Executive Certificate Architecte Cloud Industriel et Technologique

université PARIS-SACLAY

Maîtrisez les systèmes d'information industriels et devenez un expert en architecture cloud

Code EC : AC25

Le cloud industriel et technologique révolutionne la gestion des systèmes d'information en offrant des solutions flexibles, évolutives et sécurisées. Un architecte cloud conçoit, implémente et optimise des infrastructures cloud adaptées aux besoins industriels, garantissant efficacité et innovation. Cette formation vous offre les compétences nécessaires pour piloter la transformation numérique des entreprises et maîtriser les environnements cloud complexes.

11 jours - 77 heures - Présentiel

Prix : 6900 €*
Prix pour les particuliers : **4890 €***
* Inclus petit déjeuner et déjeuner 25 € par jour

Adresse : Université Paris-Saclay, 9 Rue Joliot Curie, 91190 Gif-sur-Yvette

3 sessions au choix :

Session 1 : 2-3 Avril, 7-10 avril, 12-13-14 Mai, 15-16 Mai

Session 2 : 16-17 Juin, 23-26 Juin, 30 Juin-1-2 Juillet, 3-4 Juillet

Session 3 : 2-3 Octobre, 7-10 Octobre, 14-15-16 Octobre, 22-23 Octobre

Objectifs :

- Comprendre les principes de l'architecture des systèmes d'information et leur application dans les processus industriels
- Maîtriser la modélisation et l'optimisation des processus industriels
- Appliquer les meilleures pratiques en matière de sécurité et de gestion des risques pour les systèmes d'information industriels

Prérequis

Connaissances de base en systèmes d'information et en informatique

Public concerné

Professionnels de l'informatique, ingénieurs système, responsables IT, consultants en transformation numérique

Compétences acquises

Concevoir, implémenter et gérer des architectures cloud industrielles sécurisées et optimisées, tout en intégrant les meilleures pratiques de sécurité et de conformité

Référent pédagogique

Edy Hourany
Ingénieur logiciel senior DOCTOLIB

Formateurs

Nadim Henoud
Ingénieur logiciel et cybersécurité POTECH

Yacine Ladjici
Responsable de la cybersécurité du groupe VALEO POWER

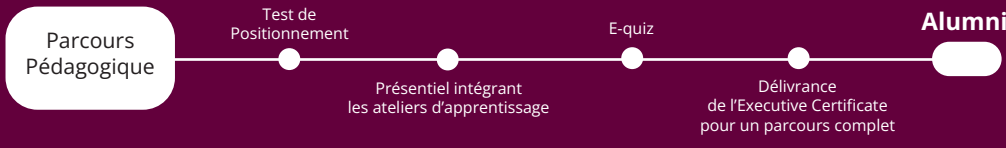
L'Executive Certificate Architecte Cloud Industriel et Technologique

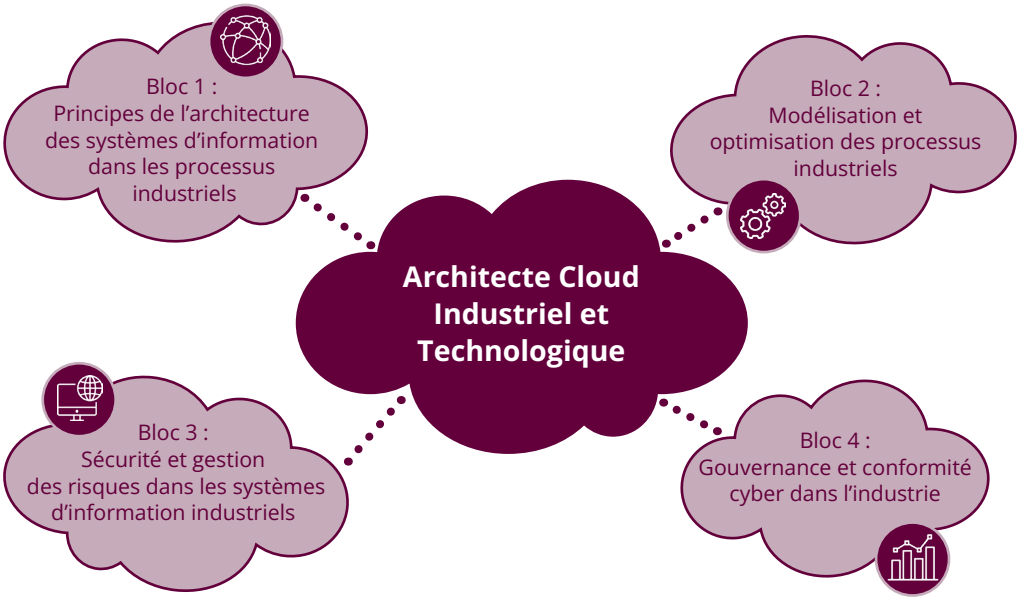
est une formation intensive de 11 jours, avec 7 heures de cours chaque jour, divisée en 4 blocs spécialisés.

- Bloc 1 : Principes de l'architecture des systèmes d'information dans les processus industriels
- Bloc 2 : Modélisation et optimisation des processus industriels
- Bloc 3 : Sécurité et gestion des risques dans les systèmes d'information industriels
- Bloc 4 : Gouvernance et conformité cyber dans l'industrie

Plusieurs options d'inscription sont disponibles :
• En suivant l'ensemble des blocs, vous pouvez obtenir l'Executive Certificate de l'Université Paris-Saclay.
• En suivant un seul bloc spécifique, vous recevrez une attestation de participation pour le bloc suivi. Pour deux blocs choisis vous bénéficiez d'une réduction de 10% sur l'ensemble de la commande.

Vous trouverez ci-dessous les fiches descriptives détaillant le contenu de chaque bloc ainsi que la biographie de nos experts qui animent cette formation.





Principes de l'architecture des systèmes d'information dans les processus industriels

2 jours | 1450 € repas inclus | Initiation

Bloc 1

Réf. AC202501

Maîtrisez les fondamentaux de l'architecture des systèmes d'information industriels

3 SESSIONS AU CHOIX

SESSION 1 – 2025
2-3 avril

SESSION 2 – 2025
16-17 juin

SESSION 3 – 2025
2-3 Octobre

Objectifs :

- Comprendre les composants essentiels des systèmes d'information industriels
- Identifier les différents types de systèmes d'information utilisés dans l'industrie et en décrire leurs caractéristiques
- Analyser les interactions entre différents composants dans un environnement industriel complexe
- Appliquer des principes d'architecture pour optimiser l'efficacité et la résilience des systèmes d'information industriels

Prérequis

Connaissances de base en systèmes d'information et en informatique

Public concerné

Professionnels de l'informatique, ingénieurs système, responsables IT, consultants en transformation numérique

Compétences acquises

Maîtriser les principes fondamentaux de l'architecture des systèmes d'information industriels

Intervenants

Edy Hourany, Ingénieur logiciel senior DOCTOLIB

Programme :

Composants essentiels des systèmes d'information industriels

- Exploration des composants clés tels que les serveurs, les bases de données, les réseaux et les systèmes de stockage utilisés dans l'industrie, ainsi que des technologies émergentes comme les microservices et conteneurs

Étude de cas : analyse de l'architecture du système d'information d'un système de gestion d'entrepôts utilisé par une entreprise de logistique, pour identifier ses points faibles et proposer des améliorations afin d'optimiser la performance et la sécurité

Types de systèmes d'information industriels

- Identification et description des différents types de systèmes d'information déployés dans l'industrie, comme les ERP, les systèmes MES, et les systèmes de gestion de la chaîne d'approvisionnement. Une introduction aux bases de données non relationnelles (NoSQL) et au traitement des Big Data dans les environnements industriels est également incluse

Exercices d'application : analyse à partir de deux scénarios, soit la gestion des stocks, soit les flux logistiques, pour identifier les inefficacités présentes, puis proposer des solutions concrètes afin d'améliorer la performance et l'intégration entre les différents systèmes industriels (ERP, MES, SCM)ses points faibles et proposer des améliorations afin d'optimiser la performance et la sécurité

Interactions et interopérabilité des systèmes

- Analyse des interactions entre les différents composants d'un système d'information industriel et des défis liés à l'interopérabilité, y compris l'intégration des API et l'architecture orientée services (SOA)

Atelier pratique : élaboration d'une stratégie d'optimisation pour un système d'information industriel en environnement multi-cloud (ex. AWS, Azure), avec un focus sur la gestion des données en temps réel et les contraintes budgétaires

Challenge de clôture :

- Un E-Quiz pour valider les acquis

Modélisation et optimisation des processus industriels

Maîtrisez les méthodes et outils de modélisation pour l'optimisation des processus industriels

4 jours | 3100 € repas inclus | Perfectionnement

Bloc 2

Réf. AC202502

3 SESSIONS AU CHOIX

SESSION 1 – 2025
7-10 avril

SESSION 2 – 2025
23-26 juin

SESSION 3 – 2025
7-10 Octobre

Objectifs :

- Appliquer les principes fondamentaux d'architecture pour concevoir des systèmes d'information industriels efficaces
- Comprendre les concepts clés de la modélisation des processus industriels
- Maîtriser les outils et techniques d'optimisation des processus pour améliorer l'efficacité et réduire les coûts
- Mettre en place des méthodologies de modélisation pour identifier, simuler et résoudre des problématiques complexes en milieu industriel

Public concerné

Professionnels de l'informatique, ingénieurs système, responsables IT, consultants en transformation numérique

Compétences acquises

Maîtriser les principes fondamentaux de l'architecture des systèmes d'information industriels

Prérequis

Connaissances de base en systèmes d'information et en informatique

Intervenants

Edy Hourany, Ingénieur logiciel senior DOCTOLIB

Programme :

Conception avancée des systèmes d'information industriels

- Approfondissement des principes de scalabilité, d'interopérabilité et de résilience des systèmes d'information industriels, avec une application à des systèmes spécifiques tels que les ERP, MES et SCM dans des scénarios complexes

Atelier pratique : élaboration d'un schéma d'architecture pour une infrastructure industrielle répondant à des exigences réelles, avec prise en compte des contraintes budgétaires et techniques

Méthodologies et techniques de modélisation

- Introduction aux méthodologies de modélisation telles que BPMN, UML et IDEF, permettant de comprendre leur application dans des environnements industriels complexes. Ces techniques sont essentielles pour représenter divers processus industriels, incluant les workflows, la gestion des stocks et la production en flux tendu. La maîtrise de ces outils de modélisation est cruciale pour optimiser et organiser les processus dans un cadre industriel

Exercice d'application : analyse d'un processus industriel existant (exemple : gestion des stocks ou production en flux tendu) pour créer un modèle en utilisant BPMN ou UML. Présentation de ce modèle en justifiant les choix méthodologiques effectués, et en proposant des améliorations pour optimiser le processus représenté

Outils modernes et mise en place des concepts fondamentaux

- Apprendre à utiliser les outils de modélisation avancés tels que Simulink, Draw.io et Excalidraw pour créer des modèles industriels détaillés et précis. En parallèle, comprendre l'intégration des méthodologies de conteneurisation, comme Docker, Kubernetes et Container Registry. Ces compétences facilitent la gestion des infrastructures complexes et le déploiement d'applications dans les environnements industriels, offrant ainsi une meilleure agilité et flexibilité dans l'exploitation des systèmes

Exercice d'application : conception d'un modèle détaillé d'une chaîne de production automatisée en utilisant les outils Draw.io ou Excalidraw. À partir de ce modèle, identification des points critiques dans la gestion des infrastructures, notamment le stockage et la gestion des flux, et proposition de solutions concrètes pour intégrer les technologies de conteneurisation

Optimisation des processus industriels

- Étude approfondie des approches d'optimisation telles que Waterfall, Agile, Lean, et Six Sigma pour améliorer l'efficacité des processus industriels. L'objectif est d'identifier les gaspillages, de maximiser la valeur ajoutée et d'adapter les méthodes d'optimisation aux spécificités de chaque industrie

Exercice d'application : modélisation de l'un des deux processus industriels suivants : soit l'optimisation des stocks avec la méthode Lean, soit la gestion des flux de production avec la méthode Agile. Séances de feedback et d'ajustement pour affiner les modèles proposés

Simulation et validation des modèles

- Apprendre à valider les modèles à l'aide d'outils de simulation avancés, tout en mettant l'accent sur la création de simulations basées sur des données réelles et des scénarios concrets issus de l'industrie

Études de cas : analyse de cas réels d'optimisation de processus dans des industries dans les secteurs de l'automobile ou de la logistique, où des méthodologies d'optimisation comme Six Sigma ou Lean ont été appliquées avec succès. Identification des problèmes initiaux, étude des solutions mises en oeuvre et proposition d'ajustements ou d'améliorations supplémentaires. Un focus particulier sera mis sur la gestion des ressources et la réduction des gaspillages

Challenge de clôture :

- Un E-Quiz pour valider les acquis

Sécurité et gestion des risques dans les systèmes d'information industriels

3 jours | 2325 € repas inclus | Perfectionnement

Bloc 3

Réf. AC202503

Protégez vos systèmes industriels grâce à une gestion efficace des risques et des stratégies de sécurité avancées

3 SESSIONS AU CHOIX

SESSION 1 – 2025
12-13-14 Mai

SESSION 2 – 2025
30 Juin -1-2 juillet

SESSION 3 – 2025
14-15-16 Octobre

Objectifs :

- Comprendre les concepts de base de la sécurité des systèmes d'information
- Identifier et analyser les risques spécifiques aux environnements informatiques industriels
- Mettre en oeuvre des stratégies de gestion des risques pour sécuriser les systèmes d'information
- Anticiper les menaces émergentes et développer des plans de réponse adaptés aux environnements industriels
- Évaluer l'efficacité des mesures de sécurité mises en place et les ajuster en fonction des évolutions technologiques et des nouvelles menaces

Public concerné

Professionnels de l'informatique, ingénieurs système, responsables IT, consultants en transformation numérique

Compétences acquises

Gérer les risques de sécurité dans les systèmes d'information industriels, et proposer des mesures correctives pour renforcer la sécurité

Prérequis

Connaissances générales en gestion des risques ou en audit

Intervenants

Nadim Henoud
Ingénieur logiciel et cybersécurité POTECH

Programme :

Introduction à la sécurité des systèmes d'information

- Comprendre les principes fondamentaux de la sécurité des systèmes d'information industriels, tout en analysant les menaces émergentes telles que la cybercriminalité, les ransomwares, et les attaques sur les infrastructures critiques

Étude de cas : analyse d'un exemple concret d'infrastructure industrielle pour étudier les modèles de sécurité (confidentialité, intégrité, disponibilité) appliqués. Identification des failles courantes et évaluation des risques associés

Identification et analyse des risques

- Apprendre à identifier, évaluer et analyser les risques spécifiques aux environnements informatiques industriels tout en adoptant une approche proactive. Cette démarche permet d'anticiper et de détecter les failles potentielles avant qu'elles ne soient exploitées, en s'appuyant sur des méthodologies reconnues comme EBIOS et ISO 27005

Mise en situation : évaluation d'un système industriel réel, identification des vulnérabilités potentielles et mise en oeuvre d'une méthodologie pour analyser les risques. Proposition de mesures préventives pour limiter l'impact de ces failles

Mise en oeuvre de stratégies de gestion des risques

- Mettre en place des politiques et procédures efficaces pour atténuer les risques et sécuriser les systèmes d'information, tout en assurant une amélioration continue de la sécurité grâce à des audits réguliers et à l'actualisation des procédures face aux nouvelles menaces et évolutions technologiques, afin de garantir la résilience à long terme des infrastructures industrielles

Étude de cas : analyse d'exemples réels d'entreprises ayant implémenté des stratégies de gestion des risques, évaluation des approches utilisées, identification des améliorations possibles et élaboration d'un plan pour assurer une gestion continue des risques

Utilisation d'outils et de techniques de protection

- Se familiariser avec les outils de sécurité tels que les firewalls, systèmes de détection d'intrusion et cryptage, ainsi que leur déploiement efficace dans les environnements industriels, tout en adoptant les bonnes pratiques de configuration et de mise à jour pour éviter les erreurs humaines et maximiser la résilience des systèmes

Exercide d'application : configuration et déploiement de divers outils de sécurité dans un environnement simulé, puis application des mises à jour et des configurations de sécurité en suivant les meilleures pratiques pour assurer une protection optimale contre les menaces

Évaluation des vulnérabilités et propositions de mesures correctives

- Évaluer la sécurité des systèmes en analysant les résultats des tests de pénétration et des scans de vulnérabilités, recommander des mesures correctives pour renforcer la sécurité, établir des priorités d'intervention, développer un plan d'action correctif, et assurer l'efficacité à long terme des mesures à travers des audits post-implémentation

Études de cas : analyse de cas concrets pour comprendre les vulnérabilités et discuter des mesures correctives appropriées en comparant les différentes approches

Challenge de clôture :

- Un E-Quiz pour valider les acquis

Gouvernance et conformité cyber dans l'industrie

2 jours | 1550€ repas inclus | Perfectionnement

Maîtrisez les réglementations et normes de cybersécurité et apprenez à mettre en conformité votre organisation

Bloc 4

Réf. AC202504

3 SESSIONS AU CHOIX

SESSION 1 – 2025
15-16 Mai

SESSION 2 – 2025
3-4 juillet

SESSION 3 – 2025
22-23 Octobre

Prérequis

Connaissances générales en gestion des risques ou en audit

Public concerné

Professionnels de l'informatique, ingénieurs système, responsables IT, consultants en transformation numérique

Compétences acquises

Maîtriser les réglementations et normes de cybersécurité et mettre en conformité une organisation industrielle, tout en gérant efficacement les risques et les crises cyber

Intervenants

Yacine Ladjici
Responsable de la cybersécurité du groupe VALEO POWER

Objectifs :

- Comprendre les risques cyber dans le contexte actuel
- Identifier les réglementations et normes cyber et leur déclinaison opérationnelle
- Appliquer les méthodologies d'audit cyber et les mettre en oeuvre

Programme :

Introduction aux risques cyber dans l'industrie

- Introduction aux principaux risques de cybersécurité affectant les environnements industriels, avec une analyse approfondie des menaces actuelles, des vulnérabilités spécifiques et des tendances émergentes

Étude de cas : exemple réel d'entreprise industrielle ayant subi une cyberattaque, en analysant les menaces spécifiques, les impacts sur les systèmes industriels, les actions mises en place par l'entreprise pour limiter les dégâts et rétablir les systèmes, et les mesures adoptées pour renforcer la sécurité post-attaque

Normes et réglementations de cybersécurité

- Exploration des principales normes et réglementations de cybersécurité (NIS2, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, etc.), avec un focus sur leur application dans différents contextes industriels, ainsi que comparaison des réglementations européennes et internationales en matière de cybersécurité

Étude de cas : analyse d'entreprises ayant implémenté des normes spécifiques à travers l'identification des failles éventuelles et des ajustements ou des améliorations proposés pour optimiser l'implémentation des normes

Analyse de risques et gestion de crise cyber

- Approfondissement des méthodologies d'analyse des risques (EBios RM, ISO 19011) et des stratégies de gestion de crise cyber, y compris la gestion des incidents et la mise en place de plans de réponse aux cyberattaques

Mise en situation : gestion en direct d'une cyberattaque, pour coordonner une réponse, gérer les communications de crise et limiter les impacts sur les opérations

Audits cyber et tests de vulnérabilité

- Apprentissage des techniques d'audit cyber, englobant les aspects organisationnels et techniques, ainsi que des méthodes avancées pour évaluer la sécurité des systèmes. En parallèle, étude des tests de pénétration et des techniques de détection de vulnérabilités, telles que les scans de sécurité et le pentesting

Exercice d'application : réalisation d'un audit complet sur une organisation, incluant l'évaluation des aspects organisationnels et techniques

Challenge de clôture :

- Un E-Quiz pour valider les acquis

Vos intervenants

Edy Hourany

Edy Hourany est docteur en ingénierie logicielle, spécialisé dans la conception de systèmes distribués. Titulaire d'un doctorat de l'Université de Besançon, il possède plus de 15 ans d'expérience dans les technologies cloud et les architectures évolutives. Ancien professeur à l'Université de Besançon, il est actuellement ingénieur logiciel senior chez Doctolib, où il développe des solutions robustes pour des applications critiques et crée des infrastructures cloud fiables et sécurisées, répondant aux défis technologiques actuels.

Nadim Henoud

Nadim Henoud est ingénieur logiciel et expert en cybersécurité avec plus de 15 ans d'expérience. Il combine une connaissance technique approfondie et une expertise stratégique en méthodologie agile pour concevoir des architectures évolutives et livrer des solutions technologiques complexes. Il intervient également à Télécom Paris, EPITA, ESIEA et à l'USJ de Beyrouth, où il enseigne sur des sujets liés à l'ingénierie, la sécurité, l'intelligence artificielle et l'apprentissage automatique.

Yacine Ladjici

Yacine Ladjici est responsable de la cybersécurité du groupe Valeo Power, avec un parcours solide dans l'industrie automobile en conception et sécurisation de produits pour la mobilité intelligente et connectée. Il est intervenant à la Société des Ingénieurs de l'Automobile, Télécom ParisTech et à l'Université de Paris-Saclay. Il préside également la communauté des experts cybersécurité de la SIA.

Executive Certificate Architecte Cloud Industriel et Technologique

INFORMATIONS PRATIQUES

INSCRIPTION

Merci d'envoyer le(s) bloc(s) que vous souhaitez suivre à l'adresse e-mail suivante : julie.sampoux@universite-paris-saclay.fr.

CONTACT & ACCESSIBILITÉ

Maria FAHED, PhD
Responsable de l'offre Executive Certificate Architecte Cloud Industriel et Technologique
maria.fahed@universite-paris-saclay.fr

Titulaire d'un Phd, Maria est en charge de créer les nouvelles formations certifiante et diplômantes de la Direction de la Formation Tout au Long de la Vie à l'université Paris-Saclay, première université d'Europe classée 12ème au classement Shangaï 2024. Maria a débuté sa carrière en tant que chercheuse et enseignante, notamment au CEA et dans une école d'ingénieurs en numérique.

handicap.cfadftlv@universite-paris-saclay.fr
Plus d'informations sur le site de l'Université Paris-Saclay :
www.universite-paris-saclay.fr
Rubrique Vie de Campus > Handicap

LIEU DE LA FORMATION

Accueil administratif
Université Paris-Saclay, 9 rue Joliot Curie, 91190 Gif-sur-Yvette

université PARIS-SACLAY