



V2GEVIL

GHOST IN THE WIRES

whoarewe

Pavel Khunt



Cyber Security Researcher

Thomas Sermpinis

@cr0wtom



Technical Director

AUXILIUM
Pentest Labs

REFERENCES

- **Talk is just summary of the research**
 - Exhaustive details are in the Pavel's Diploma Thesis
 - All resources/tools/libraries/etc described and referenced in the thesis
- **Thesis link:**
 - <https://dspace.cvut.cz/handle/10467/113764?locale-attribute=en>
 - <https://dspace.cvut.cz/bitstream/handle/10467/113764/F8-DP-2024-Khunt-Pavel-thesis.pdf?sequence=-1&isAllowed=y>

GOALS OF THIS TALK

- Analyze the state of cybersecurity in the automotive industry
- In-depth look at EV architectures and the emerging attack vector
- Exploration of communication protocols used in EV charging
- Introduction to V2GEvil
- Create a reference point for EV security research and evaluation

KAPITOLA 1

INTRODUCTION TO VEHICLE CYBER SECURITY



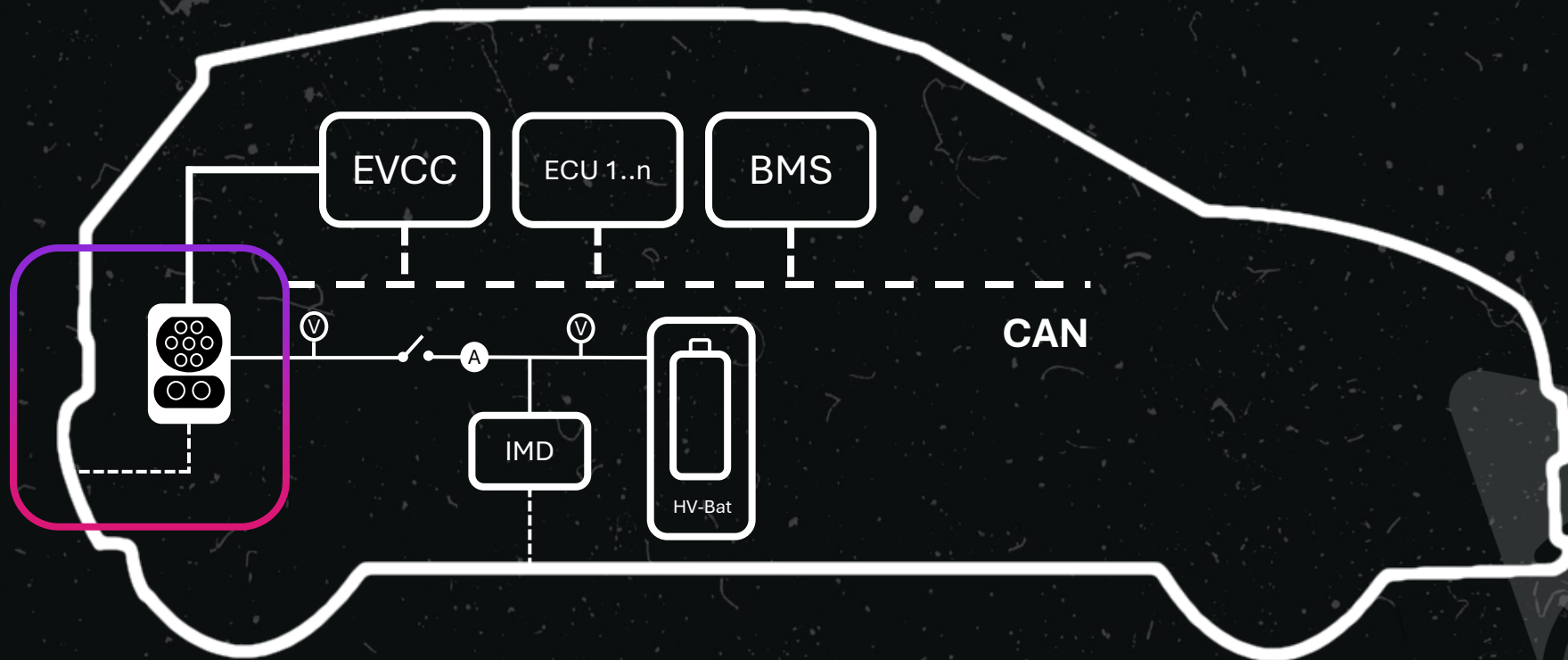
THE STATE OF AUTOMOTIVE CYBER SECURITY

- The automotive industry cannot be considered new
- The connectivity and technological aspect of it though, is not so old
- Entertainment and constant need for connectivity, are the reasons for technological advancements and integration
- Usually, 100+ year old industries, trying to catch up with young start-ups

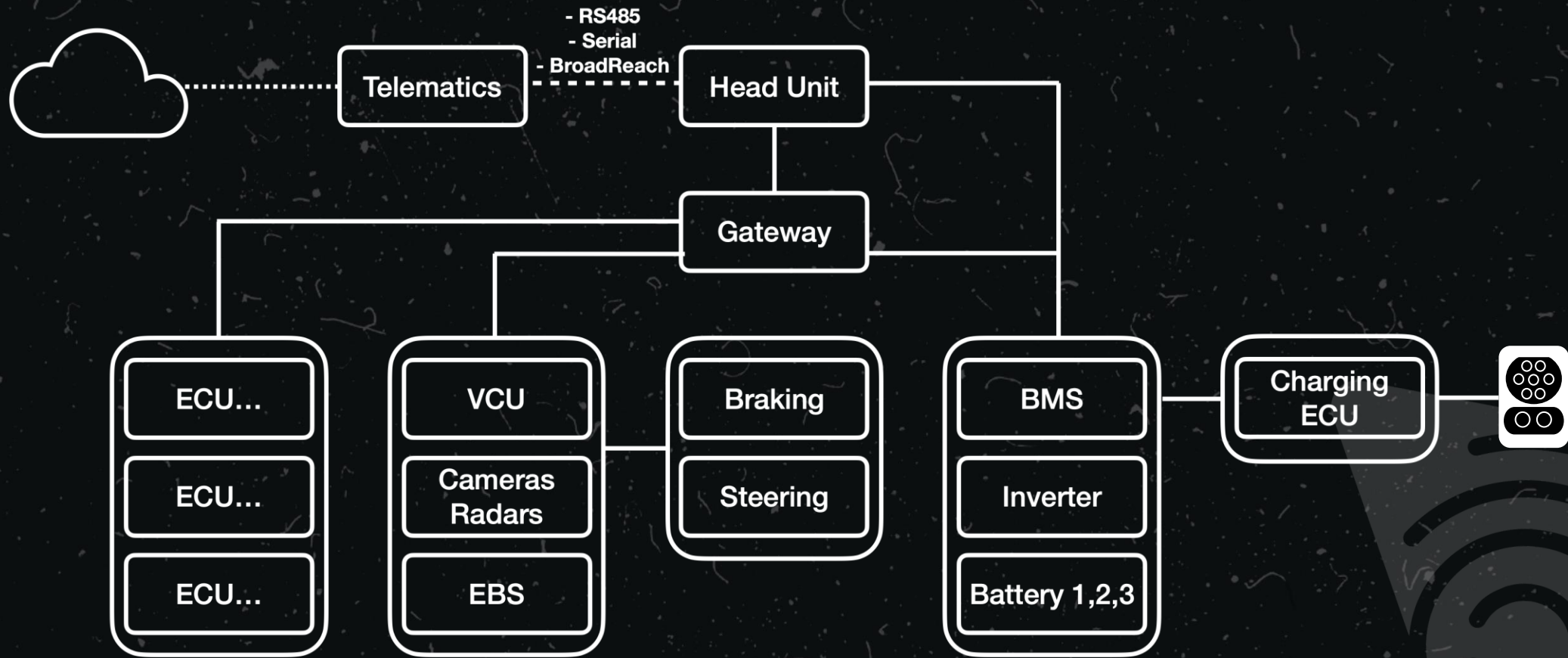
THE STATE OF AUTOMOTIVE CYBER SECURITY

- Hybrid vehicles and EVs became more popular
 - Need for direct use of renewable energy sources
 - Direct gains on speed and efficiency
 - And more...
- While early models used basic charging, last decade charging standards are applied and enforced in many ways

INTRODUCTION TO EV



INTRODUCTION TO EV



KAPITOLA 2
CHARGING



CHARGING BASICS I






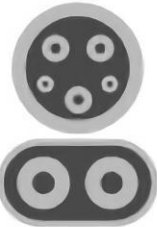

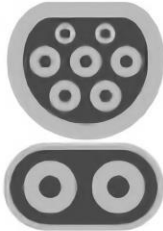
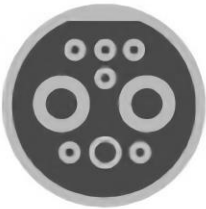
- **Charging methods**
 - **Conductive, Wireless, Battery Swap, Bidirectional**
- **Charging types**
 - **AC vs DC**
- **Charging modes**
 - **4 modes**



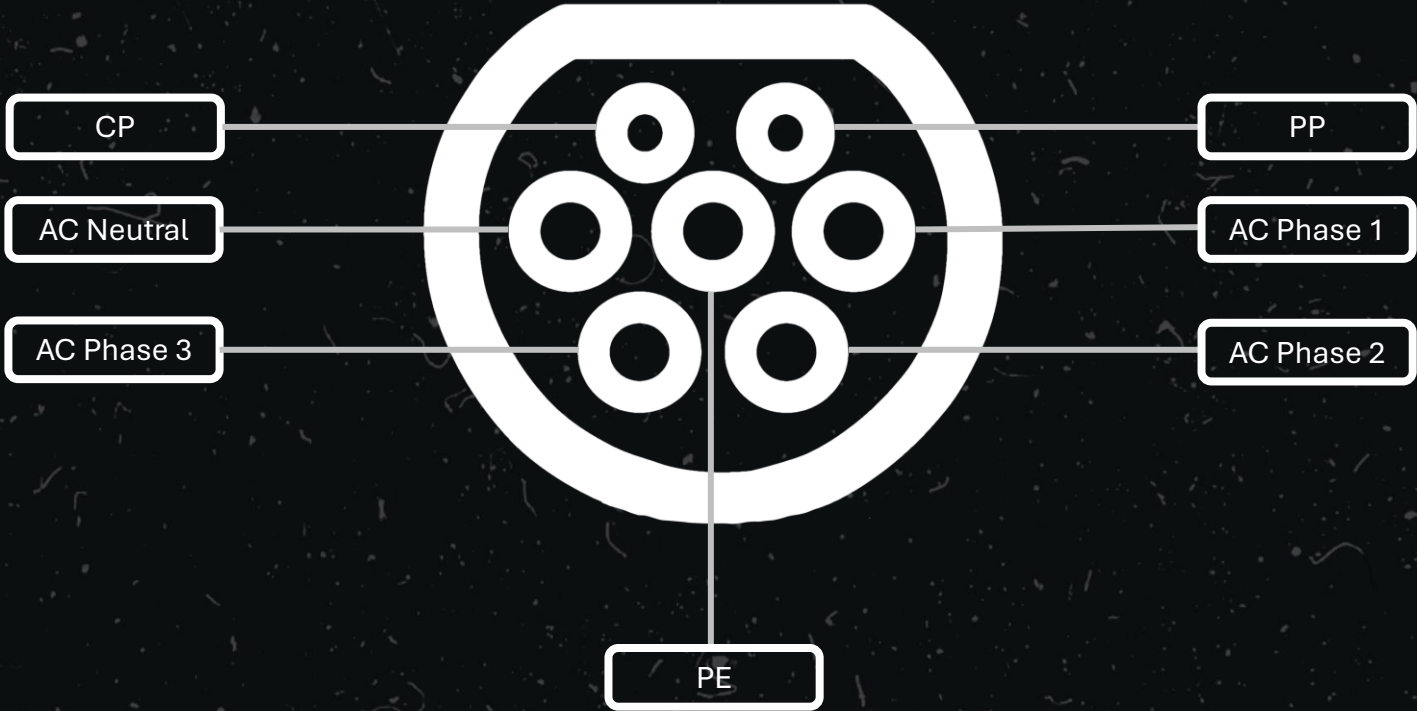
CHARGING BASICS II

- **Many different available charging standards**
 - **We are interested only in standards used in CCS (Europe)**
 - Connectors, Inlet, Plugs: IEC 62196, SAE J1772, GB/T 20234, CHAdeMO;
 - Onboard Charger, EVSE: IEC 61851, GB/T 18487, GB/T 27930;
 - Wireless Power Transfer (WPT) Systems: IEC 61980, SAE J2954;
 - Communication EV To EVSE: ISO 15118, DIN SPEC 70121, GB/T 27930, SAE J2847/2
- **Charging Combined System - CSS**
 - **Efforts towards a single unified system**
 - **Defines standards for communication, plugs, sockets and more**

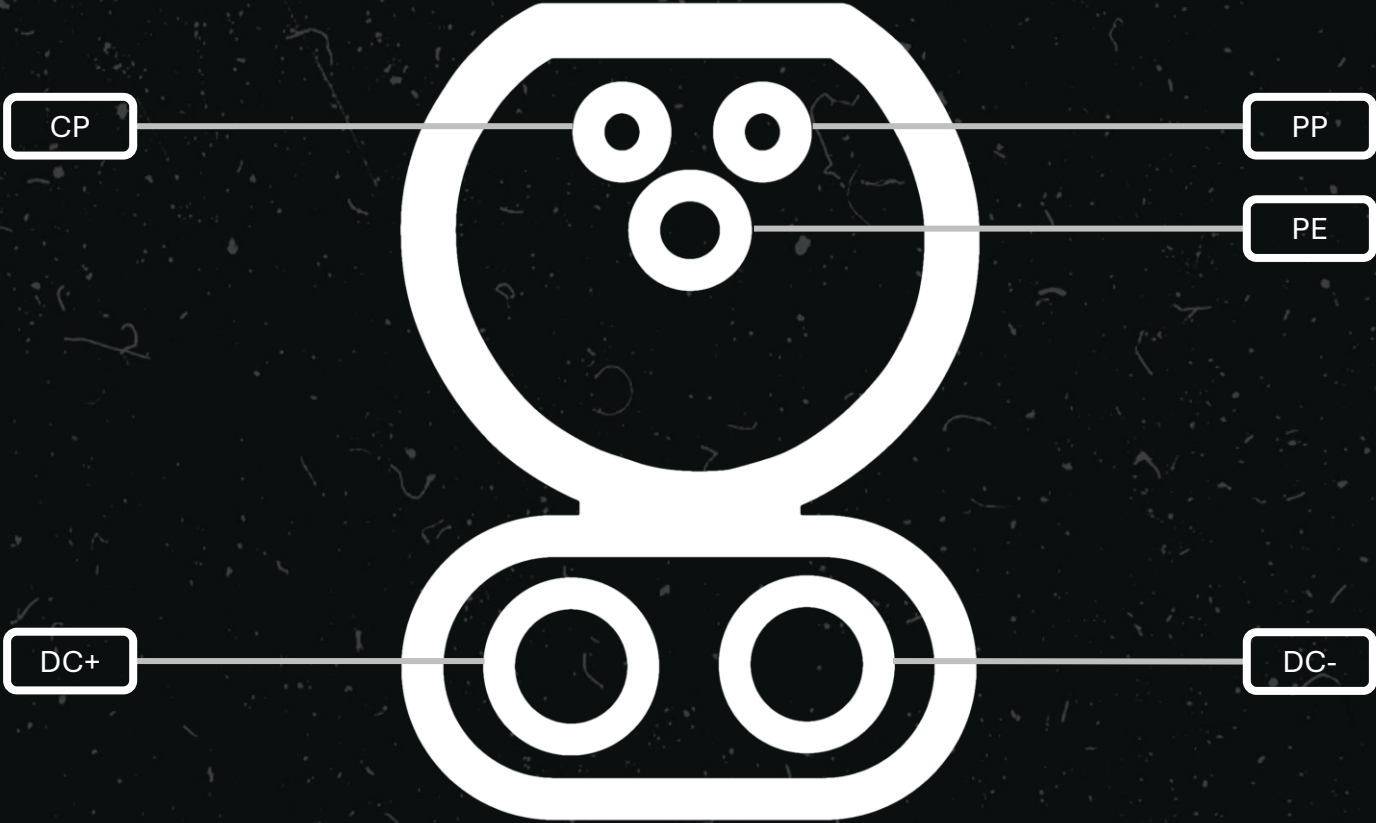
CHARGING BASICS III

	N. America	Japan	EU <i>and the rest of markets</i>	China	All Markets <i>except EU</i>
AC	 J1772 (Type 1)	 J1772 (Type 1)	 Mennekes (Type 2)	 GB/T	 Tesla
DC	 CCS1	 CHAdeMO	 CCS2	 GB/T	

CHARGING BASICS III - AC TYPE 2

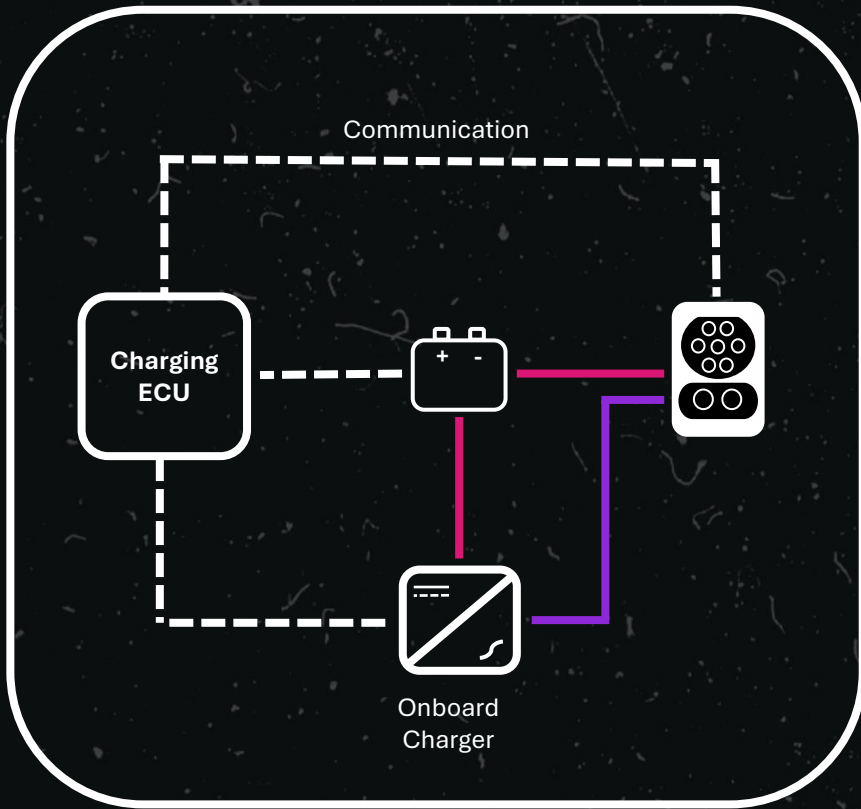


CHARGING BASICS III - CCS TYPE 2

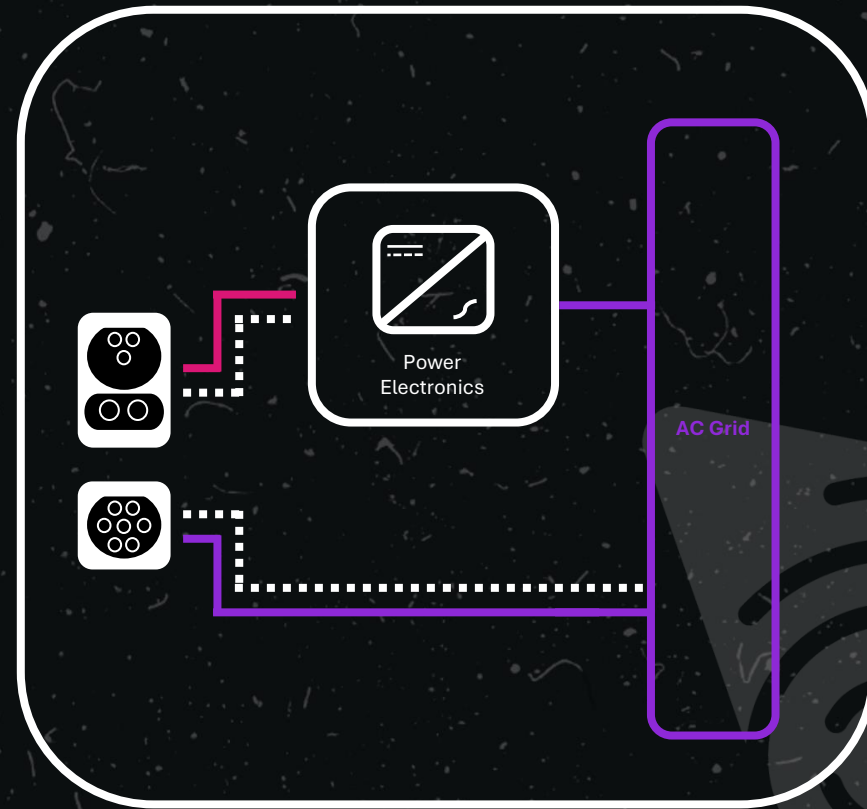


CHARGING BASICS IV

EV



EVSE



CHARGING COMMUNICATION I

- Charging is NOT only simple power transfer
- Digital data exchange
 - e.g. payment details, Required Voltage, Current, Time of charging
- Low level vs High level communication

CHARGING COMMUNICATION II



CHARGING COMMUNICATION III



KAPITOLA 3

LOW LEVEL COMMUNICATION



LOW LEVEL COMMUNICATION I

- **Basic signaling**
- **Physical signaling – Pilot function**
 - Control pilot circuit (CP and PE pins), PWM
- **Voltage differentiate State of EV**

Voltage	State	Description
+12V	State A	No coupler engagement, no EV is connected to EVSE
+9V (1kHz PWM)	State B	Coupler engagement detected (EV is connected to the EVSE), but EV not ready for charging. EVSE does not supply energy.
+6V (1kHz PWM)	State C	EV is connected and ready for charging. EVSE supplies energy.
+3V (1kHz PWM)	State D	EV is connected and ready for charging. EVSE supplies energy. Ventilation is required.
0V	State E	Short of CP to PE on the EVSE, no power supply.
-12V	State F	Charging station is not available.

LOW LEVEL COMMUNICATION II

- Based on duty cycle
 - Info about current
 - Force High level communication
- IEC 61851

Duty Cycle	Description
Duty cycle > 97%	Charging is not allowed.
96% < duty cycle 97%	Maximum current consumption for AC charging is 80 A.
85% < duty cycle 96%	Available current = (duty cycle - 64) * 2A.
10% duty cycle 85%	Available current = duty cycle * 0.6A.
8% duty cycle < 10%	Maximum current consumption for AC charging is 6 A.
7% < duty cycle < 8%	Charging is not allowed.
3% duty cycle 7%	Force use of high-level communication protocol (ISO 15118 or DIN 70121). If pilot function wire is used for digital communication, then the duty cycle 5 % shall be used.
Duty cycle < 3%	Charging is not allowed.

LOW LEVEL COMMUNICATION III



Low Level
Comm.



High Level
Comm.



KAPITOLA 4

HIGH LEVEL COMMUNICATION



HIGH LEVEL COMMUNICATION I

- **Why do we need that?**
 - **Optimized Charging**
 - **Thermal Management**
 - **Precise Communication for Optimal Charging**
 - **Fault Detection and Safety Mechanisms**
 - **Interoperability**
 - **Enhanced User Experience**
 - **Future-Proofing the EV Ecosystem**



HIGH LEVEL COMMUNICATION II

- Prerequisite: low-level comm. defined in IEC 61851
- Charging modes 3 and 4
- Communication between EVCC and SECC
- Protocols for high level communication are defined in ISO 15118

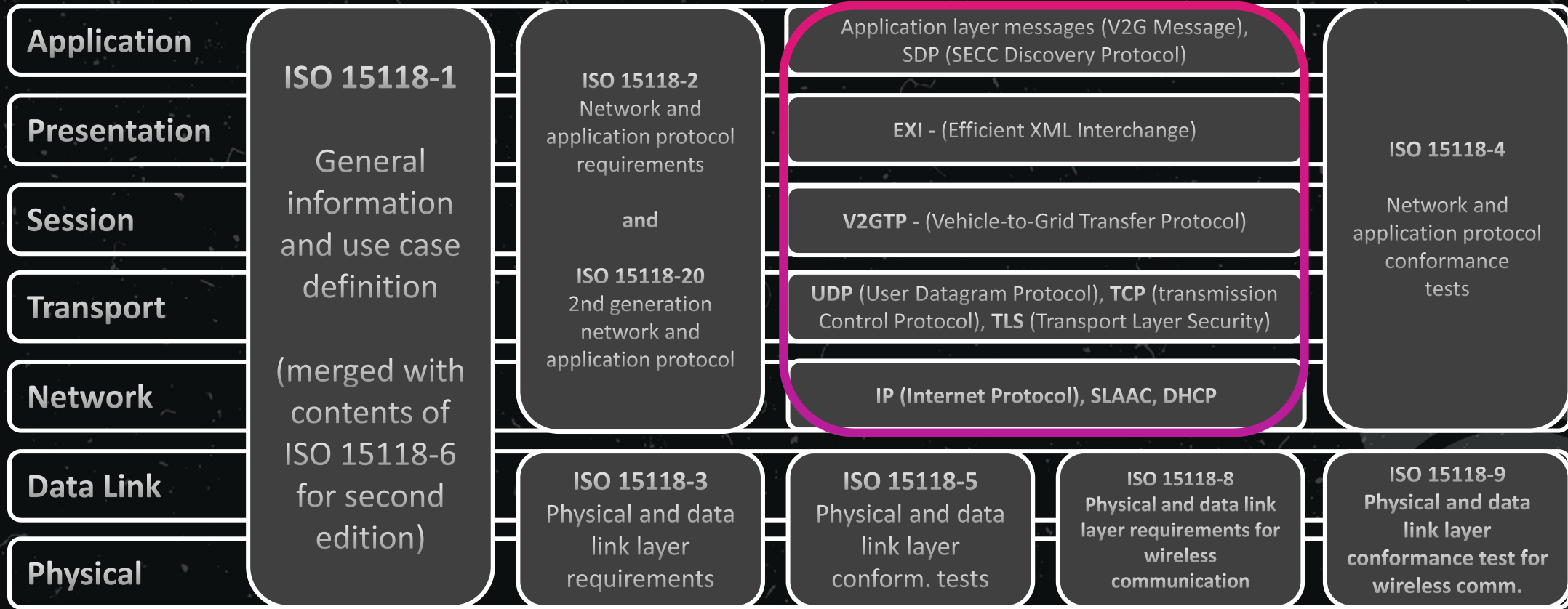
ISO 15118 I

- Vehicle-to-Grid Communication Interface = V2G
- PLC - Control Pilot circuit (CP and PE)
- Signal Level Attenuation Characterization (SLAC)
- Digital communication
 - Provides enhancements:
 - *Identification, payment, load levelling, energy transfer control, charging parameters*

ISO 15118 VS IEC 61851

Application	Application layer messages (V2G message) SDP (SECC Discovery Proto.)	Application layer messages (V2G Message) SDP (SECC Discovery Protocol)	ISO 15118-4 Network and application protocol conformance tests
Presentation	EXI	EXI - (Efficient XML Interchange)	
Session	V2GTP	V2GTP - (Vehicle-to-Grid Transfer Protocol)	
Transport	UDP, TCP, TLS	UDP (User Datagram Protocol), TCP (Transmission Control Protocol), TLS (Transport Layer Security)	
Network	IP	IP (Internet Protocol), SLAAC, DHCP	
Data Link	HomePlug GreenPHY	ISO 15118-5 Physical and data link layer requirements for	
Physical		ISO 15118-8 Physical and data link layer requirements for	ISO 15118-9 Physical and data link layer
		PWM	Resistive Signaling

ISO 15118 II



ISO 15118 III



V2G COMM. FLOW

IEC 61851

ISO 15118

State A

State B

State C

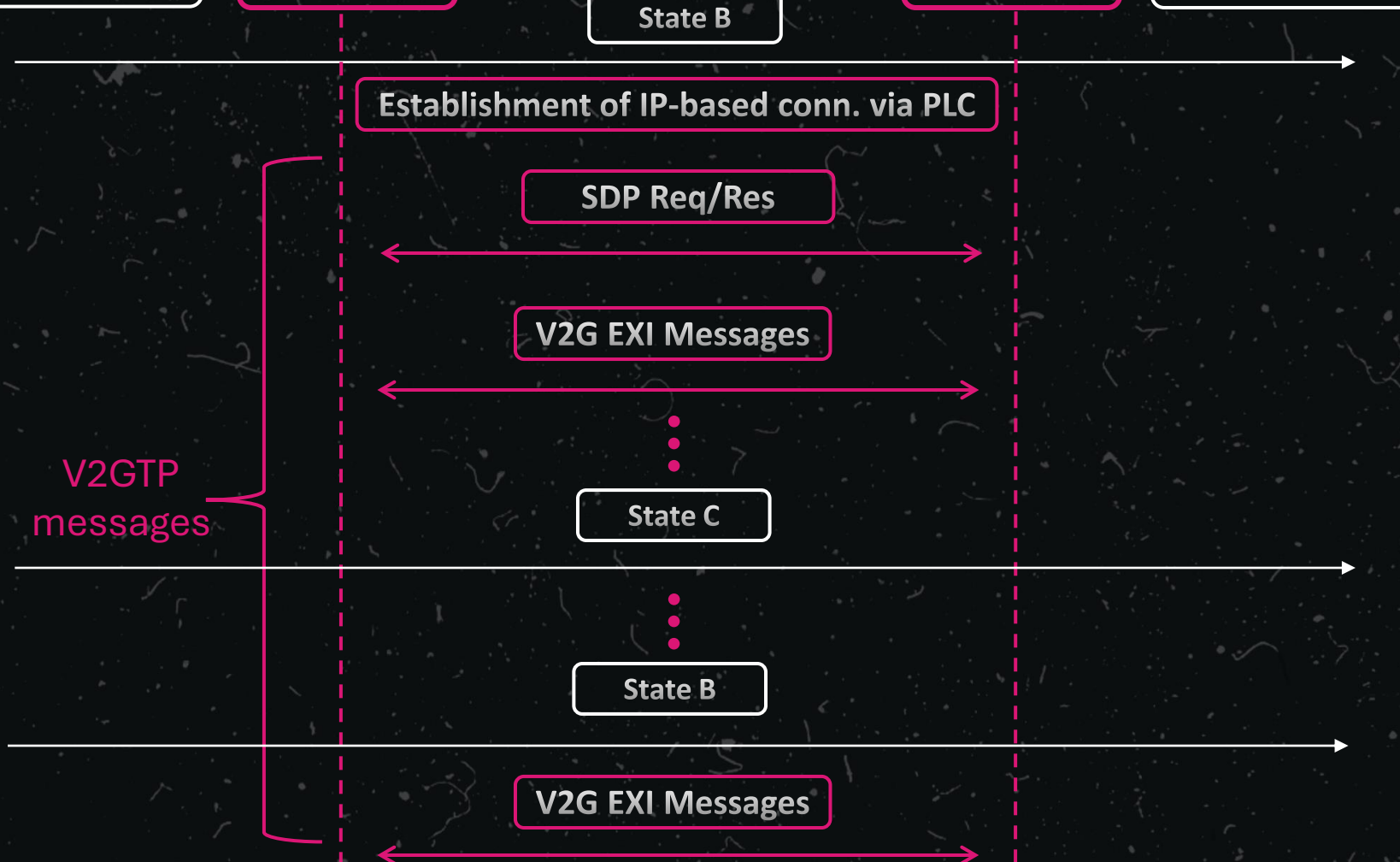
State B

EV controller – Low level

EVCC

SECC

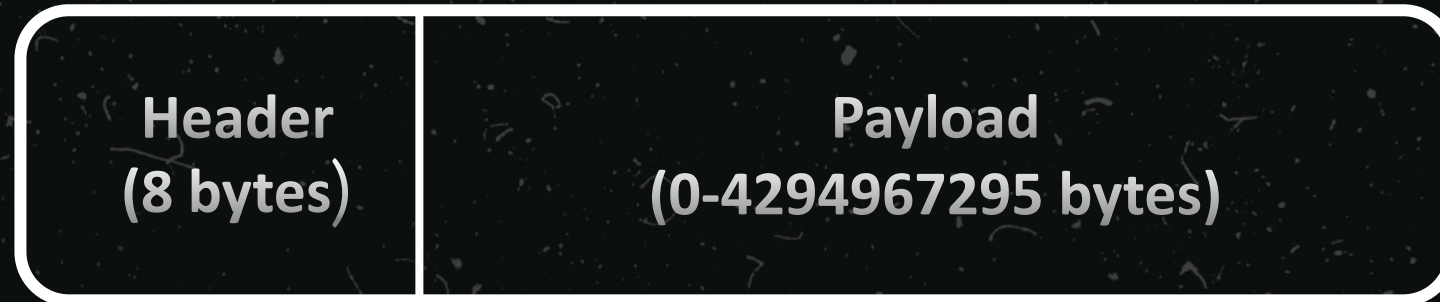
EVSE controller – Low level



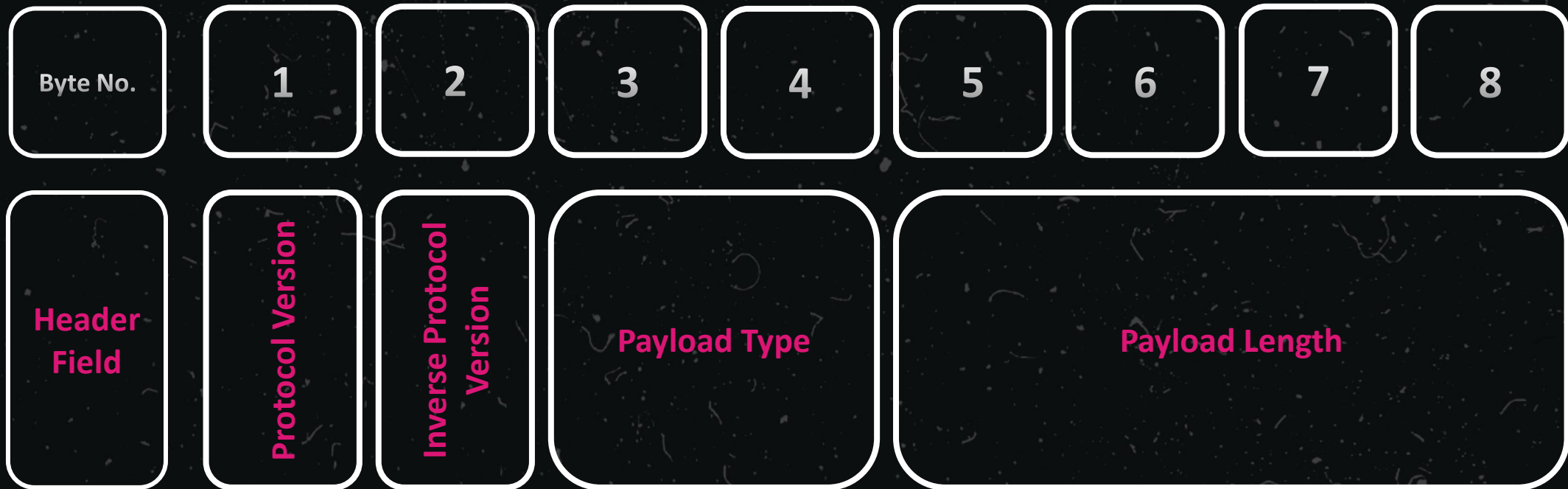
V2G GTP messages

Duty cycle 5%

V2GTP MESSAGE - PDU



V2GTP MESSAGE - HEADER



V2G PDU PAYLOAD TYPES

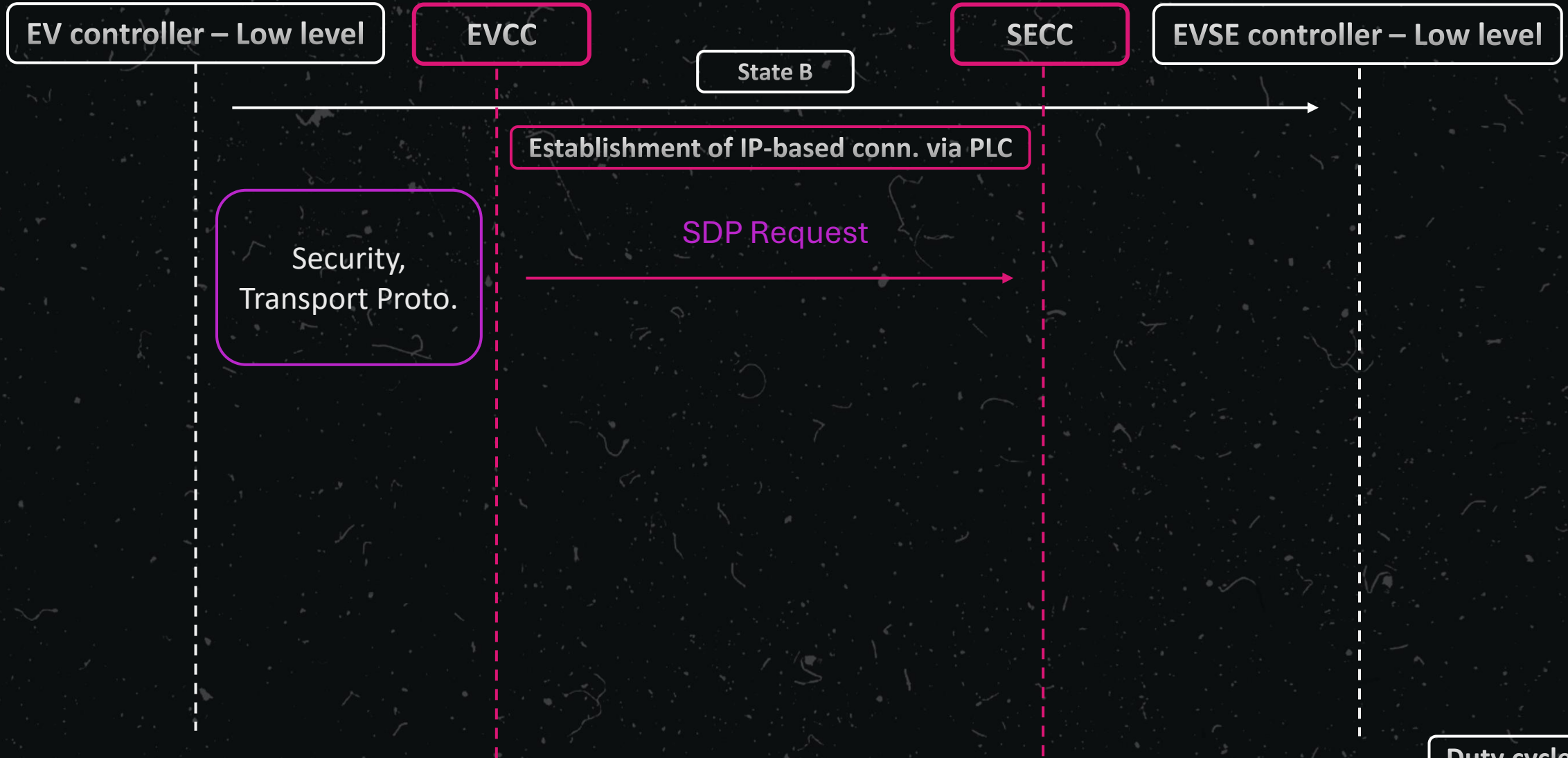
- SDP request message – 0x9000
- SDP response message – 0x9001
- EXI encoded V2G Message – 0x8001
- Manufacturer specific use – 0xA000 - 0xFFFF



V2G COMM. FLOW - SDP

IEC 61851

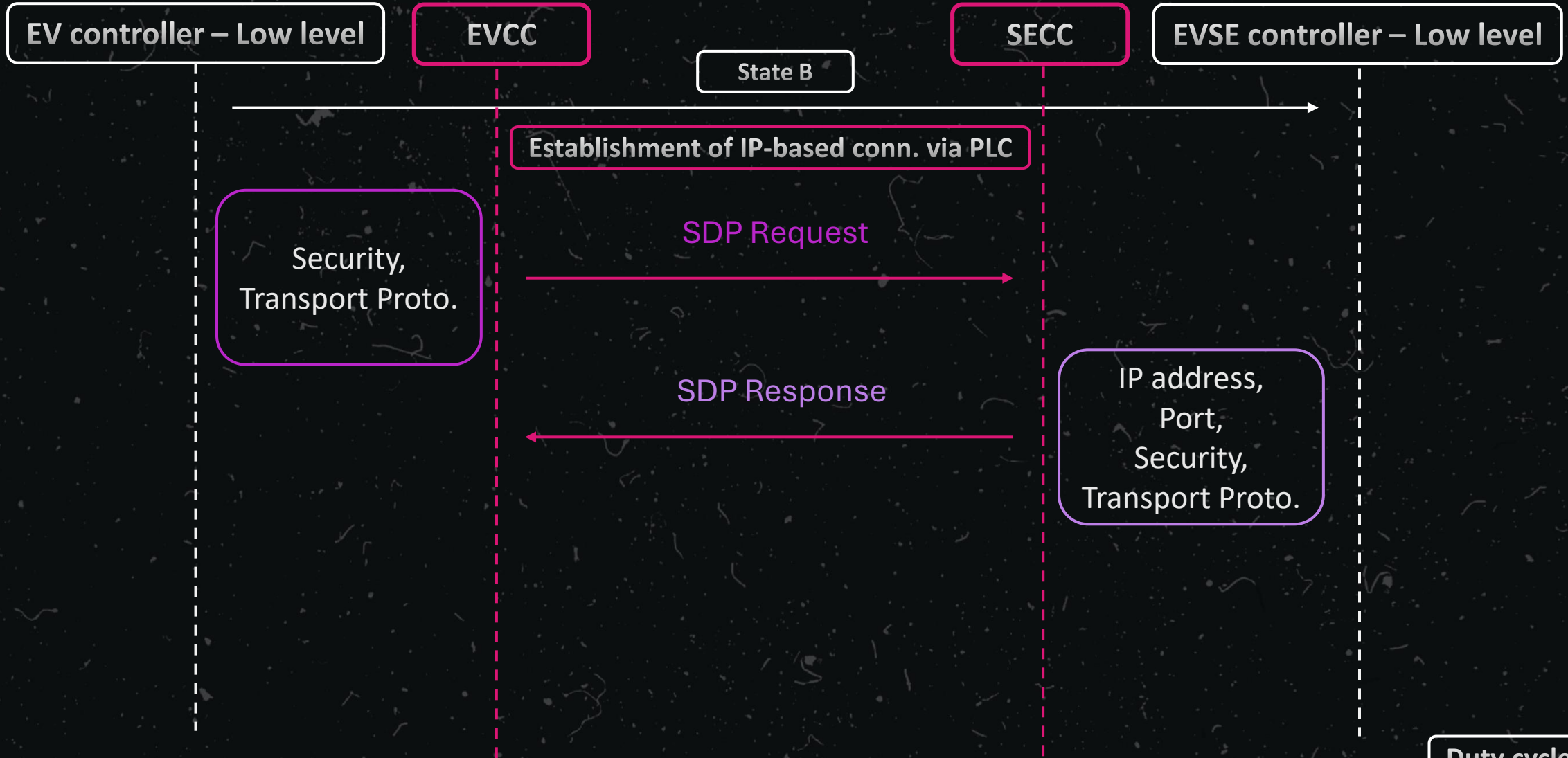
ISO 15118



V2G COMM. FLOW - SDP

IEC 61851

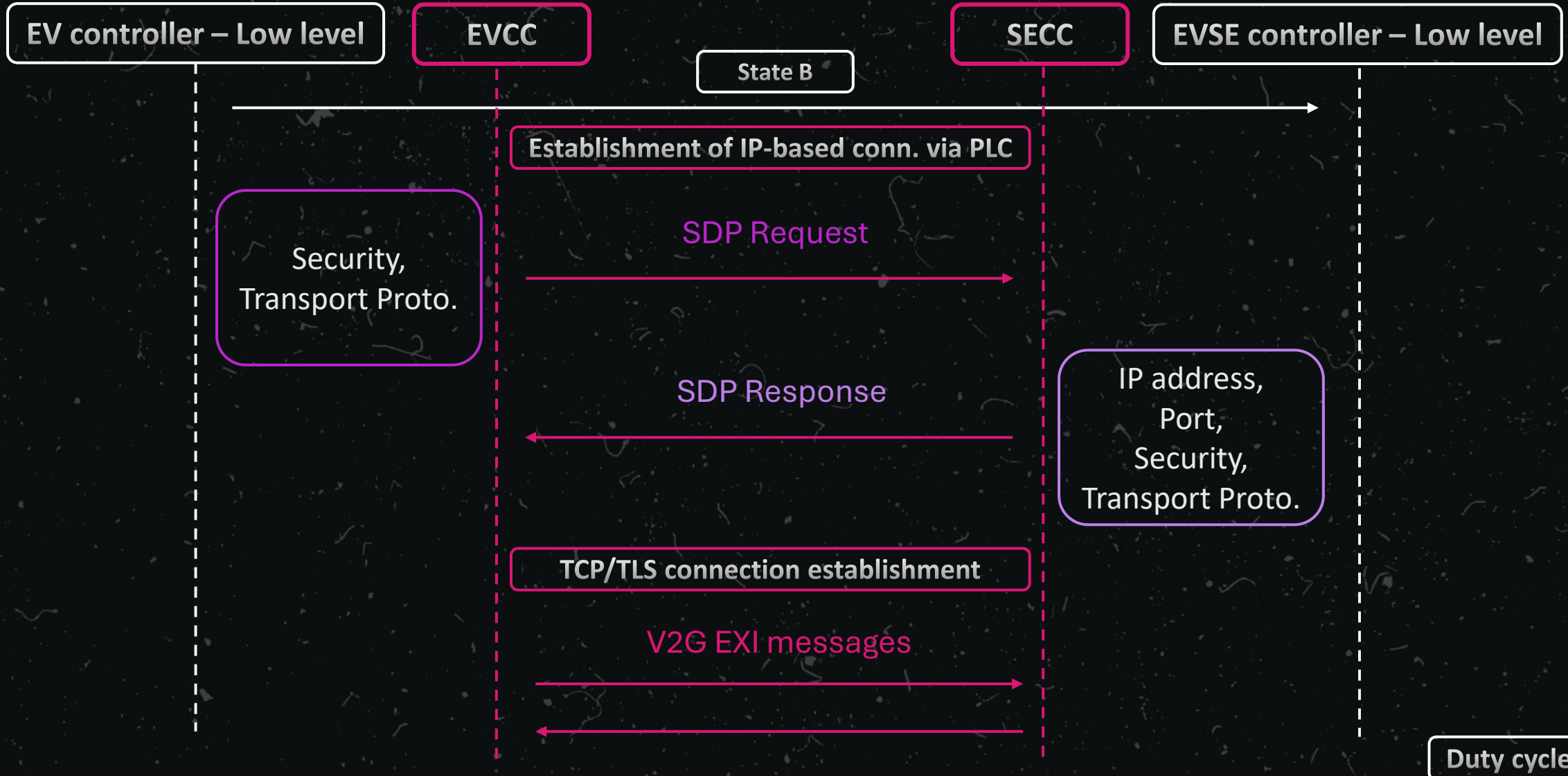
ISO 15118



V2G COMM. FLOW - SDP

IEC 61851

ISO 15118



EXI ENCODED V2G MESSAGE

Header

Payload

0x01

0xfe

0x8001

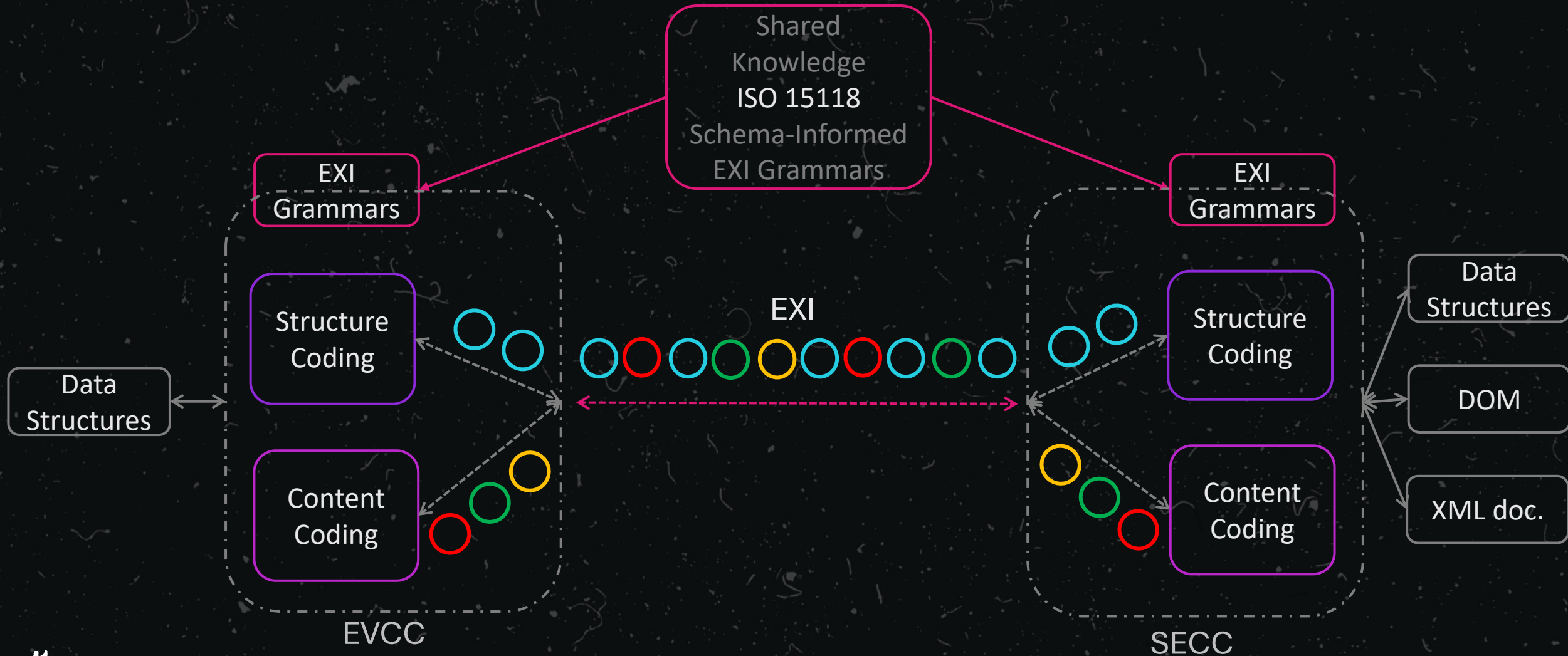
0x00000014

EXI encoded V2G message

V2G application layer protocol handshake messages

V2G application layer messages

EXI ENCODED V2G MESSAGE CONCEPT



EXI ENCODED V2G MESSAGE EXAMPLE

Plain XML representation of a SessionSetupRes

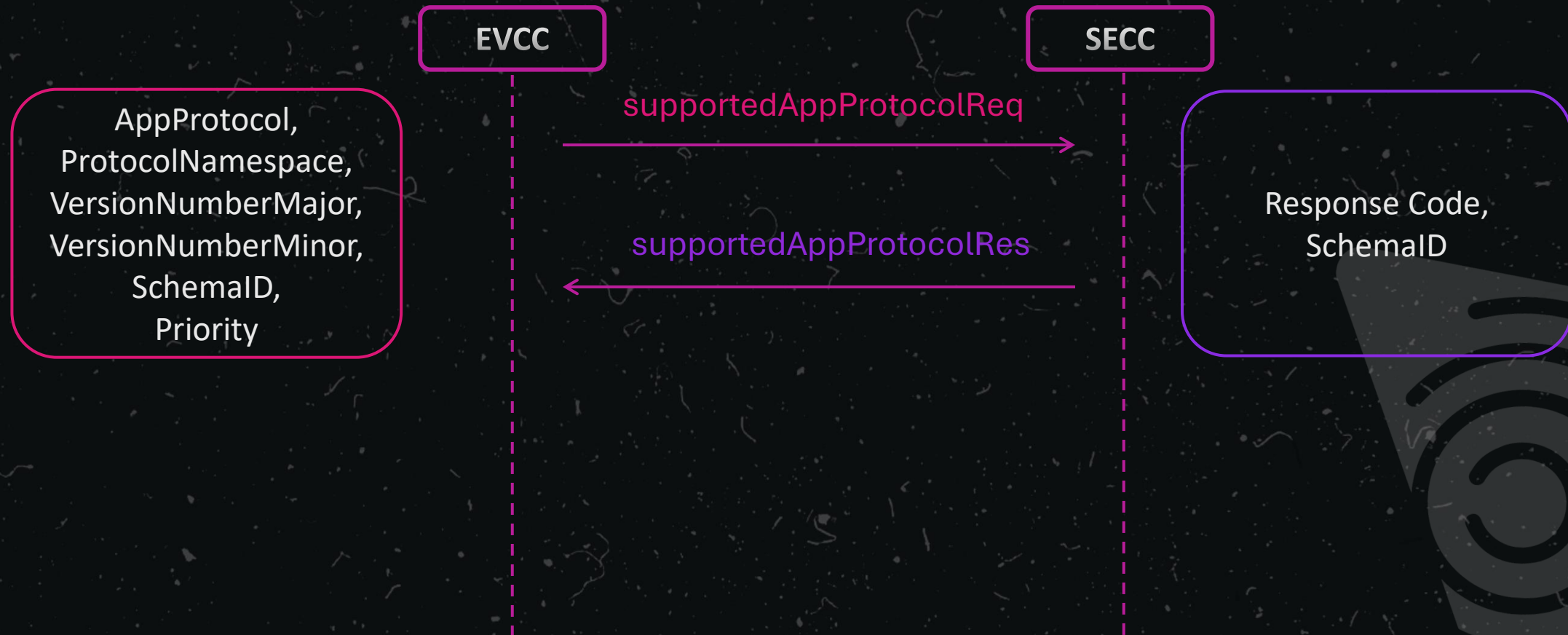
```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <v2gci_d:V2G_Message xmlns:v2gci_h="urn:iso:15118:2:2013:MsgHeader"
3   xmlns:v2gci_d="urn:iso:15118:2:2013:MsgDef"
4   xmlns:v2gci_t="urn:iso:15118:2:2013:MsgDataTypes"
5   xmlns:xmldsig="http://www.w3.org/2000/09/xmldsig#"
6   xmlns:v2gci_b="urn:iso:15118:2:2013:MsgBody"
7   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
8   <v2gci_d:Header>
9     <v2gci_h:SessionID>3031323334353637</v2gci_h:SessionID>
10  </v2gci_d:Header>
11  <v2gci_d:Body>
12    <v2gci_b:SessionSetupRes>
13      <v2gci_b:ResponseCode>OK</v2gci_b:ResponseCode>
14      <v2gci_b:EVSEID>FRA23E45B78C</v2gci_b:EVSEID>
15    </v2gci_b:SessionSetupRes>
16  </v2gci_d:Body>
17 </v2gci_d:V2G_Message>
```

EXI data stream representation of the SessionSetupRes

80 98 02 0C 0C 4C 8C CD 0D 4D 8D D1 E0 00 39 19 49 04 C8 CD 14 D0 D5 08 DC E1 0C 80

V2G APPLICATION LAYER PROTOCOL HANDSHAKE

- Application layer protocol negotiation between EVCC and SECC



V2G APPLICATION LAYER PROTOCOL HANDSHAKE

```
<?xml version="1.0" encoding="UTF-8"?>
<n1:supportedAppProtocolReq
  xsi:schemaLocation="urn:iso:15118:2:2010:AppProtocol ../V2G_CI_AppProtocol.xsd"
  xmlns:n1="urn:iso:15118:2:2010:AppProtocol"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <AppProtocol>
    <ProtocolNamespace>urn:iso:15118:2:2013:MsgDef</ProtocolNamespace>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<n1:supportedAppProtocolRes
  xsi:schemaLocation="urn:iso:15118:2:2010:AppProtocol ../V2G_CI_AppProtocol.xsd"
  xmlns:n1="urn:iso:15118:2:2010:AppProtocol"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <ResponseCode>OK_SuccessfulNegotiation</ResponseCode>
  <SchemaID>10</SchemaID>
</n1:supportedAppProtocolRes>
  <Priority>2</Priority>
</AppProtocol>
</n1:supportedAppProtocolReq>
```

V2G APPLICATION LAYER MESSAGES

- Messages for exchanging info during charging session
- V2G Message
 - Header
 - Body



V2G APPLICATION LAYER MESSAGES

- Example message

```
<?xml version="1.0" encoding="UTF-8"?>
<v2gci_d:V2G_Message xmlns:v2gci_h="urn:iso:15118:2:2013:MsgHeader"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:v2gci_b="urn:iso:15118:2:2013:MsgBody"
  xmlns:v2gci_d="urn:iso:15118:2:2013:MsgDef"
  xmlns:v2gci_t="urn:iso:15118:2:2013:MsgDataTypes"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <v2gci_d:Header>
    <v2gci_h:SessionID>3031323334353637</v2gci_h:SessionID>
  </v2gci_d:Header>
  <v2gci_d:Body>
    <v2gci_b:PaymentServiceSelectionReq>
      <v2gci_b:SelectedPaymentOption>Contract</v2gci_b:SelectedPaymentOption>
      <v2gci_b:SelectedServiceList>
        <v2gci_t:SelectedService>
          <v2gci_t:ServiceID>1</v2gci_t:ServiceID>
          <!-- charge service -->
        </v2gci_t:SelectedService>
        <v2gci_t:SelectedService>
          <v2gci_t:ServiceID>3</v2gci_t:ServiceID>
          <!-- internet service -->
          <v2gci_t:ParameterSetID>3</v2gci_t:ParameterSetID>
        </v2gci_t:SelectedService>
      </v2gci_b:SelectedServiceList>
    </v2gci_b:PaymentServiceSelectionReq>
  </v2gci_d:Body>
</v2gci_d:V2G_Message>
```

KAPITOLA 5

TESTING ENVIRONMENT



V2G BOARD SETUP I

- dLAN[®] Green PHY eval board with **dLAN[®] Green PHY Module**
- PLC support, PLC-to-Ethernet bridging support, support of HPGP, local connection to PC via RJ45



V2G BOARD SETUP II

- QCA7000_GreenPHY_Firmware
 - Allow to configure module as an emob-charger or emob-vehicle
 - Implicit support of the SLAC – EVCC and SECC side

```
PS D:\FIT_CVUT\Ing\NI-DIP\Master's_Thesis\Devol_Boards\dlan-greenphy-sdk-master\QCA7000_GreenPHY_Firmware\qca7000_1-2-4-00-1_kit_2022-03-11_windows\qca7000_1-2-4-00-1_kit\windows> .\qca7000-update.cmd
Usage:
qca7000-update <config-profile> [mac-address]

config-profile must be one of:

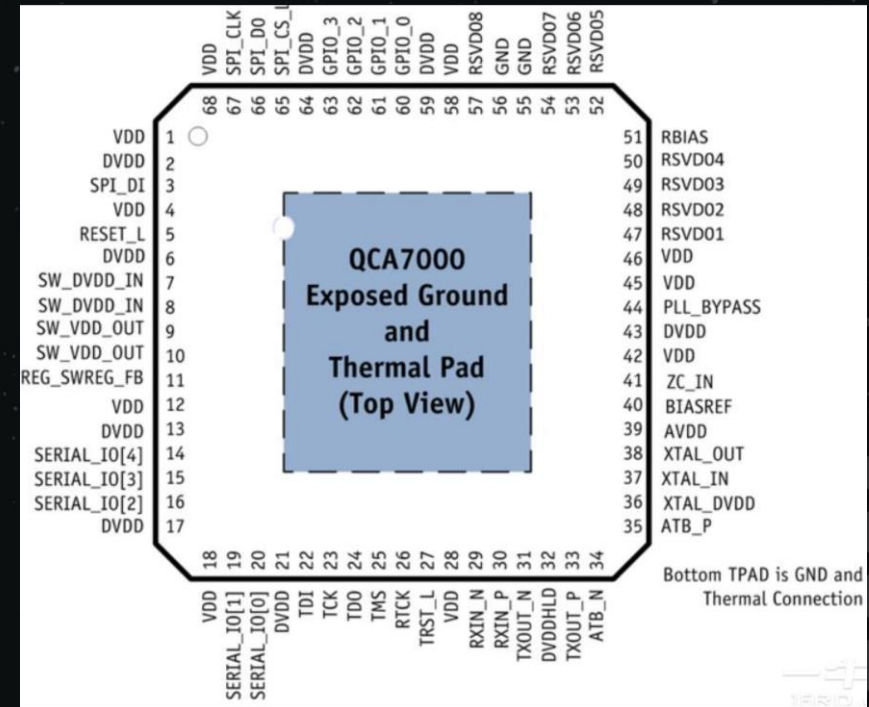
iot-generic      IoT generic, optimized for performance: 50561 off (SLAC off)
iot-conform      IoT over mains, optimized for conformity: 50561 on (SLAC off)
emob-charger     e-mobility use as charging station: SLAC in EVSE mode (50561 off)
emob-vehicle     e-mobility use as vehicle: SLAC in PEV mode (50561 off)

mac-address is optional, if omitted, the first
locally attached adapter will be programmed
```

V2G BOARD SETUP III



V2G BOARD SETUP IV



V2G TESTING ENVIRONMENT

- SLAC implementation is provided by FW
 - emob-charger or emob-vehicle
- Josev – Joint Operating System for EV chargers
 - Repository called iso15118
 - EVCC part to simulate the EV controller
 - SECC part to simulate the EVSE controller



KAPITOLA 6
V2GEVIL



V2GEVIL - ARCHITECTURE

- Tool is modular
 - cli
 - v2gtp
 - sniffer
 - messages
 - station
 - enumerator
 - fuzzer

```
└─$ v2gevil --help

Usage: v2gevil [OPTIONS] COMMAND [ARGS]...

Main entry point for the CLI

Options
  --version          Show the version and exit.
  --debug/--no-debug Enable/Disable debug mode, default: Disabled
  --help            Show this message and exit.

Commands
  car-tools          Car tool related commands
  message-tools     Message tool related commands
  modules-tools     Modules tool related commands
  sender-tools      Sender tool related commands
  sniffer-tools     Sniffer tool related commands
  station-tools     Station tool related commands
  v2gtp-tools       V2GTP tool related commands
```

V2GEVL - FUNCTIONALITY I

- **V2GTP Module:**
 - Packet parsing - IPv6, UDP/TCP, V2GTP PDUs
 - V2GTP packet - SDP response/request, V2G EXI message
 - Decoding V2G EXI message - using V2Gdecoder
 - Creating V2GTP responses
- **Sniffer Module:**
 - Live and static sniffing of V2G communication
 - Inspect specific packet from pcap file
 - Decoding and filtering capabilities



V2GEVIL SNIFFER



(v2g@v2g-virtual-machine)-[~/V2G/repos/V2GEvil]

\$

```

}}}}
INFO 2023-08-11 12:26:38,585 - iso15118.shared.comm_session (235): PowerDeliveryRes received
INFO 2023-08-11 12:26:38,587 - iso15118.shared.exi_codec (245): Message to encode (ns=urn:iso:15118:2:2013:MsgDef): {"V2G_Message": {"Header": {"SessionID": "D1255DC60E8D278A"}, "Body": {"SessionStopReq": {"ChargingSession": "Terminate"}}}}
INFO 2023-08-11 12:26:38,653 - iso15118.shared.comm_session (428): Sent SessionStopReq
INFO 2023-08-11 12:26:38,653 - iso15118.shared.states (139): Entered state SessionStop
DEBUG 2023-08-11 12:26:38,653 - iso15118.shared.states (143): Waiting for up to 2.0 s
INFO 2023-08-11 12:26:38,959 - iso15118.shared.exi_codec (299): Decoded message (ns=urn:iso:15118:2:2013:MsgDef): {"V2G_Message": {"Header": {"SessionID": "D1255DC60E8D278A"}, "Body": {"SessionStopRes": {"ResponseCode": "OK"}}}}
INFO 2023-08-11 12:26:38,961 - iso15118.shared.comm_session (235): SessionStopRes received
INFO 2023-08-11 12:26:38,961 - iso15118.shared.comm_session (396): The data link will terminate in 2 seconds and the TCP connection will close in 5 seconds.
INFO 2023-08-11 12:26:38,961 - iso15118.shared.comm_session (400): Reason: Communication session terminated
INFO 2023-08-11 12:26:40,964 - iso15118.shared.comm_session (407): terminated the data link
INFO 2023-08-11 12:26:43,968 - iso15118.shared.comm_session (414): TCP connection closed to peer with address ('fe80::d237:45ff:fe88:b12b', 52342, 0, 8)
^CDEBUG 2023-08-11 12:26:58,148 - __main__ (37): EVCC program terminated manually

```

(v2g@v2g-virtual-machine)-[~/V2G/repos/iso15118]

.\$./scripts/start_evcc.sh

130 ×

(v2g@v2g-virtual-machine)-[~/V2G/repos/V2Gdecoder]

\$

130 ×

```

INFO 2023-08-11 12:26:38,782 - iso15118.shared.comm_session (235): SessionStopReq received
INFO 2023-08-11 12:26:38,787 - iso15118.shared.exi_codec (245): Message to encode (ns=urn:iso:15118:2:2013:MsgDef): {"V2G_Message": {"Header": {"SessionID": "D1255DC60E8D278A"}, "Body": {"SessionStopRes": {"ResponseCode": "OK"}}}}
INFO 2023-08-11 12:26:38,890 - iso15118.shared.comm_session (428): Sent SessionStopRes
INFO 2023-08-11 12:26:38,891 - iso15118.secc.controller.simulator (634): iso15118 state: SessionStop
INFO 2023-08-11 12:26:38,897 - iso15118.shared.comm_session (396): The data link will terminate in 2 seconds and the TCP connection will close in 5 seconds.
INFO 2023-08-11 12:26:38,899 - iso15118.shared.comm_session (400): Reason: EV requested to terminate the communication session
INFO 2023-08-11 12:26:40,904 - iso15118.shared.comm_session (407): terminated the data link
INFO 2023-08-11 12:26:43,909 - iso15118.shared.comm_session (414): TCP connection closed to peer with address ('fe80::d237:45ff:fe88:b12a', 34132, 0, 7)
WARNING 2023-08-11 12:26:43,909 - iso15118.secc.transport.tcp_server (151): Closing TCP server
WARNING 2023-08-11 12:26:43,910 - iso15118.secc.comm_session_handler (319): Unexpected error ending current session: ('fe80::d237:45ff:fe88:b12a', 34132, 0, 7)
INFO 2023-08-11 12:26:43,910 - iso15118.secc.transport.udp_server (206): UDP server has been resumed.
^CDEBUG 2023-08-11 12:27:10,702 - __main__ (35): SECC program terminated manually

```

(v2g@v2g-virtual-machine)-[~/V2G/repos/iso15118]

.\$

130 ×

SNIFFER MODULE

```
L$ sudo v2gevil sniffer-tools sniff --live --ipv6 --decode
Sniffing packets...
Sniffing packets live on interface %s eth_car
Packet from: fe80::d237:45ff:fe88:b12a to ff02::1.
  V2GTP header: 01fe900000000002
  V2GTP payload: 1000
  Decoded V2GTP packet:
  SDP request:
  Security: 0x10 => No transport layer security
  Transport layer: 0x00 => TCP

Packet from: fe80::d237:45ff:fe88:b12b to fe80::d237:45ff:fe88:b12a.
  V2GTP header: 01fe900100000014
  V2GTP payload: fe80000000000000d23745fffe88b12bcdd21000
  Decoded V2GTP packet:
  SDP response:
  IP address: fe80000000000000d23745fffe88b12b
  Port: 52690
  Security: 0x10 => No transport layer security
  Transport layer: 0x00 => TCP

No VTGTP layer for this packet:
  Ether / IPv6 / TCP fe80::d237:45ff:fe88:b12a:56122 > fe80::d237:45ff:fe88:b12b:52690 S
```


SNIFFER MODULE

No VTGTP layer for this packet:

Ether / IPv6 / TCP fe80::d237:45ff:fe88:b12b:52690 > fe80::d237:45ff:fe88:b12a:56122 SA

No VTGTP layer for this packet:

Ether / IPv6 / TCP fe80::d237:45ff:fe88:b12a:56122 > fe80::d237:45ff:fe88:b12b:52690 A

Packet from: fe80::d237:45ff:fe88:b12a to fe80::d237:45ff:fe88:b12b.

V2GTP header: 01fe800100000024

V2GTP payload: 8000ebab9371d34b9b79d189a98989c1d191d191818999d26b9b3a232b30020000040040

Decoded V2GTP packet:

```
<?xml version="1.0" encoding="UTF-8"?><ns4:supportedAppProtocolReq xmlns:ns4="urn:iso:15118:2:2010:AppProtocol" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:ns3="http://www.w3.org/2001/XMLSchema"><AppProtocol><ProtocolNamespace>urn:iso:15118:2:2013:MsgDef</ProtocolNamespace><VersionNumberMajor>2</VersionNumberMajor><VersionNumberMinor>0</VersionNumberMinor><SchemaID>1</SchemaID><Priority>1</Priority></AppProtocol></ns4:supportedAppProtocolReq>
```

V2GEVIL - FUNCTIONALITY II

- **Messages Module**
 - V2G EXI messages - XML schema
 - Conversion between formats (XML, JSON, EXI)
 - Default dictionaries for AC/DC charging modes
 - Message dictionary generator
- **Station Module**
 - Based on the V2GTP and Messages modules
 - Implementation of SECC
 - SDP (UDP) and TCP/TLS servers
 - Core for security modules



V2GEVIL - FUNCTIONALITY III

- **Enumerator Module**
 - TLS required or not
 - TLS version
 - TLS supported cipher suites
 - Application protocols
 - Any type of V2G EXI request can be added for enumeration

V2GEVIL ENUMERATOR



```

XML
{Format=EXI, Accept=*/, User-Agent=python-requests/2.31.0, Connection=keep-alive, Host=localh
ost:9000, Accept-Encoding=gzip, deflate, Content-Length=28}
EXI
{Format=XML, Accept=*/, User-Agent=python-requests/2.31.0, Connection=keep-alive, Host=localh
ost:9000, Accept-Encoding=gzip, deflate, Content-Length=674}
XML
{Format=EXI, Accept=*/, User-Agent=python-requests/2.31.0, Connection=keep-alive, Host=localh
ost:9000, Accept-Encoding=gzip, deflate, Content-Length=12}
EXI
{Format=XML, Accept=*/, User-Agent=python-requests/2.31.0, Connection=keep-alive, Host=localh
ost:9000, Accept-Encoding=gzip, deflate, Content-Length=1749}
XML
{Format=EXI, Accept=*/, User-Agent=python-requests/2.31.0, Connection=keep-alive, Host=localh
ost:9000, Accept-Encoding=gzip, deflate, Content-Length=18}
EXI
{Format=XML, Accept=*/, User-Agent=python-requests/2.31.0, Connection=keep-alive, Host=localh
ost:9000, Accept-Encoding=gzip, deflate, Content-Length=594}
XML
{Format=EXI, Accept=*/, User-Agent=python-requests/2.31.0, Connection=keep-alive, Host=localh
ost:9000, Accept-Encoding=gzip, deflate, Content-Length=72}
EXI

```

```

(v2gevil-zORstogo-py3.10)-(v2g@v2g-virtual-machine)-[~/V2G/repos/V2GEvil]
$ v2gevil modules-tools enumerate-EV --mode all

```

```

onnection
INFO 2024-01-09 17:00:27,458 - iso15118.shared.comm_session (407): terminated the data link
INFO 2024-01-09 17:00:30,461 - iso15118.shared.comm_session (414): TCP connection closed to
peer with address ('fe80::d237:45ff:fe88:b12b', 53313, 0, 9)
ERROR 2024-01-09 17:00:30,461 - iso15118.evcc.comm_session_handler (557): EVCC tried to initi
ate a V2GCommunicationSession, but maximum number of SDP retry cycles (1) is now reached. Shut
ting down high-level communication. Unplug and plug in the cable again if you want to start ane
w.
Traceback (most recent call last):
  File "/home/v2g/V2G/repos/iso15118/iso15118/evcc/comm_session_handler.py", line 555, in get_f
rom_rcv_queue
    await self.restart_sdp(True)
  File "/home/v2g/V2G/repos/iso15118/iso15118/evcc/comm_session_handler.py", line 378, in resta
rt_sdp
    raise SDPFailedError(
iso15118.shared.exceptions.SDPFailedError: EVCC tried to initiate a V2GCommunicationSession, bu
t maximum number of SDP retry cycles (1) is now reached. Shutting down high-level communication
. Unplug and plug in the cable again if you want to start anew.
^CDEBUG 2024-01-09 17:00:32,640 - __main__ (37): EVCC program terminated manually

```

```

(v2g@v2g-virtual-machine)-[~/V2G/repos/iso15118]
$ ./scripts/start_evcc.sh

```

130 x

```

o:15118:2:2013:MsgDef): {"V2G_Message": {"Header": {"SessionID": "29782C50551B53DA"}, "Body": {
"SessionStopRes": {"ResponseCode": "OK"}}}}
INFO 2024-01-09 14:13:27,646 - iso15118.shared.comm_session (428): Sent SessionStopRes
INFO 2024-01-09 14:13:27,646 - iso15118.secc.controller.simulator (634): iso15118 state: Ses
sionStop
INFO 2024-01-09 14:13:27,646 - iso15118.shared.comm_session (396): The data link will termin
ate in 2 seconds and the TCP connection will close in 5 seconds.
INFO 2024-01-09 14:13:27,646 - iso15118.shared.comm_session (400): Reason: EV requested to t
erminate the communication session
INFO 2024-01-09 14:13:29,649 - iso15118.shared.comm_session (407): terminated the data link
INFO 2024-01-09 14:13:32,657 - iso15118.shared.comm_session (414): TCP connection closed to
peer with address ('fe80::d237:45ff:fe88:b12a', 38542, 0, 10)
WARNING 2024-01-09 14:13:32,658 - iso15118.secc.transport.tcp_server (151): Closing TCP serv
er
WARNING 2024-01-09 14:13:32,658 - iso15118.secc.comm_session_handler (319): Unexpected error
ending current session: ('fe80::d237:45ff:fe88:b12a', 38542, 0, 10)
INFO 2024-01-09 14:13:32,658 - iso15118.secc.transport.udp_server (206): UDP server has been
resumed.
^CDEBUG 2024-01-09 14:15:16,499 - __main__ (35): SECC program terminated manually

```

```

(v2g@v2g-virtual-machine)-[~/V2G/repos/iso15118]
$

```

130 x

ENUMERATOR MODULE

EV enumeration results:

Supported App protocols result:

```
{'AppProtocol': [{'ProtocolNamespace': 'urn:iso:15118:2:2013:MsgDef', 'VersionNumberMajor': 2, 'VersionNumberMinor': 0, 'SchemaID': '1', 'Priority': 1}]}
```

Supported protocols by EV:

Number of supported protocols: 1

ProtocolNamespace: urn:iso:15118:2:2013:MsgDef, VersionMajor: 2, VersionMinor: 0, SchemaID: 1, Priority: 1

TLS check result:

EV requested security: TLS and as a transport protocol: TCP for communication

TLS enumeration result:

TLS negotiated version: TLSv1.2

TLS negotiated cipher suite: ('ECDHE-ECDSA-AES128-SHA256', 'TLSv1.2', 128)

TLS shared ciphers: [('ECDHE-ECDSA-AES128-SHA256', 'TLSv1.2', 128)].

Shared ciphers are ciphers available in both the EV and the EVSE.

V2G EVIL - FUNCTIONALITY IV

- **Fuzzer Module**
 - **Testing resilience of EVCC implementation**
 - **Invalid values for parameters in V2G response message**
 - **Modes: all, custom, config, message**
 - **Can cause message processing failures**
 - **Focus on EXI/XML parsing issues**



V2GEVIL FUZZER




```
EXI
{Format=XML, Accept=*/, User-Agent=python-requests/2.31.0, Connection=keep-alive, Host=localh
ost:9000, Accept-Encoding=gzip, deflate, Content-Length=1640}
XML
{Format=EXI, Accept=*/, User-Agent=python-requests/2.31.0, Connection=keep-alive, Host=localh
ost:9000, Accept-Encoding=gzip, deflate, Content-Length=72}
EXI
{Format=XML, Accept=*/, User-Agent=python-requests/2.31.0, Connection=keep-alive, Host=localh
ost:9000, Accept-Encoding=gzip, deflate, Content-Length=322}
XML
{Format=EXI, Accept=*/, User-Agent=python-requests/2.31.0, Connection=keep-alive, Host=localh
ost:9000, Accept-Encoding=gzip, deflate, Content-Length=28}
EXI
{Format=XML, Accept=*/, User-Agent=python-requests/2.31.0, Connection=keep-alive, Host=localh
ost:9000, Accept-Encoding=gzip, deflate, Content-Length=674}
XML
{Format=EXI, Accept=*/, User-Agent=python-requests/2.31.0, Connection=keep-alive, Host=localh
ost:9000, Accept-Encoding=gzip, deflate, Content-Length=12}
EXI
{Format=XML, Accept=*/, User-Agent=python-requests/2.31.0, Connection=keep-alive, Host=localh
ost:9000, Accept-Encoding=gzip, deflate, Content-Length=1677}
XML
```

```
(v2gevil-zORstogo-py3.10)-(v2g v2g-virtual-machine)-[~/V2G/repos/V2GEvil]
$ v2gevil modules-tools fuzz-EV --mode config --config-filename ev_fuzzer_example_3.toml
```

```
(iso15118-gAdVIpLN-py3.10)-(v2g v2g-virtual-machine)-[~/V2G/repos/iso15118]
```

```
130 x
```

```
(v2g v2g-virtual-machine)-[~/V2G/repos/iso15118]
```

FUZZER MODULE

```
Created response object: [0/1939]
{'ResponseCode': 'OK_SuccessfulNegotiation', 'SchemaID': '1'}
-----
Received from client: 01fe80010000000e8098004011d01b40dd1622c4ac00
{'Header': {'SessionID': '00'}, 'Body': {'SessionSetupReq': {'EVCCID': 'D0374588B12B'}}}
Created response object:
{'Header': {'SessionID': '00'}, 'Body': {'SessionSetupRes': {'ResponseCode': 'OK', 'EVSEID': 'FRA23E45B78C', 'EVSETimeStamp': 1700593914}}}
-----
Received from client: 01fe8001000000068098004011b8
{'Header': {'SessionID': '00'}, 'Body': {'ServiceDiscoveryReq': {}}}
Created response object:
{'Header': {'SessionID': '00'}, 'Body': {'ServiceDiscoveryRes': {'ResponseCode': -9140007322155668586, 'PaymentOptionList': {'PaymentOption': ['dyMubdnLHoshpVttmAWLkqOTOXKvXLmNwAdUIsqsjBrp vdsGTvQfcfCALOLxWSSBuVhRGGV']}, 'ChargeService': {'SupportedEnergyTransferMode': {'EnergyTransferMode': ['yUdzaDMRZUmjwqzAYuHqpgyeEhgilXUsmXHmkftxhpWPGLEWGWeVLMqkKoFojXGWhgtgVqxowieOSYrMwC']}, 'ServiceID': 9152111138964487569, 'ServiceName': -244716853120383435}, 'ServiceList': {'Service': [{'ServiceID': 3, 'ServiceName': 'Fast Internet', 'ServiceCategory': 'Internet', 'FreeService': True}, {'ServiceID': 2, 'ServiceName': 'Certificate', 'ServiceCategory': 'ContractCertificate', 'FreeService': True}]}}}}}}
TCP connection closed
SDP server is running in while loop
```

FUZZER MODULE

```
DEBUG 2024-01-10 14:54:17,490 - iso15118.shared.states (143): Waiting for up to 20. [35/1909]
INFO 2024-01-10 14:54:17,682 - iso15118.shared.exi_codec (299): Decoded message (ns=urn:iso:15118:2:2013:MsgDef): {"V2G_Message":{"Header":{"SessionID":"00"},"Body":{"SessionSetupRes":{"ResponseCode":"OK","EVSEID":"FRA23E45B78C","EVSETimeStamp":1700593914}}}}
INFO 2024-01-10 14:54:17,682 - iso15118.shared.comm_session (235): SessionSetupRes received
INFO 2024-01-10 14:54:17,683 - iso15118.shared.exi_codec (245): Message to encode (ns=urn:iso:15118:2:2013:MsgDef): {"V2G_Message":{"Header":{"SessionID":"00"},"Body":{"ServiceDiscoveryReq":{}}}}
INFO 2024-01-10 14:54:18,569 - iso15118.shared.comm_session (428): Sent ServiceDiscoveryReq
INFO 2024-01-10 14:54:18,569 - iso15118.shared.states (139): Entered state ServiceDiscovery
DEBUG 2024-01-10 14:54:18,569 - iso15118.shared.states (143): Waiting for up to 2.0 s
ERROR 2024-01-10 14:54:19,727 - iso15118.shared.comm_session (222): EXIDecodingError (Exception): Transformer Exception: java.lang.RuntimeException: EXI profile stream does not respect parameter maxBuiltInElementGrammars. Expected 0 but was 2
Traceback (most recent call last):
  File "/home/v2g/V2G/repos/iso15118/iso15118/shared/exi_codec.py", line 285, in from_exi
    exi_decoded = self.exi_codec.decode(exi_message, namespace)
  File "/home/v2g/V2G/repos/iso15118/iso15118/shared/exifluent_exi_codec.py", line 50, in decode
    raise Exception(self.exi_codec.get_last_decoding_error())
Exception: Transformer Exception: java.lang.RuntimeException: EXI profile stream does not respect parameter maxBuiltInElementGrammars. Expected 0 but was 2
```

FUZZER MODULE

```
└─$ v2gevil modules-tools fuzz-EV --mode message --message-name ServiceDiscoveryRes
WARNING 2024-01-10 09:43:29,842 src.v2gevil.fuzzer.fuzz_datatypes: Not fuzz_datatypes.py:159
all required parameters are specified for fuzz in method .
WARNING 2024-01-10 09:43:29,846 src.v2gevil.fuzzer.fuzz_datatypes: Not fuzz_datatypes.py:159
all required parameters are specified for fuzz in method .
WARNING 2024-01-10 09:43:29,848 src.v2gevil.fuzzer.fuzz_datatypes: Not fuzz_datatypes.py:159
all required parameters are specified for fuzz in method .
WARNING 2024-01-10 09:43:29,849 src.v2gevil.fuzzer.fuzz_datatypes: Not fuzz_datatypes.py:159
all required parameters are specified for fuzz in method .
Station configuration:
Interface: eth_station
IPv6 address: fe80::d237:45ff:fe88:b12b
Protocol: b'\x00'
SDP port: 15118
TCP port: 54497
TLS flag: False
Accept security: True
Charging mode: AC
Validate flag for model_dump/construct: False
Cert PATH: /home/v2g/V2G/repos/V2GEvil/src/v2gevil/station/certs/cpoCertChain.pem
Keyfile PATH: /home/v2g/V2G/repos/V2GEvil/src/v2gevil/station/certs/seccLeaf.key
SDP server started
```

FUZZER MODULE

```
SDP server started
SDP server is running in while loop
Plain TCP, Connected by: ('fe80::d237:45ff:fe88:b12a', 38792, 0, 12)
TCP server loop ended after connection established
TCP server connection established
-----
Received from client: 01fe8001000000248000ebab9371d34b9b79d189a98989c1d191d191818999d26b9b3a23
2b30020000040040
{'AppProtocol': [{'ProtocolNamespace': 'urn:iso:15118:2:2013:MsgDef', 'VersionNumberMajor': 2,
'VersionNumberMinor': 0, 'SchemaID': '1', 'Priority': 1}]}

Created response object:
{'ResponseCode': 'OK_SuccessfulNegotiation', 'SchemaID': '1'}
-----
Received from client: 01fe80010000000e8098004011d01b40dd1622c4ac00
{'Header': {'SessionID': '00'}, 'Body': {'SessionSetupReq': {'EVCCID': 'D0374588B12B'}}}
Created response object:
{'Header': {'SessionID': '00'}, 'Body': {'SessionSetupRes': {'ResponseCode': 'OK', 'EVSEID': '
FRA23E45B78C', 'EVSETimeStamp': 1700593914}}}
```

FUZZER MODULE

```
-----  
Received from client: 01fe8001000000068098004011b8  
{'Header': {'SessionID': '00'}, 'Body': {'ServiceDiscoveryReq': {}}}  
Created response object:  
{'Header': {'SessionID': '00'}, 'Body': {'ServiceDiscoveryRes': {'ResponseCode': -474379419508  
8843863, 'PaymentOptionList': {'PaymentOption': [2557011587430418181]}, 'ChargeService': {'Ser  
viceID': 1261313794055509673, 'ServiceName': -631972600500673573, 'ServiceCategory': 'YYhpZimb  
bvQAkakMIhaavNkAJVpAAQWbAzjBjuWNEXbPGOgpdMRCaODNIWeSEWETxoLUsltmbzAfXgGvSTxPsKuCyKbwgvJZi', 'F  
reeService': 'wcjuqlnQxnXkFHbedUfjSkPUnhhGc', 'SupportedEnergyTransferMode': {'EnergyTransferM  
ode': ['CYZQyPpaMfUyUzIhgGzxmPANGNmCjkkfIaPmHKqhuhXoCskkDmesCNNqmPfsUSuvDEvhtRGdD']}}, 'Servic  
eList': {'Service': [{ 'ServiceID': 6.078804982723869e+18, 'ServiceName': 'FvVKbfXbJXSrdiTXQKPE  
CeIAMHXXGSlZyMpqCTXsTYyodoReAhbfb', 'ServiceCategory': 503402615467551945, 'FreeService': -588  
9312028921686995}]}}}}}  
TCP connection closed  
SDP server is running in while loop
```

FUZZER MODULE

```
INFO 2024-01-10 09:47:25,683 - iso15118.shared.exi_codec (245): Message to encode (ns=urn:iso:15118:2:2013:MsgDef): {"V2G_Message": {"Header": {"SessionID": "00"}, "Body": {"SessionSetupReq": {"EVCCID": "D0374588B12B"}}}}
INFO 2024-01-10 09:47:25,791 - iso15118.shared.comm_session (428): Sent SessionSetupReq
INFO 2024-01-10 09:47:25,791 - iso15118.shared.states (139): Entered state SessionSetup
DEBUG 2024-01-10 09:47:25,791 - iso15118.shared.states (143): Waiting for up to 20.0 s
INFO 2024-01-10 09:47:25,941 - iso15118.shared.exi_codec (299): Decoded message (ns=urn:iso:15118:2:2013:MsgDef): {"V2G_Message": {"Header": {"SessionID": "00"}, "Body": {"SessionSetupRes": {"ResponseCode": "OK", "EVSEID": "FRA23E45B78C", "EVSETimeStamp": 1700593914}}}}
INFO 2024-01-10 09:47:25,941 - iso15118.shared.comm_session (235): SessionSetupRes received
INFO 2024-01-10 09:47:25,942 - iso15118.shared.exi_codec (245): Message to encode (ns=urn:iso:15118:2:2013:MsgDef): {"V2G_Message": {"Header": {"SessionID": "00"}, "Body": {"ServiceDiscoveryReq": {}}}}
INFO 2024-01-10 09:47:26,036 - iso15118.shared.comm_session (428): Sent ServiceDiscoveryReq
INFO 2024-01-10 09:47:26,036 - iso15118.shared.states (139): Entered state ServiceDiscovery
DEBUG 2024-01-10 09:47:26,036 - iso15118.shared.states (143): Waiting for up to 2.0 s
ERROR 2024-01-10 09:47:26,194 - iso15118.shared.comm_session (222): EXIDecodingError (Exception): Exception: javax.xml.bind.UnmarshalException
Traceback (most recent call last):
  File "/home/v2g/V2G/repos/iso15118/iso15118/shared/exi_codec.py", line 285, in from_exi
    exi_decoded = self.exi_codec.decode(exi_message, namespace)
```

KAPITOLA 7
THE END



FURTHER ENHANCEMENTS

- **Basic signaling and implementation of SLAC**
- **Modules for bidirectional testing (both to and from EV)**
- **Modules for testing the bidirectional power transfer**
 - e.g. charging of other vehicles, vehicle as powersource, etc.
- **Fuzzing of PDU structure**
- **And more...**



CONCLUSION

- **Communication in Electric Vehicles hasn't reached its assumed potential**
- **With bigger needs in the future, more sensitive data will start to flow and subsequently parsed by EVs and EVSEs**
- **No opensource tools are available to cover this emerging attack surface**
- **We want our tool to act as an easy way for people to get introduced and start researching both EVs and chargers in an efficient and modular way**

[HTTPS://GITHUB.COM/KHUNTPAV/V2GEVIL](https://github.com/khuntpav/v2gevil)

THANK YOU FOR YOUR ATTENTION



PAVEL KHUNT

THOMAS SERMPINIS