



COMMUNIQUÉ DE PRESSE

Paris, le 7 mars 2024

Confiance.ai Day

Confiance.ai dévoile sa méthodologie outillée, un "bien commun numérique" au service du développement d'une IA industrielle et responsable

Ce "bien commun numérique" est désormais ouvert aux communautés scientifiques et industrielles. Il se compose d'une méthodologie de bout en bout bâtie sur de nombreux composants technologiques open source. Il vise à maintenir le leadership technologique des entreprises françaises en favorisant la conception d'applications industrielles critiques intégrant des composants d'IA de confiance, en toute sécurité. Il contribuera ainsi à renforcer la compétitivité des acteurs économiques nationaux sur la chaîne de valeur de l'IA industrielle et responsable. Confiance.ai annonce également un projet de fondation pour en assurer à terme la diffusion et la pérennisation.

A l'occasion de l'événement [Confiance.ai Day](#) qui se tient ce 7 mars 2024, les membres fondateurs du collectif [Confiance.ai](#) (Air Liquide, Airbus, Atos, Naval Group, Renault Group, Safran, Sopra Steria, Thales, Valeo, le CEA, Inria, l'IRT Saint Exupéry et l'IRT SystemX) ont dévoilé la méthodologie et le catalogue de composants technologiques développés ces trois dernières années pour augmenter le niveau de confiance dans l'IA intégrée aux systèmes critiques. Conçue comme un véritable guide de bout en bout à destination des industriels, cette méthodologie outillée permet de caractériser et qualifier la confiance d'un système intelligent dirigé par les données et de l'intégrer dans leurs produits et services industriels. Elle est applicable à tout secteur d'activité.

Lancé en 2021, ce programme structurant de la Stratégie nationale pour l'intelligence artificielle financé par France 2030 a été précurseur au niveau mondial. Né de l'ambition de faire de la France un des pays leaders de l'IA industrielle et responsable en développant un environnement méthodologique et technologique souverain, ouvert, interopérable et pérenne, il favorise l'intégration d'une IA industrielle (explicable, robuste, etc.) et responsable (de confiance, éthique, etc.) dans les secteurs industriels stratégiques. Il a suscité une véritable dynamique et permis de fédérer, notamment par le biais de plusieurs appels à manifestation d'intérêt (AMI), un riche écosystème composé de près d'une cinquantaine de partenaires (laboratoires et instituts de recherche, startups, et grands groupes). Enfin, le programme prend une part active dans la préparation à l'implémentation de l'AI Act au sein des filières industrielles françaises et européennes, en lien avec les organismes spécifiques à chacune.

« France 2030 a investi dans Confiance.ai en 2021 dans l'objectif de traduire l'excellence de notre recherche en IA en capacité de leadership industriel. Les résultats sont prégnants : les projets de R&D qui en résultent nous permettent de bâtir dans les meilleures circonstances nos stratégies industrielles mais aussi de restaurer un climat de confiance et d'acceptabilité autour d'une technologie structurante pour notre économie de demain », déclare Bruno Bonnell, secrétaire général pour l'investissement, en charge de France 2030.

Confiance.ai en chiffres :

25 partenaires industriels (10 grands groupes dont 9 fondateurs, 15 start-up)

17 partenaires académiques dont 4 fondateurs
4 collaborations internationales

Près de 120 documents publiés et plus de 60 composants logiciels évalués et mis à disposition (dont près de 30 développés dans le cadre du programme)

Fin du programme en septembre 2024



Se projetant dans une dynamique à horizon 2030, les acteurs du programme s'organisent déjà pour maintenir leur leadership dans le domaine de l'IA industrielle et responsable, en définissant les prochains verrous technologiques prioritaires à lever et en assurant la diffusion, l'évolution, la pérennisation et l'utilisation de la méthodologie outillée à travers un projet de création de fondation.

L'ouverture de la méthodologie outillée à la communauté

L'une des grandes réussites des acteurs du programme est d'être parvenus à **transversaliser les approches entre industries**. La méthodologie outillée de bout en bout mise au point permet de traiter les mêmes problématiques technologiques, quel que soit le contexte d'application et l'industrie visés.

A l'occasion de Confiance.ai Day, les partenaires annoncent l'ouverture aux communautés scientifiques et industrielles de la méthodologie mise au point ainsi que des composants open source associés. Ces actifs sont accessibles sur <https://bok.confiance.ai/>.

Les composants ont été regroupés en neuf ensembles fonctionnels correspondant à des processus d'ingénierie bien précis : ingénierie de bout en bout, gestion du cycle de vie de la donnée, gestion du cycle de vie des modèles et des composants, évaluation des composants d'IA, déploiement des composants IA, gestion des systèmes d'IA en opération, robustesse, explicabilité et quantification de l'incertitude.

Par sa large adoption, les partenaires du programme ambitionnent de faire de la méthodologie outillée un standard *de facto* au niveau mondial.

Un impact industriel majeur : une démarche de transition vers une ingénierie augmentée permettant l'intégration d'une IA de confiance

Au terme de trois années de travaux, le programme a permis aux industriels partenaires des domaines de l'automobile, de l'aéronautique, de l'énergie, de la défense ou encore de l'industrie de revisiter leurs ingénieries de manière à prendre en compte en particulier l'IA dirigée par les données et a permis de progresser dans le déploiement de fonctions d'IA dans leurs systèmes critiques.

Quelques exemples de résultats sur des cas d'usage industriels :

L'applicabilité de la méthodologie outillée de bout en bout a pu être testée sur des cas d'usage apportés par les partenaires du programme et directement au sein de leurs ingénieries :

Air Liquide

Air Liquide s'est appuyé sur les approches d'IA générative pour améliorer la robustesse et la fiabilité de fonctionnement de ses modèles de comptage automatique de bouteilles utilisés pour la gestion de son inventaire, dans des conditions météorologiques défavorables (ex : pluie, neige). **Elle a notamment permis de réduire de moitié l'erreur de comptage de nuit, pour arriver à des performances de précision supérieures à 98 %**. Grâce à un prétraitement des données consistant à éliminer les gouttes de pluie et les flocons de neige, à la transformation des images de nuit en jour, le système a pu traiter, sans entraînement supplémentaire, ces données comme en condition normale d'apprentissage. Une meilleure maîtrise de nouvelles données (étude, visualisation, caractérisation) et la complétion de la base de scénarios d'entraînement sont à l'origine de ces performances.

Thales

Conscient de la nécessité de revisiter les ingénieries classiques (ingénierie algorithmique, ingénierie logicielle et ingénierie système) au regard des exigences posées par leur intégration dans des systèmes critiques, **Thales s'est fortement impliqué dans la définition de la méthodologie d'ingénierie de bout en bout, approche rigoureuse et**



interdisciplinaire, compatible avec les usages métier, permettant de garantir un déploiement et un maintien en condition opérationnelle « safe & secure », de par la conception et la validation de ces systèmes.

Cette approche va permettre une plus grande fluidité sur l'ensemble de la chaîne d'ingénierie d'un système critique doté d'IA. Par exemple, dans le cadre de son cas d'usage sur la « détection d'objets d'intérêts à partir d'images aériennes », Thales a pu vérifier la correction de ses algorithmes, améliorer la qualité des données d'apprentissage par un enrichissement avec des images synthétiques, caractériser, évaluer et monitorer les performances grâce aux attributs et scores de confiance proposés par la méthodologie de bout en bout. Ces premières étapes sont nécessaires pour un déploiement industriel d'un composant doté d'une capacité d'apprentissage dans un système critique.

Renault Group

Renault Group a soumis au programme Confiance.ai le cas d'usage « Welding » qui porte sur la vérification par un système d'IA de la qualité des soudures sur le châssis d'un véhicule. La faisabilité en avait été démontrée avant le début du projet mais les responsables qualité de l'usine hésitaient à la déployer sur des postes où le contrôle est aujourd'hui effectué par un opérateur, en particulier sur des soudures critiques. **Les méthodes et outils du programme Confiance.ai s'appliquaient donc parfaitement à ce cas d'usage qui a été très largement traité par les partenaires du programme, avec des composants pour évaluer en particulier la robustesse de l'IA, son explicabilité et des fonctions de monitoring notamment.** Ce cas d'usage a été le premier sur lequel une évaluation de bout en bout de la méthode a été effectuée. Les outils et méthodes proposées par Confiance.ai arrivent à point nommé pour accompagner le programme AI@Scale de Renault Group, qui déploie une organisation, des ressources humaines, matérielles, logicielles et méthodologiques pour accélérer et sécuriser le passage à l'échelle de l'IA dans toute la chaîne de valeur du groupe.

Confiance.ai, moteur du développement de l'écosystème mondial de l'IA de confiance

Précurseur dans le domaine de l'IA de confiance, le collectif Confiance.ai est **moteur dans la construction et l'animation d'un écosystème au niveau mondial.** Cela se traduit par :

- la signature de MoU (Memorandum of Understanding) :
 - o **Au Québec (Canada)**, avec le programme [Confiance IA](#) en 2024 qui fédère des acteurs privés et publics afin de supporter les industriels dans leurs besoins d'industrialisation et d'adoption d'une intelligence artificielle robuste, sécurisée, durable, responsable et éthique. Autour de cas d'usage génériques, les entreprises de secteurs d'activité différents peuvent ainsi codévelopper des outils pré-compétitifs et des méthodes qui qualifieront, voire quantifieront, les propriétés de confiance de l'IA générée. Ce programme collabore depuis plus d'un an avec son homologue français Confiance.ai. Cette coopération devrait s'amplifier dans les mois à venir grâce au partage de cas d'usage, de méthodes et d'outils. Le CRIM (Centre de Recherche en Informatique de Montréal) est fiduciaire du programme Confiance IA.
 - o **En Allemagne**, avec [VDE](#) en 2022, l'une des plus importantes organisations technologiques d'Europe pour créer le futur label franco-allemand de l'IA responsable.
- ou la création de liens privilégiés avec des initiatives *ad hoc* dans le reste du monde :
 - o **En Australie**, avec l'initiative « Opérationnalisation de l'IA responsable » ([CSIRO](#)) de Data61 dont l'ambition est de développer des technologies et des outils innovants d'ingénierie logicielle/système reposant sur une approche basée sur les risques que les experts en IA, les développeurs de systèmes et d'autres parties prenantes peuvent utiliser pour rendre les systèmes d'IA et leurs processus de développement dignes de confiance.
 - o **En Allemagne**, avec le projet [ZERTIFIZIERTE KI](#), dirigé conjointement par le [Fraunhofer IAIS](#), l'[Institut allemand de normalisation \(DIN\)](#) et l'[Office fédéral allemand de la sécurité de l'information \(BSI\)](#). Ce dernier vise à développer des procédures de test pour l'évaluation des systèmes d'intelligence artificielle. Ainsi qu'avec [CERTAIN](#), une initiative collaborative du [DFKI \(Deutsches Forschungszentrum für Kunstliche Intelligenz / Centre de recherche allemand pour l'intelligence artificielle\)](#) impliquant divers partenaires, axée sur la recherche, le développement, la normalisation



et la promotion de techniques d'IA de confiance, pour fournir des garanties et une certification des systèmes d'IA.

Enfin, moteur dans la proposition de normes sur les risques de l'AI Act, **Confiance.ai contribue à apporter, avec sa méthodologie outillée, l'une des réponses à sa mise en œuvre opérationnelle.** Les exigences de cette réglementation se concentrent principalement sur les systèmes à haut risque et à risque systémique, et portent sur divers aspects de la confiance (robustesse, explicabilité, maintien du contrôle par les humains, transparence, absence de biais, etc.). Les travaux de Confiance.ai fournissent des éléments concrets au service de ces objectifs : taxonomies, méthodologies, technologies et outils.

« Nous nous sommes attaqués à une problématique particulièrement complexe et ambitieuse. Les résultats obtenus sont en ligne avec nos objectifs et remarquables à plusieurs égards. Tout d'abord, sur le plan humain, nous sommes parvenus à faire collaborer un écosystème hybride composé d'industriels, de scientifiques, de data scientists, d'ingénieurs, etc. Nous avons également relevé un grand nombre de défis scientifiques et technologiques – plus que nous l'avions imaginé - et nous avons été moteur dans de nombreuses d'initiatives au niveau international. Une véritable communauté mondiale autour de l'IA de confiance est en train d'émerger », explique Juliette Mattioli, Présidente du comité de pilotage de Confiance.ai et Expert sénior en Intelligence Artificielle chez Thales.

"Il reste encore de nombreux défis scientifiques et technologiques à relever pour que la France maintienne son avance dans le domaine et nous sommes en train de les répertorier. Les sujets du transfert et de la valorisation de nos travaux sont des chantiers prioritaires, tout comme la résolution de nouveaux verrous scientifiques et technologiques", ajoute Fabien Mangeant, Président du comité de direction de Confiance.ai et Directeur Scientifique Digital d'Air Liquide.

Vision et perspectives à l'horizon 2030

Alors que leurs travaux s'achèveront fin 2024, les partenaires du programme travaillent également au sujet de **l'après Confiance.ai**. Leurs ambitions s'articulent autour de trois axes : approfondir, pérenniser et industrialiser.

En tout premier lieu, du fait des avancées toujours plus nombreuses dans le domaine de l'IA, de nouveaux verrous continuent à émerger. Les partenaires du programme identifient actuellement plusieurs problématiques sur lesquelles il serait intéressant de **lancer des projets de R&T : IA hybride, IA génératives (ex : LLM), cybersécurité des IA intégrées aux systèmes critiques, etc.** Ces nouveaux projets R&T pourront venir enrichir les méthodes outillées sur de nouveaux champs d'application.

Un autre objectif poursuivi est **la pérennisation et diffusion de la méthodologie outillée.** La première étape est son ouverture, mais plus largement, le lancement d'une **initiative de fondation** pour fédérer un ensemble d'acteurs à l'échelle internationale autour d'une feuille de route commune. Par le biais de cette fondation, les acteurs contribueront à maintenir ce « bien commun numérique » en conditions opérationnelles, à le faire gagner en maturité via les retours et propositions d'améliorations. La formation, à travers le Mastère Spécialisé sur l'IA de Confiance co-conçu avec CentraleSupélec, sera un autre levier permettant cette montée en maturité.

Enfin, la troisième ambition poursuivie est **l'industrialisation des résultats du programme** pour aider leur montée en maturité en vue de les rendre utilisables à grande échelle par les ingénieries des industriels. L'ambition visée à travers cette démarche est la création et la mise à disposition d'outils de compétitivité tenant compte des spécificités propres à chaque entreprise en matière de typologie, de données et de cas d'usage.

« Le développement de l'IA ouvre des perspectives extraordinaires pour notre société. De la médecine personnalisée aux transports intelligents, en passant par la lutte contre le changement climatique, l'IA a le potentiel de révolutionner de nombreux aspects de notre vie. Cette révolution ne peut cependant se faire sans confiance. Cette dernière conditionne l'acceptabilité de l'IA par la société et l'adoption des systèmes intelligents par nos citoyens, entreprises et administrations. Les préoccupations publiques grandissantes quant aux risques associés aux modèles d'IA les plus avancés, ainsi que la multiplication des initiatives sur la gouvernance internationale de l'IA, renforcent cette urgence. Le programme



Confiance.ai est ainsi une initiative essentielle de la Stratégie nationale pour l'IA. Il permet à nos industriels de développer de manière sûre des systèmes intelligents et surtout, il prépare l'ensemble des filières industrielles françaises à l'entrée en vigueur de l'AI ACT », commente Guillaume Avrin, Coordonnateur national pour l'intelligence artificielle.

A propos de Confiance.ai

Porté par un collectif de 13 partenaires fondateurs, acteurs industriels et académiques français majeurs*, Confiance.ai est l'un des programmes structurants sur lesquels s'appuie le second volet de la Stratégie nationale pour l'IA, annoncé en octobre 2021. Ce programme est financé à hauteur de 30M€ par France 2030. Lancé en janvier 2021 pour une durée de 4 ans, ce programme ambitionne de créer une plateforme souveraine, ouverte, interopérable et pérenne d'outils logiciels pour favoriser l'intégration de l'intelligence artificielle dans les produits et services critiques. Il fédère aujourd'hui près de cinquante partenaires industriels et académiques sur Saclay et Toulouse autour de 7 projets de R&D.

En outre, il contribue à la mise en œuvre par les industriels du futur règlement européen « AI Act » de la Commission Européenne.

Plus d'informations sur : <https://www.confiance.ai/>

* Air Liquide, Airbus, Atos, CEA, Inria, Naval Group, Renault Group, Safran, IRT Saint Exupéry, Sopra Steria, IRT SystemX, Thales, Valeo

A propos de France 2030

Le plan d'investissement France 2030 :

- ✓ **Traduit une double ambition** : transformer durablement des secteurs clefs de notre économie (santé, énergie, automobile, aéronautique ou encore espace) par l'innovation technologique, et positionner la France non pas seulement en acteur, mais bien en leader du monde de demain. De la recherche fondamentale, à l'émergence d'une idée jusqu'à la production d'un produit ou service nouveau, France 2030 soutient tout le cycle de vie de l'innovation jusqu'à son industrialisation.
- ✓ **Est inédit par son ampleur** : 54 Md€ seront investis pour que nos entreprises, nos universités, nos organismes de recherche, réussissent pleinement leurs transitions dans ces filières stratégiques. L'enjeu : leur permettre de répondre de manière compétitive aux défis écologiques et d'attractivité du monde qui vient, et faire émerger les futurs leaders de nos filières d'excellence. France 2030 est défini par deux objectifs transversaux consistant à consacrer 50 % de ses dépenses à la décarbonation de l'économie, et 50% à des acteurs émergents, porteurs d'innovation sans dépenses défavorables à l'environnement (au sens du principe *Do No Significant Harm*).
- ✓ **Sera mis en œuvre collectivement** : pensé et déployé en concertation avec les acteurs économiques, académiques, locaux et européens pour en déterminer les orientations stratégiques et les actions phares. Les porteurs de projets sont invités à déposer leur dossier via des procédures ouvertes, exigeantes et sélectives pour bénéficier de l'accompagnement de l'Etat.
- ✓ **Est piloté par le Secrétariat général pour l'investissement** pour le compte du Premier ministre et mis en œuvre par l'Agence de la transition écologique (ADEME), l'Agence nationale de la recherche (ANR), Bpifrance, et la Caisse des Dépôts et Consignations (CDC).

Plus d'informations sur : france2030.gouv.fr | [@SGPI_avenir](https://twitter.com/SGPI_avenir)

Relations médias Confiance.ai

Marion Molina

Tél : 06 29 11 52 08

marionmolinapro@gmail.com

Secrétariat général pour l'investissement

Tél : 01 42 75 64 58

presse.sgpi@pm.gouv.fr