

Comment le feed-back des objets renforce la sécurité et la sûreté dans l'Industrie 4.0

Auteur : Johan Kraft est PDG et fondateur de Percepio AB

La boucle de rétroaction d'un périphérique peut être un outil inestimable pour surveiller la sûreté et la sécurité des équipements distribués sur l'Internet des Objets industriel. L'une des caractéristiques déterminantes de l'Industrie 4.0 est la détection distribuée. Cette dernière mouture de l'automatisation industrielle connaît une augmentation spectaculaire des nœuds de capteurs utilisés pour surveiller les équipements et les processus, tous reliés à des dispositifs de passerelle dans un Internet des Objets industriel complexe (IIoT).

Ces capteurs contribuent à améliorer les performances et la fiabilité des processus industriels et à garantir une plus grande disponibilité. L'efficacité accrue est un facteur clé de cette transition vers l'Industrie 4.0, avec un fonctionnement fiable 24h/24 et 7j/7 et des usines dans le monde entier, toutes surveillées à partir d'un seul emplacement. Mais cela nécessite également de se concentrer davantage sur la sécurité du réseau pour garantir un fonctionnement sûr.

Les algorithmes d'apprentissage automatique dans les passerelles qui collectent les données, ou même dans les nœuds de capteurs eux-mêmes, surveillent les performances des équipements industriels. Les données des capteurs peuvent être analysées pour identifier les problèmes de matériel avant qu'ils ne deviennent critiques.

Cependant, ce qui manquait à ce déploiement de l'IIoT, c'était la possibilité de faire de même avec le logiciel. Ces capteurs et passerelles sont des unités de traitement de plus en plus sophistiquées, au code complexe. Alors que la majorité de ce code peut être mature et bien testé, la mise en œuvre des systèmes de l'Industrie 4.0 nécessite de nouveaux logiciels. L'ajout de plusieurs milliers de capteurs augmente aussi considérablement l'ampleur du défi de surveiller les performances des logiciels. Avec une augmentation exponentielle des données, des cas extrêmes d'erreurs d'exécution qui n'étaient pas visibles auparavant peuvent se produire. Cela peut être aussi simple qu'un câble défectueux qui provoque des problèmes de production intermittents ou même l'effet d'un logiciel malveillant provoquant un déni de service distribué (DDoS).

Être capable de tester en profondeur les interactions de milliers de nœuds de capteurs dans toutes sortes de situations différentes avec des latences et des débits de données variables, ainsi que différents algorithmes d'apprentissage automatique et architectures de collecte de données, n'est tout simplement pas possible. Alors que la modélisation numérique peut aider à résoudre cette complexité, le monde réel peut générer des résultats inattendus.

Les systèmes IIoT peuvent être extrêmement complexes. Les capteurs surveillent non seulement les machines en fonctionnement, mais également les composants et les matériaux qui y entrent, ainsi que les produits chimiques liquides ou gazeux utilisés dans le processus. Alors que les systèmes SCADA traditionnels (contrôle de supervision et acquisition de données) gèrent ces paramètres dans des automates programmables industriels (automates programmables ou PLC) avec des seuils hauts et bas, l'avantage de l'Industrie 4.0 est d'optimiser ces seuils avec des changements réguliers. Ceci rend le processus plus efficace avec moins de gaspillage. Ces automates programmables ajoutent désormais des algorithmes d'apprentissage automatique, rendant les décisions clés plus proches de l'équipement pour une latence plus faible et un fonctionnement plus efficace.

Entrez dans la boucle de rétroaction du périphérique

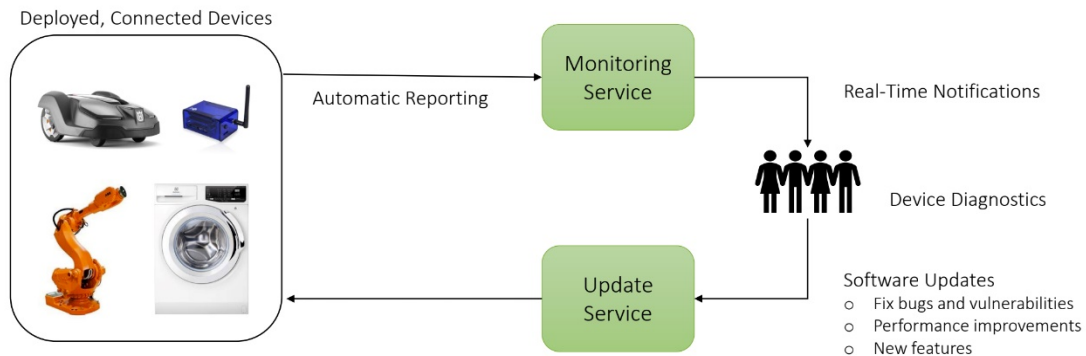
Cependant, cela crée un réseau de périphériques de plus en plus complexe dans l'usine. Et tôt ou tard, l'un des nœuds de périphériques distribués est susceptible de rencontrer des problèmes inattendus. À mesure que le nombre de nœuds augmente, la probabilité d'un comportement problématique augmente également.

Connaître les performances des différents logiciels dans toutes sortes de nœuds de capteurs différents, ainsi que surveiller le logiciel dans chaque passerelle et système de collecte de données est un énorme défi qui rend nécessaire une boucle de rétroaction de périphérique de type DevOps. L'idée de la boucle de rétroaction de périphérique est de fournir une surveillance continue du périphérique et des avertissements automatiques. Cela permet aux développeurs de prendre conscience des problèmes potentiels avant qu'ils ne deviennent un problème sur la chaîne de production. Idéalement, l'avertissement est suffisamment précoce pour qu'un correctif puisse être produit et distribué via une mise à jour en direct avant que la ligne ne soit impactée. Une telle boucle de rétroaction aide les développeurs des systèmes embarqués à améliorer la qualité des logiciels et les performances des produits afin de prendre en charge la fiabilité et l'évolutivité des systèmes de contrôle industriels.

Appel aux agents logiciels

Une approche pour mettre en œuvre une boucle de rétroaction de périphérique réussie consiste à utiliser un petit bloc de logiciel indépendant, appelé agent, dans chaque nœud. Celui-ci doit être relié au réseau de communication et examine le fonctionnement du matériel et des logiciels du périphérique. Cela peut inclure des exceptions matérielles et des données de minuterie de chien de garde, des codes d'erreur du système d'exploitation en temps réel (RTOS), des intergiciels ou des API de pilote de périphérique, ou la capture de données en cas de redémarrage.

En cas de panne, l'agent peut fournir des informations détaillées sur l'état des registres à partir du point de détection, avec des vidages de pile et de mémoire qui permettent de trouver le problème et de le résoudre beaucoup plus rapidement. L'agent peut même suivre l'exécution du logiciel pour montrer ce qui s'est passé juste avant qu'un problème ne soit détecté, fournissant un contexte pour reproduire le problème.



Un agent logiciel dans un équipement industriel peut fournir des données inestimables sur l'Internet des Objets industriel pour identifier tout problème, avant même qu'il ne se produise, et aider à développer rapidement une solution.

Mais il ne s'agit pas seulement d'analyse des défaillances logicielles, mais également d'alertes préventives. La surveillance de certaines métriques telles que l'utilisation de la pile, l'utilisation du tas, la charge du processeur, le stockage et les métriques spécifiques à l'application peut créer les conditions d'avertissements proactifs, tels que « l'utilisation de la pile est supérieure à 95 % », qui signale au développeur qu'un problème peut être imminent.

L'agent peut également être utilisé pour améliorer la qualité des algorithmes de contrôle et les réinjecter dans les tests du système. Des alertes peuvent être générées à partir de n'importe quel événement logiciel d'intérêt, donnant une visibilité sur la façon dont les algorithmes fonctionnent dans la pratique. Cette visibilité n'est tout simplement pas possible autrement et peut aider à améliorer et à affiner les performances du système. Ces enseignements peuvent être appliqués au déploiement de nouvelles usines et à la revalorisation de friches industrielles.

La surveillance est également essentielle pour une cybersécurité accrue

Un autre enjeu clé du contrôle industriel est la sécurité. La plupart des systèmes industriels ont été isolés dans des systèmes en boucle fermée. L'Industrie 4.0 ouvre ces systèmes à un Internet plus large et à des risques de compromission plus élevés. Un agent indépendant avec un canal de communication distinct peut surveiller les performances de chaque nœud et passerelle, en recherchant et en signalant les opérations inattendues. Cela peut être utilisé pour renforcer la sécurité de l'ensemble du système.

Le dernier malware [Pipedream](#) cible délibérément l'automatisation industrielle et les systèmes SCADA. Cela n'exploite pas une vulnérabilité mais utilise les fonctions inhérentes aux contrôleurs logiques programmables (PLC). En conséquence, les autorités américaines recommandent d'utiliser un logiciel de surveillance pour rechercher les mouvements inattendus de données.

Conclusion

Cette surveillance doit être hautement automatisée pour répondre aux applications de contrôle industriel avec des milliers de nœuds de capteurs et de passerelles. L'agent doit être indépendant et robuste, survivre aux pannes logicielles dans le nœud et fournir un canal séparé vers un système centralisé où les développeurs ont un contrôle total, même si cela signifie anonymiser les données pour préserver le caractère privé des données de diagnostic. L'agent doit également être évolutif, avec un faible encombrement-mémoire pour s'adapter aux microcontrôleurs utilisés sur les nœuds de capteurs ainsi qu'aux moteurs Linux des passerelles.

Mais les données doivent aussi être utilisables. Avec plusieurs milliers de nœuds dans une implémentation de l'Industrie 4.0, les alertes automatisées sont essentielles pour mettre en évidence les problèmes, avec des liens directs avec les données pertinentes vers des traces visuelles dans le code qui peuvent montrer rapidement et efficacement ce qui s'est passé. Cela donne au développeur la voie la plus rapide vers une solution, avec une voie de mise à jour en direct pour apporter les modifications, idéalement avant qu'un problème ne se produise réellement et certainement avant qu'il ne soit remarqué.

www.percepio.com