Richard « Barney » Carlson,
Kenneth Rohde
Idaho National Laboratory

Séance d'experts de Transports Canada
24 mars 2022

Cybersécurité axée sur les conséquences pour les infrastructures de recharge des véhicules électriques (VE) à haute puissance

INL/MIS-21-62225

Idaho National Laboratory

Impact et pertinence :

- Risques importants liés à l'exploitation des failles de cybersécurité des infrastructures de recharge des VE à haute puissance :
  - Systèmes de recharge de VE accessibles au public
    - Haute tension
    - Haute puissance
  - Complexité accrue du système
    - Plusieurs voies de communication entre le VE, la borne de recharge pour VE, le fournisseur de services de charge, le service public, etc.
    - Gestion avancée de l'énergie : Gestion intelligente des charges, véhicule vers le réseau électrique, services de réseau, etc.
    - Systèmes avancés d'électronique de puissance
    - Systèmes de gestion thermique
  - Intégration dans l'infrastructure essentielle nationale (réseau électrique)
    - Une charge de plusieurs MW est possible avec une borne de recharge/plaza de taille moyenne (c.-à-d., six chargeurs de 350 kW).
    - Le transfert de puissance transitoire (charge rapide) est inhérent à la charge en CC.
      - La recharge d'un VE cible en moins de 10 minutes nécessite un transfert de haute puissance.

Information sur le projet et objectif

- Un projet financé par le DOE des États-Unis met l'accent sur la cybersécurité de l'infrastructure de recharge des VE à haute puissance.
  - Analyse, évaluation du matériel de laboratoire, élaboration de solutions d'atténuation
- Équipe de projet
  - Idaho National Lab (INL)
  - Oak Ridge National Lab (ORNL)
  - National Renewable Energy Lab (NREL)
  - ABB
  - Tritium
  - Electrify America

Objectif :

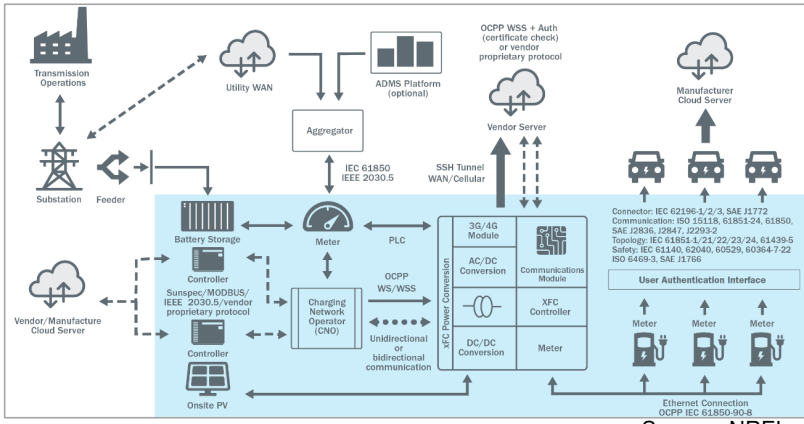
- Quantifier, analyser et réduire les risques associés aux vulnérabilités et à l'exploitation de l'infrastructure de recharge des VE à haute puissance, qui peuvent entraîner des événements à haute conséquence (EHC).
  1. Sécurité
  2. Impact sur le réseau électrique
  3. Dommages matériels
  4. Déni de service
  5. Vol ou altération de données

Approche du projet :

1. Conceptualiser les événements à haute conséquence (EHC)
2. Donner la priorité aux EHC
   - D'après la cotation de la **gravité de l'impact** et de la cotation de la **complexité** de la cybermanipulation
3. Évaluation en laboratoire des EHC :
   - Complexité de la cybermanipulation
   - Gravité de l'impact
   - Affinement itératif de la cotation et de la hiérarchisation des EHC en fonction des résultats de laboratoire
4. Élaborer des solutions et des stratégies d'atténuation
   - Évaluation de la preuve de concept en laboratoire
5. Publier les résultats et les conclusions du projet

Limites et hypothèses du projet :

- Chargement en CC (pas en CA)
- Uniquement les événements provenant de cyberexploitations
- Événements naturels non compris (météo, vandalisme, etc.)
- Avec suffisamment de temps et d'efforts, un adversaire compétent et bien informé peut accéder à presque tous les systèmes à commande électrique ou les compromettre



Source : NREL

Événements à haute conséquence (EHC)

Analyse et classement par ordre de priorité

Classement des EHC par ordre de priorité

Cotation des EHC = impact **x** complexité

- Cotation de la gravité de l'impact fondée sur 8 critères
- Cotation du multiplicateur de complexité (facilité de cybermanipulation)

Cotation du multiplicateur de complexité de la cybersécurité

Cotation	Description
10	**Complexité extrêmement faible** – Seul un système unique doit être modifié. Le système est facilement accessible par l'adversaire (physique ou virtuel). Aucune condition préalable n'est requise.
8	**Complexité faible** – Seul un système unique doit être modifié. Le système n'est pas facilement accessible, mais la compromission du système est anodine une fois l'accès disponible. Aucune condition préalable n'est requise.
6	**Complexité moyenne** – Un ou plusieurs systèmes doivent être modifiés. Le(s) système(s) est (sont) accessible(s) avec des efforts, mais la compromission est généralement réussie. Des conditions préalables peuvent être requises.
4	**Complexité difficile** – Plus d'un système doit être modifié. Les systèmes sont difficiles à atteindre. La compromission exige des compétences spécialisées. Des conditions préalables sont requises pour une exploitation réussie.
2	**Complexité extrêmement difficile** – Plus d'un système doit être modifié. Les systèmes sont difficiles à atteindre. La compromission ne réussit pas toujours. Des conditions préalables sont requises pour une exploitation réussie et ces conditions sont rares.

Cotation des EHC

Multiplicateur de complexité	Gravité de l'impact				
10	20	40	60	80	100
8	16	32	48	64	80
6	12	24	36	48	60
4	8	16	24	32	40
2	4	8	12	16	20
0	2	4	6	8	10

Cotation de la gravité de l'impact

Critères	S.O. (0)	Faible (2)	Moyenne (6)	Élevée (10)
Niveau d'impact	S.O.	Unité unique concernée (VE, recharge ultrarapide ou TESF)	Plusieurs unités sur un même site sont concernées (VE, recharge ultrarapide et/ou TESF)	Plusieurs unités sur plusieurs sites sont concernées (VE, recharge ultrarapide et/ou TESF)
Magnitude (propriétaire ou standardisée)	S.O.	Mise en œuvre du protocole propre au fabricant (VE ou borne de recharge pour VE)	> 1 mise en œuvre du protocole des fabricants (chaîne d'approvisionnement) (VE ou borne de recharge pour VE)	Dans tous les systèmes normalisés (à la fois les bornes de recharge pour VE et les VE)
Durée	S.O.	< 8 heures	> 8 heures à < 5 jours	> 5 jours
Effort de rétablissement	Rétablissement automatisé sans intervention externe	L'équipement peut être remis en état de fonctionnement par une réinitialisation ou un redémarrage (effectué à distance ou par le personnel sur place).	L'équipement peut être remis en état de fonctionnement normal grâce à un redémarrage ou à une intervention du personnel hors site (remplacement d'une pièce consommable; déplacement sur place).	L'équipement ne peut être remis en état de fonctionnement normal que par le remplacement du matériel (remplacement de composants, nécessite un équipement spécial, remplacement d'unités entières).
Sécurité	Aucun risque de blessure	Risque de blessure mineure (pas d'hospitalisation), AUCUN risque de décès	Risque de blessure grave (hospitalisation), mais faible risque de décès	Risque important de décès
Coûts	Aucun coût encouru	Le coût de l'événement est important, mais l'organisation n'a pas la capacité de l'absorber.	Le coût de l'événement nécessitera plusieurs années de rétablissement financier (bilan)	Le coût de l'événement déclenche une crise de liquidités qui pourrait entraîner la faillite de l'organisation.
Propagation de l'effet au-delà du VE ou de la borne de recharge pour VE	Pas de propagation	Localisé sur place	Dans la zone métropolitaine; au sein d'une seule ligne de distribution	Régional; impact sur plusieurs lignes de distribution
Dommages à la confiance et à la réputation dans l'industrie des VE	Aucun impact sur la confiance ou la réputation	Impact minime sur l'adoption des VE	Adoption stagnante des VE	Adoption négative des VE

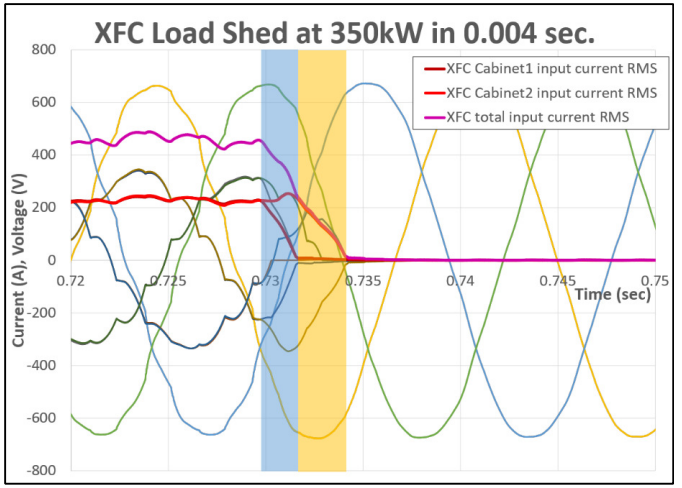
Évaluation en laboratoire de la gravité de l'impact et de la complexité de la cybermanipulation

Évaluation de la cybersécurité de ABB TerraHP-350kW (recharge ultrarapide)

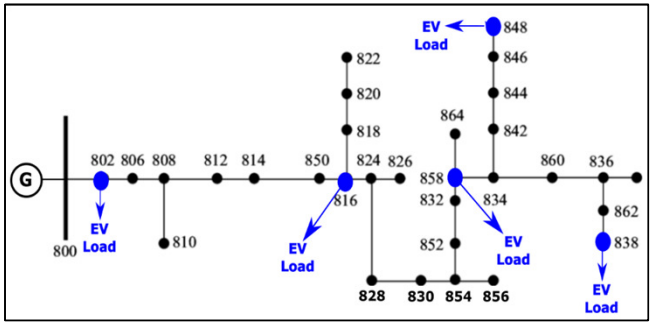
1. **Déterminer les voies d'attaque**
   - Accès cellulaire par le réseau d'ABB, la connexion locale et l'accès physique (ouverture du boîtier)
2. **Déterminer les vulnérabilités**
   - Vulnérabilités d'exécution de code à distance
   - Techniques d'attaque « homme du milieu » du protocole OCPP
   - Accès physique pour compromettre le système (risqué)
3. **Tenter de compromettre le système**
   - Méthodes de compromission à distance
   - Évaluation des clients du protocole OCPP et du test de pénétration
   - Les protections d'accès physique sont fortes.
   - Le rapport sur les résultats de la vulnérabilité a été fourni au fournisseur.
4. **Fournir des recommandations sur les mesures d'atténuation**
   - Les solutions d'atténuation sont en cours d'élaboration et seront publiées à la fin de ce projet

EHC nº 1 : Impact sur le réseau : Délestage multiple simultané de la recharge ultrarapide

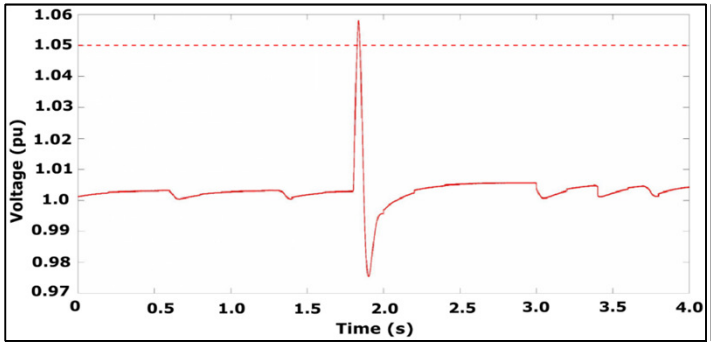
- « Arrêt de charge » simultané de plusieurs recharges ultrarapides.
  - Délestage de la pleine puissance en **0,004 s**
  - Plusieurs façons de mettre en œuvre le délestage (p. ex., « arrêter la charge »).
    - Demande normale d'« arrêter la charge » de la part du VE, de l'IHM ou autre
    - État d'erreur de contrôle interne de la recharge ultrarapide
    - Commande du protocole OCPP
- Un délestage simultané peut provoquer des tensions transitoires > 1,05 pu.
- Dépend de la charge totale et de la quantité de délestage au nœud.



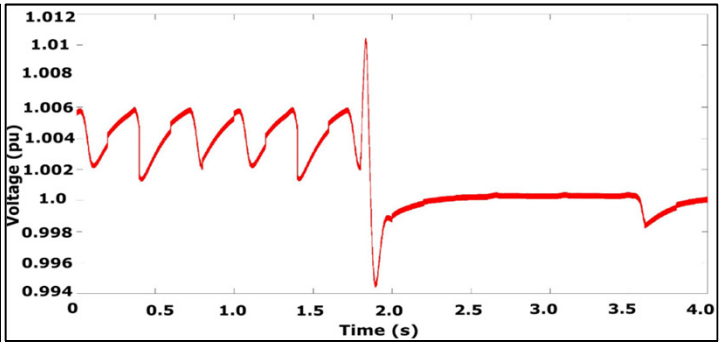
Système de distribution de l'IEEE à 34 autobus avec charge distribuée



15 délestages de la recharge ultrarapide au nœud 816



15 délestages de la recharge ultrarapide répartis sur les nœuds



<u>Principal élément à retenir</u> : Le délestage simultané de plusieurs recharges ultrarapides peut provoquer une excursion ou une instabilité de la tension d'alimentation.

EHC nº 1, nº 6, nº 7 et nº 9 : Manipulation du protocole OCPP entraînant un délestage, une mauvaise gestion de la charge ou un déni de service

- Nº 1 : Le délestage simultané de plusieurs recharges ultrarapides a des répercussions sur l'instabilité du réseau.
  - Cause : Commande du protocole OCPP « *RemoteStopTransaction* » lancée simultanément pour plusieurs recharges ultrarapides.

- Nº 6 : Réponse incorrecte du site de charge aux demandes de gestion de l'énergie.
  - Cause : Usurpation de la gestion de l'énergie du protocole OCPP « *TxProfile* » pour plusieurs sites de charge.

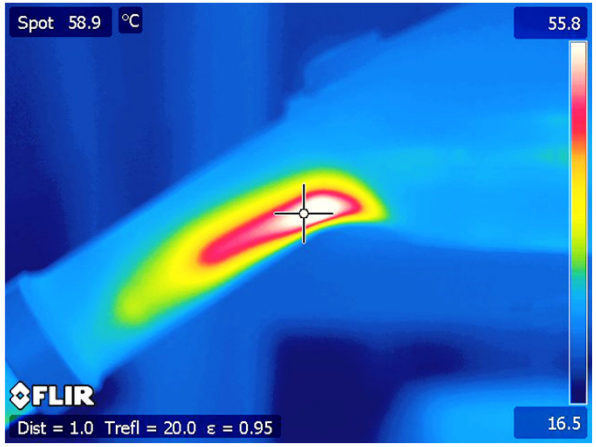
- Nºs 7 et 9 : Déni de service de plusieurs sites de charge.
  - Cause : Commande du protocole OCPP « *ChangeAvailability : Inoperative* » envoyée à plusieurs sites de charge entraînant « Out of Order ».

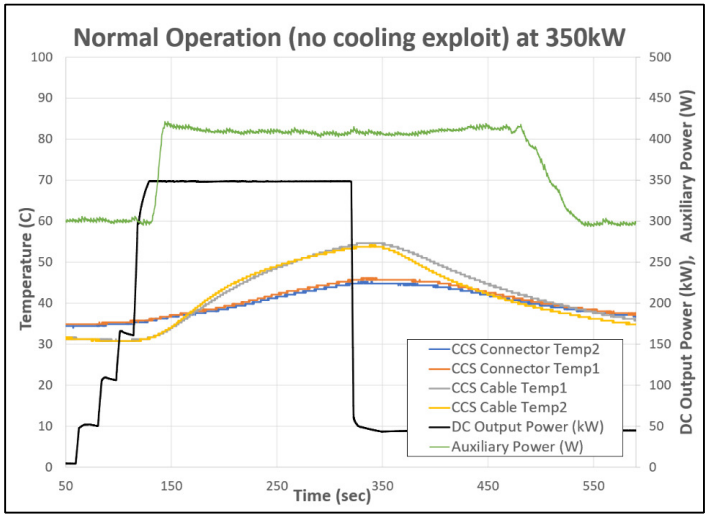
<u>Principal élément à retenir</u> : La mise en œuvre et le fonctionnement corrects du protocole OCPP sont essentiels pour éviter plusieurs EHC à cotation élevée.

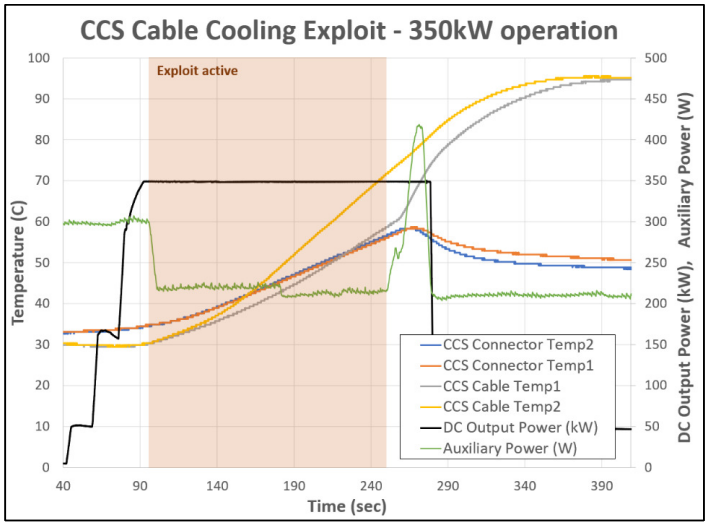
EHC nos 2 et 8 : Exploiter le câble refroidi par liquide

- VE <u>avec</u> mesure de la température de l'orifice d'admission du CSC
  - L'exploitation est significativement difficile (manipuler les VE et les recharges ultrarapides).
- Normes industrielles avec mesure de la température de l'orifice d'admission du véhicule
  - ISO 17409
  - CEI 61851-23, 2e éd.
- VE <u>sans</u> mesure de la température de l'orifice d'admission du CSC
  - L'exploitation est moins difficile (manipuler les recharges ultrarapides uniquement).
- Évaluation de l'exploitation en laboratoire du système de refroidissement de liquide par câble des recharges ultrarapides
  - Mesure de la température
  - Commande de la pompe du liquide de refroidissement
- L'exploitation s'est avérée efficace à 350 kW.

<u>Principal élément à retenir</u> : L'exploitation du système de refroidissement liquide par câble est possible lorsque la température de l'orifice d'admission du VE n'est pas contrôlée.

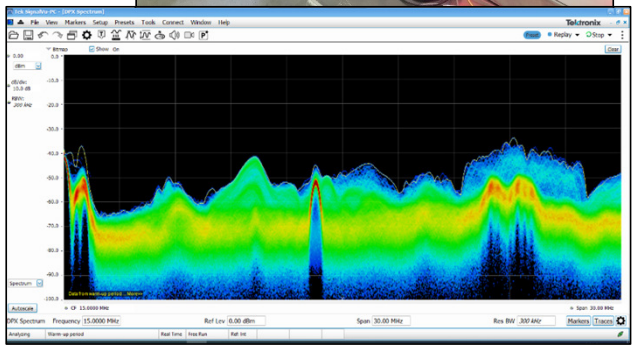


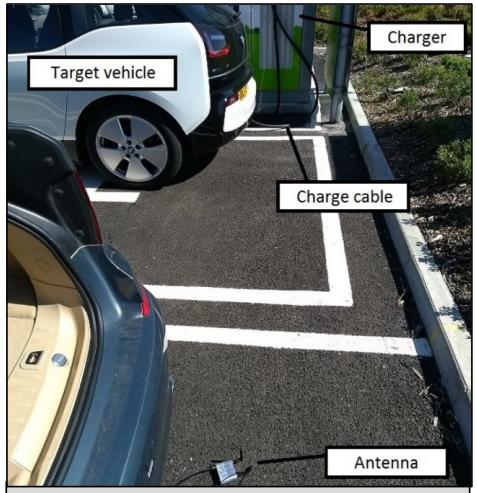




EHC no 12 : Vol ou altération des données / informations

- Le vol de données de la communication du CSC est possible sans connexion physique (c.-à-d. « reniflage sans fil »).
  - Les démonstrations matérielles confirment l'efficacité du « reniflage sans fil » du CSC.
    - L'Université d'Oxford a démontré la capture de formes d'onde et le décryptage de paquets de données avec un câble de CSC refroidi par air à chargeur rapide à courant continu.
    - Le INL a démontré une capture similaire de forme d'onde des informations de CSC à partir du câble refroidi par liquide des recharges ultrarapides.





« Perdre les clés de la voiture : Insécurité de la couche PHY sans fil dans la recharge des VE ». Richard Baker et Ivan Martinovic, *Université d'Oxford* https://www.usenix.org/conference/usenixsecurity19/presentation/baker

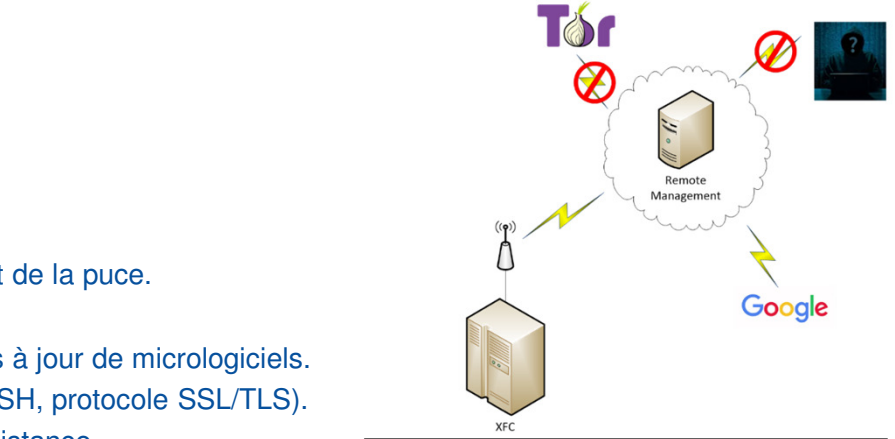
<u>Principal élément à retenir</u> : Avec les connaissances et l'équipement adéquats, il est possible d'obtenir sans fil certaines informations sur la charge du CSC à plusieurs mètres de la recharge ultrarapide.

Solutions d’atténuation

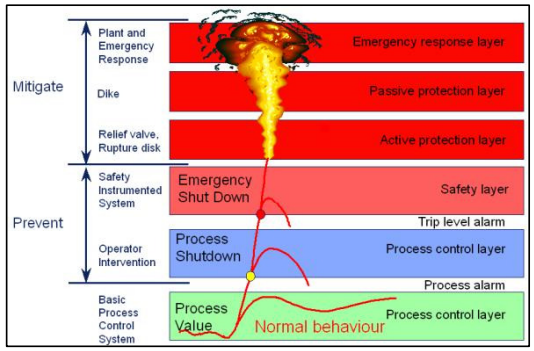
Stratégies et solutions d'atténuation

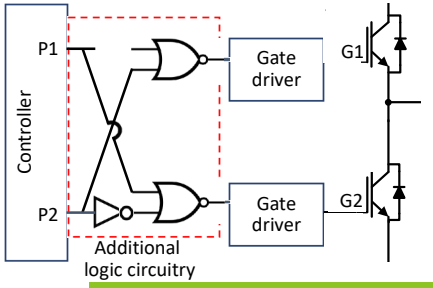
- Atténuations générales :
  - Mettre en œuvre un démarrage sécurisé : utiliser les fonctionnalités du fabricant de la puce.
  - Contrôler la segmentation du réseau (isoler les appareils connectés à Internet).
  - Mettre en place une signature de code sécurisée pour les correctifs et les mises à jour de micrologiciels.
  - Utiliser des méthodes de communication réseau sécurisées (p. ex., protocole SSH, protocole SSL/TLS).
  - Détection et prévention des intrusions (SDI/SPI) sur le(s) serveur(s) d'accès à distance.
  - Mettre en œuvre une architecture de réseau à confiance nulle.

- Atténuations particulières :
  - Arrêt plus lent et contrôlé lors d'un événement d'arrêt de charge.
  - Stockage local de l'énergie pour amortir la connectivité du réseau.
  - Blindage en treillis métallique du câble de CSC.
  - Logique de commande de porte supplémentaire (transistors SCOM à technologie μm).
  - Détection d'intrusion dans l'hôte (SDIH) pour surveiller les fichiers système critiques.
  - Système d'instrumentation de sécurité (SIS) surveillant le fonctionnement des recharges ultrarapides.
    - Performances électriques, températures, communications, etc.
  - Gérer et filtrer la connectivité Internet (tunnel ou RPV).



Source : Emerson *DeltaV* SIS





INPUT		OUTPUT	
P1	P2	G1	G2
LOW	LOW	LOW	LOW
LOW	HIGH	LOW	HIGH
HIGH	LOW	HIGH	LOW
HIGH	HIGH	LOW	LOW

Principal élément à retenir : Plusieurs solutions d'atténuation générales et particulières sont disponibles pour améliorer la sécurité des recharges ultrarapides et du TESF et réduire les EHC potentiels.

Résumé

- Événements à haute conséquence (EHC) conceptualisés pour l'infrastructure de recharge des VE à haute puissance
- Hiérarchisation et classement des EHC :
  - D'après la **gravité de l'impact et le multiplicateur de complexité de la** cybermanipulation (similaire aux DFMEA [Analyses des modes de défaillance de conception et de leurs effets])
- Évaluation en laboratoire des EHC terminée :
  - Complexité de la manipulation de la cybersécurité
    - Évaluation des contrôles matériels et des systèmes de communication
  - Gravité de l'impact
    - Essais en laboratoire et simulation par modélisation
  - Affinement itératif de la notation de la priorisation des EHC en fonction des résultats de l'évaluation en laboratoire
- Élaboration de solutions et de stratégies d'atténuation
- Publier les résultats, les conclusions et les mesures d'atténuation
  - Projet de publication en cours d'examen par le VTO du DOE des États-Unis à l'intention du :

Energies Journal : Édition spéciale « Cybersecurity Solutions for Electric Vehicle Chargers »