

Technicien spécialisé en systèmes IT/OT sécurisés pour l'industrie ou les infrastructures urbaines

RNCP40564 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	201, 326
Formacode(s)	24491, 24231, 24426, 24472, 24478
Code(s) ROME	I1302, I1304, I1401, M1802, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	30/04/2025
Date d'échéance	30/04/2028

Certificateur(s)

ECAM LaSalle · SIRET : 77988344600014

Partenaires habilités

1 organisme habilité, d'après la liste publiée par France compétences : 1 à former.

Organisme	SIRET	Habilitation
ASSOCIATION POUR LA FORMATION DES INFORMATIENS PAR L'APRENTISSAGE	3910872100004 6	Former

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'Industrie 4.0, issue de la quatrième révolution industrielle, intègre des technologies comme l'IoT, l'IA et la robotique pour optimiser la production en temps réel. Toutefois, cette transformation expose les systèmes à des risques cyber, notamment avec la convergence IT/OT. En 2022, plus de 40 % des équipements OT ont été attaqués (source : Kaspersky), rendant la cybersécurité stratégique pour les entreprises afin de protéger leurs infrastructures et données. Il en est de même pour les systèmes d'infrastructures urbaines, tels qu'un réseau électrique urbain, un système de transport en commun, d'assainissement, de gestion des déchets, ou de télécommunications.

Dans ce contexte relativement récent, le métier de technicien spécialisé en systèmes IT/OT sécurisés pour l'industrie ou les infrastructures urbaines, souffre d'une pénurie de main-d'œuvre qualifiée. Malgré la forte demande, les entreprises peinent à recruter, avec 2/3 structures en difficulté. La pénurie persiste en raison de la rareté des profils combinant compétences techniques et expertise en cybersécurité.

L'objectif de la certification est d'attester des compétences de ce type de techniciens, ayant des compétences transverses de "convergence IT-OT", et venant en appui des ingénieurs, de façon opérationnelle, pour relayer et mettre en œuvre sur le terrain et au quotidien la maintenance et les stratégies de cybersécurité des entreprises et autres types d'organisations.

ACTIVITÉS VISÉES

Etat des lieux d'un parc d'automates industriels et préparation technique d'une intervention sur des automates

Installation et programmation d'automates industriels

Maintenance d'automates industriels

Installation de réseaux informatiques

Analyse et maintenance des réseaux informatiques
Prise en compte de la durabilité des infrastructures
Prévention contre les risques et sécurisation d'un système informatique industriel
Phase de remédiation : détection d'incidents, investigations, endiguement, éviction, éradication puis reconstruction d'un système informatique industriel
Suivi de crise après une cyberattaque
Mise en œuvre d'une communication en anticipation d'une crise cyber
Organisation d'exercices de simulation de cyberattaques et entraînement à la communication de crise
Communication en réaction à une crise cyber

COMPÉTENCES ATTESTÉES

Formaliser l'état des lieux d'un parc d'automates industriels ou d'infrastructures urbaines, en analysant les processus industriels existants, et en identifiant les moyens techniques et technologiques mis en œuvre pour opérer les flux de production ou d'exploitation, afin de répertorier chaque automate, ses fonctionnalités et ses besoins de maintenance ou de renouvellement.

Préparer la documentation, le matériel et les équipements nécessaires à l'installation d'automates, en vérifiant l'état de bon fonctionnement des moyens techniques et la mise à jour de la documentation, afin de s'assurer de leur fiabilité.

Evaluer les risques de chaque intervention sur des automates industriels, liés notamment à leur fonctionnement et à leur environnement, afin de mettre en œuvre les actions de prévention correspondantes et de s'équiper en conséquence.

Installer des automates de natures différentes, en les programmant avec le langage adapté, pour assurer leur bon fonctionnement, leur fiabilité et leur niveau de performance, dans le respect des mesures de prévention de santé, de sécurité au travail et d'adaptation à l'environnement de travail (besoins ergonomiques des opérateurs, en situation de handicap ou non).

Modifier la programmation d'automates industriels ou d'infrastructures urbaines, pour adapter leur fonctionnement aux évolutions des besoins de production, d'exploitation ou en réponses à des aléas, et permettre une bonne flexibilité en la matière.

Réaliser la maintenance d'un parc d'automates en appliquant des techniques de maintenance prédictive, préventive et curative, afin d'optimiser leur fonctionnement, de permettre la continuité de service d'un système industriel ou urbain, et de faire face à un dysfonctionnement.

Mettre en œuvre les évolutions d'un parc d'automates en tenant compte des critères de durabilité, notamment par la réduction de la consommation d'énergie et de fluides, par la gestion des déchets et par l'anticipation de l'obsolescence, pour participer aux efforts de transition de l'entreprise en la matière.

Apporter son expertise technique à l'installation d'un réseau informatique d'infrastructures industrielles ou urbaines, conformément aux dispositions des normes nationales et internationales en vigueur, pour assurer la stabilité et la pérennité du réseau, dans le respect des mesures de prévention de santé, de sécurité au travail et d'adaptation à l'environnement de travail (besoins ergonomiques des utilisateurs, en situation de handicap ou non).

Analyser les performances de réseaux informatiques d'infrastructures industrielles et urbaines, en utilisant des outils de surveillance en temps réel et des rapports de performance, pour détecter des anomalies et des pannes.

Evaluer les risques de chaque intervention sur des réseaux informatiques d'infrastructures industrielles et urbaines, liés notamment à leur fonctionnement et à leur environnement, afin de mettre en œuvre les actions de prévention correspondantes et de s'équiper en conséquence.

Réaliser la maintenance d'un réseau informatique d'infrastructures industrielles ou urbaines en appliquant des techniques de maintenance prédictive, préventive et curative, afin d'optimiser son fonctionnement, de permettre la continuité de service, et de faire face à un dysfonctionnement.

Tenir à jour la cartographie de réseaux informatiques et l'historique des interventions, pour pouvoir partir de la connaissance de l'existant en cas de besoins d'analyse, d'évolutions, ou dans une démarche d'amélioration continue.

Développer un réseau de systèmes informatiques existant en tenant compte des critères de durabilité, notamment par la réduction de la consommation d'énergie et de matériaux, par la gestion des déchets et par l'anticipation de l'obsolescence des systèmes, afin de contribuer à la transition environnementale de l'entreprise.

Analyser les failles de sécurité d'un système incluant des réseaux et des automates industriels, afin de contribuer à établir un plan de prévention face à des cyber-risques.

Mettre en œuvre des mesures de prévention de sûreté et sécurité les plus efficaces possibles au bénéfice d'un système industriel ou d'infrastructures urbaines, pour protéger un parc d'automates, un réseau informatique et leur

environnement, des conséquences, dysfonctionnements et dangers qui résulteraient d'une cyberattaque.

Analyser des mesures et indicateurs en lien avec le fonctionnement d'un système incluant des automates et un réseau informatique, pour détecter des anomalies en cas de dysfonctionnements et/ou d'instabilité même marginale ou faible du système.

Identifier les causes d'une instabilité de signaux numériques au sein d'un système incluant des automates et un réseau informatique, pour les catégoriser selon leur criticité, et pour mettre notamment en évidence la probabilité d'une cyberattaque difficilement détectable.

Réagir efficacement et en situation d'urgence, en cas de cyberattaque, pour mettre en sécurité un système informatique industriel, comprenant un parc d'automates et un réseau informatique.

Contribuer à l'éradication d'incidents résultant d'une cyberattaque, en apportant des solutions techniques et en appliquant un plan de continuité et de reprise d'activité, pour assurer la continuité des opérations.

Formaliser les retours d'expérience après une sortie de crise, pour capitaliser sur les apprentissages, améliorer les pratiques, et partager en interne comme en externe, dans la limite de ses autorisations.

Réaliser une veille technologique, réglementaire, normative et sociétale régulière, pour anticiper les évolutions technologiques, liées aux cybermenaces, cyberattaques, et en matière de cybersécurité.

Formaliser des documentations techniques et d'utilisation à destination d'autres équipes techniques d'une part et des collaborateurs d'autre part, pour permettre une utilisation adéquate des équipements d'un système d'information.

Développer une écoute active pour recueillir les informations issues des opérateurs, des autres types d'utilisateurs ou des autres équipes techniques, pour collecter et restituer des informations sur le fonctionnement d'un réseau informatique industriel (OT et IT).

Promouvoir les bonnes pratiques en matière de cybersécurité, en coanimant des actions de sensibilisation adaptées au public visé (opérateurs, techniciens, communicants notamment) et tenant compte des situations de handicap de certains collaborateurs, pour favoriser une utilisation adéquate des équipements d'un système d'information.

Contrôler le respect des protocoles de sécurité lors d'interventions de sociétés extérieures sur un parc d'automates et son réseau informatique, en analysant la nature des actions prévues et en formulant ou non son accord sur la faisabilité de l'intervention, afin de préserver l'intégrité du système industriel ou urbain concerné.

Collaborer avec l'ensemble des équipes techniques concernées lors d'un exercice de gestion de crise d'origine cyber pour s'entraîner à y faire face et développer des réflexes et des méthodes, pour mieux travailler en synergie interne, notamment en langue anglaise.

Contribuer à la préparation de stratégies de communication en gestion de crise cyber, en concevant des messages adaptés pour expliquer la nature de l'attaque et les impacts sur l'organisation, donner de la visibilité sur les actions techniques mises en œuvre et rassurer les parties prenantes en interne, voire en externe (autorités concernées).

Communiquer en interne et en externe lors d'une gestion de crise cyber, pour transmettre des éléments techniques et des points de situation factuels, dans le cadre de son champ d'actions.

Blocs de compétences

RNCP40564BC01 — Installer et maintenir un parc d'automates de systèmes industriels ou d'infrastructures

LISTE DE COMPÉTENCES

Formaliser l'état des lieux d'un parc d'automates industriels ou d'infrastructures urbaines, en analysant les processus industriels existants, et en identifiant les moyens techniques et technologiques mis en œuvre pour opérer les flux de production ou d'exploitation, afin de répertorier chaque automate, ses fonctionnalités et ses besoins de maintenance ou de renouvellement.

Préparer la documentation, le matériel et les équipements nécessaires à l'installation d'automates, en vérifiant l'état de bon fonctionnement des moyens techniques et la mise à jour de la documentation, afin de s'assurer de leur fiabilité.

Evaluer les risques de chaque intervention sur des automates industriels, liés notamment à leur fonctionnement et à leur environnement, afin de mettre en œuvre les actions de prévention correspondantes et de s'équiper en conséquence.

Installer des automates de natures différentes, en les programmant avec le langage adapté, pour assurer leur bon fonctionnement, leur fiabilité et leur niveau de performance, dans le respect des mesures de prévention de santé, de sécurité au travail et d'adaptation à l'environnement de travail (besoins ergonomiques des opérateurs, en situation de handicap ou non).

Modifier la programmation d'automates industriels ou d'infrastructures urbaines, pour adapter leur fonctionnement aux évolutions des besoins de production, d'exploitation ou en réponses à des aléas, et permettre une bonne flexibilité en la matière.

Réaliser la maintenance d'un parc d'automates en appliquant des techniques de maintenance prédictive, préventive et curative, afin d'optimiser leur fonctionnement, de permettre la continuité de service d'un système industriel ou urbain, et de faire face à un dysfonctionnement.

Mettre en œuvre les évolutions d'un parc d'automates en tenant compte des critères de durabilité, notamment par la réduction de la consommation d'énergie et de fluides, par la gestion des déchets et par l'anticipation de l'obsolescence, pour participer aux efforts de transition de l'entreprise en la matière.

MODALITÉS D'ÉVALUATION

Mise en situation individuelle reconstituée sur plateau technique : Chaque candidat tire au sort un cas pratique de résolution de panne, d'incident ou de besoin de maintenance, concernant un ou plusieurs automates industriels.

Mise en situation individuelle sur poste informatique : Chaque candidat se voit proposer une situation de programmation d'automate permettant de vérifier sa capacité à programmer des automates en respectant les exigences techniques, les normes de sécurité, les besoins ergonomiques associés à l'environnement de travail et la prise en compte du développement durable.

RNCP40564BC02 — Installer et maintenir des réseaux informatiques d'infrastructures industrielles et urbaines

LISTE DE COMPÉTENCES

Apporter son expertise technique à l'installation d'un réseau informatique d'infrastructures industrielles ou urbaines, conformément aux dispositions des normes nationales et internationales en vigueur, pour assurer la stabilité et la pérennité du réseau, dans le respect des mesures de prévention de santé, de sécurité au travail et d'adaptation à l'environnement de travail (besoins ergonomiques des utilisateurs, en situation de handicap ou non).

Analyser les performances de réseaux informatiques d'infrastructures industrielles et urbaines, en utilisant des outils de surveillance en temps réel et des rapports de performance, pour détecter des anomalies et des pannes.

Evaluer les risques de chaque intervention sur des réseaux informatiques d'infrastructures industrielles et urbaines, liés notamment à leur fonctionnement et à leur environnement, afin de mettre en œuvre les actions de prévention correspondantes et de s'équiper en conséquence.

Réaliser la maintenance d'un réseau informatique d'infrastructures industrielles ou urbaines en appliquant des techniques de maintenance prédictive, préventive et curative, afin d'optimiser son fonctionnement, de permettre la continuité de service, et de faire face à un dysfonctionnement.

Tenir à jour la cartographie de réseaux informatiques et l'historique des interventions, pour pouvoir partir de la connaissance de l'existant en cas de besoins d'analyse, d'évolutions, ou dans une démarche d'amélioration continue.

Développer un réseau de systèmes informatiques existant en tenant compte des critères de durabilité, notamment par la réduction de la consommation d'énergie et de matériaux, par la gestion des déchets et par l'anticipation de l'obsolescence des systèmes, afin de contribuer à la transition environnementale de l'entreprise.

MODALITÉS D'ÉVALUATION

Étude de cas : Le candidat reçoit une présentation d'une entreprise multisite, de ses activités, des process utilisés pour la sécurisation des systèmes d'information. Il doit, à partir de ces informations, réaliser la cartographie du système d'information afin de recenser les vulnérabilités, identifier les scénarii de risques et leurs impacts sur l'organisation.

Mise en situation dans un hub informatique : En temps réel, le candidat doit suivre les performances du réseau, analyser les données collectées pour identifier ou anticiper des anomalies. Il propose des solutions pour améliorer le système soumis aux anomalies (existantes ou créées par des évaluateurs). Il doit également proposer des actions pour améliorer la durabilité du réseau.

RNCP40564BC03 — Assurer la continuité d'un système informatique industriel, en faisant converger les technologies opérationnelles (OT) et celles de l'information (IT)

LISTE DE COMPÉTENCES

Analyser les failles de sécurité d'un système incluant des réseaux et des automates industriels, afin de contribuer à établir un plan de prévention face à des cyber-risques.

Mettre en œuvre des mesures de prévention de sûreté et sécurité les plus efficaces possibles au bénéfice d'un système industriel ou d'infrastructures urbaines, pour protéger un parc d'automates, un réseau informatique et leur environnement, des conséquences, dysfonctionnements et dangers qui résulteraient d'une cyberattaque.

Analyser des mesures et indicateurs en lien avec le fonctionnement d'un système incluant des automates et un réseau informatique, pour détecter des anomalies en cas de dysfonctionnements et/ou d'instabilité même marginale ou faible du système.

Identifier les causes d'une instabilité de signaux numériques au sein d'un système incluant des automates et un réseau informatique, pour les catégoriser selon leur criticité, et pour mettre notamment en évidence la probabilité d'une cyberattaque difficilement détectable.

Réagir efficacement et en situation d'urgence, en cas de cyberattaque, pour mettre en sécurité un système informatique industriel, comprenant un parc d'automates et un réseau informatique.

Contribuer à l'éradication d'incidents résultant d'une cyberattaque, en apportant des solutions techniques et en appliquant un plan de continuité et de reprise d'activité, pour assurer la continuité des opérations.

Formaliser les retours d'expérience après une sortie de crise, pour capitaliser sur les apprentissages, améliorer les pratiques, et partager en interne comme en externe, dans la limite de ses autorisations.

MODALITÉS D'ÉVALUATION

Mise en situation reconstituée sur une plateforme d'intégration et de simulation de systèmes IT/OT, permettant de jouer des scénarios réalistes, comprenant de véritables cyberattaques : Le candidat est immergé dans le centre opérationnel de sécurité d'une structure fictive. La structure subit une cyberattaque virtuelle.

RNCP40564BC04 — Promouvoir les bonnes pratiques d'utilisation des technologies opérationnelles (OT) et de l'information (IT), notamment en matière de cybersécurité

LISTE DE COMPÉTENCES

Réaliser une veille technologique, réglementaire, normative et sociétale régulière, pour anticiper les évolutions technologiques, liées aux cybermenaces, cyberattaques, et en matière de cybersécurité.

Formaliser des documentations techniques et d'utilisation à destination d'autres équipes techniques d'une part et des collaborateurs d'autre part, pour permettre une utilisation adéquate des équipements d'un système d'information.

Développer une écoute active pour recueillir les informations issues des opérateurs, des autres types d'utilisateurs ou des autres équipes techniques, pour collecter et restituer des informations sur le fonctionnement d'un réseau informatique industriel (OT et IT).

Promouvoir les bonnes pratiques en matière de cybersécurité, en coanimant des actions de sensibilisation adaptées au public visé (opérateurs, techniciens, communicants notamment) et tenant compte des situations de handicap de certains collaborateurs, pour favoriser une utilisation adéquate des équipements d'un système d'information.

Contrôler le respect des protocoles de sécurité lors d'interventions de sociétés extérieures sur un parc d'automates et son réseau informatique, en analysant la nature des actions prévues et en formulant ou non son accord sur la faisabilité de l'intervention, afin de préserver l'intégrité du système industriel ou urbain concerné.

Collaborer avec l'ensemble des équipes techniques concernées lors d'un exercice de gestion de crise d'origine cyber pour s'entraîner à y faire face et développer des réflexes et des méthodes, pour mieux travailler en synergie interne, notamment en langue anglaise.

Contribuer à la préparation de stratégies de communication en gestion de crise cyber, en concevant des messages adaptés pour expliquer la nature de l'attaque et les impacts sur l'organisation, donner de la visibilité sur les actions techniques mises en œuvre et rassurer les parties prenantes en interne, voire en externe (autorités concernées).

Communiquer en interne et en externe lors d'une gestion de crise cyber, pour transmettre des éléments techniques et des points de situation factuels, dans le cadre de son champ d'actions.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle écrite et orale : Le candidat est sollicité par son manager pour sensibiliser des acteurs impactés par une cyberattaque portant sur la sécurité des données, des réseaux et des systèmes.

Cas pratique individuel, présenté à l'oral : Le candidat dispose du protocole global de la politique de sécurité d'une entreprise et des fiches techniques d'automates. Il reçoit une demande d'intervention d'une société extérieure sur un automate et sur le réseau informatique.

On lui demande de produire une analyse des menaces potentielles, à partir des données reçues et de son travail de veille, puis de se prononcer sur la faisabilité de l'intervention.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Secteur industriel et secteur des infrastructures urbaines, tels qu'un réseau électrique urbain, un système de

transport en commun, d'assainissement, de gestion des déchets, ou de télécommunications.

TYPE D'EMPLOIS ACCESSIBLES

- Analyste programmeur informatique industrielle
- Consultant en cybersécurité IT/OT/IoT
- Analyste Cybersécurité SI industriel
- Automaticien cyber
- Automaticien informatique industrielle
- Technicien Cybersécurité Industrielle IT/OT
- Technicien Support Sécurité des Réseaux Industriels
- Technicien Maintenance Sécurisée des Systèmes Automatisés
- Technicien informatique industrielle IT-OT
- Technicien informatique industrielle
- Technicien Systèmes IT/OT
- Technicien Maintenance Automatisation et Réseaux Industriels

RÈGLEMENTATIONS D'ACTIVITÉ

- Cadre législatif et réglementaire
- Directive NIS : cadre pour la sécurité des réseaux et de l'information au sein de l'UE.
- RGPD : réglementation sur la protection et la libre circulation des données personnelles.
- Normes et standards internationaux
- Norme ISO/IEC 27001 : norme internationale dédiée à la gestion de la sécurité de l'information, élaborée par l'Organisation Internationale de Normalisation (ISO) en collaboration avec la Commission Electrotechnique Internationale (IEC).
- Norme IEC 62443 : concernant spécifiquement la sécurité des systèmes de contrôle industriel, visant à protéger les systèmes industriels contre les incidents de cybersécurité potentiellement nuisibles.

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Très élevée (5/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 490 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % des actifs en emploi)
Familles professionnelles (FAP)	G0A40 — Ouvriers de la maintenance générale et mécanique · tension 5/5 (Très élevée) G0A41 — Ouvriers de la maintenance en électricité et en électronique · tension 5/5 (Très élevée) G1X72 — Techniciens et agents de maîtrise en maintenance générale et mécanique industrielle · tension 5/5 (Très élevée) G1X77 — Techniciens et agents de maîtrise en maintenance électrique, électronique et automatismes · tension 5/5 (Très élevée) H1X92 — Ingénieurs en maintenance et support technique client · tension 5/5 (Très élevée) M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	40 470

Jugés difficiles à recruter	58 %
Emplois saisonniers	4 %
Familles professionnelles (FAP)	G0A40 — Ouvriers de la maintenance générale et mécanique G0A41 — Ouvriers de la maintenance en électricité et en électronique G1X72 — Techniciens et agents de maîtrise en maintenance générale et mécanique industrielle G1X77 — Techniciens et agents de maîtrise en maintenance électrique, électronique et automatismes H1X92 — Ingénieurs en maintenance et support technique client M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Avoir validé un niveau 4 (type baccalauréat scientifique ou technologique), ou obtenu une certification de niveau 4, dans l'un des domaines suivants : automatisme, informatique industrielle, informatique.

Ou disposer d'une expérience professionnelle récente ou en cours, de six mois au moins, liée aux domaines précités, sur présentation d'un dossier de candidature, soumis à la validation de la Direction de l'Enseignement et des Formations.

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, VAE

Le jury de certification est composé de quatre personnes 100% externes à ECAM LaSalle :

- Le président du jury est un professionnel du secteur, en activité,
- Trois membres externes, également représentants qualifiés de la profession.

Base légale

Date de décision	30/04/2025
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	30/04/2028
Date de dernière délivrance possible	30/04/2032

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.ecam.fr/formation/bachelor-cybersecurite/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/40564/>