

NOTICE:

! " # \$ % & ' () * + , - . / : ;

!!
 (*! + & ,
 * # ' - ./ - 0
 1 2 / , 3 4 5 6 . 7 0
 8 1 2 / , 3 4 5 6 . , /
 59 1 : ; ! %
 * 1 1 : ; " " ! ! % ;

)%
 !!
 3 - 7 0 " ' %
) & <) - 0
 1 2 / 7 7 4 5 3 6 . -
 8 1 2 . 7 - 4 5 , = 7 8 7
 59 1 : ; ! %
 * 1 1 : ; ! ! ! % ; ; ;



NNSA
 National Nuclear Security Administration

ABSTRACT

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

ACKNOWLEDGEMENTS

" # "
5 776/Q=

!!

<

*

\$

CONTENTS

0!+ #	!!!!!!!	4
! (@	!!!!!!!	10
-! 9	!!!!!!!	10
-!0! * 0350(A	!!!!!!!	10
6!) # \$!!!!!!!	10
3! <)	!!!!!!!	7
3!0) >)	'!!!!!!!	7
3!0!@!	" # *	10
3!0! <	!!!!!!!	10
3!0!-<	" # *	10
3!0!6!	< *	10
,! ("	? !!!!!!!!	4
,!0!	!!!!!!!	4
,!0!0!	!!!!!!!	13
,!0! !	9 %	17
,! !	!!!!!!!	6
,! !0<	5 \$ <	18
,! ! !*	!!!!!!!	18
.! ("	! ! # !!!!!!!!	14
/! 9	'	3
/!0!9	!!!!!!!	3
/!0!0!	" # *	3
/!0! !<	!!!!!!!	3
/!0!-<	" # *	3
/!0!6!	< *	3
/! !+ (!!!!!!!	3
=!	!!!!!!!	3
) &)!)	3
)!0!+	" # *	3
)! ! <	!!!!!!!	3
)!-<	" # *	7
)!6!	< *	7

LIST OF FIGURES

8	50! (@	! ! # !!!!!!!!	10
8	5!	%	10
8	5! <	"	13
8	5! <	"	10
8	5!	'	14
8	56 <) # \$!!!!!!!!	17
8	56	9 8	17
8	56) # \$!!!!!!!!	17
8	50! (<	7

```

8    5!  8  ?    % !    +    !!!!!!!!!C! 7! 9 <
8    5!  <    % !    +    !!!!!!!! 0! 7! 9 <!)!!!!!!
8    5!  <    %    % !    +    !!!!!!!! C
8    5!
8    5!
8    5!          %           ;
8    5!          ! 3! 9! B!!!!!!!
8    5!          2 B < D' 4    "    2' 9 D' 4    %
8    5!  E    "    %           )
8    5!  <    %           !!!!!!!!
8    5!  <    ' ! #! 9! ! &! !!!!!!!!
8    5!  <           ) # 9    !!!!!!! #! 9! ! & !! 3! 7!
8    5!  < + ( !!!!!!!!
8    5!  < %           < ?
      "#! !!!!!!!!

```

LIST OF TABLES

```

59!  '          !!!!!!!!
1          !!!!!!! 6 7! !!!!!!!
-! 9 &          %           !!!!!!! 6! !!!!!!!!
6 1 9          ?          ' ?           !!!!!!! %! 6! !!!!!!!!

```

#

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 < 4 " & " "

! " "

> % # "

% !) " % # %

" % # %

" " % " ! E " % # %

@ % ? 8 2 < 4 !

% ! 8 < 5 5 %

5 % F " # "

> %

!

(" " " %

" " — ! ! 2 & 8 4

2 G 8 4 9 " 2 9 ! 4 #

% % " #

% % " "

% - 6 ! 9 " "

% 3 . . / ! "

' ? > < * < " * % 2 < * 4

? % @ ! = ! %

@ " # & # 5 " < "

? # " % "

0 A! A " & ! , "

(% 7 0 7 !

A! A H! ! A 5 ! H # E H ! A " Cybersecurity for autonomous v

defense, " Computers & Security, 07! 070, u @ ! 1 0 3, 7! 07 0 37

- * ; E ; * < 9 < * 5 ' !

< 5 * 5 5 0 9 7 0 /

6 9 8) \$ ' 9 9 * ; < ! 9 E % <

< 0 ! ! 0 9 ! - 7 7 0 /

3 H! H on, T. Berg, B. Anderson, and B. Wright, "Review of

Potential Impacts, and Defenses," Energies, 1 vol. 15, n

1 ; & ! ! ; 0 7 ! - - = 7 ; 0 3 0 0 - - = 0

' < ' ? ' ! " # !

! < 0 ! 7 0 !) ' 1 7 0 ! . ! ; ! 5 ; " ; 7 0 . ; 5 7 ; < 5 5

5 ? < !

' <) ! " 8 # <)

7 0 , !

/ < " # 8 <) 7 0 , !

= ' / = 6 8 8 ' <

2 < 4) 7 7 !

2. PROJECT STRUCTURE

- chargers. To improve the vehicle industry
- 5 ?
- <
- > " # !
-) @ 1 < 2 - %
- ' 9 4
- 3 < / 9 % ' 4 <
- (" # ? . (" ' 4 # 2 ,
- " # 2 / 9 ' < 4 " "

Vulnerability assessment and threat model development

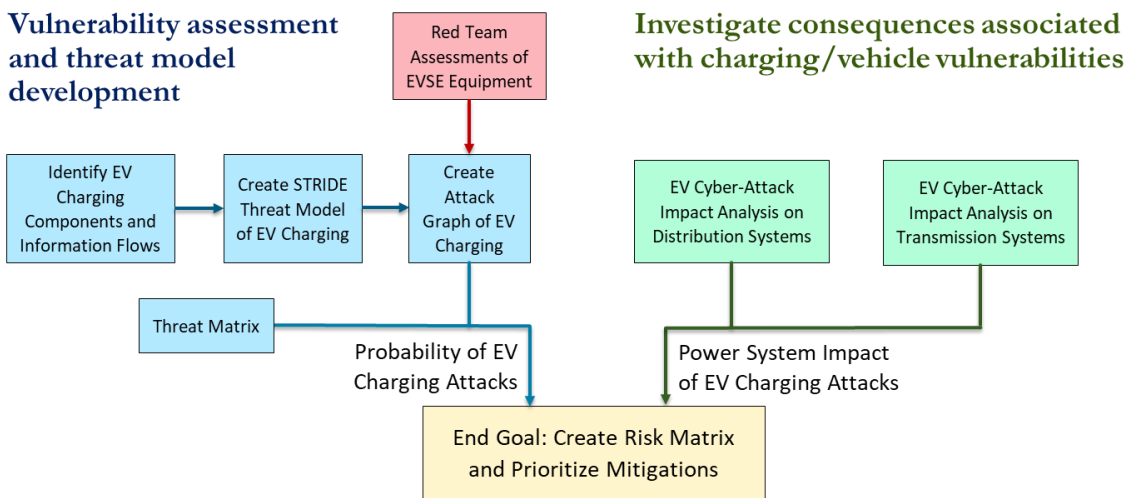


Figure 2-1. Project tasking.

B # 8 50 " % " @ 1

- Identify EV Charging Components and Information Flows ! B

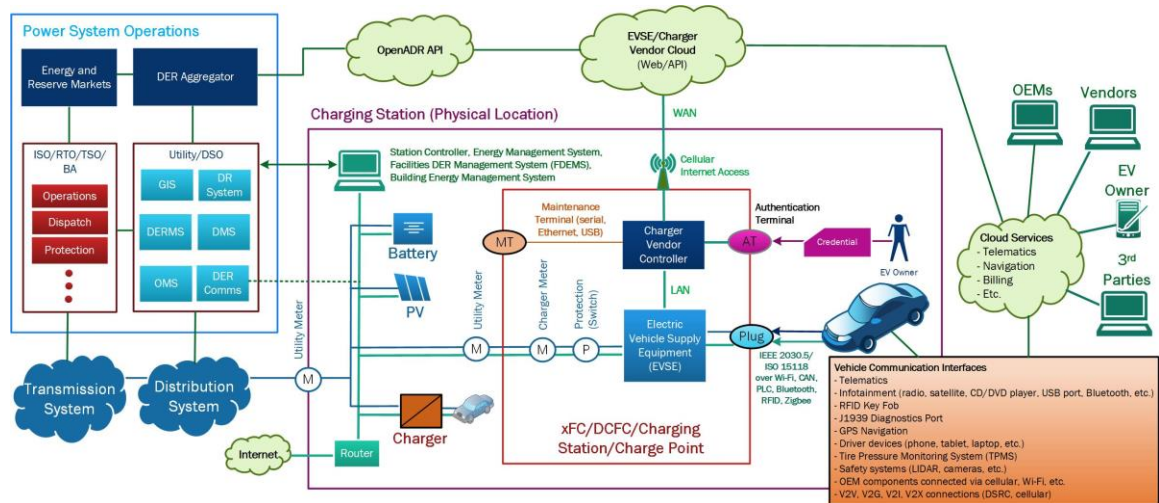


Figure 2-2. Electric vehicle communication systems to different components and entities.

- Create STRIDE Threat Model of EV Charging !

- Create Attack Graph of EV Charging !

- EV Cyber-Attack Impact Analysis on Transmission Systems !

- EV Cyber-Attack Impact Analysis on Distribution Systems !
 " 5 5 2% \$ 4 > "
- Penetration Testing of EVSE Equipment !
 5 5 5 < ? " % >5 % " # ?
 " # % & # ! " #
- Risk Analysis !
 ? " # < # " # " >
 # % # & 5 5 0 ?
 # % < " # ! #
 " # ! #
 00 !
- Prioritize Mitigations ! +
 > " 5 ? # ; 5 " %
 # ! " #
 # % !

07 , 665, "Security for industrial automation and control design," 2020.
 00 !(! ! ! ! A! A! < !B , "Categorizing Threat: Build Threat Matrix = 0 ! 77!
 0 !(! ! ! H9 , # ") 8 , " # A N 5 2=0 0 7 ! 77.!

3. THREAT MODEL

(" (4 2 # % 5 "

% " 5 ? ? ! (% %

% ? ? 5 % % ' 12 4 %

? ? ? % F 2 4 %

? ? 5 > ? !

% ! ? % >

% ! ? % !

" & % > *et al.* ! +

% 5 " # % " % 0q

@ 5 % A \$ " ! ' 9

0q * % % 5

0.0.1 ' 5 ! > " "

" 9 ! > " "

" -501

! Spoofing: masquerading as a legitimate user

! Tampering: modification/editing of legitimate

! Information disclosure: data breach or unauthorized

! Denial of Service: disruption of service

! % % 1 % % "

!

) % ! @ " ?

2 & < % ! " # 4 !

? ? ? !

0-+ A < % E B , 9 H, ' A # threat 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

! ! ' ! % ! % 0 ! 7 0 ! ! ! -

0q Lee, S, Park, Y, Lim, H, & Shon, T, 'Study on analysis of electric vehicle charging technology', Proc. of the 2016 IEEE SmartWorld, 2016, pp. 7046-7051.

03 Kohnfelder, L & Garg, P, 'The threats to our products', A 9 A % er, S, 5 > STRIDE physical systems', (% % \$ 2 \$ 4 70.!

0Shevchenko, N, "Threat modeling: 12 available methods" [1; ; ! ! ! ; D 5 7 0 ; 5 % 5 ! 7 0 !](#)

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/Mi l l e r , M , ' M o d e l i n g t h e t j r e u s t s ' h o u p r d a c G i B o s f # c t r h e a t 2 e d b y s * % 2 B 7 4

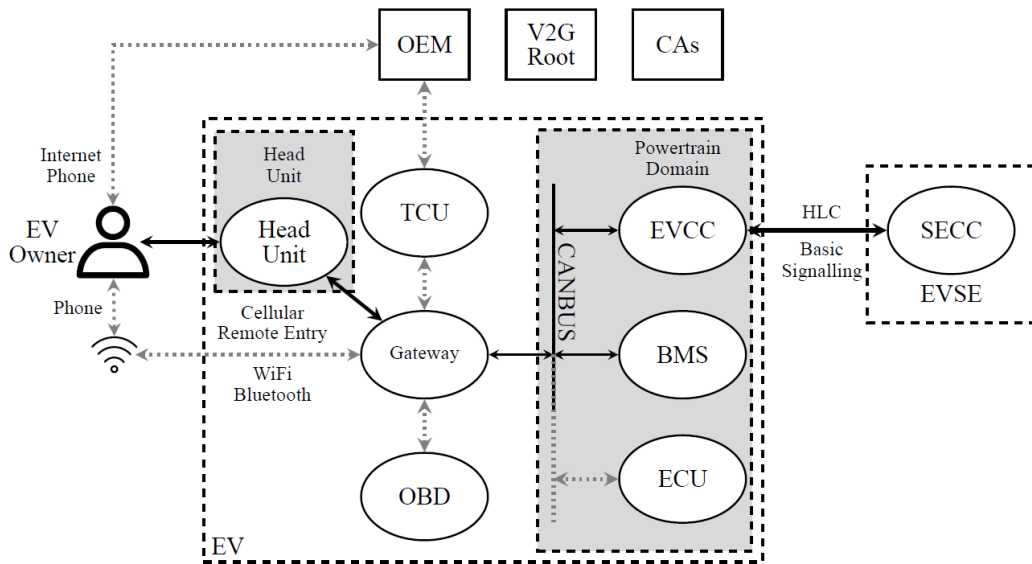


Figure 3-1. The EV data flow diagram.

|| " " % " % " !
 < < " <
 ? + ! 9 + 9 4 2
 #
 " ! + 9 #
 " " 7!
 F
 + 9 !
 9 5 % 5 5 5 % " # " ! # 2)) 4
 5 5 5 % " # " 5
 !)
 0! " E " %
 ! % % 5 & ! !)
 2 * + 4 % % % " % & ! !)
 ? ? 2 4
 ? " B 8 + 2 * 9 4 !) - 50 " %
 ! ! & 6 \$; 3 \$ " # ")
 ! " 2 " ")
 " # 4 ! \$ " 2 " %)
 % " %
 - ! >
 < \$ ' 2) 4 &
 !)
 < \$ ') 5 %) F ! < \$ ')
)) !) !) % #)
) < \$ ') !) ! % #)
 !)
 % !)

⁰Brandl, M., Gall, H., Wenger, M., Lorentz, V., et al., 'Ba
 (!) & 2) 4 - . ! 7 0 0 !
 Ulrich, L., 'Exclusive: GM - e a a m d n r a e n n a o g t e e l a y n ' , E V I ' E S E H b a S t p t e e c r t i r e u s
 7 7 !

⁰E >) " # ' %
1 ; ; % ! " ! ; : 6 . . . = . / 7 ; 0 . !
 Sommer, F., Dürrewang, J., & Kriesten, R., 'Survey and cla
 07 ! 6 7 0 = !
 -) *) ' 7 0 / (% 6 ! 6 ! 7) *

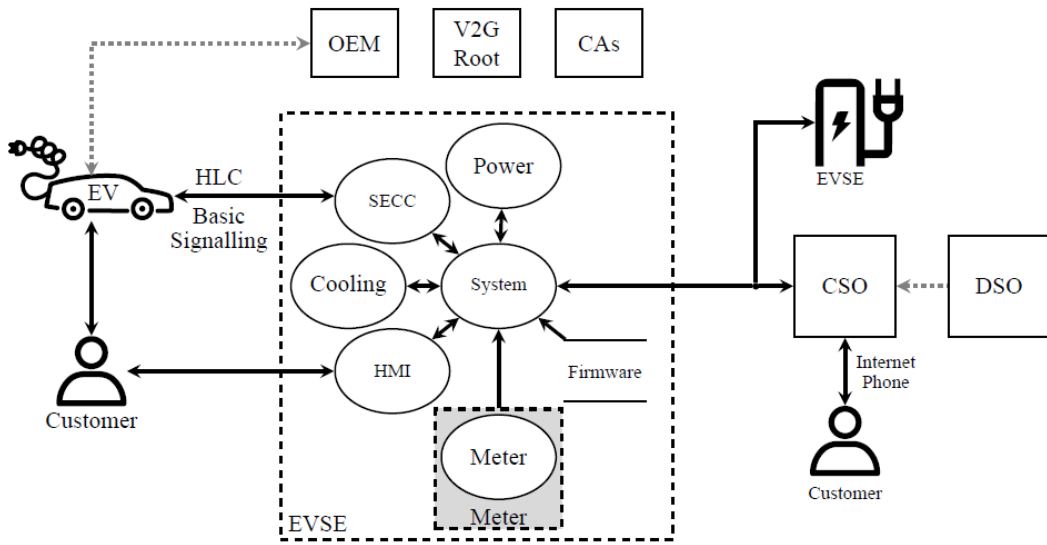


Figure 3-2. The EVSE data flow diagram.

! % 8 -5! %
 ! % & "
 % # !
 5)5 % % " ? ! (
 % 24 " * 0300/ < ? !
 ! E " " < 5 ! "
 (6774 # ?!) 5 # 2E9 4 # > %
 B ! 4 2 2 * " @ 4 " " #
 % 4 2 * " @ 4 " " #
 !

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

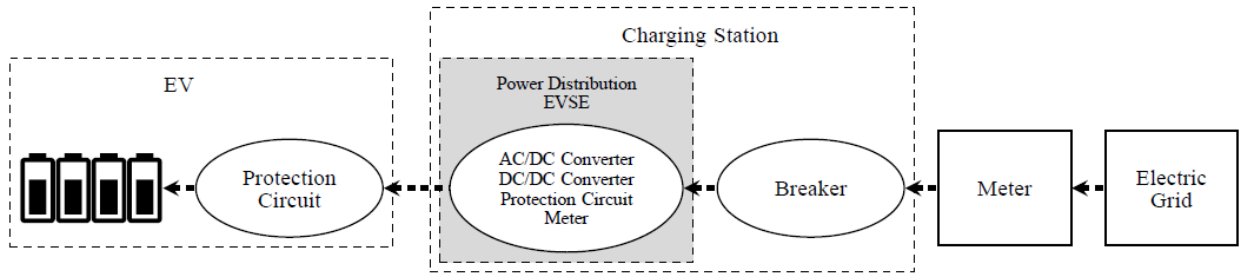


Figure 3-3. Charging infrastructure electric power flow diagram.

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

Consequence #1:

Attacker Payoff: (" ; !

Threat:) > 1

- "5 5 < " 1 &
 - (Local)
 - (Local)
 - (Local) applicable *t 0.300 / remote" 4 @
 - (Remote) ; # !
 - (Local) < & < " #
- Threat:**) " 1
- (Remote) " 5 5 < " 2 < ! 5-7.\$, 003 * 03 50/

³Bohn, T, "Multiport, 1+5MW charging system for m horizon?", 2020.
 ·Falk, R & Fries, S, 'Electric vehicle charging infrastructure ! ! % % 2 ' 4)') 70 !
 ·Baker, R & Martinovic, I, 'Losing the car keys: Wireless US ENIX Security Symposium 70= ! SEC ' 19, pp. 407

- (Remote) " 5 5 < " *
 - (Local) " " " 4
- Threat:) " 1
- (Remote) Tamper with logs in the charger's memo
 - (Remote) " 5 " "
 - (Local) " 5 5 * " " 2 #
 - (Local) " # ? 4 " "
 - (Local) " <5 5 " "
 - (Remote) " < " "
 - (Local) " E 9 %

Consequence #2:

- Attacker Payoff: < " ! !
- % " !
- Threat:) " 1
- (Local) " + 9 " "
 - (Local) < 5 5 " 1
 - (Local) - (Local) " "
 - (Remote) - (Remote) " "
 - (Local) (" " " "
- Threat:) % # 1 % %
- (Remote) % * % %
 - (Remote) " E 9 " "
 - (Remote) * " 5 5 * " "

Consequence #3:

- , ! 0 4 V % / " " = % V ? ? V ?
- % - 0!
- Attacker Payoff: !
- Threat:) 1
- (Remote) V %
 - (Remote) " % %
 - (Remote) " * ? % # %
- ? & " 8 % # %

1 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 n o p w a e c r t G o

7 0 = (" - 3 2 7 0 = ! ! 0 5

= ' A B 8 1 (

0 / 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 / !

Threat:)
 • (Remote)
 • (Remote)
 • (Remote)

Threat:)
 • (Remote)
 • (Remote)

Threat:)
 • (Remote)
 • (Remote)

Consequence #4:

Attacker Payoff: <
 Threat:)
 • (Remote)
 • (Remote)
 • (Local)
 • (Local)

Threat:)
 • (Local)
 • (Remote)
 • (Remote)

Attacker Payoff: (
 Threat:)
 • (Local)
 • (Local)

Consequence #5:

Attacker Payoff: \$
 Threat:)

- Fairley, P, "800,000 micro-crimes a day, reveals trend of Aug 1: 5! 5: 577757 % 5 5 5 5 703!"
 -- + A 5 ?% " < %
 70 77! ' 1
 1:""! ! %: ; ; ; 7 7;7.;.3: 0==D D 7!7D D3!0! 7D0!0
 -6 (" 1 \$5% % % <
 00) 70 70=!1:; "!" ! :5% 5 5 #5 5 5 ;
 -3Oyler, A & Saiedian, H, "Security in automotive telematics the existing and emerging attacks 6-6-77 70, Security Cor

- (Remote)
- (Remote)

Consequence #6:

Attacker Payoff:

Threat:)

- (Local)

- (Remote)

3.1. ISO 15118-2 PKI

) * 0300/ # # # 2(A 4
 5 5 < < and 5 p 5 m a r k 4' "(
 % ! < 5 5 ! * 0300/ @
 % " # * 0300/ !
 & % " ? " <
 ? " 5 5 % & -3 % ! " <
 ! " % < & % (?
 * 0300/ ! 9 " % " > " !
 (" '8 ! 8
 % % % % 2 5
 % 5 % % % !
 % 5 % % % (5/3, !
 ! 5 * 0300/ & % 5 2"
 4 " ! < \$?
 5 3(5" ? ! ? ?
 -7 - 2 5 4 ? ! /!73&07

07!3 -...! K
& -/! * 03 507/ % (5 0 0305/ -66/ *

" # " 5* 0300/ # !

% " 6.0= ? 0!0-&07. % 5 0# (33

5 F ? !) * 0300/ & #

" " ! " " % 5 7 " ? % * 03

0305/ > " # " * 03 50/ " "

1 " % % 5 7 0 3 9 0 / % " F

" " % > % ! 9 0!-? 2

4 " % % ! <

* 03 507/ & 7 ! " % 5 1 7 0 6 ! " ? * 0300/

? % ! 5) 5 % — 8 9 5 — E * 0300 / % 5 1 7 0 6 3 0 0 /

" (A ! * 03 507/ " " % 5 & "

! % <

— * 0 3 5 0 0 / B 0 3 * 0 5 7 # " * 0 3 5 0 0 /

7 o r b o t h d o n ' t s u p p o r t I S O 1 5 1 1 8 % / 5 * 0 3 0 0 /

? % ! " # % > #

% > @ % % % ! B #

% !) % %

"

? % < % ! % % " %

#

%

?

" #

% " ! 88

<

! % *safety instrumented system* " #

+et al. #

67 " "

7-7

6q<

Following a whitepaper titled " (" ?

>6 " # *10\$00/ (A ?

% ' " (2 %4 " !) " #

" & " !) " #

address the governance concerns raised in the

L M < (463! A

" % " # %

5' * 0300/ < !) " *

>

" # " " # # * 0300/

? (A \$ < !! # #

67. Metere, R, Neaimeh, M, Morisset, C, Maple, C, et al. 2015. 'Infrastructure', CORR: & %! abs:/0273075=73905,

68. A. Fuchs, D. Kern, C. Krauß, M. Zhanogaa, "Proceedings 03)% ' -, 77! ! 0

69. van den Broek, E. Poll, B. Vieira, "Securing the Ir 1.60 703!

70. Lee, Y. Park, H. Lim, T. Shon, "Study on analysis of 15118 based electric vehicle charging technology", Proc 2 4 706!

71. (" 9 06 !70=

72. Sidles, "I SeO, 15EIP1R8I PIIWIG & Mcheatrigng, White Plains, NY,

73. Berman, "The I S O h i s t o r i c a l b a c k g r o u n d o f f o r e d e x t r a s e c u r i t y c o n c e r n s 1.60 703!

74. " SAE kicks off project to 5757e7" o p U R d y: b e r 1.60 703!

75.) " SAE International 5757e7" o p U R d y: b e r 1.60 703!

76.) " SAE International 5757e7" o p U R d y: b e r 1.60 703!

77.) " SAE International 5757e7" o p U R d y: b e r 1.60 703!

78.) " SAE International 5757e7" o p U R d y: b e r 1.60 703!

(# # 2 4 \$# < 5'5 /750750 E @
 ? ! E @ @ \$ % % %
 < # " 2 !!) 4!B " " +B
 < \$ (A 1

0!Certificate Policy.)

) ! * 0300/
 %
 # 8 2 84 !
 !) ; + " 37 8 %
 % " 5 (A
 !) ; + "
 ? & & #
 # 3!
 * 0300/ < \$ " 5)
 ' 3) 2 0 ! %4 5
 " ! % " (A%
 ! (% ? % @ ! ; %
 * 035070/ " & !
 % % (A !

2. Algorithms and Protocols. (A ;

! — & % % ! — !

6. < 5'5 /750750 E %
 " # " , * 01300/ 20191.1.1.1 URL: ! ! ; :05'5, -0;<
 N 7 / 70750
 6/Subject EGn@ H, (" for (the Subject ISO 15118 V2 G P
 70=!)
 6= & (A * 0300/ <)
 % 70/!
 37) ; + " 8 ' 1 1.1.1.1 ! ; = ; 0 ; 0!
 30) ; + " 8 , " # ? " 8 \$ < 0! 1
 1.1.1.1 ! 5 ; " ; :) + 85 " 5 50!! 505070 =!
 3) ; + " 8 " + ' ? 9 5 ("
 < 0! , ! , ' 1 1.1.1.1 ! 5 ; " ; 5+) " 5 5+ 50! , ! , ! 505070 =!
 3- ! + # 5 (7/7 Part 1 Rev. 5, " Recommenda-tion 9, 7.7 r Key Mana

public key cryptography and transport charge" use case.

36' 8 /6.6, "
 0 3 5 7 0 !=

33B !) 7 < (A ' < \$!

3. PKI Hierarchy.

36' 8 /6.6, "
 0 3 5 7 0 !=

33B !) 7 < (A ' < \$!

6 !Key Management.

" " < % 5 % 2 % !4 " < % 5 % ! % % % " % < ! E " % " " % " % " !

5. Certificate Revocation Policy.

* 0300/ % G! 37= (2 * % 4 " * ! (% 5 5 5 % !

, ! Identity and Access Management.

? # % % * 0300/! < " % % ! ' ? % % ! % " %

7. Business Continuity.

* 0300/ " ! E ! " %) " ! %

8. Audit Policy. 8

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

> !

4. ATTACK GRAPHS

) # " # # ; '% #
 ? @ % ! # @ % " #
 # # % @ % ?
 8 650
 < " #! # % %
 compromise of an EVSE provider's business network
 > # % % %
 " # (? - < %
 ! % # " # !
 " # "" @? 1 # !
 • Can the attacker "pivot" between the components P

• # > # # P
 8 " # < % 3, could ! #

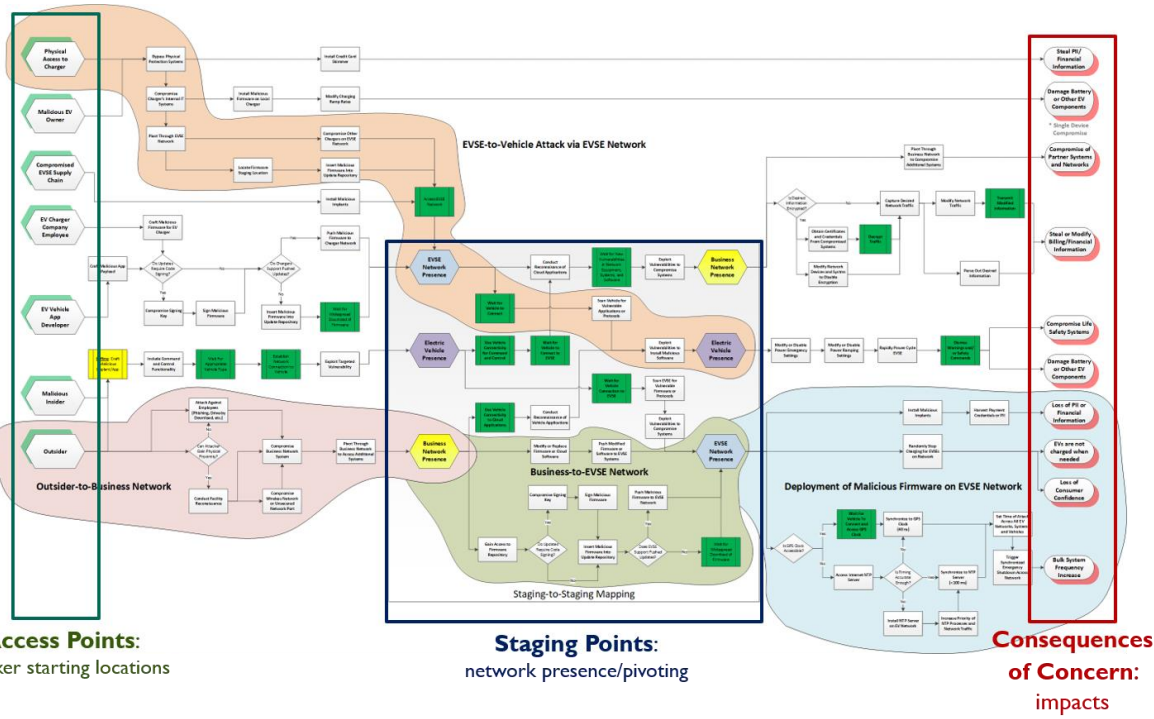


Figure 4-1. EVSE Ecosystem Attack Graph.

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

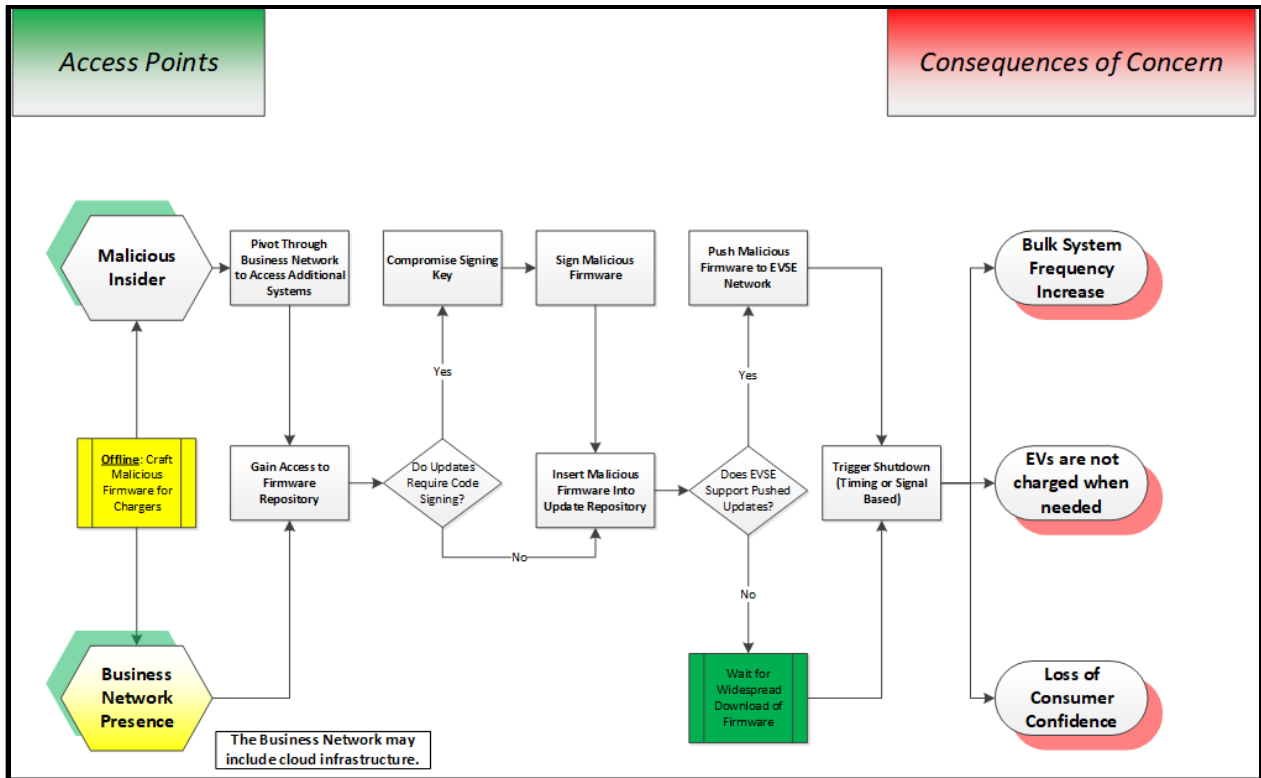


Figure 4-2. Deployment of Malicious Firmware

the attacker needs to be

attacker can choose that route to immediately

mechanism that will achieve the attacker's

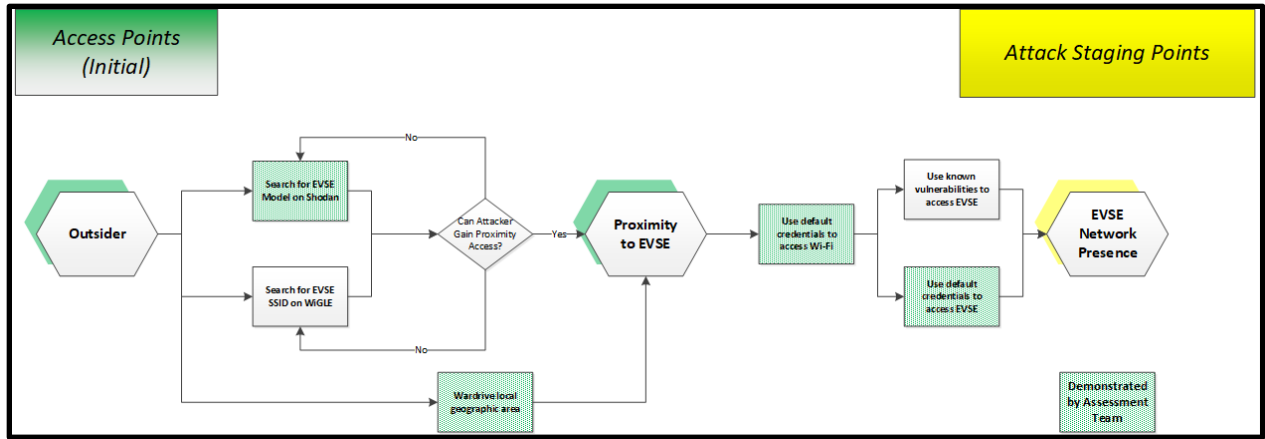


Figure 4-3. Assessment Attack Graph

³B. Roy, Z. Ivanic, P. Windover, C. Hargraves, et al. "DoS and DDoS: A Survey of Attacks, Mitigation, and Defense." *Journal of Network Security*, vol. 2017, no. 1, pp. 1-10, 2017.

5. EVSE ASSESSMENTS

@ % # "
% < " ! < " % %
% " % \$ % !
(8 650! # % "
" % % < " " # " "
< % " # ! % @
" % % " !# "
% # " " # % !
% % < " "
) " 8 /50! @ " % >
8 /5! " ! ' %

5.1. Anonymized Assessment Results

% > # " # < ! E " %
" " # # <
! " # % " # %
% % % # % # %
> % # % ! # %
% " # E 9 n t t h e " t e a m ' s %
% % ') ! " ') % ?
• - B % & # P
• ' - B # % ? # P
• & - B # % ? # P
•) - E " " 2 ;# P
• % - B % # " ? "

E " % ? %
 % # % F %
 & % ! % & ? %
 ! @ % & ? %
 " # % % " # * % <
 < " # * 1 + ! " # * % <
 " # * < " ! " # &)
 @) # &)
 (3!

5.1.1. Business Network & Operations

L)! 2 4 " % >
 L)! 2 4 (" > <
 !
 L)! 2M " 4 < > "
 !

5.1.2. EVSE Security

L+! 2 4 < % ?
 !
 L+! 2 4 % ! <
 L+! 2 4 ! %
 L+! 2 M" 4 % !

5.1.3. EVSE Network & Operations

L ! 2 4 < " " "
 !
 L !M E 4 < " # 2 & 4 " ! " #
 L -!M E 4 < % >
 L 6M E 4
 L 3M E 4 < !
 L ,!M E 4 < % !
 L .!M 9 4
 L /!M 9 4 < ? " + #!
 L #M 9 4 < " "

L 0 129 4 < % !

5.1.4. *Electric Vehicle Operations*

% !

6. POWER SYSTEM CONSEQUENCES

B @ < ^{3/} %
" ! & 5 # < 5 " %)
? " % !5 " # " 5 " ?
" %
" # " %
!

6.1. Transmission Impacts

& 5 "" " 2 B 4
" B 1 5' < B &
? % <%
5 r e a o s c i l l a t i o n s a l o n g t h e C a l i f o r n i a O r e g
% " #
! % " #
! 8 %
!
) 5 # " 4 ? 2
! B) %
+ # ^{only} 3=2+ 4 04
& 77 % 4 5 % # < 077 % !
8 9 < β 9 <) 7 ! 8
+ % (' 57 6! 7 % ' ?
% 5 ! E " 5% " "
must) ! % % %
% B ! * + ?
% " # !
5' %
2 " ! ! 4 ? !
& 5 5 " ! &
" >

^{3/}Edison Electric Institute, "Electric Vehicle Sales For 70/!"

³⁼ ' O+ # % O 706!
,7 ' O 57 6— \$ 8 ? < % ' O)%
1 ; ; " " ! ! ; ; ; ' N 757 6! ! ; (') M! 70=

composite load model's internal protection and

!)

? 5 5!

% # "8 "

impact factor

$$I F = \frac{\text{peak-to-peak load (MW)}}{\text{control load (MW)}}$$

% " " * % "

! 5 # " & % "

% " % 07 " * " 5

" 8 ! & 07 B * % 7 397B

")

! % ") " ! B

) % 5 Q ! 3 Q 0 ! 3

% 8 ") 5 %

Q 0 ! 6 Q 0 ! 0 3 * !

B " %

Q ! 3 * 5 5 %

" 5' ! % >

" % " #

% " < &

" !

0) ' O' \$ 8 * 9

1 ; ; " " ! ! ; ; (D' D \$ = 70 ! L * M !) % 1

7 5 0 8) ! ! L) 07 7 7 M ! D D \$ 5 8 D D * 5 7 6 D

! ! A) ! ! B ! B !) ! 9 O 9 <) 07 0

* O (" % = 5 . 0 6 0 = ± = !

- H ! ! B 9 !) ! > H ! E ' ! E 0 = ± = ! ' ! 8 E ! A # ! ! 9 %

B 5+ O % 5 B 9 5 * (" O

70 !

6.1.1. Load Drop Scenario

The Power World's simulation used WECC's production cost model simulation of 22 load areas used by this work's transient simulation of 10.8 million electric vehicles nationwide. The simulation used WECC's production cost model simulation of 22 load areas used by this work's transient simulation of 10.8 million electric vehicles nationwide. The simulation used WECC's production cost model simulation of 22 load areas used by this work's transient simulation of 10.8 million electric vehicles nationwide.

1. A. E. ...
 2. ...
 3. ...

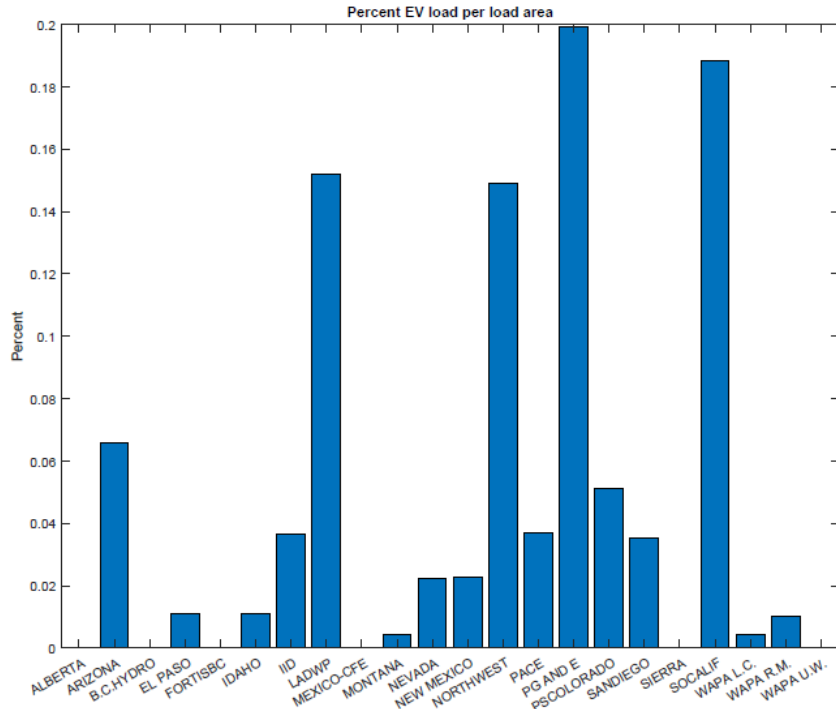


Figure 6-1. Percent EV load distributed to each load area in 2028 WECC planning model.

8 & / , 77 9 B < " "

% ! " % "

% " ! 8 ? % "

% " + 2 C 7 9 <) % 4 "

% 8 , 5 8 , 5 8 , 56 !) / , 77 9 B

% 2 Q - 7 9 B Q 6 , , 9 B 4 !

% Q 0 , = \$ B % Q 0 , - \$ B

WECC's % ! 7 ! - N

B + !) , % 8, 9 B 5

8 , 5 , ? % ! %

+ (' 5 6 + ' s " % 5 ? ? , 7 ! , E > 5

0 / 7 ! A % 50 ! 0 7 ! = " !

" % 7 ! = % 7 ! = ! \$ % % # 8 , 5 % !

% @ , 5 8 , 56 % > % 7 ! = ! \$ % % % % %

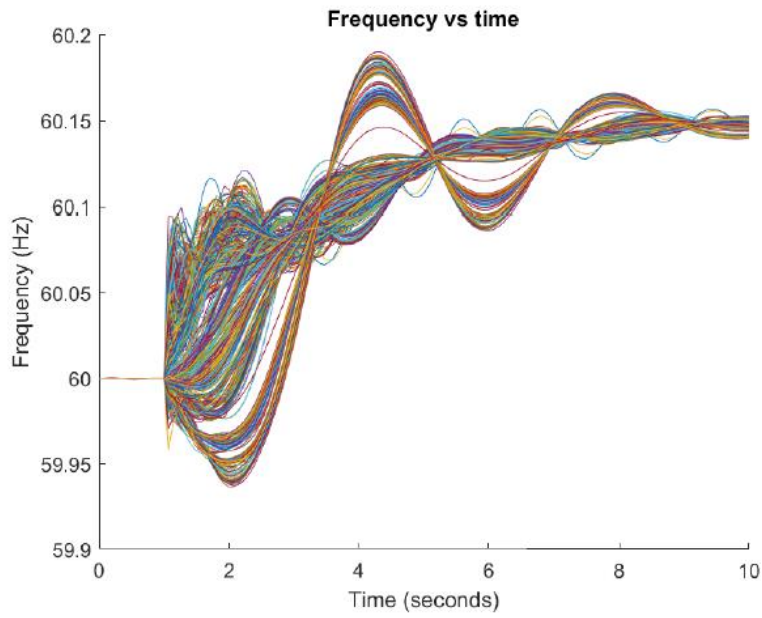


Figure 6-2. Frequency vs. time for operational BES generator buses with >20 MVA base.

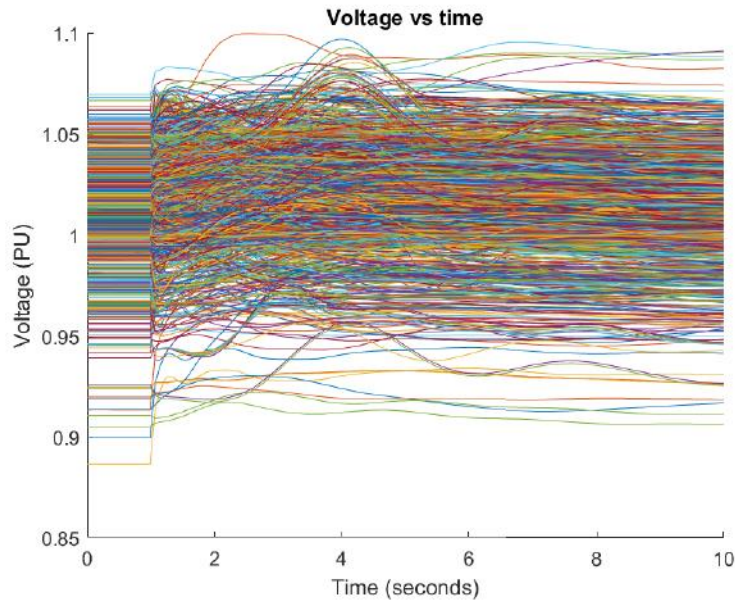


Figure 6-3. Voltage vs. time for operating BES generator buses and >20 MVA base.

? % 5 B ! 8
 /6 " # % 7 / < / /-! " # 7
 70/ < % " # " (" 4
 PSS makes the generator "resist" changes in t
 B + % (% ?
 " 5 ! ! & ! /3 #
 " ! & !
 > # " " 1
 0! & % ! 8 77# 9B0 # "
 % !
 ! System modes are determined using Power Wor
 bus voltage angle profiles generated in s
 ! A
 and the magnitude of the mode's real porti
 -! & 377 9B
 ? # " ! \$)% "
 + B "
 < " !
 6!) > # ? !? %
 # 397B7 -!
 3! " %
 " B ") !
 0! 5 9)" B % 5 9) 1
 ! " 5 ! 2 41 377 9B

" g%nerator's
 & ! / 9!) & 50(< 9 # (@ ! -77 700,0- 0
 ' () 70.! O @ < 9! \$(7 7!
 /- 9! A 59 ! % ! ! + ! 9 O (' O 9!
 1 E <) B ! ! (" \$ O (' O 7 7!
 /6 H! \$! *! + (! ' ! 9 !) " ! ! ' ! 9! (' O <
) 5' % ! 5=306 O (" B) 7 7!
 /3 S! H! 8 ' ! ! T T! E 8! O 5 9 70
 O (" 700 \$ 9 9 70

! 5 8 ? ' 2 7 8 ' 9 4 B " !
 ? 5 8 ? ') 2 3 7 8 ' 4 9 1 B !
 9 > B ! (3 % ! 0 0 6 0 3 U 0 - U U
 - 3 7 " B ") !
 ! 1 3 7 7 9 B ! " !
 ! 8 ' 1 3 7 7 9 B ? ! "
 + ! 8 ' 1 3 7 7 9 B 7 > 3 9 B !
 0 0 . U 0 = 7 0 6 1 7 - U 7 " %
 8 , 5 3 5 8 ? ' 1 * !
 " Q 0 / 7 " " " " * !
 " " " " * !

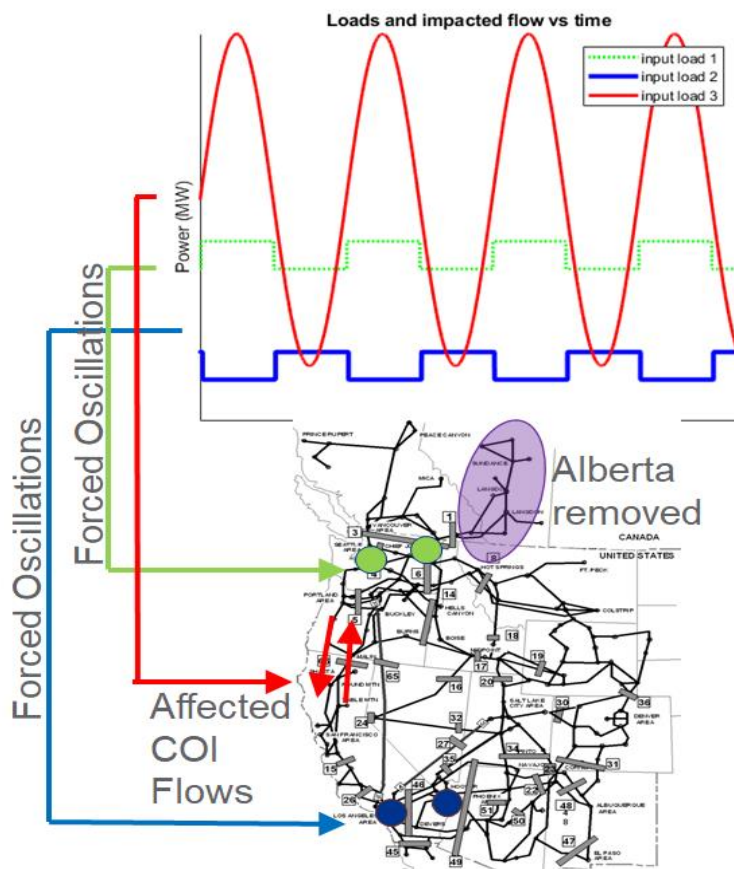


Figure 6-5. Load oscillation simulation.

? " 5 % 3/7 " 5 "
 5 & 15 " 50 ! # E > !

8 ,5! 8 5 # # " %
 05 " 0 " % " *
 5 8' 50 8' " 377 9B
 % * 5 "8! 0 ?
 0!3! "5 8' 0 % " B
 " " F " % " ! B % B
 % 5 8' 5 8' %
 5 8' 50 8 0! 5
 0 ! E " % 8' 5 8' * " 0 %
 5 8' 50803 0!6!
 0 377 9B ? ! E " %
 2 '8'4 " 2 '8'4
 model's internal protection, shown in
 %) % " #
 < " " !

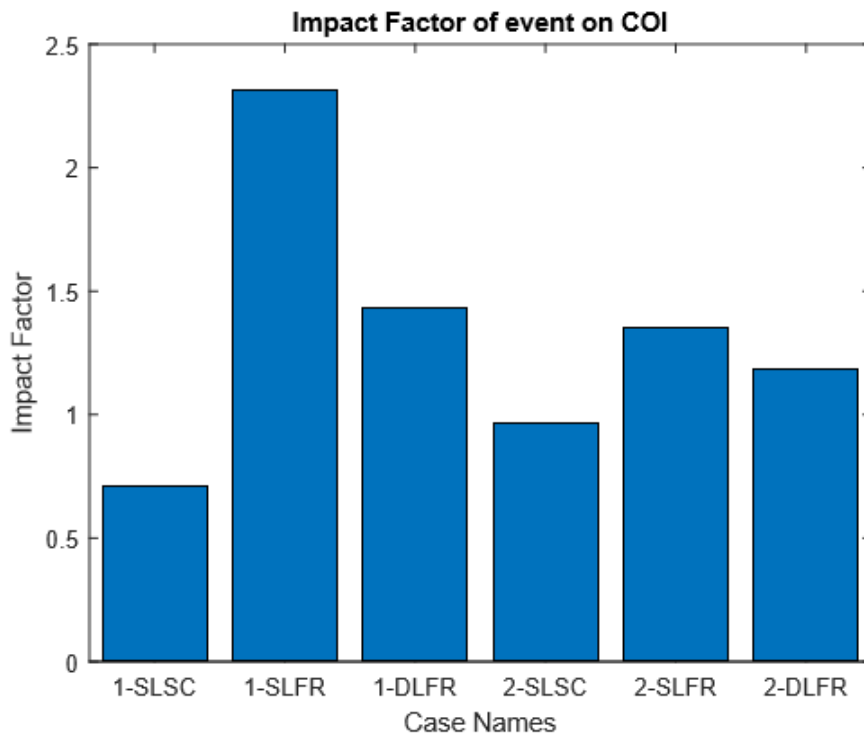


Figure 6-6. Impact factors by case names

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 % ! %
 # " ! % " # %
 " " !
 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 # #
 2* 41
 /! 8 5? %5 5 2 < \$4 < "
 =! % " 2 '4 ?
 %
 !
 "

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

" # " 0 # <
 ! * 03 - = % "
 " -5 " % " 37 # B - 4
 % " % ! 3 9B
 ? " < " < \$ " %
 G 8 ! ") H / = 6 ; 0 67 2 ; ! !
 < Q 0 4

5 " " 8
 ,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, *Penetration of High Power Integration Handbook-006* for Distribution
 H 70,!

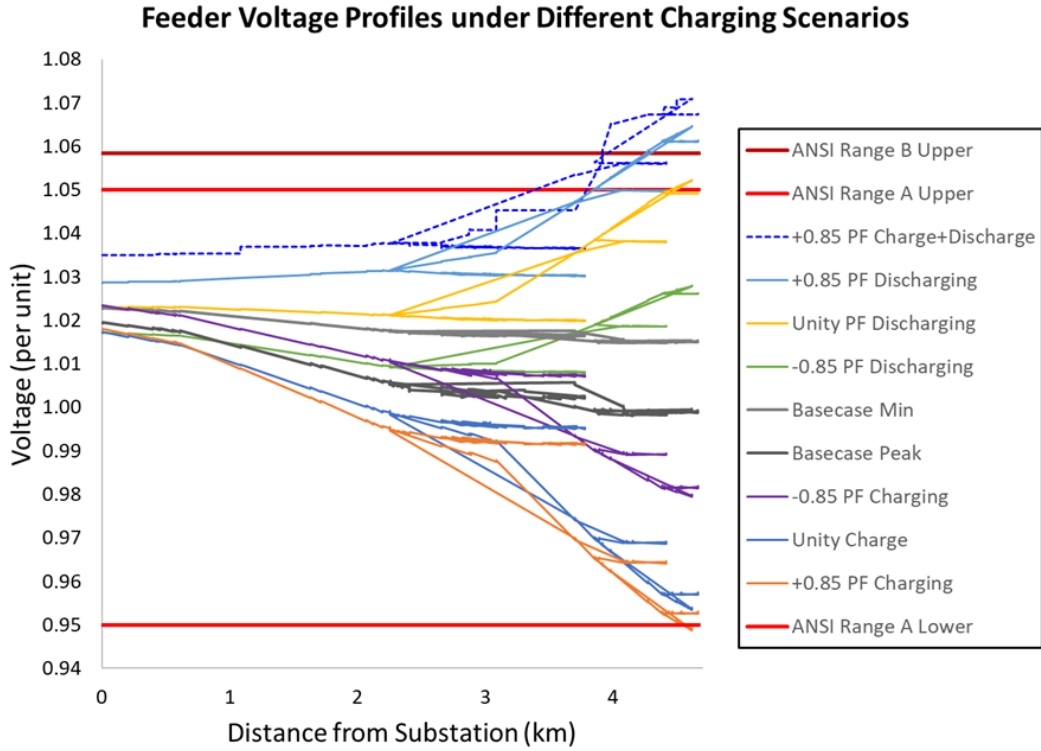


Figure 6-7. Different distribution voltage profiles for coordinated charging/discharging of EVSE totaling 2.25 MW.

6.2.2. Oscillations on the Distribution System

" ,! 0!

!"

% * 5

!"

!" 0 7

" 5 " ? 2 K 4

2 ' 9 D ' 4 " 2 B < D ' 4

5 %

" ,5! "

" B "

" %

" ! + "

" %

" ! "

! ! H! + # H! ! K > 9! H! ' ' !)! O H! (" 8 ")

(< \$ O 5 3 - 7 0 -) 7 0 -

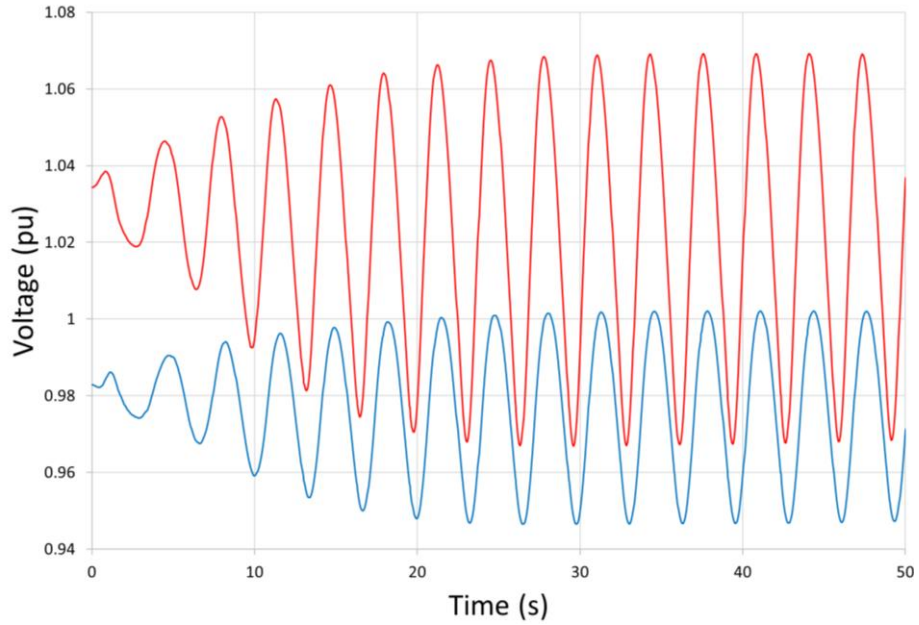


Figure 6-8. The highest (NWV_RES) and lowest (RMN_RES) of the transmission voltage profiles used in the distribution system simulations.

K " 37
 " 03 ; 2 Q , , ! 5 , . 5-7 4! " 03
 % ! % " % "
 " # " " % 1 "
 0! (! 9 " " % %
 % " ! 8 ! - & " % % " % 07
 ! " & %

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

As shown in Table 1, feeder "DA2" experienced

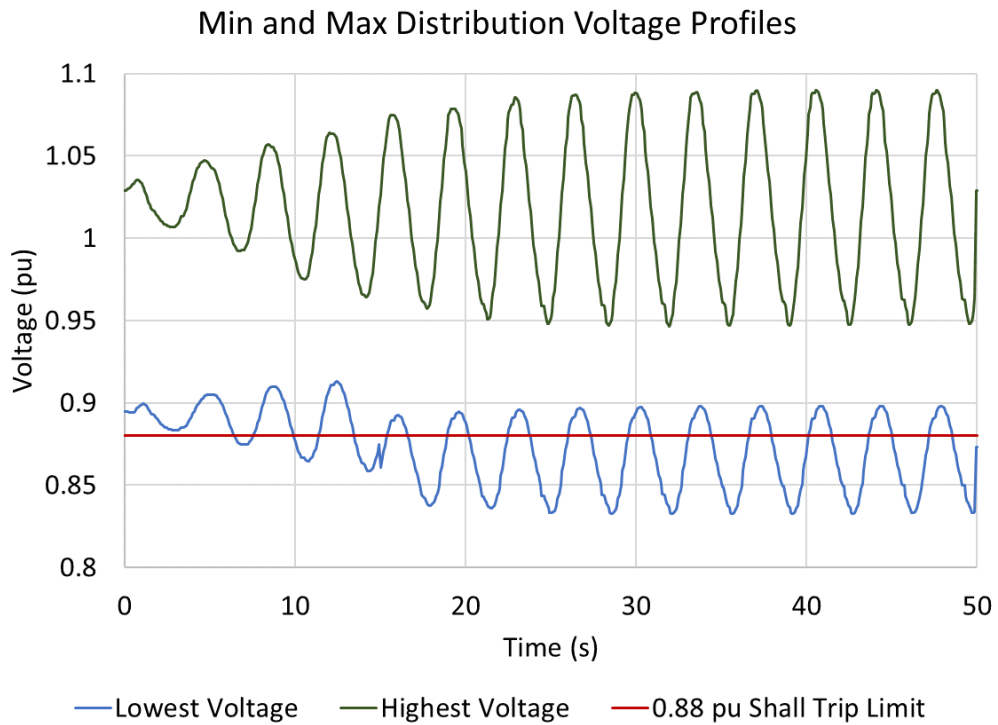


Figure 6-9. Highest and lowest voltage profiles for feeder DA2 under the implementation of the transmission voltage profiles.

036.!

0365706 " ? " " ? 577-

? 570/!

036.

%

6!)

0536.

? 5 "

%

?

6!

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

03677-		0365.706		03670/	
Voltage (% of base)	Clearing time (s)	Voltage (% of base)	Default Clearing time (s)	Voltage (% of base)	Default Clearing time (s)
< U 37	7!0,	< U 63	7!0,	< U 63	!77
5 0 ≤ V < 8	!77	4 5 ≤ V < 6	0!77	5 0 ≤ V < 8	0!77
1 1 0 ≤ V < 1 1 5	0!77	6 0 ≤ V < 6 5	!77	1 1 0 ≤ V < 1 1 5	0-!77
V ≥ 1 2 0	7!0,	1 1 0 ≤ V < 1 1 5	0!77	V ≥ 1 2 0	7!0,
		V ≥ 1 2 0	7!0,		

) % % 8 ,5 " ' ? "

7!!! 5!!!. % — " & 0!0 ! E " %

8 ,5 ' ? " 0.88 pu Shall Trip Limit "

5 !

!)

% " 7!!! 7 ! " "

! % !

?

7. POWER SYSTEM RISK

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

		Consequence (Power System I)				
		Insignificant No Observable Impact to Power System	Minor Local Power System Impacts	Moderate Regional (Distribution) Blackout	Major Widespread (Transmission) Blackout	Severe Widespread Outage for Extended Period
Likelihood (Threats +)	Almost Certain <i>Vulnerability Exploitable By</i> Attacker: Script Kiddie Funding: None Time: Days	Medium	High	High	Extreme	Extreme
	Likely <i>Vulnerability Exploitable By</i> Attacker: Skilled Actor Funding: Little Time: Weeks	Medium	Medium	High	Extreme	Extreme
	Possible <i>Vulnerability Exploitable By</i> Attackers: Moderately-Skilled Team Funding: Some Time: Months	Low	Medium	Medium	High	Extreme
	Unlikely <i>Vulnerability Exploitable By</i> Attackers: Skilled Team Funding: Substantial Time: Years	Low	Low	Medium	High	High
	Rare <i>Vulnerability Exploitable By</i> Attackers: Nation State Funding: Substantial Time: Decades	Low	Low	Low	Medium	High

Figure 7-1. EVSE Cybersecurity Risk Matrix

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

56 //M. Mateski, et al. "Cyber Threat Metrics" SAND2012-0566.
 57 /D. P. Duggan, S. R. Thomas, C. K. Vittich, L. Woodard. "Cybersecurity Risk Matrix." SAND2007-0534.
 58 J. Johnson, et al., "Power System Effects and Mitigation (H70-1)"

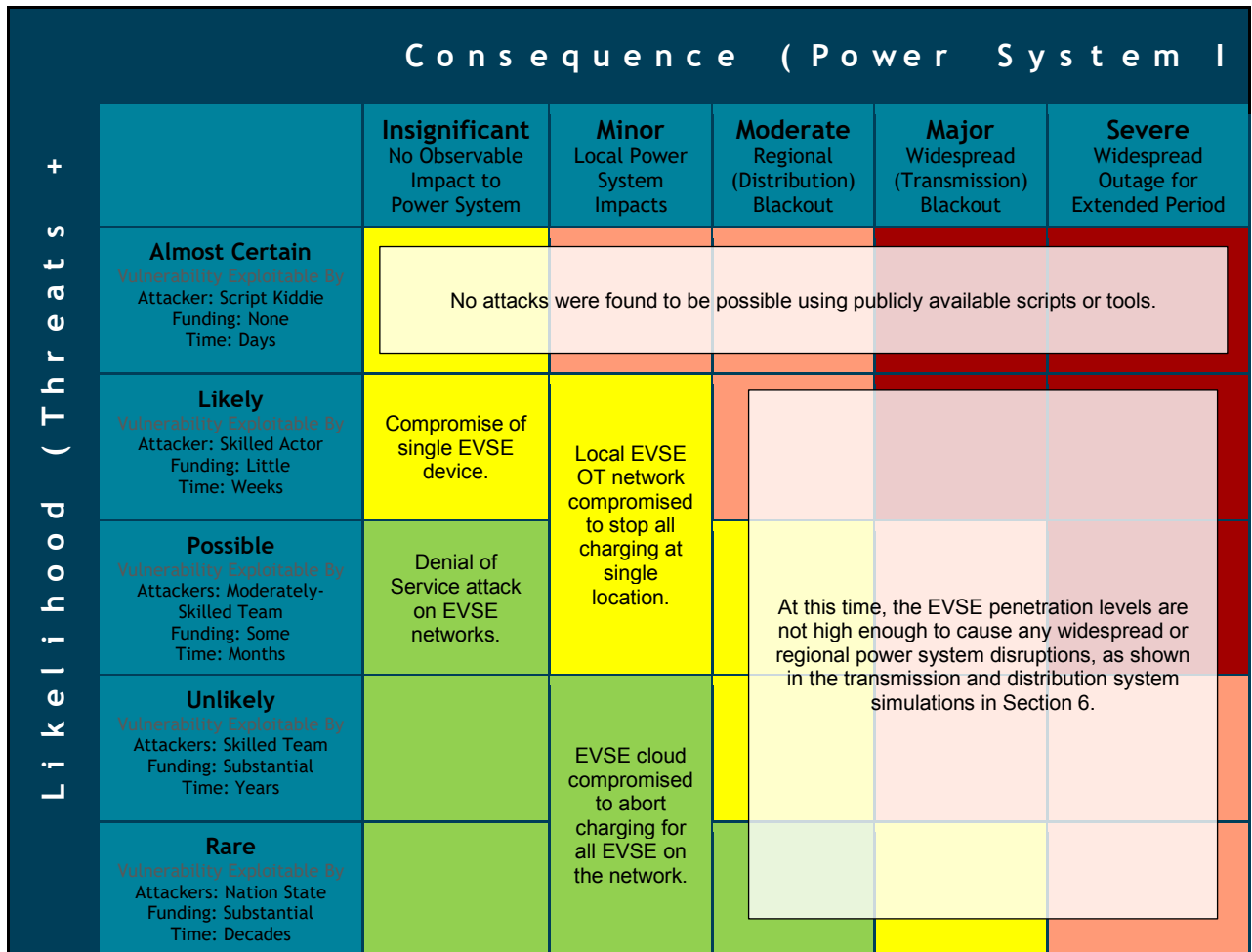


Figure 7-2. EVSE Cybersecurity Attacks Mapped onto the Risk Matrix

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

=0A! ' +!l s o n , " (8 or ni s v e e q n u e C y 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 6 7 ' / = 6 8 8
 ? 2 < 4 ! 0 7 0 =!

5 9 #! 2 !! 4! # < " #
" #
% " " %
+ " ! # " > " & !
"

8. MITIGATIONS AND RECOMMENDATIONS

8.1. Mitigations

8.1.1. Business Network & Operations

- " > % % 3!0 ! <; < "
 - % 3!!0)
 -) &) 3!
- ' % " " % !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) ! 3M +! % %
- % < L) ! 3M +!

8.1.3. EVSE Network & Operations

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

-) " # < " # " " # !
- " # L) ! M !
- " < ! L) M !
- & " 2 &! !4L) M !
- " 5 < " " % !L) < -M ! " #
- * * 4" 2 !
- & !
- L) -M !
- " "
- 5 " !L) 6M !
- (% " L) ! 6M !
- > " ?" 5 " #
- L!) 3M !
- % ? < ?
- L) # ! ,M !
- " " Door " Op e a r m s , s y s t e m l o g i n n o t i
- % > L) <M ! !
- " % L) 1
- !/M
- < ?
- L) /M !
- < % =M
- < " L) ! 01M !

8.1.4. Electric Vehicle Operations

% !

8.2. Best Practices

8 " "

% < %

!

E 9 ! 2 95 9 4 %

" 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
" # !) " # " 1
• % > <
! <
• % ? 2 < " 4 !
5 5 " ? 2 < " 4 !
• " ; %
! " % % !
• 5 "5 # !
5 % " !
!

APPENDIX A. DETAILED ASSESSMENT RESULTS

A.1. Business Network and Operations

4 " % >

H 1) " > " - % " - %

" ! " # ** (

4 " !

9 1' % " " % !

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

L)! 20 4 (" >

H 1) " " % "

% " ! " 5 "

! 8 " % # " #

" # !

9 1

!

! challenge anyone they don't recognize at t

! < > & % !

L)! 2M" 4

H _____ 1 9
%

%
< " "

9 _____ 1
>
!

< ! %

<

<

" !

" #

?
!

!!

%

% !

>

>

<

" %

&

"

"

>

<

" %

<

"

<

<

?

"

%

"

A.2. EVSE Security

L+! 0 4 <
!

H _____ 1 9
%
5
"

"

9 _____ 1
#

5 %

? !

% "

< !

< &

" #

&

#

F !

" 2

% ?

&

" %

%

! ! ! (

%

!

> !

4

L+! 2 4

%

< !

H _____ 1 % < & <
" %
< ! < " < %
9 _____ 1 B ? !
> ! !

L+!2 4 % !
H _____ 1 " % % < !
% % % % !
! & % % (<
9 _____ 1 ! " !
& " !

L+!6M 2E 4 < " " < !
H _____ 1 " ? #
% < " !
9 _____ 1 > % !

L-3M2 " 4 % !
H _____ 1 " % " # < " % " !
i s r a t e d " # " 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 !0M 2E 4 < " "

H _____ 19 < < " ? ! B % #

9 _____ 1 > !

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

H _____ 1 < " # " ;

! < " # & " ! " < (" % " # " ! " detected. Even with the proposed use of a " # " % " # !

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

L ! 2 E 4 < % > " # !

H _____ 1 < " # ! < " # !

% ! B % !

9 _____ 1 " 5 % # ! %

L ! 2 E 4

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

9 _____ 1 " 5 " ! " " <

% " !
% & !
L ! 3 4 <
H 1 " # " < E " %
" # " " # ! " " #
% " " " # ! " " < #
9 1 % # ! # 5 ?
< " #

L ! 2 4 < % !
H 19 " # " % < " " -
" # " % ! " " "
\$ " " "
" fingerprint " to < !
" % & & " "
" % < ! " "
9 1 ? < ! ? %
! " 5 " " %
% !

L ! 2 4
H 1 %
< " # ! A " # !
" ; " 5 !
E " % % ; & 5 % !
& 5 % !
9 Ensure that " Door Open " alarms , sys
% > < !
" > % # !
&

L ! 2 4 < ? " + # !

$\frac{H}{?} 1^*$ < ! " +
 + #! % " > " +
 $\frac{9}{1}$ < % " % " <
 ? # ! < " " <
 L ! 2 M 4 < " " < ! B %
 $\frac{H}{<} 1$ < % ! %
 " " < ! B %
 % " !
 $\frac{9}{5} 1$ " % % <
 L ! 0 7 M 4 < % !
 $\frac{H}{<} 1^*$ < ! " , *9 K(0 ! " #
 < > ! " ! #
 $\frac{9}{#} 1 <$!) " # " " #
 # " ! " # " " "

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 Energy National Nuclear Security Administration under contract DE-NA0003525.