

Huracán Security Analysis Edition

Quick Start Guide



What is in the box.....	3
Typical setups involving Huracán.....	5
Huracán hardware features	7
Huracán breakout board	11
Installing the USB driver	17
Python3 API	19
Inspector Java API	21
Firmware update.....	22
Help and troubleshooting	23
Technical specifications	25
Declaration of conformity	29

Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty of fitness is implied. The information is provided on an as-is basis. Riscure shall have neither liability nor responsibility to any person or entity with respect to any loss or damage arising from the information contained in this document.

The information contained in this document is subject to change without notice.

This tool must be used according to the user guide. Any operation related to maintenance, repair or calibration must be carried out by qualified personnel. Consequently, in case of failure, contact Riscure to find out about the procedure to follow.

Copyright

Copyright © 2018 Riscure BV. All rights reserved. No part of this document may be reproduced nor translated by any means without the written consent of Riscure.

Manufactured by

Riscure BV

Delftechpark 49, 2628 XJ Delft, The Netherlands

Phone: +31 15 251 40 90, Fax: +31 15 251 40 99

Email: inforequest@riscure.com

Web: www.riscure.com











What is in the box

The box contains the Huracán and all accessories to connect it to a computer and an oscilloscope.

Box content checklist

Qty [1]	Description		Identifier [2]
1	Huracan Security Analysis Edition		HRCN
1	15V 5.33A DC Power Supply Unit, input 100 - 240 V, AC 50 - 60 Hz		PSU
-	Power cable (included with PSU)	 Country specific	
1	Communication cable: USB-A - USB-B, 2 m		USB
1	Ethernet cable 3m		ETHCBL
3	Signal cable: - SMB - SMB, 50 Ω , coaxial, 3 ft		SMB2SMB

Qty [1]	Description		Identifier [2]
2	Huracán breakout board		HBOB
2	10 way, 2.54mm pitch, flat cable 40cm		BOFLC
1	OBDII-to-SUBD9 cable		O2DB9
1	Breakout board DB9 female adapter		BODB9F
1	Breakout board DB9 male adapter		BODB9M
10	Jumper cables (female-to-female)		IMPA50
1	microSD Card 8GB		MSD
1	Software package USB stick		SWUSB
-	This “Huracán Security Analysis Edition - Quick Start Guide”		

[1] The amount or number of registered items (quantity, Qty)

[2] Identifier used in this document to refer to the item.

Typical setups involving Huracán

EMFI setup

Electromagnetic Fault Injection (EMFI) allows the user to introduce a fault in a targeted chip of the target system in the hope of bypassing security features.

Comparing to laser FI and power FI, performing EMFI requires almost no modification to the target printed circuit board (PCB), making it very efficient in setup preparation.

Figure 1 shows a high-level block diagram of an EMFI setup using Huracán and other Riscure equipment. The target can be any device with active CAN interface.

Huracán plays several roles in this EMFI setup. It supplies +12V to the system, communicates with the target chip directly or indirectly via CAN protocol, generates a trigger signal to Spider at the beginning or the end of a CAN frame transmission that kick starts a certain operation. The Spider will then control the EMFI transient probe to fire an EM pulse at the specified moment by the user.

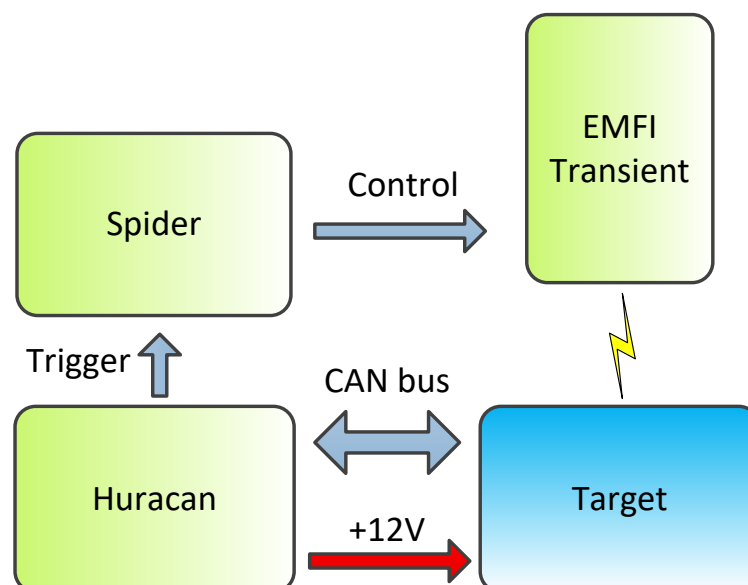


Figure 1 EMFI setup

EM SCA acquisition setup

Side-channel Analysis (SCA) techniques can be applied to extract signals through unintended information channels such as power consumption, EM radiation, finger prints on a key pad etc. The extracted signals may contain information related to the security operation of the target system. The goal of SCA is to compromise the security operation of the target system by analyzing this information.

The SCA often starts with signal acquisition from the side channel. Figure 2 illustrates a block diagram of a SCA acquisition setup using Huracán and other Riscure equipment.

Huracán communicates over the CAN bus to the target which kick starts target security operation (e.g. encryption/decryption operation of a certain cipher), it then sends a trigger to the oscilloscope to start the sample acquisition, recording the side-channel signals during the security operation. Alternatively, the Huracán triggers the oscilloscope indirectly via icWaves to overcome signal misalignment due to jitter or any security countermeasures.

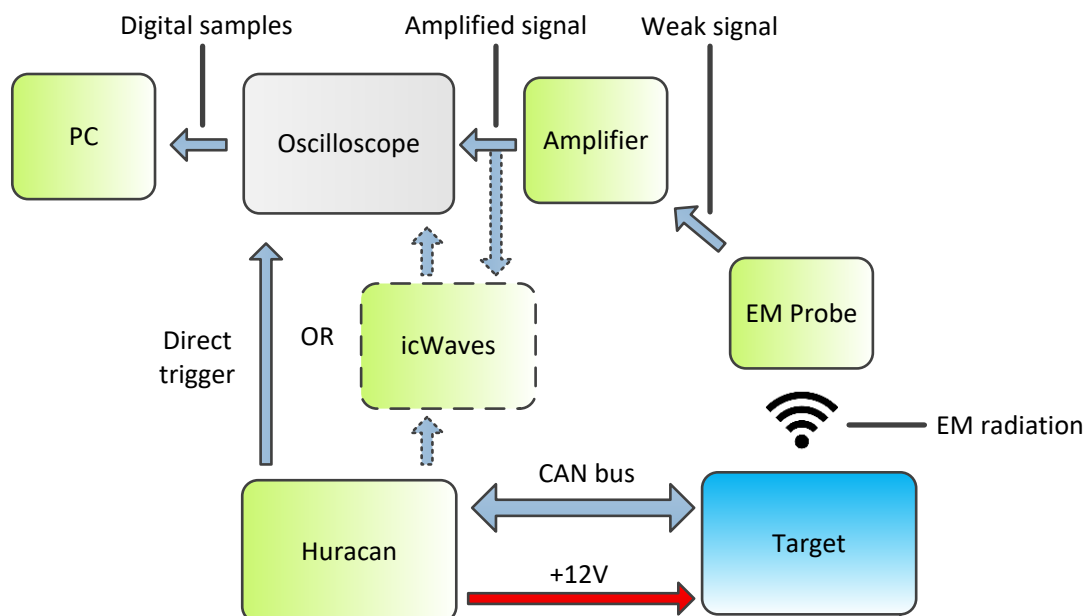


Figure 2 EM SCA acquisition setup

Huracán hardware features

The trigger output port

Huracán generates trigger signals at these ports to provide timing reference to FI equipment or oscilloscopes.

The SUB-D9 male port

Huracán delivers the CAN bus signals, +12V power supply, ground and ignition signals in SUB-D9 male format. Figure 3 illustrates the signal layout of such a port. Pin 4, 5, 6 and 8 of the SUB-D9 port are not connected.

There are 2 SUB-D9 ports available per Huracán device, connecting to 2 separate groups of these signals. Next to a target SUB-D9 socket, the port can also be connected to the Huracán breakout board for a more flexible connection format.



The ignition signal is +12V when asserted, and is not designed to supply strong current to a target.



There is no termination resistor between the CAN HIGH signal and CAN LOW signal

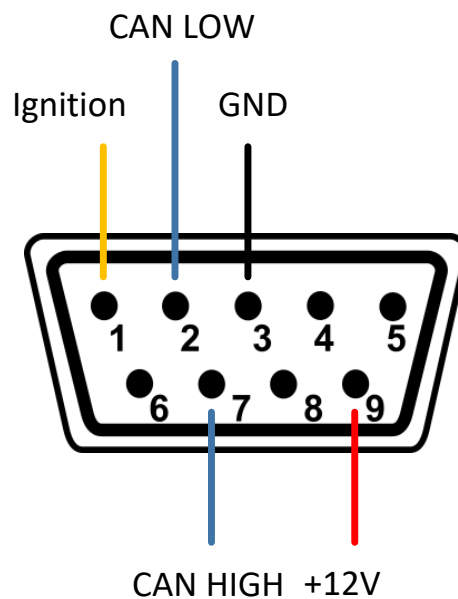


Figure 3 Huracán SUB D9 port pinout

The 10-pin socket

Next to the 3.3V and GND rails, the socket contains a group of GPIO ports. They are meant as reserve IOs that can be used to deploy experimental features.

Currently they have not yet been assigned with any useful functions.



P0.3, P0.2 and P2.10 can be used to access the In-System Programming (ISP) feature of the on-board micro-controller. Use of this feature is not supported by Riscure, and can lead to firmware corruption.



Do not connect this socket to the Huracán breakout board 10-pin socket. It will cause irreversible damage to the components of the Huracán device.

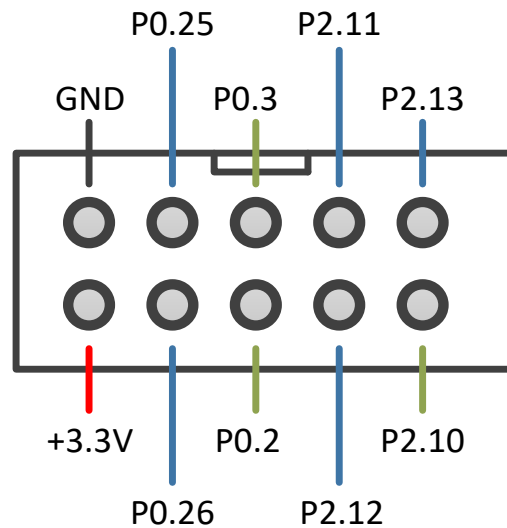


Figure 4 Huracán 5x2 socket pinout

The Ethernet port

The Ethernet port supports communication speed up to 100Mb/s, and hence significantly faster than that of the full-speed USB port.

It is reserved for the features developed in a future firmware version.

The microSD card slot

Providing support to a microSD storage with up to 8GB storage capacity. It is reserved as non-volatile storage for future feature-specific information.

The USB 2.0 port

The USB 2.0 port operates at 12Mb/s rate (Full-speed) and serves as the primary connection between the device and the host PC.

Once connected to the PC and with corresponding driver installed successfully, Huracán will appear as a virtual COM port device.

Trigger input port

The port is reserved for an incoming trigger signal to provide timing reference that triggers Huracán device reaction. This feature has not yet been implemented.

Huracán breakout board

The SUB-D9 female port

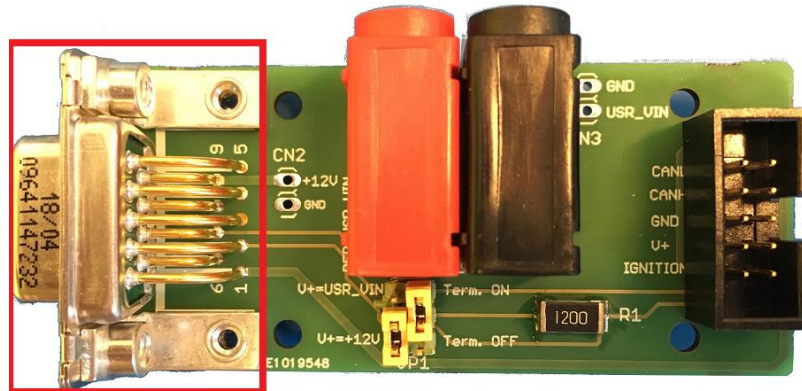


Figure 5 Huracán breakout board SUB-D9 female port highlighted by red rectangle

Figure 5 highlights the SUB-D9 port of the Huracán breakout board. It is meant to connect to the Huracán SUB-D9 port.

Its pin layout is identical to that of the Huracán SUB-D9 port. See Figure 3 for details.

The 10-pin socket

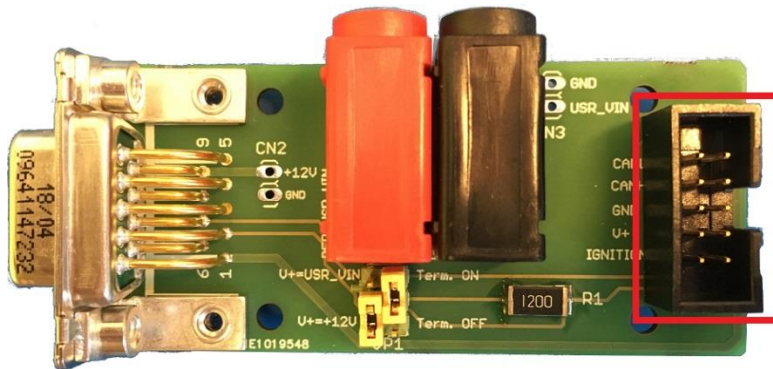


Figure 6 Huracán breakout board 10-pin socket highlighted by red rectangle

The 10-pin socket is meant to relay the signals and power lines provided by Huracán SUB-D9 port and connects to a connector with a different mechanical format.

There are 2 adapters shipped with Huracán product that can be used to connect to a target with SUB-D9 female or male connector. The intention is to make more adapters available to support other mechanical formats.

Figure 7 illustrates the pin layout of the 10-pin socket. Besides V+, all other signals are directly routed from the SUB-D9 port.

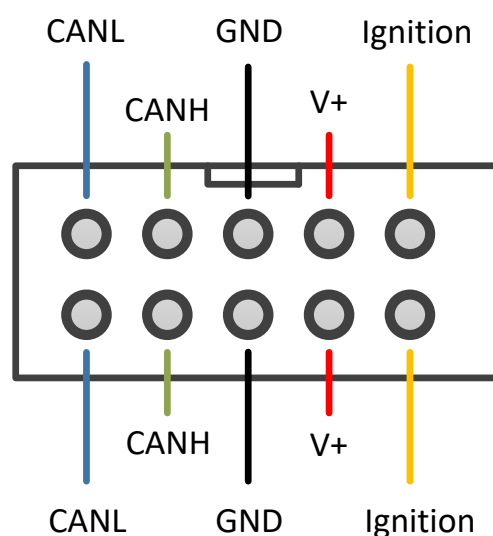


Figure 7 Huracán breakout board 10-pin socket signal layout

The V+ signal can be either the +12V delivered from Huracán or a user-supplied voltage through the RED and BLACK banana jacks, depending on the position of the jumper on the left column of JP1.

Bus termination and power control switch

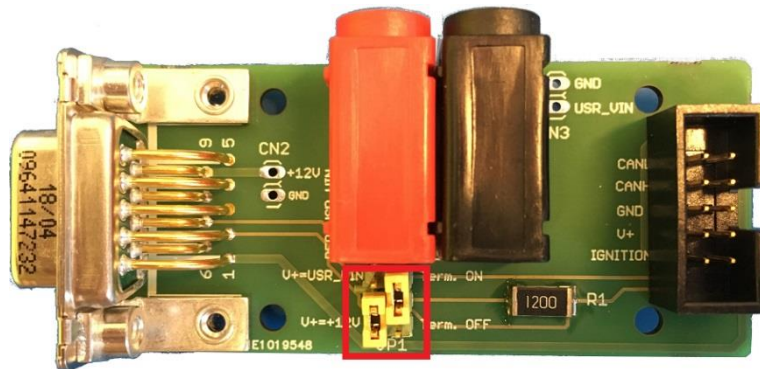


Figure 8 Huracán breakout board termination and power control switch

The control switch consists of 2 jumpers. One is located on the left side of the connector, and the other one is located on the right side.

Figure 9 illustrates the jumper position and its corresponding effect on the voltage supplied to the V+ signal of the 10-pin socket (See Figure 7).

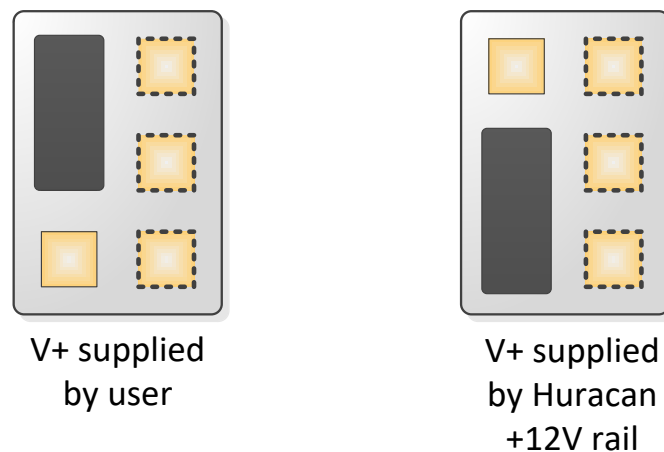


Figure 9 Jumper configuration to select V+ voltage source

Figure 10 illustrates the jumper position and its corresponding effect on the bus termination resistor connection.

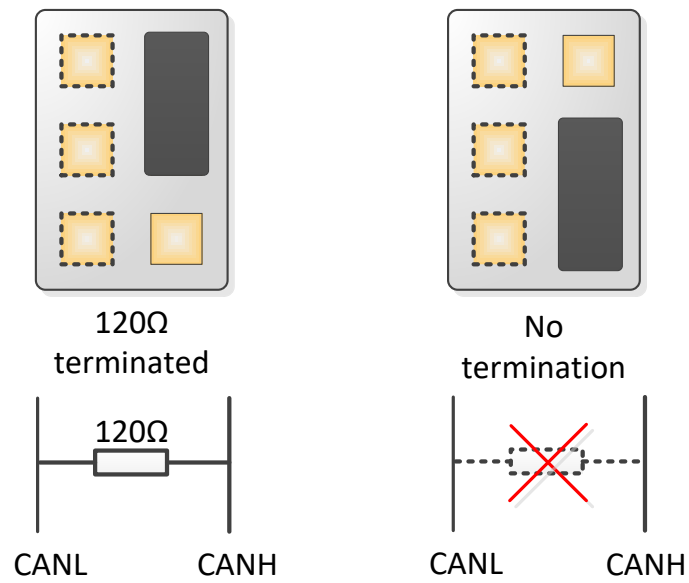


Figure 10 Jumper configuration to switch CAN bus termination

Unsoldered connectors

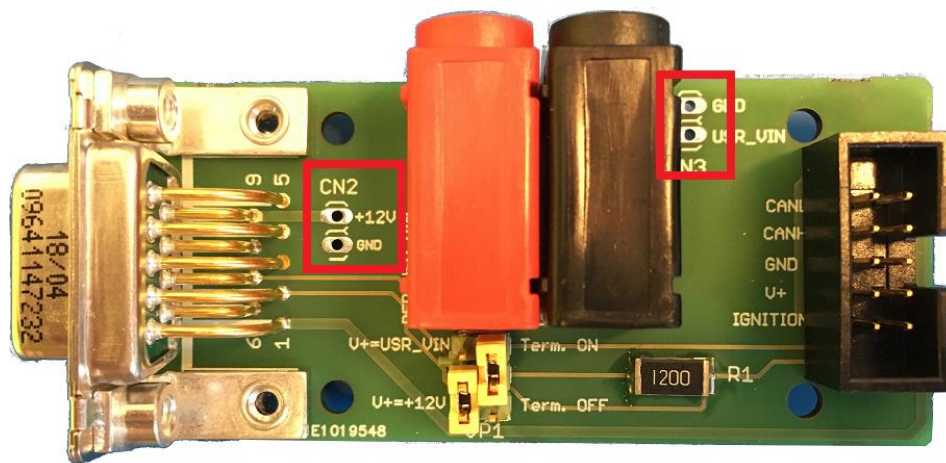


Figure 11 Huracán breakout board connector footprints

They are only intended for users with desperate need of connecting to the +12V or supplying the user voltage via a 2.54 mm pitched header format.

Installing the USB driver

Installing the USB driver on Windows 7

Acquiring the driver

Login to the Riscure download portal.

Download the Huracán driver.

Installing the driver

Connect the Huracán device to the PC.

Launch Windows Device Manager.

Right click on the "Huracan" device under the "Other devices" category and select option "Update Driver Software".

In the pop-up dialog window, click on the option "Browse my computer for driver software".

Check the "Include sub-folders" option and click on the "Browse..." button.

Select the directory containing "huracan.cat" and "huracan.inf" files in the file browser and click "OK" to confirm the selection. The path to the selected directory should then be displayed in the text field next to the "Browse..." button.

Click "Next" to initiate the driver installation.

The Huracán device should then appear under the "Ports (COM & LPT)" category in Device Manager.

Installing the USB driver on Windows 10

Windows 10 automatically installs its default USB COM port driver when a Huracán device is connected for the first time.

Installing the Riscure driver has the additional benefit of displaying "Huracan" as the name of the COM port device. The installation procedure is identical to that for a Windows 7 PC.

Python3 API



The Huracán Python3 API is not backwards compatible with Python2.

Downloading and installing Python3

Download the Python3 (32-bit or 64-bit) installer from <https://www.python.org/downloads/>. Install the downloaded Python3 by following the guidance of the installer. Optionally add the directory containing "python.exe" to your path variable.

Installing the *pyserial* library

Launch command prompt and execute the following command to install pyserial:

```
> [path_to_python3_directory]/Scripts/pip install pyserial
```

Alternatively, download and install the pyserial package from the Internet.

Acquiring the Huracán Python API package

Log in to the Riscure download portal.

Download the Python API package.

Running "example_huracan_driver.py"

Open the "example_huracan_driver.py" script from the "example" folder of the package in a text editor.

Modify the COM port string to that of your Huracán device COM port number enumerated in Windows Device Manager.

Save the modified script to the root directory of the Python API package and launch a command in the directory containing the modified script.

The script can be executed by invoking python on the command line similar to below:

```
> [path_to_python3_directory]\python.exe example_huracan_driver.py
```

For further information on the API, read the documentation in the "huracan.py" file for the Huracan class.

Inspector Java API

A Java API for the Huracán is included with Inspector. An example sequence can be generated to help you get started building an acquisition module (go to "File" > "New Module wizard..." and choose "Huracan Sequence" in the wizard).

Please refer to the Inspector manual for more information on module development.

Firmware update

The Huracán device may have to be updated in order to stay compatible with software APIs from a newer release.

To perform a firmware update, acquire the installer from the Riscure download portal and execute the installer as Administrator and follow the guidance of the installer.

Help and troubleshooting

Huracán does not show up in Windows Device Manager

Confirm that the power switch of the Huracán device has been switched to the ON position. And make sure that the Huracán USB driver has been successfully installed.

I cannot run the "example_huracan_driver.py" script

Confirm that the python executable invoked in the command prompt is Python3.x. Also confirm that the "pyserial" library has been correctly installed to the Python3 distribution. Finally, check if the COM port string written in the script corresponds to the actual COM port of the Huracán device.

Sending a CAN frame fails and Tx LED lights up

The CAN controller in Huracán requires at least another CAN node to acknowledge a transmitted frame in the ACK slot of a frame. If the acknowledge does not occur, the CAN controller will automatically retry the transmission until the frame gets acknowledged. Connecting the Huracán to a CAN bus with another active node will resolve this issue.

Tx trigger signal is generated too early for the frame

The Tx trigger is generated 17µs before the SOF bit of the Tx frame, assuming the CAN bus is free for new frame transmission and the frame will not lose the arbitration. Otherwise, the transmission of the frame will be delayed, making the trigger signal having appeared "early".

There is no voltage present on breakout board V+ pin

Check if the power control jumper is located at the intended position.

Still have questions?

Please contact Riscure support professionals.

Technical specifications

Operational conditions

- Room temperature 25 °C (77 °F).



Maintain stable environmental conditions (temperature, humidity, airflow etc.) in order to reliably repeat tests and compare test results.



Unplugging the PSU from the product is not required, but recommended when not used for an extended time.

Power supply input

- 15 V DC, min. DC current capability 5.33A
- Center-positive plug, inner-Ø 2.5 mm, outer-Ø 5.5 mm.



Use of a PSU other than supplied by Riscure is not supported. Power spikes may cause internal damage and loss of accuracy.

Huracán SUB-D9 CAN bus signals

- Max. baud rate 1Mbps
- Not 120 Ω terminated

Huracán SUB-D9 port voltage output

- 12V DC, max. DC current capacity 3A

Huracán SUB-D9 port ignition signal

- 12V DC, min. DC current capacity 500mA

Huracán trigger output port

- V_{OH} max. 3.6 V
- V_{OL} min. 0.01 V
- Output current max. 125mA

Huracán trigger input port

- V_{IN} max. 5.5 V
- V_{IH} min. 1.37 V
- V_{IL} max. 0.8 V

Huracán USB port

- USB2.0 full-speed, self-powered

Huracán Ethernet port

- Maximum bandwidth 100Mbps

Huracán microSD card

- Support up to 8GB storage capacity

Product casing

- Dimensions L x W x H: 220.00 x 169.50 x 34.63 [mm], 8.661 x 6.673 x 1.363 [inch].

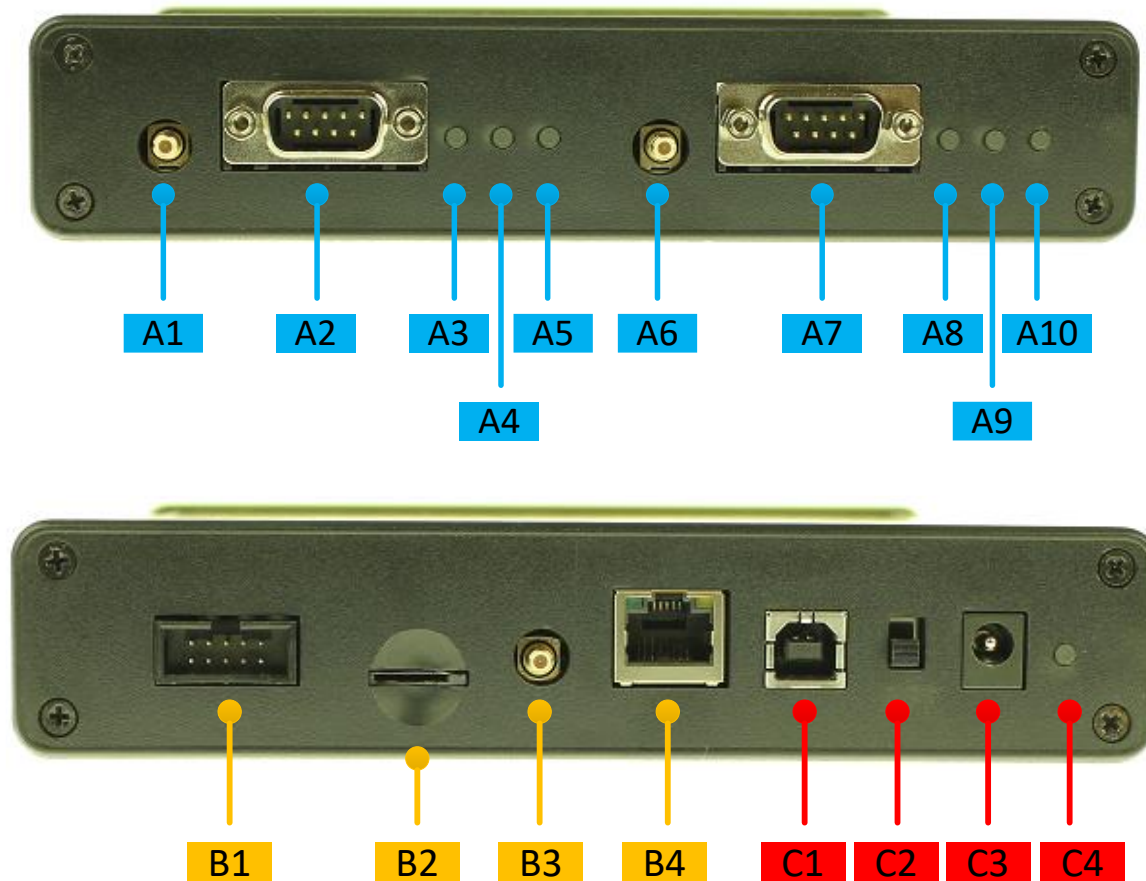


Table 1 Details of interfaces and functions.

Port	Label	Description
A1	can 1 trigger out	CAN1 trigger output signal
A2	can 1	CAN1 SUB-D9 port
A3	can 1 tx	CAN1 Tx activity indication LED
A4	can 1 rx	CAN1 Rx activity indication LED
A5	can 1 power	CAN1 +12V power indication LED
A6	can 2 trigger out	CAN2 trigger output signal
A7	can 2	CAN2 SUB-D9 port

Port	Label	Description
A8	can 2 tx	CAN2 Tx activity indication LED
A9	can 2 rx	CAN2 Rx activity indication LED
A10	can 2 power	CAN2 +12V power indication LED
B1	gpio	10-pin socket containing auxiliary GPIOs, GND and 3.3v power rail
B2	microSD	microSD card slot
B3	trigger in	Trigger input port
B4	ethernet	Ethernet port
C1	usb	USB 2.0 port. Type USB-B. Communication link with a computer.
C2	on/off	15 V DC power switch
C3	15 VDC	15 V DC power supply input.
C4	powered	15 V DC power indication LED

Declaration of conformity

EC-DECLARATION OF CONFORMITY

Suppliers Details

Name

Riscure B.V.

Address

Frontier Building, Delftechpark 49, 2628 XJ Delft, The Netherlands

Product Details

Product Name

Inspector

Model Name(s)

Huracan

Trade Name

Riscure

Applicable Standards Details

Directives:

- LVD (2006/95/EC) - EMC directive (2004/108/EC)

Standards:

- IEC 60825-1; IEC 320 C8; IEC 60950-1; 21 CFR 1040; ANSI/ESD S20.20:2007; BS EN 61340-5-1:2007; EN55022-B; EN61000-4-2, 4-5; CISPR 11; CISPR22-B; UL 1950

Supplementary Information

The appliance fulfils the relevant requirements of the EMC-directive and the LVD-directive according to our technical documentation TCD-Huracan

Declaration

I hereby declare under our sole responsibility that the product(s) mentioned above to which this declaration relates complies with the above mentioned standards and Directives

Riscure B.V.
Frontier Building
Delftechpark 49
2628 XJ Delft
The Netherlands
Tel.nr.: +31 (0) 15 251 4090

Name

Dr.ir. F.G. de Beer /
Technical Director

Issued Date

04 / 03 / 2015



Signature of representative

Notes