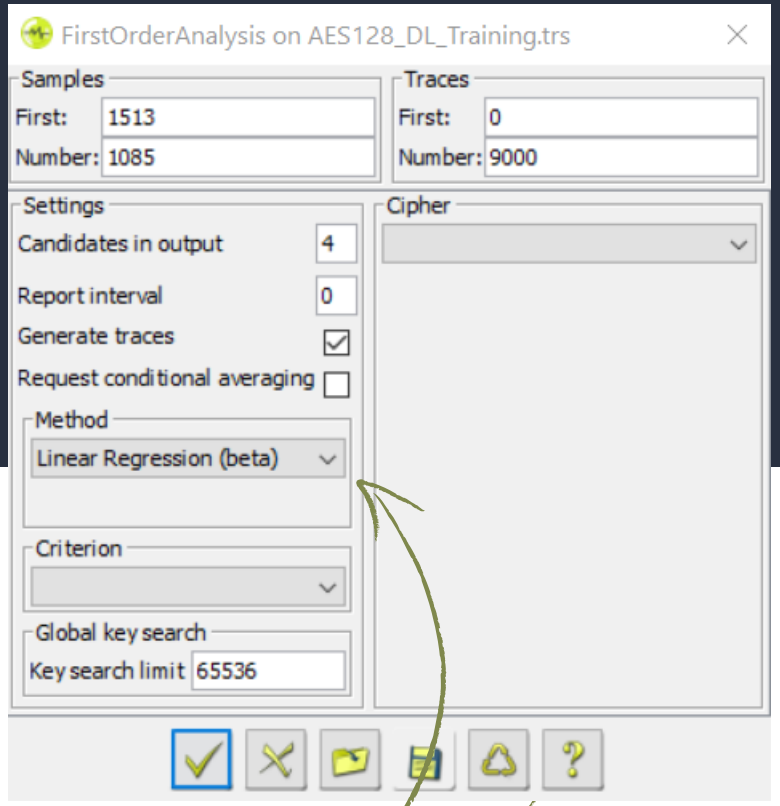
riscure

What's new in Inspector 2020.1

SCA & FI
software update
April 2020

Linear regression

- ✓ 2 pass method that first selects the best fitting leakage model per key candidate
- ✓ Works on leakage model based on ID
- ✓ Gives the best results compared to other methods but requires more computer resources
- ✓ Best used in combination with conditional averaging

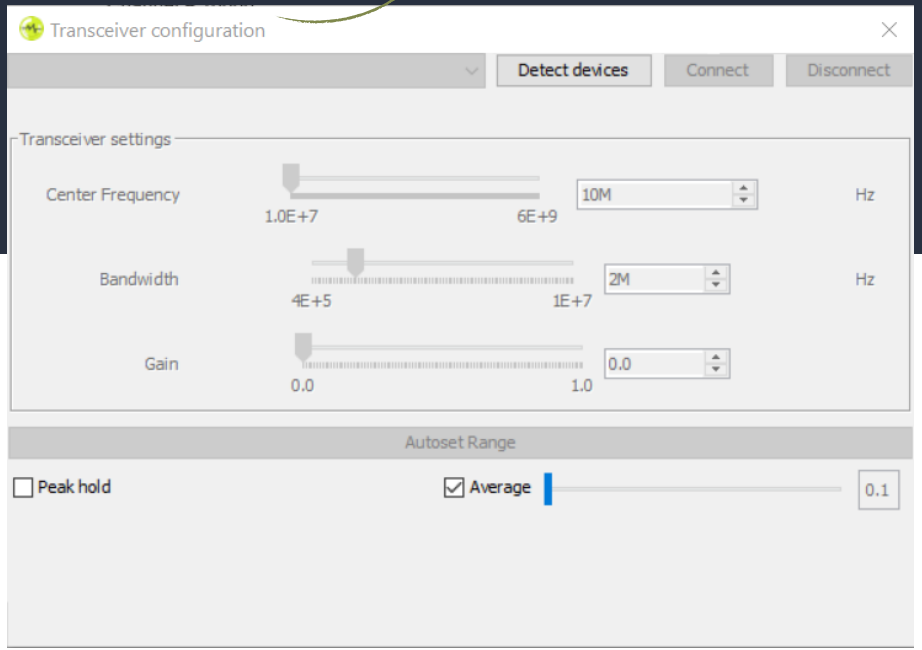


Linear regression can be chosen as a method in first order analysis

Transceiver

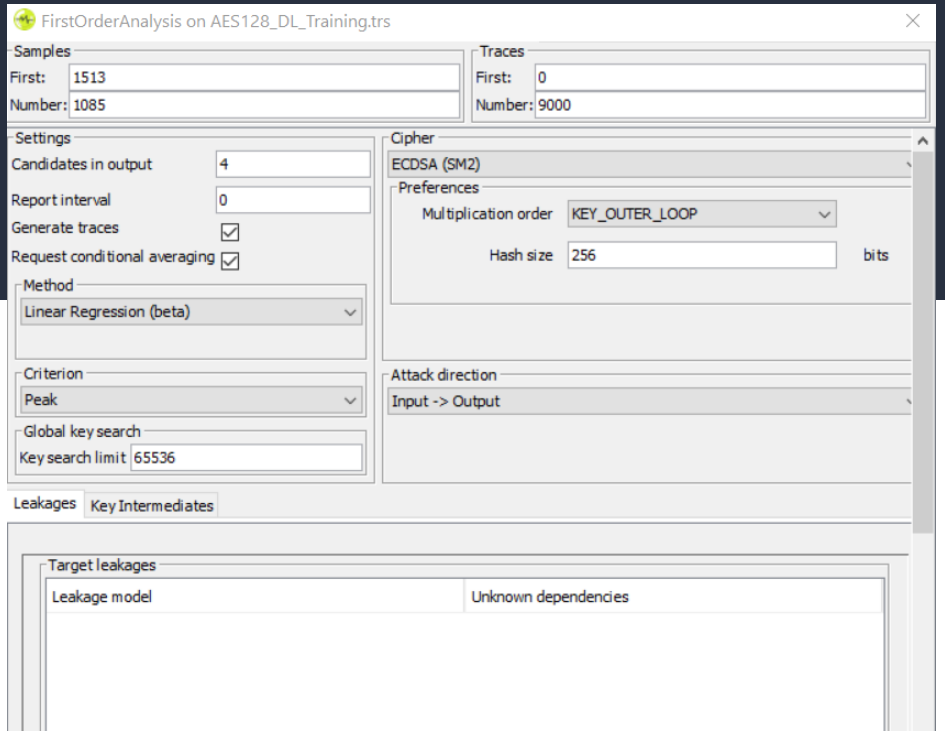
- ✓ Transceiver let's you easily identify valuable signals hidden in noise
- ✓ Transceiver configuration can now be fully done from within Inspector
- ✓ Easily set the center frequency, bandwith and gain
- ✓ Use of the previous virtual machine for tuning is now optional

Transceiver configuration can be found in the tools menu



SM2 Cipher

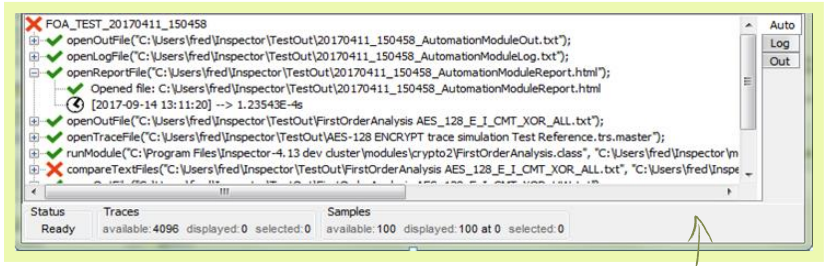
- ✓ Added SM2 for first order analysis
- ✓ The attack targets the multiplication of the key with 'r' (which is part of the output), and assumes a byte wise multiplication
- ✓ Select Key-inner or Key-outer loop as multiplication order
- ✓ Set HASH size in bits
- ✓ Works with new feature Linear Regression



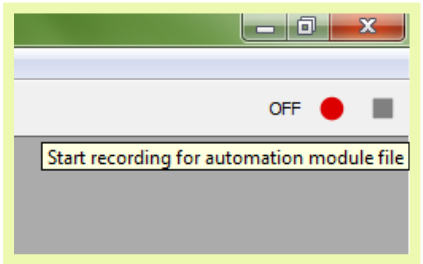
Automation & HPA

- ✓ Generates a programmable user module
- ✓ Build loops to run a automation scenario with multiple settings

- ✓ Premium subscription includes Inspector High performance Analysis
- ✓ Maximum of 10 Inspector instances included
- ✓ Windows and Linux both supported



Progress of the automation scenario is shown in new “auto’ tab



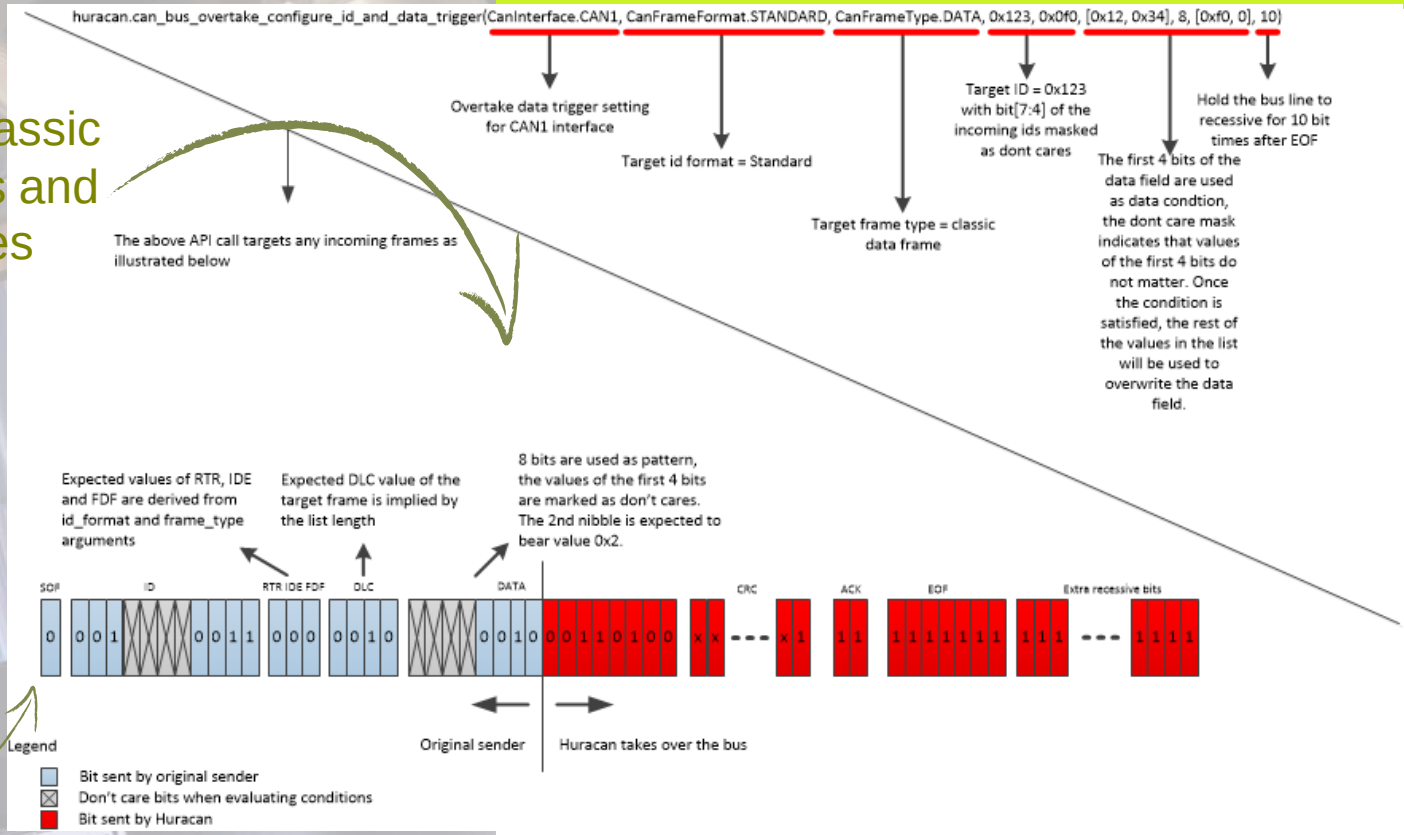
Buttons enable ‘macro like’ recording of automation scripts

Huracan API

Bus overtake feature

Works on classic CAN frames and FD frames

Supports trigger on a specified id and/or data pattern



Huracan API

- ✓ Triggering on incoming data frames to Huracan
  - ✓ Immediately after receiving the first bit of the packet (start bit)
  - ✓ Immediately receiving the ID of the packet and matching it with a mask
  - ✓ Immediately after receiving the payload and matching it with a mask
  - ✓ Immediately after the end of a packet, with and without matching
- ✓ Huracan Java APIs now supports regulated frame transmission (a response must be received before the next transmission occurs)

Technical features

- ✓ An Inspector.bat has been added, which launches Inspector with run-time log message output for easy debugging
- ✓ For Matlab .trs support, an import/export library is now available on Riscure's GitHub (https://github.com/Riscure/java-trsfile)
- ✓ Updated the XML schema for leakages files to a structure which can be loaded more quickly

Upgrade procedure & SDK changes

Inspector installation & SDK updates

Where

- Customers with a Subscription Contract receive a download link
- Download from Riscure license portal

Installation guidance

- Inspector software can be installed on the same PC workstation next to your previous version. You can still revert back to the previous version if you want to.
- You will need a license file next to your dongle to work with Inspector 2020.1
- API is backwards compatible.

Your own modules & traces

- Inspector software points by default to the same user module folder as previous versions.
- In case you have trouble porting an older module to this Inspector version, please contact our support portal for assistance.

Release notes & bug fixes

For the full list of bug fixes, please refer to the release notes:

https://www.riscure.com/security-tools/inspector-sca/#support

Java update

- Inspector now uses Java 11. The JDK and JRE shipped with Inspector are also this Java version.

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90

www.riscure.com

Riscure North America
550 Kearny St., Suite 330
San Francisco, CA 94108 USA
Phone: +1 650 646 99 79

inforequest@riscure.com

Riscure China
Room 2030-31, No. 989, Changle Road, Shanghai 200031
China
Phone: +86 21 5117 5435

inforcn@riscure.com

riscure

Challenge your security