AUTOTRACE

A device for anomaly detection in complex industrial and automotive networks

Based on the innovative Xilinx Systems-on-Chip (SoC) approach, the company ***EUROS Embedded Systems GmbH* (EUROS)** offers Asymmetric Multiprocessing (AMP)-based solutions bridging the hard real-time requirements – covered by its RTOS EUROS - and the need for cloud-enabled processing capabilities offered by a Linux-System, like Debian.

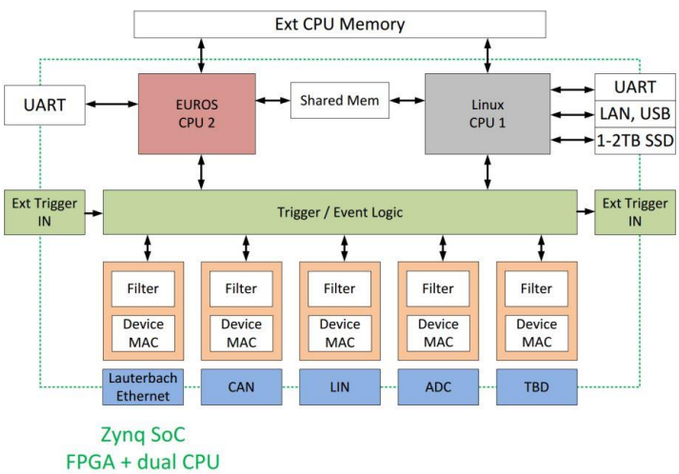
EUROS has created a unique industrial device for anomaly detection in complex industrial and automotive networks - referred to as ***AUTOTRACE***. The latter is built around the SoM-K7 hardware platform of the company ***solectrix GmbH*** and is equipped with two ARM Cortex A9 cores.

An eventual abnormal program behavior can be only detected by comparing the nominal program behavior with the actual one. For this purpose, relevant data must be constantly collected and analyzed. The final step in the process is to locate and eliminate the cause of the detected anomaly by taking and analyzing program traces from the microcontroller itself.

Thus, one of the primarily intended usage of the ***AUTOTRACE*** is to selectively collect and analyze data traces gathered from digital and analog sources in distributed embedded systems. The ***AUTOTRACE*** device is connected to a so called 'System under Observation' (SuO) and can be programmed for the performing of the following modes of operation:

Collecting external traces:

The first phase of the analysis process is the acquisition of external traces using a special application referred to as ***Trace Manager***. In this context '*external*' is referred to the available signals or communication data and, if possible, also contents, including ADC, CAN, LIN, TSN, sensors, etc. outside of the microcontroller.



Anomaly detection:

After collecting and processing the gathered data, the ***AUTOTRACE*** provides the user with information on eventually detected anomalies based on a previously generated nominal behavior model by using machine learning algorithms. For this purpose, a special application referred to as '***Embedded Verifier***' is employed. However, data collected solely for recording purposes don´t necessarily have to be checked for abnormalities.

Collecting internal traces:

In case of a detected anomaly the next step is to pinpoint the reason causing it. Therefore the internal behavior of the SuO must be investigated. In this context '*internal*' means collecting of microcontroller program traces to be used for code inspection in order to find the cause of the detected anomaly. For this purpose, a JTAG debugger integrated into the ***AUTOTRACE*** is employed. By using parallel build-in microcontroller circuitry the internal traces are collected synchronously with the currently running program without any interferences.

Due to the large amount of data that could potentially be generated by the embedded environment under observation, ***AUTOTRACE*** primarily collects and if necessary, stores only such data, which are relevant for the purpose of the recording as specified by the user. For this purpose, the ***AUTOTRACE*** deploys configurable trigger and filter mechanisms.