Riscure Inspector 4.12 Release Notes

Date 12 May 2017

Release Highlights

4.12

- Windows 10 and Java 8 support
- Improved Chain
- Laser Station 2 now support Twin Scan
- First Order Analysis module speed up to 5 times
- History info in Inspector Log and Out Tab are saved into files
- Many bug fixes

Questions and Support

- Please contact Riscure support If you experience problems or need help:

https://support.riscure.com/

Riscure BV Delftechpark 49 2628 XJ Delft The Netherlands Phone: +31 15 251 40 90 Fax: +31 15 251 40 99 E-mail: inforequest@riscure.com
www.riscure.com Chamber of Commerce: 27287509 VAT: NL815984753B01 Bank: ING The Netherlands 68.35.07.338 IBAN: NL 69 INGB 0683507338

Riscure Inspector 4.12 Release Notes

Issue key	Release Note
INS-7826	Fixed issue that chains with acquisition and First Order Analysis didn't work and could lead to Inspector freeze.
INS-7818	Fixed issue that acquisition in Chain with "Show device properties during acquisition" caused Inspector to freeze
INS-7790	First Order Analysis locked up Inspector when output was not available. This is resolved so that Inspector will no longer print all keys when brute forcing the key without output in the trace data field.
INS-7789	Included LeCroy Inspector server 1.7.0 with LeCroy 8000 support in "hardware\Lecroy" folder of Inspector
INS-7785	Spider SDK 1.3.1, icWaves SDK 3.9, VC Glitcher 2.7 included in Inspector installer
INS-7774	Implemented a new architecture for all chainable modules
INS-7739	Support for the latest version of the DPSS stepper motor attenuator.
INS-7737	Fixed a bug where VC Glitcher randomly produces 1 extra glitch with jitter when perturbation tab option "On rising external trigger" or "On falling external trigger" is selected.
INS-7723	Included 64-bit support for Picoscope 5203 in Framework 1
INS-7719	Solved an issue that caused the VC Glitcher power monitor offset setting to reset when the device receives a power down trigger.
INS-7710	Changed the window title of KnownKeyAnalysis 2D plot so that is does not show the encryption algorithm anymore
INS-7702	The Windows Start Menu structure for Inspector is changed to accommodate Windows 10 defaults. Manual, tutorial and javadoc links are removed and can only be accessed from Inspector directly
INS-7685	Added timestamps of when a module is loaded to Out and Log windows of Inspector .
INS-7676	When Inspector is being installed the Visual Studio C++ 2008 x86 redistribution package is installed accordingly to support the USB helper application
INS-7665	Fixed a bug of enabling closed loop function on Z axis for LS2.

Riscure BV Delftechpark 49 2628 XJ Delft The Netherlands Phone: +31 15 251 40 90 Fax: +31 15 251 40 99 E-mail: inforequest@riscure.com
www.riscure.com Chamber of Commerce: 27287509 VAT: NL815984753B01 Bank: ING The Netherlands 68.35.07.338 IBAN: NL 69 INGB 0683507338

Riscure Inspector 4.12 Release Notes

INS-7653	The GUI for the alignment module is updated by separating the internal and external reference trace indexes and issues resolved so that a user is able to execute the same alignment module multiple times in a row.
INS-7642	Fixed a bug in the leakage definitions for all AES EqInv Sbox in XOR out
INS-7640	Updated Module Wizard to reflect the new module architecture
INS-7638	Fixed an issue where VC Glitcher generates an extra glitch when operated in any smart card perturbation module (perturbation 1 and perturbation 2).
INS-7596	Increased LeCroy scope sample limit to 128M samples.
INS-7552	Added timestamps to the log window when inspector recovers from a temporarily lost dongle.
INS-7541	The number of shift results displayed in the "Out" tab for Static Align was not displayed when the first trace index is not 0. This issue is solved so that the result is always shown
INS-7540	Improved GUI for the alignment modules: - A new panel is added for reference pattern samples selection - The internal reference trace case and the external reference trace case are separated more clearly
INS-7531	Fixed ECDSA KEY_OUTER_LOOP leakage files.
INS-7519	Fixed a bug that causes readAll() to return more bytes than requested by setting the 2nd timeout to 0.
INS-7517	When implementing new function modules the new superclass BaseModule should be extended
INS-7510	Solved an issue that cuased inherited fields from JavaBeans to be displayed incorrectly.
INS-7508	Improved precision of sample data correlation calculations and made correlation treat NaN values as zero while this caused floating point arithmetic rounding errors during processing small number of traces.

Riscure Inspector 4.12 Release Notes

INS-7482	Unplugging a USB device in use by Inspector, will no longer result in multiple exceptions being thrown.
INS-7470	Fixed an issue in the alignment module that prevented the user to use the same external reference trace multiple times in a row.
INS-7468	Fixed an issue for the Twin Scan which caused an exception when speed slider was set to its maximum value.
INS-7444	Traces created in a chain were not represented correctly when a logarithmic scale was applicable. This issue is solved so that those traces are now presented properly
INS-7420	When doing a Scope Acquisition, using a "Sine generator" for Oscilloscope and selecting "Show advanced settings", the "Noisy" checkbox is displayed. However when clicking the checkbox it did not change the state. This is resolved so the selected / deselected state of the "Noisy" checkbox is now reflected in the GUI
INS-7415	Fixed exception caused by using the simulator with "Randomize key" selected when the entered fixed key was invalid.
INS-7401	The east-west direction of the laser spot was inverted. This is corrected so that the east-west direction of laser spot movement for the right-hand side laser port of the Twin Scan now behaves correctly.
INS-7395	Added option to all POI modules to abort execution when too many traces are skipped because of missing input/output data or failed key validation.
INS-7367	Framework 1 modules support for icWaves is reintroduced.
INS-7346	Several modules, e.g. Spectrum, Spectral, Harmonics, Resample, Sync Resample, did not produce the correct result or threw exceptions when used in chain during acquisition when they were not used as top modules in the chain. The behavior of these modules is changed so that they can be used in a chain also when not a top level module
INS-7336	Renamed all RF Tracer occurrences in Inspector manual to CleanWave.
INS-7224	In some situations the first trace produced by Picoscope 3000 or 5000 was incorrect. A enhancement has been made so that the 1st measurement of PicoScope is now useful.
INS-7221	Increased First Order Analysis key iteration speed (up to 5 times for small traces).

Riscure BV Delftechpark 49 2628 XJ Delft The Netherlands Phone: +31 15 251 40 90 Fax: +31 15 251 40 99 E-mail: inforequest@riscure.com
www.riscure.com Chamber of Commerce: 27287509 VAT: NL815984753B01 Bank: ING The Netherlands 68.35.07.338 IBAN: NL 69 INGB 0683507338

Riscure Inspector 4.12 Release Notes

INS-7111	Added support of the Twin Scan module by integrating Twin Scan controller. The Twin Scan can be configured via Hardware Manager. Selection can be done via Perturbation 2 module. There is a test laser pulse repetition button and a go to origin button available.
INS-7095	Extended Framework 2 for icWaves 2 so that is accepts a max. acquisition trigger timeout to 30 seconds.
INS-7094	The camera interface in 'Tools > Open Camera View' is now similar to the camera interface in 'Perturbation2 module > Camera'. Additionally when camera is used in the tools menu it now stays available in perturbation.
INS-7030	Added AES-128 leakages of Hamming Distance between last round input and output for First Order Analysis, Known Key Analysis and the Simulator in the normal view, instead of only in the expert view
INS-7006	The glitcherIsFinished() method is updated. The polling interval of glitcherIsFinished() method in TriggeredPerturbation module is reduced from 100ms to 1ms so as to improve perturbation module performance.
INS-6890	XY Intensity Plot and XY Average Plot will remain open and functional until explicitly closed by user. Previously these plots were automatically closed by starting a new module.
INS-6884	On low resolution displays not all fields from the module window where visible. Scroll bars are added to module window when it is not big enough to show its content.
INS-6881	In perturbation2 it was not possible to disable the display of the communication. A checkbox is added on the Perturbation2/Acquisition2 target tab so that the user can enable/disable the communication log
INS-6876	When running multiple instances with long CPU-intensive processes, Inspector sometimes lost the license key and the only way to recover was to restart Inspector. Inspector now will recover from losing the license dongle temporarily, without having to restart.
INS-6858	Due to hardware limitations, sequence needs a minimum of 4ns as glitch offset. When a user specifies a glitch offset less than 4ns for VC Glitcher in perturbation2 modules, the user will get a warning.
INS-6842	FirstOrderAnalysis now will return the result traces on abort instead of discarding them.
INS-6838	User can now fill in an arbitrary range value for Lecroy oscilloscopes. In this case the Lecroy oscilloscope will use the closest supported range to do trace acquisition.

Riscure BV Delftechpark 49 2628 XJ Delft The Netherlands Phone: +31 15 251 40 90 Fax: +31 15 251 40 99 E-mail: inforequest@riscure.com
www.riscure.com Chamber of Commerce: 27287509 VAT: NL815984753B01 Bank: ING The Netherlands 68.35.07.338 IBAN: NL 69 INGB 0683507338

Riscure Inspector 4.12 Release Notes

INS-6718	Inspector is upgraded to Java 8 version 1.8.0_121. Note: Not all Java 8 language features for development may be available.
INS-6707	The loading and saving of Chain parameters now also includes sample and trace selection
INS-6706	The state of "Advanced settings" check box is now kept persistent in the target tab of a protocol acquisition / perturbation module.
INS-6703	Fixed a bug that enabled Inspector to proceed with SCP protocol when an intermediate response is 61 XX.
INS-6670	Two alignment modules can be used correctly in a chain also when those alignment modules are not placed directly after each other.
INS-6664	The font sizes used Inspector now will scale accordingly to the user's Operating System font settings.
INS-6663	In serial communication when a timeout < 100ms is specified, the system operates normally instead of hanging
INS-6621	A new feature is added that enables you to log the Out and Log windows of Inspector to a text file.
INS-3893	Several instability issues fixed with regard to the use of the Spectrum module in combination with the chaining function in Inspector. Chaining can now be used in combination with the Spectrum module: - When there is an Acquisition 2 module prior to Spectrum - In chains of the Acquisition 1 modules - In any chain, when there is a Compress module prior to Spectrum

Riscure BV Delftechpark 49 2628 XJ Delft The Netherlands Phone: +31 15 251 40 90 Fax: +31 15 251 40 99 E-mail: inforequest@riscure.com
www.riscure.com Chamber of Commerce: 27287509 VAT: NL815984753B01 Bank: ING The Netherlands 68.35.07.338 IBAN: NL 69 INGB 0683507338