

riscure

inspector 4.10

SCA & FI software update
July 2016

Contents

Page 3

What's new in 4.10?

- icWaves usability improvements
- Template Analysis
- Major speed up of DPA
- Perturbation control Spider
- Perturbation improvements
- Miscellaneous

Page 17

Upgrade procedure & SDK changes

- Inspector 4.10 installation
- SDK changes

What's new in 4.10?



icWaves usability improvements

Improvements

- Visibility on settings inside icWaves
- Save & load parameters from file
- Improved stability from several bug fixes
- Acquisition speed 8x faster (icWaves 3)
- Live tuning of trigger parameters during acquisition (icWaves 3)
- Advanced settings easier to use (icWaves 3)



Current view of loaded pattern

Settings explained (example)

Load toggles with clear

Renamed

Renamed

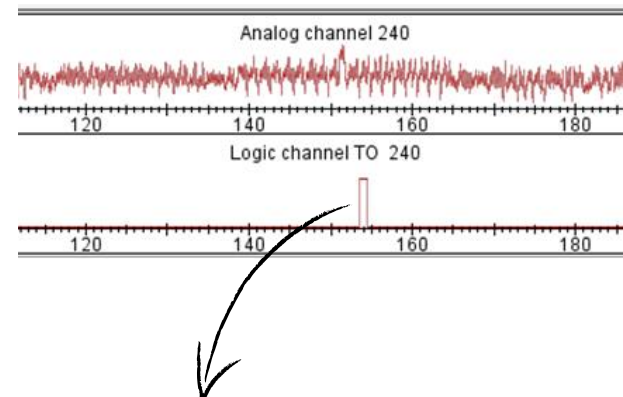
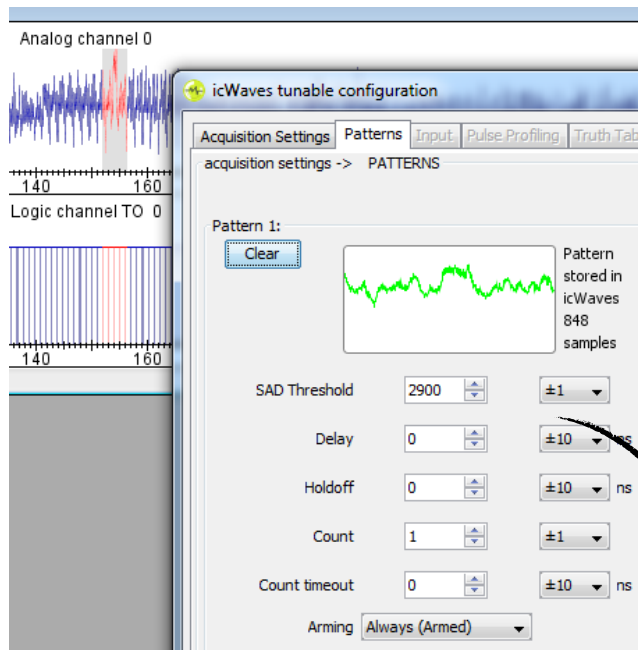
Settings in readable xml

Save and Load configuration settings

Live tuning (icWaves 3)

Real time feedback on your trigger parameters

Now you can live tune all trigger parameters until you have the optimal settings. For instance, play around with the SAD Threshold and observe the effect in the Logic Channel output trace:



Tune parameters live until you have a steady trigger output (Logic channel TO)

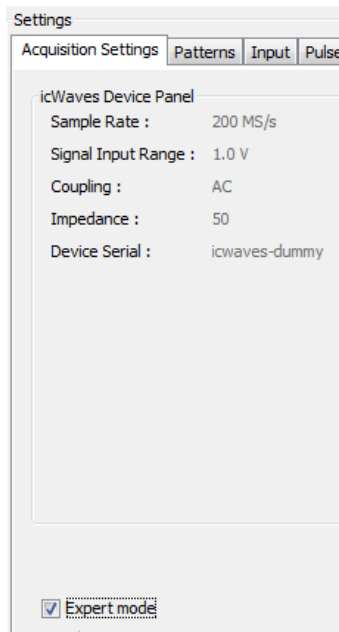
Advanced settings (icWaves 3)

Workflow support and less programming

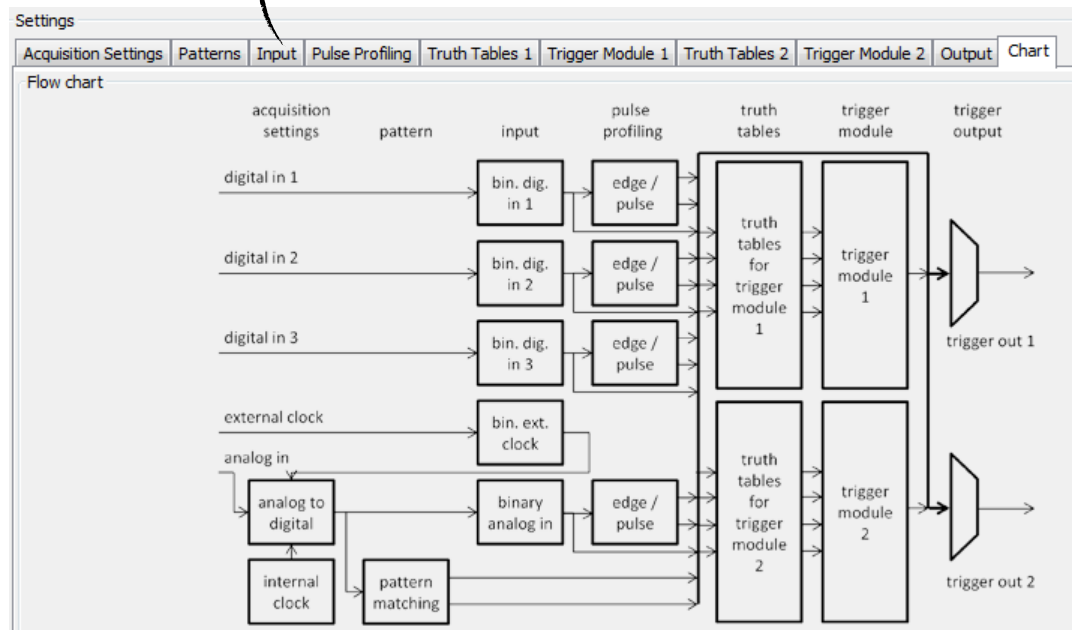
The advanced settings were difficult to use. With user feedback we implemented several tabs to match your workflow. The tabs allow for flexible configuration without a need to program.

Workflow:

input → truth tables → trigger module → output



For advanced settings



Advanced settings example use case

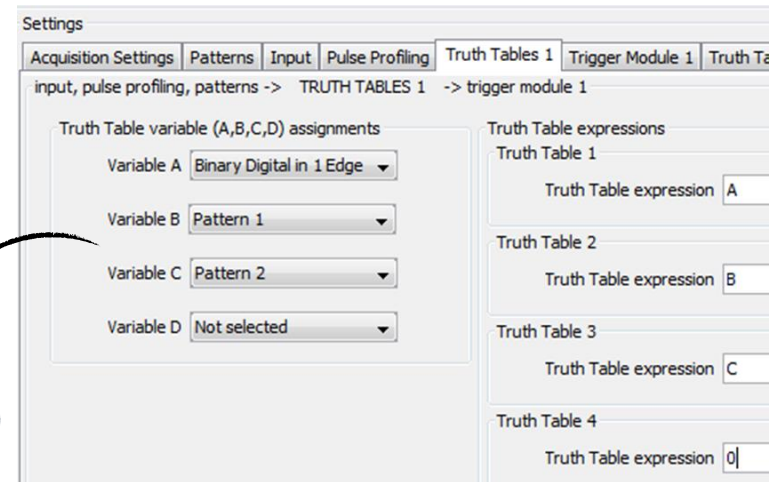
Trigger on edge and two patterns

There are cases in which you want to trigger on two different patterns that happen in a specific order.

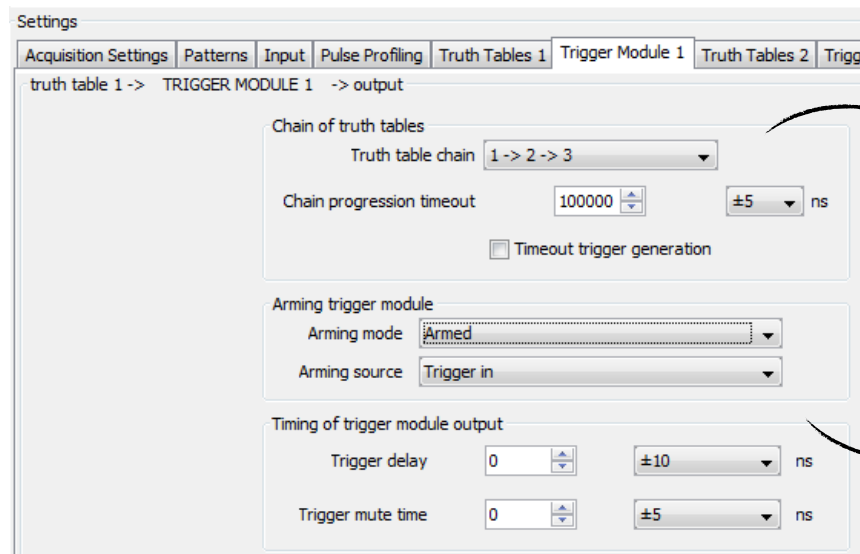
This is one way to do it:

1. Prepare truth tables:
 - Detect edge (A)
 - Wait for Pattern 1 (B)
 - Wait for Pattern 2 (C)

1. Prepare the truth tables for chaining



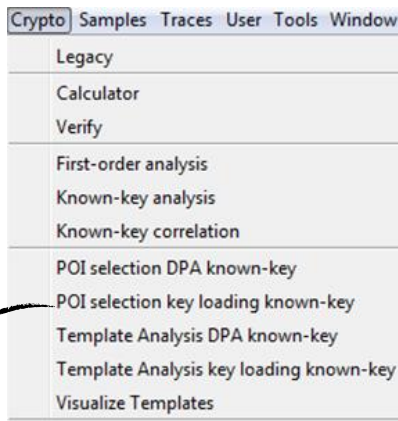
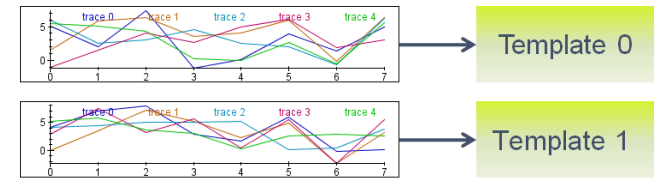
2. Chain them
3. Trigger



2. Define the chain for triggering

3. Trigger

Template Analysis



Added "Key loading" attack

Template Analysis methods overview

In Inspector 4.10

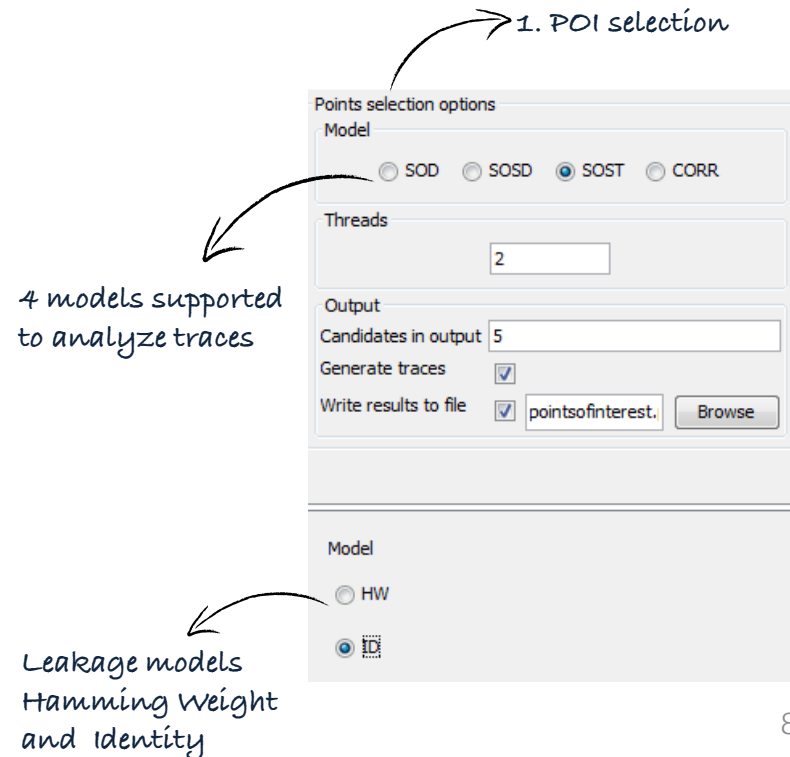
- TA on key loading
- TA on AES + DES with known-key analysis

In next releases in 2016 (coming up)

- Unknown-key analysis
- TA on RSA

Inspector 4.10 better supports the workflow

1. Points of Interest (POI) selection - below
2. Learn phase TA – next page
3. Apply phase TA – next page



Learn & apply in template analysis

2. Learn phase

3. Apply phase

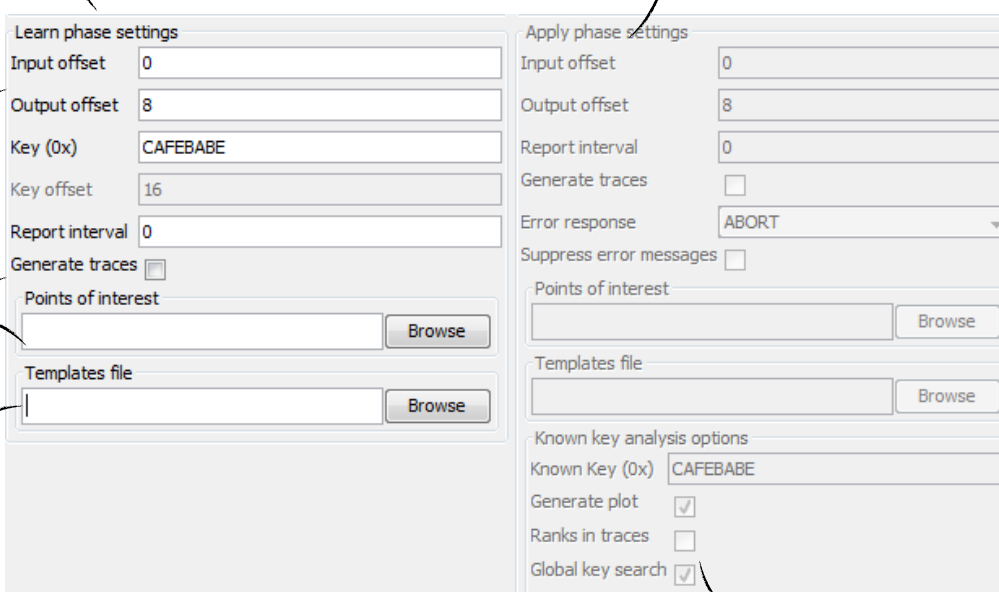
Flexible I/O data definition

Show templates

POI text file

Save templates after learning

Known key options



Learn phase settings

Input offset 0

Output offset 8

Key (0x) CAFEBABE

Key offset 16

Report interval 0

Generate traces ☐

Points of interest Browse

Templates file Browse

Apply phase settings

Input offset 0

Output offset 8

Report interval 0

Generate traces ☐

Error response ABORT

Suppress error messages ☐

Points of interest Browse

Templates file Browse

Known key analysis options

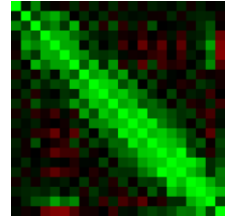
Known Key (0x) CAFEBABE

Generate plot ☒

Ranks in traces ☐

Global key search ☒

Mean + COV: highly informed templates



Tweak your learning

Template analysis settings

Phase

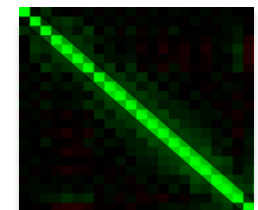
☒ Learn ☐ Apply

Model

☐ Mean ☐ +Var ☒ +Cov

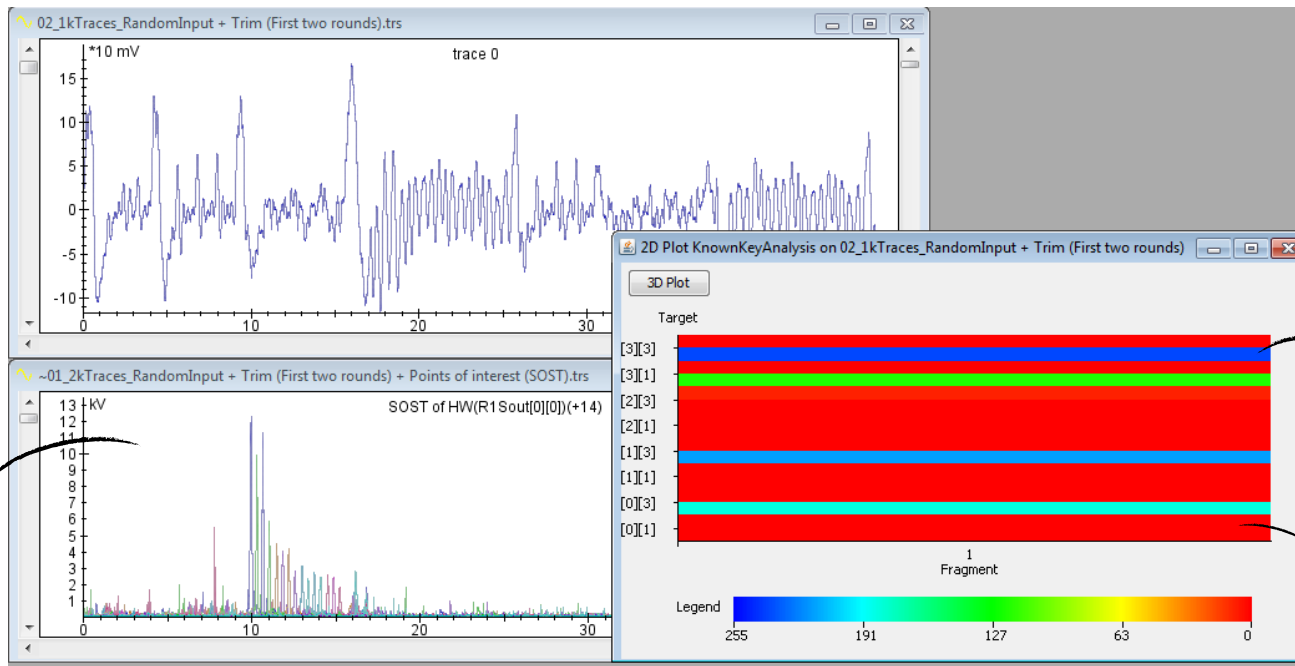
Optimiser

☒ None ☐ Pooled



Mean + var: simplified templates

Results template analysis – known key



Blue = attack failed
on key byte 15

Red = attack
succeeded on key
byte 2

Results after 1000 traces

Best score Round 0: Key: Column 0, Row 0:
rank: 1, candidate: 202 (0xCA), confidence: -2.94978007263585030000 at positions: [9928, 9932, 9941]

Best score Round 0: Key: Column 0, Row 1:
rank: 1, candidate: 254 (0xFE), confidence: -3.05737807004152230000 at positions: [33456, 11453-11454]

Best score Round 0: Key: Column 0, Row 2:
rank: 185, candidate: 170 (0xAA), confidence: -4.96057573001445550000 at positions: [12960, 12969-12970]

Best score Round 0: Key: Column 0, Row 3:

Key byte results – template scoring

Major speed up of DPA

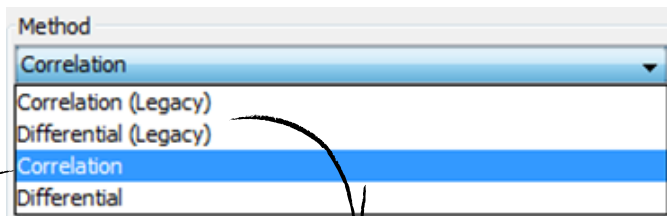
Performance increase

Significant performance increase for **analysis of > 200 samples**.
Increase mostly depends on # cores.



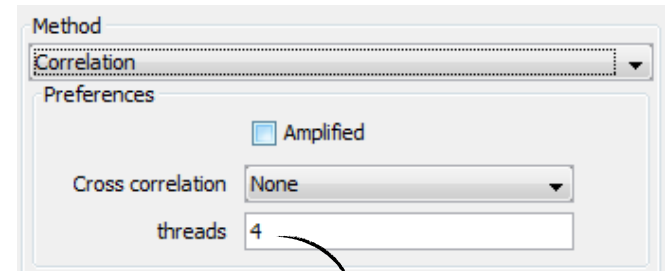
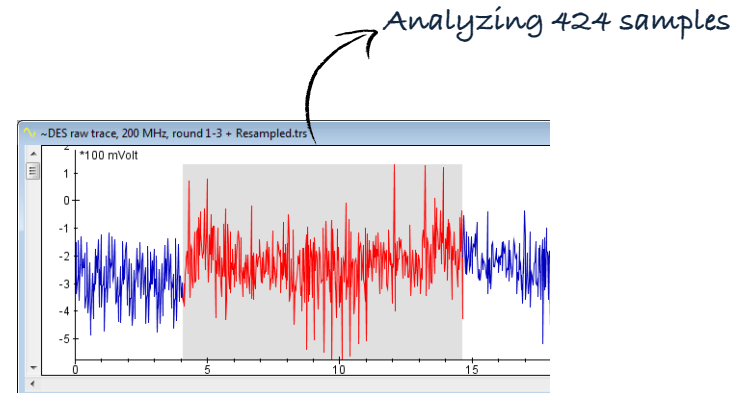
Multithreading in

- First-order
- Known-key analysis



Single-threaded (legacy)

Default is multithreaded.
Both in Correlation + Differential



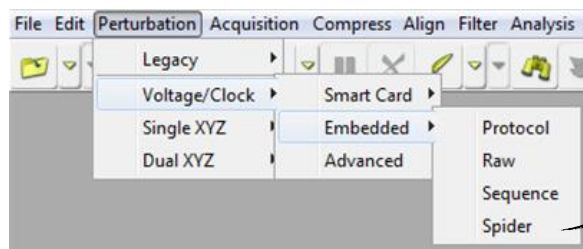
Auto tuned based on # cores in
your PC



Device settings (via Sequence)

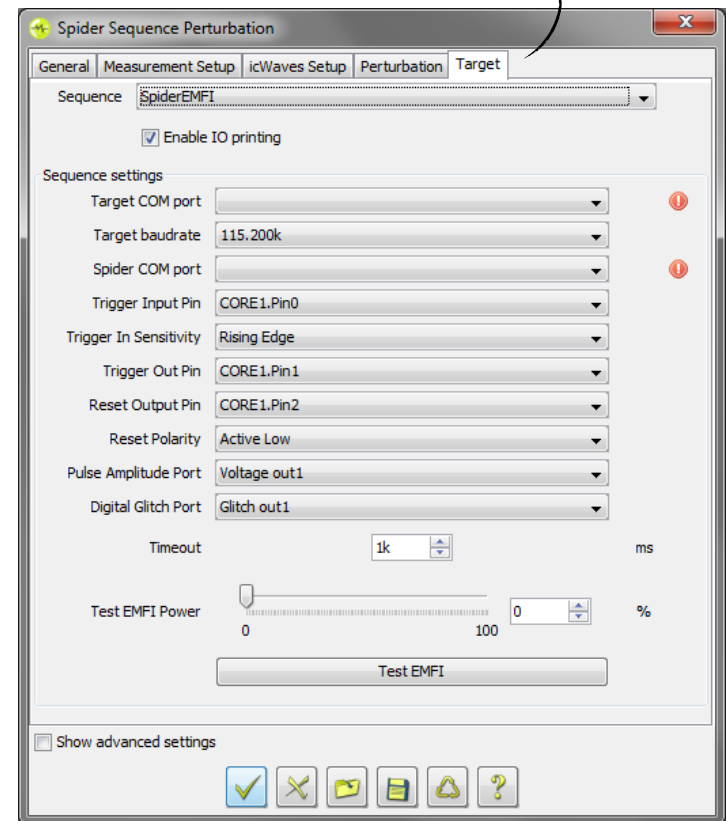
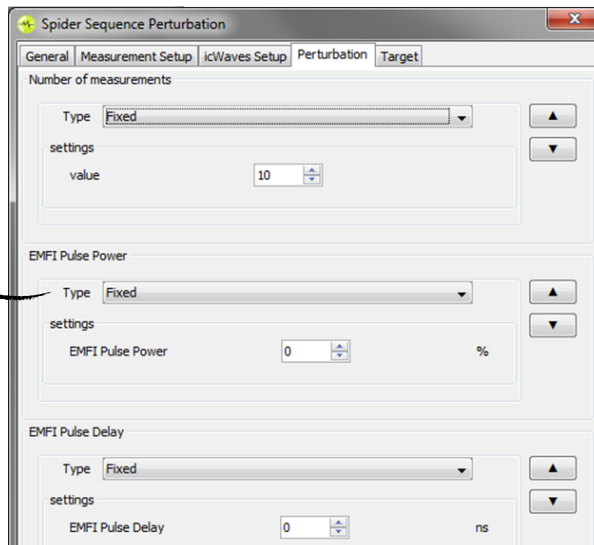
Spider perturbation control

For fault injection on embedded chips
Requires SDK installation delivered with Spider product.



FI with Spider

E.g.
perturbation
settings for
EMFI



Perturbation improvements

Perturbation log

Now latest on top by default
(instead of bottom)

VC Glitcher report - MySequence_Spider Sequence Perturbation (started 2016-06-29 12:43:41)

id	Perturbati...	Timed out	Data
9	4.000000	false	AE 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 5B AA 49 6F
8	4.000000	false	AE 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 5B AA 49 6F
7	4.000000	false	AE 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 5B AA 49 6F
6	4.000000	false	AE 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 5B AA 49 6F
5	4.000000	false	AE 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 5B AA 49 6F
4	4.000000	false	AE 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 5B AA 49 6F
3	4.000000	false	AE 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 5B AA 49 6F
2	4.000000	false	AE 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 42 61 64 43
1	4.000000	false	AE 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 42 61 64 43
0	4.000000	false	53 69 67 6E 61 74 75 72 65 20 63 68 65 63 6B 3A 20 4F 4B 2C 20

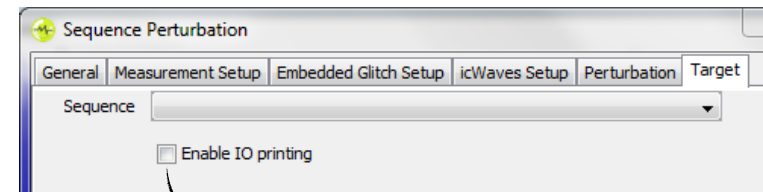
Filter expression Apply ASCII/Hex

Convert Hex to ASCII

Timed out	Data
false	0000000000000000 [Io:Tfb] fàUA""Æ
false	0000000000000000 [Io:Tfb] fàUA""Æ
false	0000000000000000 [Io:Tfb] fàUA""Æ
false	0000000000000000 [Io:Tfb] fàUA""Æ
false	0000000000000000 [Io:Tfb] fàUA""Æ
false	0000000000000000 [Io:Tfb] fàUA""Æ
false	0000000000000000 [Io:Tfb] fàUA""Æ
false	0000000000000000 BadCmd fàUA""Æ
false	0000000000000000 BadCmd BadCmd
false	Signature check: OK, Booting...BadCmd BadCmd

I/O printing from Sequence

Added an "I/O printing" option to Sequence Perturbation to make it easier for you to see all the I/O activity:



See the I/O activity from
Sequence module

Perturbation improvements

Colors in perturbation log

So far you had 3 colors (green, red, yellow). With ColorVerdict you can now show many more verdicts.

This makes it much easier to see different types of faults!

VC Glitcher report - MyProtocol_SC Single XYZ Perturbation (started 2015-08-28 11:27:22)			
Device...	XYZ Device...	Timed out	Data
00000	0.000000	false	00 00 01 02 03 04 05 06 C7 39 D7 EA FA E4 ED A3 00 00 01 02 0
00000	0.000000	false	00 00 01 02 03 04 05 06 C7 39 D7 EA FA E4 ED A3 00 00 01 02 0
00000	0.000000	false	00 00 01 02 03 04 05 06 C7 39 D7 EA FA E4 ED A3 00 00 01 02 0
00000	0.000000	false	00 00 01 02 03 04 05 06 C7 39 D7 EA FA E4 ED A3 00 00 01 02 0
00000	0.000000	false	00 00 01 02 03 04 05 06 C7 39 D7 EA FA E4 ED A3 00 00 01 02 0
00000	0.000000	false	00 00 01 02 03 04 05 06 C7 39 D7 EA FA E4 ED A3 00 00 01 02 0
00000	0.000000	false	00 00 01 02 03 04 05 06 C7 39 D7 EA FA E4 ED A3 00 00 01 02 0
00000	0.000000	false	00 00 01 02 03 04 05 06 C7 39 D7 EA FA E4 ED A3 00 00 01 02 0
00000	0.000000	false	00 00 01 02 03 04 05 06 C7 39 D7 EA FA E4 ED A3 00 00 01 02 0
00000	0.000000	false	00 00 01 02 03 04 05 06 C7 39 D7 EA FA E4 ED A3 00 00 01 02 0
00000	0.000000	false	00 00 01 02 03 04 05 06 C7 39 D7 EA FA E4 ED A3 00 00 01 02 0
00000	0.000000	false	00 00 01 02 03 04 05 06 C7 39 D7 EA FA E4 ED A3 00 00 01 02 0

```
//verdict(NORMAL);  
// Alternative for more colors from ColorVerdict:  
verdict(ColorVerdict.MAGENTA);
```

Example configuration

Overview	Package	Class	Use	Tree	Deprecated
Prev Class	Next Class	Frames	No Frames		
Summary: Nested	Enum Constants	Field	Method	Detail: Er	

perturbation2.lib

Enum ColorVerdict

java.lang.Object
java.lang.Enum<ColorVerdict>
perturbation2.lib.ColorVerdict

All Implemented Interfaces:

Verdict, Serializable, Comparable<ColorVerdict>

```
public enum ColorVerdict  
extends Enum<ColorVerdict>  
implements Verdict
```

Enum Constant Summary

Enum Constants

Enum Constant and Description

CYAN

GREEN

LIGHT_GRAY

MAGENTA

ORANGE

PINK

RED

WHITE

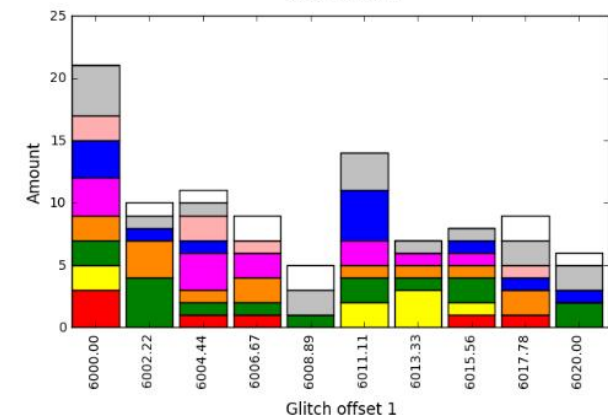
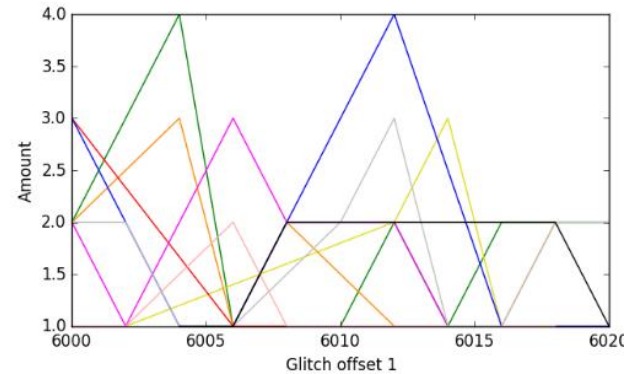
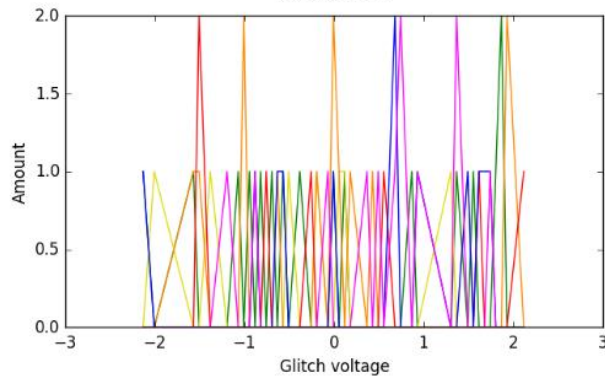
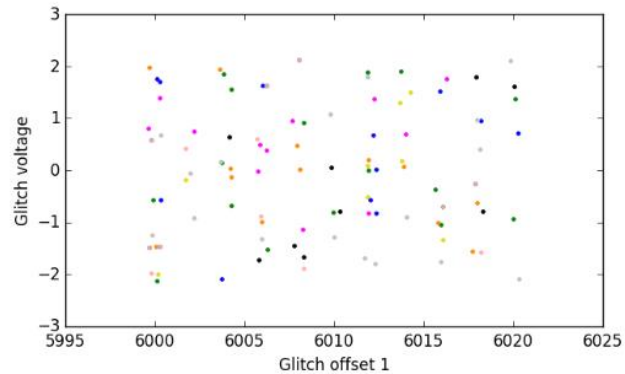
YELLOW

Colors available
(API documentation)

Perturbation improvements

FI GraphIt update

For customers that have FI GraphIt : it has been updated to reflect the new colors:



Miscellaneous

Sequence API change

`read()` in Class `BasicSequence`

- was not easy to use because of many variations
- was insufficient for certain perturbation scenarios

The change:

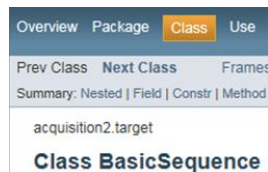
- `readAll()` replaces all `read()` methods.
- `read()` is deprecated

For example, the code below:

```
int bytesRead;
byte[] response = new byte[16];
bytesRead = read(rawIOTarget, response, 1000, NO_LOG);
if(bytesRead != response.length) {
    response = Arrays.copyOf(response, bytesRead);
}
```

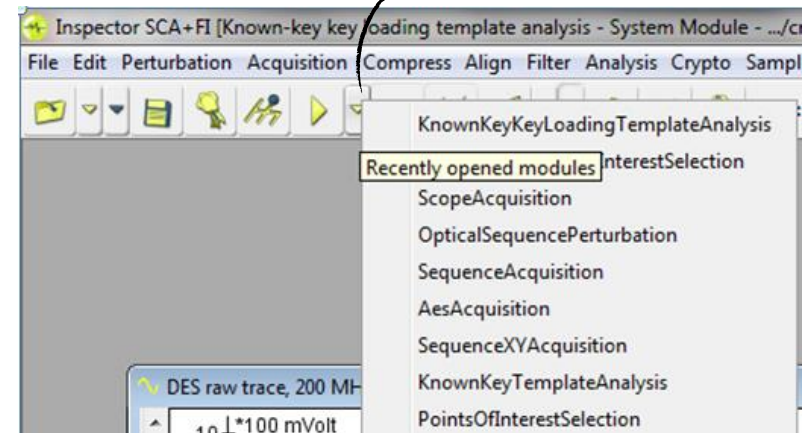
is simplified by

```
byte[] response = readAll(rawIOTarget, 16, 1000, 0);
```



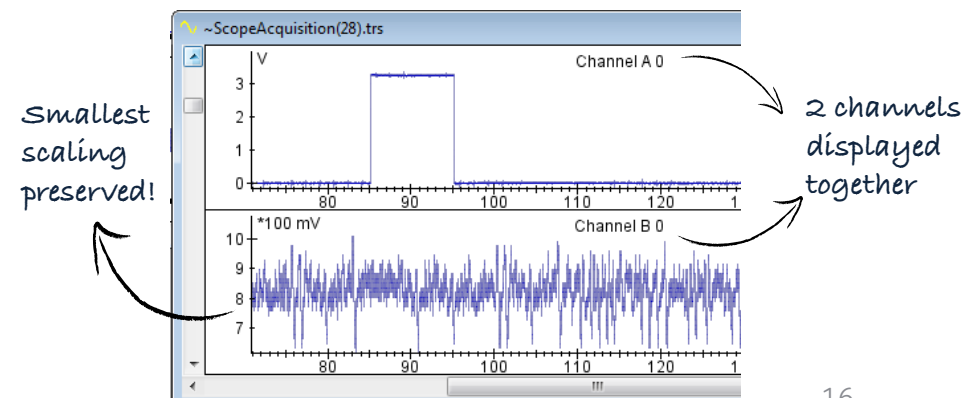
Recent modules

New: open recently used modules



Oscilloscope multi-channel display

Viewing 2 channels used to take several clicks and have scaling issues. Now, when you use more than 1 channel:



Upgrade procedure & SDK changes



Inspector 4.10 installation

Where

- Customers with Support Contract receive download link
- Download from Riscure download 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.
- API is backwards compatible with Inspector 4.7

My own modules & traces

- Inspector software points by default to the same user module folder as previous versions.
- Your own modules and traces from Inspector 4.7 are compatible with this Inspector release.
- In case you have trouble porting an older module to this Inspector version, please contact our support portal for assistance.

SDK and firmware updates

- icWaves: SDK 3.8. Bug fixes and improvements (APIs threading safe). icWaves 3 improvement: additional digital acquisition channel, includes automatic firmware upgrade.
- VC Glitcher 2: SDK 2.6. Perturbation CPU upgrade, Bug fixes, firmware upgrade.

For full SDK release notes:

C:\Program Files (x86)\Riscure\[yourSDK]

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>

<https://www.riscure.com/security-tools/inspector-fi/#support>

Please contact Riscure for more information

You can reach us by email : inforequest@riscure.com

by phone : +31 15 251 4090 US: +1 650 646 9979

Or on the web: riscure.com

riscure

