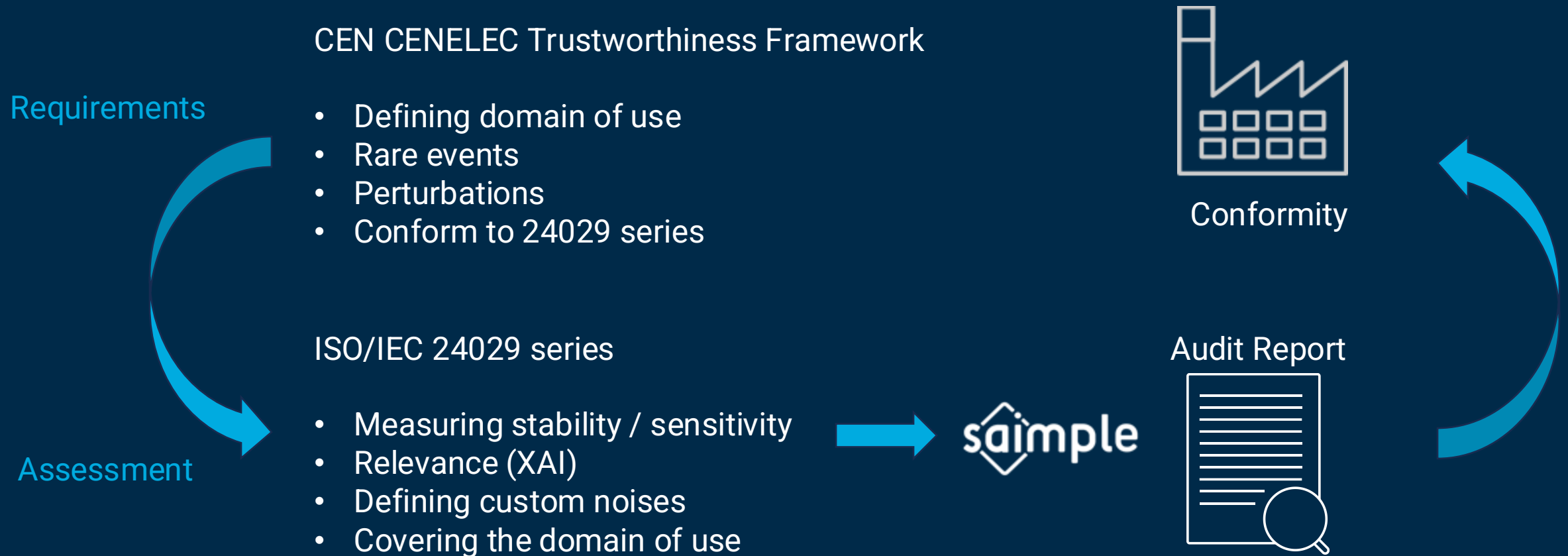
We help demonstrate model's trustworthiness through formal proof, ensuring transparency and accountability. By explaining how models function and make decisions, we enable to build trust, detect biases, and comply with regulations, improving both user confidence and system reliability.

EU AI Act mechanics

The regulation is implemented through harmonized standards produced by CEN and CENELEC using ISO documents. For robustness, the Trustworthiness Framework lays out the requirements and refers to the ISO/IEC 24029 standards, which Saimple ensures compliance with.

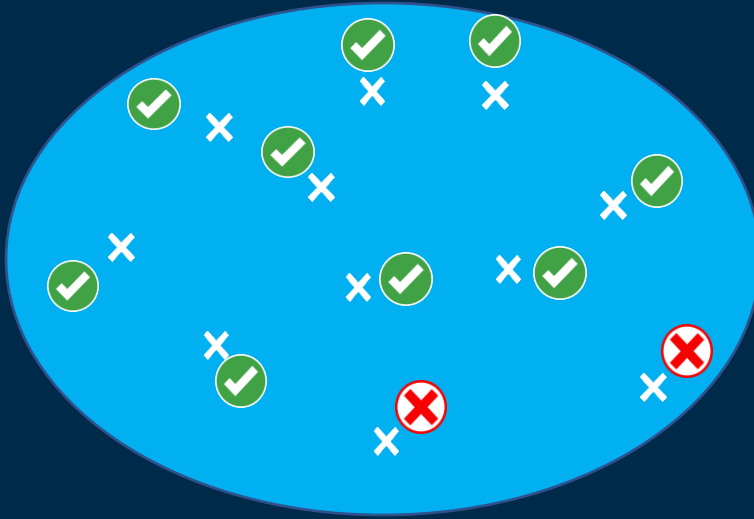


Robustness' standards and saimple



Using in your existing process

Statistical
methods



Formal
methods



Existing metrics

- Accuracy
- Recall
- F1-score
- AUC
- ...

Audit Report



- Stability and robustness
- Sensitivity
- Relevance
- Reachability
- ...

New metrics



Set of Tools for Achieving Trustworthy AI Models

Neural Network Explainability and Robustness Validation Solutions

saimple main features

Preparing

Applications :

- Domain specification
- Custom perturbation
- Training and support

Use :

- Expert at your disposal
- Fully scriptable tool

Evaluating

Applications :

- Understand the model behavior
- Identify bias
- Visualize input space robustness

Use :

- CI/CD integration
- Full automation

Correcting

Applications :

- Detect unbalanced robustness
- Identify errors in the training set
- XAI to adjust your training set
- Guide your data augmentation

Use :

- Before/After comparison
- Trigger correction request

Documenting

Applications :

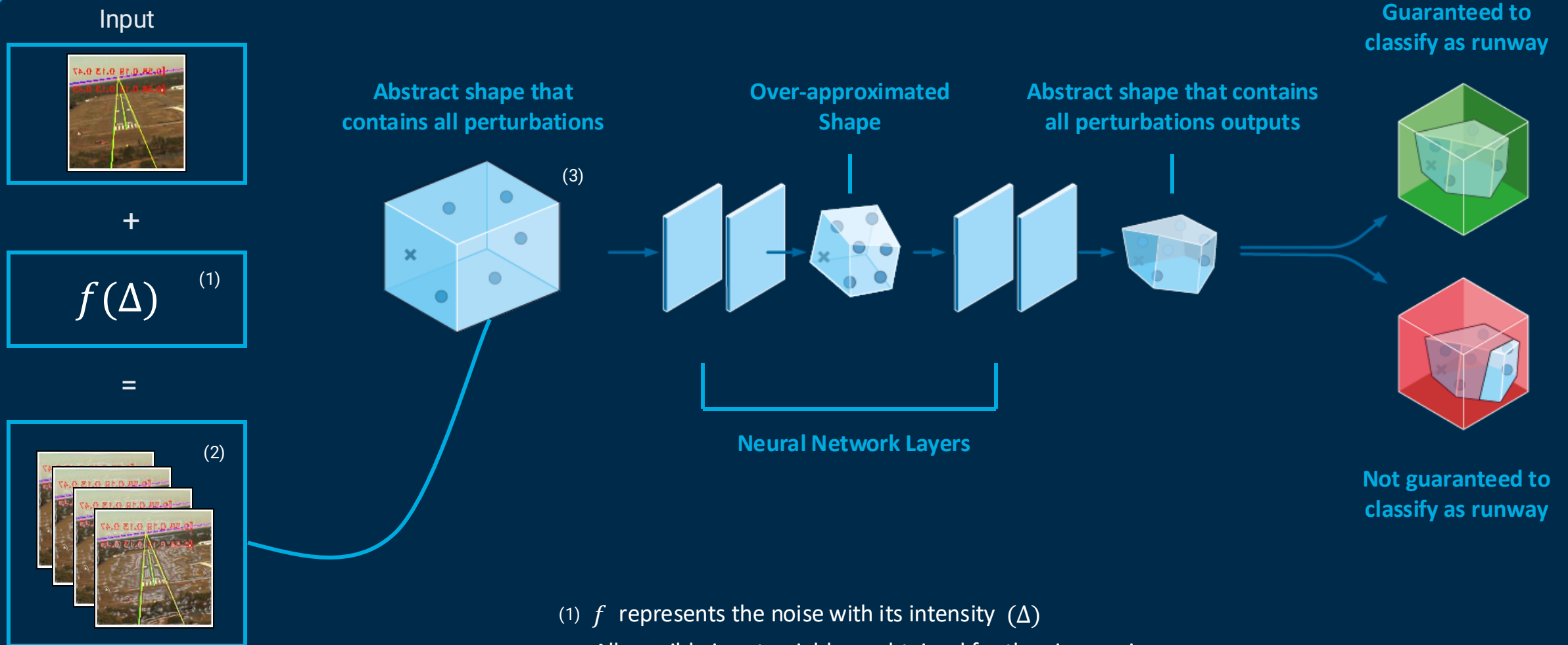
- Document testing procedure
- Validation process progress
- Impact of correcting actions

Use :

- Report generation
- Dashboard visualization
- Requirements traceability

Model Robustness Validation Principle

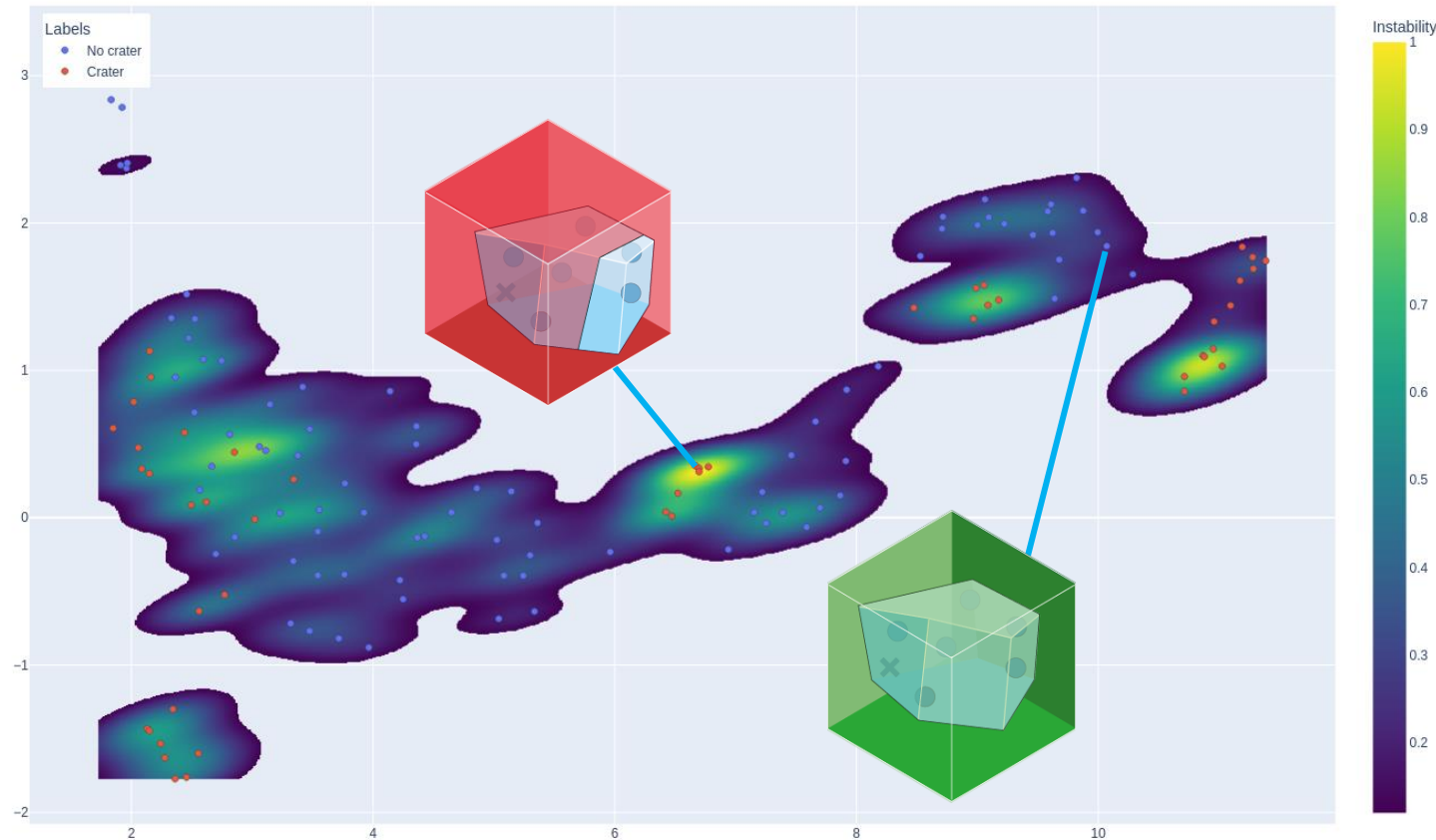
Based on ISO/IEC 24029-2



- (1) f represents the noise with its intensity (Δ)
- (2) All possible input neighbors obtained for the given noise
- (3) Mathematical object containing all possibilities

Robustness Map Visualization

UMAP Density Mapping of Model Representations by Delta max

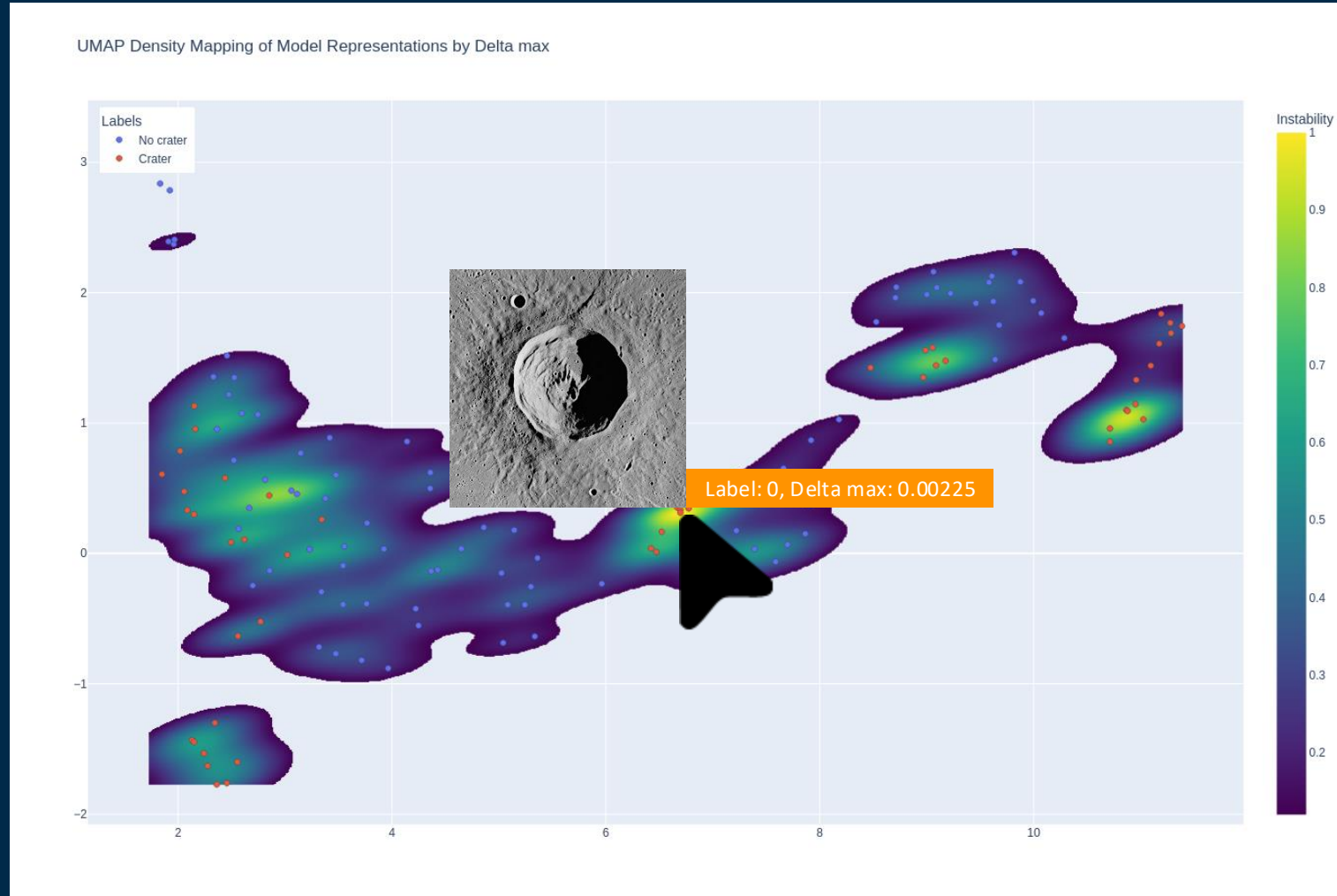


Feature

The robustness map visualization allows users to quickly identify robust and weak areas across the input domain for each data point from the validation dataset.

The more yellow a cluster is, the more unstable its data points; the more blue it is, the more stable they are.

Robustness Map Visualization

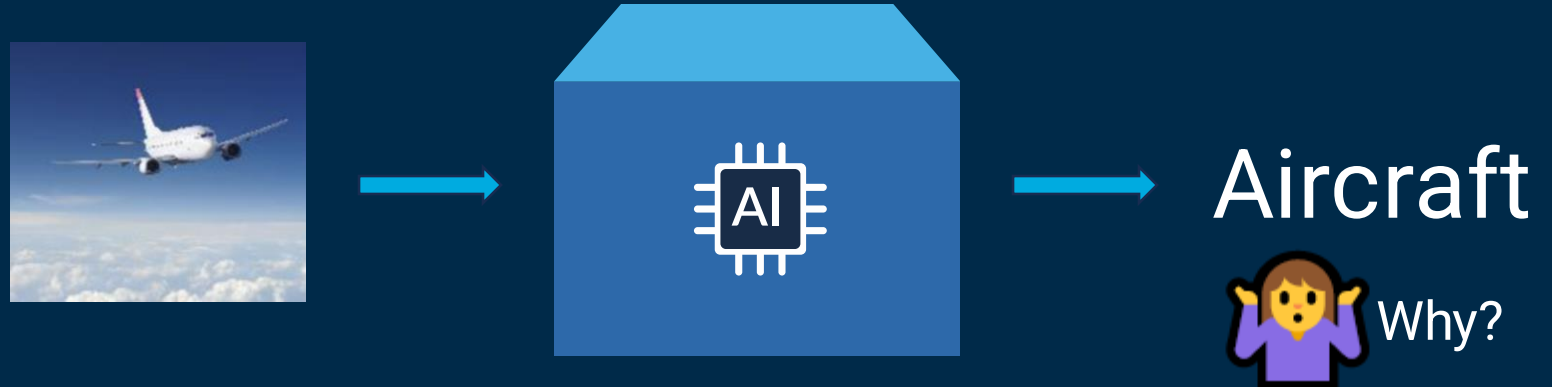


Feature

Get valuable insights to guide improvement efforts by inspecting each data point with relevant information

Explainability (XAI) Feature

Move from opaque decisions

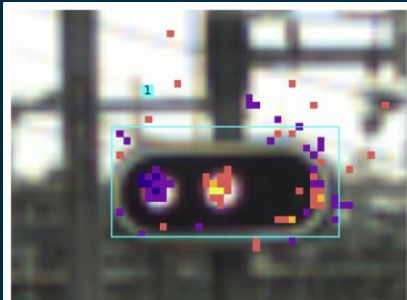


To explainable decisions

Saimple helps you validate your model decisions through human-understandable visualizations

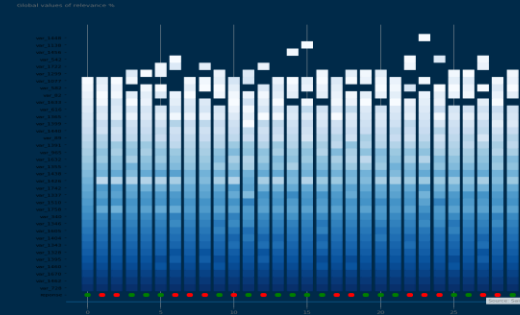


Applicability of our Technology



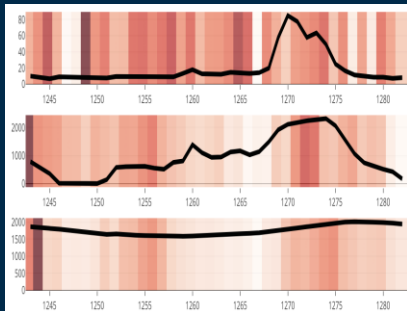
Computer vision

- Classification
- Detection
- Segmentation
- Industrial quality check



Tabular Data

- Scoring / Finance
- Pattern identification
- High level XAI



Time Series

- Predictive maintenance
- Anomaly detection
- Acoustic overwatch
- Medical diagnostic



NLP (on going R&D)

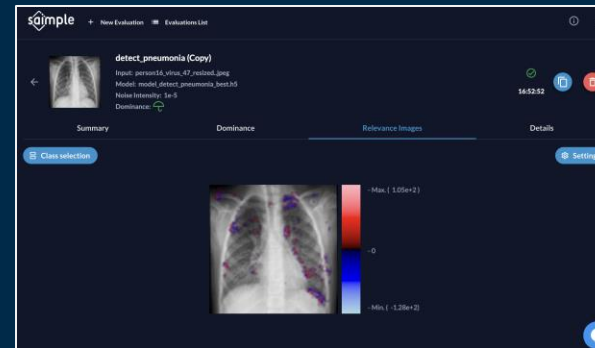
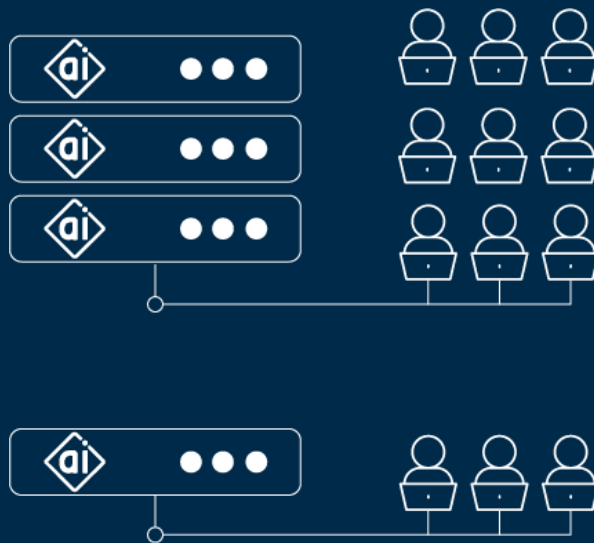
- Conversational AI
- Speech to text
- Report summary

Supported models

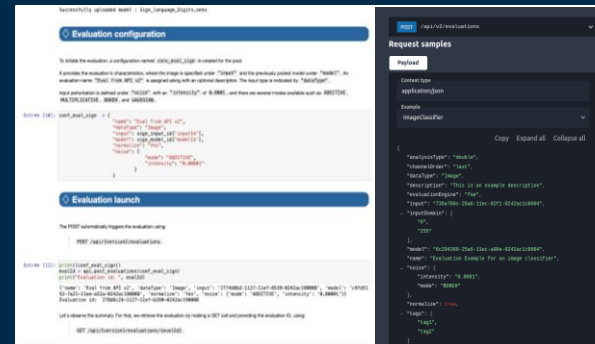
- Neural Networks (Convolutional, Recurrent, Residual, Detectors)
- Support Vector Machine, random forest, decision trees

A Versatile Solution

Highly scalable solution available on-premise or secured HPC SaaS

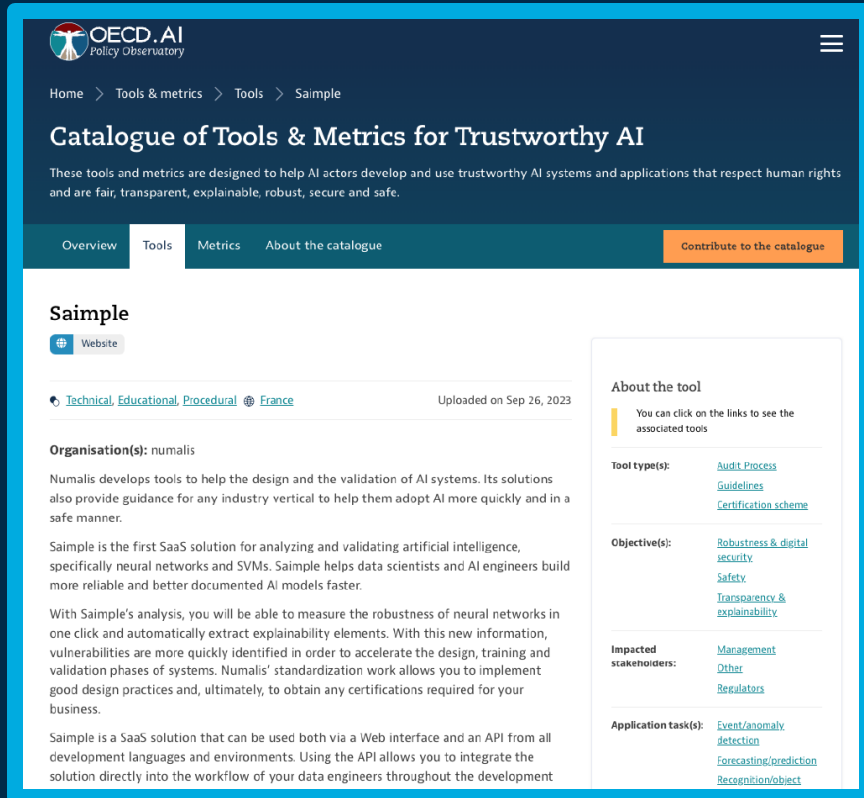


Comprehensive & easy to use GUI




Easy integration in any development environment with API and SDK

Proudly Featured On



The screenshot shows the OECD.AI Policy Observatory website. The header includes the OECD.AI logo and a navigation menu with 'Home', 'Tools & metrics', 'Tools', and 'Saimple'. The main heading is 'Catalogue of Tools & Metrics for Trustworthy AI'. Below this, a sub-header states: 'These tools and metrics are designed to help AI actors develop and use trustworthy AI systems and applications that respect human rights and are fair, transparent, explainable, robust, secure and safe.' The navigation bar includes 'Overview', 'Tools', 'Metrics', 'About the catalogue', and a 'Contribute to the catalogue' button. The 'Saimple' tool is highlighted, showing its 'Website' link, tags for 'Technical', 'Educational', 'Procedural', and 'France', and an upload date of 'Sep 26, 2023'. The 'About the tool' section describes Saimple as a SaaS solution for analyzing and validating artificial intelligence, specifically neural networks and SVMs. It mentions that Saimple helps data scientists and AI engineers build more reliable and better documented AI models faster. The 'Impacted stakeholders' section lists 'Management', 'Other', and 'Regulators'. The 'Application task(s)' section lists 'Event/anomaly detection', 'Forecasting/prediction', and 'Recognition/object'.

OECD.AI catalogue of trustworthy AI development tools



The screenshot shows the CONFIANCE.AI website. The header includes the CONFIANCE.AI logo and a navigation menu with 'Home', 'Tools & metrics', 'Tools', and 'Saimple'. The main heading is 'Catalogue of Tools & Metrics for Trustworthy AI'. Below this, a sub-header states: 'These tools and metrics are designed to help AI actors develop and use trustworthy AI systems and applications that respect human rights and are fair, transparent, explainable, robust, secure and safe.' The navigation bar includes 'Overview', 'Tools', 'Metrics', 'About the catalogue', and a 'Contribute to the catalogue' button. The 'Saimple' tool is highlighted, showing its 'Website' link, tags for 'Technical', 'Educational', 'Procedural', and 'France', and an upload date of 'Sep 26, 2023'. The 'About the tool' section describes Saimple as a SaaS solution for analyzing and validating artificial intelligence, specifically neural networks and SVMs. It mentions that Saimple helps data scientists and AI engineers build more reliable and better documented AI models faster. The 'Impacted stakeholders' section lists 'Management', 'Other', and 'Regulators'. The 'Application task(s)' section lists 'Event/anomaly detection', 'Forecasting/prediction', and 'Recognition/object'.

CONFIANCE.AI catalogue of trustworthy AI development tools

Thank you for your attention

+33 (0)4 67 15 10 78
contact@numalis.com