Riscure Inspector 2018.3 Release Notes

Date 4 December 2018

Modified behavior

Issue number	Description
INS-7918	Modified behavior: When using the distribution module when choosing 'get Y range from first trace, in some cases the Y max and Y min values were editable. This is now changed.
INS-8291	Modified behavior: For the perturbation log, Inspector 2018.3 makes use of a SQLite database instead of the PostgreSQL database.
INS-8293	Modified behavior: The Perturbation History is replaced by a Perturbation Log file chooser, since the perturbation module now uses a SQLite database instead of the PostgreSQL DB.
INS-8294	Modified behavior: Since Inspector 2018.3 uses a SQLite database instead of a PostgreSQL database, the Database option is deleted from the Inspector Installer.
INS-8861	Modified behavior: Spider Java classes are now included as Inspector system modules. When compiling any Sequence module operating a Spider device, the system module Spider classes would be used for compilation by default.
INS-8939	Modified behavior: Rounded timing parameters of glitch() method in Spider Chronology class to nearest multiple of 4 to avoid deviation in actual timing generated by Spider device.
INS-8961	Modified behavior: In Inspector 2018.3 the Spider SDK version 1.4.1 is included.
INS-8979	Modified behavior: Fraction sets and Output (the lines containing the “print scores per iteration”, “print training accuracy” and “report interval” options) panels are removed when “Test Phase” is selected.
INS-8986	Modified behavior: to compensate for backlash of EM Probe Station the driver is now implemented in a way that it always approaches a location that you need to navigate to from the same direction. Since backlash of EM Probe Station 3 and 4 is significantly larger compared to EM Probe Station 5, the user can set EM Probe Station generation in Hardware Manager > Create EM Probe Station.

Riscure Inspector 2018.3 Release Notes

INS-9134	Modified behavior: Inspector binary is now compatible with JVM 8 and includes 64-bit JDK8.
INS-9196	Modified behavior: The dongle validity dates are now printed in the dongle report that can be chosen from the Help menu.
INS-9274	Modified behavior: Users can now update their dongle as they could in version 4.12 and before, by pasting a dongle certificate obtained from Riscure into the dialog box. The dialog is accessible from the Help menu and from the Licensing tab in Settings.

Riscure Inspector 2018.3 Release Notes

New features

Issue number	Description
INS-8292	New feature: Inspector 2018.3 now uses a SQLite database instead of an PostgreSQL database to store perturbation results. The installation includes a tool to migrate perturbation logs from the legacy PostgreSQL database to the new SQLite database files. Please read the manual for additional information.
INS-8947	New feature: Inspector 2018.3 has a pipeline module added to increase performance. The pipeline module works like the 'chain' module where you can create a set of modules that run subsequently. The pipeline module though runs the modules added to a sequence in parallel instead of subsequently and in this way speeding up the process. Please check the manual for details on how to use this new module.
INS-8985	New feature: The new EM probe station as well as EM probe station 4 will always use the highest resolution possible for the setting of the micro step size. This will result in the smallest possible step size when using EM probe station.
INS-9116	New feature: Inspector 2018.3 features a complete new way to visualize the results of a fault injection session. The product used for the visualization is Riscure FI Spotlight and is installed automatically when Inspector is installed. The manual is extended with several chapters on this new product and the tutorial is as well. To get the most out of this new product please read these documents carefully. FI Spotlight makes use of a SQLite database, FI results from previous sessions stored in the PostgreSQL database must first be converted with the conversion tool that is available in Inspector 2018.3.
INS-9186	New feature: For subscribers to the premium analysis package, Inspector 2018.3 includes an option to run 10 Inspector agents in parallel by using Inspector HPA (high performance analysis). Users will be notified of this options in a startup dialog and referred to the manual for detailed information on how to setup Inspector HPA.
INS-9319	New feature: Inspector 2018.3 features support for Tektronix oscilloscopes. Oscilloscopes of the 5000 and 7000 Tektronix series are supported. Support is implemented based on the implementation of a Visa driver and Inspector supports fast frame acquisition mode. Please read the manual for all details on the usage.
INS-9360	New feature: The new Python FI framework is shipped with many example script that you can find in the example_scripts directory. The

	scripts in this folder are read-only and can be copied to your working directory to work with.
INS-9416	New feature: A module for correlation collision attacks has been added to Inspector. The core idea of the attack is to exploit the fact that the same value after SubBytes lead to similar side channel leakages for different bytes of the input. In Inspector 2018.3 this attack can be done on AES. Check the manual for details on how to use this new feature and the tutorial for a walk through.

Fixes

Issue number	Description
INS-8240	Fix: Fixed issue that settings from the icWaves configuration were multiplied by arbitrary values when opening the configuration dialog again.
INS-8333	Fix: In Inspector 2018.3 we fixed an issue that caused an incorrect update of field strength instead of frame waiting time for Micropross 300.
INS-8785	Fix: When the user started Inspector without the dongle connected and then connected it, exception messages were printed in the Log window. This is now resolved.
INS-8854	Fix: Fixed issue with relative paths for the VisualizeTemplates module and for external reference trace sets for alignment modules. Previously, only a simple relative file name, but not a relative folder path could be used
INS-8862	Fix: When the neural network file name was changed in the Deep Learning module, the cursor moves to the end of the line after each character entered. Now the cursor no longer jumps to the end of the line when typing in the filename field
INS-8863	Fix: When Key Loading is selected in the Deep Learning module, the key field no longer goes missing in the Training & Validation phase, when 'Unknown key' is selected in the Test phase.
INS-8864	Fix: There is a tooltip added to the deep learning GUI to clarify that the number of iterations depends on the number of traces, training fraction and batch size.
INS-8968	Fix: The newer PicoScope 3000 models have an 11 digit serial number that caused an error when using the PicoScope in acquisitions. This issue is now solved.
INS-8973	Fix: When using the PicoScope 3000to measure, the threshold for the trigger in the UI is off significantly. This was not always a problem but in the case of a noisy trigger line it may trigger too early. This issue is now fixed.
INS-8978	Fix: In the DES leakage models with the Deep Learning the cursor jumped to Round In XOR Round Out every time the module is opened.

	This is now fixed.
INS-8980	Fix: The progress bar during hyper-parameter search only took into account the first searched model, and remains at 99% for the rest of the execution. This is now fixed.
INS-8981	Fix: In the Deep Learning module when PUBLIC_KEY was selected with the hyper-parameters search option, the processor (that converts results into algorithm result) was not reinitialized and threw a null exception. This is now fixed.
INS-8982	Fix: In Inspector 2018.3 we have fixed an issue which caused wrong results when key ranking was used a as termination condition for a hyper parameter search in Deep Learning.
INS-9056	Fix: Acquisition with a smartcard plugged in a laptop smartcard reader threw an error. This is now fixed.
INS-9057	Fix: Saving and loading of parameters for chains with First Order Analysis failed with NPE. This is now fixed.
INS-9081	Fix: When unplugging a USB device (such as a memory stick), Inspectors hardware detection thread could crash and would no longer accept new hardware causing an IndexOutOfBounds exception. This issue is now solved and no longer an IndexOutOfBounds exception is thrown when unplugging USB device.
INS-9208	Fix: In some cases, deep learning analysis was very slow on machines with many cores (a lot slower than on machines with fewer cores). This has been fixed. The solution adopted was to set the value of the OMP_NUM_THREADS environment variable used by Inspector to 1 in order not to interfere with the OpenBLAS library used by Inspector which is already multithreaded.

Riscure Inspector 2018.3 Release Notes

Known issues

Issue number	Description
INS-9431	Bug: On systems with Java SE 8u171 and higher, the start menu entry for the Inspector uninstaller may launch Inspector instead of the uninstaller. Inspector can still be uninstalled by launching Uninstaller.jar from the Inspector installation folder.

Questions and Support

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

https://support.riscure.com/