

IA embarquée de confiance

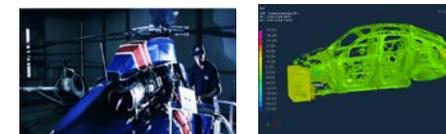
François Terrier (CEA/INSTN)



« L'IA offre de nouvelles opportunités d'enrichissement des systèmes embarqués si on arrive à en maîtriser finement l'intégration dans les environnements embarqués à la fois en termes de performance et de qualité. »

Le cours est organisé en un ensemble de séminaires associés à des TP quand des technologies accessibles le permettent.

- **Enjeux de la confiance pour les IA embarquées** : Panorama des questionnements et des acteurs.
- **Embarqué (Cours + TP)** :
 - Optimisation de l'implantation de réseaux de neurone (Cours+TP)
 - Micro-contrôleurs et architectures dédiées
- **Méthode pour la confiance (Cours + TP)** :
 - Analyse de risque et cadres de certification pour les applications critiques (Cours)
 - Validation formelle du fonctionnement de réseaux de neurones
 - Attaque et robustesse des réseaux de neurones
- **Algorithmie, modélisation avancée (Séminaires)** :
 - Compréhension et modélisation des réseaux de neurones (Séminaire)
 - Interprétabilité et explicabilité des intelligences artificielles (Séminaires)



F. Terrier



O. Bichler



M. Adedjouma



Z. Chihani



A. Mayoue



F. Espinoza Castellon



M. Tamaazousti

P. Blanchart

15h cours - 9h TP

IA embarquée de confiance

Objectif du module : sensibiliser aux enjeux, techniques du domaine

Approche : balayer un ensemble de sujets clés avec un expert du sujet

- Deux formats : cours/séminaire et TD/TP
 - Exploration des concepts via des TD/TP à chaque fois que possible
- Contact : responsable du module, francois.terrier@cea.fr
- Cours spécialisé : voir avec chaque intervenant <prénom.nom@cea.fr>
- Contrôle :
 - Contrôle continu : investissement dans les TPs (présence, participation active et résultat)
 - Examen final étude d'article en lien avec les cours → les articles seront diffusés en janvier
 - Rendu d'un résumé critique 1-2 pages max 15 jours avant l'examen final
 - Présentation de l'analyse critique à l'oral, avec des slides, 10' (5-6 slides : sujet, positionnement, atouts, limites, conclusion)
 - Positionner vis-à-vis de l'état de l'art (chercher d'autres articles, liens avec le cours, etc.)

Détail de l'emploi du temps prévu

Date	Horaire	Type	Sujet	Intervenant
9/12	9h00-10h25	Cours	Introduction (1/1) - Enjeux de la confiance pour les IA embarquées.	François Terrier
	10h35-12h00	Cours	Embarqué (1/4) - Optimisation de l'implantation de réseaux de neurone	Olivier Bichler
16/12	9h00-10h25	Cours	Embarqué (2/4) - Micro-contrôleurs et architectures dédiées	Olivier Bichler
	10h35-12h00	Cours	Méthodes pour la confiance - Compréhension et modélisation des réseaux de neurones	Mohamed Tamaazousti
6/1	9h00-12h00	TP	Embarqué (3&4/4) - Optimisation de l'implantation de réseaux de neurone avec N2D2	Olivier Bichler
13/1	9h00-12h00	Cours	Validation et certification (1&2/5) - Validation formelle du fonctionnement de réseaux de neurones	Zakaria Chihani
20/1	9h00-12h00	Cours	Validation et certification - Analyse de risque et cadres de certification pour les applications critiques	Morayo Adedjouma
27/1	9h00-12h00	TP	Validation et certification (3&4/5) - Validation formelle du fonctionnement de réseaux de neurones	Julien Girard
3/2	9h00-12h00	Cours	Méthodes pour la confiance (1&2/4) - Attaque et robustesse des réseaux de neurones	Aurélien Mayoué
10/2	9h00-12h00	TP	Méthodes pour la confiance (3&4/4) - Attaque et robustesse des réseaux de neurones	Fabiola Espinoza Castellon
17/2	9h00-10h25	Cours	Méthode pour la confiance (5/5) - Interprétabilité des réseaux de neurones	Zakaria Chihani
	10h35-12h00	Cours	Méthodes pour la confiance - Explicabilité des intelligences artificielles	Pierre Blanchart
24/2	9h00-12h00	Examen	Examen : rendu sur les études d'article ==> distribués début janvier (2 ou 3 de tous les intervenants)	F. Terrier + resp sujets