go2signals

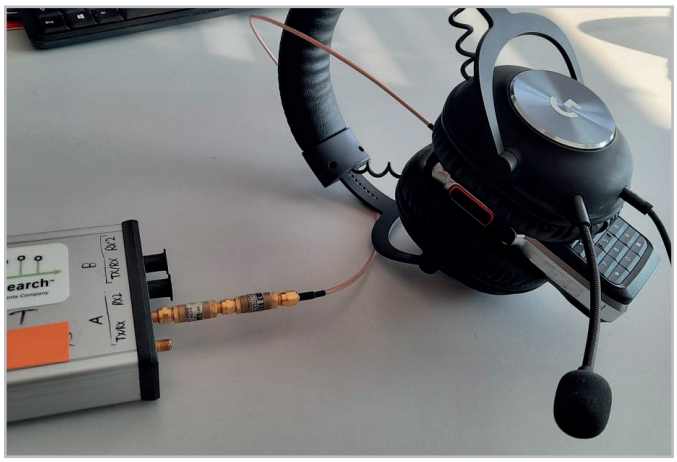
RELEASE NEWS
VERSION 23.2

PROCITEC®
HOUSE OF SIGNALS

NEW PRODUCT:
go2key - DMR ARC4 key finder

Digital mobile voice radios (PMR) are currently of great interest due to their worldwide use, especially in security-relevant environments. Most radios are able to use encryption methods to protect their user groups. In order to be able to listen to encrypted voice, go2signals offers the possibility of decryption in its decoders. Depending on the used encryption method, the required keys are automatically detected (e.g. DMR Motorola Basic, Alinco, Hytera Basic) or can be manually entered by the user.

As one of the first providers, PROCITEC now offers with this new release 23.2 the possibility to automatically detect the keys for ARC4 (e.g. Motorola Enhanced) encryption of DMR radios.



Recording of DMR test signals

The new product required is called go2key. The input is a short recording of the data output (typically 1-4 sec) of the DMR decoder. In this data go2key searches automatically for the used keys. With the help of special statistical methods developed by our decoding specialists, a result is determined extraordinarily quickly. Despite the high number of about 1.1 trillion possible keys, a search usually takes only up to 1 hour (on a high-end server, up to 12-24 hours on a standard laptop).

```
                                /DMR_ARC4$ ./go2key crack -a -k 209  20180201-141406-951__0000000000_D01.json
 0.003%     9332613 keys/s   remaining: 1 day, 8:43:30.202220  (0x0002100000)
 0.006%     9349522 keys/s   remaining: 1 day, 8:39:53.548669  (0x0004000000)
 0.009%     9352489 keys/s   remaining: 1 day, 8:39:12.655331  (0x0006100000)
 0.012%     9355258 keys/s   remaining: 1 day, 8:38:34.275018  (0x0008100000)
 0.015%     9357230 keys/s   remaining: 1 day, 8:38:05.923403  (0x000A100000)
 0.018%     9363463 keys/s   remaining: 1 day, 8:36:44.132703  (0x000C100000)
 0.021%     9362931 keys/s   remaining: 1 day, 8:36:47.219831  (0x000E000000)
 0.025%     9363110 keys/s   remaining: 1 day, 8:36:41.391604  (0x0010000000)
 0.028%     9362229 keys/s   remaining: 1 day, 8:36:48.855232  (0x0012200000)
 0.031%     9363337 keys/s   remaining: 1 day, 8:36:31.378189  (0x0014000000)
 0.034%     9366262 keys/s   remaining: 1 day, 8:35:51.135431  (0x0016100000)
 0.037%    10049121 keys/s   remaining: 1 day, 6:22:53.643187  (0x0017F00000)
 0.038%     9367807 keys/s   remaining: 1 day, 8:35:26.408283  (0x0019100000)
------------------------------------------------
KEYS FOUND: 0x0019751987
------------------------------------------------
```

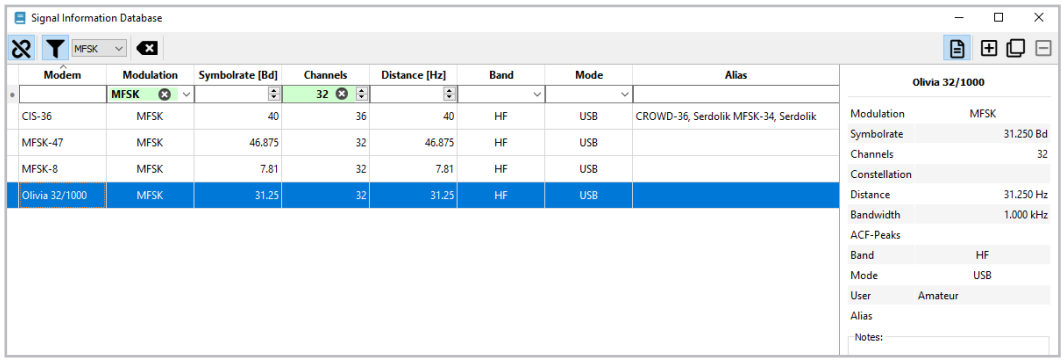
Find Motorola Enhanced ARC4 encryption keys in DMR decoder output

The results are 10-digit keys which can be stored in the DMR decoder as decoder parameters. Thus all recorded, current and future DMR ARC4 emissions by this user group can be decrypted, enabling real-time decoding and monitoring of the speech content.

SIGNAL ANALYZER ENHANCEMENTS

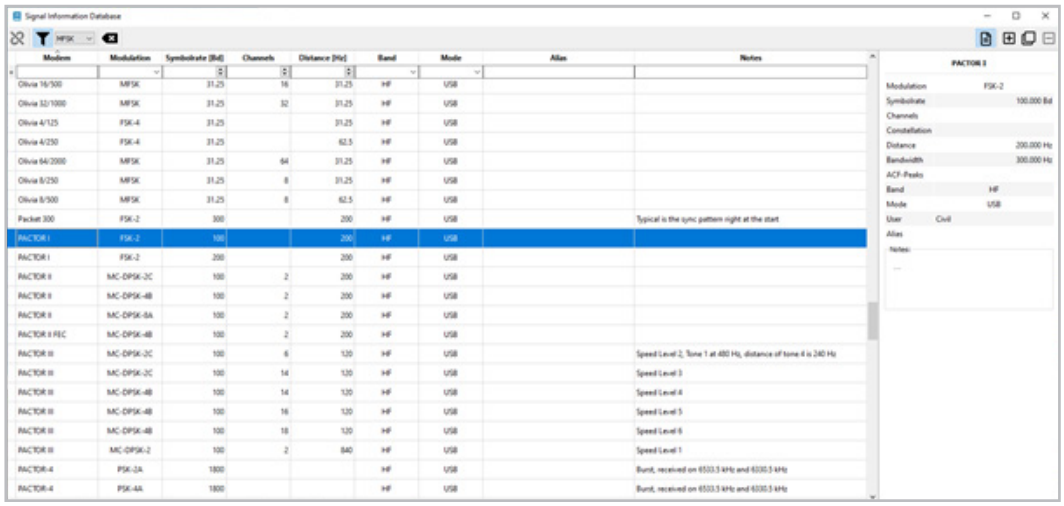
SIGNAL INFORMATION DATABASE

In order to quickly access existing knowledge during the analysis and to compare the results with known signals, Signal Analyzer now offers an integrated database. Measured parameters are automatically used with this new feature, the Signal Information Database.Measured parameters are automatically used with the next new feature, the Signal Information Database. Filtering the database with the parameters provides a quick indication of the signal type, its parameters and usage.



Get the signal type from the Signal Information Database using the measured parameters

The database comes with a first set of around 250 entries from communication signals and their different modes used mainly in HF and VUHF frequency range. The users are able to edit its content and add their own signal entries.

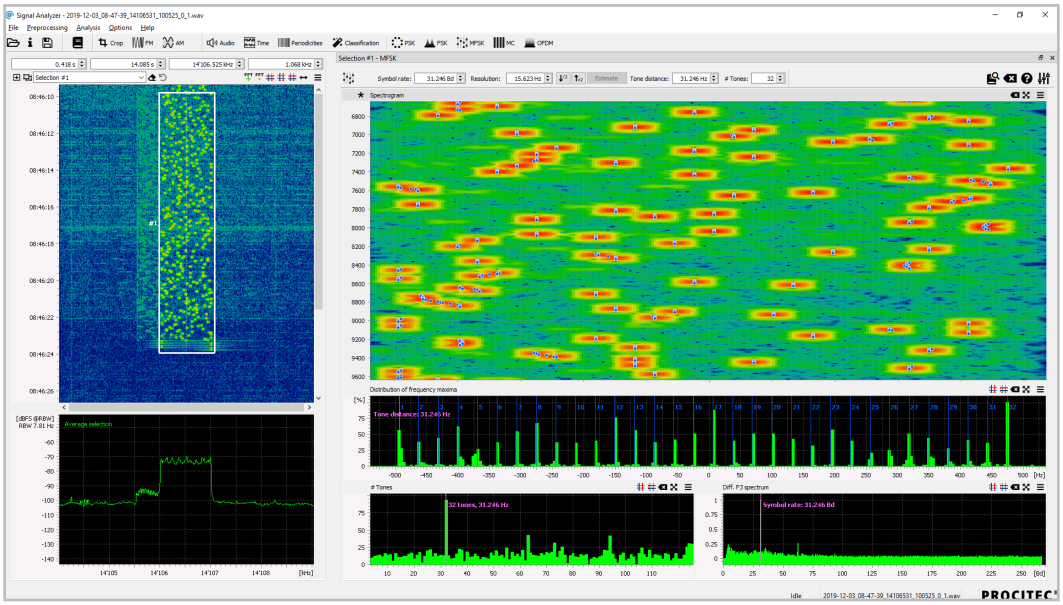


The Signal Information Database starts with a first set of around 250 modems and modes

SIGNAL ANALYZER ENHANCEMENTS

NEW ANALYZING TEMPLATE FOR MULTITONE (MFSK)

Going further with our second new software product Signal Analyzer we added a new template to analyze Multitone (MFSK) modulated signals. With this template, signal parameters such as tone count, tone distance and symbol rate are measured in a simple and accurate way.

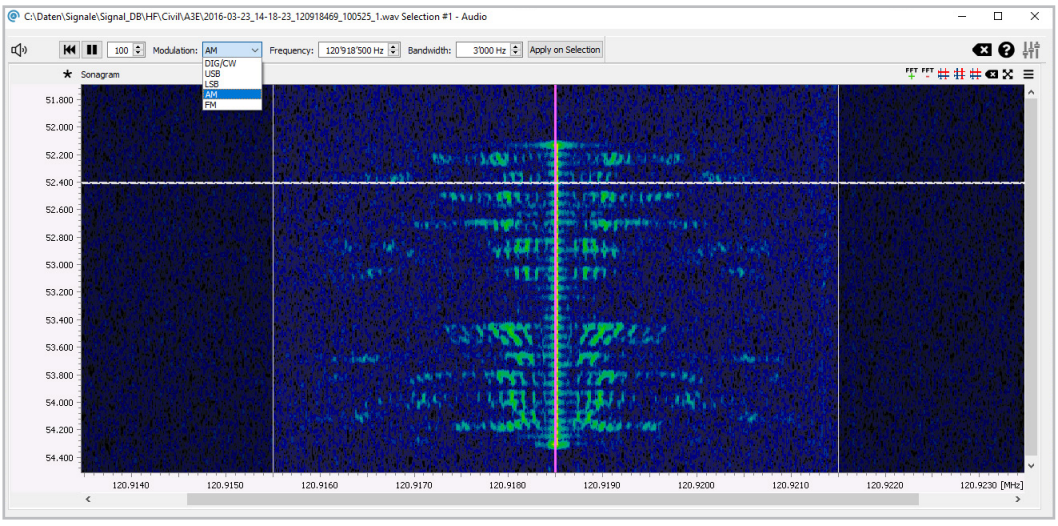


Multitone analysis: Just select the signal in the recording and you get all modulation parameters

AUDIO PLAYER FUNCTION

Another new feature in the Signal Analyzer is the audio player function. It can be freely parameterized by setting start and end time as well as its center frequency and bandwidth. Its demodulation modes are CW, USB, LSB, AM and FM.

This enables the user to listen to speech signals or to categorize a signal by its sound.

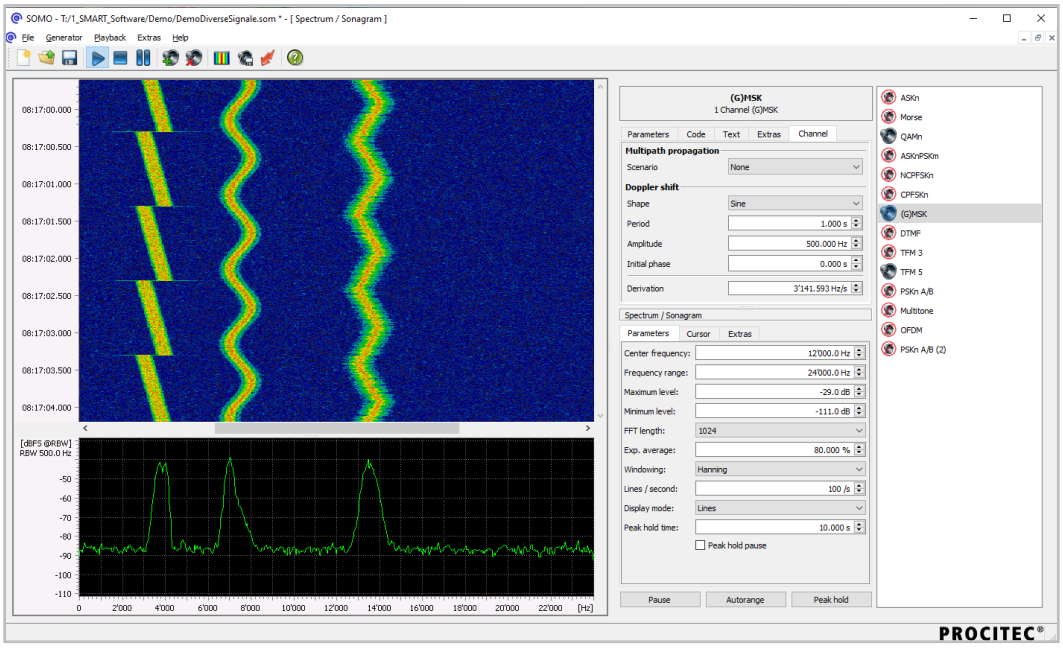


Signal Analyzers audio player listens to an AM signal

SOMO ENHANCEMENTS

SIMULATE DOPPLER SHIFT WITH SOMO SIGNAL GENERATOR

In the case the sender or receiver of a signal are moving, the center frequency of the signal shifts according to the difference speed (Doppler shift). SOMO is now able to simulate this effect with different parameters to each generated signal for a maximum of flexibility. Shape type, period, amplitude and initial phase are parametrizable.



Example of multiple signals with a strong Doppler shift and different shape types

ANALYSIS SUITE

Technical Specifications Document
www.procitec.com/go2signals-specifications-analysis

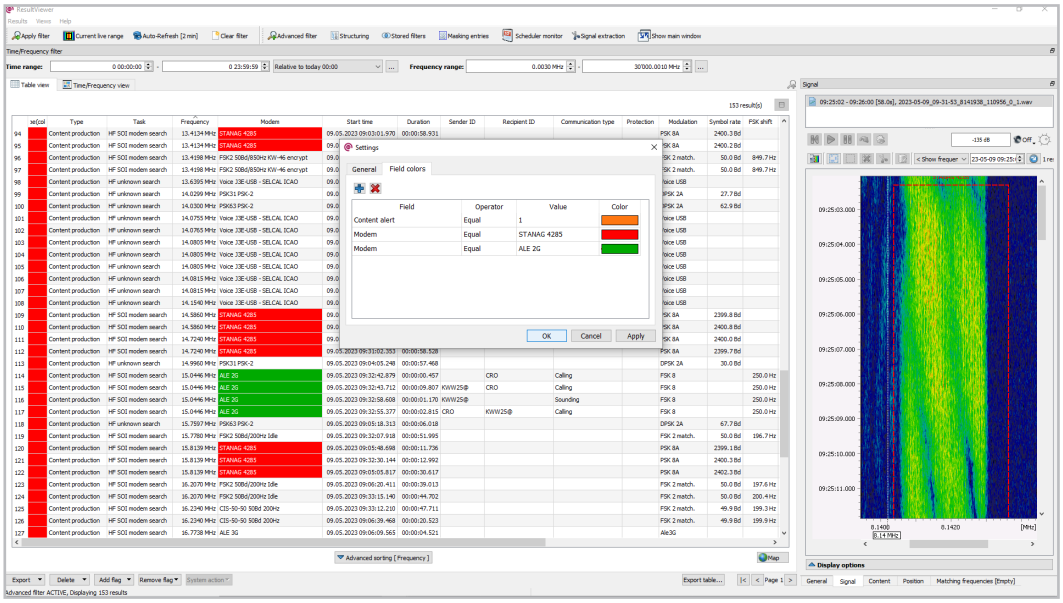
DECODERLIST

List of all available Decorders
www.procitec.com/go2signals-decoderlist

GO2MONITOR ENHANCEMENTS

MARK CELLS USING USER-DEFINED RULES IN RESULTVIEWER

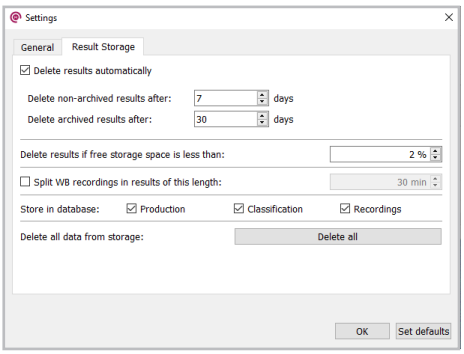
Cells in ResultViewer result table can now be colored based on user-defined rules, depending on the column and values in each field. This gives the operator the opportunity, for example, to highlight important content and thus make it easier to see.



Example how to mark result cells (modem type) based on their content

RESULTS ARCHIVE WITH LONGER STORAGE TIME

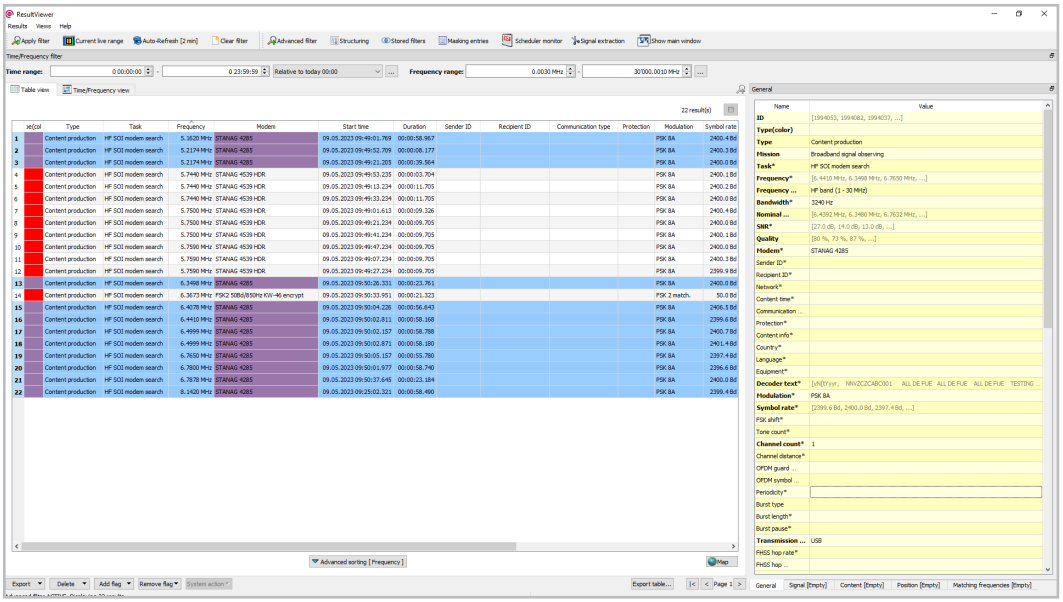
go2MONITORs database stores different types of results like classification parameters, demodulated bits, decoded content (e.g. text, voice, files), post-processed results etc. To avoid storage overflow, automatic deletion can be parametrized. Marking results with an “archive” flag, they are now stored in a result archive with different, longer storage time.



Setting different storage time for results in archive

BULK-EDITING WITH RESULTVIEWER

For manual post processing and signal parameter adapting, ResultViewer has the possibility to edit automatic generated result. With this new release it is now possible to edit multiple results at once using general details tab (bulk-editing).

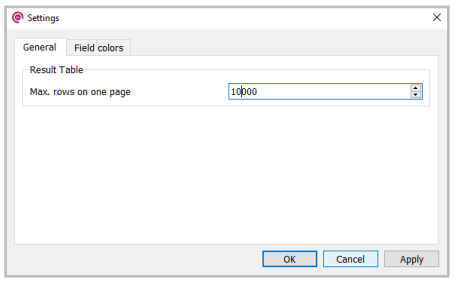


Selecting and editing of multiple results

SETTING A HIGHER LIMIT OF LINES PER TABLE PAGE

To keep the time for a display update short and thus the usability high, the number of results shown in one table page in the ResultsViewer is limited to 1000 lines as default.

On computers with sufficient performance and a fast database connection, this default can now be set to higher values in the settings dialog.



Setting a higher limit of lines per table page

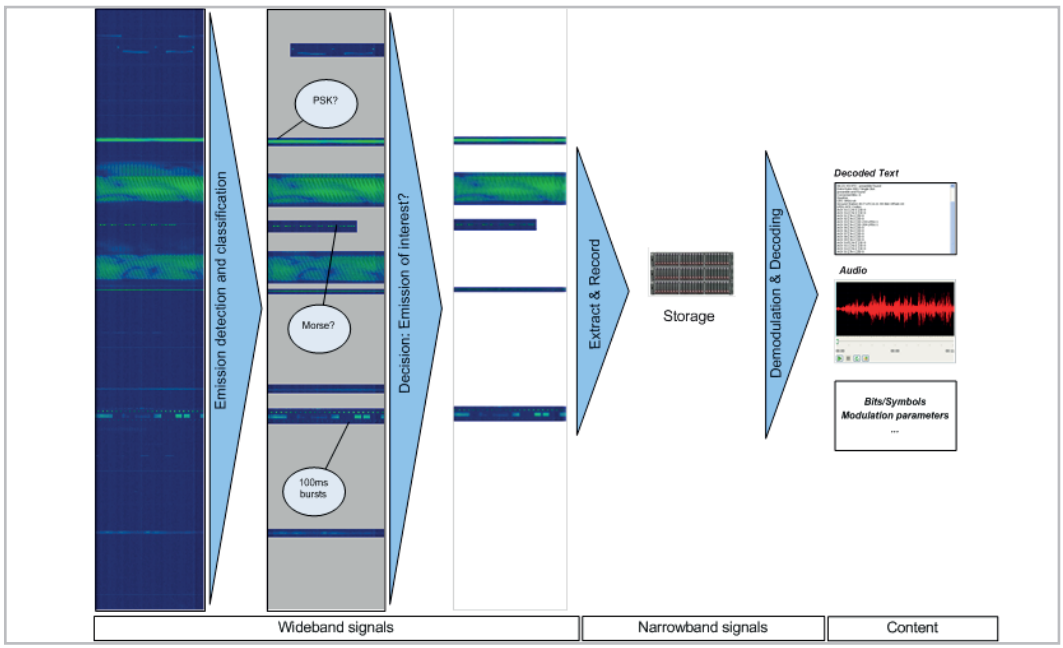
CLASSIFIER ENHANCEMENTS

The signal classification in the go2signals software works both in the wideband input with many parallel concurrent emissions and in the narrowband channel, processing only one emission. In both cases the classifier is able to track signal behavior, measure modulation type and its parameters and even detects known modem types.

With the previous version we started to support signals with very large bandwidths not only in the modem classification but also in the modulation classification. With this release, OFDM classification has been extended to work on signals with a bandwidth of up to 12.5 MHz.

Release changes:

- Add new modem classifier for CIS 60
- Add new modem classifier for CIS Akula
- Add new modem classifier for Link 22
- Enhance classification of OFDM signals up to 12.5 MHz bandwidth



Use of classification results in go2signals to filter for Signals Of Interest (SOIs)

MONITORING SUITE

Technical Specifications Document
www.procitec.com/go2signals-specifications-monitoring

DECODERLIST

List of all available Decorders
www.procitec.com/go2signals-decoderlist

DECODER AND DEMODULATOR ENHANCEMENTS

One of the core functions of go2signals is the demodulation and decoding of different modem signals. With over 350 modems and modes, a wide range is already available to the user today. To keep up with the evolving signal world, we have also added new functions with this release.

DEMODULATOR NEWS

- FSK discr.: Parameter shift is now interpreted as distance between neighboring frequencies instead of distance of the outer tones
- PSK/QAM: Number of symbols for initial synchronization was previously dependent on channel filter length
- PSK2A: Improved burst detection
- PSK2B: Improved symbol synchronization

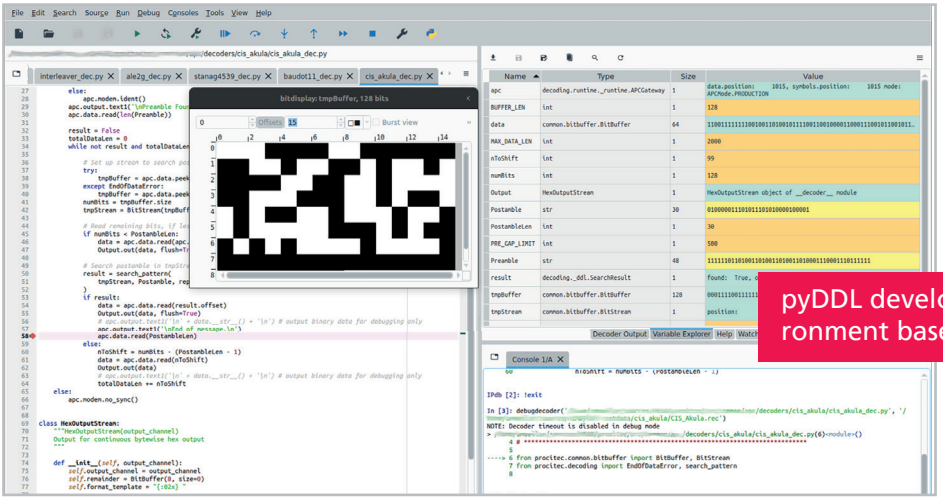
DECODER NEWS

- CHN MIL Hybrid 8FSK-PSK
  - Decoding of MFSK and QPSK part
  - Moved to MIL decoder package
- Added detection of KW-46 encryption in several decoders
  - STANAG 4481 FSK
  - STANAG 4285
  - STANAG 4415
  - STANAG 4539
  - STANAG 5065
- STANAG 5065: Distinguish modes FSK 75Bd 85Hz and FSK 50Bd 850Hz
- Morse:
  - Detection of call sequences and call signs
  - Detection of telegram end
  - Detection of parameterizable words/codes (e.g. Q-Codes)
  - Suppression of single characters with bad quality
- CIS Akula: Added decoding and output of raw data
- Clover: Postprocessing of Clovermail
- Motorola Smartnet: Added frequency range 380-520 MHz (ASTRO P25)
- ALE3G: Added binary reassembly of fragmented data units
- DMR Burst: Improved sideband detection
- Tetra Uplink: Split production into info units (optional)
- Link22: Improved burst end detection
- Distress Radiobeacons: Improved signal detection and synchronization

NEW DECODER DETECTION FEATURES:

- Added detection of ENAGAL Buoy HF Link
- Added detection of Datawell Buoy 2FSK HF Link

PYDDL NEWS



pyDDL development environment based on Spyder

With this release we have completed the last step of the porting from DDL to pyDDL. All included decoders are now available in pyDDL as language (source code mostly included, see decoder list).

To enable our customers to add their own decoders and detectors, the go2signals software has its own decoder development environment. Due to the change to pyDDL, standard programming commands from the Python language are included in addition to the special commands for decoding.

ADDITIONAL PYDDL FEATURES

- Decoder parameters:
  - Added option to use list or 2D-tables
- Demodulator parameters:
  - Added access to primary modulation setting
- New BitBuffer utility functions:
  - BitBuffer.from_iter: creates a new bitbuffer from multiple integer values
  - BitBuffer.split_to_array: creates numpy.ndarray from bitbuffer
  - BitBuffer.__setitem__ / BitBuffer.__getitem__: multiple individual bit access

UPDATED DECODERS TO PYDDL

- ALE3G
- Clover II / 2000

ADDITIONAL NOTEWORTHY CHANGES

- „Source“ result field now contains information if the result originates from a manual channel, including the user name of the user who created it, in the form of „[Manual:username]“
- New function allows NB-channels to be assigned to AMT tasks. In that case, all results from those NB-channels will be marked as results from the assigned AMT-Tasks
- Matching results with recordings is no longer an internal function of the ResultViewer. The whole process is automated and performed in the system for all results. Result flag „Result matching“ is provided to check if this matching has been performed or not
- New Scheduler functions are provided to export or import frequency lists automatically. This can be used to exchange frequency lists between two systems
- Multiselect-Combobox GUI component has been improved (easier filtering, design), and is now used throughout the GUI
- New optional function to report various system parameters and performance values to an external nagios/checkmk monitoring system (custom configuration needed)
- New functions in Wideband Input spectrogram, Result Viewer and NB-channel to create a new fixed-frequency AMT task by using predefined frequencies from the current context
- Continuous wideband classification will now only be used if there are actual search tasks which require that function in a certain wideband input. Antenna information is also considered for that decision
- Blocked frequencies for wideband classification are now displayed only in the bottom of the spectrogram
- New result field „Last Editor“ is automatically filled with the user name of the user who made the last change on that result
- New „Copy task“ function in Mission View
- Multiple tasks can now be imported in TaskOverview at once
- Task Overview filters can now be saved in a file and loaded later to restore filter settings
- Y-axis can now be turned on or off in the NB-channel spectrogram
- Automatic range adjustment can now be turned on or off in spectrograms in Wideband Input and NB-channel
- Besides filtering on specific Tasks, ResultViewer now also includes a filter based on task name (string with wildcards)
- Frequencies and Frequency groups are now updated automatically in the GUI if they change in the database (for multi-user installations)
- Hopper-Detection function now reports some monitoring values which are visible in the Resource View
- There is new system function to split results (recordings, productions, ...) automatically after specified time. This function is available for custom configurations only. Standard configuration splits all recordings after 1h
- Performance optimization: Database, Messaging, Frequency-Views, Task-Overview etc.

PROCITEC®

HOUSE OF SIGNALS

PROCITEC GmbH
Rastatter Strasse 41
75179 Pforzheim
Germany

Phone +49 7231 155 61-0
Fax +49 7231 155 61-11
sales@procitec.com
www.go2signals.de / www.procitec.com

23.2 I 06/2023 (Subject to modification)