Tendances technologiques

Systèmes SCADA

Architecture d'entreprise, Direction générale du dirigeant principal de la technologie

Version 0.1
Date 2019-07-10

Shared Services Canada
Services partagés Canada

Canada

Table des matières

Sommaire opérationnel

Un système d'acquisition et de contrôle de données (SCADA) est un système informatique (matériel et logiciels) utilisé pour recueillir, analyser et présenter des données en temps réel sur divers aspects des infrastructures et des équipements industriels utilisés dans des industries comme les télécommunications, les services de traitement des eaux et des déchets, ainsi que l'industrie pétrolière et gazière[1].

Un système SCADA peut contrôler les processus industriels sur place ou à distance, surveiller, recueillir et traiter les données en temps réel et interagir directement avec des dispositifs (capteurs, valves, pompes, moteurs, etc.) au moyen d'un logiciel d'interface homme-machine (IHM). Le système consigne aussi les événements dans un journal sur disque dur[2]. De plus, un système SCADA peut déclencher des alarmes en cas de situations dangereuses dans des installations industrielles.

On utilise ces systèmes pour gérer et maintenir l'efficacité, distribuer des données pour permettre des décisions éclairées et communiquer des problèmes liés au système afin de réduire les temps d'arrêt. Les systèmes SCADA sont essentiels dans de nombreuses industries modernes[3].

Même si l'industrie a commencé à utiliser des ordinateurs au cours des années 1950, l'utilisation de systèmes SCADA n'a pas commencé avant les années 1960[4]. Les communications automatisées permettaient alors de transmettre, au moyen de la télémétrie, des données pertinentes de sites éloignés à du matériel de surveillance[5]. La télémétrie permettait d'utiliser des communications automatisées pour transmettre des mesures et d'autres données de sites éloignés au matériel de surveillance.

Le terme SCADA remonte au début des années 1970, lorsque l'utilisation de microprocesseurs et d'automates programmables industriels (API) a ouvert la voie au contrôle et à la surveillance de processus automatisés[6]. Le SCADA et l'infrastructure de mesure avancée (IMA) ont évolué pour en arriver à la technologie et aux dispositifs d'Internet des objets (IdO).

Avant l'introduction du SCADA, les organisations industrielles dépendaient de leur main-d'œuvre pour contrôler et surveiller manuellement l'équipement, au moyen de relais, de minuteries, de compteurs analogiques, de cadrans et de boutons-poussoirs. L'élargissement des espaces industriels a créé le besoin de gérer l'équipement à distance sans qu'il soit nécessaire d'envoyer quelqu'un à l'endroit éloigné pour agir directement[7].

Sommaire technique

Un système SCADA comprend une architecture logicielle et matérielle. De nombreux composants matériels interagissent pour traiter les données et effectuer les activités de contrôle. Le système est centralisé et communique au moyen technologies filaires et sans fil sur les dispositifs clients. Un système SCADA comprend des ordinateurs de supervision, des terminaux à distance (RTU), des automates programmables industriels (API), une infrastructure de communication et une interface homme-machine (IHM). Sont installés sur un ordinateur de supervision les logiciels utilisés pour communiquer avec les connecteurs et les actionneurs sur le terrain. Cela comprend les logiciels de RTU, d'API et d'IHM exécutés sur le poste de travail de l'opérateur. On peut utiliser un RTU ou un API pour relier les capteurs aux actionneurs et les connecter en réseau pour l'échange de commandes et de données avec l'ordinateur de supervision. Aux fins d'exécution de commandes, les RTU utilisent une logique de commande (p. ex., en langage Ladder). Les API fonctionnent de manière semblable, mais peuvent exécuter des commandes plus complexes et sont donc souvent utilisés au lieu de RTU. Un API est un contrôleur rapide qui fournit un temps de réponse quasi réel. Par contre, lors de la mise à l'échelle dans le cadre d'une solution de grande envergure, un système de commande réparti (SCR) est préférable puisqu'il peut traiter un plus grand nombre de points d'entrée-sortie. On utilise une infrastructure ou un réseau de communication pour relier les RTU ou API aux ordinateurs de supervision. Il peut s'agir d'un réseau local ou étendu, en fonction du traitement de données Web à l'interne ou au moyen du nuage d'un fournisseur tiers. Le réseau utilise des protocoles normalisés de l'industrie ou des protocoles de fabrication. Les RTU et PLC fonctionnent de manière autonome avec une latence en temps quasi réel [2]. En cas de panne du réseau, ils continuent à exécuter la dernière commande transmise par l'ordinateur de supervision. L'interface homme-machine permet à l'opérateur de surveiller le système de supervision. Les données sur les installations sont présentées au personnel d'exploitation graphiquement au moyen de schémas synoptiques.

Utilisation par l'industrie

On prévoit que le marché SCADA mondial atteindra environ 21,57 milliards de dollars US d'ici 2023, soit un taux de croissance annuel composé (TCAC) de 9,8 % au cours de la période de prévision. Le segment des solutions et services devrait présenter le TCAC le plus important, soit 11,37 % au cours de la période

de prévision, en raison des besoins de gestion des processus industriels et de connaissances opérationnelles grâce au traitement de quantités massives de données.

Des industries comme la production d'énergie et le raffinage pétrolier et gazier tirent profit des systèmes SCADA depuis une dizaine d'années. AES est une société internationale de production d'électricité qui investit dans de multiples sources d'énergie renouvelable, comme l'énergie hydroélectrique, éolienne, solaire et de biomasse. En 2010, la North Palm Springs Corporation a décidé de mettre en œuvre un système SCADA dans le cadre de son projet AES IV d'énergie éolienne. Le plan était de préparer 49 turbines éoliennes dans le cadre d'un système SCADA et d'alerte. On visait à surveiller la situation des éoliennes et de fournir des mesures de disponibilité. De plus, le système devait valider la quantité d'énergie produite par rapport à la quantité prévue selon la courbe de puissance du fabricant. AES a utilisé un serveur OPC et ne voulait pas intégrer de logiciel au protocole des éoliennes. L'entreprise voulait pouvoir modifier indépendamment le processus de données de l'éolienne et le processus de surveillance. De plus, elle ne voulait pas installer d'IHM sur les ordinateurs clients. Ainsi, les utilisateurs de contrôle à l'extérieur du domaine ne rencontreraient pas de problèmes d'autorisation, mais pourraient néanmoins exécuter des fonctions SCADA. L'entreprise a signalé une grande réduction des coûts de développement et une plus grande efficacité [12].

Pemex est une entreprise pétrolière et gazière qui utilise depuis quelque temps un système SCADA, mais qui a récemment décidé de mettre à jour sa solution. L'objectif était de créer un site efficace de mesure du gaz naturel. Ils voulaient transmettre des calculs complexes sur les débits au site de contrôle des mesures du gaz.

Utilisation par le gouvernement du Canada

Le gouvernement du Canada (GC) utilise beaucoup les technologies de l'information (TI) pour mener à bien ses opérations et ses activités opérationnelles quotidiennes. Les TI jouent un rôle intégral dans le fonctionnement du gouvernement, en plus d'être un catalyseur clé dans la transformation des affaires du GC. Elles constituent également une composante essentielle de la stratégie du GC pour relever les défis liés à la transformation numérique et à l'amélioration des services au public dans l'intérêt des citoyens, des entreprises, des contribuables et des employés[8].

Par contre, puisque les systèmes SCADA sont principalement appliqués dans le cadre des services et de l'équipement industriels, les gouvernements

provinciaux et les administrations municipales sont les principaux organismes publics qui utilisent les technologies connexes. Ces paliers sont responsables de la gouvernance des industries qui relèvent de leurs compétences et de la gestion directe de services industriels.

Par exemple, le gouvernement provincial de l'Ontario utilise des systèmes SCADA au sein de l'Agence ontarienne des eaux, un organisme du ministère de l'Environnement, qui fournit aux clients de l'Ontario des solutions complètes en matière de gestion des eaux et des eaux usées[9].

De même, le gouvernement provincial de l'Alberta utilise des systèmes SCADA pour la gestion de l'eau dans le cadre de multiples projets provinciaux. Le SCADA Data Management System (SDMS) du gouvernement de l'Alberta est installé sur 30 postes de travail et utilise quatre serveurs [13].

Le GC n'utilise peut-être pas les systèmes SCADA à la même échelle que les organismes provinciaux et municipaux, mais Sécurité publique Canada (SP), dans le cadre de son mandat de protéger les infrastructures essentielles, doit renseigner les propriétaires d'infrastructures essentielles sur les enjeux cybernétiques et les pratiques exemplaires liés au SCADA. SP organise des événements sur la sécurité des systèmes de contrôle industriels (SCI) afin d'aider les propriétaires d'infrastructures essentielles au Canada à sécuriser leurs ICS, par exemple les actifs de SCADA et de TI[10].

Répercussions pour Services partagés Canada (SPC)

Proposition de valeur

Les systèmes SCADA sont généralement conçus pour la surveillance et le contrôle de processus industriels et de fabrication, mais il y a quand même des cas d'utilisation potentiellement utiles pour un organisme comme SPC.

Les centres de données ont besoin de systèmes fiables de refroidissement et de gestion de l'alimentation. On peut utiliser des systèmes SCADA pour ces fonctions afin d'améliorer l'efficacité et la fiabilité opérationnelle. On peut ainsi surveiller l'équipement et fournir des données à des appareils mobiles connectés au réseau [7]. Cela simplifie les notifications et le traitement des alarmes afin de réagir plus rapidement aux problèmes de maintenance. On peut activement détecter des situations avant qu'elles ne deviennent des problèmes.

Les systèmes SCADA peuvent fournir de grandes quantités de données sur les installations et l'équipement des centrales, au moyen d'interfaces graphiques, pour connecter des milliers de capteurs d'une grande région dans le cadre d'un système de surveillance et de contrôle des opérations. L'affichage peut être présenté aux opérateurs selon divers formats, en fonction de l'application. Le principal avantage est qu'on peut, au moyen de protocoles et de logiciels sophistiqués, surveiller les données de n'importe où dans le monde et consigner tous les événements en cas de pannes du système[11]. Un système SCADA peut prolonger la durée de vie de l'équipement en permettant aux utilisateurs de formuler des prédictions relatives au cycle de vie. Il peut aussi réduire les coûts de main-d'œuvre grâce à une attribution efficace des ressources de dépannage. Le système permet de choisir l'équipement et les systèmes en fonction du rendement plutôt que de la compatibilité avec le parc actuel.

Lorsqu'on utilise le SCADA pour la gestion des bâtiments, les processus automatisés de journalisation des données et de production de rapports éliminent le besoin qu'un employé effectue ce travail, ce qui réduit les coûts de main-d'œuvre et permet aux analystes de se concentrer sur des tâches plus importantes.

De plus, on peut élargir les processus liés à une installation puisque toutes les données sont stockées dans un seul référentiel. Un système SCADA utilise généralement une base de données pour stocker l'ensemble des données. On peut donc traiter les données à partir de cette base et générer automatiquement des rapports. Un utilisateur peut mettre en valeur des paramètres d'intérêt dans le cadre de la surveillance. On peut attribuer à ces paramètres des seuils et des sévérités pour déterminer quand déclencher des alarmes [1].

Défis

Les défis particuliers liés aux systèmes SCADA dépendent de la nature du système : dans un périmètre ou non. Le système réside-t-il dans un seul bâtiment ou une seule installation ou est-il distribué dans divers emplacements?

Les applications distribuées présentent un plus grand risque. Les principales limitations liées à ces applications sont l'alimentation et les communications. Un système distribué exige une plus grande couverture réseau : le système ne peut se limiter à un réseau local à l'échelle du bâtiment. Le système est donc plus exposé à des cybermenaces, puisqu'un réseau distribué a besoin d'adresses IP,

ce qui pose un défi pour les opérateurs en ce qui concerne l'exactitude et l'efficacité du SCADA.

En général, il y a deux types de menaces pour les systèmes SCADA. Il y a, en premier, la menace d'un accès non autorisé au logiciel de contrôle. Des humains, des virus ou d'autres menaces informatiques pourraient apporter des modifications au serveur de contrôle. Il y a ensuite l'accès possible aux paquets ou aux segments de réseau qui hébergent les dispositifs SCADA. Cette menace se manifeste particulièrement dans le cadre d'une mise en œuvre SCADA distribuée. La sévérité des menaces dépend de la conception et du déploiement du réseau. Le problème peut être particulièrement grave lorsqu'on ajoute un système SCADA à un réseau d'entreprise qui a déjà ses propres protocoles de sécurité et d'authentification [11].

Il y a deux problèmes possibles dans le cadre d'un centre de données. Le déclenchement d'une cascade d'alarmes pourrait masquer la cause sous-jacente du problème. De plus, puisque les réseaux SCADA utilisent des protocoles Internet normalisés, ils sont exposés à des attaques et à des interruptions. Dans le cas d'un centre de données, l'utilisation d'outils de gestion d'infrastructure de centres de données (DCIM) est préférable. Il s'agit encore d'une forme de SCADA, qui comprend la surveillance des données et l'exécution de fonctions de contrôle, mais c'est axé sur le centre de données.

Un autre défi est l'obsolescence croissante des systèmes SCADA. La technologie SCADA se fait dépasser et est absorbée par la technologie et les dispositifs d'Internet des objets (IdO). Le chevauchement fonctionnel entre les exigences et les capacités SCADA et d'IdO augmente constamment dans les systèmes de renseignement industriels et opérationnels.

La complexité des systèmes SCADA fondés sur les automates programmables industriels (API) présente un défi en ce qui concerne les unités matérielles et les composantes dépendantes. Un système SCADA complexe exige des opérateurs, des analystes et des programmes compétents pour créer et maintenir la valeur du système. De plus, l'intégration à distance d'actifs aux systèmes SCADA est complexe.

La connectivité présente un autre défi. Les opérateurs des télécommunications peuvent offrir une bonne couverture dans une région, mais un signal limité dans d'autres. L'obtention de cartes SIM et de forfaits de données de multiples entreprises pour assurer une connectivité fiable et la vérification de la fiabilité et de la puissance du réseau des entreprises pour chacun des emplacements éloignés sont des tâches complexes et dispendieuses.

De plus, la force d'un réseau peut varier considérablement en fonction de conditions imprévisibles comme la météo[12]. La technologie LPWAN (Low Power Wide Area Network) est prometteuse, mais la couverture réseau est encore limitée et les faibles débits restreignent le type, la quantité et la fréquence de transmissions de données. Par contre, de nombreux réseaux LTE cellulaires et satellitaires sont trop énergivores pour permettre des opérations pleinement autonomes de longue durée qui comportent de fréquentes transmissions de données[13].

Considérations

Le GC investit une part importante de son budget annuel en matériel de TI et en infrastructure de soutien. Sans surveillance et visibilité adéquates, les approches de gestion des investissements en TI peuvent être difficiles à appliquer, ce qui pourrait nuire à la prestation efficace des programmes et des services du GC.

Pour SPC, l'utilisation d'un système SCADA pour appuyer la gestion des centres de données d'entreprise peut être utile pour permettre la surveillance des systèmes de refroidissement et de l'équipement de TI sensible. Par contre, SPC doit aussi tenir compte des besoins en infrastructure, en réseaux et en stockage des ministères partenaires pour utiliser des systèmes SCADA dans leurs propres opérations.

La plupart des entreprises auront besoin de compétences à la fois pour développer et pour gérer leurs propres capacités SCADA et pour exploiter les capacités de tiers. SPC doit envisager les talents requis pour les travaux spécialisés nécessaires à la mise en œuvre de systèmes SCADA et pour adapter les services SCADA au matériel existant et aux stratégies ministérielles.

SPC doit s'assurer que les stratégies d'infrastructure à venir comprennent des directives ou orientations en matière de SCADA. Celles-ci devraient tenir compte des besoins opérationnels des ministères partenaires en matière de SCADA et de stockage. SPC devra mettre en place un plan pour gérer les besoins futurs en infrastructure et en réseaux si les ministères partenaires adoptent la technologie SCADA à grande échelle.

SPC doit comprendre comment gérer la mise en œuvre du SCADA pour lui-même et pour les ministères partenaires, en tenant compte de l'obsolescence croissante de cette technologie. La technologie SCADA est dépassée et absorbée par la technologie et les dispositifs d'Internet des objets (IdO). Il s'agit d'une technologie verticale qui est donc particulière à certains types d'industries, comme les services publics. Le SCADA évolue des logiciels

propriétaires vers des systèmes ouverts (Open-SCADA) qui utilisent de plus en plus du matériel et des systèmes d'exploitation courants. Qui plus est, de nombreux besoins de surveillance et de contrôle peuvent être gérés au moyen de plateformes IdO qui comprennent des cadres de source ouverte. De plus, puisque le marché IdO est plus important et répond aux besoins d'un grand nombre de clients grâce à l'interfonctionnalité, cela sera probablement la tendance en matière de surveillance et de contrôle. De nombreuses petites sociétés de services publics peuvent utiliser des modèles Open-SCADA, mais les grandes entreprises continueront d'adopter les plateformes IdO. SPC doit comprendre cette évolution technique et planifier ses activités en conséquence.

En ce qui concerne la sécurité des systèmes SCADA, SPC peut prendre diverses mesures pour atténuer les risques. Des limites strictes en matière de gestion de l'accès et des autorisations seront nécessaires pour les connexions externes, particulièrement en ce qui concerne les réseaux SCADA distribués.

On peut aussi utiliser des réseaux privés virtuels (RPV) pour améliorer la sécurité. Les chemins d'accès au réseau interne doivent être restreints. Cela comprend le chiffrement des fichiers, des répertoires et des courriels ainsi que l'élaboration de méthodes de contrôle et de surveillance qui tiennent compte des imprévus liés à l'équipement SCADA. Il est important de balayer les systèmes SCADA pour détecter les vulnérabilités. L'application de correctifs de sécurité demeure la solution la plus efficace. Les logiciels de contrôle SCADA devraient utiliser, à titre de mesures de protection, des contrôles d'authentification, d'autorisation et de journalisation au niveau de l'utilisateur.

SPC devrait examiner la possibilité d'évaluer le catalogue de services actuel afin de déterminer les situations pour lesquelles le SCADA peut être mis à profit afin d'améliorer l'efficacité, de diminuer les coûts et de réduire le fardeau administratif manuel en ce qui concerne les services existants. On doit aussi déterminer comment intégrer le SCADA de manière uniforme aux services existants. Tous les nouveaux appareils ou plateformes acquis (p. ex., Terraform ou AWS) doivent avoir une valeur élevée sur le marché et doivent pouvoir être facilement intégrés au réseau du GC. SPC ne doit pas appliquer dès le départ le SCADA aux applications essentielles en production. Il doit plutôt créer des projets pilotes et des grappes d'essai, puis élargir la portée des solutions retenues. Comme pour les nouvelles technologies infonuagiques, l'utilisation de projets pilotes est recommandée. On doit d'abord mettre l'accent sur un nombre limité d'objectifs et un scénario simple (une seule application) dans le cadre des essais.

Références

1. https://www.quora.com/What-are-the-benefits-of-a-SCADA-System
2. https://www.elprocus.com/scada-systems-work/
3. https://www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf
4. https://www.dpstele.com/scada/tutorial-white-paper.php
5. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf
6. https://www.manufacturing.net/article/2017/04/scada-data-center
7. https://www.datacenterknowledge.com/archives/2014/04/16/optimizing-power-system-monitoring-control
8. https://www.csemag.com/articles/selecting-a-critical-power-monitoring-and-control-technology/
9. https://iiot-world.com/smart-manufacturing/values-challenges-scada-systems-outside-fence-applications/
10. https://www.parasyn.com.au/article/the-top-5-problems-with-scada-systems/
11. https://journals.sagepub.com/doi/pdf/10.1155/2012/268478
12. https://iconics.com/Production/media/Literature/SuccessStories/ss-AES.pdf
13. https://ca.linkedin.com/jobs/view/scada-systems-support-specialist-at-government-of-alberta-1068747485
14. https://www.marketwatch.com/press-release/scada-market-2019-global-industry-share-size-future-demand-global-research-top-leading-players-emerging-trends-region-by-forecast-to-2023-2019-05-09

[1] https://www.webopedia.com/TERM/S/SCADA.html
[2] https://inductiveautomation.com/resources/article/what-is-scada
[3] https://inductiveautomation.com/resources/article/what-is-scada
[4] https://www.webopedia.com/TERM/S/SCADA.html
[5] https://www.theearthawards.org/a-brief-history-of-the-scada-system/
[6] https://www.theearthawards.org/a-brief-history-of-the-scada-system/
[7] https://www.theearthawards.org/a-brief-history-of-the-scada-system/
[8] https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12755
[9] http://www.ocwa.com/who-we-are
[10] https://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/ndstrl-cntrl-sstms/vnts-fr.aspx
[11] https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-SCADA.html
[12] https://iiot-world.com/smart-manufacturing/values-challenges-scada-systems-outside-fence-applications/
[13] https://iiot-world.com/smart-manufacturing/values-challenges-scada-systems-outside-fence-applications/