AI PROCESSES CERTIFICATION

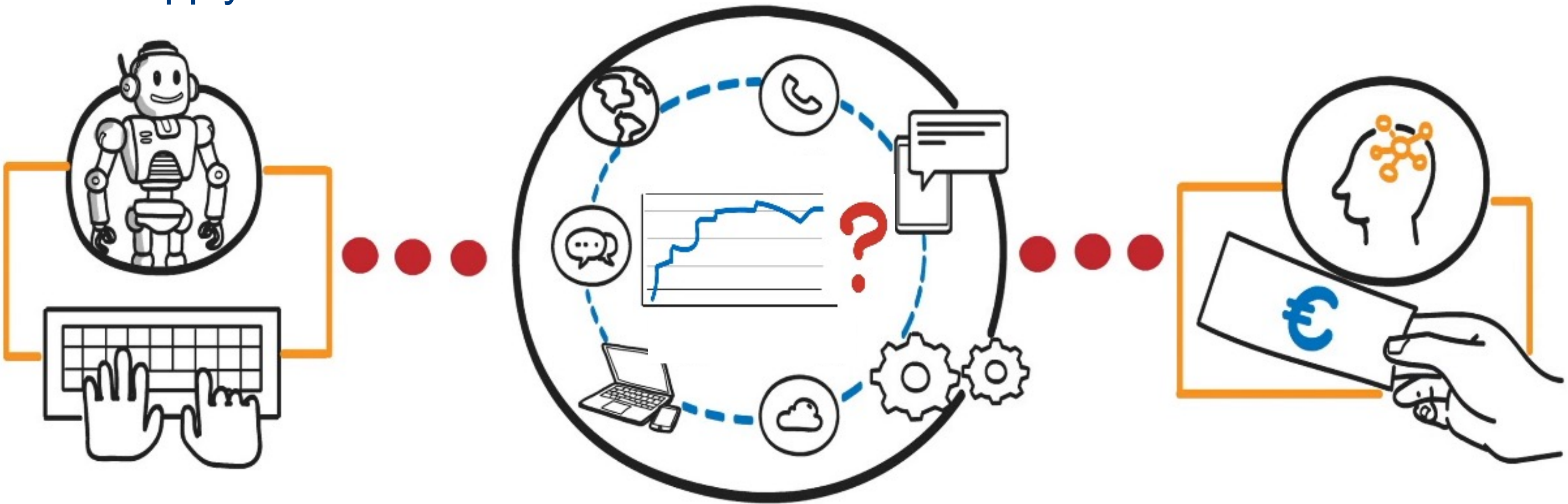
Dr Agnes DELABORDE
Evaluation of AI systems and cybersecurity – Head of department
LNE – French laboratory for metrology and testing
agnes.delaborde@lne.fr

LABORATOIRE
NATIONAL
DE MÉTROLOGIE
ET D'ESSAIS

MATCHING AI SUPPLY AND DEMAND

AI supply

AI demand



Black-box, non convex, evolutive systems

Need: AI evaluation & certification

Trustworthy and efficient functionalities

LNE'S ACTIVITIES IN AI EVALUATION

Activity n°1: development of **evaluation standards**

Activity n°2: AI systems **testing**

Activity n°3: certification of AI development and evaluation processes

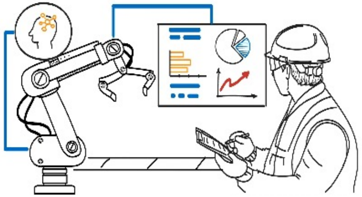
Activity n°4: development of **evaluation tools**

Activity n°5: professional training on AI evaluation

Application areas:

- **NLP:** speech-to-text, translation, speaker recognition, etc.
- **Image processing:** person recognition, object segmentation, OCR, etc.
- **Robotics:** Smart MD, industrial robots, inspection robots, autonomous cars, agricultural robots, etc.

- 10+ years of experience
- 15+ ongoing R&D projects
- 950+ systems evaluated
- 10+ experts on AI evaluation



POSSIBLE APPROACHES TO AI CERTIFICATION

Process certification:
The AI functionality has been properly constituted (evaluation of the learning, evaluation and maintenance phases)

➔ Create confidence in the AI developed based on process control

➔ Analogous approach to creating trust via processes (management system certifications, CE marking of medical devices, aerospace etc.)

Product certification:
The AI functionality has a compliant behavior (test of the functionality)

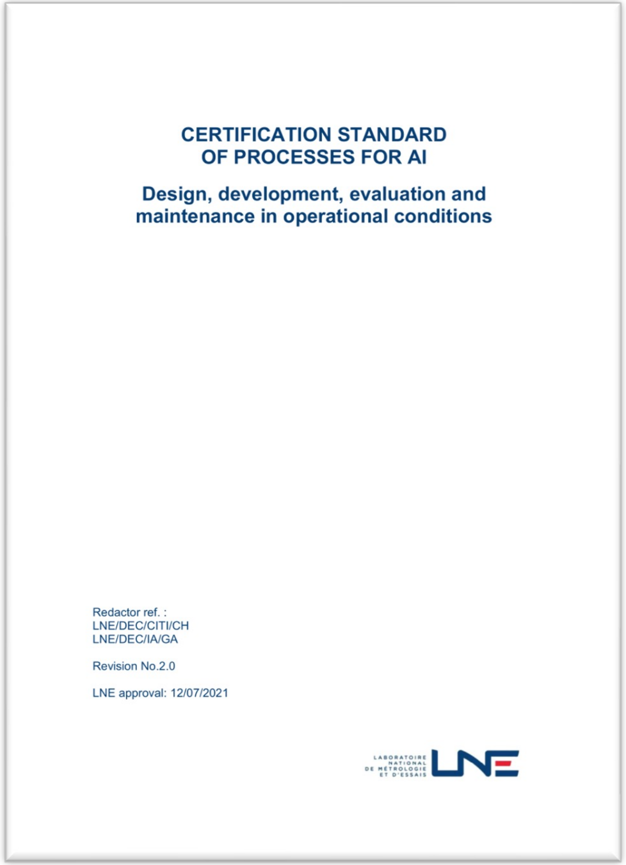
➔ Potential limitations to overcome (sectorial specificities, testing cost, test methods)

People certification:
Those involved in the development or use of AI throughout its life cycle are competent.

CERTIFICATION OF PROCESSES FOR AI

https://www.lne.fr/en/service/certification/certification-processes-ai

NUMÉRIQUE LNE CERTIFICATION



CERTIFICATION STANDARD
OF PROCESSES FOR AI

Design, development, evaluation and
maintenance in operational conditions

Redactor ref. :
LNE/DEC/CITI/CH
LNE/DEC/IA/GA

Revision No.2.0

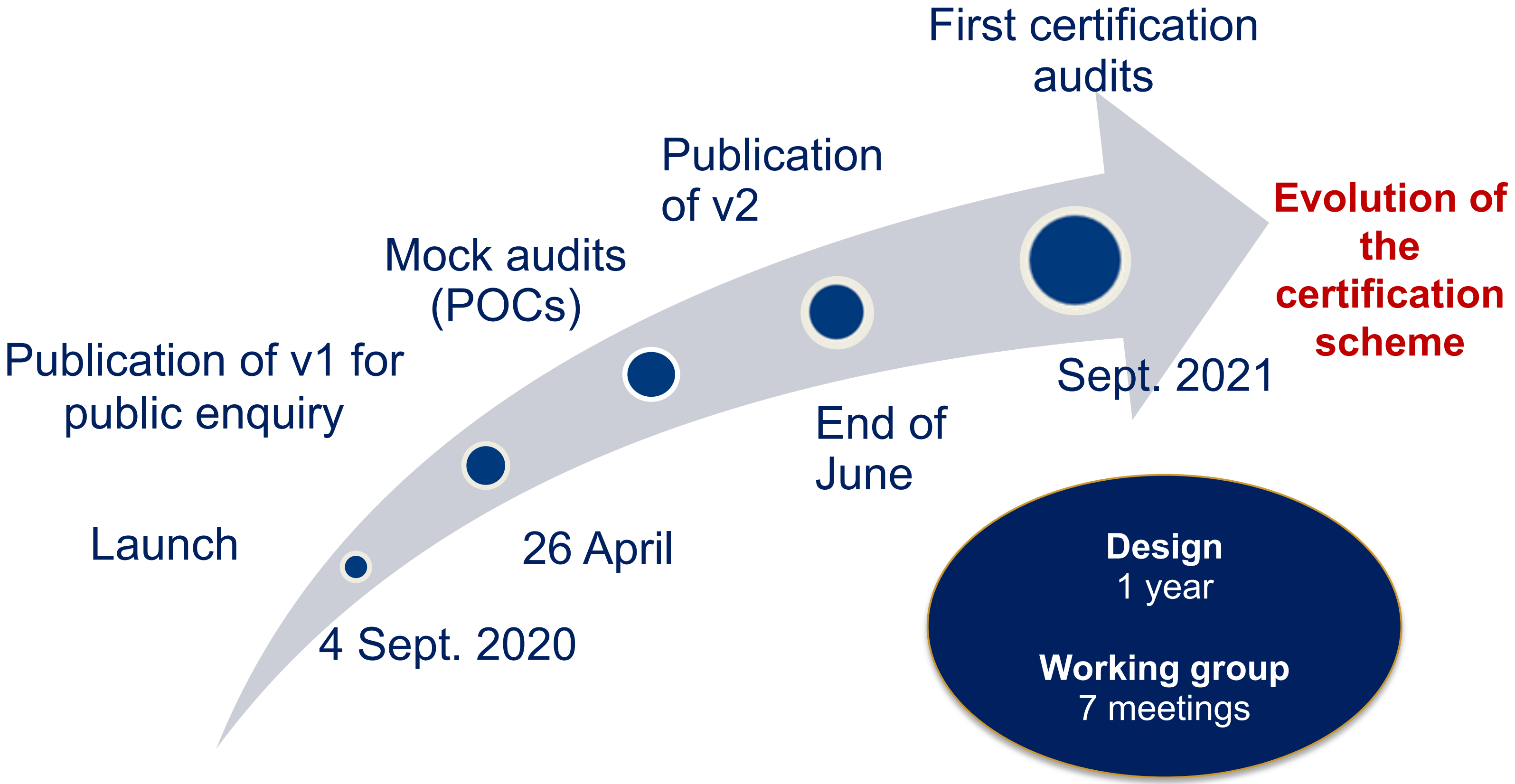
LNE approval: 12/07/2021

LABORATOIRE NATIONAL DE MÉTROLOGIE ET D'ESSAIS LNE

OVERVIEW OF THE CERTIFICATION

- Not meant to certify the AI product itself, but guarantee that it has been **designed correctly**.
- Contributes to ensuring a trustworthy product, through **control of the processes and use of good practice**.
- Voluntary certification.
- For Machine Learning (and hybrid ML/expert).
- Focus of the certification:
  - Design, development, evaluation and maintenance in operational conditions

AI PROCESS CERTIFICATION – CREATION



Launch

4 Sept. 2020

Publication of v1 for public enquiry

Mock audits (POCs)

26 April

Publication of v2

End of June

First certification audits

Sept. 2021

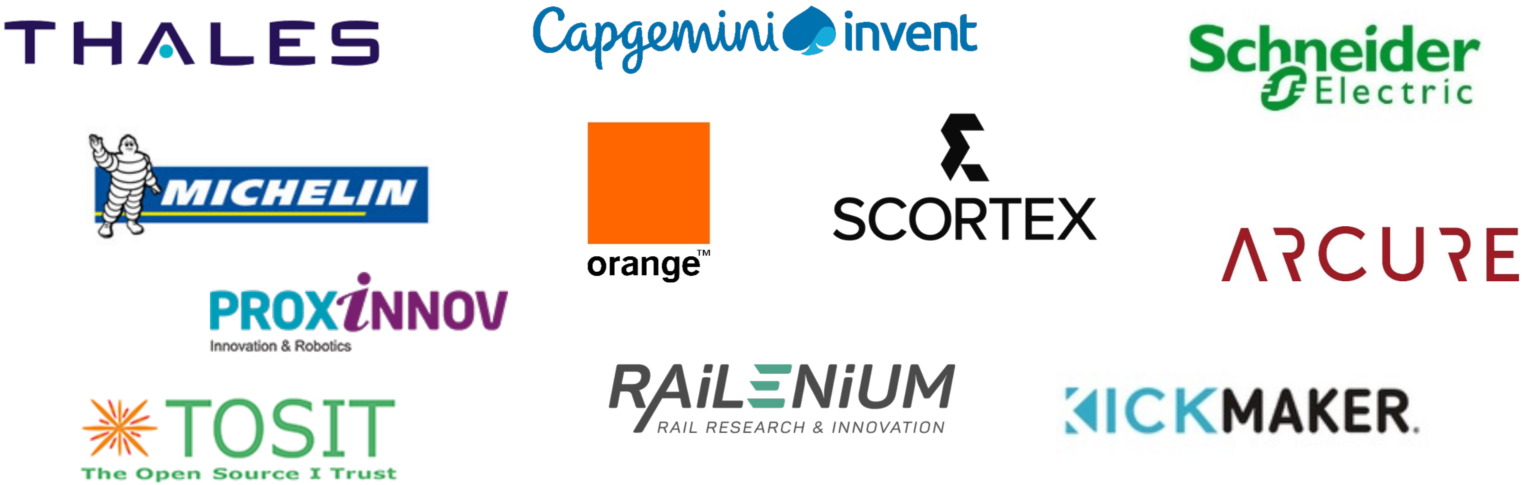
Evolution of the certification scheme

Design
1 year

Working group
7 meetings

WORKING GROUP

Composition: Large companies; SMEs; Consulting firms; Clusters



CERTIFICATION OF FOUR KEY PROCESSES

Design process

- Transform an expression of need into functional specifications

Development process

- Translate these specifications into an evaluation-ready version of the AI functionality

Evaluation process

- Verify the conformity of the system to the defined specifications before its deployment

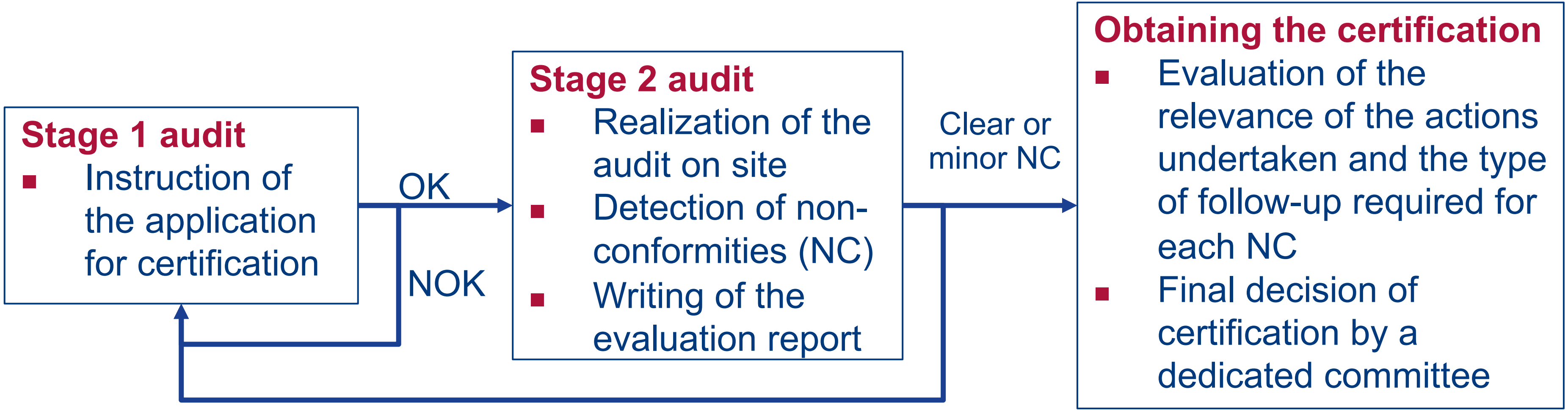
Maintenance process

- Ensure compliance of AI functionality with defined specifications after deployment and throughout its operational phase

HIGHLIGHTS OF THE CERTIFICATION SCHEME

- No imposed technical solutions, but objectives to be achieved (quality, control, monitoring)
- Documentation and justification are required
- Importance of informing those concerned
- Consideration of the wider ecosystem (customers, users, regulations, business constraints, internal organisation, etc.)
- Importance of a risk-based approach

OVERVIEW OF THE CERTIFICATION PROCESS



Stage 1 audit

- Instruction of the application for certification

OK

NOK

Stage 2 audit

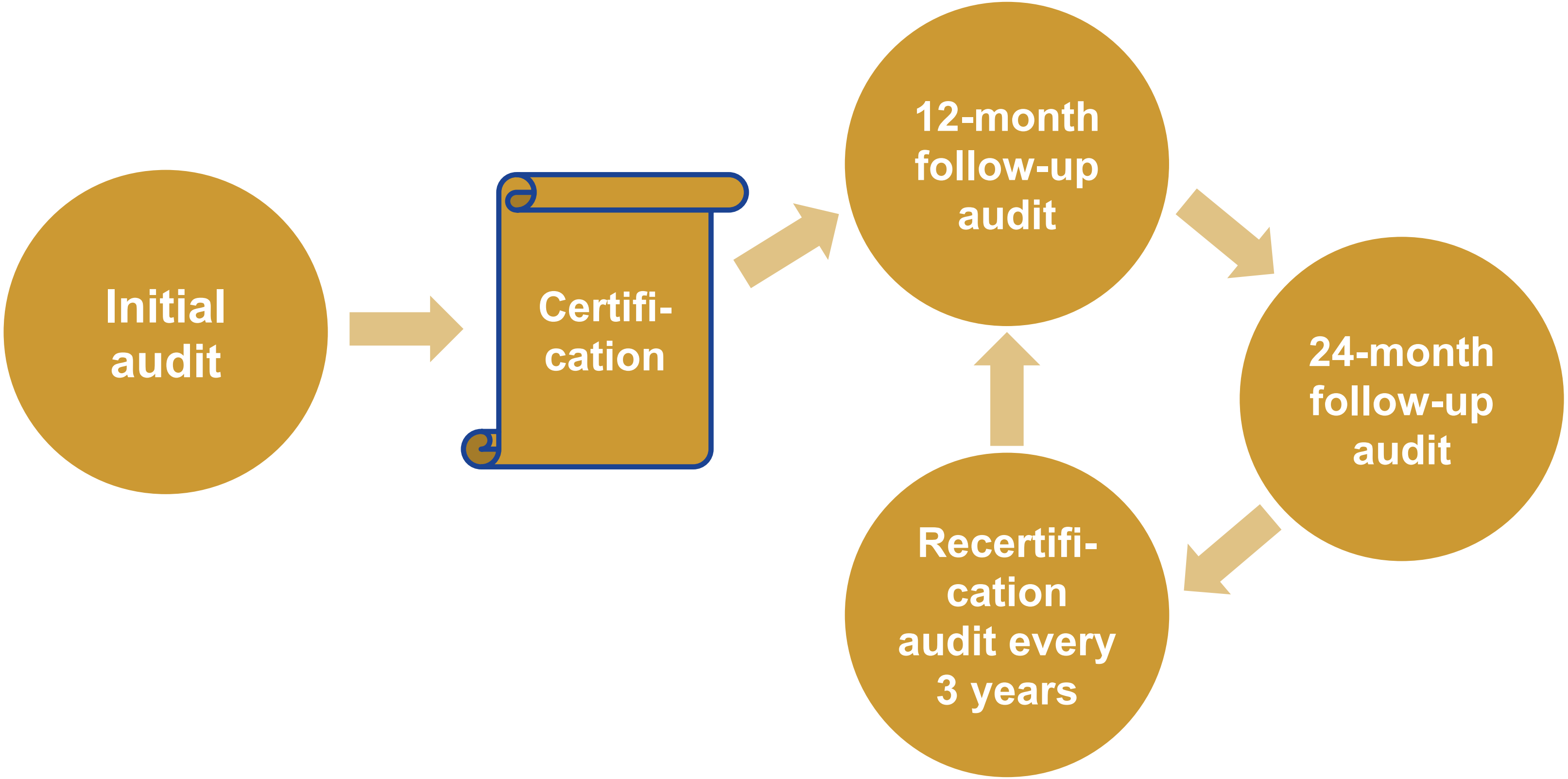
- Realization of the audit on site
- Detection of non-conformities (NC)
- Writing of the evaluation report

Clear or minor NC

Obtaining the certification

- Evaluation of the relevance of the actions undertaken and the type of follow-up required for each NC
- Final decision of certification by a dedicated committee

OVERVIEW OF THE CERTIFICATION PROCESS



Initial audit

Certification

12-month follow-up audit

24-month follow-up audit

Recertification audit every 3 years

KEY ELEMENTS (1/3)

Design process

- Documented and available specifications
- Acceptance criteria agreed with the customer
- Documented design hypotheses and evaluation approach
- Preliminary risk analysis

Development process

- Documentation: model type, required resources, deployment infrastructure, interfaces, intended operating domain, contraindications, non-indications, source-code and network architecture
- Data quality control (for learning and test sets): representativeness, uniqueness, sanity, annotation quality, independence, traceability and access rights, detection and management of missing and erroneous data
- Learning process control: control of over and underfitting, traceability and archiving of models and development tools, etc.

KEY ELEMENTS (2/3)

Evaluation process

- Documented evaluation protocol and metrics
- Identification of factors influencing performance and potential biases
- Evaluation of overfitting/underfitting; resilience; robustness
- Reproducibility of experiments and repeatability of performance measurements
- Separate development and evaluation roles
- Tests in real operating conditions ; validation of test environments
- Documented evaluation results
- Verification of regulatory requirements

Maintenance process

- Post-deployment learning process control
- Communication with end users (information and customer feedback)

KEY ELEMENTS (3/3)

All processes

- Document process inputs and outputs
- Determine the resources needed to keep these processes running smoothly of these processes
- Consider the risks identified with the use of AI functionality (revision, update)
- Evaluate the processes

RESPONDING TO A NEED FOR TRANSPARENCY

Product sheet

Communicate the information essential to making an informed choice about AI functionality:

- Intended use
- Operating domain (and limitations)
- Performance
- Integration possibilities (open-source, processing to be done, etc.)
- Maintenance
- Communication methods between the developer and the customer
- Risk analysis

Thank you for your attention