Étude de cas : Mise en œuvre d'une méthode sans intervention utilisant SDN pour améliorer la sécurité, la fiabilité et l'ingénierie des systèmes d'automatisation de poste électrique en Slovénie

Darko Bordon
ELES, d.o.o.

Robert Meine, Sagar Dayabhai et Jason Dearien
Schweitzer Engineering Laboratories, Inc.

Présenté à la
Conférence mondiale PAC 2023
Glasgow, Royaume-Uni
Du 26 au 29 juin 2023

Traduit en français en novembre 2023

Étude de cas : Mise en œuvre d'une méthode sans intervention utilisant SDN pour améliorer la sécurité, la fiabilité et l'ingénierie des systèmes d'automatisation de poste électrique en Slovénie

Darko Bordon, ELES, d.o.o.

Robert Meine, Sagar Dayabhai et Jason Dearien,
Schweitzer Engineering Laboratories, Inc.

Courriel : papers@selinc.com

Royaume-Uni

1. Introduction

L'utilisation de dispositifs électroniques intelligents (DEI) modernes a amélioré le niveau d'intégration et d'information existant dans le système d'automatisation de poste électrique. Ces DEI et applications permettent aux entreprises de service public comme ELES d'exploiter le réseau électrique de manière plus économique et plus sûre, d'améliorer l'efficacité et d'accroître la disponibilité et la fiabilité du réseau. Ils facilitent en outre l'exploitation et la maintenance à long terme, améliorent les temps de restauration du système, permettent un diagnostic rapide et une notification rapide des alarmes et des évènements anormaux dans le réseau électrique.

Pour de nombreux services publics, le déploiement de grands réseaux de communication pour faciliter les systèmes d'automatisation de poste électrique a posé de nombreux défis en matière de sécurité et de gestion de la technologie. Les normes des commutateurs gérés basés sur le protocole d'arbre maximal rapide (RSTP) ne sont pas non plus conçues pour répondre aux exigences de performance et de fiabilité qui sont essentielles pour le réseau électrique. Dans le domaine des infrastructures critiques, les solutions plug-and-play et les solutions dans la mesure du possible (best-effort) ne suffisent tout simplement pas.

La configuration des dispositifs de mise en réseau suivant les réglages appropriés sur la base d'une conception efficace, évolutive et sécurisée peut être un processus long qui exige des coûts de main-d'œuvre et des ressources élevés. En outre, le réseau électrique est une cible de choix pour les cyberattaques, c'est pourquoi les réseaux Ethernet modernes de technologie opérationnelle (OT) doivent être conçus dans un souci de sécurité afin d'assurer une protection contre les cybermenaces. La compromission de ces réseaux peut entraîner des pannes généralisées, des dommages aux équipements et au personnel. Ces difficultés sont encore plus marquées dans les postes électriques de grande taille et lorsqu'on envisage des communications entre postes pour des applications de protection et contrôle. Ces difficultés sont encore plus marquées dans les postes électriques de grande taille et lorsqu'on envisage des communications inter entre postes électriques pour des applications de protection et contrôle.

Ce document explore les avantages de la mise en réseau défini par logiciel (SDN) de la technologie opérationnelle et la manière dont cette solution peut être utilisée pour répondre aux exigences rigoureuses des réseaux OT. Au travers d'une étude de cas réelle, ce document aborde plusieurs défis auxquels sont confrontées les entreprises de service public lors de la mise en œuvre d'un réseau OT sécurisé pour les systèmes d'automatisation de poste électrique et propose une approche de déploiement sans intervention (Zero-Touch) (ZTD) pour concevoir un réseau sécurisé ayant un comportement reproductible et prévisible. Cette approche renforce la cybersécurité, exploite les éléments communs des technologies de l'information et de l'espace OT (par exemple, utilisation du réseau IP/commutation multiprotocole par étiquette (MPLS)) tout en préservant un équilibre dans leur convergence, réduit les coûts d'ingénierie et de mise en service, et améliore la gestion du réseau et la prise de conscience de la situation.

2. Contexte

Des recherches préalables sur les tendances de développement des équipements de communication, de protection et contrôle, menées par le département des systèmes secondaires de l'opérateur de réseau de transport ELES, ont permis de mettre en place un réseau de transport stable, disponible, sûr et plus fiable en Slovénie.

Cette étude de cas découle de la construction d'un nouveau poste électrique de 400/110 kV et de nouvelles lignes électriques de 400 kV vers la Hongrie et la Croatie par l'opérateur de réseau de

transport (TSO) ELES entre 2018 et 2022. Cette construction a également été à l'origine de l'introduction de nouveaux concepts et de nouvelles technologies dans le domaine des systèmes secondaires. Par la suite, il s'est avéré nécessaire de franchir une nouvelle étape dans le domaine des communications relatives aux systèmes secondaires, étant donné que les concepts et les technologies associées dans le secteur de l'énergie n'ont cessé d'évoluer et d'être régulièrement mis à jour.

La décision de recourir au protocole de communication GOOSE, basé sur la norme CEI 61850, pour un nouveau poste électrique à des fins de verrouillage et de téléprotection nécessitait non seulement un réseau fiable et disponible favorisant le transfert de données à grande vitesse, mais aussi un réseau résilient et cybersécurisé. Cette exigence a nécessité la prise de plusieurs décisions innovantes au cours de la phase de conception du projet de construction du nouveau poste électrique.

La première décision a été de créer un réseau de communications pour la barre de poste CEI 61850. La topologie choisie pour la barre de poste était d'utiliser le protocole de redondance parallèle (PRP) basé sur la norme CEI 62439-3:2016 [1]. Cette approche a été rendue nécessaire pour plusieurs raisons. La redondance totale permet non seulement une communication fiable, mais présente également des avantages lors de la maintenance du poste électrique et de la mise à niveau du réseau, car elle assure une performance ininterrompue pour toutes les communications au sein de la barre de poste CEI 61850.

ELES possède une expérience considérable dans l'utilisation de GOOSE, en particulier lorsqu'il s'agit d'appliquer le protocole aux ordinateurs de la baie. La deuxième décision a donc été d'utiliser les communications GOOSE à des fins de protection, à la fois pour l'envoi de commandes de déclenchement et pour les signaux d'envoi et de réception entre les postes électriques (comme décrit dans l'étude de cas ci-dessous). Cette solution éliminerait également la nécessité pour les dispositifs de téléprotection d'envoyer les signaux par l'intermédiaire du réseau SDH ou MPLS d'ELES.

La troisième décision a été prise sur la base des tests rigoureux de la technologie OT SDN pour les commutateurs de réseau, qui ont débuté en 2016. Il est devenu évident que l'introduction de la technologie SDN nécessitait une approche totalement nouvelle de l'ingénierie des réseaux. Au cours de la phase de test, il a été observé que la technologie SDN améliorait la cybersécurité, la fiabilité du réseau et la disponibilité du système et s'avérait être une excellente solution sécurisée pour l'échange de données entre les postes électriques. L'utilisation de la technologie SDN par ELES et la confiance qu'elle inspire ont conduit à la quatrième décision, qui consistait à utiliser la barre de poste CEI 61850 récemment mis au point et un pare-feu de nouvelle génération pour fournir un accès à distance à des fins de protection et contrôle. Cela a permis de se passer d'un réseau dédié pour l'accès à distance aux dispositifs de protection et contrôle.

3. SDN

L'utilisation de la technologie SDN par les opérateurs de réseau de transport dans le monde entier pour leurs installations d'infrastructures critiques est en constante augmentation. Ces installations utilisent des configurations très statiques pour les dispositifs et attendent des communications machine à machine cohérentes et très performantes pour effectuer des transferts de données à grande vitesse pour les systèmes de protection critiques. Nombre de ces systèmes doivent fonctionner de manière fiable, même en cas de défaillance du réseau, en moins de 3 ms, conformément à la norme CEI 61850-5 [2].

La technologie des commutateurs gérés basée sur le protocole RSTP ne convient pas aux réseaux OT critiques. Tout d'abord, elle repose sur la confiance pour permettre aux dispositifs de communiquer facilement entre eux en modifiant automatiquement le plan de données utilisé par le réseau pour déplacer les paquets sur la base d'un trafic réseau dynamique et non fiable. Ce comportement rend le réseau et les dispositifs connectés sensibles à de nombreuses vulnérabilités en matière de sécurité et de performances, notamment l'empoisonnement du protocole de résolution d'adresse (ARP), l'usurpation d'identité MAC et les attaques par déni de service. Deuxièmement, les réseaux traditionnels utilisent souvent des mécanismes de rétablissement très lents, comme le protocole d'arbre maximal rapide (RSTP), qui rétablissent le réseau en cas de défaillance d'un dispositif ou d'une liaison. Le temps nécessaire au réseau pour se rétablir varie considérablement, de 10 millisecondes à 30 secondes, en fonction de la topologie du réseau et de l'importance du trafic. Lors de ces évènements de reconvergence, de grandes quantités de trafic peuvent être interrompues, entraînant une perte de communication, ou le trafic peut être dupliqué, entraînant des messages hors séquence pouvant désactiver la protection.

L'utilisation de l'OT SDN atténue ces défis en fournissant un plan de données entièrement en refus par défaut qui déplace les paquets sur la base d'un provisionnement de circuits redondants proactifs et géré par le trafic, ou ce que la technologie SDN qualifie de « flux ». Ces flux sont préconçus sur la base des communications souhaitées entre les différents dispositifs du réseau et sont optimisés pour déplacer le trafic aussi rapidement que possible en fonction de la priorité du message et, en cas de défaillance du réseau, pour acheminer automatiquement les paquets par le biais d'une voie de réseau alternatif sans avoir recours à de longs algorithmes de reconversion. Ces avantages sont possibles parce que la technologie OT SDN utilise une méthode « match-then-action » (appariement puis action) qui permet de reconnaître la signature d'un paquet Ethernet et de l'envoyer à la bonne destination sur la base de règles prédéterminées. Cela signifie qu'il n'y a pas d'algorithmes d'apprentissage dynamique susceptibles d'être manipulés à des fins d'attaques ou de reconnaissance de réseaux malveillants. La technologie OT SDN ne déplace les paquets que sur la base de règles prédéfinies, ce qui signifie qu'elle est intrinsèquement en refus par défaut. Étant donné que les voies empruntées par le trafic à travers le réseau sont calculées au moment de la conception, il est également possible de précalculer les voies de défaillance, de sorte qu'en cas de défaillance d'un câble ou d'un commutateur, la voie que le trafic doit emprunter est déjà connue, ce qui réduit le temps de rétablissement à moins de 100 µs dans certains commutateurs OT SDN disponibles dans le commerce.

Le SDN découple la fonctionnalité de gestion du réseau et de configuration des commutateurs du matériel de commutation et la place dans un contrôleur de SDN centralisé appelé plan de contrôle. La charge de traitement des commutateurs s'en trouve allégée, ce qui permet d'améliorer la fiabilité et les performances. Ce découplage permet de gérer les commutateurs SDN de manière centralisée, ce qui présente plusieurs avantages :

- Aucun accès physique aux commutateurs n'est nécessaire pour effectuer les changements de configuration.
- Le provisionnement des circuits de bout en bout est possible pour la fourniture de services et d'applications entre les dispositifs, indépendamment de la taille du réseau ou de la topologie. Le contrôleur de SDN est chargé de la configuration du réseau, fournit automatiquement les circuits de bout en bout nécessaires et configure les commutateurs SDN.
- La gestion centralisée et la prise de conscience de la situation à l'aide du contrôleur de SDN fournissent une visibilité complète de tous les réseaux OT de postes électriques.
- Les commutateurs SDN peuvent fonctionner de manière autonome sans le contrôleur de SDN une fois la configuration appliquée.

4. Étude de cas

Figure 1 décrit l'architecture du réseau du poste électrique nouvellement construit par ELES.

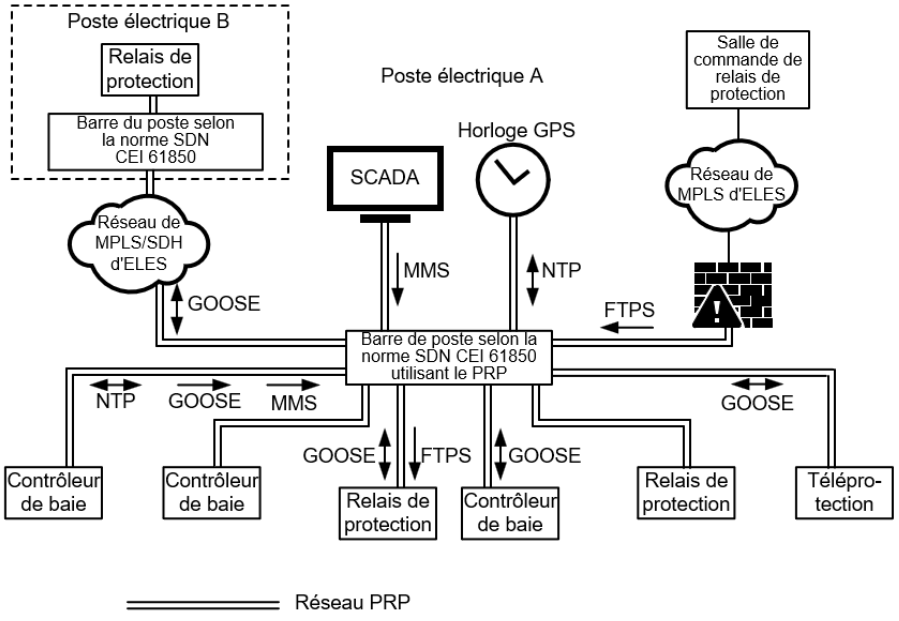

Figure 1 Architecture du réseau du poste électrique ELES.

La mise en place de la technologie SDN a nécessité l'aide de spécialistes des réseaux SDN, car elle a exigé de nouveaux aspects et principes de construction des réseaux. Il fallait répondre à trois questions fondamentales, à savoir :

1. Combien de dispositifs communiqueront sur le nouveau réseau du poste électrique ?
2. Quels sont les flux de communications et de données entre les dispositifs du poste électrique ?
3. Quel système de classe de service (CoS) peut être appliqué sur le réseau ?

Outre la barre de poste CEI 61850, la conception prévoyait l'utilisation d'un réseau à nœud connecté unique (SAN ou Single Attached Node) distinct pour les DEI tels que les compteurs de qualité de l'énergie et compteurs tarifaires, les unités de mesure de phaseur (PMU), les dispositifs de surveillance du transformateur et les dispositifs de commutation de réacteur.

4.1 DEI du poste électrique

Le poste électrique comprenait 25 ordinateurs de baie, 70 DEI multifournisseurs, trois régulateurs de tension, trois dispositifs de commutation de transformateur synchrone et de réacteur, 16 dispositifs de téléprotection, un moniteur de localisation de défauts à ondes progressives, deux plateformes de passerelle d'automatisation de poste électrique et de centre de commande, une plateforme informatique de télésurveillance et d'acquisition de données (SCADA), une horloge GPS (serveur de protocole de temps de réseau [NTP]) et un pare-feu de gestion unifiée des menaces (UTM). L'UTM sert de pare-feu de protection des frontières et d'interconnexion avec le centre de commande SCADA et facilite également l'accès à distance aux DEI de protection. En outre, des connexions indépendantes existent sur la barre de poste CEI 61850 pour le transport de messages GOOSE entre les postes électriques à des fins d'envoi de signaux d'émission/réception de supports. L'utilisation du SDN prend en charge le provisionnement de circuits de communication physiques indépendants entre les postes électriques. Chaque circuit repose sur le PRP, le réseau local (LAN) A communiquant sur le réseau MPLS d'ELES et le LAN B communiquant sur le réseau de SDH d'ELES. Le réseau SAN se compose de 28 compteurs, 13 PMU, 4 dispositifs de qualité de l'énergie, 2 dispositifs de surveillance du transformateur et 1 dispositif de surveillance des réacteurs.

Il a été observé que peu d'interactions et de transferts de données étaient nécessaires entre les niveaux de tension. L'utilisation de SDN a permis de répartir le réseau entre les différents niveaux de tension. Cela a permis à ELES de faire fonctionner le réseau du poste électrique de 400 kV sans interruption si le système de 110 kV est indisponible. Cette répartition facilite également le dépannage du réseau et fournit un mécanisme permettant d'étendre le système et de gérer l'augmentation du trafic sur le réseau pour l'expansion et le provisionnement de l'utilisation des valeurs échantillonnées sur le système lors des futures mises à niveau.

4.2 Flux de données de communication

Pour préparer le profil de communication et le flux de données de tous les DEI du réseau, comme le montre la Figure 1, il faut comprendre les échanges de communication qui ont lieu entre les DEI. Des dispositions ont dû être prises pour les échanges de données suivants :

- Chaque dispositif communique avec l'horloge GPS (serveur NTP) pour la synchronisation temporelle
- Le poste électrique et l'ordinateur SCADA communiquent avec tous les DEI du poste électrique pour en assurer la surveillance et le contrôle
- L'ordinateur de la baie communique les informations relatives à l'installation pour le verrouillage
- Communication pour la configuration du dispositif
- Communications à distance pour la saisie d'enregistrements de perturbations provenant de DEI de protection
- Communications à distance pour l'accès d'ingénierie à distance

Les manuels d'utilisation des fabricants d'équipements ont été utilisés pour déterminer le type de trafic et de flux de données existant pour chaque type de dispositif. Dans les cas où ces informations n'étaient pas disponibles, des analyseurs de réseau ont été utilisés pour inspecter le trafic provenant du

dispositif. Une quantité considérable d'informations a été recueillie grâce à cet exercice concernant les profils de communication de chaque dispositif. Ces informations ont été utilisées pour définir le trafic qui devrait être autorisé sur le réseau SDN. Le trafic appris, tel que présenté dans la Figure 1, comprenait le MMS CEI 61850, NTP, GOOSE, les paquets de surveillance PRP, FTPS, les interruptions SNMP, et divers ports TCP/UDP pour les logiciels d'ingénierie des dispositifs, etc.

4.3 Priorisation du trafic

À l'aide des données recueillies sur le type de trafic existant sur le réseau, un régime de CoS a été appliqué sur la base des lignes directrices en matière de communication définies dans la norme CEI 61850-90-4 [3]. La priorité absolue a été attribuée à la transmission des messages GOOSE de déclenchement et de protection de distance. Par la suite, une priorité légèrement inférieure a été définie pour les messages GOOSE utilisés pour l'enclenchement. Tous les MMS et autres trafics se sont vu attribuer une priorité inférieure à celle de tous les messages GOOSE. Par la suite, les documents de conception ont dû être préparés pour le ZTD sur la base des informations recueillies.

5. ZTD

Le déploiement de commutateurs de réseau dans l'environnement OT est devenu une tâche complexe qui exige des ingénieurs qu'ils procèdent à la configuration et à la gestion des micrologiciels pour chaque commutateur de réseau. La configuration des commutateurs de réseau avec les applications, la sécurité, la redondance et les réglages de gestion d'utilisateur et du réseau appropriés peut être un processus laborieux. Ces tâches sont encore accrues en fonction de la taille et de la complexité du réseau OT. Au fur et à mesure que le nombre de dispositifs augmente dans le réseau électrique, la gestion des dispositifs et du réseau peut devenir extrêmement complexe et l'expansion du réseau peut provoquer des perturbations dans les réseaux stratégiques et frustrer les ingénieurs chargés de l'exploitation et de la maintenance. Par conséquent, une solution est nécessaire pour assurer la configuration et la gestion des équipements de réseau sur l'ensemble du cycle de vie des équipements/systèmes et du processus de développement de la solution, afin de faciliter ces tâches.

5.1 Le concept de ZTD

Le concept de ZTD est largement déployé dans l'environnement informatique et commercial [4]. Il permet d'approvisionner un dispositif sans qu'un ingénieur n'ait à configurer manuellement chaque commutateur du réseau [5]. En outre, il réduit le temps nécessaire pour déployer des commutateurs de réseau sur le système. Ce concept plug-and-play n'est pas nouveau dans le domaine de la mise en réseau et peut être utilisé pour fournir différents niveaux d'automatisation pour la configuration et la gestion du réseau. L'utilisateur peut ainsi configurer un réseau entier à l'aide d'une plateforme entièrement orchestrée et réaliser des circuits de communication de bout en bout ou la fourniture de services d'applications sur le réseau [6].

ZTD relève plusieurs défis auxquels sont confrontées les entreprises de service public en matière de configuration et de gestion d'un grand nombre de dispositifs de mise en réseau. Cela comprend les points suivants :

- Coût/effort - le processus de configuration de chaque dispositif est coûteux, nécessite un effort important et est sujet à des erreurs [7]. Ce processus est simplifié et rentable à l'aide de l'approche ZTD.
- Évolutivité - la configuration manuelle de chaque commutateur de réseau complique la configuration des grands réseaux et fait de l'extension du réseau une tâche difficile qui nuit à l'évolutivité du réseau. Le ZTD permet de relever ce défi à l'aide des circuits de communication de bout en bout sans avoir à se soucier de la voie de communication, de la redondance et de la configuration de chaque commutateur individuel, ce qui simplifie considérablement la configuration du réseau et en améliore l'évolutivité.
- Interopérabilité - chaque fabricant de commutateurs a sa propre méthode de configuration du dispositif de réseau. La prise en charge des normes ouvertes et des interfaces de programmation d'applications (API) pour la configuration et la gestion du réseau fournit une grande flexibilité d'utilisation de ZTD pour automatiser entièrement la configuration du réseau.

Sur la base de ce qui précède, il a été décidé d'utiliser ZTD avec le contrôleur de SDN pour automatiser entièrement la configuration du réseau des commutateurs OT SDN dans le réseau d'ELES. Cela a conduit à la mise au point d'un outil automatisé de configuration, de gestion et de diagnostic du réseau qui sera utilisé pour configurer les commutateurs du réseau SDN et communiquer avec le contrôleur

de SDN (à l'aide d'une API REST ouverte) afin de fournir des circuits de communication complets de bout en bout entre les DEI [8].

5.2 Exigences

Les exigences spécifiques peuvent varier selon les programmes ZTD. Les exigences spécifiques les plus courantes sont les suivantes :

- Le besoin d'une infrastructure de communication pour soutenir le programme de déploiement. Dans ce cas, cela était fait au moyen du réseau IP/MPLS d'ELES.
- Un outil ZTD entièrement automatisé qui peut configurer chaque commutateur de réseau automatiquement sur l'ensemble du réseau.

Au cours de la phase de conception de l'outil ZTD, deux catégories de spécifications ont dû être prises en considération pour répondre aux exigences d'ELES en matière de mise en réseau. Il s'agit des spécifications de l'outil lui-même et du niveau d'automatisation de mise en réseau requis. La seconde catégorie comprenait les données préalables et le format des données dont l'outil avait besoin pour se préparer à ZTD et pour configurer et gérer le réseau avec succès. Ces deux catégories sont décrites en détail ci-dessous.

5.2.1 Spécification de l'outil ZTD

L'outil ZTD doit pouvoir fournir une visibilité sur de nombreux aspects du système. Il doit être en mesure de visualiser la conception souhaitée du système de manière à ce qu'elle puisse être examinée par différents experts en la matière avant d'être déployée. En fonction de la tâche, cette visualisation peut prendre différentes formes, telles que des listes d'hôtes détaillées et des détails de connexion à l'usage des installateurs pour s'assurer que les données adéquates sont collectées. Au nombre des spécifications de l'outil ZTD figuraient les suivantes :

- Une méthode permettant de préciser les adresses IP, les emplacements physiques et les connexions des DEI et des commutateurs.
- Il est facile de spécifier la configuration de la communication entre les DEI à l'aide des alias pour les protocoles et les hôtes.
- Plusieurs postes électriques/réseaux/configurations devraient être représentés dans les mêmes documents de configuration. L'outil ZTD devrait gérer intelligemment la séparation des données afin de garantir que seuls les circuits et postes électriques souhaités sont configurés.
- Un processus devrait être mis en œuvre pour reproduire intégralement l'ensemble du réseau à partir d'un seul ensemble de documents de configuration. Cette approche facilitera également la production d'un comportement reproductible et prévisible.
- L'outil devrait comporter un mécanisme permettant de vérifier la conception par rapport à la configuration et de vérifier la configuration par rapport à ce qui a été déployé sur le réseau. Par conséquent, des rapports devraient être mis à la disposition d'ELES pour montrer la différence entre le réseau actif et la configuration souhaitée.
- Lors de l'application des modifications au réseau, l'outil ZTD ne devrait mettre à jour que les différences sur l'ensemble du réseau. Les circuits de communication existants ne devraient subir aucune modification. Il doit être possible d'effectuer à tout moment un contrôle de l'état du réseau ou un rapport sur les différences afin de s'assurer que la configuration active correspond à la conception souhaitée. Un rapport montrant les différences éventuelles doit être créé s'il en existe. Ce rapport sur les différences serait utilisé lors de la maintenance ou des modifications du réseau pour s'assurer que les changements souhaités correspondent à ce qui est prévu avant de les appliquer au système actif.
- Lors du déploiement automatique de la configuration du réseau, toute erreur constatée pendant le déploiement doit être signalée à l'utilisateur.

L'outil ZTD devrait également fournir une série de rapports pouvant être utilisés par ELES au cours du cycle de vie du réseau d'ELES. Les rapports détaillant chaque circuit de communication fourni dans le système doivent être disponibles pendant l'essai d'acceptation en usine (FAT) et l'essai d'acceptation sur site (SAT) afin de permettre une vérification complète de toutes les communications autorisées sur le système. Étant donné qu'il détaille toutes les conversations autorisées sur le réseau et qu'il inclut les détails des dispositifs concernés, ce rapport peut être utilisé lors de la résolution de tout problème de

communication. Ce même rapport peut être utilisé pour des rapports périodiques de référence et d'audit afin de vérifier l'état du système. En raison de la nature du refus par défaut du système SDN, le dépannage est grandement amélioré par l'examen des compteurs de flux et des paquets refusés par la configuration actuelle du réseau, qui sont tous deux disponibles auprès du contrôleur de SDN.

5.2.2 Préparation pour Zero-Touch

L'ensemble de la configuration de chaque aspect du réseau doit figurer dans les documents de configuration. Ces documents peuvent ensuite être utilisés par l'outil ZTD comme condition préalable pour se connecter au contrôleur de SDN et automatiser la configuration du réseau. Les conditions préalables à l'utilisation de l'outil ZTD sont les suivantes :

- Dresser une liste des applications et des protocoles utilisés sur le réseau.
- Comprendre la topologie du réseau.
- Documenter les exigences de redondance en tenant compte des nœuds à rattachement double et des réseaux de stockage SAN.
- Planifier la voie de communication.
- Réaliser un audit du site et/ou saisir et analyser le trafic d'un réseau Ethernet traditionnel pour comprendre le flux de données et les profils de communication.
- Comprendre les exigences en matière de latence et de gigue.
- Analyser les contraintes liées à la bande passante et à l'infrastructure du réseau étendu (WAN) (le cas échéant). Cela comprend l'emplacement du contrôleur de SDN et de l'outil ZTD, ainsi que la connectivité à tous les commutateurs de réseau pour la configuration et la gestion.

Un modèle Microsoft Excel a été utilisé pour documenter les informations de réseau susmentionnées pour chaque poste électrique afin que l'outil ZTD puisse utiliser directement la configuration du réseau et l'automatiser. La Figure 2 illustre le flux de travail utilisé par l'outil ZTD.

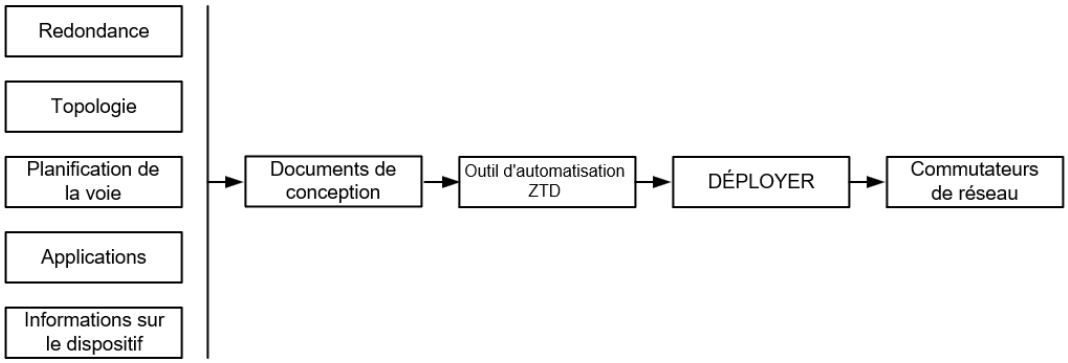

Figure 2 Flux de travail de l'outil ZTD développé pour le déploiement SDN.

5.3 Description fonctionnelle

Cet outil ZTD peut être décrit en trois fonctions générales : 1) Conception 2) Configuration 3) Diagnostic, comme l'illustre la Figure 3. Il ne s'agit pas d'un processus à sens unique, mais chaque fonction est affectée par l'autre et affecte d'autres fonctions. Par exemple, si un circuit manque après l'application de la configuration, la conception est mise à jour et la configuration actualisée est appliquée.

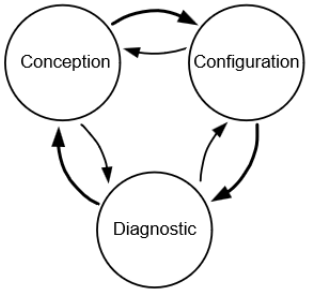

Figure 3 Flux de travail représentant les principales fonctions du ZTD.

5.3.1 Conception

L'objectif de la conception est de disposer d'une méthode indépendante du système pour compiler et partager des informations avec toutes les parties prenantes d'ELES. La documentation n'a pas besoin d'être complexe, mais elle devrait être lisible par l'homme. Une description simplifiée de la documentation de ce système est présentée ci-dessous.

La conception de ce système comprenait deux parties générales : la description des DEI et les circuits. La partie conception des DEI a consisté à documenter les dispositifs en indiquant les paramètres tels que le nom, l'adresse IP pour les hôtes et les réglages spécifiques des commutateurs, tels que l'adresse IP et l'adresse IP du contrôleur utilisées pour la configuration des commutateurs. La partie circuits de la conception se compose de trois parties : les DEI documentés précédemment, les profils de communication et les circuits de communication spécifiques. Les profils de communication fournissent un modèle auquel on peut se référer pour définir les circuits de communication spécifiques.

Tableau 1
Bref exemple de définition d'un profil

Nom	Destination Ethernet	VLAN ID (VID)
GOOSE M2M	01:0C:CD:00:00:01	123

Comme le montre le Tableau 1, un profil est créé pour une application machine à machine (M2M) GOOSE qui définit les informations de configuration utilisées par le commutateur lors de la génération du circuit : en particulier l'adresse MAC et le VID attribués au protocole.

Tableau2
Bref exemple de conception d'un dispositif et d'un circuit

Dispositif	Profil de communication	Destination
Dispositif de téléprotection	NTP Client	Serveur du NTP
	GOOSE M2M	Relais de protection 1
Relais de protection	NTP Client	Serveur du NTP

Comme le montre le Tableau2, un utilisateur a défini deux DEI, ainsi que le profil utilisé pour communiquer avec le(s) destinataire(s). Certains trafics dérivables, comme le protocole de résolution d'adresse. (ARP), le plus courant, n'ont pas besoin d'être spécifiés, sauf cas particulier. Si un dispositif communique avec un protocole IP monodiffusion (unicast) tel que le MMS au sein du réseau local, l'ARP doit être présent, de sorte que le circuit de communication peut être généré automatiquement par l'outil ZTD et n'a pas besoin d'être documenté explicitement.

La plupart des DEI hôtes sont constitués de relais de protection, de contrôleurs de baies, de serveurs SCADA et d'horloges GPS. Toutefois, d'autres dispositifs sont également présents, notamment des commutateurs de réseau et des routeurs MPLS. L'outil ZTD a introduit un algorithme de coloration intelligente des paquets à l'aide des identifiants de réseau local virtuel (VID), dans le but de faciliter et d'automatiser la création de règles SDN (ou flux) nécessaires pour les communications sur l'ensemble du réseau WAN MPLS. Étant donné que le réseau MPLS nécessitait une coloration des paquets, la conception comprenait également le VID nécessaire et la configuration permettant d'appliquer la coloration.

Il s'agit également à la conception d'attribuer à chaque port de dispositif une désignation de réseau, c'est-à-dire le réseau auquel il appartient et le poste électrique. Dans le cas du réseau, il peut s'agir d'un SAN ou de l'un des réseaux PRP (LAN A ou LAN B) avec une interface appartenant à chacun d'eux. Ainsi, un dispositif PRP dans le poste électrique X aurait deux ports, l'un appartenant au réseau X et au LAN A et l'autre à X et au LAN B. Un port SAN serait connecté à X et au SAN. Ces réseaux permettent une division intelligente des dispositifs qui peuvent former une collection minimale à laquelle appliquer une configuration.

5.3.2 Configuration

La synchronisation de la conception avec le système comporte deux étapes générales : 1) la configuration initiale des commutateurs de réseau SDN et l'ajout des réglages pour les DEI au contrôleur de SDN afin que les voies traversant les postes électriques soient identifiées, et 2) l'application des circuits de communication de bout en bout aux commutateurs de réseau de sorte que les communications entre les dispositifs soient possibles sur les voies identifiées. Cette configuration

est appliquée par l'outil ZTD qui vérifie intelligemment les différences de configuration et applique les modifications nécessaires.

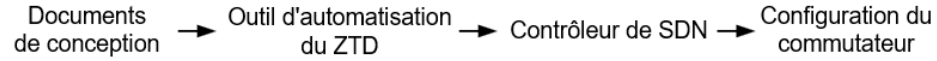

Figure 4 Flux de travail de la configuration du réseau.

Le principal avantage de l'automatisation est que les documents de conception ont été utilisés pour générer directement l'ensemble de la configuration et que les processus de configuration manuels ont été exclus, comme le montre la Figure 4. Le mécanisme de contrôle des modifications s'en trouve simplifié, car les modifications apportées à la conception peuvent être appliquées directement à l'aide d'un modèle d'automatisation prévisible.

Si le dispositif source et le(s) dispositif(s) de destination sont tous deux connectés au réseau à l'aide de PRP, les réseaux LAN A et LAN B se voient attribuer les mêmes circuits de communication pour maintenir les deux réseaux locaux synchronisés et les circuits d'ARP sont ajoutés là où ils sont nécessaires, sans complexité de conception supplémentaire.

Étant donné que certains postes électriques peuvent être en service alors que d'autres sont en cours de rénovation ou de construction, les modifications sont appliquées par poste électrique, par réseau local, de sorte que les différences sont appliquées de manière contrôlée. Cela représentait un avantage significatif pour ELES, car les configurations pour les projets de rénovation et les nouveaux postes électriques pouvaient être traitées à l'aide de l'outil ZTD tout en gardant le réseau existant complètement opérationnel et intact.

5.3.3 Diagnostic

La fonction de diagnostic de l'outil ZTD est utilisée pour diagnostiquer, trouver la cause profonde ou trouver une solution aux problèmes de configuration ou d'exécution de l'automatisation. Cette fonction peut être divisée en trois catégories : conception, configuration, exploitation.

Le contrôle de la conception consiste à vérifier que le même nom d'hôte n'est pas saisi deux fois, que les valeurs sont placées là où elles doivent l'être ou, plus important encore, là où elles ne doivent pas l'être, et qu'il existe un profil de communication et des destinations référencés.

Les diagnostics de configuration sont utilisés pour vérifier la configuration, par exemple pour s'assurer que les adresses IP sont uniques ou qu'un circuit de communication est en état de réussite, ainsi que d'autres vérifications diverses qui ne peuvent pas être effectuées dans la fonction de conception.

Les problèmes opérationnels comprennent les raisons pour lesquelles un circuit de communication fonctionne, mais le trafic ne circule pas, ce qui peut se produire si l'adresse IP est incorrecte ou si le circuit de communication lui-même ne correspond pas correctement au trafic de communication échangé ou si un autre trafic doit être activé pour que le circuit fonctionne.

Les commutateurs de réseau SDN et les contrôleurs de SDN génèrent des données sous diverses formes qui peuvent être modifiées pour fournir des moyens supplémentaires de résoudre les problèmes. Les commutateurs de réseau eux-mêmes fournissent des diagnostics tels que des compteurs pour chaque saut d'un circuit, qui peuvent être collectés et affichés pour déterminer si le trafic emprunte la voie programmée.

Les commutateurs de réseau SDN ont la capacité de transmettre le trafic refusé ou le trafic qui ne correspond à aucune règle spécifique à un capteur de système de détection des intrusions (IDS) ou à un analyseur de réseau. Ce trafic non conforme peut être dû à une mauvaise configuration ou à une intention malveillante. Une partie importante d'un système de diagnostic fonctionnel consiste à collecter le trafic non conforme et à créer la configuration nécessaire pour le transmettre à un capteur, un analyseur de réseau ou un IDS afin d'identifier le trafic que les DEI envoient et qui ne correspond à aucun des circuits de communication actuels : qu'il soit involontaire ou intentionnel (malveillant ou lié à la configuration). Les contrôles à cet effet font également partie de la conception.

De plus en plus d'outils de dépannage ont été développés au cours de la durée de vie du projet et pendant les phases de maintenance du projet, notamment la simulation du trafic pour confirmer que la planification de la voie du circuit est correcte, ainsi que l'installation de compteurs de flux accompagnés d'informations sur la voie afin de détecter les problèmes d'acheminement du trafic.

5.4 Considérations relatives à la conception

Plusieurs considérations de conception ont dû être prises en considération en raison de leur incidence sur le processus fonctionnel du système. Le système comprend à la fois des réseaux actifs (LAN A et LAN B), des réseaux en FAT/SAT ou en construction. C'est pourquoi la configuration est appliquée par réseau local, de sorte que les autres réseaux ne sont pas perturbés. Les postes électriques ne sont pas souvent reliés les uns aux autres, de sorte qu'un contrôleur contrôle plusieurs postes électriques disjoints et que le trafic de gestion des commutateurs est géré par le biais du réseau MPLS à l'extérieur du réseau local. Au sein du réseau local, le trafic de gestion du commutateur (ou le trafic de gestion en bande) est traité comme si le contrôleur était directement connecté.

Le trafic peut appartenir à trois domaines différents en fonction de son origine et de sa destination : à l'intérieur d'un poste électrique, entre un poste électrique et un dispositif situé au-delà du réseau MPLS, et le trafic qui est échangé entre deux postes électriques. Les deux premiers sont gérés dans l'outil en sélectionnant les postes électriques et les désignations de réseau LAN appropriés, tandis que le dernier est géré en sélectionnant deux désignations de réseau du poste électrique, ce qui demande à l'outil ZTD de ne gérer que le trafic à l'intérieur du poste électrique. Le réseau MPLS utilise l'algorithme de coloration pour acheminer correctement le trafic sur l'ensemble du réseau étendu. La fonction de conception, comme indiqué, comprend donc également des informations de coloration (à l'aide de VID) qui sont appliquées aux paquets Ethernet sortant et entrant dans le réseau MPLS.

Deux contrôleurs de réseau sont utilisés, l'un pour le LAN A et le réseau SAN, l'autre pour le LAN B. L'outil ZTD utilise un seul ensemble de documents de conception pour appliquer la configuration appropriée en fonction du contrôleur qu'il est en train de configurer.

Dans les grands réseaux et/ou les réseaux comportant un grand nombre de circuits de communication, les ressources des commutateurs peuvent être limitées, de sorte que l'ajout de câbles supplémentaires peut réduire le nombre de sauts de voie, ce qui diminue les ressources totales pour un circuit. Pour ce faire, il faut ajuster l'algorithme de provisionnement des circuits afin de produire la voie requise. Des algorithmes ont été mis au point pour évaluer les conséquences de ce phénomène.

5.5 Avantages

Le concept Zero-Touch permet aux ingénieurs réseau d'entamer une transition progressive et régulière d'un réseau de commutateurs gérés RSTP vulnérable vers un réseau sécurisé défini par logiciel. Outre les avantages liés à la sécurité et à la gestion du réseau, l'utilisation de l'outil ZTD avec le SDN a permis à ELES de bénéficier de plusieurs avantages supplémentaires, notamment :

- Le processus rationalisé a permis d'économiser du temps, des coûts et de la main-d'œuvre.
- A réduit le risque d'erreur humaine et a fourni des capacités automatisées de contrôle des erreurs [4].
- Le processus automatisé a augmenté la productivité [7].
- L'outil ZTD se connecte au contrôleur de SDN de confiance.
- Au moyen du processus d'adoption, les commutateurs de réseau SDN peuvent être configurés pour ne communiquer qu'avec le contrôleur de SDN prévu et empêcher les utilisateurs de connecter un autre contrôleur de SDN au réseau dans l'intention malveillante de modifier ou de manipuler les réglages [4].
- L'automatisation des réseaux remplace les tâches manuelles par une approche prévisible et reproductible [7].
- Possibilité de configurer plusieurs postes électriques à partir d'un ensemble de la documentation sur le réseau indépendant du système.

Dans certains cas, cela réduit également les frais de déplacement et de main-d'œuvre et permet aux ingénieurs de mise en service de se concentrer sur d'autres tâches opérationnelles telles que les travaux de maintenance préventive et réactive.

6. Défis

La sécurité nécessite des connaissances du système sous-jacent afin de savoir et de comprendre quel trafic doit être autorisé et lequel ne doit pas l'être. Traditionnellement, peu d'attention a été accordée aux détails du protocole pour les communications nécessaires à la mise en place des différentes

fonctions du système parce qu'un réseau Ethernet traditionnel fournit un modèle de sécurité ouvert, autorisant tout, pour les communications au sein des postes électriques et que le filtre TCP/UDP n'est appliqué qu'à la périphérie ou au périmètre de sécurité électrique du poste électrique. Par conséquent, les informations sont souvent incomplètes sur le trafic réseau et le flux de données qui doivent être présents pour chaque fonction du DEI, en particulier pour les dispositifs qui communiquent à l'intérieur du poste électrique. Un défi important a donc été d'obtenir ces informations, soit à partir de la documentation du fabricant, soit par le biais d'un diagnostic. Certains trafics, par exemple, peuvent nécessiter une surveillance PRP pour fonctionner, d'autres non, mais cette information n'est pas incluse dans les manuels d'instructions des dispositifs. Ce défi est d'autant plus important si l'on tient compte des dispositifs hérités. Toutefois, ce processus ne doit être réalisé qu'une seule fois et peut ensuite être utilisé pour des projets futurs.

Un autre défi à relever est que l'introduction d'une nouvelle technologie nécessite une réflexion sur la manière de l'appliquer aux processus actuels et d'adapter les nouveaux processus à la nouvelle technologie.

7. Perspectives d'avenir

Au fil du temps, l'outil ZTD et le contrôleur sous-jacent ont été perfectionnés. Plusieurs modifications futures du contrôleur amélioreront les capacités d'automatisation de ZTD. Il s'agit notamment :

- Verrouillage des réglages afin que le système/les commutateurs n'acceptent pas de changements involontaires pour une meilleure fiabilité.
- Prise en charge accrue des réseaux maillés dans la planification et l'affichage de la voie.
- Un affichage de la topologie en deux dimensions, ainsi que d'autres améliorations de l'évolutivité pour gérer le nombre croissant de réseaux locaux disjoints.
- Appliquer une fonction de déploiement de micrologiciel Zero-Touch sur les commutateurs de réseau.

Plusieurs améliorations futures de la conception sont prévues :

- La duplication du trafic pour envoyer une copie à un analyseur de trafic.
- L'utilisation accrue des techniques de télémétrie et de visualisation pour visualiser les diagnostics ou d'autres données dépendantes du temps afin de détecter les tendances et les problèmes.
- L'amélioration de la fonction de gestion de la configuration afin d'inclure le suivi des révisions depuis les documents de conception source jusqu'à la configuration finale déployée.

8. Conclusion

La sécurisation des communications sur l'ensemble des réseaux d'infrastructure critiques devient de plus en plus essentielle à mesure que les services publics exploitent les avantages des technologies CEI 61850 dans les systèmes modernes d'automatisation de poste électrique. Le présent document étudie les avantages de la mise en œuvre d'un réseau SDN pour remédier aux risques de sécurité présentés par les commutateurs gérés basés sur le protocole RSTP. Outre les problèmes de sécurité qui affectent ces réseaux, la configuration et la gestion des commutateurs de mise en réseau est une tâche complexe, et cette complexité s'accroît à mesure que le nombre de dispositifs et de types de communication dans le réseau, tels que la norme CEI 61850, continue de croître. Le ZTD est un processus par lequel les communications requises pour un dispositif sont automatiquement fournies sans nécessiter d'intervention manuelle directe sur le dispositif. Pour obtenir ces avantages, ce document décrit une solution innovante utilisant ZTD et SDN au moyen d'un projet réel mis en œuvre par le TSO d'ELES en Slovénie. Au cours du projet, un outil ZTD intelligent a été utilisé pour déployer cette solution dans un poste électrique de transport. Les exigences de l'utilisateur, la spécification et la conception de l'outil, les avantages associés à cette solution et les obstacles résolus au cours du projet ont également été abordés.

9. Références

[1] CEI 62439-3, Réseaux de communication industriels - Réseaux d'automatisation à haute disponibilité - partie 3 : Protocole de redondance parallèle (PRP) et redondance transparente à haute disponibilité (HSR), 2016.

[2] CEI 61850-5, Réseaux et systèmes de communication pour l'automatisation du service public d'électricité - partie 5 : Communication Requirements for Functions and Device Models (Exigences de communication pour les fonctions et les modèles de dispositifs), 2013.

[3] CEI TR 61850-90-4, Réseaux et systèmes de communication pour l'automatisation du service public d'électricité - partie 90- 4 : Network Engineering Guidelines (Directives d'ingénierie reseau), 2020

[4] National Cyber Security Center, « Zero-Touch Enrolment, » (Enrôlement de Zero-Touch), juin 2021. Disponible à l'adresse : https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/zero-touch-enrolment

[5] Microsoft Corporation, « Zero-Touch deployment : a cornerstone of modern device management » (Déploiement Zero-Touch : une pierre angulaire de la gestion moderne des dispositifs), 2019. Disponible à l'adresse : https://www.microsoft.com/cms/api/am/binary/RE4yfB2

[6] Demchenko Y, Filiposka S, and de Vos M, « ZeroTouch Provisioning (ZTP) Model and Infrastructure Components for Multi-Provider Cloud Services Provisioning » (Composants de modèle et d'infrastructure de provisionnement Zero-Touch (ZTP) pour le provisionnement de services en nuage multi-fournisseurs), novembre 2016.

[7] Anand V, « How Zero Touch Will Transform IoT Device Deployment » (Comment Zero-Touch va transformer le déploiement de dispositifs d'Internet des objets), Capgemini Engineering, 2021. Disponible à l'adresse : https://prod.ucwe.capgemini.com/wp-content/uploads/2023/03/How-Zero-Touch-Will-Transform-IoT-Device-Deployement_Whitepaper_November-2021.pdf

[8] Meine, R., « A Practical Guide to Designing and Deploying OT SDN Networks » (Un guide pratique pour concevoir et déployer des réseaux OT SDN), proceedings of the Power and Energy Automation Conference, Spokane, WA, mars 2019.

10. Biographies

Darko Bordon a rejoint l'opérateur de réseau de transport d'ELES en Slovénie en 1999 et occupe actuellement le poste de chef de projet et d'ingénieur des systèmes secondaires. Darko est responsable des projets de systèmes secondaires, des concepts de communication des postes électriques, de la mise en service de barre de poste, des essais d'acceptation en usine et des essais d'acceptation sur site. En 2001, il a obtenu sa licence à l'université de Ljubljana, en Slovénie, à la faculté d'ingénierie électrique.

Robert Meine est diplômé de l'université de l'Idaho, où il a obtenu une licence en science et ingénierie des matériaux ainsi qu'une licence en informatique. Robert a rejoint Schweitzer Engineering Laboratories, Inc. (SEL) en 2013 et est actuellement ingénieur d'application dans le département des communications de la recherche et du développement, où il soutient les produits liés au SDN.

Sagar Dayabhai est ingénieur d'application principal chez Schweitzer Engineering Laboratories, Inc. (SEL) en Europe. Sagar est titulaire d'une licence en génie électrique de l'université de Wits, en Afrique du Sud, et d'une maîtrise en génie électrique de cette même université en 2014. Il est ingénieur professionnel enregistré auprès de l'Engineering Council of South Africa (ECSA). Sagar a été l'un des jeunes professionnels de la CEI élus pour l'Afrique du Sud en 2016 et est actuellement membre des WG 10 et WG 15 de la CEI TC 57. Après avoir travaillé à Eskom dans le domaine des télécommunications et du SCADA, il a ensuite rejoint Consolidated Power Projects (CONCO) où il a occupé les postes d'ingénieur principal en SCADA/automatisation et de responsable du contrôle des systèmes. Sagar a été largement impliqué dans la cybersécurité, les systèmes d'énergie renouvelable, les systèmes de contrôle SCADA, DMS, l'automatisation du poste électrique, et l'intégration des générateurs embarqués dans les réseaux de services publics pendant plus de 10 ans.

Jason Dearien travaille chez Schweitzer Engineering Laboratories, Inc. (SEL) depuis plus de 20 ans et est actuellement ingénieur d'application principal au sein du département SDN R&D, spécialisé dans l'OT SDN. Il participe au soutien et à la formation pour les déploiements et les solutions de réseau d'OT SDN destinés aux clients internes et externes. Auparavant, Jason a travaillé dans de nombreux groupes de R&D en tant qu'ingénieur logiciel principal, dirigeant des déploiements de systèmes et d'architectures, y compris la première offre de la norme CEI 61850. Il était le chef technique et le chef d'équipe pour les développements de produits, y compris le contrôleur d'automatisation en temps réel (RTAC) et les produits de commutation.

***Résumé*—Les systèmes modernes d'automatisation des postes électriques sont dotés de l'intelligence nécessaire pour détecter, identifier et gérer les défauts, les événements et les perturbations du système électrique, et pour ajuster le réseau en conséquence. Pour que les entreprises de service public puissent mettre en œuvre ces technologies et profiter de leurs avantages pour évoluer vers un poste électrique numérique, il est nécessaire de disposer d'un réseau de technologies opérationnelles (OT) de communication fiable et sûr, qui prenne en charge le transfert de données à grande vitesse. Par conséquent, l'utilisation des réseaux Ethernet est devenue un élément essentiel des applications de protection et de contrôle des réseaux électriques. Cette situation a entraîné une augmentation du nombre de commutateurs de réseau utilisés dans le réseau électrique au cours de la dernière décennie, car le nombre de dispositifs électroniques intelligents (DEI), d'applications et de données disponibles ne cesse de croître.**

Le SDN peut être déployé en tant que solution dans les réseaux OT pour relever les défis posés par les réseaux Ethernet traditionnels. Le présent document présente une étude de cas basée sur une mise en œuvre réelle qui utilise SDN dans un système d'automatisation de poste électrique moderne basé sur la norme CEI 61850 au sein du TSO d'ELES en Slovénie. Cette étude de cas associe l'utilisation de SDN à une méthodologie de déploiement Zero-Touch (ZTD) afin de présenter une approche d'ingénierie innovante, axée sur les applications, pour concevoir et sécuriser les réseaux OT dans un poste électrique. Les avantages et les inconvénients de cette mise en œuvre sont documentés dans cette étude de cas. Elle couvre les aspects positifs et les défis rencontrés au cours des phases de conception, de mise en service et de maintenance du poste électrique.

20230526 • TP7122