Consequence-driven Cybersecurity for High Power EV Charging Infrastructure

Richard “Barney” Carlson
Ken Rohde

May 1, 2019

INL/CON-19-53546

www.inl.gov

Idaho National Laboratory

INL Cyber Security Timeline

2003 — DOE OE → DHS CSSP → Industry Partners → Work for Others → LDRD → DOE EERE — 2019+

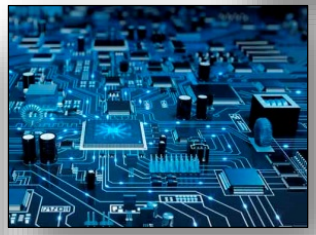


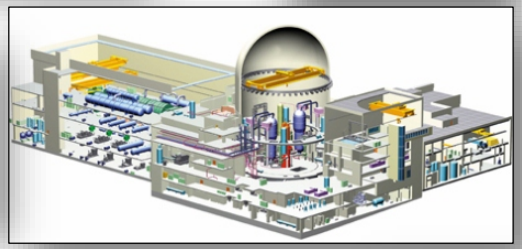




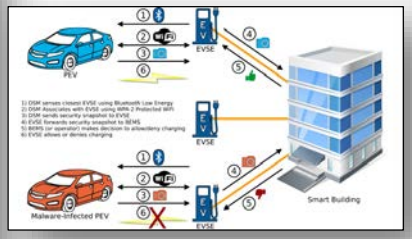











Consequence-driven Cybersecurity: High Power EV Charging Infrastructure

Objective

- Determine vulnerabilities that enable High Consequence Events (HCEs)
  - Xtreme Fast Charging (XFC) 350 kW+
  - Wireless power transfer (WPT)
- Develop mitigation strategies and solutions
  - Secure, identify, and maintain resilient operation
- Publish solutions, information, and lessons learned

Relevance

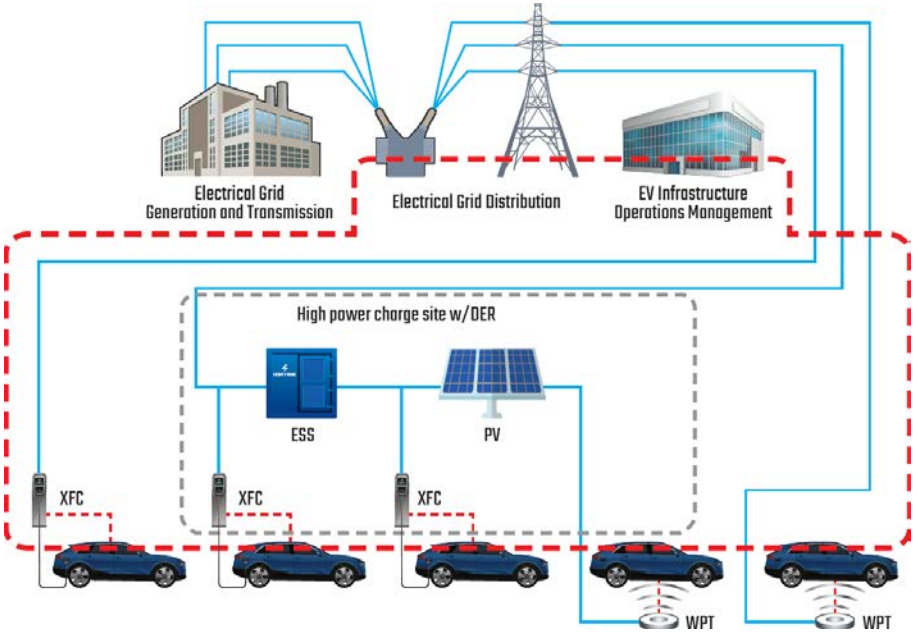
- Public access to high voltage / high current
- Consumer confidence plays major role in EV adoption
  - Safety, reliability, and financial security
- Many communication & controls pathways

  = many attack vectors for cyber attackers

Approach

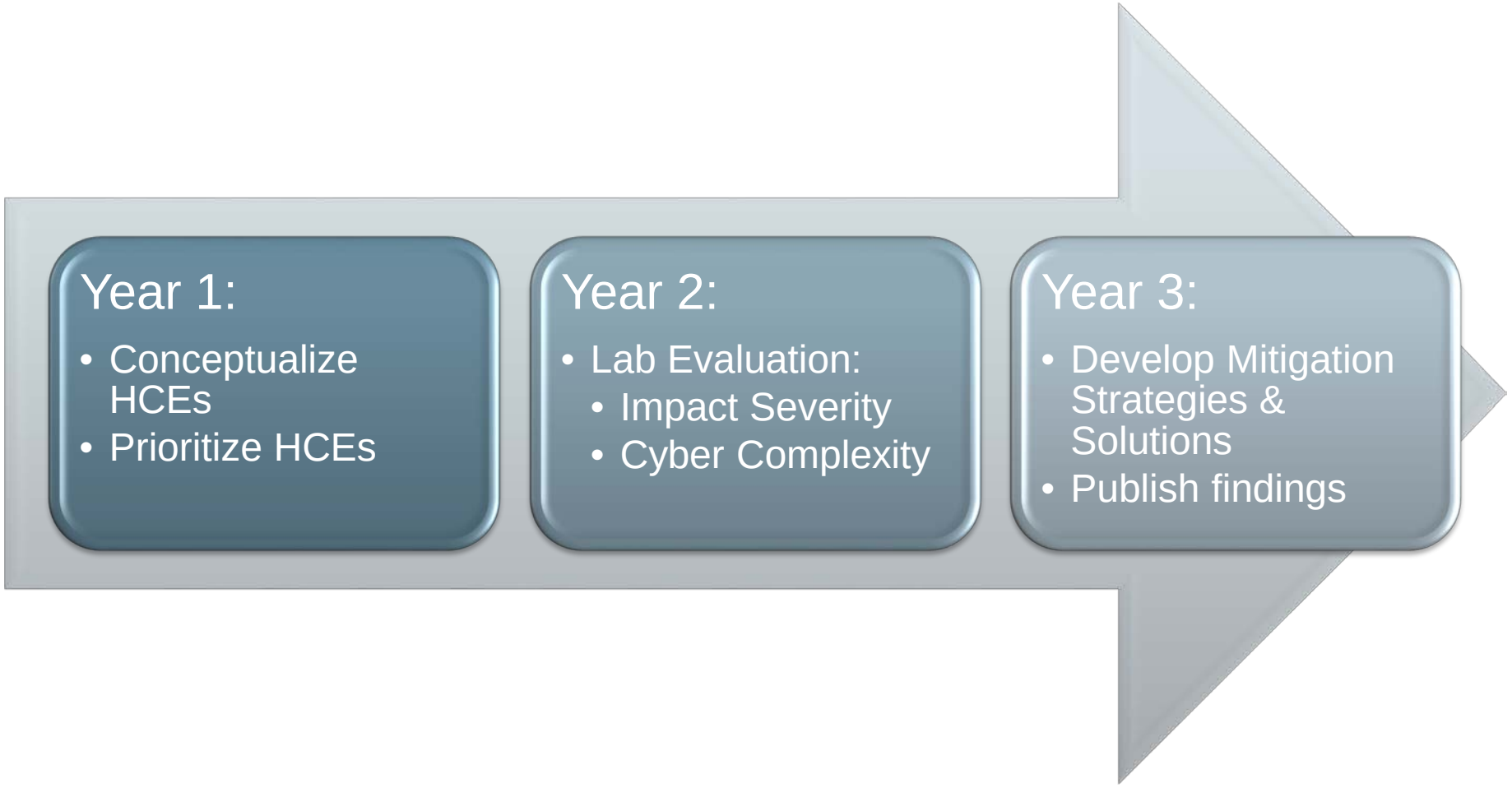
- Conceptualize high consequence events (HCE)

- Prioritize HCEs based upon:
  - **Impact Severity**
  - **Complexity Multiplier**
    - Ease of cyber manipulation



- For the highest prioritized HCEs
  - Laboratory evaluation of:
    - impact severity
    - cyber manipulation complexity
  - Recommend methods to harden attack surfaces
  - Develop mitigation strategies and solutions
  - Recommendations for safe resilient operation during cyber event
    - Cyber informed engineering practices
  - Recommend methodology(s) to safeguard personal information & data
  - Means to identify cyber malicious event

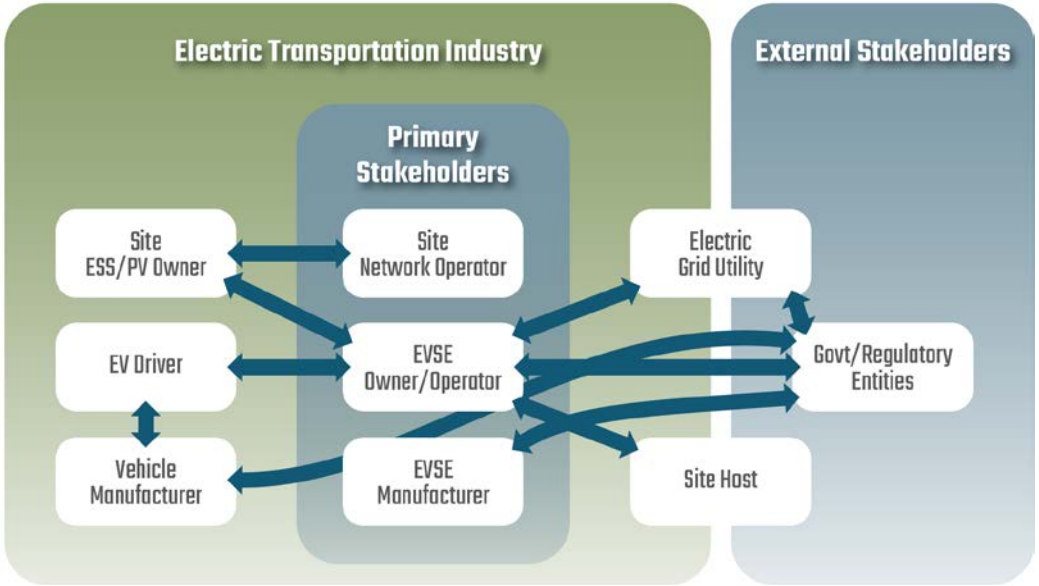
Project Timeline



Approach

- Categories of HCEs
  - Impact to the electric grid
  - Safety
  - Hardware damage (charger, vehicle, etc.)
  - Denial of service
  - Data theft or alteration

- Stake holders:
  - Charge Site Owners / Operators
  - Charge Network Operator
  - EVSE Manufacturers
  - Electrical Utilities
  - EV Drivers
  - EV Manufacturers (OEMs)
  - Government / Regulatory Entities
  - Site host
  - Electric Transportation Industry



HCE Prioritization

HCE Score = Impact x Complexity

- Impact Severity
  - Severity based on 8 criteria
  - Weighting factor used for the 8 criteria
- Complexity Multiplier
  (ease of cyber-manipulation)
  - Number of attack vectors required to be concurrently manipulated
  - Expertise of attacker(s)

HCE Scoring

Complexity Multiplier					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

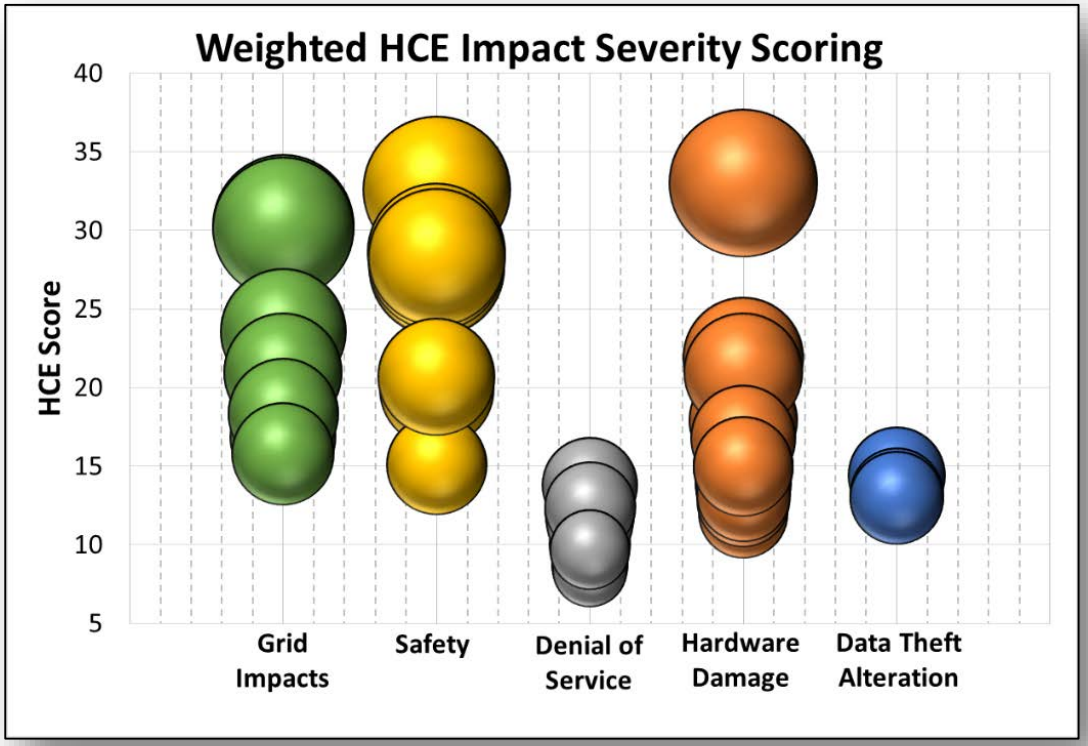
Impact Severity

Impact Severity Scoring

Criteria	N/A (0)	Low (1)	Medium (3)	High (5)
Level of Impact	N/A	Single unit affected (EV, XFC, or WPT)	Multiple units at a single site affected (EV, XFC and/or WPT)	Multiple unit at multiple sites affected (EV, XFC and/or WPT)
Magnitude (proprietary or standardized)	N/A	Manufacturer specific protocol implementation (EV or EVSE)	>1 manufacturers protocol implementation (supply chain) (EV or EVSE)	Across all standardized systems (both EVSE and EVs)
Duration	N/A	< 8 hours	> 8hr to < 5 days	> 5 days
Recovery Effort	Automated recovery without external intervention	Equipment can be returned to operating condition via reset or reboot (performed remotely or by on-site personnel)	Equipment can be returned to normal operating condition via reboot or servicing by off-site personnel (replace consumable part; travel to site)	Equipment can be returned to normal operating condition only via hardware replacement (replace components, requires special equipment, replace entire units)
Safety	No risk of injury	Risk of Minor injury (no hospitalization), NO risk of death	Risk of serious injury (hospitalization), but low risk of death	Significant risk of death
Costs	No Cost incurred	Cost of the event is significant, but well within the organization's ability to absorb	Cost of the event will require multiple years for financial (balance sheet) recovery	Cost of the event triggers a liquidity crisis that could result in bankruptcy of the organization
Effect Propagation Beyond EV or EVSE	No propagation	Localized to site	Within metro area; within single distribution feeder	Regional; impact to several distribution feeders
EV Industry Confidence, Reputation Damage	No impact to confidence or reputation	Minimal impact to EV adoption	Stagnant EV adoption	Negative EV adoption

HCE Impact Scoring

- Highest impact events:
  1. *Safety / Hardware damage*: Battery fire due to overcharging
     - site ESS or EV battery
  2. *Safety*: Shock/burn hazard from damaged cord set due to thermal manipulation
  3. *Grid Impacts*: Power outage due to sudden load shed or increase of XFC site
     - XFCs concurrent shed load or site ESS steep load increase
  4. *Safety*: Public exposure to high WPT EM-field (w/ implanted medical devices)



High Ranking: XFC Cord Set Thermal Manipulation

- XFC thermal system manipulation
  - Thermal sensors spoofed causing no cooling of cable and connector (insulation failure)
  - Unique vulnerability to XFC
- Event:
  - XFC cable failure / melting
- Impact:
  - Public safety & hardware damage
    - Burn hazard
    - Shock hazard
      - depending upon state of insulation
    - Cable replacement required
- Possible mitigation solution:
  - Minimum coolant flow rate
  - Redundancy:
    - Flow rate based on current & thermal sensors used to trim flow rate

High Ranking: WPT Operation with NO Vehicle Present

- WPT primary coil (ground-side) operating at full current
  - Wireless communications spoofed causing operation with no EV present
  - Unique vulnerability to WPT

- Event:
  - Ground-side coil at full current

- Impact: potential public safety
  - EM-field exposure
  - Metallic object heating
  - Implanted medical devices interaction

- Possible mitigation solution:
  - TBD

Low Ranking: Charger Display: "Out of Service"

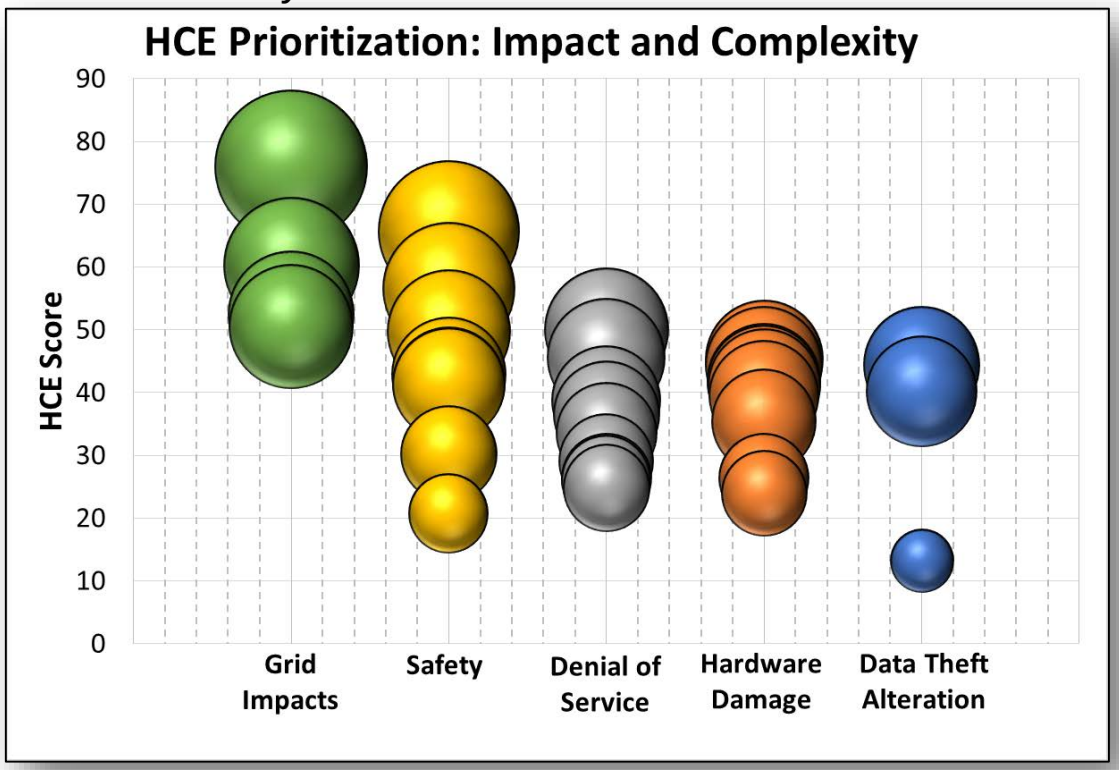
- Charger is fully operational but…..
  - Cyber manipulation spoofs charger HMI / display to indicate…
    "Out of Service"

- Event:
  - EV driver likely to not attempt to charge
- Impact: Denial / Loss of Service
  - Loss of revenue for site
  - EV driver frustration
  - Difficult to remotely identify since the charger is fully operational but not being utilized
- Possible mitigation solution:
  - Internal communications monitor to identify abnormal operation
  - Redundancy

HCE Prioritization

- Prioritized events (impact and complexity):
  - *2. Safety*: Shock / burn hazard from damaged cord set due to thermal manipulation
  - *3. Grid Impacts*: Power outage due to sudden load shed or increase of XFC site
    - XFCs concurrently shed load or site ESS steep load increase
  - *4. Safety*: Public exposure to high WPT EM-field (w/ implanted medical devices)

  ~~*1. Safety / Hardware damage*: Battery fire due to overcharging~~ **(high complexity)**
    - ~~site ESS or EV battery~~

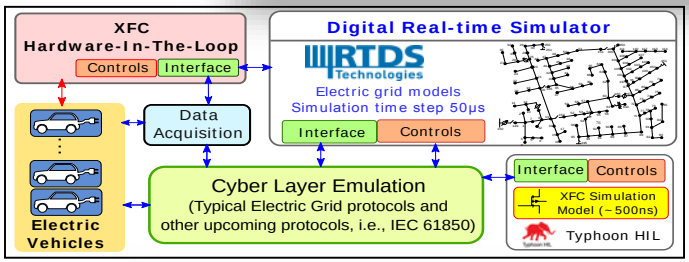


Future Research: Laboratory Evaluation & Mitigation Development

Assess the *highest* prioritized HCEs:

- Validation of cyber manipulation complexity:
  - Laboratory hardware evaluation
  - Power hardware-in-the-loop research

- Evaluation of :
  - Potential grid impacts
    - Power hardware-in-the-loop
  - Cyber complexity of
    - Communications and controls
    - Electrical operation
    - Thermal systems



- Guidance and recommended solutions
  - Solutions to hardened attack surfaces of vulnerabilities
  - Methodology to safeguard personal information & data
  - Method to identify occurrence of cyber malicious event

Any proposed future work is subject to change based on funding levels

Recommendation: Cyber Security Methodology

- **Prepare**
  - Identify potential system vulnerabilities
  - Hardened attack surfaces of vulnerabilities
  - Develop a methodology to safeguard personal information & data
  - Develop response plan & mitigation strategies and solutions
  - Design system for safe / minimum operation during cyber event

- **Attack Response**
  - Identification of cyber malicious event
  - Execute response plan
  - Communication to stake holders
  - Data collection for forensics

- **Clean-up and Close-out**
  - Forensics analysis
  - Clean-up efforts to get system back to full operation
    - Ensure attack vector has been completely closed and event has ended (not merely dormant)
  - Share lessons learned w/ others in industry

Future Research:

- Publish project results and recommendations for high power EV charging infrastructure stakeholders
  - Prioritized list of HCEs
  - Results from laboratory evaluation
    - Validation of impact severity
    - Evaluation of cyber manipulation complexity multiplier
  - Mitigation strategies and solutions
    - Methods to hardened attack surfaces of vulnerabilities
    - Means to identify cyber malicious event
    - Recommendations for resilient operation during cyber event
    - Recommend methodology(s) to safeguard personal information & data

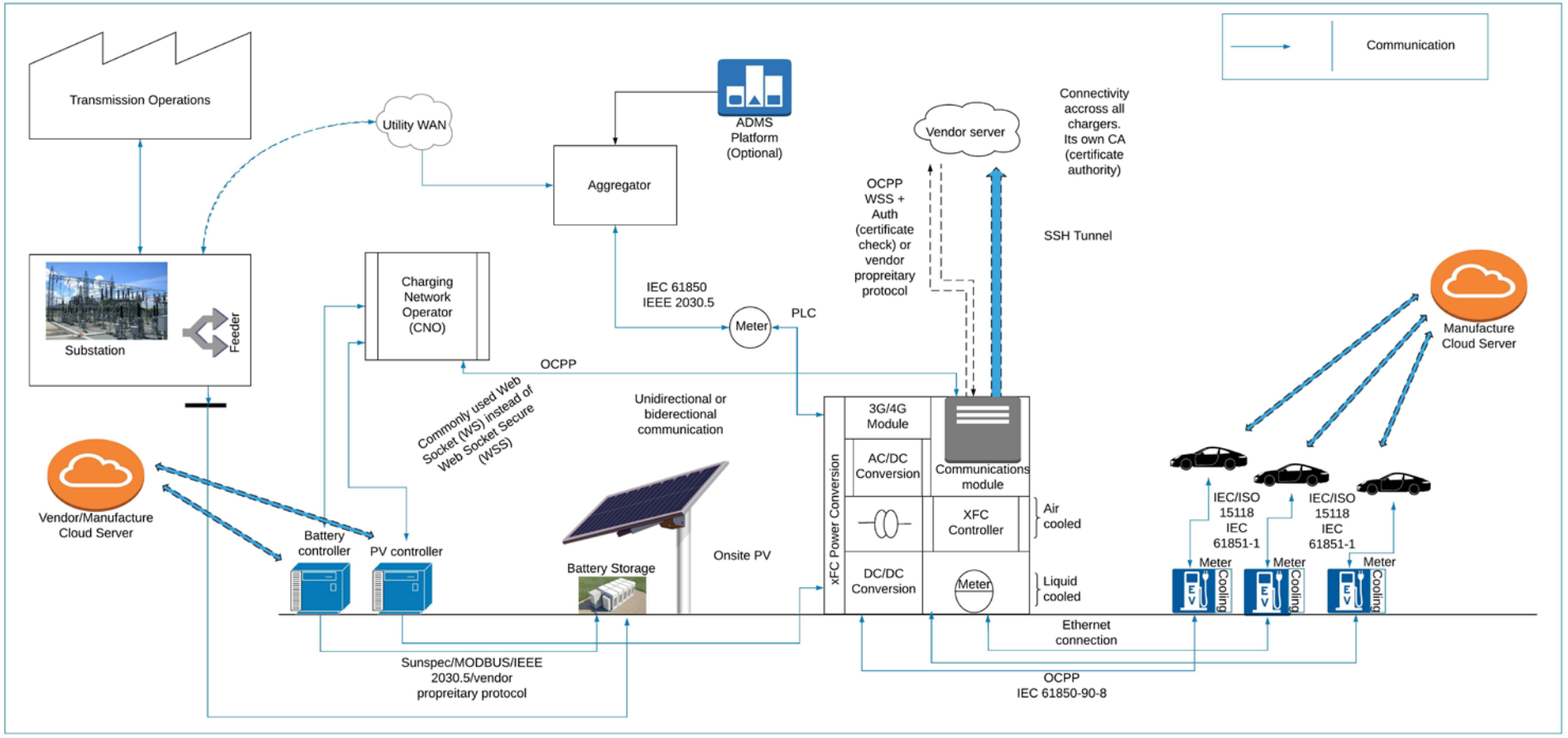
Any proposed future work is subject to change based on funding levels

Summary

- Prioritization of high consequence events for high power EV charging infrastructure
  - Guides and focuses future research efforts
- Recommended cybersecurity approach methodology
- A secure EV charging infrastructure system:
  - Reduced risk to potential grid impacts and public safety
  - Increases consumer confidence

Backup slides

XFC Site Architecture Diagram

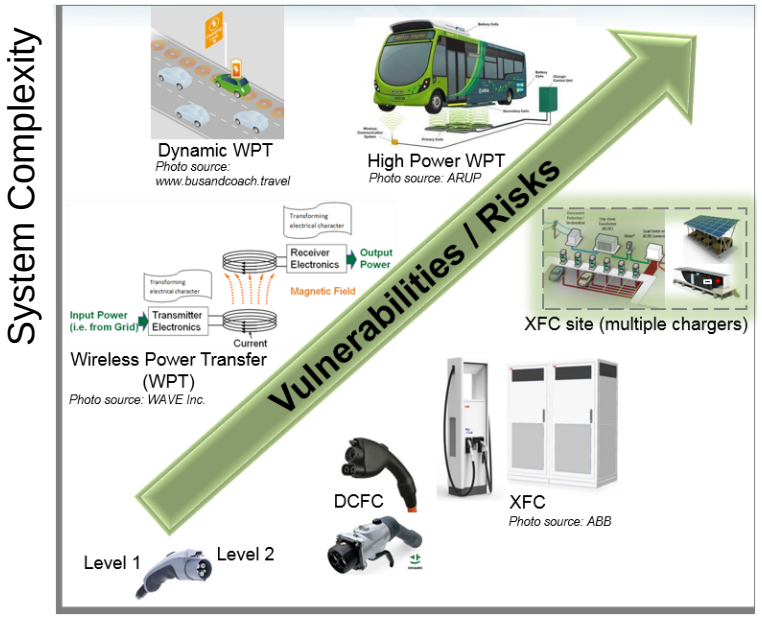


Overall Impact

- HCE process enables focused research on highest consequence events
  - Maximize output from limited budgets and resources

- Mitigating high consequence vulnerabilities for XFC & WPT
  - Supports technology growth and deployment

    (higher system power and complexity)
    - Improved consumer confidence in infrastructure
      - Reliability / functionality
      - Public Safety
    - Mitigate costly impacts to:
      - Electric grid
      - Charger hardware
      - Vehicles



HCE Prioritization

Idaho National Laboratory

HCE priortized List based on Impact Severity and Initial Likelihood Estimate (note: several similar High Consequence Events have been combined

HCE Priority	Likelihood x Weighted Score		HCE Description	Method	Assumption	
1	99.75	*Safety*	Injury or loss of life due to electrocution, electrical shock, or burns from exposed conductors of the XFC cord set cable	Overheating of cord set melts cord insulation, exposing the electrical conductors of the cable		An set sys ins
2	92.625	*Grid Impacts*	Power Outage(s) due to sudden load shed from XFCs.	Chargers or other site equipment shut down via controls manipulations or communications with the utility (i.e. OCPP).	Distributed Energy Resource (DER) is not present, site is on a heavily loaded distribution feeder, and manipulations occur during peak charging time	
3	81	*Safety*	Injury or loss of life due to electrocution or electrical shock by energized cord set while not plugged in.	Power to the cord set is turned on prior to the cord set being plugged into the EV		An set sys to
4	61	*Grid Impacts*	Power Outage(s) due to sudden load shed or load increase from on-site energy stroage manipulation.	Charge site battery controls manipulation. (Charging when it should be discharging, Adding load (ramp up) while XFC are ramping up too, Reversal of Power flow from site (battery bank) to grid as fast transient (abrupt change in load). OR Reversal of power flow from site ESS to grid followed by large load by ESS from grid as a fast transient causing sudden load decrease followed by load increase	Site and utility communicate to coordinate load balancing. If configured as anAC bus, the ESS must have fast response capabilties which is more susceptible to creating transient impacts. If site ESS is on a DC bus, the response rate (AC/DC) can be very slow since the DC bus response is inherently fast. The ESS therrefore acts as a buffer with respect to the grid.	Co fee
5	56.5	*Safety*	Medical device failure or injury caused by exposure of high electromagnetic field to implanted medical devices (applies only to wireless chargers).	Wireless charger turns on when it is not supposed to (no vehicle present) or living object detection system is manipulated		An wit ind sys
6	54	*Grid Impacts*	Damage to equipment within the feeder distribution area (transformers, switch gear, harmonics, overload capacitor bank, high reactive power)	Creation of power transients caused by cycling ESS (charge / discharge) or charger (on / off) OR Sustained voltage outside of utility specification (example: lower voltage causing higher current for constant power load); or injection of current harmonics		Gr ha op
7	52.2	*Grid Impacts*	The charger and DER at the site are not able to provide grid service (curtail, VAR support, etc.) when needed causing decreased stability/reliability of the grid	Grid service communication is manipulated; Sudden transients in load cause impact to feeder voltage stability, or non-responsive to demand response requests (via OCPP)		Th ad sit po de
8	51.5625	*Safety*	Burns caused by hot cord set	The cord set becomes hot enough to burn someone but does not become hot enough to melt the cord's insulation. (Reference OSHA burn hazard limit: 50 degC)	This danger is likely already mitigated by standardized plug safety touch-proof requirements which prevent fingers or other body parts from getting close enough to the energized components to create a safety hazard. However, if a conductive object is into the plug (such as key, screwdriver, paperclip or	Sa en co