UNIVERSITY OF OXFORD

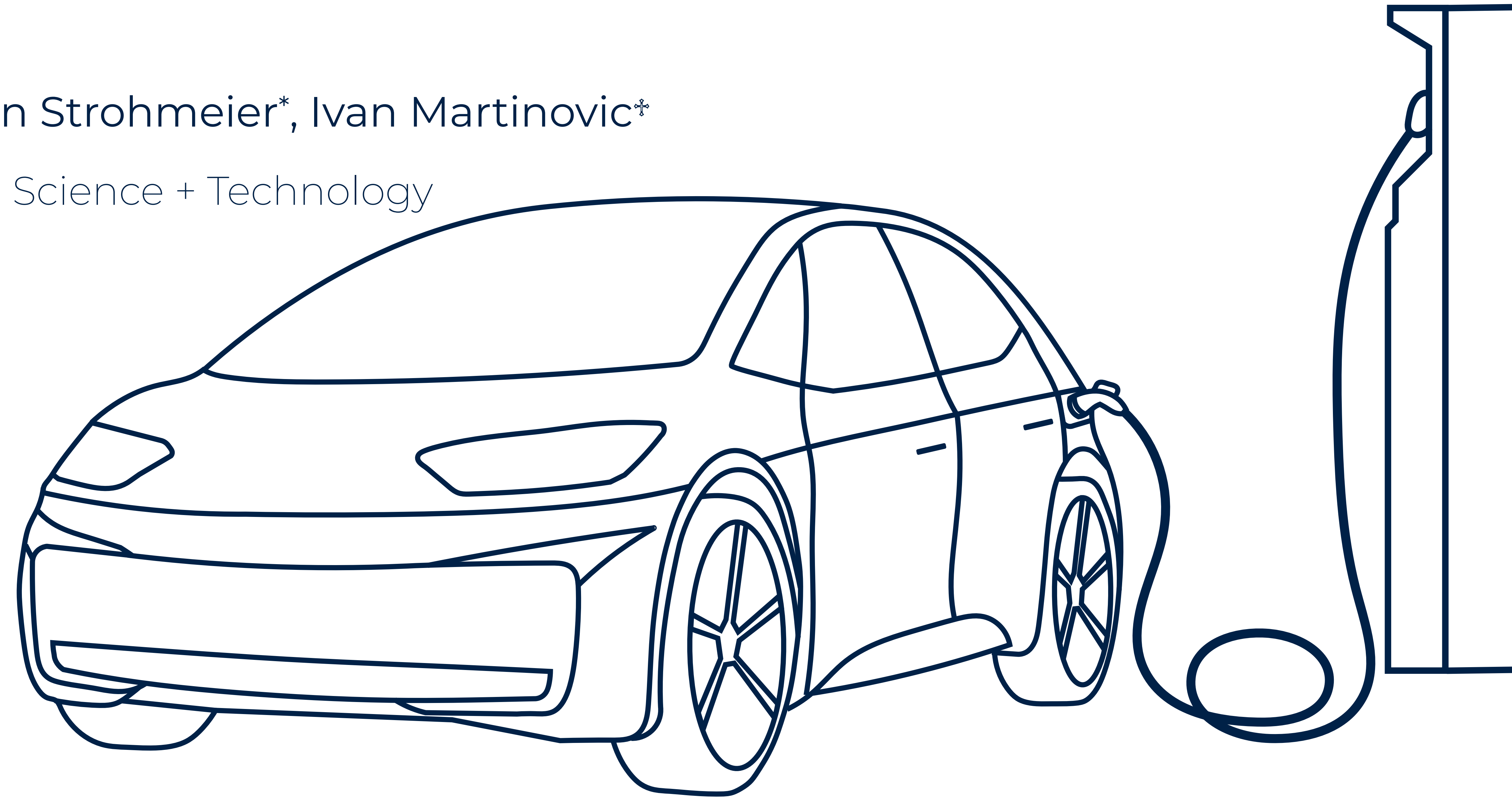
SSL Systems Security Lab

CENTRE FOR DOCTORAL TRAINING *in* CYBER SECURITY

Brokenwire:
Wireless Disruption of CCS Electric Vehicle Charging

Sebastian Köhler[‡†], Richard Baker[‡†], Martin Strohmeier[*], Ivan Martinovic[‡]

[‡]University of Oxford, [*]armasuisse Science + Technology



[†] Both authors contributed equally to this paper.

https://www.enbw.com/unternehmen/presse/groesster-enbw-schnellladepark-eroeffnet.html

https://www.ingenieur.de/technik/fachbereiche/e-mobilitaet/neue-initiative-fuer-den-aufbau-einer-ladeinfrastruktur-fuer-e-lkw/

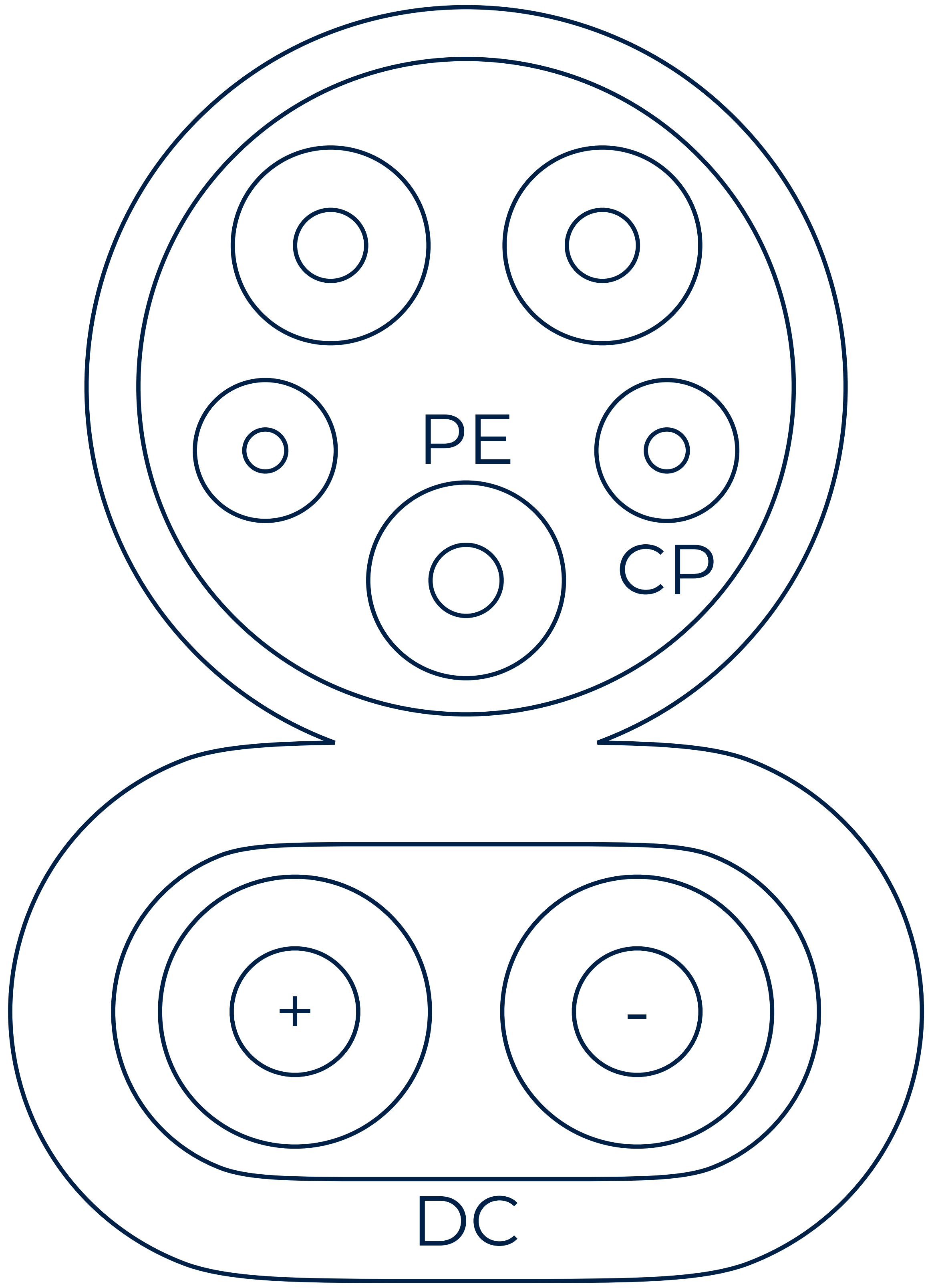
Credit: Hamburger Hochbahn AG

https://www.cleanelectric.de/mehr-baguettes-als-ladesaeulen/

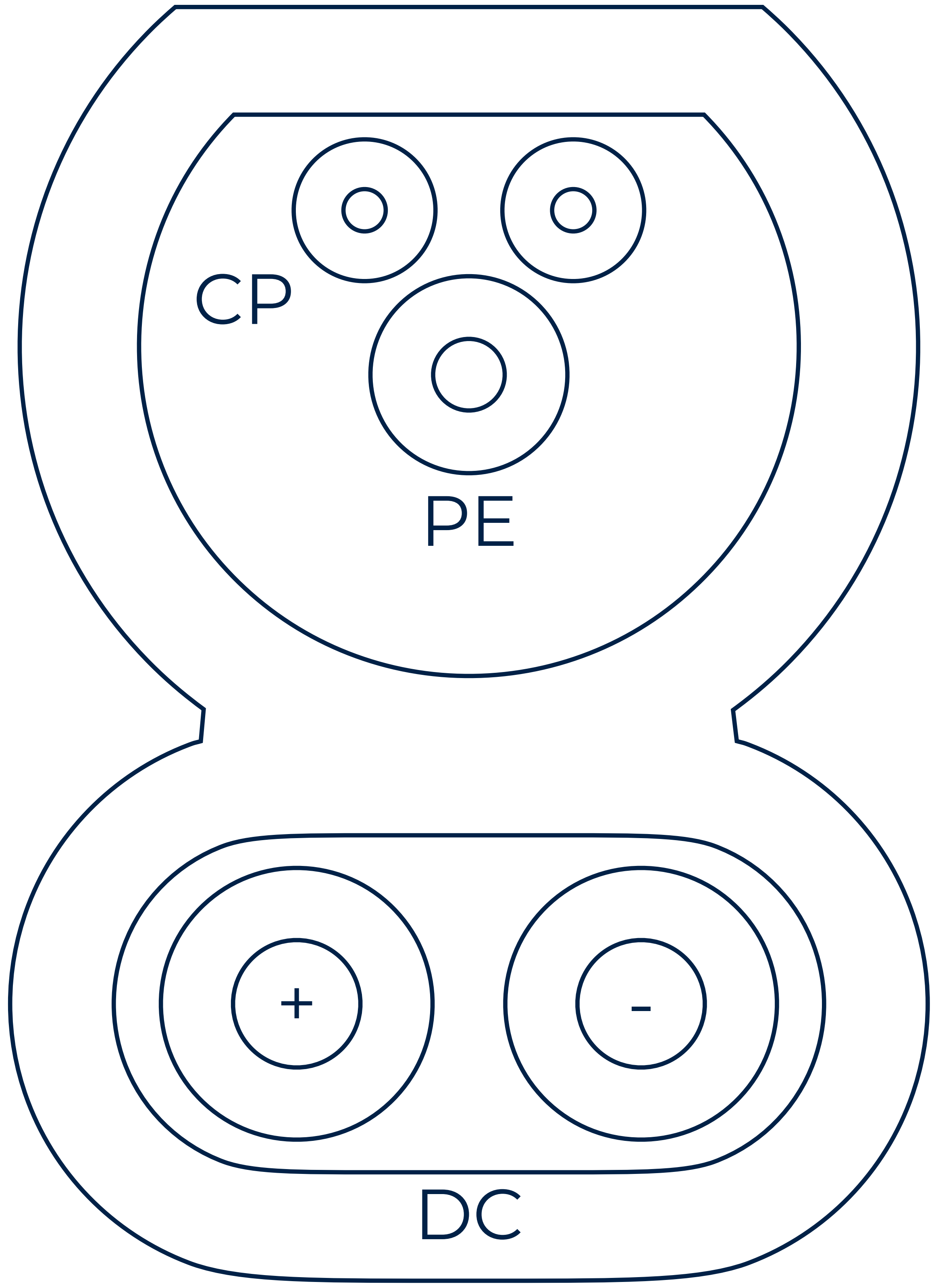
https://wall.alphacoders.com/big.php?i=933709

https://cdn.motor1.com/images/mgl/g3WJm/s2/efacec-s-first-350-kw-ccs-combo-dc-fast-chargers-already-up-amp-running.jpg

Combined Charging System (CCS)

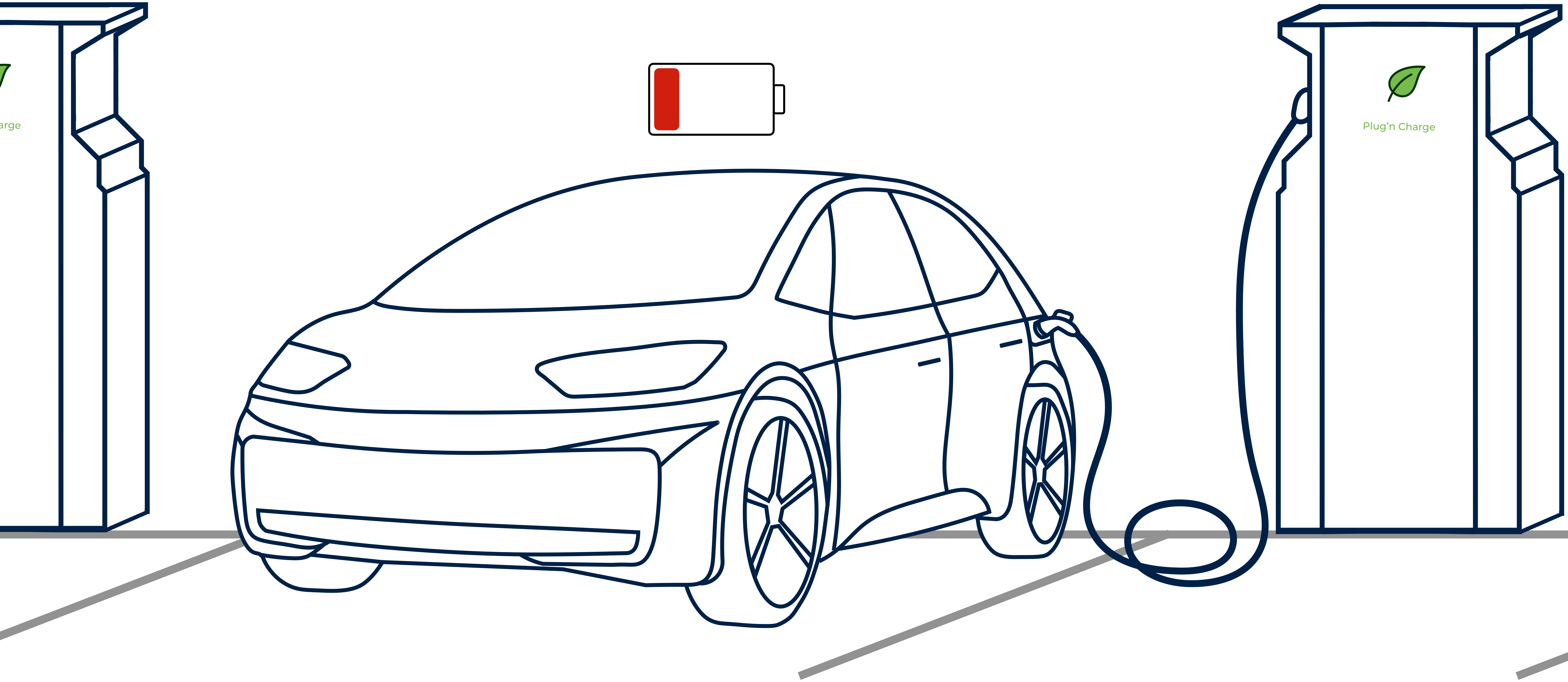


CCS Combo 1 (US)



CCS Combo 2 (EU)

CCS Power-Line Communication



Previous Work on EV Security

[1] Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.

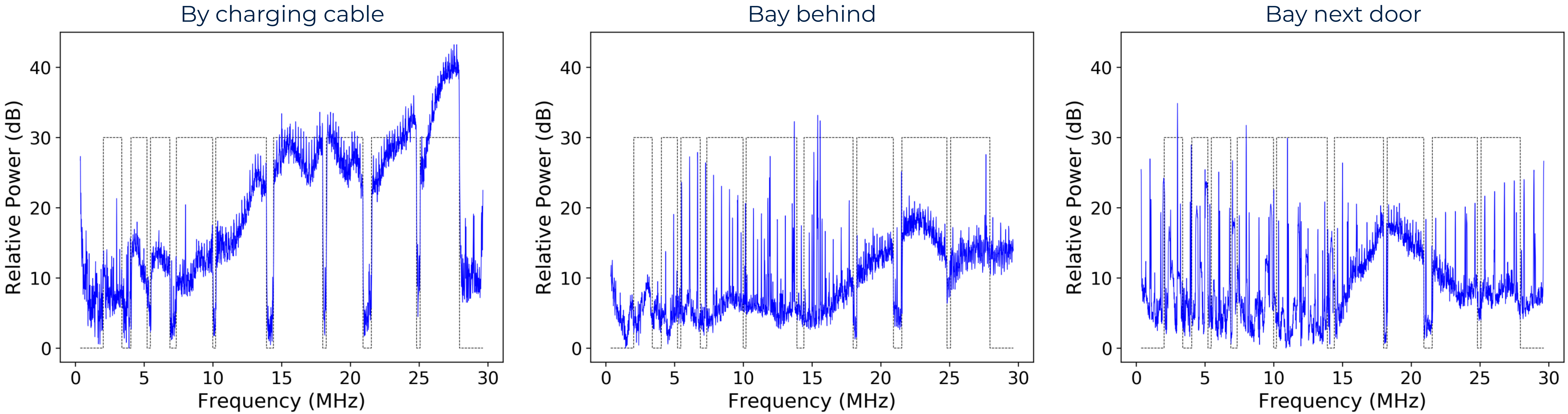
Previous Work on EV Security

*“[The] use of PLC in EV charging and the design of the CCS standard lead to a uniquely high-quality, **unintentional wireless channel**.“ [1]*

[1] Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.

Previous Work on EV Security

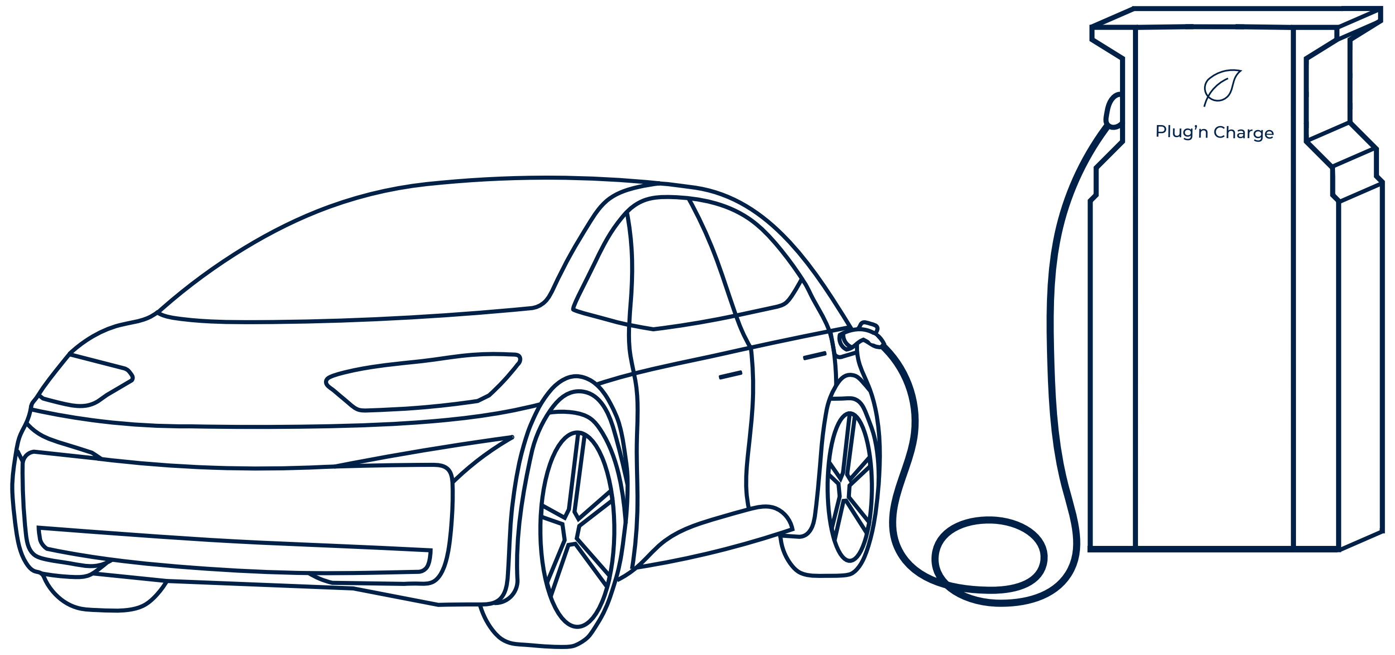
> *"[The] use of PLC in EV charging and the design of the CCS standard lead to a uniquely high-quality, **unintentional wireless channel**." [1]*



[1] Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.

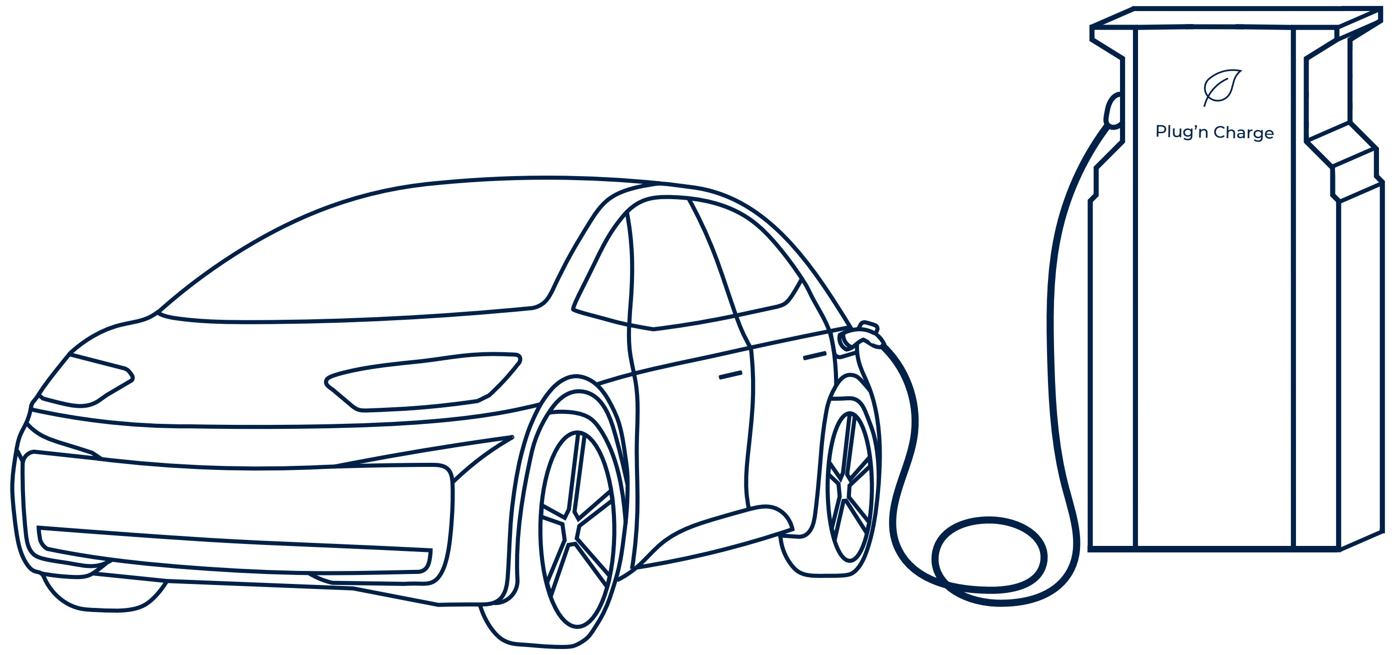
Threat Model: Goals

Threat Model: Goals

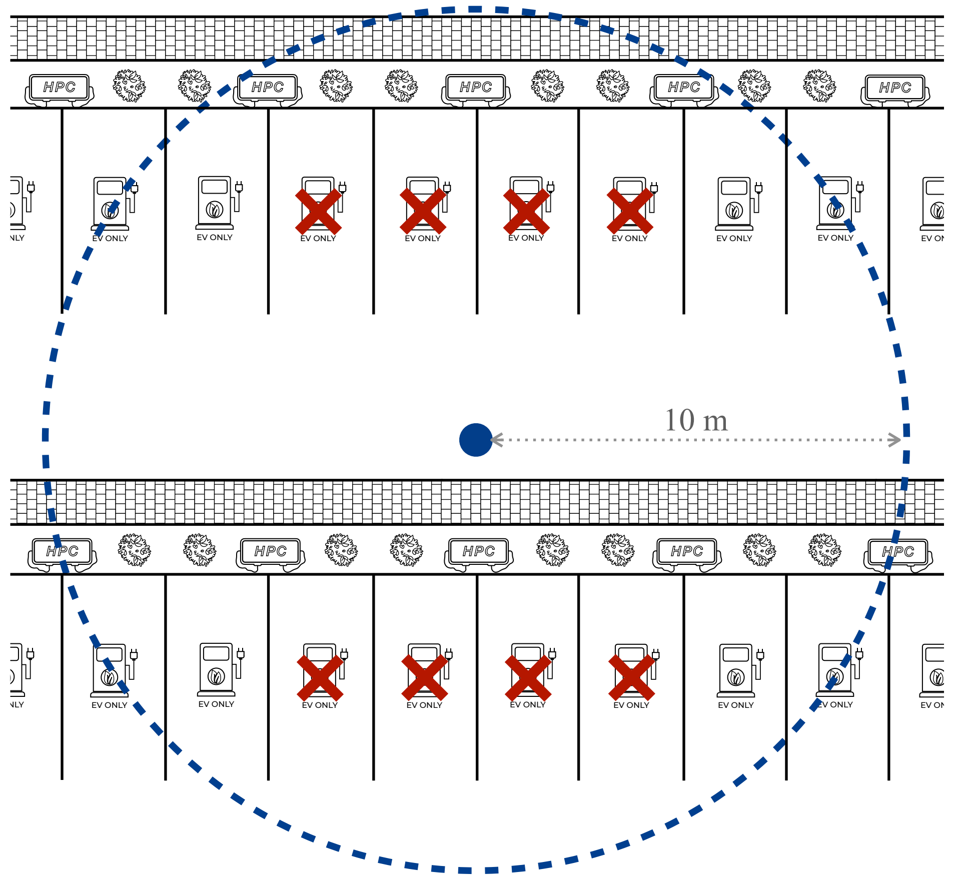


Individual Vehicle

Threat Model: Goals

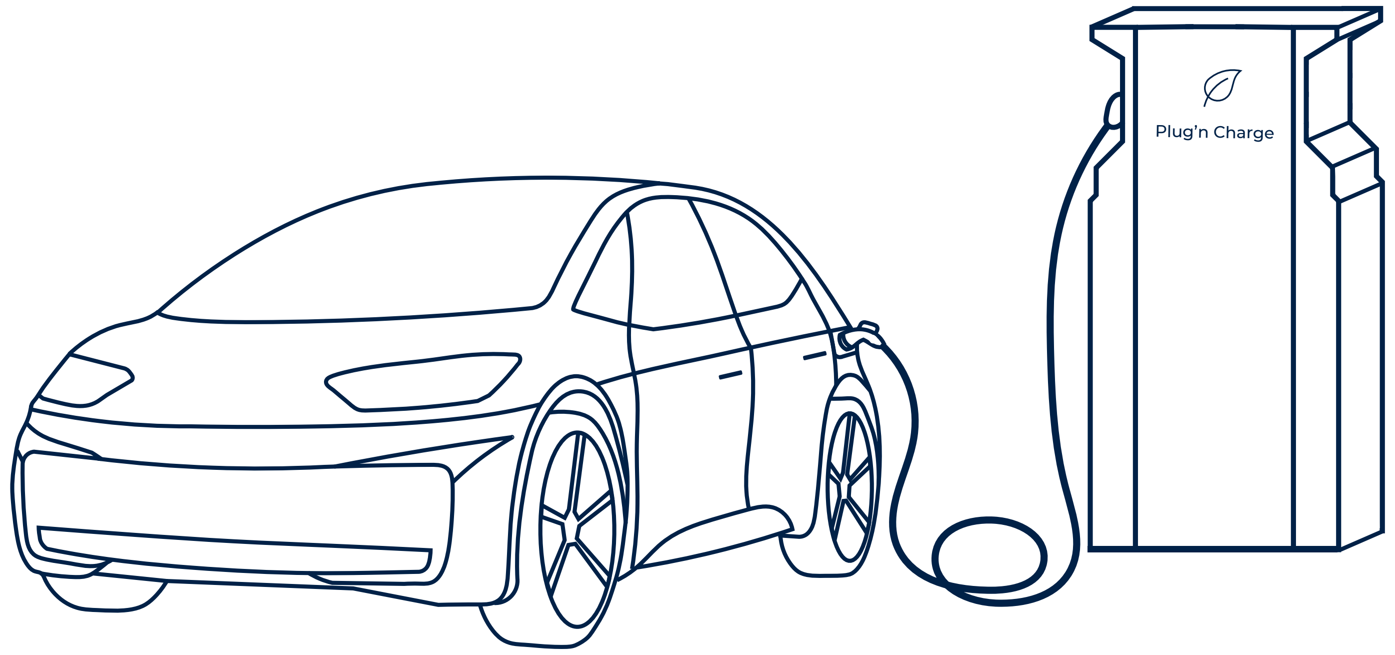


Individual Vehicle

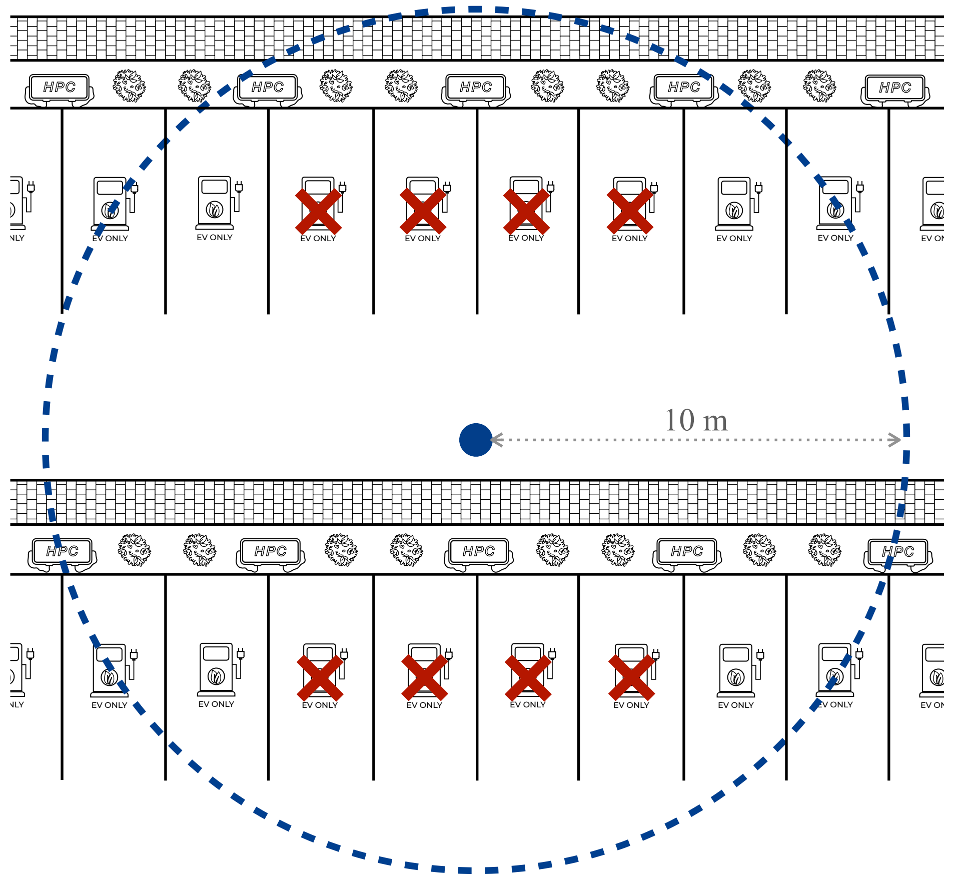


Fleet Denial

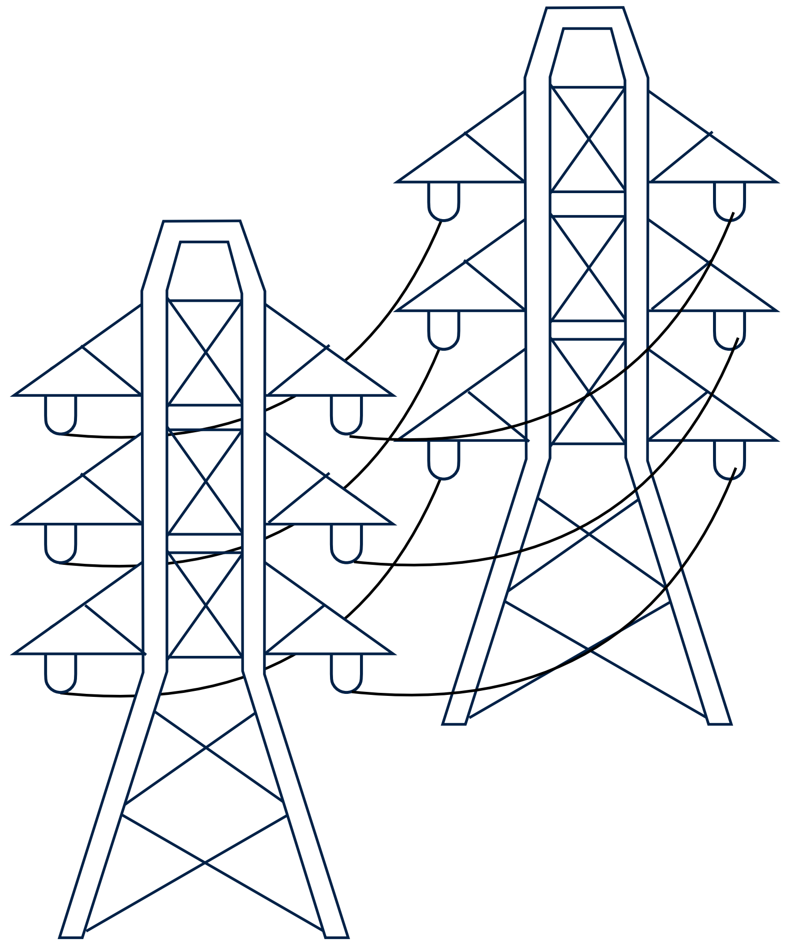
Threat Model: Goals



Individual Vehicle



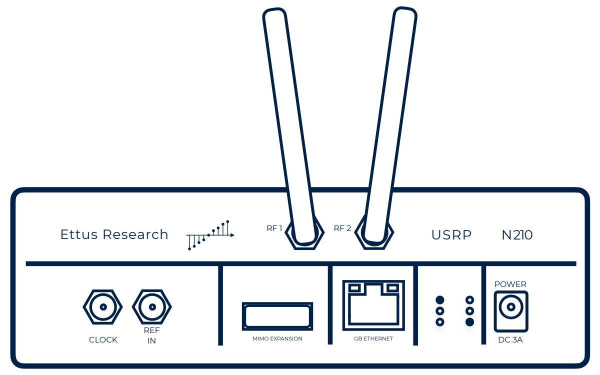
Fleet Denial



Unspecific Disruption

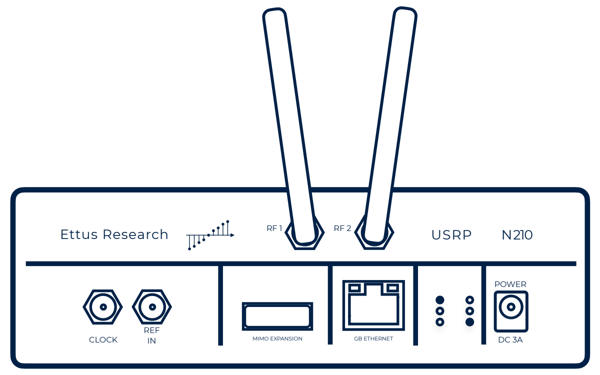
Threat Model: Capabilities

Threat Model: Capabilities



Access to off-the-shelf equipment

Threat Model: Capabilities



Access to off-the-shelf equipment

Little to no DSP knowledge

Brokenwire Attack: Wireless Exploitation of CSMA/CA

[1] Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.

[2] HomePlug Powerline Alliance. Homeplug Green PHY Specification. 2013.

Brokenwire Attack: Wireless Exploitation of CSMA/CA

“The receiver shall be able to ***detect the presence*** *of Preamble Symbols […]: When the desired Preamble Symbol waveform present at the receiver has a signal power of -35 dBm and is corrupted by Gaussian noise producing a* ***total SNR of 2 dB*** *at the receiver terminal.“ [2]*

[1] Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.

[2] HomePlug Powerline Alliance. Homeplug Green PHY Specification. 2013.

Brokenwire Attack: Wireless Exploitation of CSMA/CA

“The receiver shall be able to ***detect the presence*** *of Preamble Symbols […]: When the desired Preamble Symbol waveform present at the receiver has a signal power of -35 dBm and is corrupted by Gaussian noise producing a* ***total SNR of 2 dB*** *at the receiver terminal.“ [2]*

+

[1] Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.

[2] HomePlug Powerline Alliance. Homeplug Green PHY Specification. 2013.

Brokenwire Attack: Wireless Exploitation of CSMA/CA

“The receiver shall be able to ***detect the presence*** *of Preamble Symbols […]: When the desired Preamble Symbol waveform present at the receiver has a signal power of -35 dBm and is corrupted by Gaussian noise producing a* ***total SNR of 2 dB*** *at the receiver terminal.“ [2]*

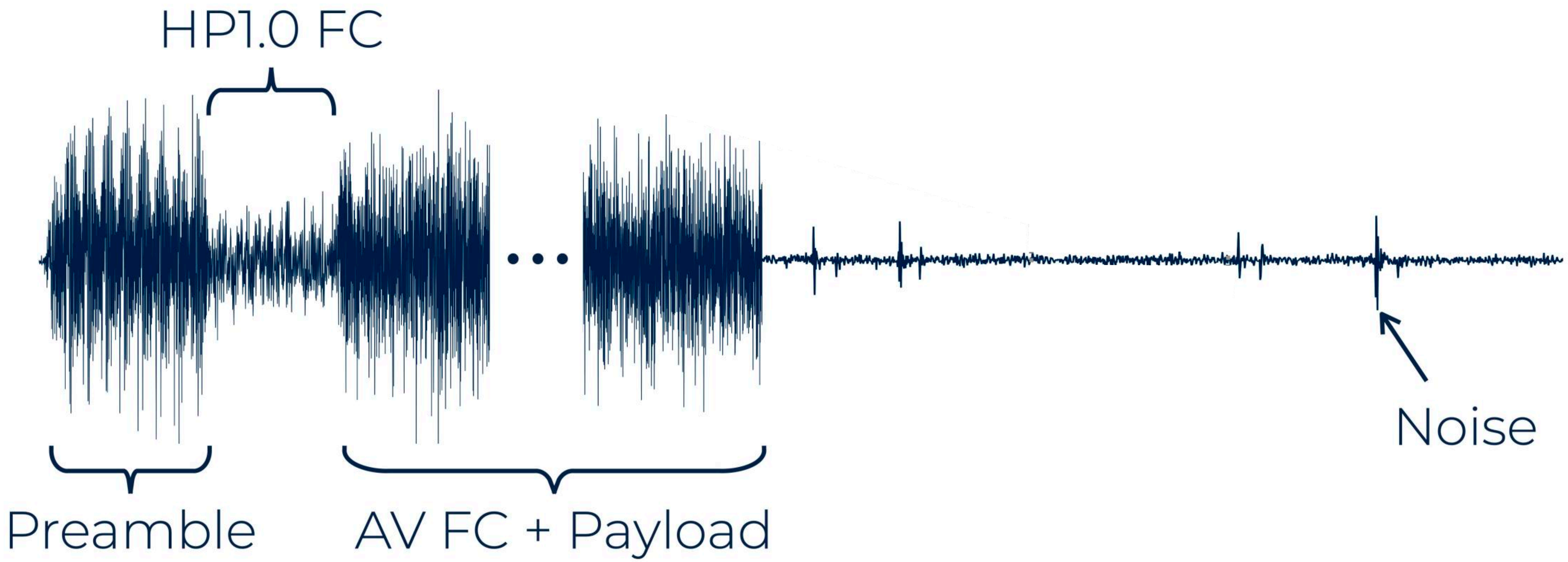
+

“[The] use of PLC in EV charging and the design of the CCS standard lead to a uniquely high- quality, ***unintentional wireless channel****.“ [1]*

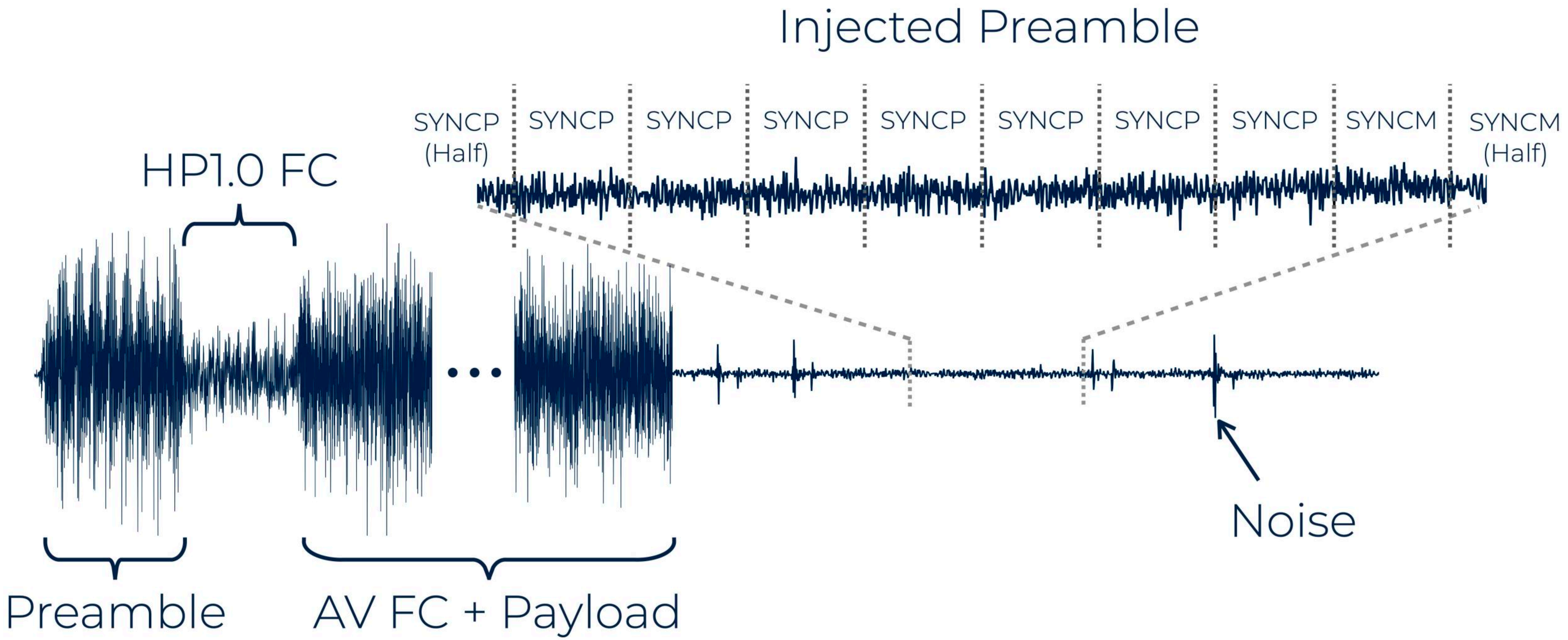
[1] Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.

[2] HomePlug Powerline Alliance. Homeplug Green PHY Specification. 2013.

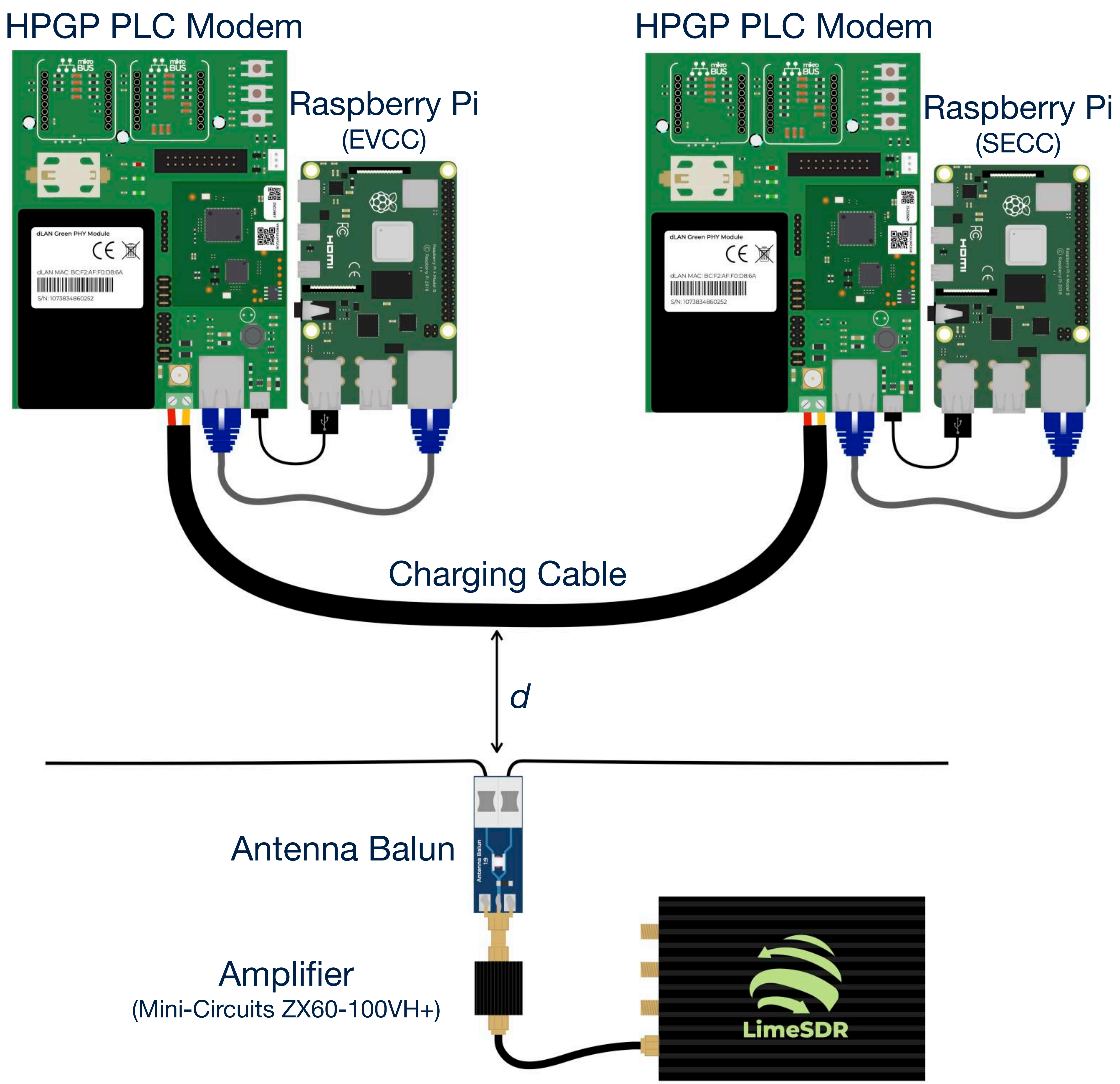
Brokenwire Attack: A closer look



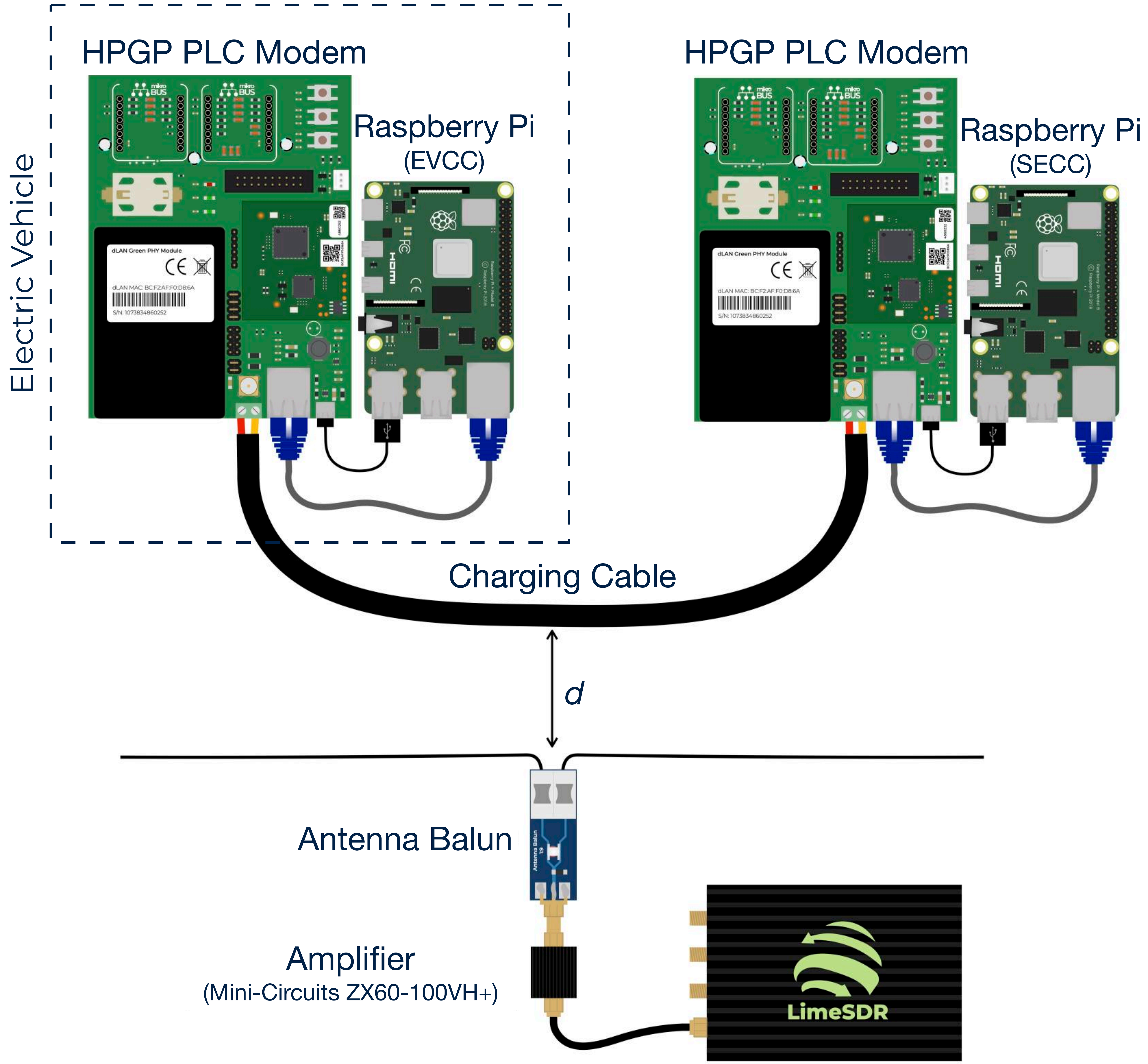
Brokenwire Attack: A closer look



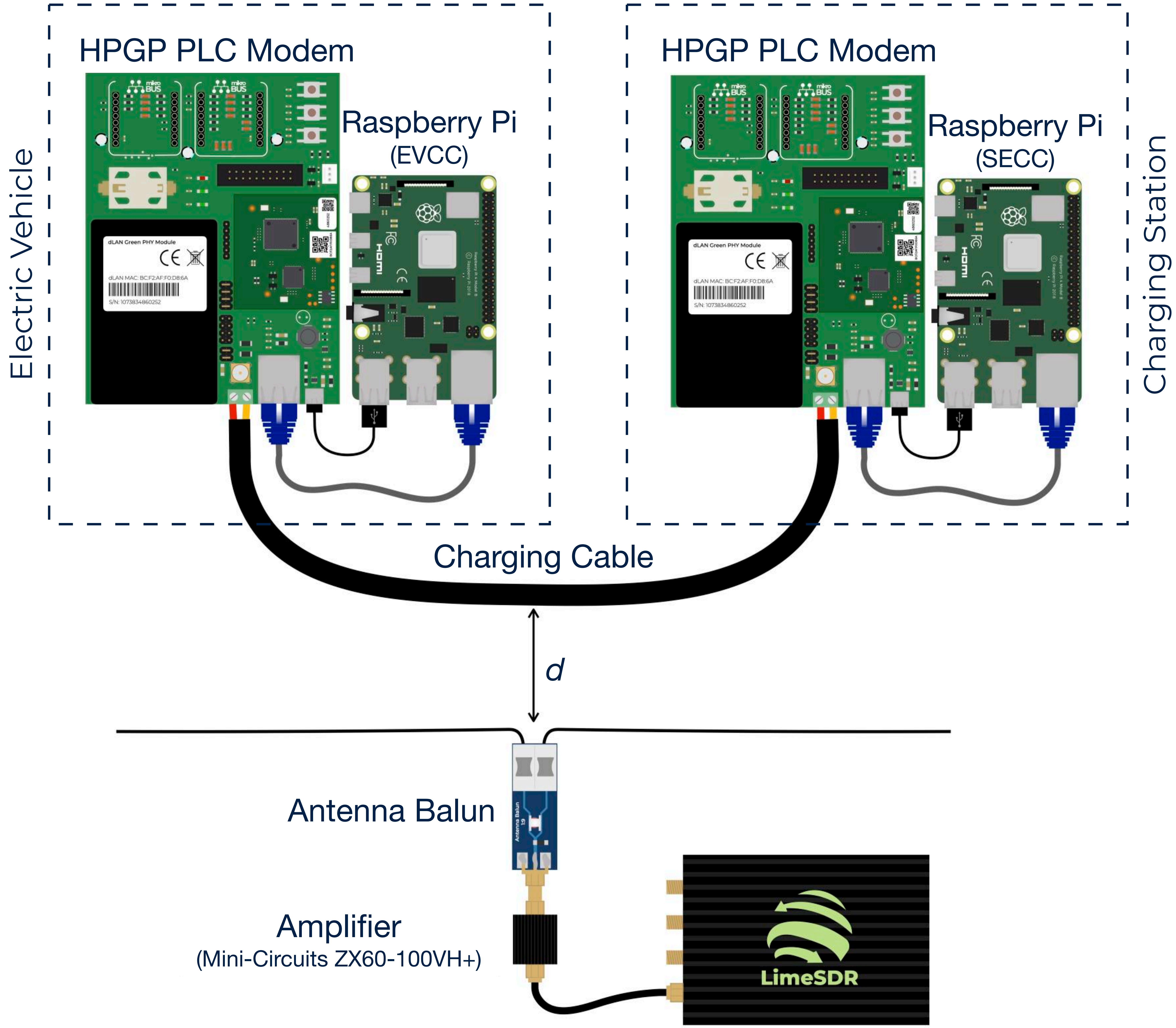
Lab Testing: Experimental Setup



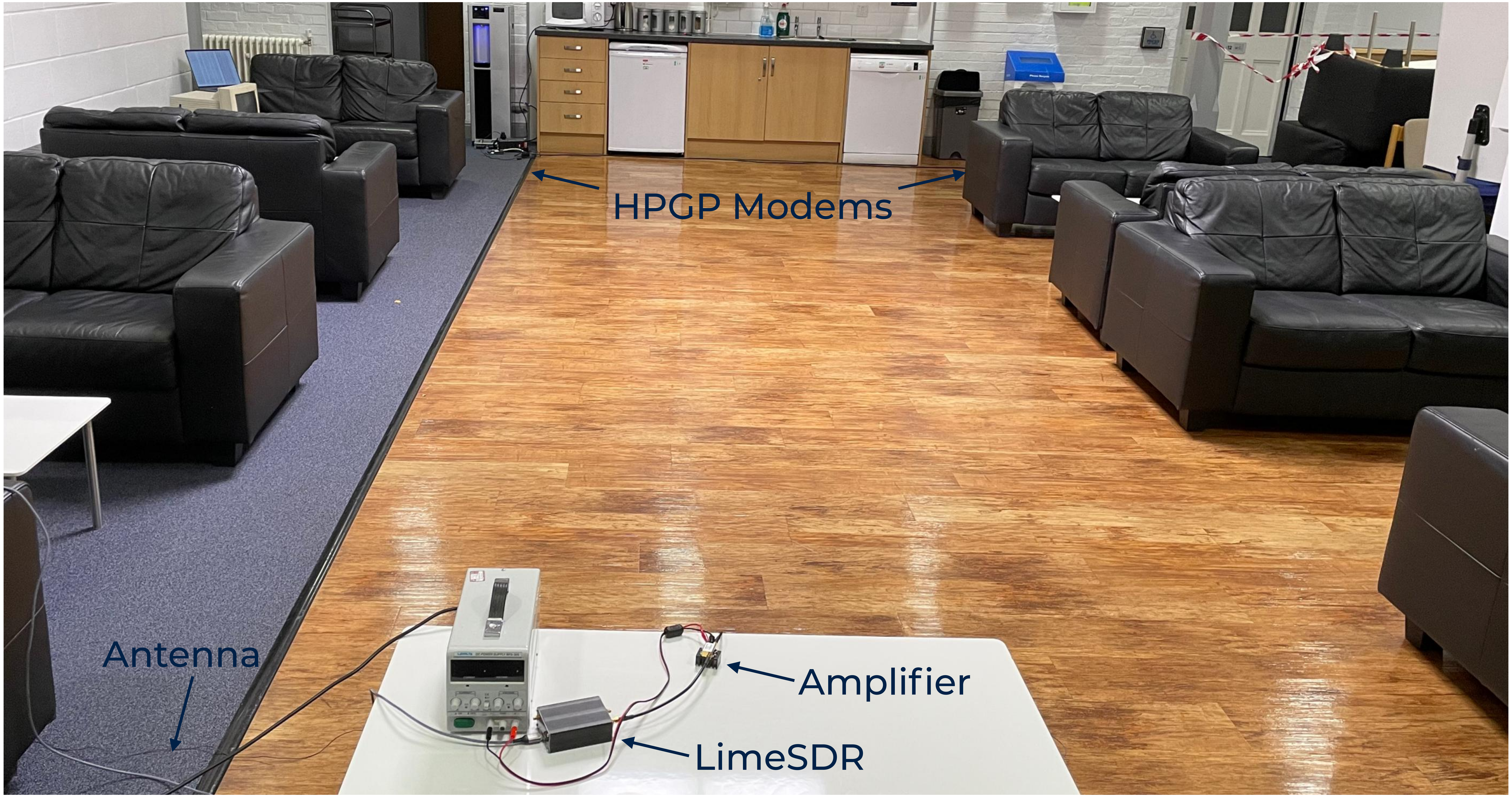
Lab Testing: Experimental Setup



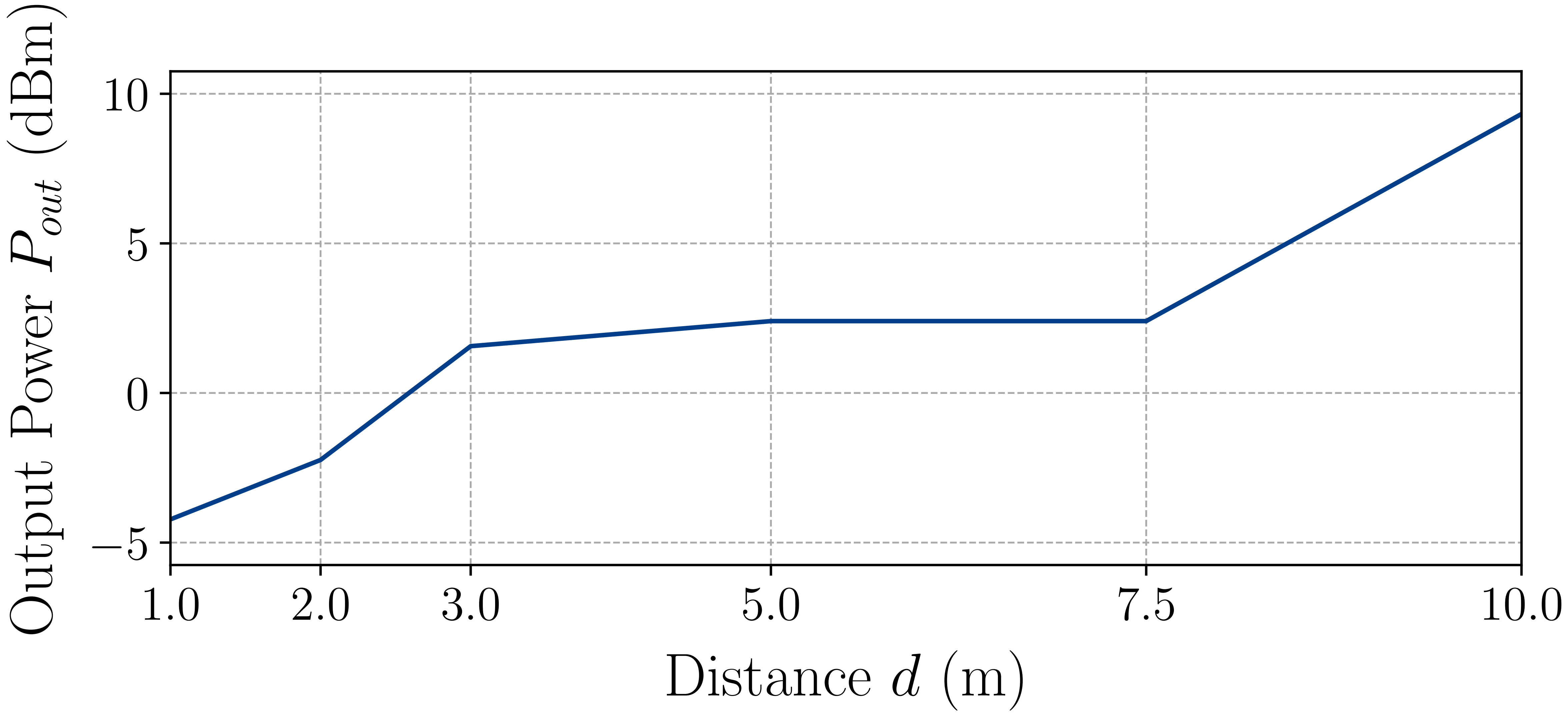
Lab Testing: Experimental Setup

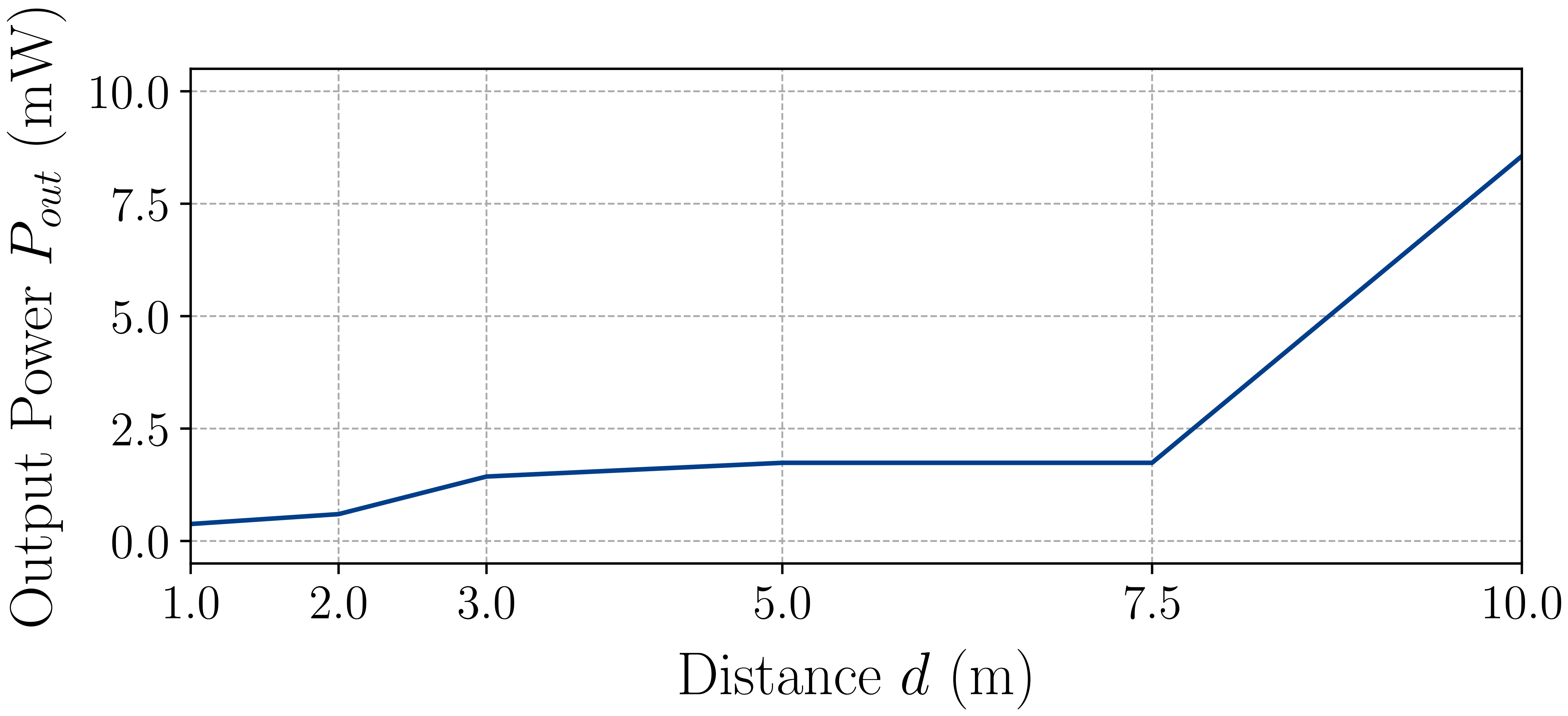


Lab Testing: Power vs. Distance

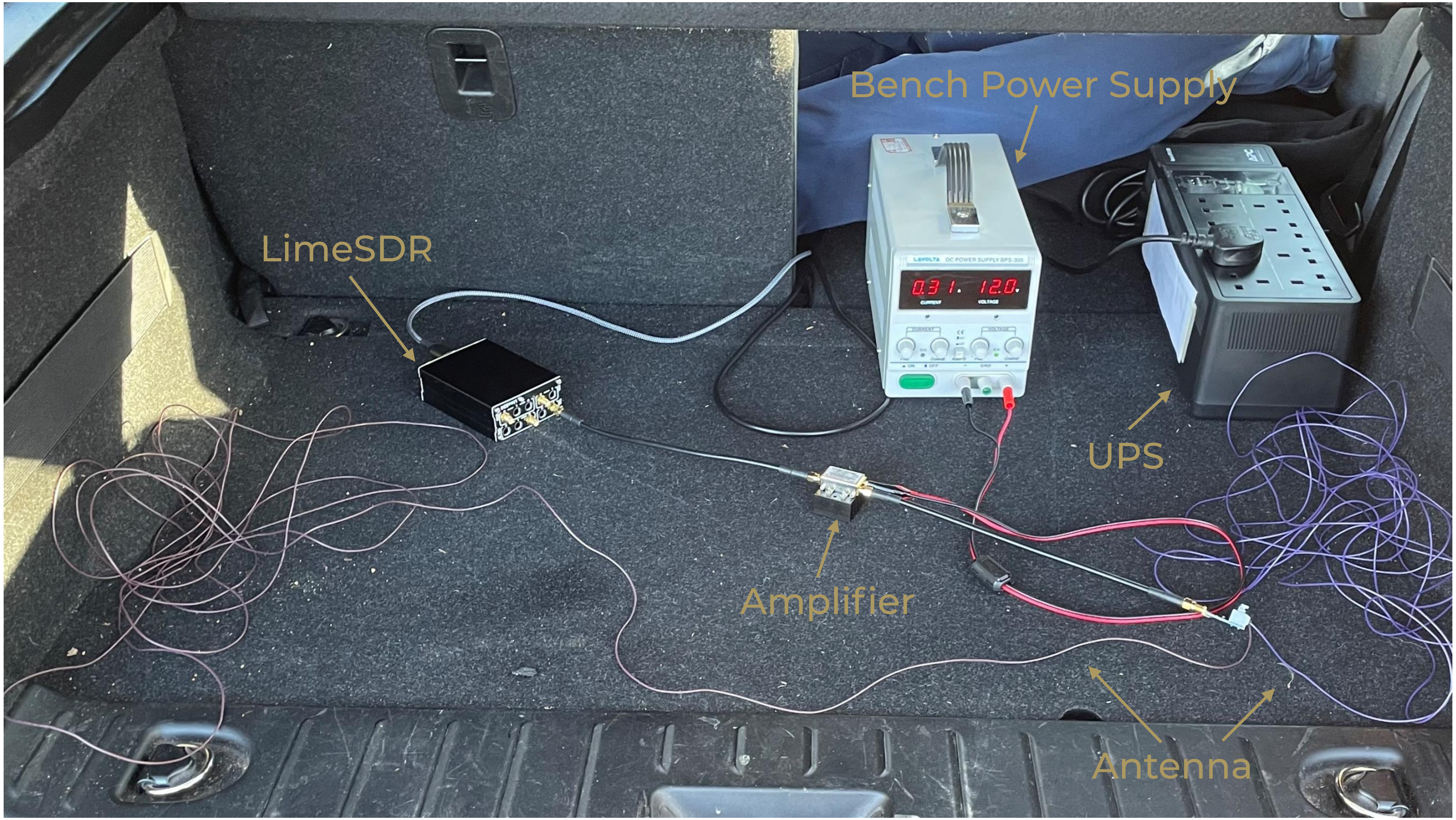


Lab Testing: Power vs. Distance

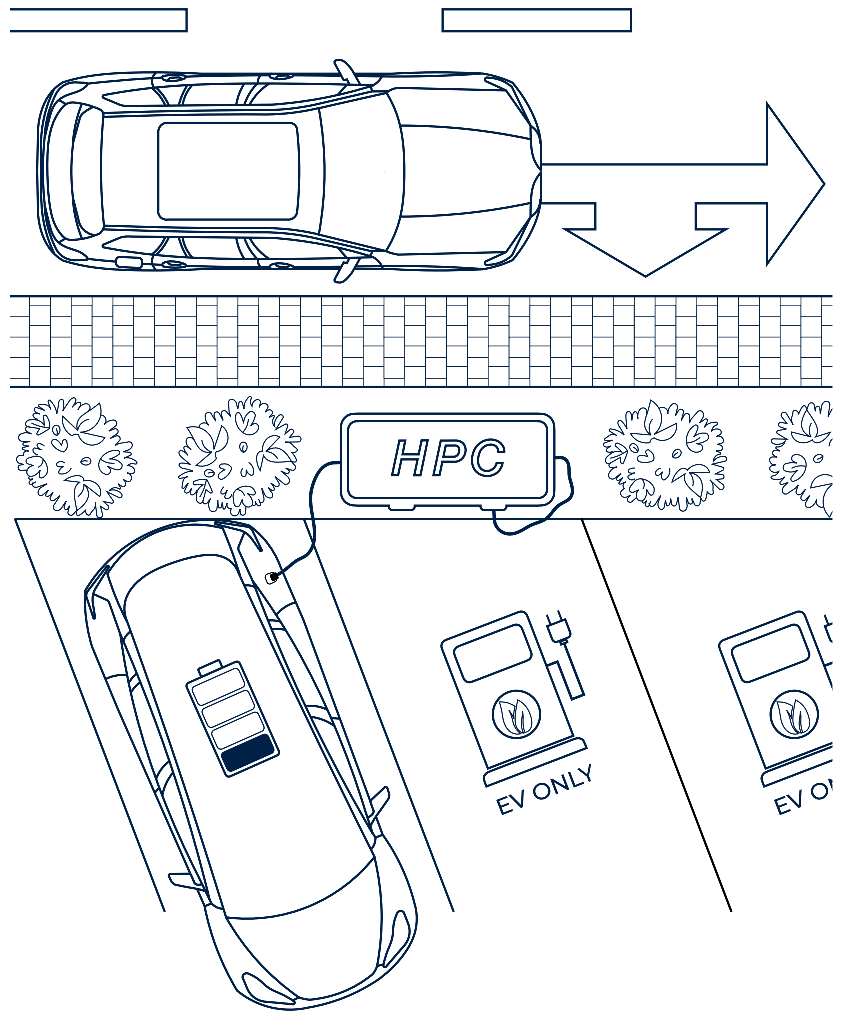




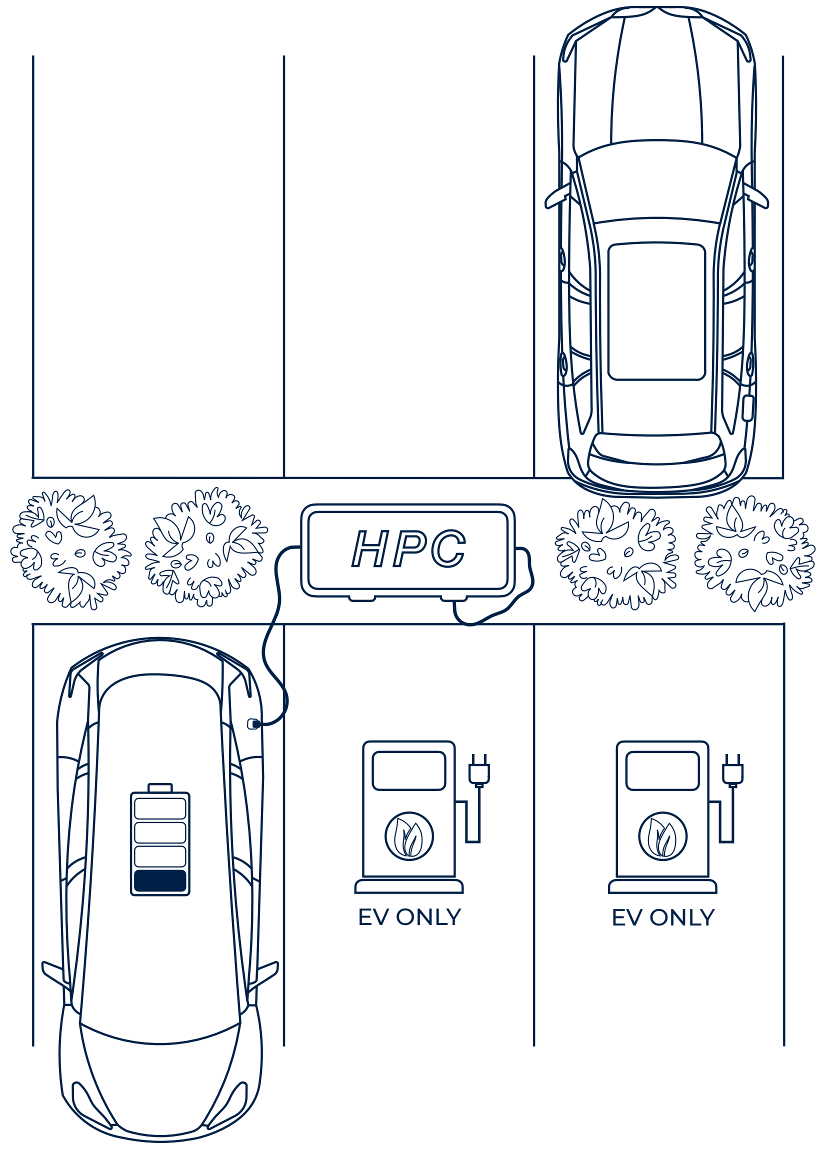
Real-World Testing: Equipment



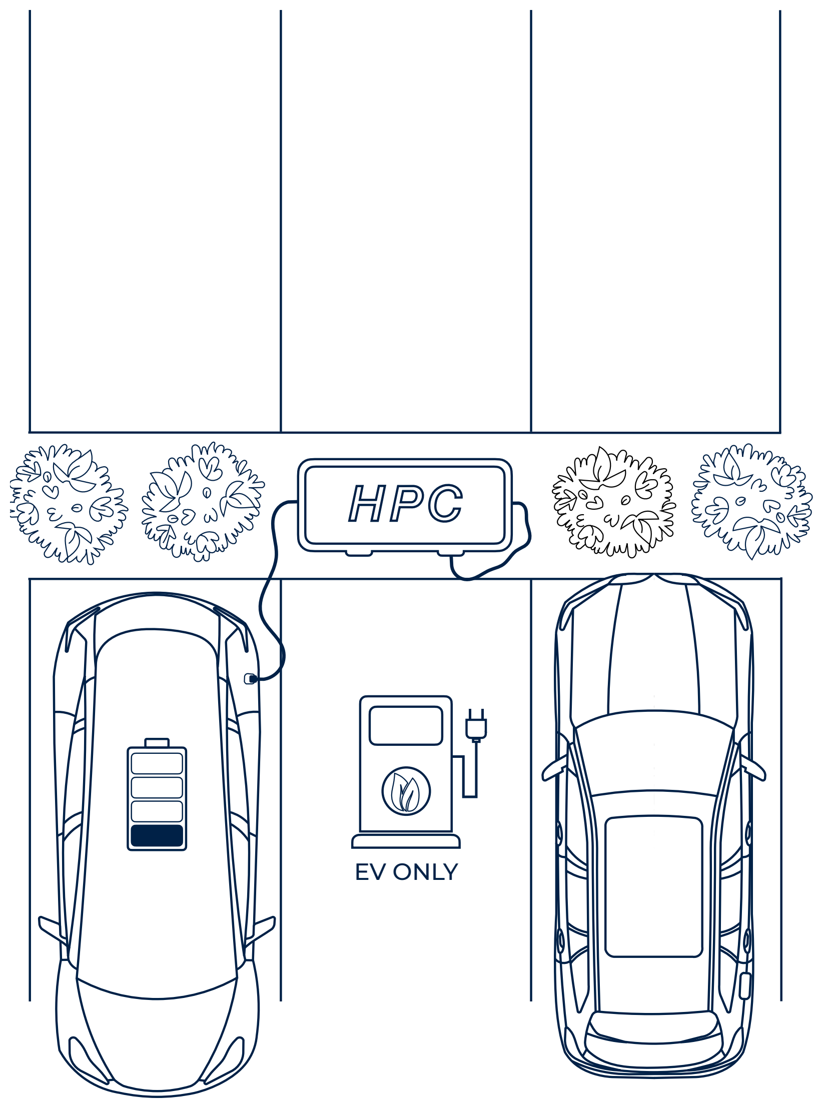
Real-World Testing



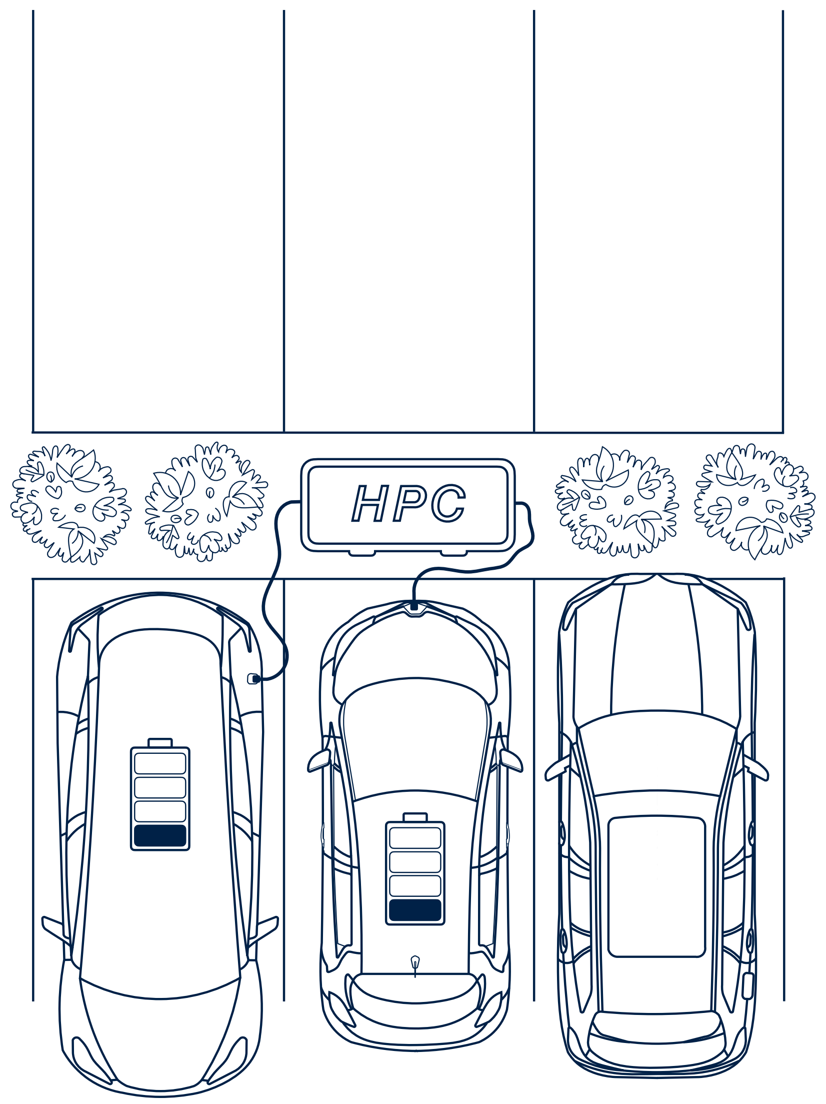
Scenario 1



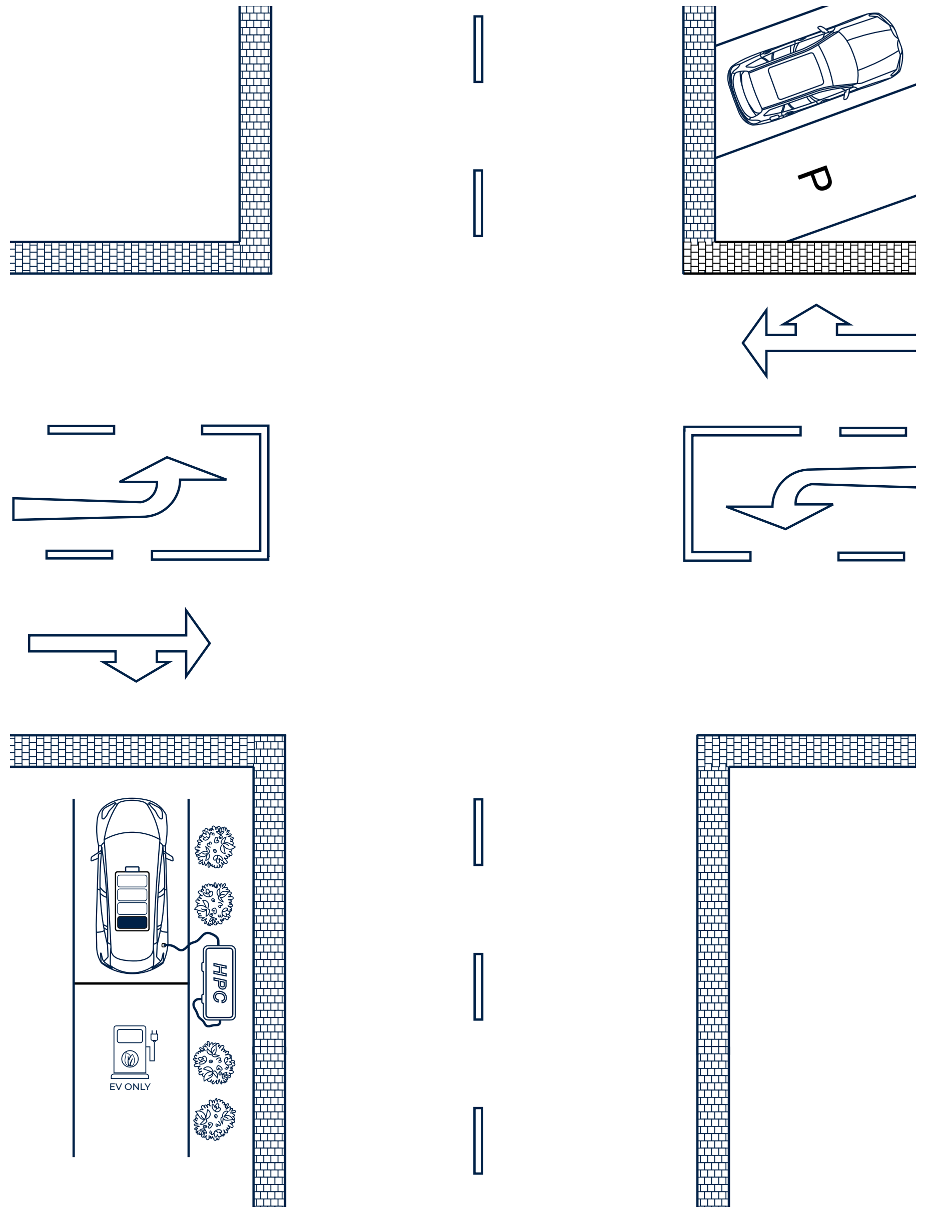
Scenario 2



Scenario 3



Scenario 4

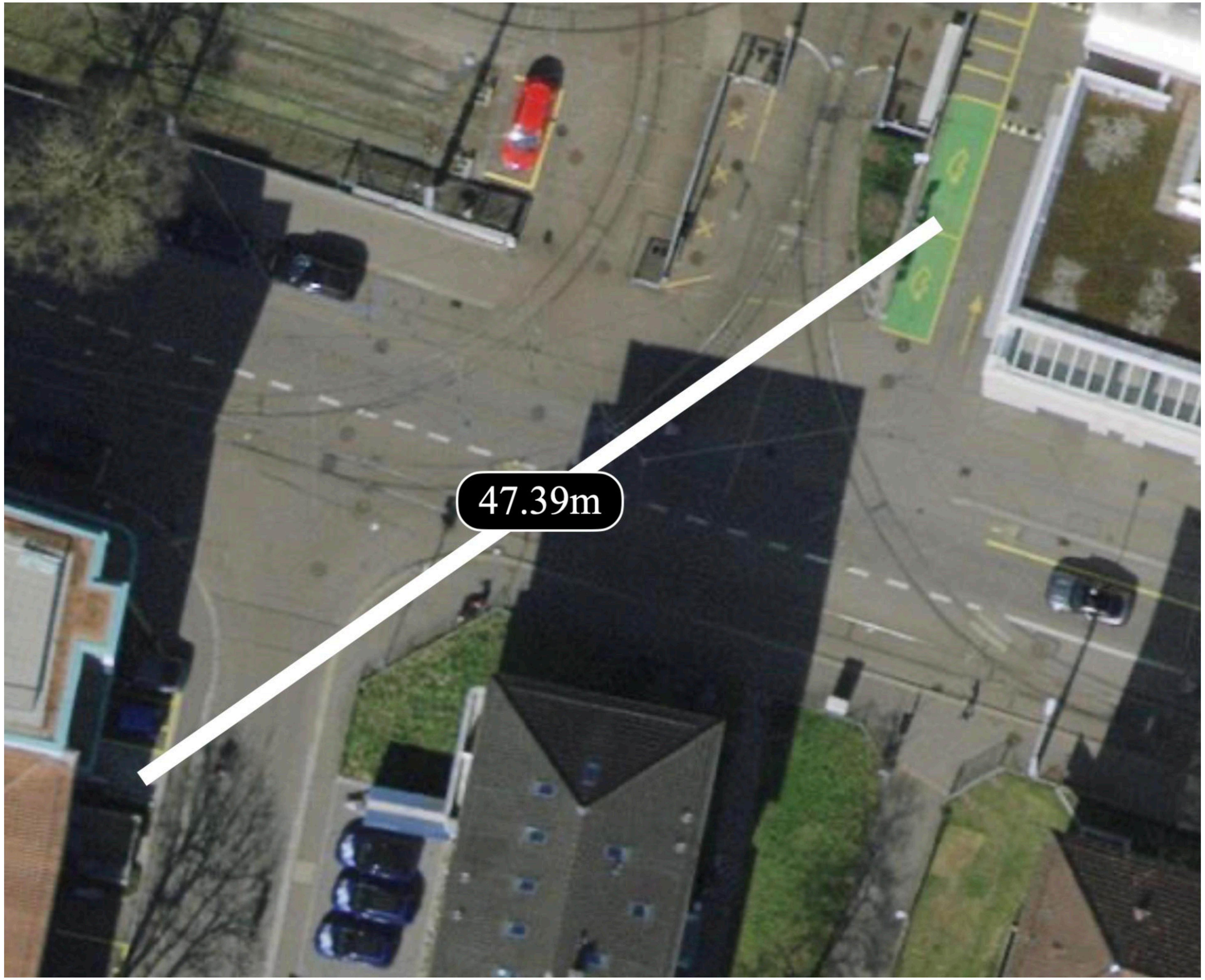


Scenario 5

Real-World Testing: Vehicle Overview

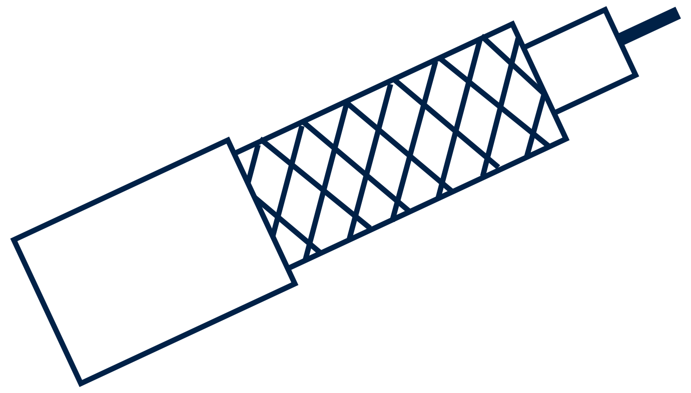
Vehicle	Class	Price ($)	Charging Capacity
A	Subcompact	50,000	50 kW
B	Compact SUV	85,000	150 kW
C	Shooting Brake	150,000	270 kW
D	Subcompact	20,000	50 kW
E	Mid-size Sedan	50,000	120 kW
F	Mid-size SUV	70,000	150 kW
G	Compact	45,000	125 kW
H	Compact	32,000	50 kW

Real-World Testing: Distance



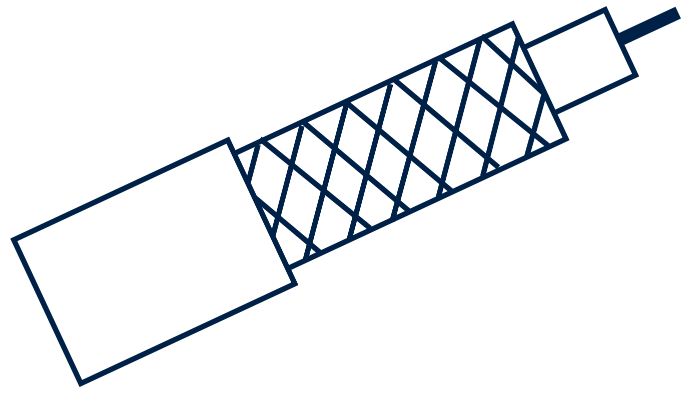
Countermeasures

Countermeasures



Shielding

Countermeasures



Shielding

Firmware Upgrade

Countermeasures

Shielding

PLC

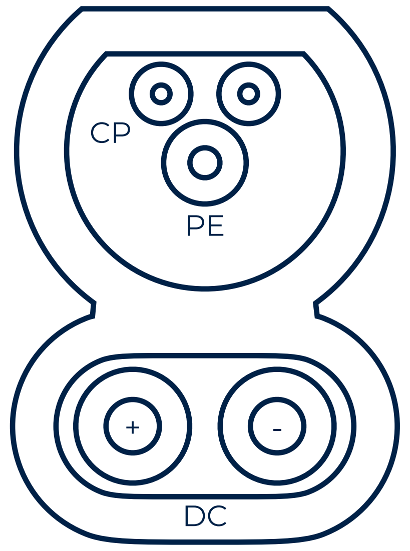
Updating…

Firmware Upgrade

Re-authentication

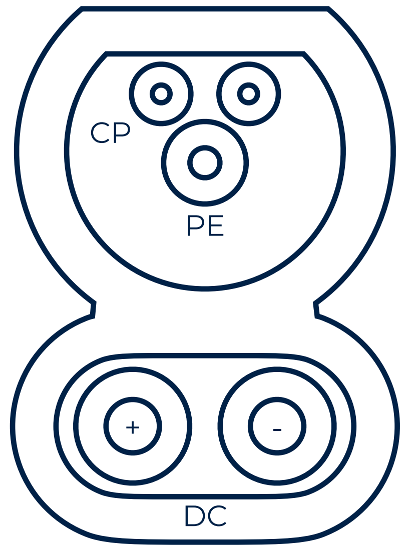
Conclusion

Conclusion



CCS is vulnerable to wireless attacks

Conclusion

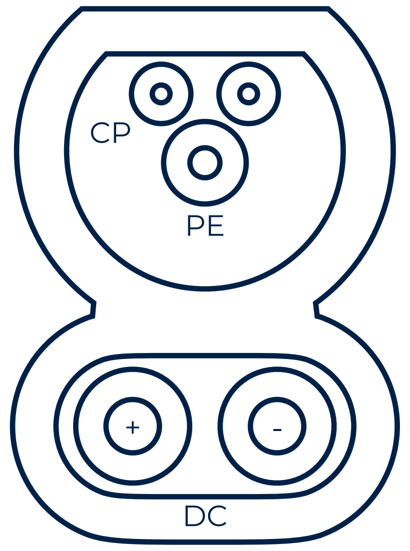


CCS is vulnerable to wireless attacks

~12M

Large number of vehicles is affected

Conclusion



CCS is vulnerable to wireless attacks

~12M

Large number of vehicles is affected

PLC is not suitable for the charging loop

Questions?

✉ info@brokenwire.fail or sebastian.kohler@cs.ox.ac.uk

https://brokenwire.fail

https://github.com/ssloxford/brokenwire

CVE https://nvd.nist.gov/vuln/detail/CVE-2022-0878