# Sécurité de la borne de recharge pour véhicules électriques (BRVE)

SOUTHWEST RESEARCH INSTITUTE®

Katherine Kozan

26 mars 2026

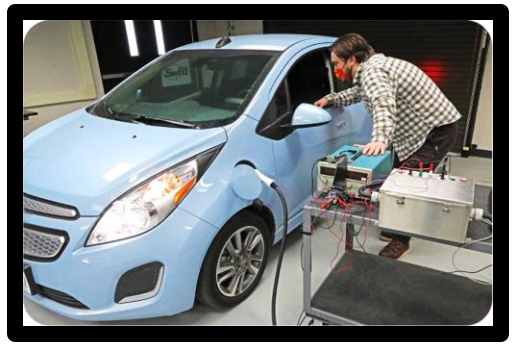
# Préoccupations

- Attaques au système de gestion de la batterie (SGB)
  - Usurpation d'identité
  - Refus de service
- Chargeur J1772 L2
  - Attaque par interception
    - Facturation excessive
    - Attaque entraînant un refus de service
    - Charge limite
- Vulnérabilités à la recharge rapide en courant continu (courants porteurs en ligne [CPL])
  - Accès au système
- Brancher et recharger (B et R)
  - Attaque par interception avec caractérisation de l'atténuation du niveau de signal (SLAC)
- Infrastructure à clé publique (ICP) pour BRVE
- Gestion des clés (GC)

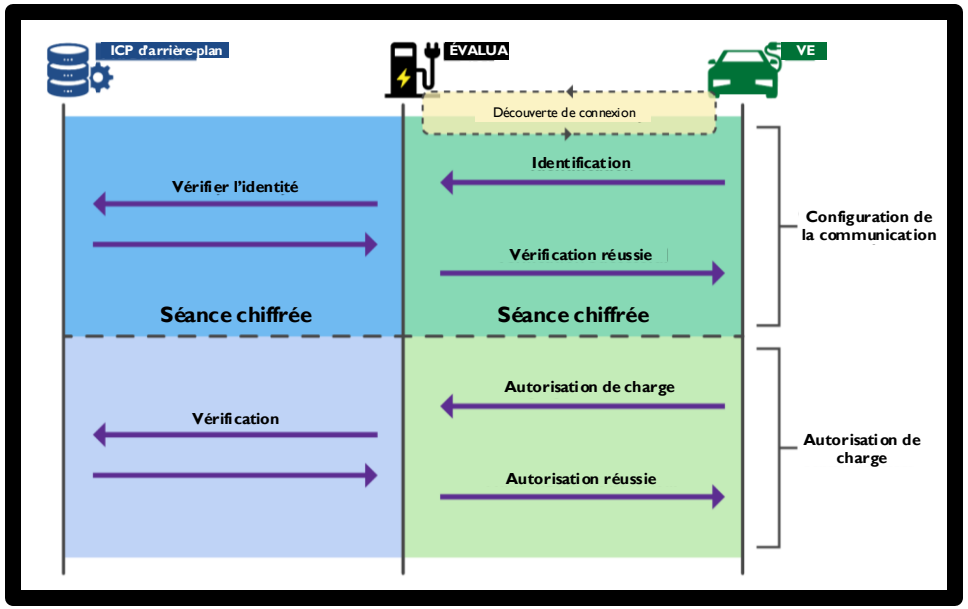
SGB
J1772 L2
CPL
B et R
ICP
GC

# L'évolution de la sécurité des communications des VE et de la BRVE

- **DIN 70121**
  - Pas de Transport Layer Security (TLS), demande et réponse
  - Caractérisation de l'atténuation du niveau du signal (SLAC)
  - Communication de base et authentification pour la recharge rapide en courant continu
  - Chiffrage limité
- **ISO15118-2**
  - Chiffrage TLS introduit
  - ICP et certificats numériques
  - Brancher et recharger
- **ISO 15118-20**
  - TLS amélioré (1,3) et soutien mutuel du protocole TLS (mTLS)
  - Sécurité de charge bidirectionnelle
  - Mises à jour régulières sur la sécurité



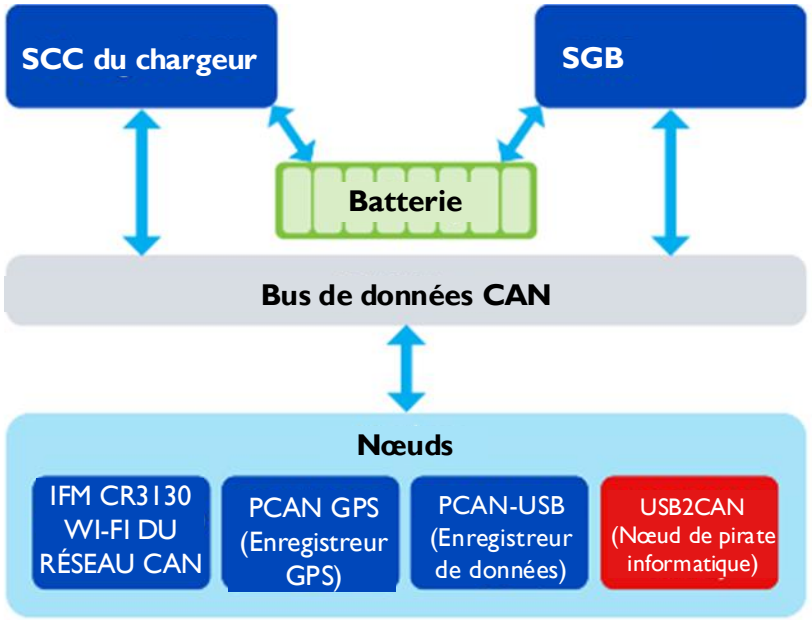
**VE et BRVE de Southwest Research Institute (SwRI) Recherche sur la cybersécurité**



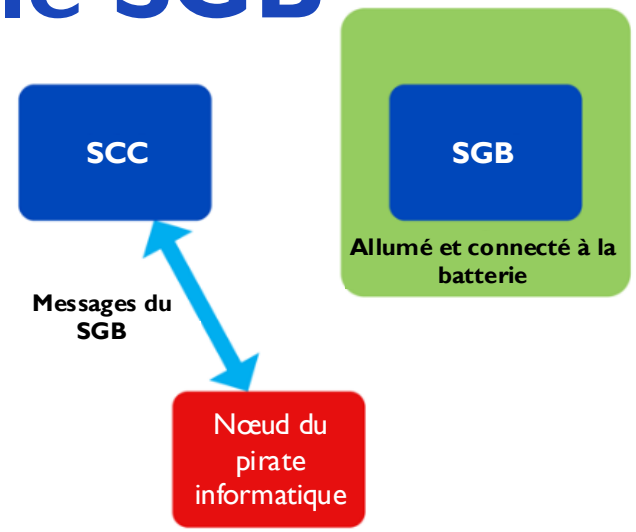

**TLS dans B et R : Séquence d'autorisation**

# Contexte du SGB

- **Système de charge combiné (SCC) :**
  - Fournit et régule le courant de charge de la batterie
  - Surveiller la tension de la batterie
- **Système de gestion de la batterie :**
  - Gère et évalue la fonction globale de la batterie et la santé de la batterie
  - Surveille chaque cellule de batterie
  - Commandes du SCC pour le chargement

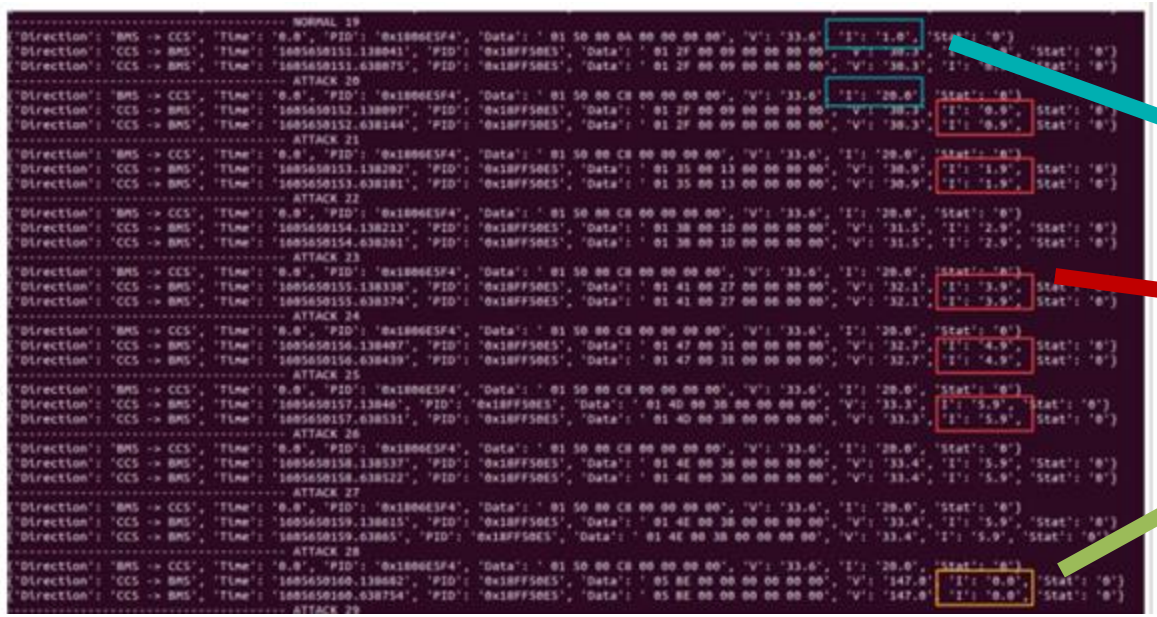


# Courant du SCC pour l'usurpation d'identité sur le SGB




- Le nœud du pirate informatique envoie des messages en tant que SGB au SCC
- Utilisation du SGB pour l'identifiant du SCC
- Le pirate envoie progressivement des messages aux SCC
- Augmenter les niveaux actuels à des niveaux dangereux

**Résultat : Charge arrêtée**



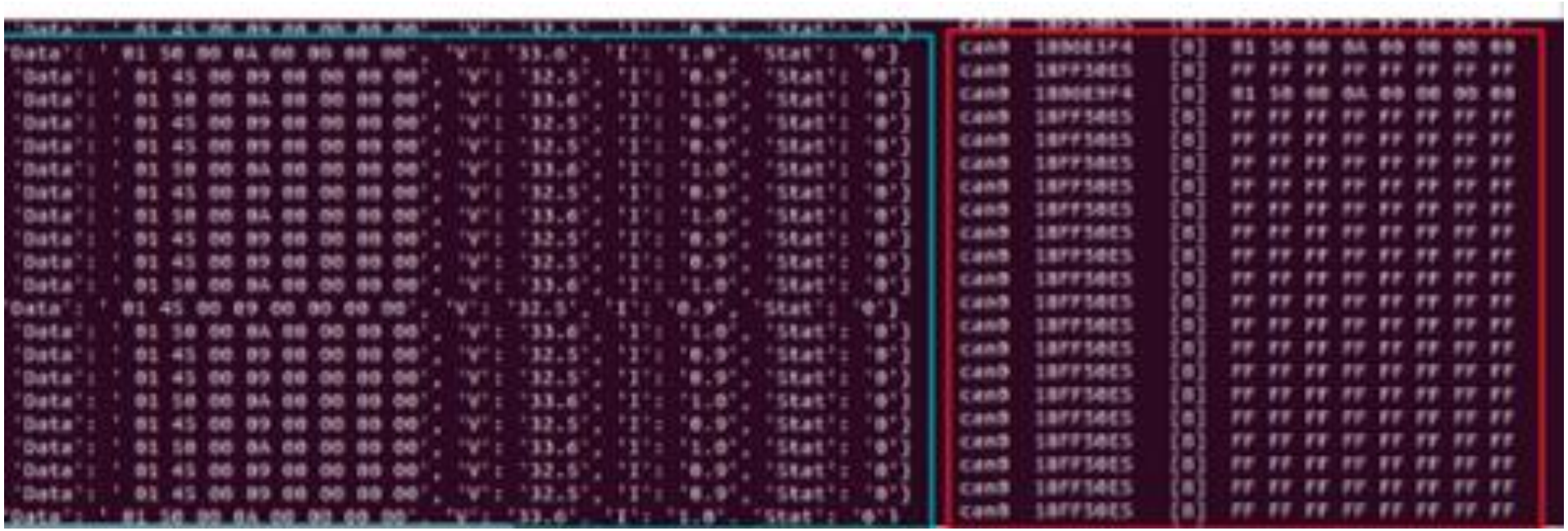
**SGB->SCC, augmentation du courant**

**SCC->SGB, courant en augmentation**

**SCC->SGB, arrêt du courant**

S G B

# Déni de service



- Le nœud du pirate informatique envoie des messages et provoque des attaques par saturation sur le bus de données CAN
- SGB réel et SCC déconnecté

**Résultat : Attaque par déni de service réussie**

SGB

# Réseaux de recharge pour véhicules électriques : Les avancées technologiques dépassent la cybersécurité nécessaire

- La dépendance accrue aux systèmes de communication électronique et aux systèmes de recharge électroniques a créé des possibilités pour de nouvelles cyberattaques.
- La recherche du SwRI a démontré que les cyberattaques sont possibles sur les réseaux actuels.

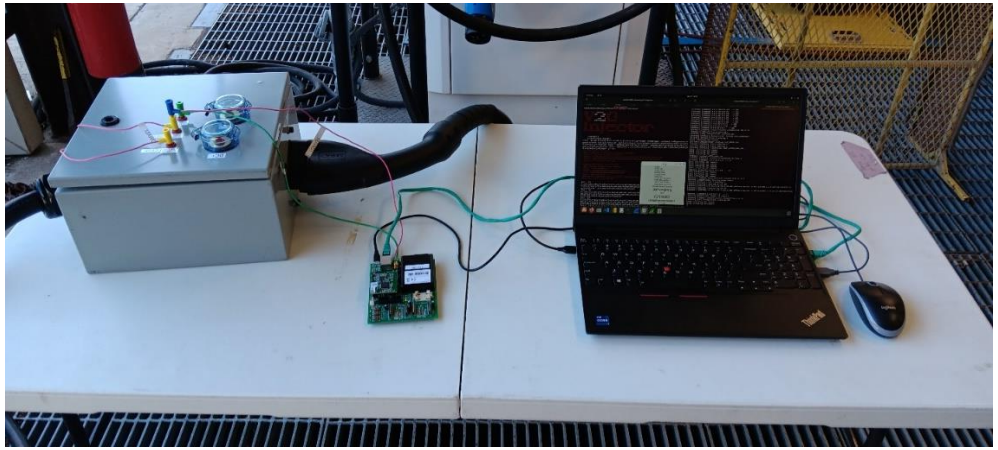

Projet du SwRI : Vulnérabilités en cybersécurité des bornes de recharge pour véhicules électriques
https://www.swri.org/press-release/electric-vehicle-charging-cybersecurity-vulnerabilities

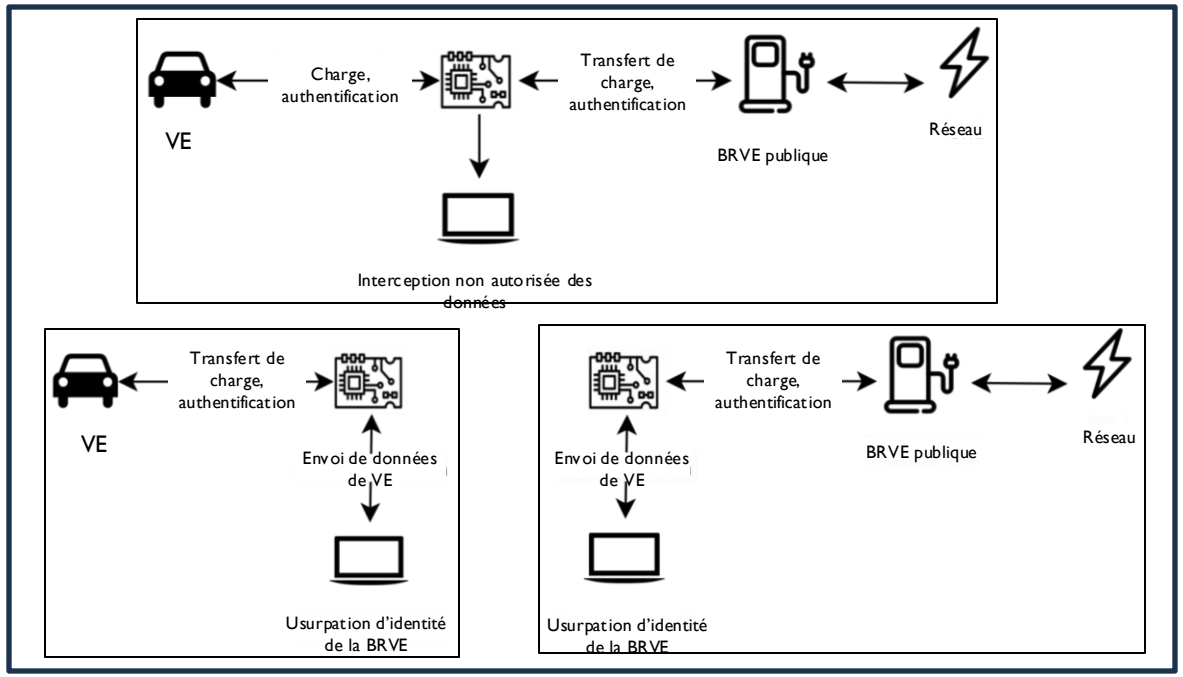
Projet du SwRI : Cybersécurité des véhicules électriques
https://www.swri.org/work-us/internal-rd/2020/automotive-transportation/10-r6022

J1772 L2

# Intervention en cas d'incident de sécurité pour la borne de recharge pour véhicules électriques (BRVE) à charge rapide en courant continu (DCFC)

**Objectif :** Analyser le processus de recharge rapide en courant continu (DCFC) des VE et les courants porteurs en ligne (CPL) utilisés





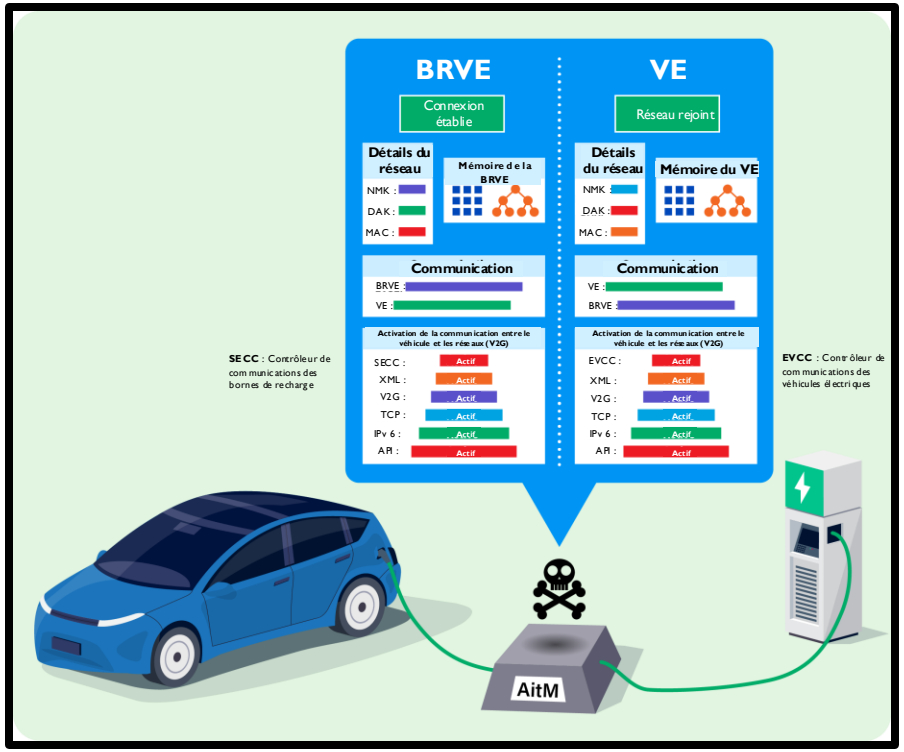

C
P
L

Communiqué de presse : https://www.swri.org/press-release/swri-evaluates-cybersecurity-risks-associated-ev-fast-charging-equipment

# Communication sur la ligne électrique DCFC

- Déterminer si les chargeurs DCFC sont sécurisés
- Conversion de CPL à Ethernet
- Dossiers de configuration vidés
- Modification et nouveau téléversement des fichiers de configuration

**Résultat : Ports ouverts**




*Ce diagramme démontre une attaque par interférence développée par le SwRI et sa capacité à émuler à la fois un véhicule électrique et une borne de recharge pour véhicules électriques (BRVE), ainsi qu'à surveiller leurs attributs définis.*

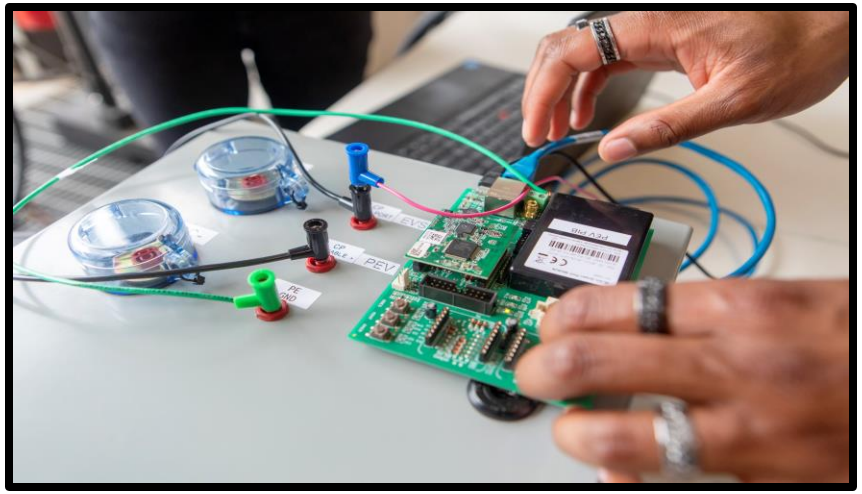
Communiqué de presse : https://www.swri.org/press-release/swri-evaluates-cybersecurity-risks-associated-ev-fast-charging-equipment

C
P
L

# Interception des communications pour Brancher et recharger

**Objectif :** Établir une attaque par interférence en exploitant les faiblesses du processus de caractérisation de l'atténuation au niveau du signal (SLAC).

- **Modifier le transport existant en transit entre les systèmes**
- **Compromettre l'échange de certificats lors de la configuration de la connexion**
- **Réduire la sécurité de la connexion**



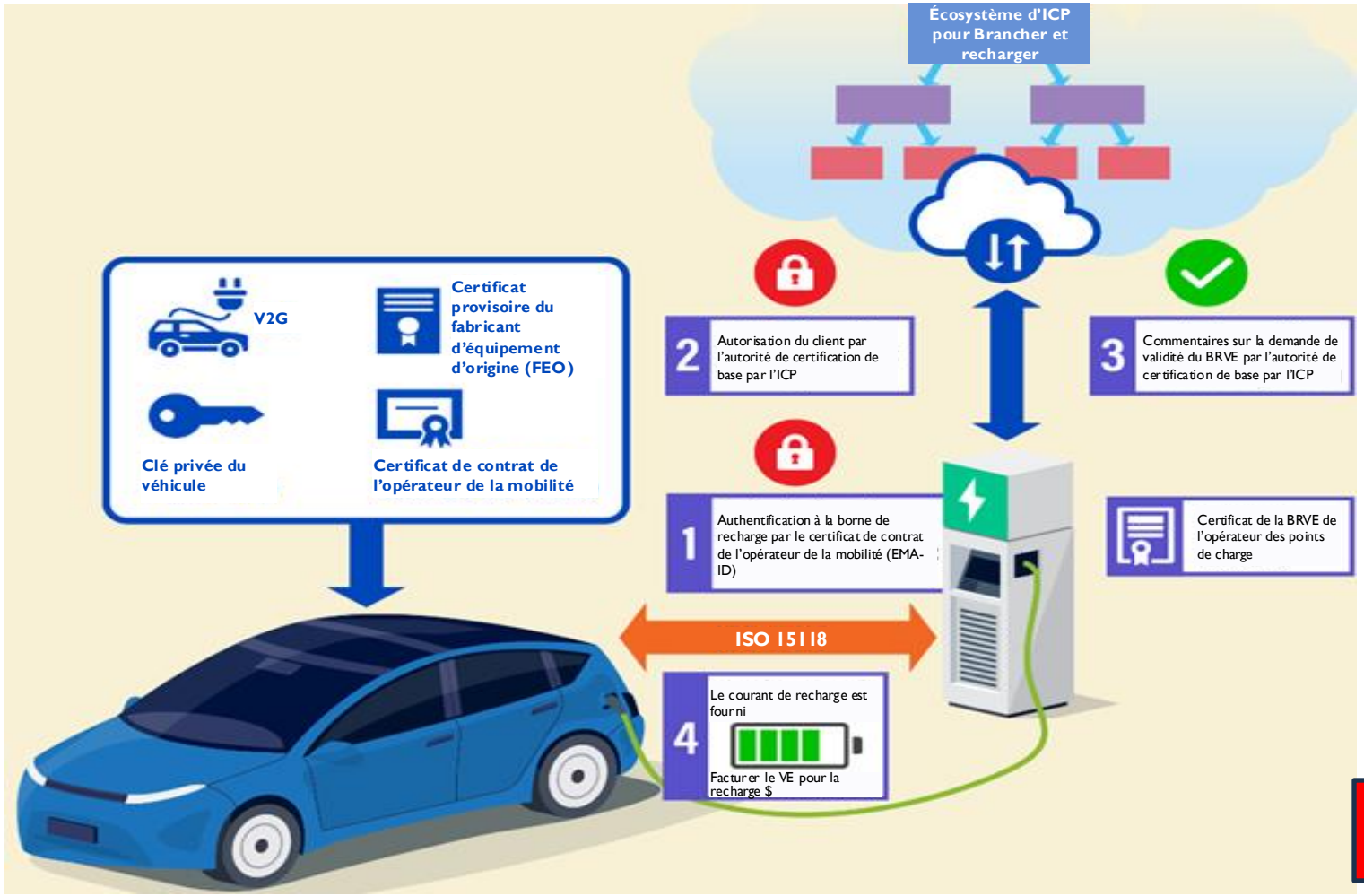
B et R

# Recherche sur l'infrastructure à clé publique (ICP) pour les bornes de recharge pour véhicules électriques (BRVE)

- **Enquête**
  - Sécurité de la communication de l'ICP dans les réseaux de charge des VE
  - Faisabilité des attaques contre les protocoles de communication et les certificats d'ICP
- **Analyser les protocoles de communication dans l'environnement de BRVE**
  - Déterminer les vulnérabilités
  - Élaborer des stratégies de mesures d'atténuation

# ICP pour une BRVE

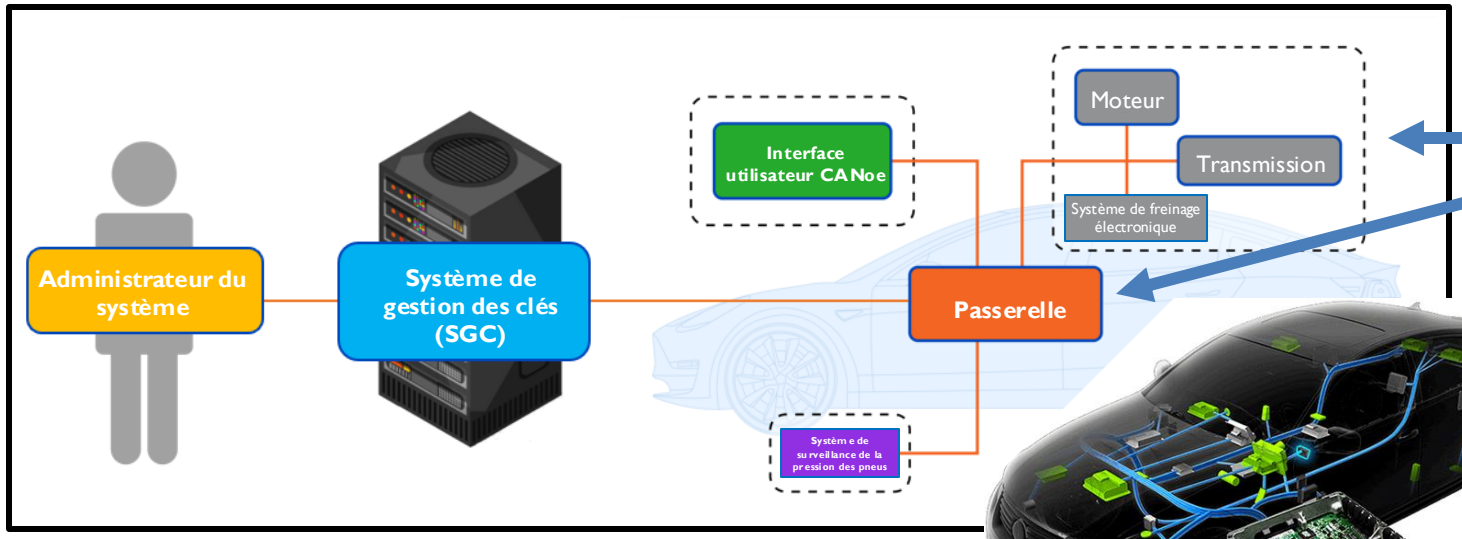
- SwRI établira une simulation de BRVE avec des capacités d'ICP et utilisera un véhicule doté d'une ICP active
- Créer une architecture de base pour les communications en arrière-plan
- Se concentrer sur l'authentification et l'autorisation



# Système de gestion des clés (SGC)

- Démonstration d'un SGC complet pour systèmes intégrés basés sur l'adaptation des logiciels à source ouverte dans un environnement automobile intégré

Preuve de concept démontrable pour d'autres applications




Fonctionne avec plusieurs types d'appareils



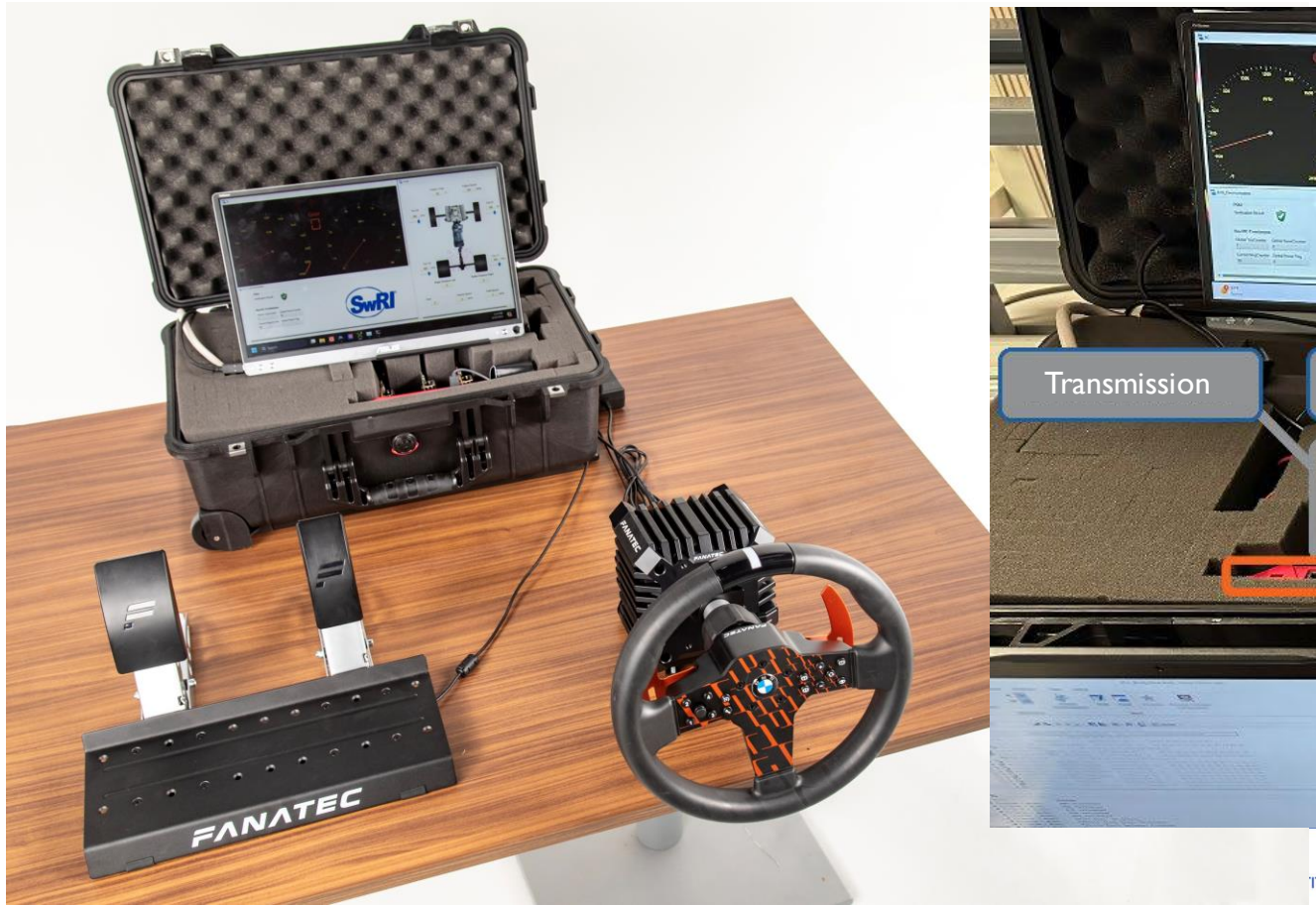
Travailler avec les applications cybernétiques existantes de SwRI

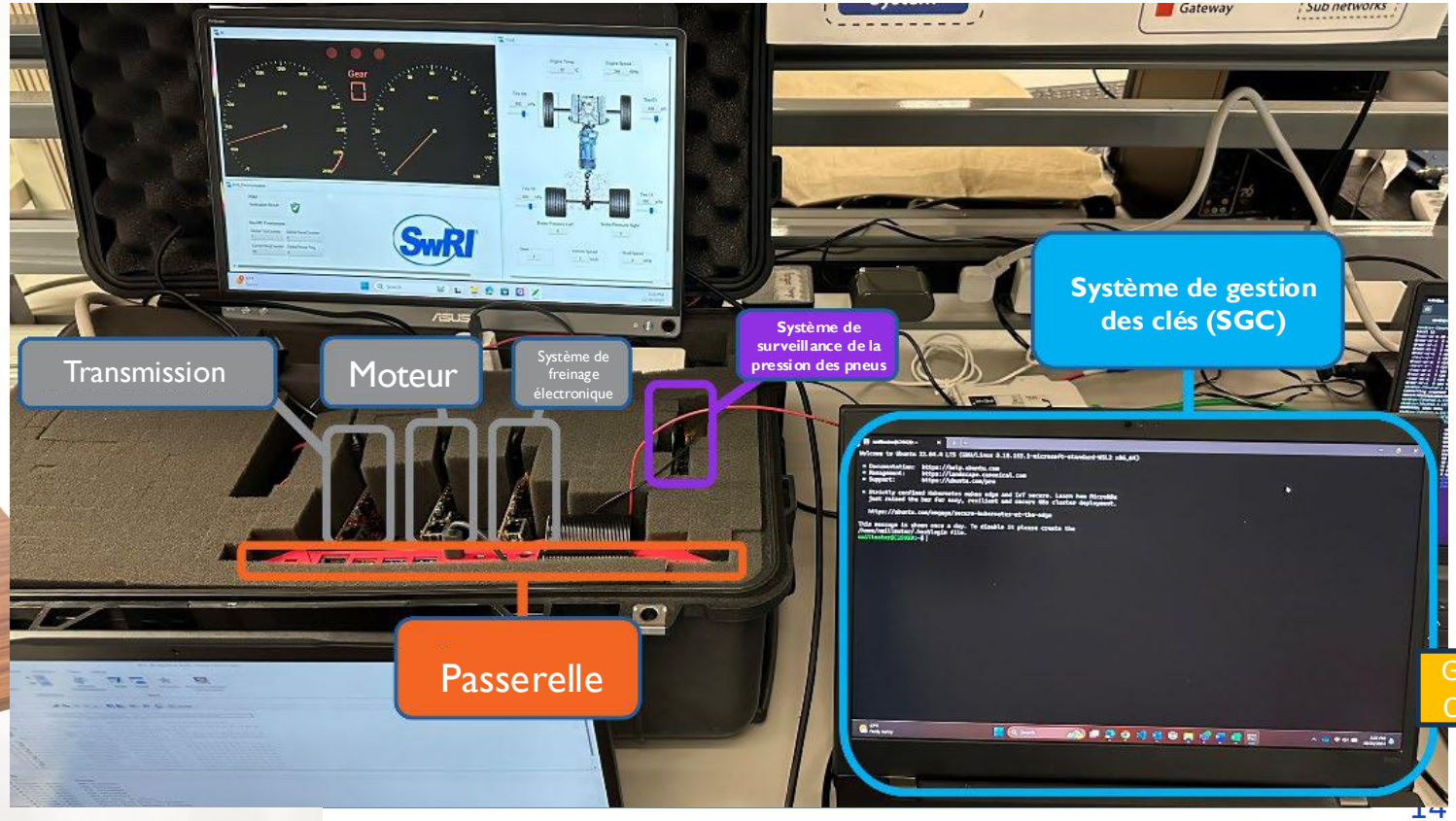
**Mesurer le succès avec un plan**

GC

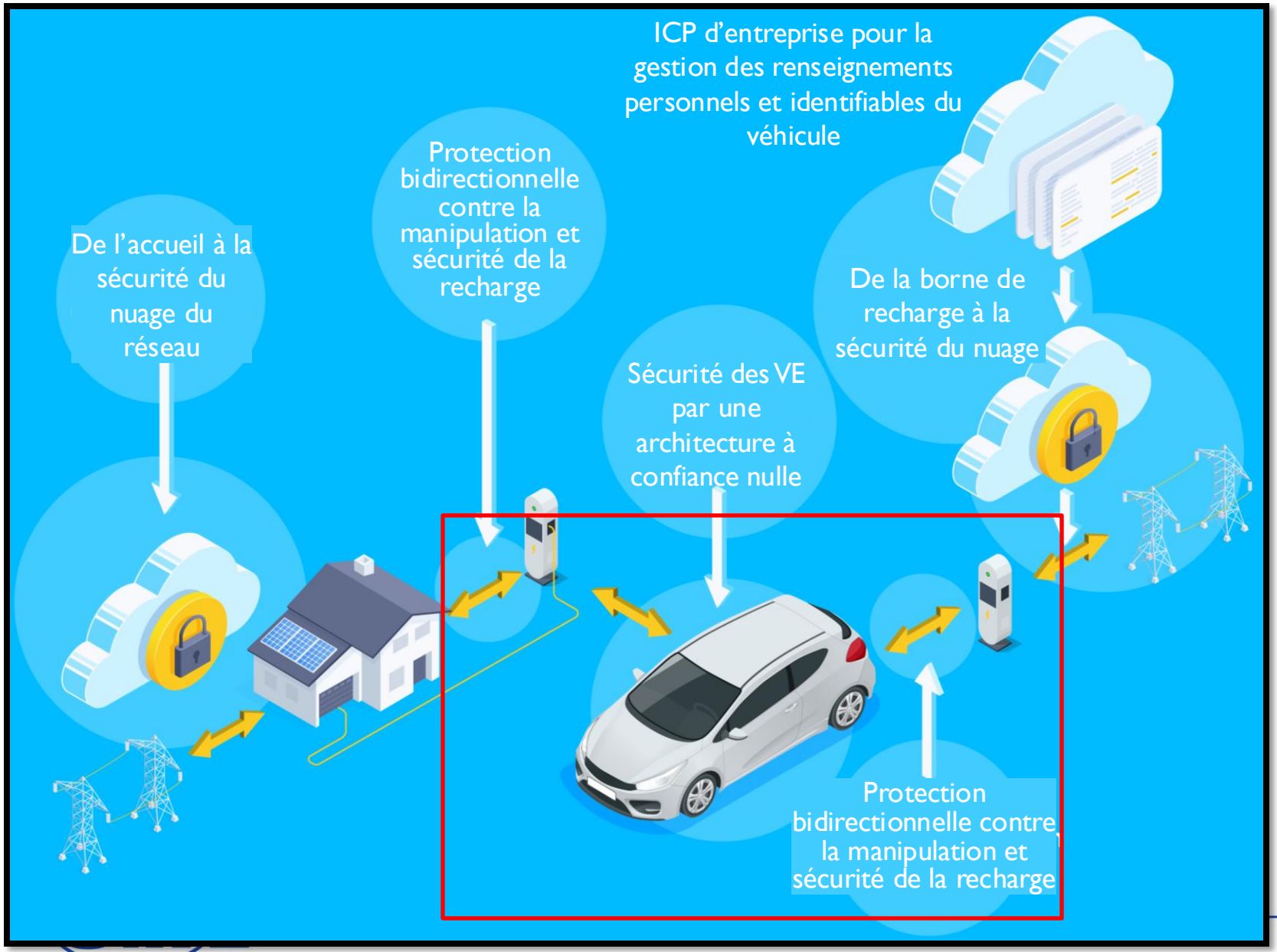
# Gestion des clés

- A démontré avec succès les échanges de clés sur un simulateur de véhicule dans la boucle du matériel
- Mis en œuvre le SecOC complet et les principes de confiance nulle



# Cybersécurité de V2G de SwRI



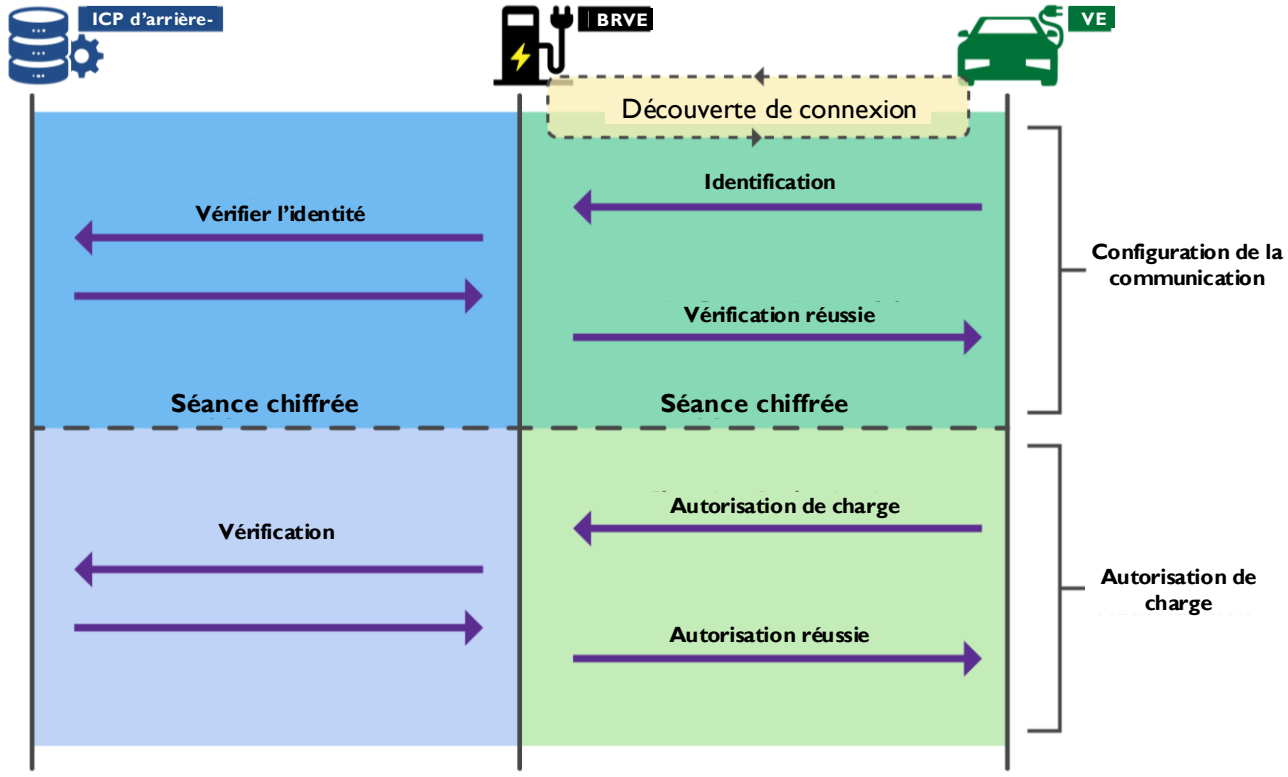

- **Domaines de recherche précédents**
  - Sécurité
  - Normalisation
  - Vitesse de la recharge
  - Fonctionnalité

**Nous croyons qu'une solution de V2G peut être conçue avec la sécurité comme base, offrant une fonctionnalité robuste à grande échelle**

- **Prochaine étape de la recherche**
  - Distribution (disponibilité)
  - Intégration
  - Facilité d'utilisation

# Authentification et autorisation

- Examen de l'échange de certificats et de l'approvisionnement
- Examiner les bases de l'authentification d'ISO 15118
- Identifier les vulnérabilités et élaborer des stratégies de mesure d'atténuation
  - Ports du réseau ouvert
  - Manipulation des données
  - Attaques d'interception



# Questions et autres discussions


Katherine Kozan
Ingénieure de recherche
210.522.2541
Katherine.kozan@swri.org