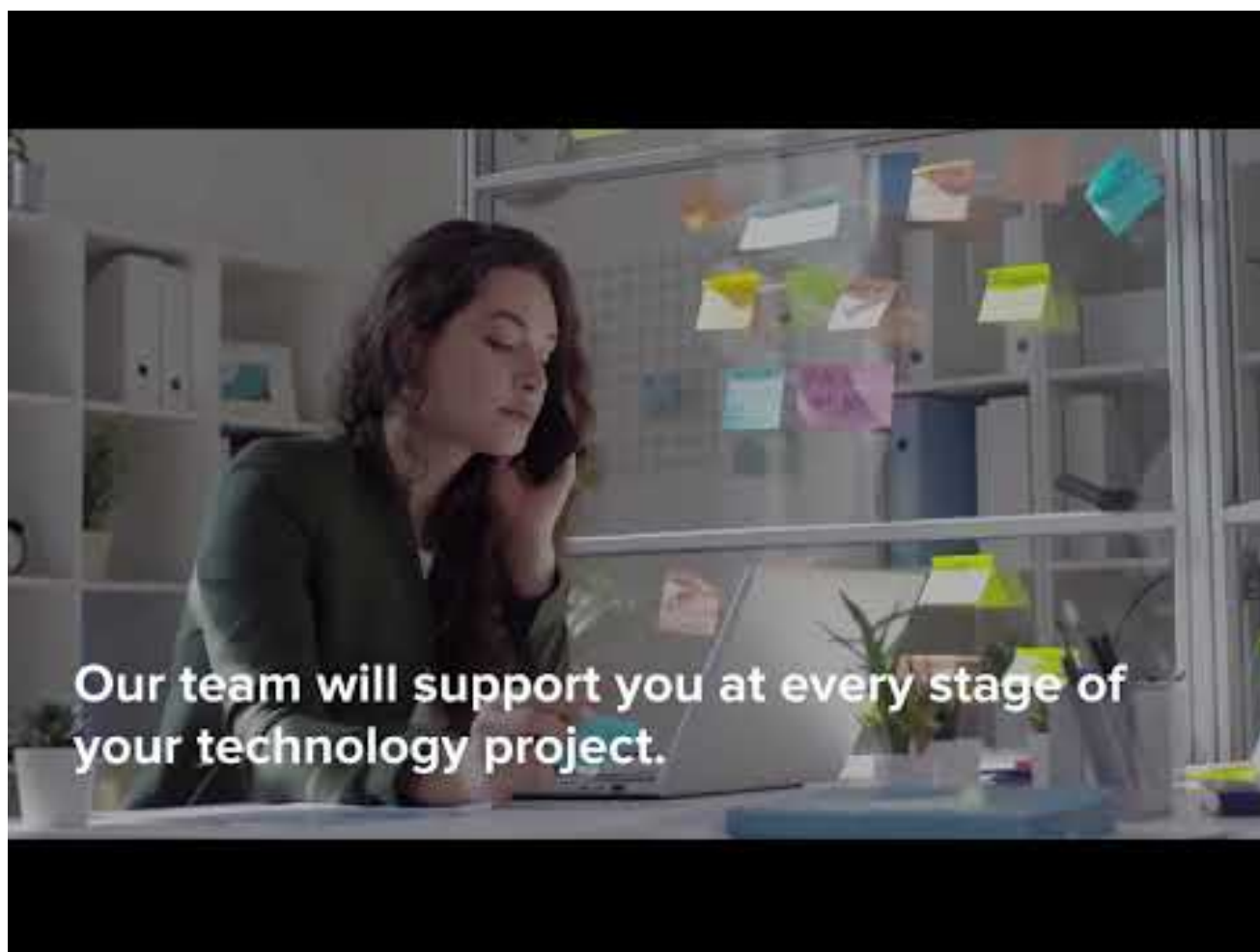


Le Rôle de l'Owner Engineer dans la Transformation Numérique des Usines

Dans le monde de l'industrie 4.0, un nouveau profil technique émerge souvent sans faire de bruit : l'Owner Engineer. Ce n'est pas un poste formel dans l'organigramme classique, mais plutôt une fonction transverse qui porte la responsabilité de la cohérence technique d'un projet, de la conception à la mise en service. En tant que consultant en technologies IT et OT, je vois régulièrement des projets de smart factory échouer parce que personne n'incarnait ce rôle. L'Owner Engineer n'est pas un chef de projet, ni un architecte détaché : c'est la personne qui connaît chaque capteur, chaque flux de Modbus TCP, chaque vulnérabilité potentielle sur un SCADA, et qui sait trancher quand le planning entre en conflit avec la sécurité.

Pourquoi l'Owner Engineer est Indispensable dans un Projet IIoT

Quand on déploie des IIoT sensors dans une ligne de production, la tentation est grande de se focaliser sur la collecte de données. Mais sans un Owner Engineer pour valider le chemin de bout en bout — du capteur jusqu'au Digital Twin —, on se retrouve avec des silos d'information. J'ai vu une usine investir dans des capteurs Zigbee pour le condition monitoring, sans vérifier la compatibilité avec le réseau LoRaWAN existant. Résultat : des données perdues et une équipe qui blâme le fournisseur. L'Owner Engineer aurait anticipé ce conflit de protocoles dès la phase de conception.



Our team will support you at every stage of your technology project.

Ce rôle devient critique quand on intègre des systèmes OT avec l'informatique classique. Les équipes IT parlent de NIST CSF, les équipes OT citent IEC 62443. L'[Owner Engineer](#) est celui qui traduit ces deux langages. Il sait qu'un patch de sécurité peut casser une liaison OPC UA entre un automate et un MES software, et il pèse ce risque contre la menace réelle. C'est un métier de jugement, pas de checklist.

L'Owner Engineer Face à la Cybersécurité des Systèmes Industriels

La cybersécurité dans l'industrie n'est plus optionnelle. Avec l'essor de l'Industry 4.0, les attaques ciblent désormais les SCADA systems et les HMI connectés. L'Owner Engineer doit intégrer la sécurité dès la conception, et non en fin de projet. Cela signifie choisir un Cybersecurity framework adapté — par exemple, combiner IEC 62443 pour les contrôles OT avec les recommandations du NIST CSF pour les couches IT — et s'assurer que chaque Edge computing device est correctement isolé.



Je me souviens d'un projet de smart factory où l'équipe voulait connecter des automates via Modbus TCP directement à un cloud public. L'Owner Engineer a refusé, arguant que le protocole n'offre aucune authentification. Il a imposé un gateway de sécurité et une couche OPC UA avec chiffrement. Ce n'était pas une posture de blocage, mais une décision éclairée par la connaissance des risques réels. Sans cette voix, le projet aurait été livré avec une vulnérabilité critique.

Quatre Compétences Clés pour un Owner Engineer

- Maîtrise des protocoles industriels : Modbus TCP, OPC UA, Zigbee, LoRaWAN, et leurs limites respectives.
- Capacité à naviguer entre les normes de sécurité : IEC 62443 pour l'OT, NIST CSF pour l'IT, et savoir où les faire converger.
- Connaissance des systèmes de production : SCADA, MES software, PLM, et leurs interfaces avec les IIoT sensors.
- Expérience terrain en condition monitoring et predictive maintenance, pour évaluer la pertinence réelle d'une donnée avant de l'industrialiser.

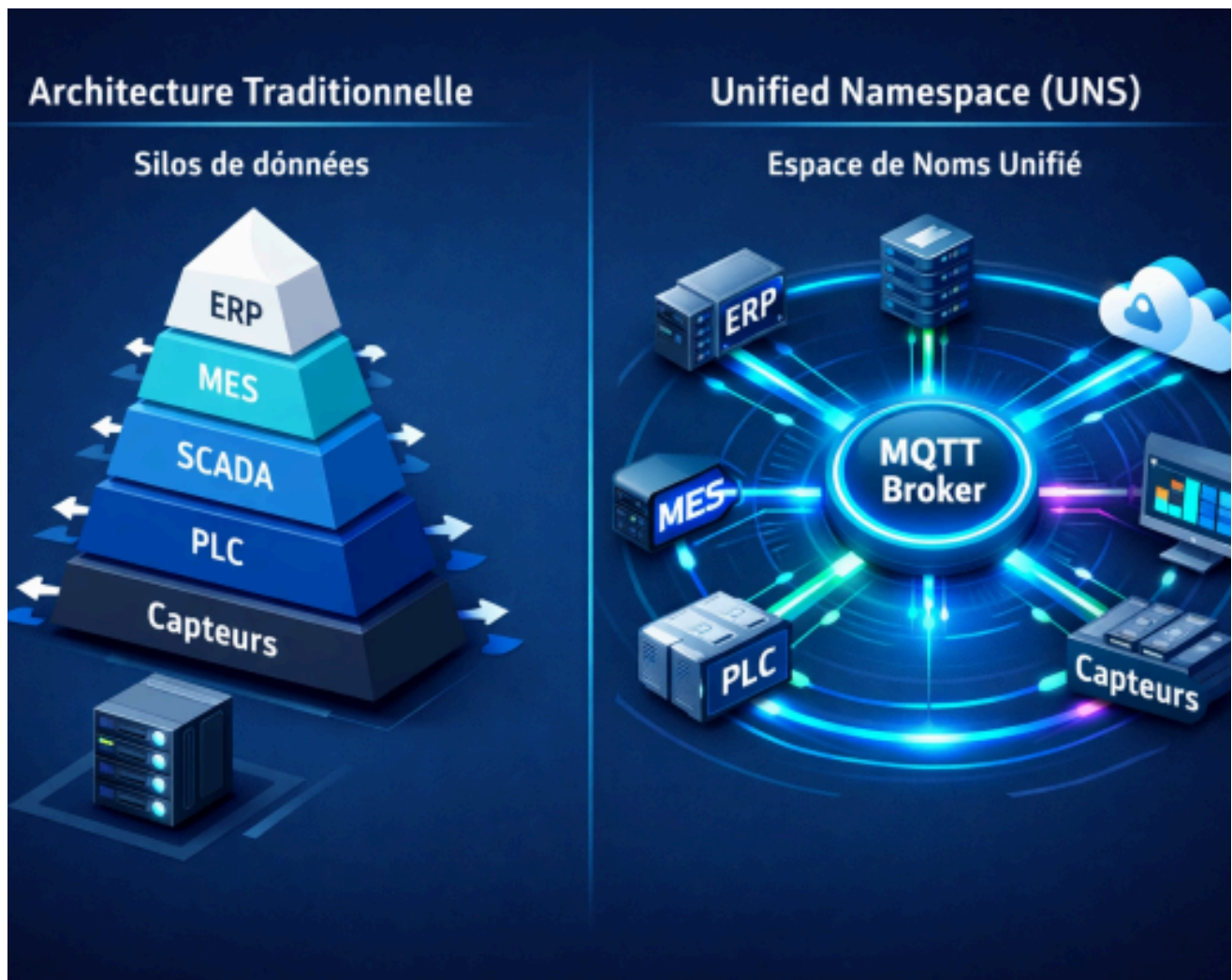
L'Intégration du Digital Twin et du MES sous l'Œil de l'Owner Engineer

Le concept de Digital Twin promet beaucoup, mais son implémentation repose sur une orchestration fine. L'Owner Engineer est celui qui vérifie que les données remontées par les IIoT sensors sont synchronisées avec le MES software, et que le modèle reflète bien l'état réel de la machine. Sans cette supervision, le Digital Twin devient un jouet de R&D, pas un outil de pilotage.

Prenons un cas concret : une ligne d'assemblage suivie en condition monitoring. Les capteurs LoRaWAN envoient des vibrations, des températures. Le MES enregistre les ordres de fabrication. L'Owner Engineer s'assure que les deux systèmes parlent via OPC UA, et que les alarmes de predictive maintenance déclenchent bien une action dans le PLM. Il teste le flux, il le documente, il le défend. C'est un travail de fond, rarement visible, mais qui évite les dérives coûteuses.

Edge Computing et Prise de Décision en Temps Réel

L'Edge computing est une réponse à la latence des traitements cloud, mais il pose des questions d'administration et de sécurité. L'Owner Engineer doit décider quels algorithmes tournent en local et quels calculs peuvent attendre le cloud. Par exemple, un diagnostic de predictive maintenance sur un moteur critique doit être instantané ; il sera traité sur une edge box proche de l'automate. En revanche, les analyses de tendances sur six mois peuvent partir vers un serveur central.



Cette répartition n'est pas triviale. Elle exige une compréhension des débits, des cycles de production, et des contraintes de OT Security. L'Owner Engineer arbitre entre performance et sécurité, sans dogmatisme. Parfois, il choisit de laisser un flux Modbus TCP non chiffré sur un réseau isolé parce que le chiffrement ajouterait une latence rédhibitoire. D'autres fois, il impose un gateway IEC 62443 pour protéger un SCADA critique. C'est un métier de compromis éclairés.

L'Importance d'un Owner Engineer dans la Maintenance Prédictive

La predictive maintenance est souvent présentée comme une solution miracle, mais elle repose sur une qualité de données que seul un Owner Engineer peut garantir. Il ne suffit pas d'installer des IIoT sensors ; il faut les calibrer, définir les seuils d'alarme, et valider que les données ne sont pas polluées par des vibrations parasites ou des interférences Zigbee. J'ai vu des équipes de data science construire des modèles sur des données erronées parce que personne n'avait vérifié la fiabilité des capteurs en environnement réel. L'Owner Engineer, lui, va sur le terrain. Il touche les machines, il écoute les opérateurs, il comprend pourquoi tel capteur dérive en été.

Dans un projet de smart factory, l'Owner Engineer est aussi celui qui coordonne le déploiement des HMI. Il s'assure que les écrans tactiles affichent les bonnes informations, que les alarmes sont priorisées, et que les opérateurs ne sont pas submergés de notifications inutiles. C'est un équilibre entre la richesse d'information et la charge cognitive.

Les Pièges à Éviter sans Owner Engineer

- Intégrer des systèmes IT et OT sans plan de sécurité commun, exposant les SCADA à des attaques venues du réseau bureautique.
- Choisir des protocoles comme Zigbee ou LoRaWAN sans évaluer leur coexistence dans un même environnement industriel (interférences, portée, fiabilité).
- Implémenter un Digital Twin sans synchronisation avec le MES, créant un décalage entre le modèle et la réalité de production.
- Déployer des solutions de predictive maintenance sans valider la qualité des données issues des capteurs, menant à des faux diagnostics.

Conclusion : Un Rôle de Cohérence, Pas de Titre

L'Owner Engineer n'est pas un titre officiel dans la plupart des organisations, mais c'est une fonction qui se reconnaît à l'impact. Dans les projets de transformation numérique, c'est souvent la personne qui empêche le projet de dérailler. Que vous travailliez sur une migration de SCADA, l'intégration d'un MES, ou la mise en place d'une plateforme IIoT, identifiez l'Owner Engineer dans votre équipe. Si personne n'incarne ce rôle, créez-le. La différence entre un projet qui livre un Digital Twin fonctionnel et un autre qui accumule les POC sans valeur tient souvent à cette seule présence.



VOUS DONNE RENDEZ-VOUS À

PRODUCTION
temps réel



DIGITAL CLASS
factory



MERCREDI 25 JUIN 2025



50 Quai Charles de Gaulle, Lyon



Fabien Villareal

Chief Strategy & Innovation Officer



Cyril Tiphineau

Sales Manager Digital Manufacturing

Le mot de la fin : l'Owner Engineer n'est pas un super-héros. C'est un ingénieur qui connaît ses limites, qui pose les bonnes questions, et qui sait dire non quand il le faut. Dans l'écosystème complexe de l'Industry 4.0, entre IIoT sensors, Edge computing, et Cybersecurity framework, c'est la voix qui rappelle que la technologie doit servir la production, pas l'inverse.