!

NOTICE: " " #
$ % ! $ %
# " &

" % " ! '
% # "
% $ %
! & % "
$ % !

( ) ! %

) % * *
! !
*
(! *! + & ,
* # ' - . / - 0

1 2 / , 3 4 5 6 7 8 . , 0
8 1 2 / , 3 4 5 8 . . , /
9 1 : ! %
* 1 1 : ; " " " ! ! % ;

) %
! !
%
3 - 7 0 " '
) & <) - 0

1 2 / 7 7 4 5 8 6 3 . -
8 1 2 . 7 - 4 5 , = 7 7 3 7
9 1 : ! %
* 1 1 : ; ! ! % 5 ; : ;

ABSTRACT

) ! ! # %
% " %
! " "
> ?
% * 9 % " # ! 4 !
#
? % % % ! (%
2 < 4 %2 < 4
< — #
__ " !
% <
< ; < !
! %
<
@ % " % "
%
% % !
# <
% % #
% " " !

ACKNOWLEDGEMENTS

" # " ! ! < * $
5 7 7 6 / Q =

CONTENTS

LIST OF FIGURES

LIST OF TABLES

#

.

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
CAN	Controller Area Network
CCS	Combined Charging System
CSO	Charging Service Operator
DCFC	DC Fast Charger
DER	Distributed Energy Resources
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
MQTT	MQTT (No expansion)
OCHP	Open Clearing House Protocol
OCPP	Open Charge Point Protocol
TCU	Telematic Control Unit
V2V	Vehicle-to-vehicle Communication
WAP	Wireless Access Point
xFC	Extreme Fast Charger

1. BACKGROUND

2. PROJECT STRUCTURE

" @ ! ! %
%
chargers. To improve the vehicle indus

- % 5 ?
- <
- > " # !

@ 1

-) < 2 - %
  9 4
- ' % <
  3 < / 9 ' 4
- # " 2 ,
  (" ? . (" '4 #
- < "
  " # 2 / 9 ' 4

@8 50 " " 2 4
2 4
! % # # #
!
% # # # 2 !
% 4 !

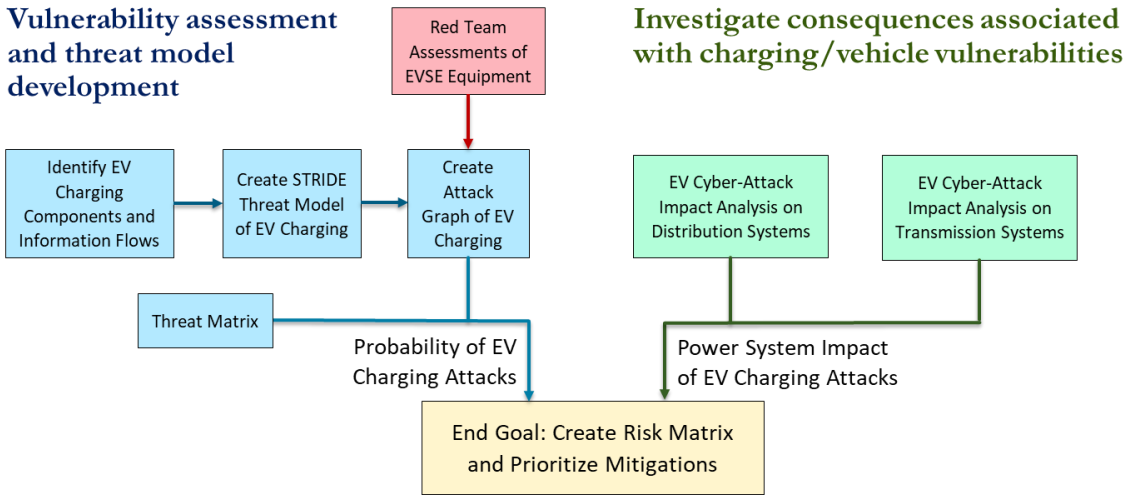


Figure 2-1. Project tasking.

B # 8 50 " % " @ 1

- **Identify EV Charging Components and Information Flows** ! B
& % " @ %
! 9 8 5 ! &
8 2 & 8 4 8 8 4 2 & "
2 ! ! 4
5
2 <5 45! <
2 5 " (4 # E) 9 * +3$; - 6
2) 5 4B! % 5 %
% " %
! < < % %
* ((2 * ((4
7 - 7 ! 3 ! % %
p r o v i d e r b a c k e n d n e t w o r k s t o v e r i f y c h a r g i
* E (2 * E (4 *
(2 * (4) ' !

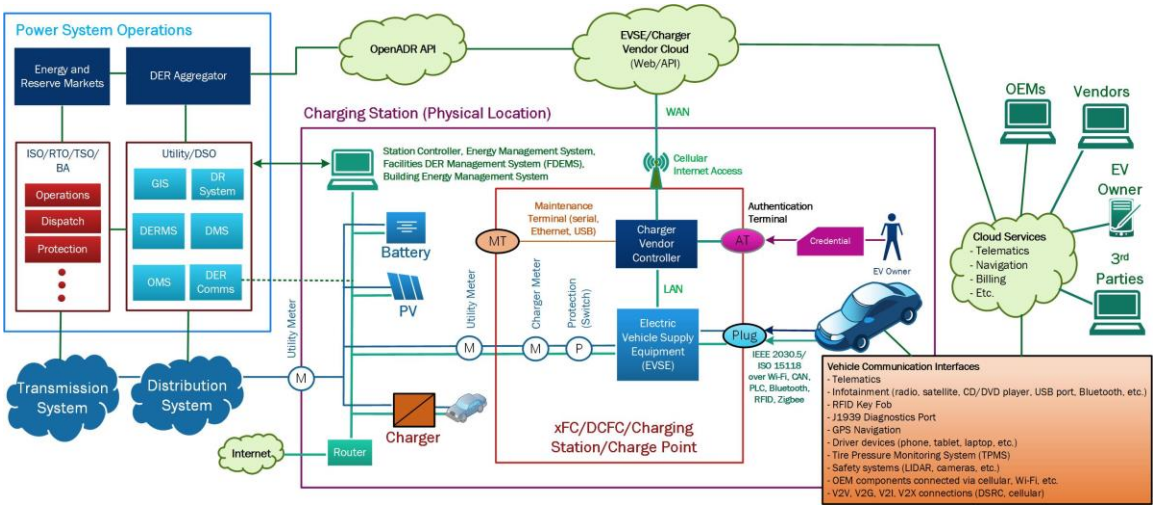


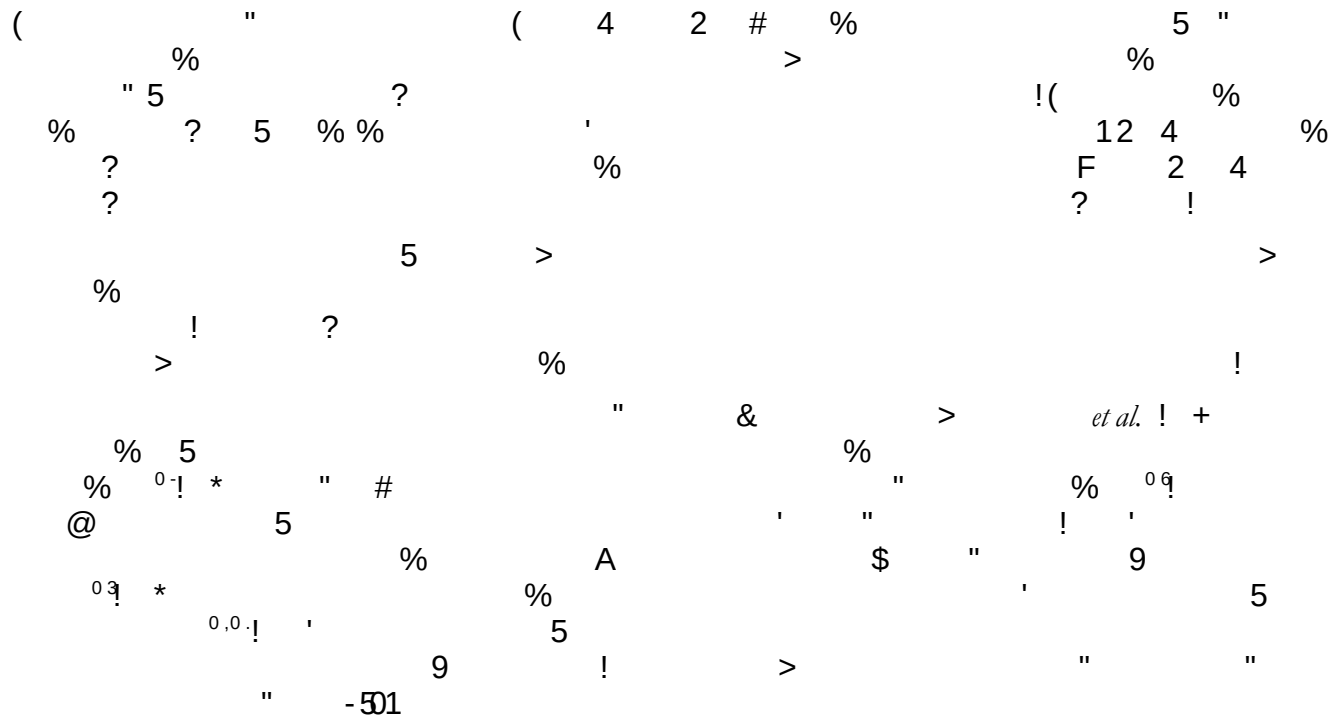
Figure 2-2. Electric vehicle communication systems to different components and entities.

- **Create STRIDE Threat Model of EV Charging** ! ?
! > <
" "
! 2 "! 4
% "
- **Create Attack Graph of EV Charging** !) # "
% % " # % ?
! & % #
" < < " # % !
- **EV Cyber-Attack Impact Analysis on Transmission Systems** ! (@ "
% " 8 % !
# " "
# " < "
!

- **EV Cyber-Attack Impact Analysis on Distribution Systems** ! > "
" 5 5 2% \$ 4
5 % " !
- **Penetration Testing of EVSE Equipment** !
5 5 5 < ? >5 % ?
" % ! " #
" # % & # !
- **Risk Analysis** ! # < # " "
? " # & 5-5[07] ! >
%
< # !
% " #
"
[00] !
- **Prioritize Mitigations** ! + # &
> " 5 ? ;5 " %
! "
% !

[07] , 6-5, "Security for industrial automation and control design," 2020.
[00] !(! !'! !A! A! < !B , "Categorizing Threat: Build Threat Matrix," ! 7!.
[0] !(! ! !H9 , #") 8 , "" S#ANS 2-007 ! 7.!

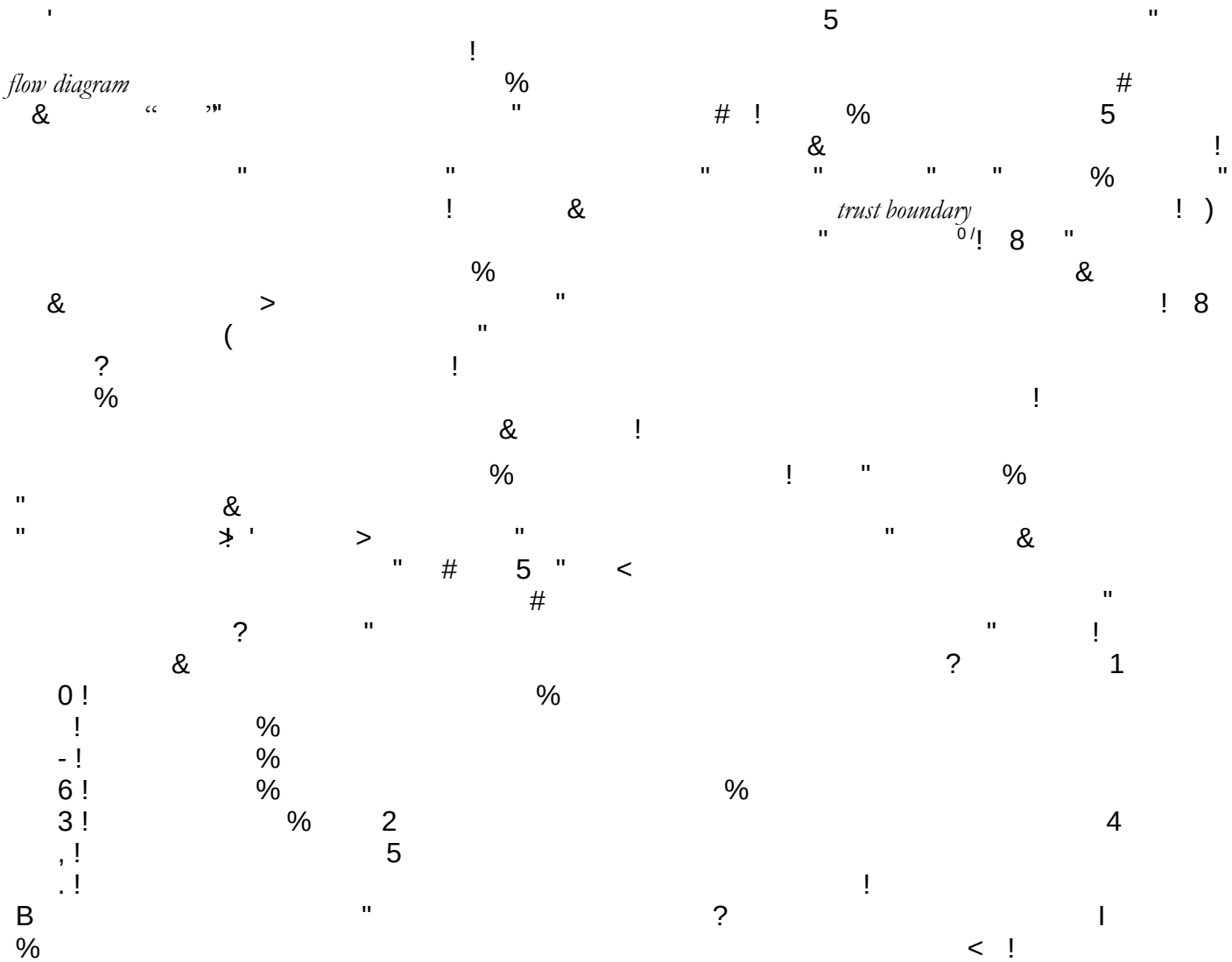
3. THREAT MODEL



! Spoofing: masquerading as a legitimate use
! Tampering: modification/editing of legitim
! a certain action executed in
! Information disclosure: data breach or una
! Denial of Service: disruption of service f
!

Table 3-1. STRIDE Threats

STRIDE Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization



[0] Miller, M, 'Modeling the threats to, your product, using data flow diagrams and trust boundaries' http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/sdl_threatmodel.asp

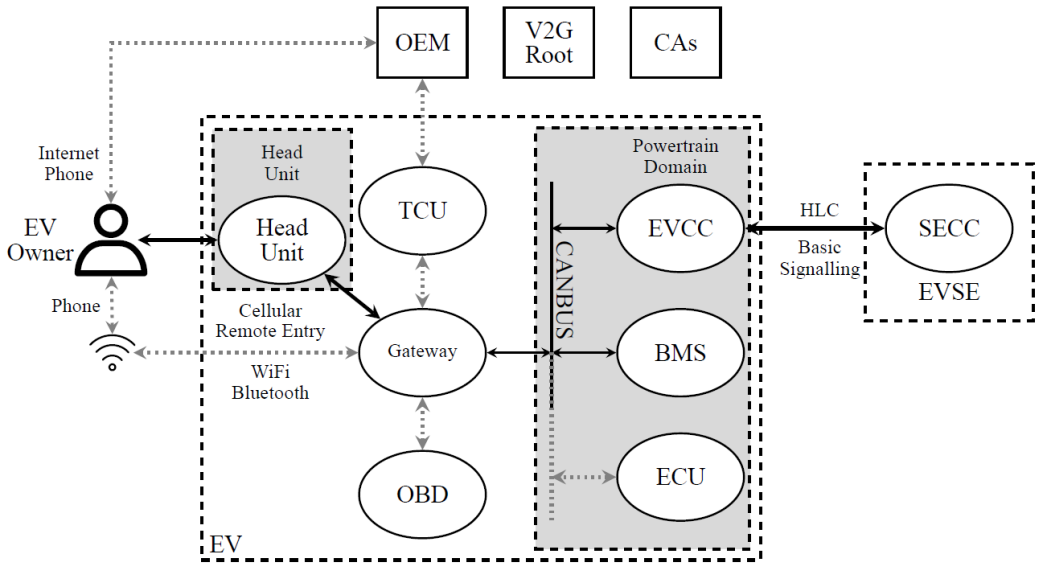


Figure 3-1. The EV data flow diagram.

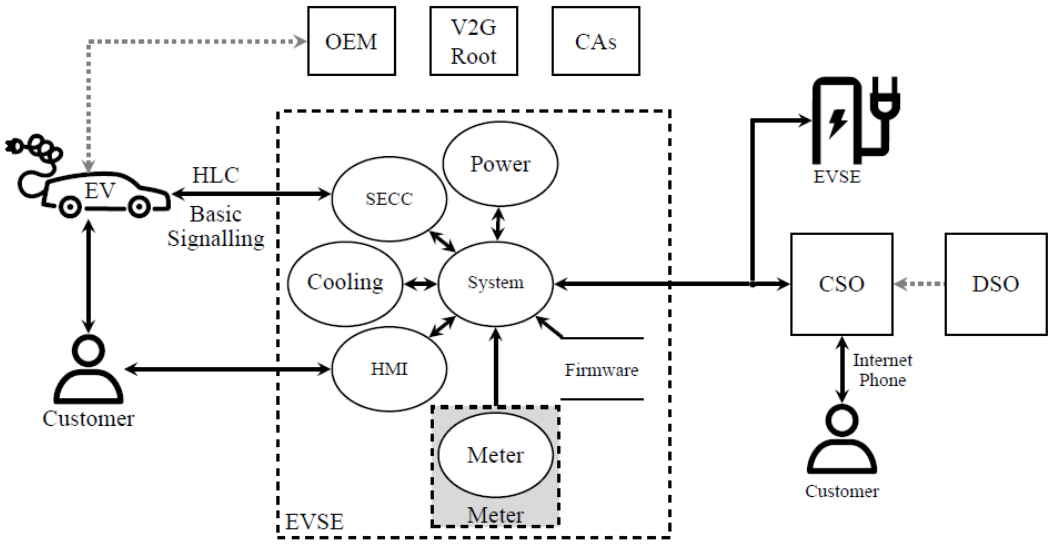


Figure 3-2. The EVSE data flow diagram.

" 8 -5! %
! %
% & "
# !
% % ! (
5)5 % " ? !
24 * 0300/ <
! E " "
< 5 ! "
(67 74 ! # #
" # ?6!) 5 2E9 4 >
" %
!
B 2 4 " " #
% 4 2 * " @
% !

6 E " + + $ > # 1)
70.! ' 1 1 ; ; " " " ! ! % ; ; % ; "5 & 5 5 5 5 5

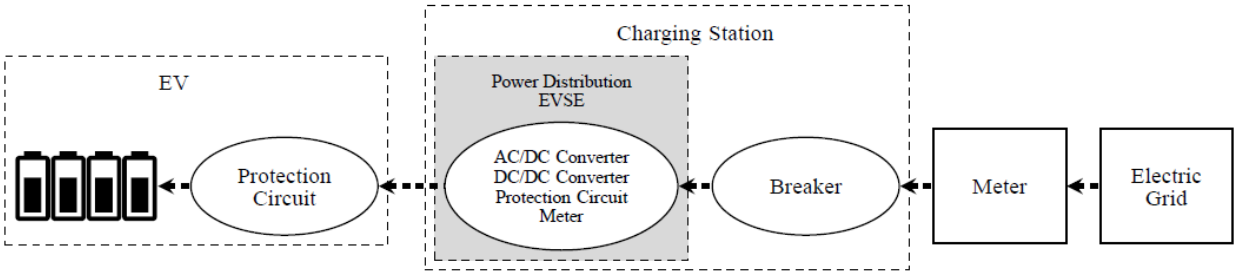


Figure 3-3. Charging infrastructure electric power flow diagram.

8 -5 "
E (# < - 3# < 6 / 7 " # !)
"
" " %
" " < " '
) 5 # 2 "
" !)
! B
" [3]!
" >
% ! ? !
' &
?
& #! ' #
" " !

Consequence #1: ; !
Attacker Payoff: (" !
Threat:) > 1

- "5 5 < " 1
  - **(Local)** '
  - **(Local)** &
    a p p l i c a b l e *t0o3 0 1 / e m o t e ” 4
  - **(Local)** 5 @
- **(Remote)** ; # !
- **(Local)** < & < " #

Threat:) " 1

- **(Remote)** " 5 5 < " 2 <
  ! 5-7 .$, 0 0 3 * 0 3 0 5 0 1 /

[3] B o h n , T , “ M u l t i p o r t , 1 + 5 M W c h a r g i n g s y s t e m f o r m h o r i z o n ? , ” 2 0 2 0 .
F a l k , R & F r i e s , S , ‘ E l e c t r i c v e h i c l e c h a r g i n g i n f r a s t ! ! % % 2 ' 4) ') 7 0 !
B a k e r , R & M a r t i n o v i c , I , ‘ L o s i n g t h e c a r k e y s : W i r e l e U S E N I X S e c u r i t y S y m p o s i u m S E C ’ 1 9 , p p . 4 0 7

- **(Remote)** " 5 5 <* " *
- **(Local)** " "
  7 0 6 ! 0 0 3 4

Threat:) " 1

- **(Remote)** T a m p e r w i t h l o g s i n t h e c h a r g e r ' s m e m o
- **(Remote)** " 5 "
- **(Local)** 5 5 * " " 2 #
  " # ? 4
- **(Local)** " <5 5 "
- **(Remote)** <
- **(Local)** " E 9 %

Consequence #2: # !

Attacker Payoff: < !
% " !

Threat:) 1

- **(Local)** " + 9 "
  < 5 5 " 1
  - **(Local)**
  - **(Remote)** "
- **(Local)** (" "

Threat:) % # 1

- **(Remote)** % * % %
- **(Remote)** " E 9 "
- **(Remote)** * " 5 5 * "

Consequence #3: % 2
, ! 0 4 V % / " " = % V ?[7] V ?
% -0!

Attacker Payoff: !

Threat:) 1

- **(Remote)** V %
- **(Remote)** %
  " %
- **(Remote)** * ? % # %
  ? " " % #
)! & 8 %

/ A *$ 9 5 a a d a n y , E , Y o u s s e f , A , & S h a e a t b s a n o , n M , h e ' I P m o p w a e c r t G o
7 0 = (" – 3 2 7 (0 = 4 ! ! 0
= ' A B 8 1 (5
0 5 3 6 5 % 5 7 7 0 = !
-7 A c h a r y a , S , D v o r k i n , Y , & K a r r i , R , ' P u b l i c P l u g i n E l e
V i a b l e ? ' , I E E E T r a n s a c t i o n s – 3 0 0 - S m a r t G r i d , v o l . 1 1 , n o .
-0 9 $ k s a g a i n s t t h e U . S . p o w e r g r i d
B % 7 0 / !

% ! ' -- -6 % #
? B ! V #
% !
Threat:) " < 1

- **(Remote)** % % " + 9 -3
- **(Remote)** < % V
- **(Remote)** 9 "

Threat:) % 1

- **(Remote)** " "
- **(Remote)**) % V

Threat:) 1

- **(Remote)** % # * V V * "
- **(Remote)** % >

Consequence #4: " % <
Attacker Payoff: < % !
Threat:) " " % 1

- **(Remote)** % %
- **(Remote)** E V S E ' s <
  " 2 ' 7 0 = 4
- **(Local)** " c h a r g e r ' s "

- **(Local)** " 2 ! ! 4

Threat:) " 1

- **(Local)** " < V V (
  "
- **(Remote)** (
- **(Remote)** (% >

Attacker Payoff: (@ " > <
Threat:) " 1

- **(Local)** "

- **(Local)** " #

Consequence #5:
Attacker Payoff: $ " #
Threat:) (" # 1

-Fairley, P, "800,000 micr-oii mvcemtedasy ,r'e mvoit cevwydr leltr hof Aug
1;; ! 5! 5 ;5777757 % 5 5 5 5 703!
-- + ' A 5 ?% " < %
7 0 7 7! ' 1
1";" "! ! %; ; ; ; 7 7;7,; .3; 0==D D 7!7D D3!0! 7D0!0
-6 (" 1 $5% % % <
00) 7 0 70=!1;';'1" "! ! ;5% 5 5 # 5 5 5 ;
-3Oyler, A & Saiedian, H, 'Security in automotive telema
the existing and emerging at%a!c+ v6-66-7 7r7s0',!, Security Co

- **(Remote)** "
- **(Remote)** & (* & #

Consequence #6: %
Attacker Payoff:
Threat:) 5 % 1
- **(Local)** " * " #
- **(Remote)** < % " % ; %

3.1. ISO 15118-2 PKI

) # # # 2 (A 4
* 0 3 5 0 0 / " ?
5 5 < < a n d 5 p 5 h a g r P g C 4 " (
% ! <> " "
% & " # * 0 3 0 0 /
" # %
! * 0 3 0 0 /
< 5 5 ! @
>
%
% ' !
% " "
& ?
! $ %
" <
? 5 5 - 3 %
" % & !
" !
% <
! & %
* 0 3 0 0 / ! 9 % " (?
" > !
(" % "
' 8 ! 8

% 5
% % % 2
5 % !
5 !
% ! 5 * 0 3 0 0 / (5 3 ,
% & % 5
! < $ 2 "
4 " 5 " ? ! ?
5 3 (, - 7 - 2 5 4 ? / ! 7 3 & 0 7

or both don't support ISO 15118

safety instrumented system

et al.

Following a white paper titled “

”

address the governance concerns raised in the

*

—

0 ! **Certificate Policy.**)

2

2. Algorithms and Protocols. (A ;

public key cryptography and transport charge" use case.

minimum

3. **PKI Hierarchy.**

[36] [33]

6 ! **Key Management.** # "
! " <
5 % 2 % < % 5
% % ! 4 %
! %
% % < ! E " % "
" " % "
!

5. Certificate Revocation Policy. * 0 3 0 0 / %
* (2 * % (4 G ! 3 7 =
! 5 5 5
" * (% % !

, ! **Identity and Access Management.** ? %
* 0 3 0 0 / ! < #
% % %
% ! % % "
%
" % ! ' ? %
%

7. Business Continuity. * 0 3 0 0 / "
E ! " %) !
" %
!

8. Audit Policy. 8
!

= ! **Incident Response, PKI Auditing, and Physical Security.**

> !

4. ATTACK GRAPHS

) # " # # ; '% #
? @ % ! # #
% @ % "
8 650 ?
< " #! # % %
compromise of an EVSE provider's business net
> # % % %
" # (? – <
! %
% # "
# % # !
" "" @? 1

- Can the attacker "pivot" between the compo
" P
- # > # P

8 % *could* #
" # < [3], !

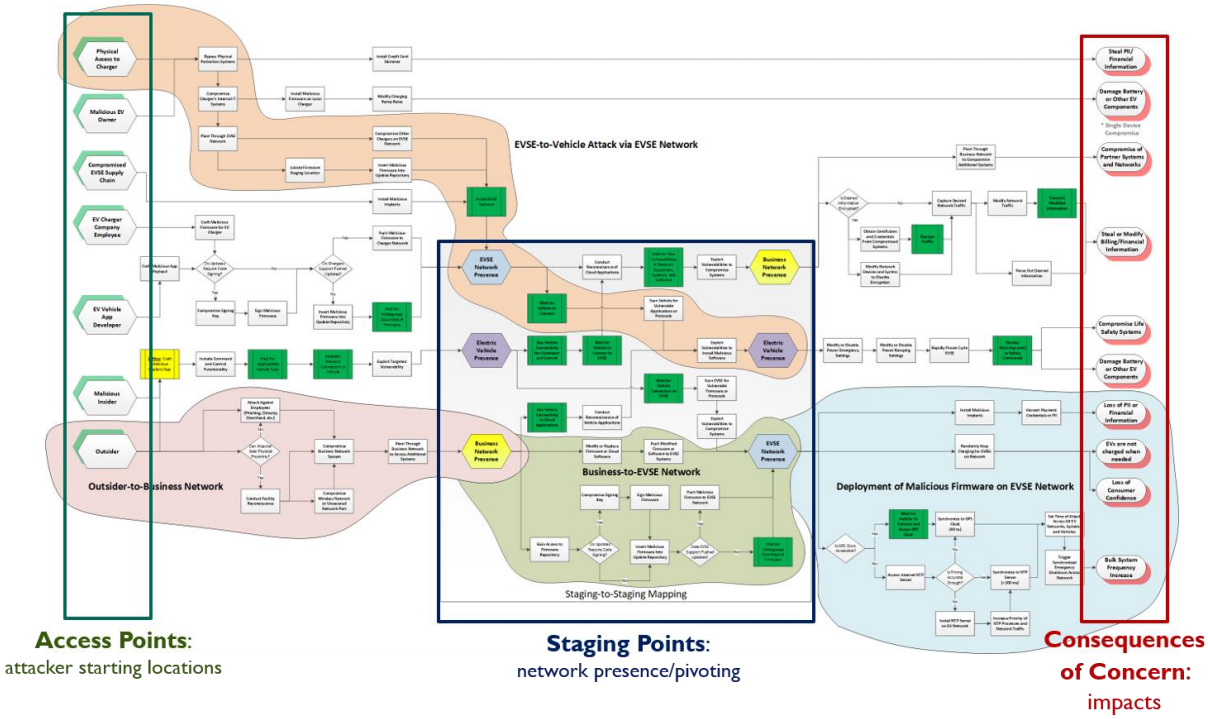


Figure 4-1. EVSE Ecosystem Attack Graph.

[3] B. Anderson, "Securing Vehicle Charging Infrastructure
< (57 H) 7/ 1! 1;;"""! ! ; ;
--=73-,-0D D< D D D) D D

.

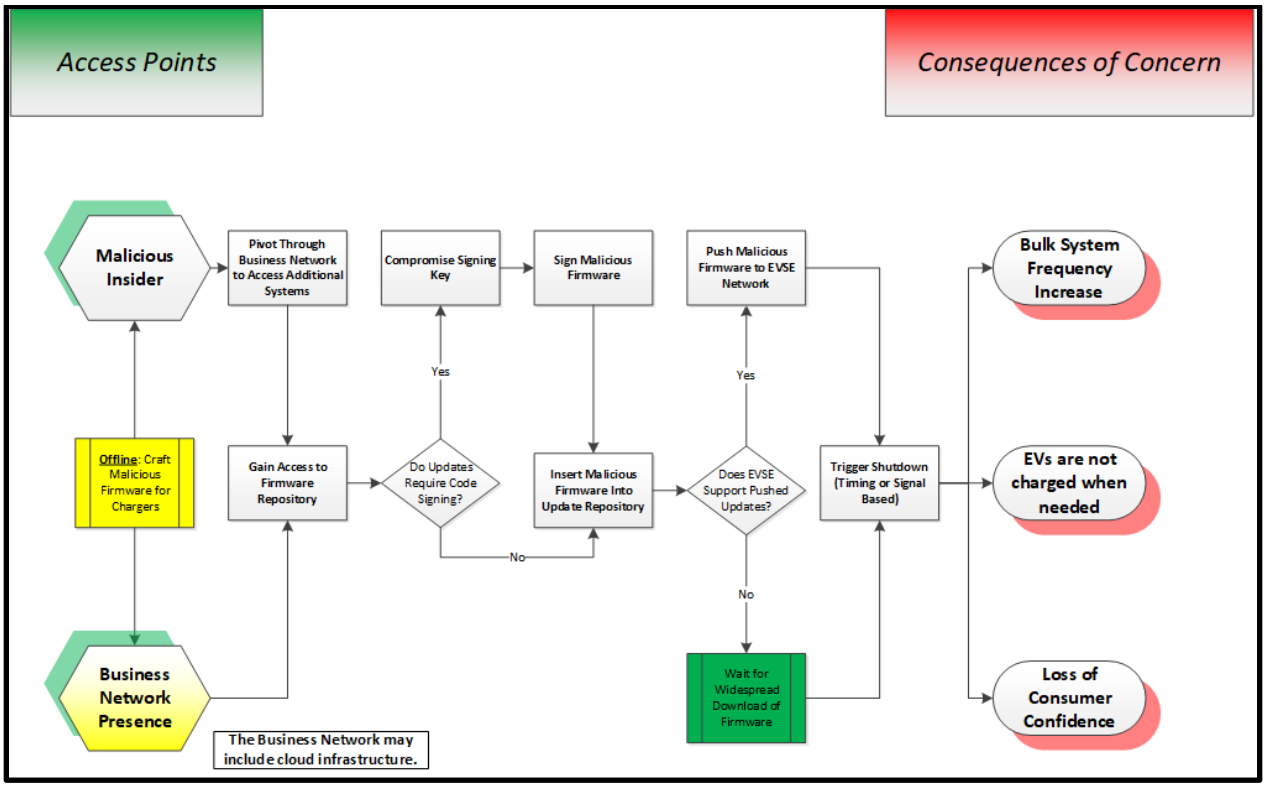


Figure 4-2. Deployment of Malicious Firmware

< ! the attacker needs to be
% "

* # " #
# ? ! 8
" # "
"
? !

* # " # % " #
% " * !% <
? # %
" " " % ! < ?
% # #
@ "
! * #
<) ! < " # "
attacker can choose that route to immediately
? < #
< " # " " !

* " # "
mechanism that will achieve the attacker's
< < " ! " "

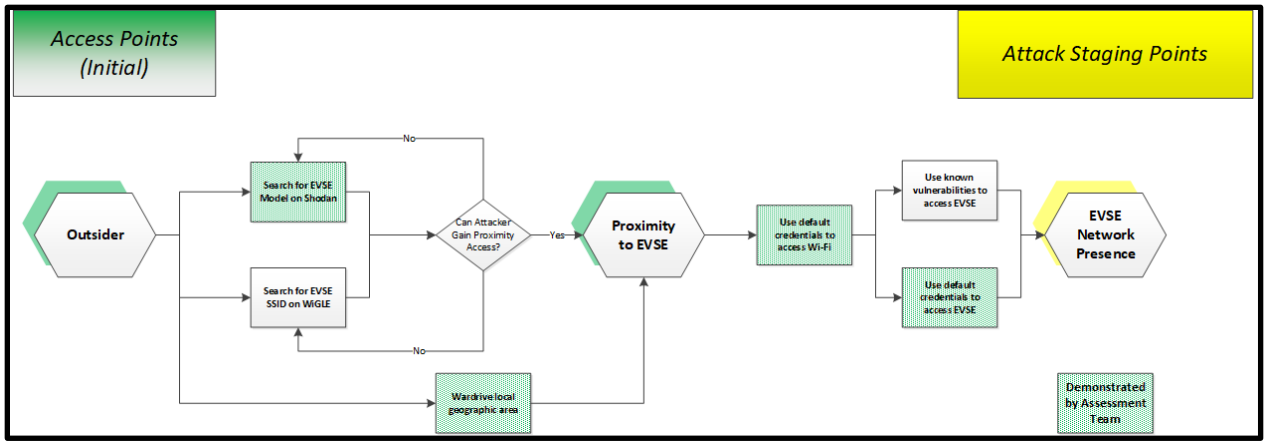


Figure 4-3. Assessment Attack Graph

[3] B. Roy, Z. Ivanic, P. Windover, ChArgRiundge rS, t aatnido nM. DeSphlioryk

5. EVSE ASSESSMENTS

5.1. Anonymized Assessment Results

- E 9 n t t h e " t e a m ' s

E " % ? %
% %
% # % F
& ! %
% @ & ? %
!

" # % % %
< ! 1 + " # * <
" # * < * !
5 "! " #
@) &)
(3 /

5.1.1. Business Network & Operations

L) ! 2 4 " % >

L) ! 2 4 (" > <
!

L) ! 2 " 4 < > "
!

5.1.2. EVSE Security

L + ! 2 4 < % ?
!

L + ! 2 4 % ! <

L + ! 2 4 ! %

L + ! 2 " 4 % !

5.1.3. EVSE Network & Operations

L ! 2 4 < " "
!

L ! 2 E 4 < " # 2 & 4 " ! " #

L - ! 2 E 4 < % >

L 6 2 E 4

L 3 2 E 4 < !

L , ! 2 E 4 < % !

L . ! 2 9 4

L / ! 2 9 4 < ? " + # !

L = ! 2 9 4 < " "
!

L 0 M2 9 4 < % !

5.1.4. Electric Vehicle Operations

% !

6. POWER SYSTEM CONSEQUENCES

6.1. Transmission Impacts

5 area oscillations along the California Oreg

only

must

[3/] Edison Electric Institute, "Electric Vehicle Sales For

composite load model's internal protection and

impact factor

$$IF = \frac{\text{peak of the applied load (MW)}}{\text{control load (MW)}}$$

6.1.1. Load Drop Scenario

% 5 " " < " 5
B PowerWorld's "simulat
5
! B
G8 ! > 5'
> !
) < " A 59 *et al.*,[6] " @ %
7 /! (',[3] " # -!, %
" ! 7 / B A 59 % 60
used in WECC's production cost model simulati
" # F 8 " 5 " #
" # < 60
of 22 load areas used by this work's transien
" > <
A 59 of 10.8 million electric vehicles natio
% # < 0/ ./ 9B "
# < Q/ ,77 9B " #! 8
" > % < "
>
" > < !! / ,7
B "8 ,50"
% 5& ! "& < " "
% % " " "
A 59 *et al.* <
!

,[6]9! A 59 ! % ! ! + ! 9 @ 9! $(O
1 E <) B ! ! (" $ O (' 7 7!
,[3]9!) & 5O(< 9 # (@ ! -77 700,0- O
' ( )) 70.!

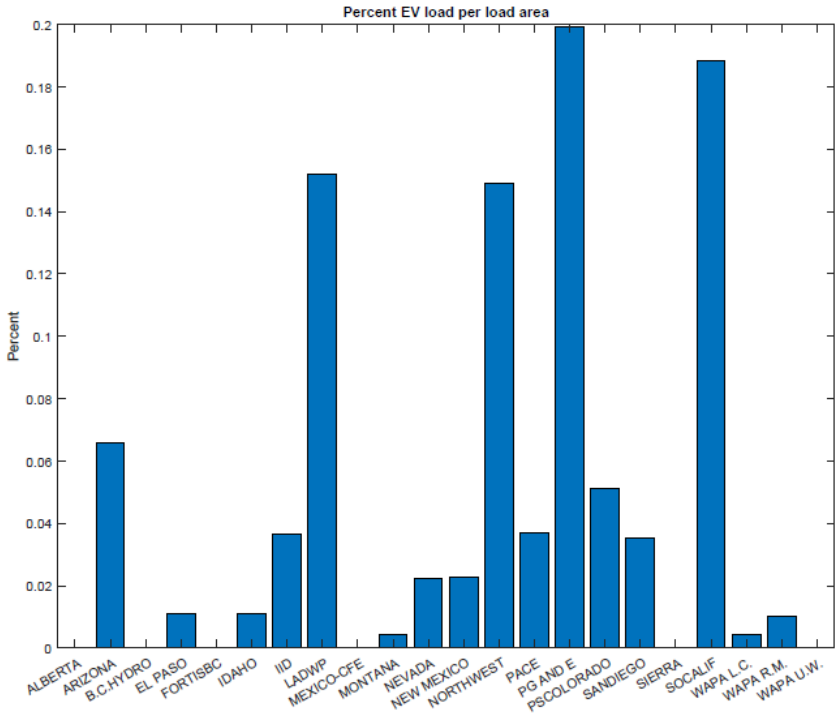


Figure 6-1. Percent EV load distributed to each load area in 2028 WECC planning model.

8 & / , 7 7 9 B < "
"
% !
" % %
< " % % !
% " ! 8 ? %
% + 2 C 7 9 <) % 4 "
%8 , 5 8 , 5- 8 , 56!) / , 7 7 9 B
%
% 2 Q - 7 9 B Q 6 , , 9 BB 4 !
% Q 0 , = $ B % Q 0 , - $ B
WE C C ' s % "
5 % % ! 7 ! - N

B
+ !) % 8, 9 B5
8 , 5- ' ? %
+ % ! ?
(' 57 6 + ' s " % 5 ? , 7 ! , E > 5
0 / 7 !A % !
+ % 50 ! 0 7 ! = "
" % % #8 , 5- !
% @ 7 ! = % 7 ! = ! $ %% % %
8 , 5- 8 , 56 % > % %

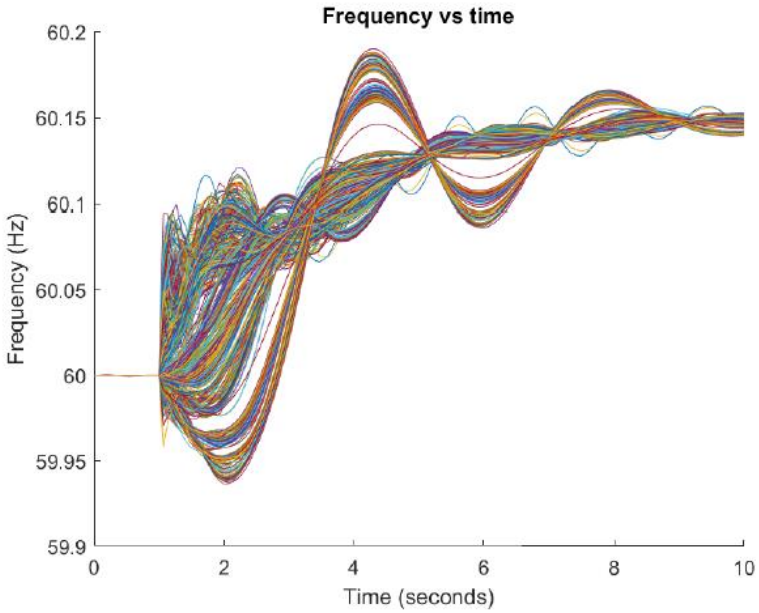


Figure 6-2. Frequency vs. time for operational BES generator buses with >20 MVA base.

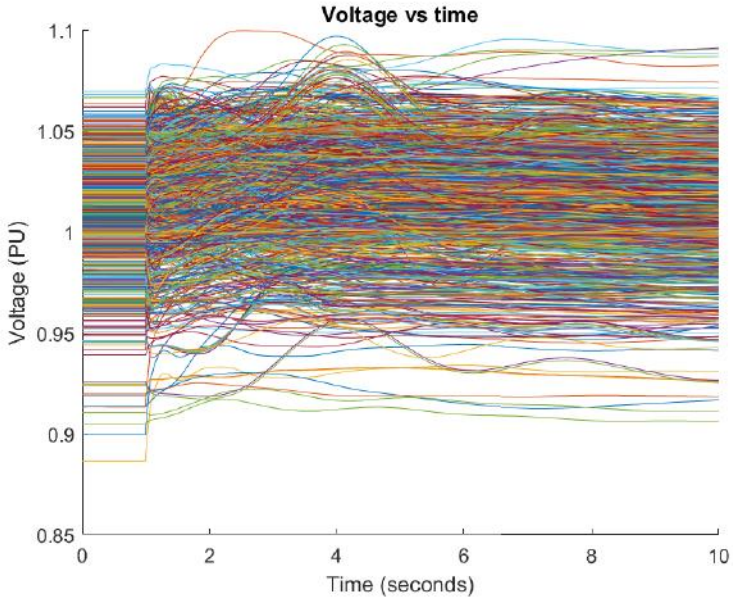


Figure 6-3. Voltage vs. time for operating BES generator buses and >20 MVA base.

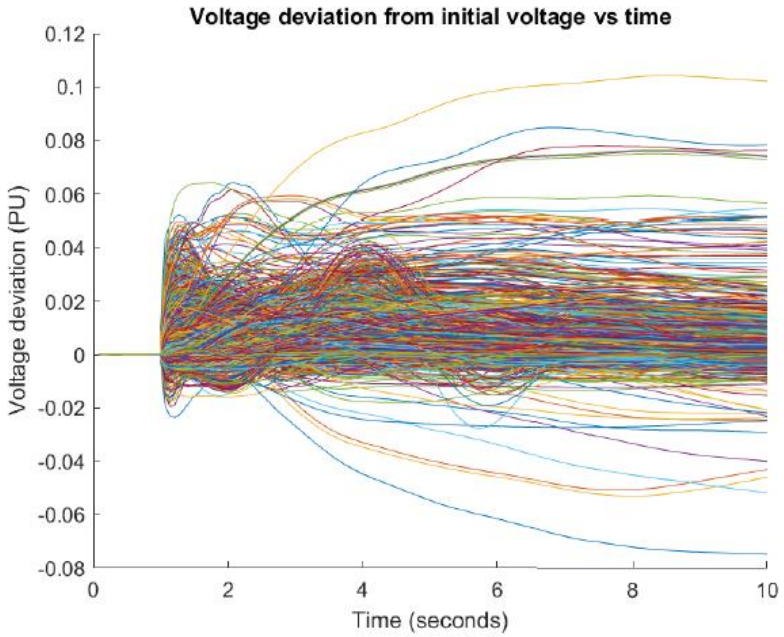


Figure 6-4. Voltage deviation vs. time for operating BES generator buses and >20 MVA base.

6.1.2. Load Modulation Event Scenarios

5 % B B 4 2
2 4! 8 & 7 7 3
7 9 5 B 5 e a # k f o r c e d o s c i l l a t i o n c l o s e
5 7 5 7 9 # B # *
'' ! 7 0 , 7 7 9 B $ $
! 6 7 9 B " S #
& 0 6 7 7 " ! '

B B " # % F %
" % " 5) 2) 4 5
+ 2 + 4 ' / !) " ? % %
) " !
+ ?) +
(" 9
") ' = !) ?
" "
) ! "

' ') ' O *) 1 '
) ' 0 0 7 0 / ! L * M !) % 1
1 ; ; " " " ! " ! ;) % ; *) ! ! L) 0 7 7
' ' !
' / ! " # O " ! O B 7 0 ! L * M !) % 1
1 ; ; " " " ! " ! ; ' ; B (0 - 7 0 0 - " # ! ! L) 0 7 7 7 M !
' = !

7 B O B H > O
0 0 7 0 - ! L * M !) % 1
1 ; ; " " " ! " ; ! ; B N 7 H N 7 9 N 5 7 N N 7 7 * 5 7 0 5 0 5
' < 0 ! 0 ! ! L) 0 0 7 7 M !
0 B O B H > O
0 0 7 ! 0) ! % L * 1 M
1 ; ; " " " ! " ! ; ' ; B N 7 H N 7 9 5) N N 7 7 N 7 5 7 0 5 0 5
' < 0 ! 0 ! ! L) 0 0 7 7 M !
!) 8 ! (? 5 E ! 9 O)) #) ("
) # 9 (O ! $ 5 % . ! = 7 0 / ! 6 ! /,
E ! ! + " ! ! O 5 (#) # % B O !
!) E ! 9 5 8 ! (? O # O ("
% % $ 2 $ 4 B 7 0 3 !
!
!) S ! % # ' ! A 5 O (< (R $ 1 # < "
< P O $ % 6 3 0 ! 0 - 0 0 % ! , 7 7 ! 3 7 1 = =
0 7 ! 0 0 7 = ; $! 7 7 ! = = 6 0 . . !
) ! (! (" O > # (
2 4 A
' ! $) ! $) ! $ O (")
))(") *European Control Conference*
(7 7 !
= ! S # 9 ! $ # O % ")) # ("
O 8 % ! 0 ! 0 7 0 = !
7) ! 5 E ! 9 5) ! 5 $ O 5 +)) #) ("
$ O ! $ % ! 5 , . 6 ! 7 6 0 0 ! ! , , .
0 & "
% !(" >

PSS makes the generator “resist” changes in t

!System modes are determined using PowerWor
bus voltage angle profiles generated in s
and the magnitude of the mode’s real porti

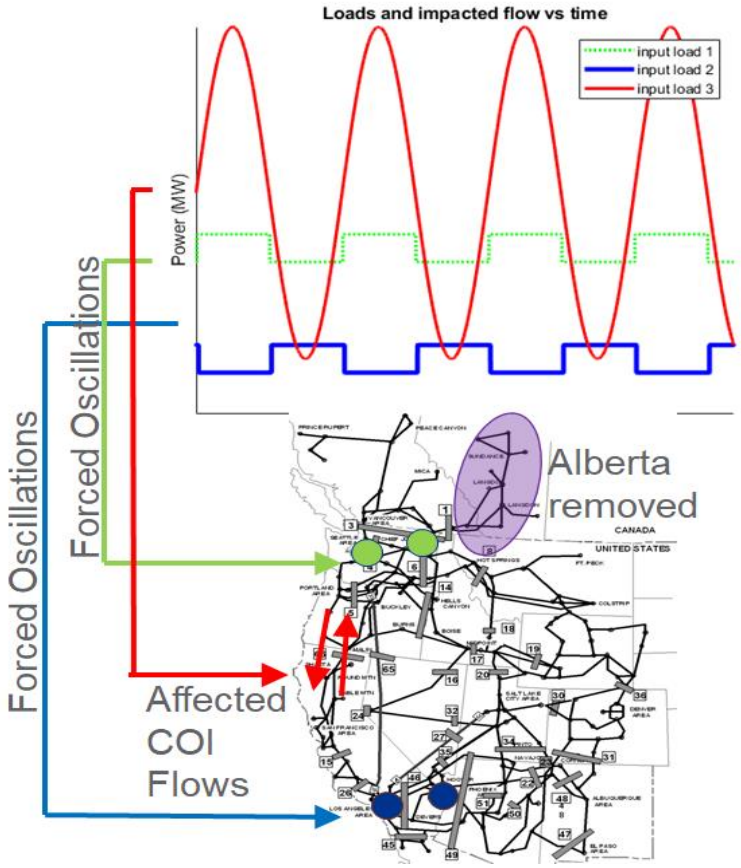


Figure 6-5. Load oscillation simulation.

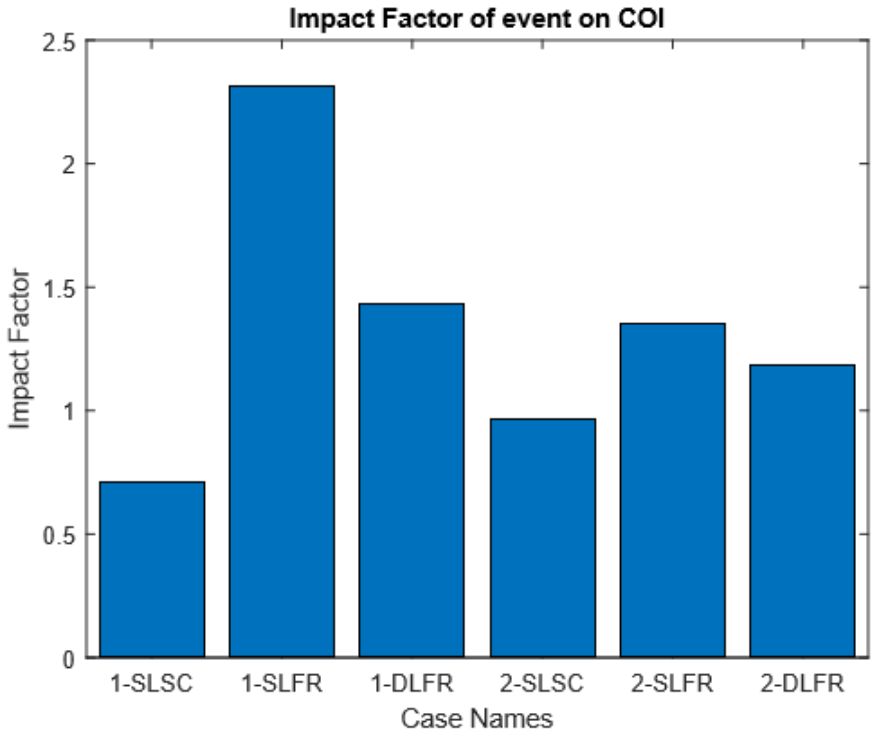


Figure 6-6. Impact factors by case names

Table 2: Summary of generation and load tripped for the load modulation in simulations.

Case	Generation Tripped (MW)	Load Tripped (MW)
1–Single Load Southern California (SLSC)	7 ! 7	7 ! 7
1–Single Load Frequency Response (SLFR)	7 ! 7	7 ! 7
1–Distributed Load Frequency Response (DLFR)	7 ! 7	!
2–Single Load Southern California (SLSC)	7 ! 7	7 ! 7
2–Single Load Frequency Response (SLFR)	7 ! 7	7 ! 7
2–Distributed Load Frequency Response (DLFR)	7 ! 7	0 = ! =

% " % '
> " %
" 8 ' ! " 5
" ? # % 5 % !
%
% " # %
" " ! !
8 % 8 ' 8 ' " " # !
(8 ' 8 ' 1

- !
- 8 8 '
?
" !
- " " # "
% # 9 B % !
< ? &
9 B !
? !

E " % <

% # !

6.2. Distribution Impacts

" # <
" ? ! # % "
? " ' ? " % " "
! < % %
" %
% ? 5 # 5 # !

of EVSE equipment at the distribution level

6.2.1. Vehicle-to-Grid EVSE at End of Feeder

, 5. The "+0.85 PF Charge+Discharge" scenario

American National Standard for Electric Power Systems and Equipment—Voltage Ratings (60 Hz)

It's important to note this is an

[1] R. Seguin, et al. *National Renewable Energy Laboratory*. NREL/TP-5400-61980.

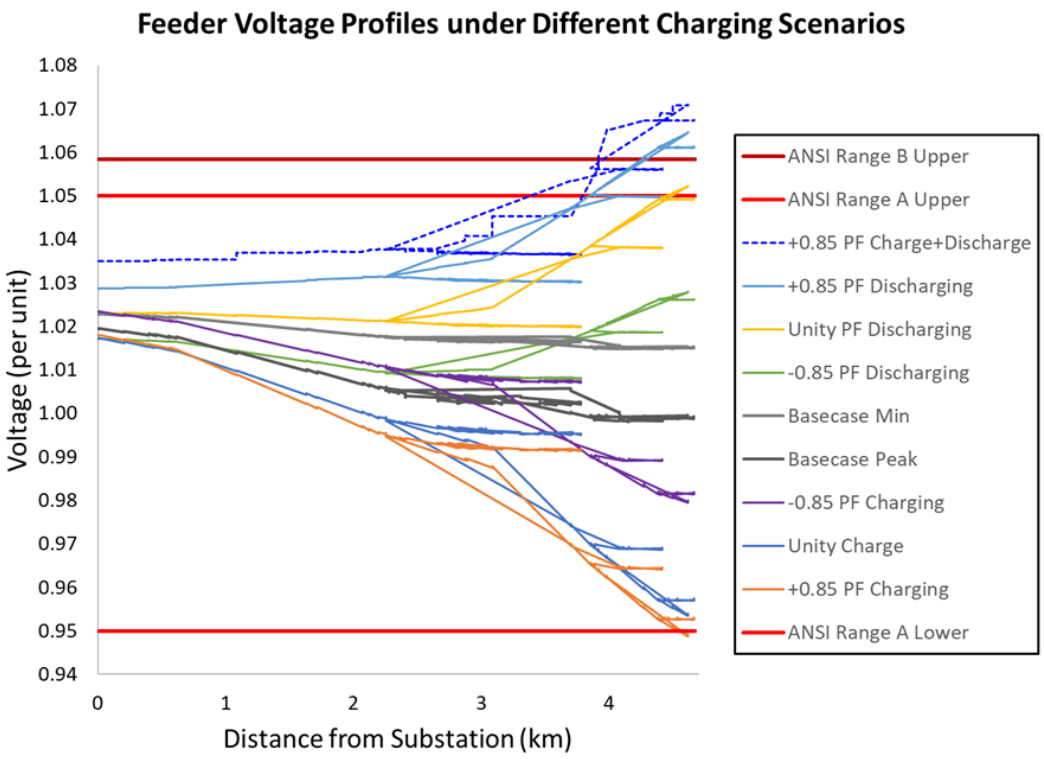


Figure 6-7. Different distribution voltage profiles for coordinated charging/discharging of EVSE totaling 2.25 MW.

6.2.2. Oscillations on the Distribution System

" ,!0! '
% !
% * 5 " 07
! ! " %
! " 5 " ? 2K 4
" " /. ! 2 B<D' 4
2'9 D' 4 % "
5 8 ,5! "
% " B "
" % ! %
"
" % ! + "
% " "
" % !

/. '! H! + # H! ! K > 9! H! ' '!)! O H! (" 8 ")
(< $ O 573-. 70-) 70-

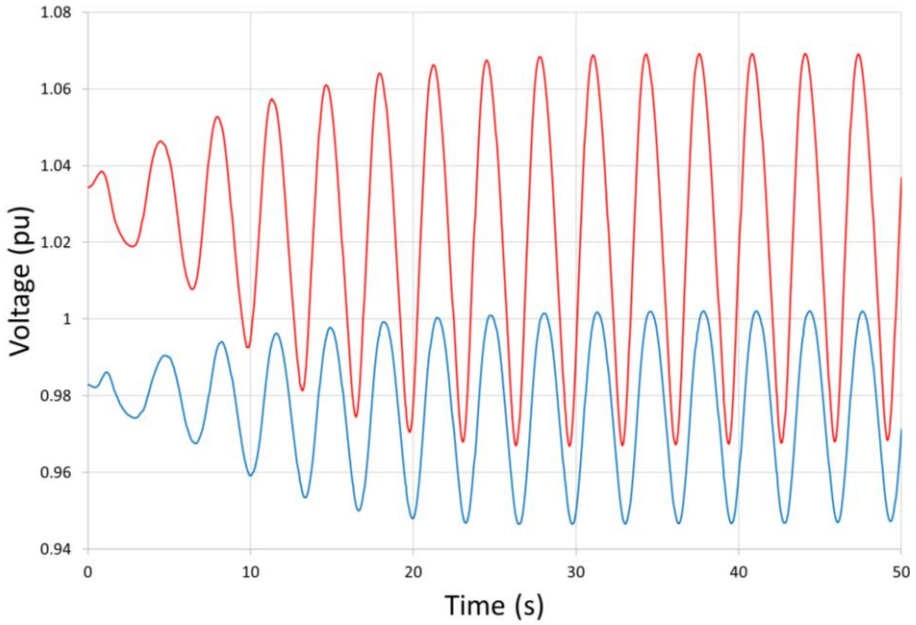


Figure 6-8. The highest (NWV_RES) and lowest (RMN_RES) of the transmission voltage profiles used in the distribution system simulations.

K " 3 7
" 0 3 ; 2 Q , , ! 5, . 5- 7 4 ! 0 3
" "
% ! %
% " "
" " 1
0 ! (# " " %
! 9 " %
%
"
! 8 " % % %
" ! - & % 0 7
" & %
!

Table 3. Maximum and minimum voltages recorded for each study feeder in per unit.

Public Name	Maximum Voltage Recorded (pu)	Minimum Voltage Recorded (pu)
)	0 ! 7 = 7	7 ! / - -
< 0	0 ! 7 . .	7 ! = 0 .
K 0	0 ! 7 , 0	7 ! / = 6
K + 0	0 ! 7 , 0	7 ! = 7
0 ,	0 ! 7 , 7	7 ! = 6 6
	0 ! 7 3 /	7 ! = 6 6
) 0	0 ! 7 3 3	7 ! = =
K 0	0 ! 7 6 .	7 ! / 3 3
K	0 ! 7 6 3	7 ! = 0 =
0	0 ! 7 6 3	7 ! = 0

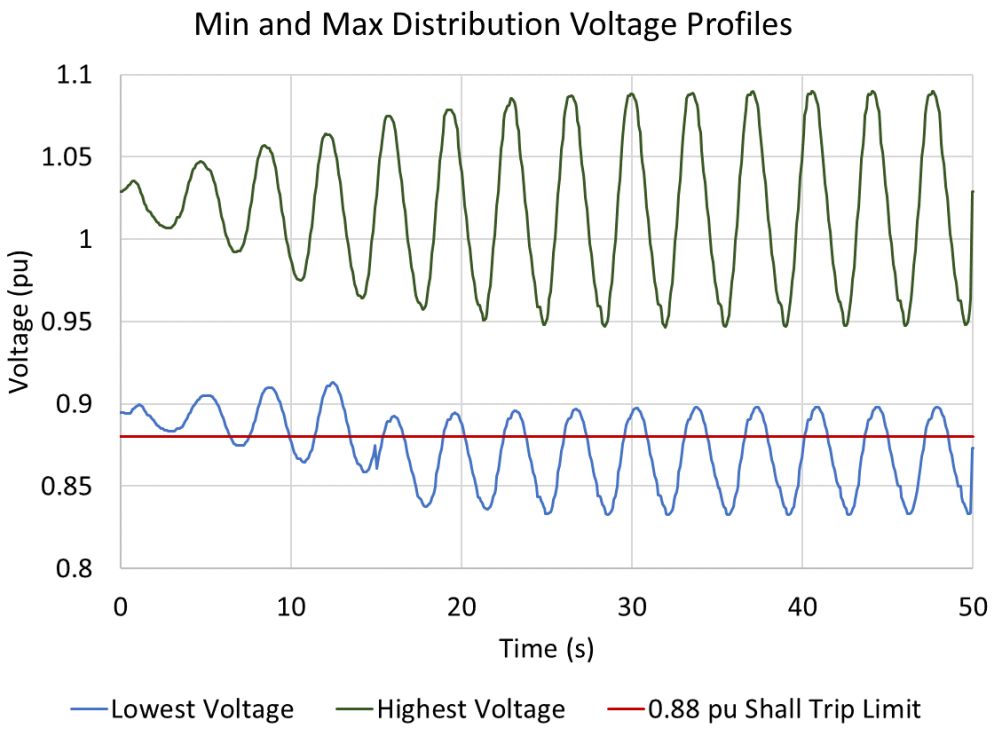


Figure 6-9. Highest and lowest voltage profiles for feeder DA2 under the implementation of the transmission voltage profiles.

Table 4: Must trip requirements for DER equipment for abnormal voltage conditions.

0 3 6 5 . 7 7 -		0 3 6 5 . 7 0 6		0 3 6 5 . 7 0 /	
Voltage (% of base)	**Clearing time (s)**	**Voltage (% of base)**	**Default Clearing time (s)**	**Voltage (% of base)**	**Default Clearing time (s)**
< U 3 7	7 ! 0 ,	< U 6 3	7 ! 0 ,	< U 6 3	! 7 7
5 0 ≤ V < 8	! 7 7	4 5 ≤ V <	0 ! 7 7	5 0 ≤ V <	0 ! 7 7
1 1 0 ≤ V <	0 ! 7 7	6 0 ≤ V <	! 7 7	1 1 0 ≤ V <	0 - ! 7 7
V ≥ 1 2 0	7 ! 0 ,	1 1 0 ≤ V <	0 ! 7 7	V ≥ 1 2 0	7 ! 0 ,
		V ≥ 1 2 0	7 ! 0 ,		

) 8 , 5= " ' ? "
% % % & 0 ! 0 ! E " %
7 ! / / 5 ! ! 7 . — " *0.88 pu Shall Trip Limit*
8 , 5= ' ? "
5 !
!)
% " 7 ! / / 7 ! " "
!
?
% !

7. POWER SYSTEM RISK

@ % # 5 "
> %
8 #! # # "
" # #
! " # F
? " " !

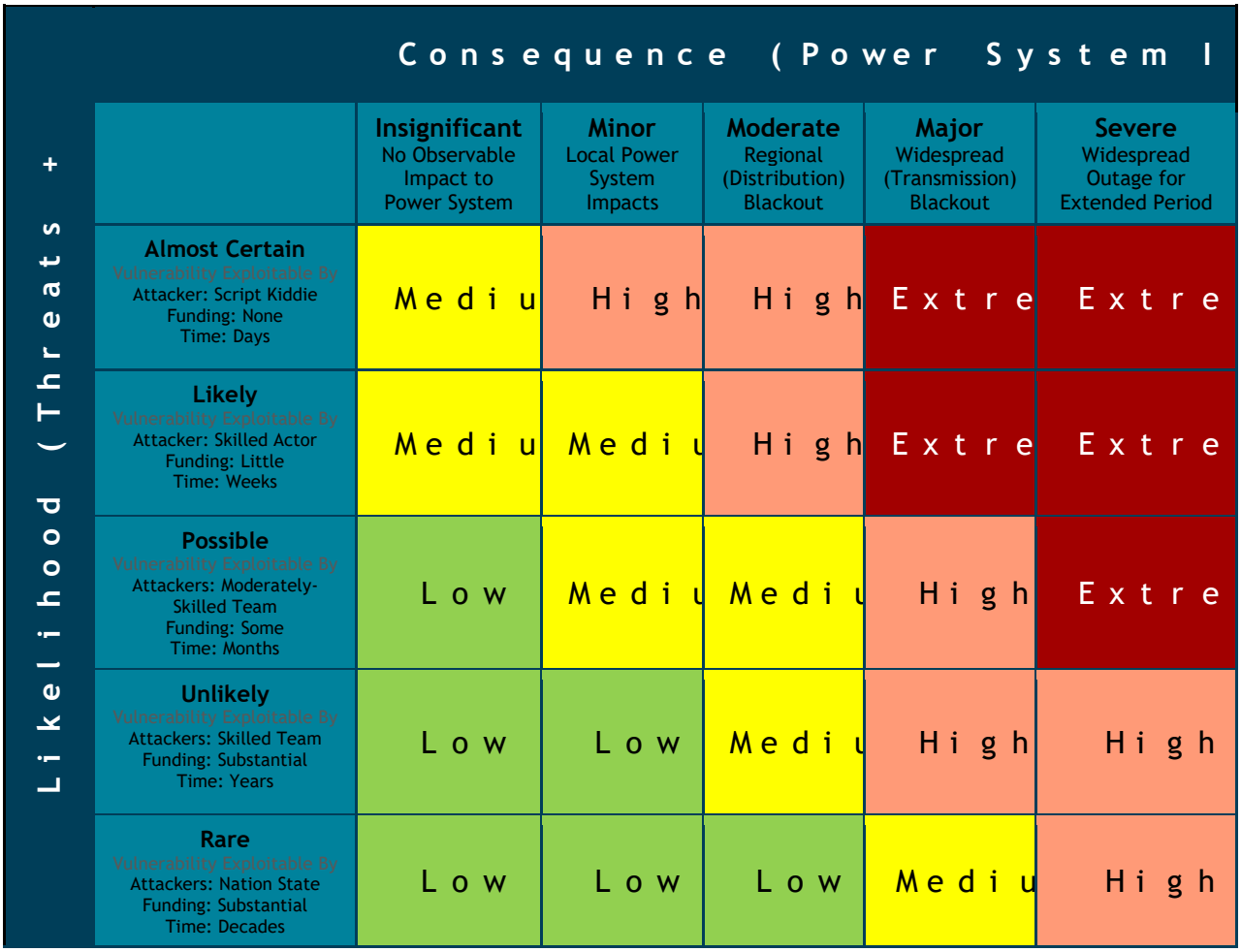


Figure 7-1. EVSE Cybersecurity Risk Matrix

8 .50 " # #&! & % " # 9 //# !
/= ! ? "& % " ,
" # " =7!
"

//M. Mateski, et al. "Cyber Threat Metrics" SAND2012
/=D. P. Duggan, S. R. Thomas, C.>K. K. Veitch, L. Woodard. "
Matrix." SAND2007
=7J. Johnson, et al., "Power System Effects and Mitigati
(1) H 70=!

% # ! " ?
# = 0 !

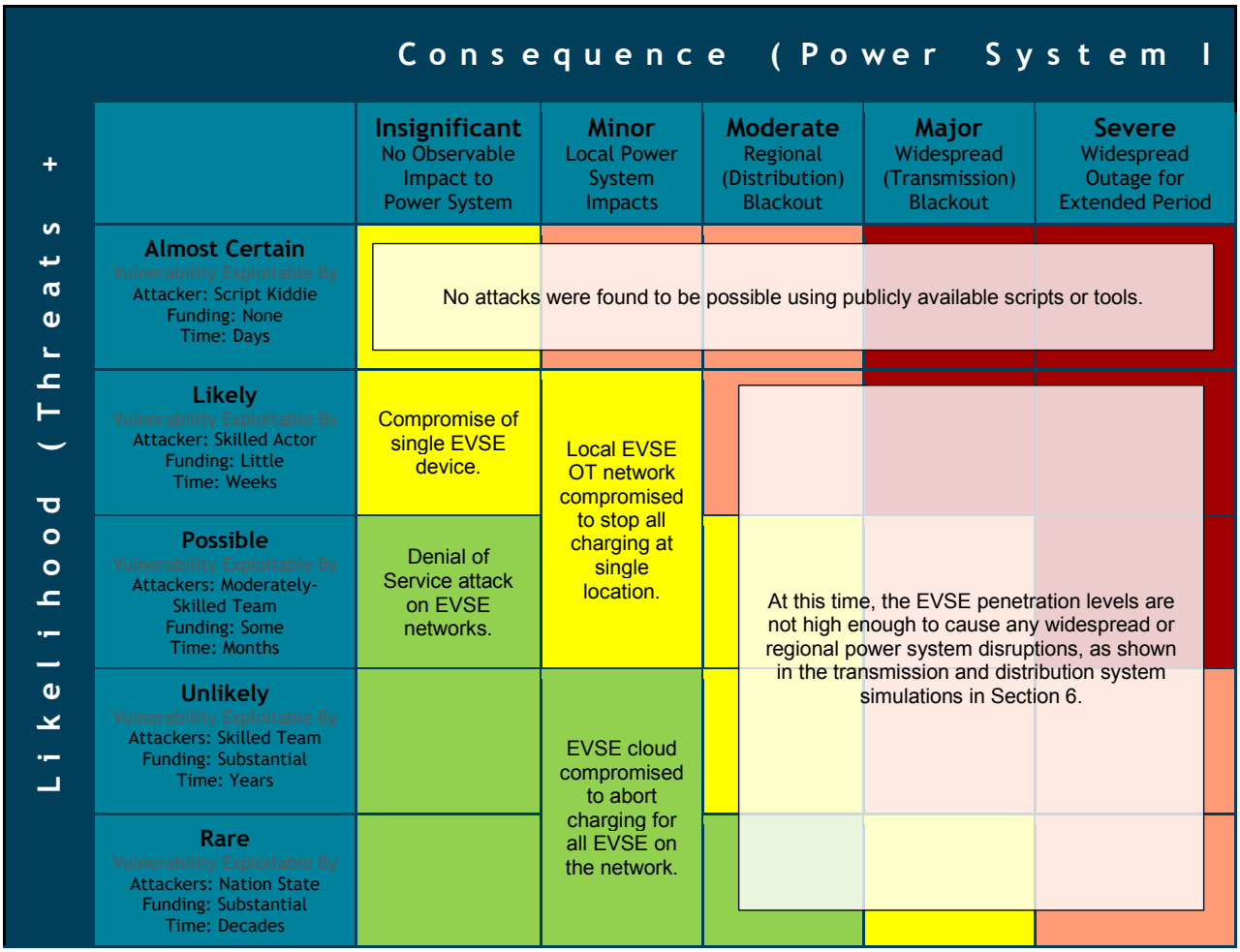


Figure 7-2. EVSE Cybersecurity Attacks Mapped onto the Risk Matrix

" @ "
& "8 .5! " #
# # A &) # "
" # % " <
< % " # 5
% ? % ! "
# " < % " " 9
# % ? !
< " # " %
" % " !

=0A! ' +!l s o n , " 5 o r n i s v e e q n u e C n y c b e e r s e c u r i t y f o r H i g h P o w e r E V
0 5 3 3 3 6 7 ' / = 6 8 8 ' ,
? 2 < 4 ! 0 7 0 = !

8. MITIGATIONS AND RECOMMENDATIONS

> 3 ! 0 "
" % % ! < ; <

8.1. Mitigations

% 3 !!0)
" &
) &) 3 /!

8.1.1. Business Network & Operations

- ' % " " %
! L) 1) ! 0 M
- # %
L) ! 1) ! M
- <
% # " % ! L) 1) ! M
- % ?
" " L) % 1
) ! - M

8.1.2. EVSE Security

- % <
5 % %
L !) 1 + ! 0 M
- " %
< L !) 1 + ! M
- % %
L) 1 + ! - M
- " + *
% ! L) 1 + ! - M
- > %
L) ! 1 + ! 6 M
- % %
? L) ! 3 1 M + !
- % < L) ! 3 1 M + !

8.1.3. EVSE Network & Operations

- ' ? " " " ! L) !0 1 M

-) " # < " # " #
  " !
  " # L) ! 1M !
- " < ! L) M1 !
- & " 2 &! !4L) 1M !
- " 5 %
  < " " !L) < -1M ! " #
- * * 4" 2
  & !
  L) -1M !
- " "
  5 " !L) 61M !
- (
  % " L) ! 61M !
- > " ?" 5
  " #
  L!) 31M !
- ? < ?
  % L) # ! ,1M !
- “Door” Open arms, system login noti
  % > L) <1M ! !
- "
  % L) 1
  !/M
- < ?
  L) /1M !
- <
  % =M
- < "
  L) ! 017M !

8.1.4. Electric Vehicle Operations

% !

8.2. Best Practices

8 " "
% < %
!

"

9 2 95 9 4 %

E ! 8 /50 8 /5!

Figure 8-1. EVSE Best Practices.

Figure 8-2. EVSE vendor recommendations based on penetration tests of EVSE equipment and networks.

9. CONCLUSIONS

@ < % " %?
# !
% % "
" # !) " # 1

- % > <
  !
- % <
  5 5 ? 2 4 !
- " ; %
  !
- ' % %
  !
- 5 "5 # !
  5 %
  "
  !

APPENDIX A. DETAILED ASSESSMENT RESULTS

A.1. Business Network and Operations

L) ! 0 2M E 4 " % >

H 1) > " – %
" – % %
% !
# # – * * (
! "
" "
4 !

9 1' % " " % !
" 1

- E %
- %
- 5
- ' ? % ?
? "
- Ensure critical credentials, keys, or c
5
- %

L) ! 2M 9 4 (" >
!

H 1) " % "
% " ! 5
" %
! 8 % #
"
" % !

9 1
!
!
challenge anyone they don't recognize at t
!

< &
> % !

%

% !

L) ! -2M" 4 < > "

H 1 9 < >
% ! 8 ? "
# > < " !
% "
< " % "
" " ! " % ! !
%
% !

9 1 <
> " # & <
! ?

! "
< % ! !

A.2. EVSE Security

L + ! Ø M 4 < % ?
!

H 1 9 < & %
% !
5 " %
" " # < !

< #
& % %
"
% # ! ! ! (!

9 1 % # %
? !
F
!

5 %
% " > !
"
" 2 # 4
< !

L + ! 2 M 4 % < !

H 1 % < &
" % <
%
< ! < %
< " < %

9 1 B ?
!
> !

L + ! 2 M 4 %

H 1 " % % <
% !
% % % <
& (
!

9 1
!
"
& !

L + ! 6 M 2 E 4 < " " < !

H 1
" ?
% < " #
!

9 1 > %
!

L + 3 M 2 " 4 % !

H 1 " %
" # < " % "
i s r a t e d " L o w " s i n c e t h e a s s e s s m e n t t e a m
% % " 5 " !

9 1 %
% % !
?
" !
% !

A.3. EVSE Network and Operations

L ! 0 M 2 E 4 < " "
!

H 19 < ? ! B %
< " #
!

9 1 > !

L !M2 E 4 < " # 2 & 4 " " #

H 1 " # "
< "
;
! < " # &
< (% " ! "
" < % < " # "
d e t e c t e d . E v e n w i t h t h e p r o p o s e d u s e o f a
" # %
< " #!

9 1) < " &
! & " # " #
" #
" ! <
% " " # "
!

L ! -2M E 4 < % > " #!

H 1
< " #!
" # < " #!

% ! B
% !

9 1 " 5 %
% # !

!
" #
> % ? ! " #

L ! 62M 4

H 1 " % %
; " !
%
" &
% % !

9 1 " "
" 5 " ! <

H 1 * < " +
? ! % " >
+ # !
9 1 < % "
% !

? <
!

L ! 2 M 4 < " "

H 1 < %
< ! %
" " < ! B
"
% !

9 1 " % <
5 % !

L ! 0 2 7 M 4 < % !

H 1* , *9 K(0 ! "
< ! " " #
< > !

9 1 < "
!) " # "
" !

A.4. Electric Vehicle Operations

% !

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Jay Johnson	08812	jjohns2@sandia.gov
Summer Ferreira	08812	srferre@sandia.gov
Technical Library	01977	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name
Lee Slezak	lee.slezak@ee.doe.gov	Department of Energy Vehicle Technologies Office

#

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of E National Nuclear Security Administration under contract DE-NA0003525.