1 IoT Sensor Solution Kit sensry ganymed®

Revolutionized New Platform for All Integrated Smart & Secure Sensors

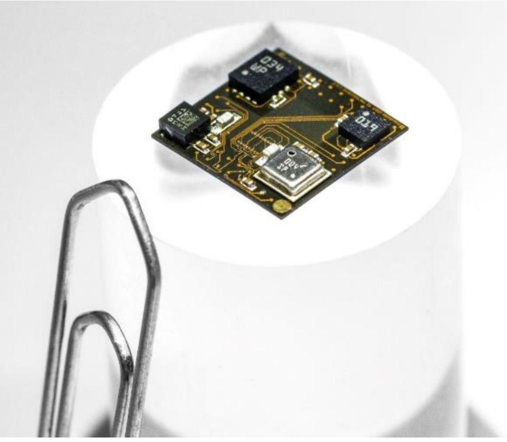
Next generation applications in logistics, robotics, automation, smart home and building, consumer and white goods, smart city and renewable energy require the adaption of smart and secure sensors with data connectivity. Existing semiconductor standard solutions often provide insufficient flexibility and missing software environment. The most critical item, however, is the missing inherent data security approach encompassing the complete value chain of the product.

The Solution

Sensry a newly established company offers an individual sensor node with highly flexible and customizable hardware configurations according to customer requirements. The universal sensor platform USeP combines cutting-edge assembly and packaging technologies with new design methods as well as various integration possibilities for sensors.

Main Product Features

- Integration of various sensors
- Support of multiple communication standards
- Low power consumption
- RISC-V performance for smart node computing
- Adequate memory resources
- Inherent multi-layer data security and authentication
- Very fast design using standard library HW chiplets
- Smallest form factor due to advanced 3D-packaging
- Available software toolchain
- Integration in fog, edge and cloud computing



Key features

- **Selection of Top-Level sensors**
  - Acceleration
  - Gyroskope
  - Magnetometer
  - Vibration
  - Temperature
  - Pressure
  - Humidity
  - VOC
- **RF tranceiver on Bottom-Level**
  - 2,4 GHz WiFi Tranceiver
  - 2,4 GHz Bluetooth Tranceiver
- **Application processor on Mid-Level**
  - RISC-V based cluster core (max. 400MHz)
  - 1 RISCY Data acquisition Unit (DAQU)
  - 8 RISCY Data Proc. Units (DPU) with FPU
  - Event bus
  - DMA
- **Security features**
  - Crypto Co-Processor
  - Secure Boot ROM
  - Secure MRAM / SRAM
  - True Random Number Generator (TRNG)
  - One-Time-Programmable Memory (OTP) for Keys and Certificates
- **Interfaces (Mid-to-Top, Mid-to-Bottom-Level)**
  - 1 HyperBus (for external RAM/Flash)
  - 3 UART (up to 2Mbit/s, two of them with hardware handshake)
  - 4 I2C (up to 400kHz)
  - 4 I2S
  - 7 SPI (up to 50MHz)
  - 1 CAN-FD
  - 1 RGMII with MDIO for Ethernet-Phy
  - Debug JTAG | System JTAG
  - 1 25MS/s 12bit SAR ADC
  - 1 100kS/s 11bit ultra low power SAR ADC
  - 1 16Bit Sigma Delta ADC (Audio)
  - 32 GPIO (configurable for 1.8V or 3.3V operation)
  - **Each interface (except GPIO) can be induvidually disabled for power saving**
- **Memory**
  - 512kB MRAM (256kB Secure MRAM + 256kB MRAM)
  - 4MB SRAM
  - 256kB SRAM for each core in the DPU (Tightly coupled)

Applications

- **Sensor node for Internet of Things (IoT)**
  - Home automation
  - Sensor networks
  - Building automation
  - Condition monitoring
  - Retro Fitting
  - Industrial applications
  - AI related applications
- **Authentication and security devices**
  - Identification key
  - Secure sensor data harvester
  - Secure blockchain wallet

Data and specifications are preliminary and subjects to change without notice

Content

2 Revision history

Date	Version	Description
December 2018	V1.0	Initial Document
January 2020	V1.1	Add Electrical Chracteristics (3.3.1) Add Analog-Front-End (3.3.2)
February 2020	V1.2	Add 3D-package Image (first page)

3 System overview

3.1 General system description

The system is considered as an adaptable system in package (SiP) split into a costumer specific Embedded System Layer (Bottom-Level), a fixed Processing Layer (Mid-Level) and a costumer specific variable Sensor Layer (Top-Level). The interface assembly layer connecting Top- and Mid-Level is customizable and can be equipped with a variety of different sensors. The footprint of the chip to the costumer specific system is fixed.

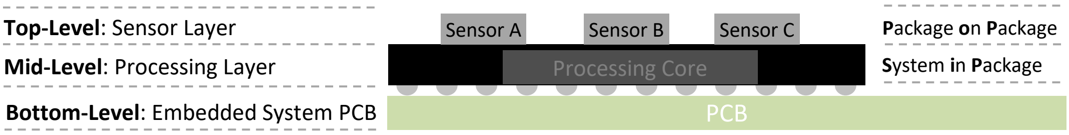

Top-Level: Sensor Layer
Mid-Level: Processing Layer
Bottom-Level: Embedded System PCB
Sensor A
Sensor B
Sensor C
Processing Core
PCB
Package on Package
System in Package

Figure 1: Sensor platform layer description

The system in package (Top- and Mid-Level) will be manufactured in the supply chain of Sensry. The Bottom-Level can be manufactured by costumer or system integration partner of Sensry. The possible workflow is shown in Figure 2.

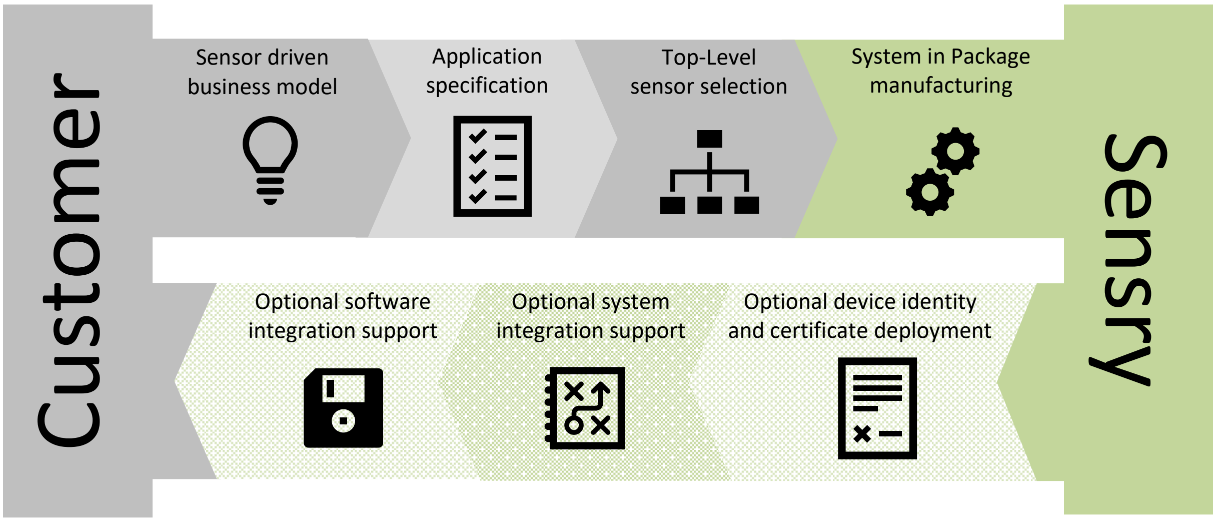

Customer
Sensor driven business model
Application specification
Top-Level sensor selection
System in Package manufacturing
Sensry
Optional software integration support
Optional system integration support
Optional device identity and certificate deployment

Figure 2: Sensry workflow

The device contains a strong security concept which allows to set-up trustful and reliable sensor data driven business models. The hardware integrated security core includes a secure one-time-programmable memory model for the device states, keys and certificates as well as cryptographic functions, security watchdog timer and a secure system boot process. The costumer deployed software must interact with these security features in order to fulfill the desired security standard. The security concept itself is explained in a different chapter.

3.2 Bottom-Level: The interface to the Embedded System

The Bottom-Level consists of the costumer specific PCB design. The System-in-Package will be placed and routed as a normal electronic part. The PCB represents the costumer specific geometric constraints, needed passives and power regulation and additional devices like memory, sensors and RF-bridges. The contract point between Bottom-Level and Mid-Level is the bottom footprint of the system in package which is defined as a standard ball grid array with a pitch of 0.8mm.

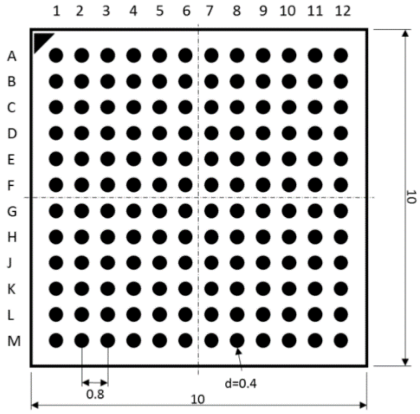


Figure 3: Array Package Outline – BGA 144 Balls, 10 mm x 10 mm, 0.8 mm pitch

The costumer is free to adapted additional sensors, devices o RF-capabilities on the PCB of the Embedded System. Fort a certain number of sensors there will be an integration support by Sensry. This includes the integration in the software application programming interface (Sensor-API). The current subset of supported sensor in the Bottom Level is shown in Table 1.

Table 1: Current sensor support list

Sensor class	Sensor type	Manufacturer	Sensor name
Environment	Microphone	Infineon	IM69D130
Environment	Microphone	STMicroelectronics	MP34DT02
Environment	Microphone	TDK InvenSense	ICS-41352
Environment	Microphone	Knowles	SPH0645LM4H-B
Environment	Humidity	Bosch Sensortec	BME680
Environment	Temperature	Bosch Sensortec	BME680
Environment	Air pressure	Bosch Sensortec	BME680
Environment	Air pressure	Infineon	DPS310
Environment	Temperature	Infineon	DPS310
Gas	VOC	Bosch Sensortec	BME680
Gas	VOC	Sensirion	SGP30
Gas	CO	SGXSensortech	MICS-4514
Gas	CO	Alphasense	CO-B4
Gas	CO2	AmphenolSensors	T6713
Gas	CO2	SGXSensortech	IR11GM
Gas	NO2	SGXSensortech	MICS-2714
Gas	NO2	Alphasense	NO2-B43F
Gas	Particles	Alphasense	OPC-N2
Gas	MOS	SGXSensortech	MICS-5524

3.3 Mid-Level: The Processing Layer

The processing core is based on the Open Source RISC-V instruction set architecture. The implementation consists of a Data Acquisition Unit (DAQU) which handles the wired and wireless communication, security features and memory and the Data Processing Unit (DPU) which consists of eight powerful RISCY processing cores with tightly coupled own memory and separate floating-point units. Additional several interfaces are integrated and distributed to the Top-Level and the Bottom-Level. Figure 5 shows an overview of system interfaces and their connection to the different Levels.

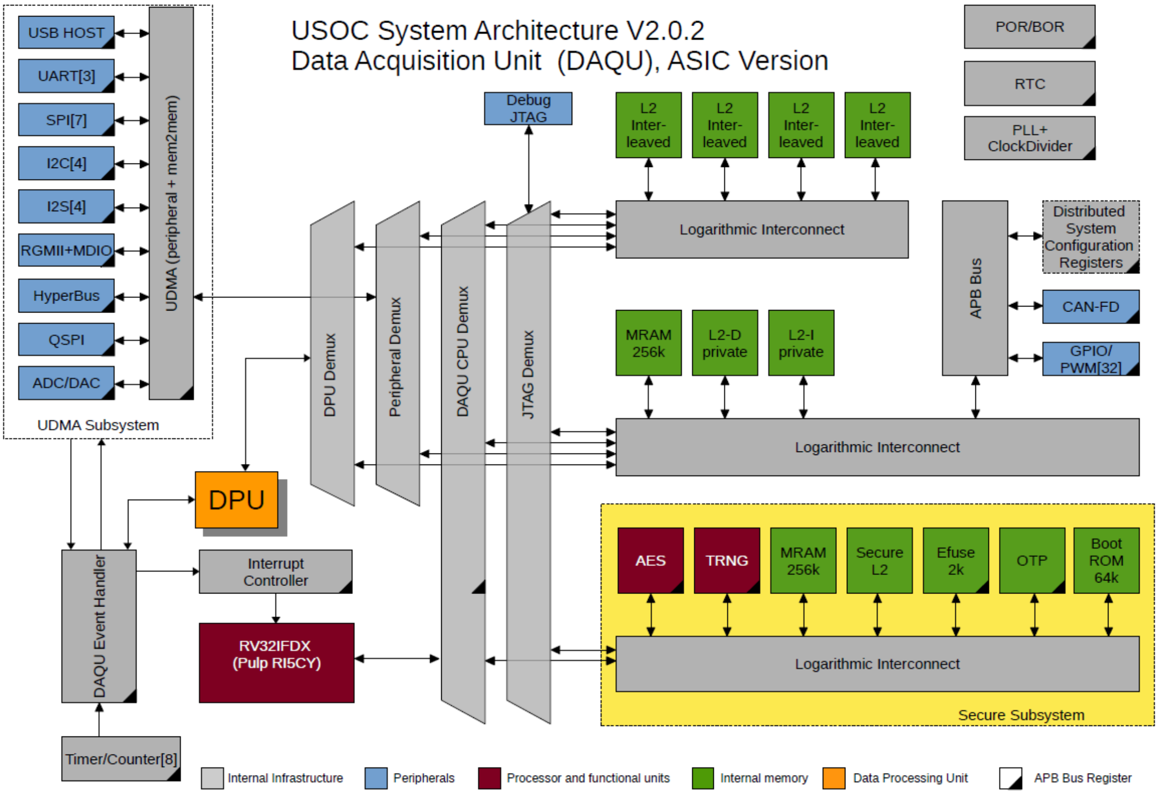


Figure 4: Sensor platform processing core

The processing core is divided basically into a data acquisition unit (DAQU) which controls the interfaces, main memory security subsystem (see Figure 4 for the DAQU schematic overview) and the data processing unit (DPU). The DPU is part of the heterogeneous multicore system and includes eight independent RISCY cores with tightly coupled memory and dedicated floating point units to enhance the system to high performance calculation platform. The DPU is designed to process sensors data independently to the main core and exchange data due to a direct memory access (DMA) controller. This allows to implement computationally intensive operations and data preprocessing needed for Edge and Fog Computing approaches.

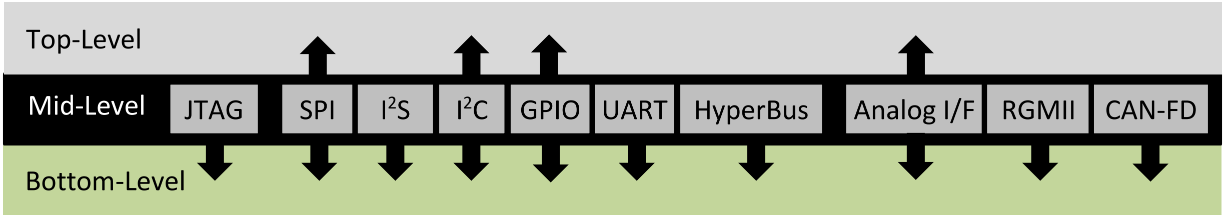


Figure 5: Interface distribution

Beside the standard interfaces like JTAG for programming and debugging, several serial interfaces, GPIOs and the HyperBus for HyperRAM and HyperFlash memory extension, the device includes a powerful analog interface to adapt raw analog sensors. This includes several analog-to-digital and digital-to-analog converter and their matching circuits. The RGMII interface implements a set of IEEE 802 Ethernet sub-standards in order to provide an ethernet time sensitive network (Ethernet TSN) interface. The automotive interface CAN is implemented regarding the latest standard ISO 11898-1 with flexible data rate (CAN-FD).

3.3.1 Electrical Characteristics & Timing

Operating voltages & power

Core Voltage	0.8V
IO voltage	1.8V or 3.3V(*)
MRAM voltages	0.6V and 1.5V
Analog Subsystem voltages	0.8V and 1.8V
Maximum total power dissipation	<1W

(*) Individually configurable by separate voltage supply pins. Some pins have fixed voltages.

Clock Sources

Low power operation clock/boot clock	32kHz
System reference clock(external oscillator)	25MHz
System clocks (internal)	Generated from external clock via PLL, as required for functional units.
CPU clock	400MHz maximum

The CPU clock frequency can be set exclusively by the DAQU CPU core. All DPU cores operate at the same clock frequency (unless disabled), while the DAQU core frequency may be different.

Reset Modes

Five reset modes are available. After reboot, the cause for the previous reset can be read from a status register during boot mode, except for power-on reset:

- Power on reset (POR)
- External reset from a reset input pin (XR)
- Software initiated reset (SOR)
- Brown-out reset (BOR)
- Watchdog reset by watchdog controller (WDR)

The watchdog reset can be issued by an internal watchdog controller.

3.3.2 Integrated Analog-Front-End

The core chip has three different analog-to-digital conversion blocks to allow the processing of a wide range of sensor signals. Each block can be shut down individually for optimized power consumption. A high speed 25MS/s SAR ADC with four parallel sampled inputs is used to convert the multiplexed analog signals with a resolution of 12 bit. It may be used to convert up to 4 parallel sensor signals with 3 MHz bandwidth in normal operation mode or in fast mode a 12 MHz analog signal at channel 0. For ultralow power applications a 100kS/s SAR ADC with 11bit resolution is available for the conversion of sensor signals up to 50kHz. Finally, a high resolution 16bit delta sigma ADC is provided for audio signals up to 16kHz, allowing audio applications like sound activation or speech recognition.

The analogue channels are controlled by the digital controller. Output data is provided to the digital part via a register bank. The three different conversion blocks can run in parallel.

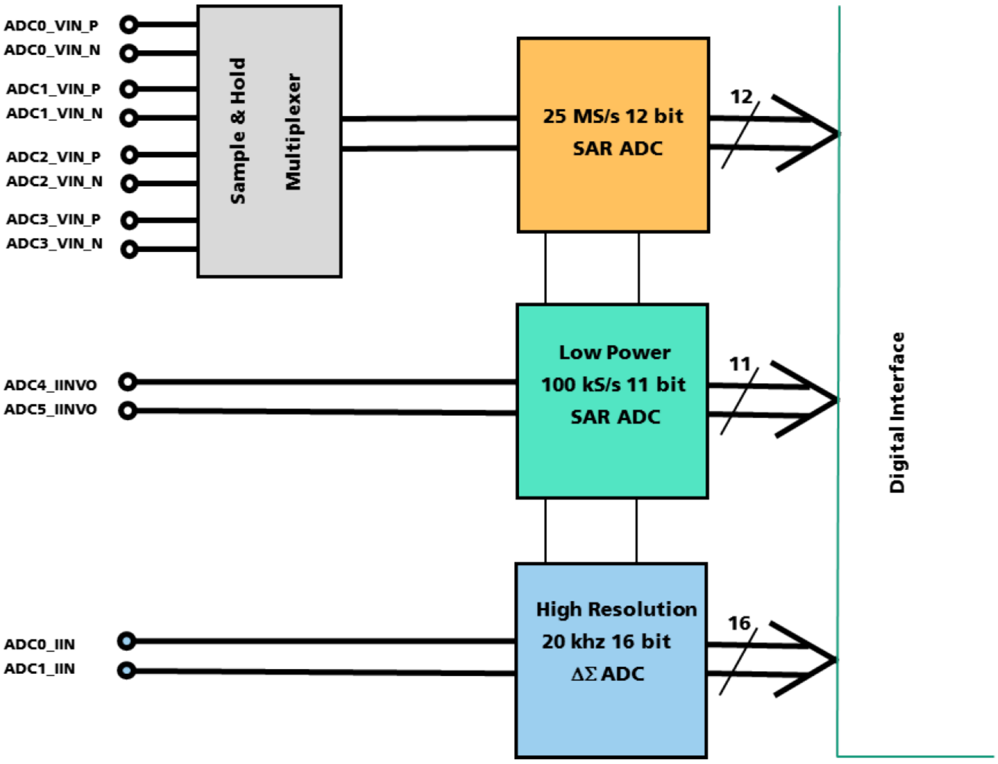


Figure 6: Blockdiagram of the analog signal input block

High Speed ADC Block

The fast 25 MS/s 12bit ADC is provided with a S&H stage which samples the four differential input signals x at the ADCx_VIN_P / ADCx_VIN_N interface (x=0 to 4) simultaneously. Then the sampled signal is multiplexed to the input of the 25 MS/s SAR ADC for conversion. After end of conversion, the 12bit output data is stored in a register to be read by the controller. This multichannel input block is intended for parallel sensors channels where a synchronous sampling is needed. The ADC run on a 500 MHz clock provided by the internal clocking block. However, in a fast mode the first of the four input channels can be selected permanently and an analog signal with a bandwidth up to 12,5MHz may be processed. All four input channels ADCx_VIN_P / ADCx_VIN_N interface (x=0 to 4) are specified for a differential input signal range of 0.4V +/- 0.3V, however they tolerate input signal levels from 0 to 0.8 Volt. Multichannel ultra sound or vibration sensors are one of the classes of sensors suitable for this block, due to its high frequency range. The digital result is provided in a 16bit frame – 12bit data, 2bit channel address, 2bit not used – to a FIFO register to be read by the controller on demand.

Ultralow Power ADC

An ultralow power SAR ADC with less than 40µA is implemented, to allow the conversion of sensor signals up to 50kHz bandwidth in battery operated mobile applications, e. g. for audio stand by and wake up modes. Sounds from the environment are monitored in an ultralow power standby listening mode and after activation the USOC is awakened to its full performance. Further applications may include standalone intrusion alarm or energy harvesting based early anomaly detection in machinery. The ADC is directly connected to the analog inputs ADC4_IINVO / ADC5_IINVO interface. The inputs are specified for a differential input signal range of 0.4V +/- 0.35V, however they tolerate input signal levels from 0 to 0.8 Volt. The maximum ADC sampling rate is specified with 100kS/s. The ADC can be operated in continuous conversion mode and in single shot operation mode. The conversion clock of 1.25 MHz is provided by the clocking block.

High resolution ADC

A 16bit Delta Sigma ADC is implemented for high resolution analog signal conversion. It may be used in combination with the low power ADC in audio and speech processing applications where the former is utilized in standby mode and after sound or command wakeup the DS-ADC provides a high-resolution audio signal to the digital processor. The ADC is directly connected to the analog inputs ADC0_IIN / ADC1_IIN pads. The inputs are specified for a differential input signal range of 0.4V +/- 0.3V, however they tolerate input signal levels from 0 to 0.8 Volt. A block diagram of the ADC is shown in the following figure.

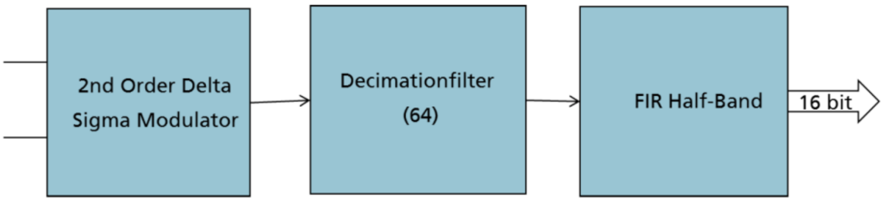


Figure 7: SAR ADC block diagram

A 2nd Order Delta Sigma Modulator is followed by a 64-tap decimation filter and a FIR Half Band filter. The filter with an order of 120 is designed for a 20 kHz Bandwidth as shown in the following figure.

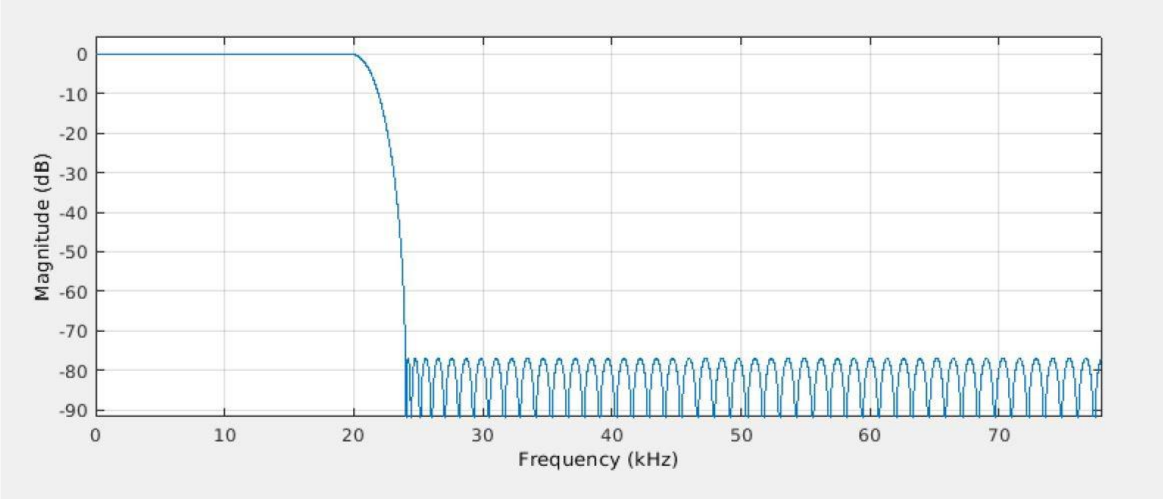


Figure 8: High precision ADC filter

Data and specifications are preliminary and subjects to change without notice

The 2nd order Delta Sigma modulator is operated with 12.5 MHz from the clocking part. With an OSR or 256 the ADC converts a 1 kHz bandwidth analog input signal with an SNDR of more than 80dB, available at a 16 bit register accessible by the controller.

3.4 Top Level: The Sensor Area

Top of the processing layer additional sensors and devices can be assembled package-on-package. Referring to Figure 5 a subset of communication interfaces is available to connect a variety of sensors. The footprint is an outlined ball grid array with access to the power sources and analog and digital interface to connect the devices. The type of sensor will be defined and placed by costumer based on the set of selectable devices. The complete system in package will be manufactured in the SENSRY supply chain in order to get a costumer specific device.

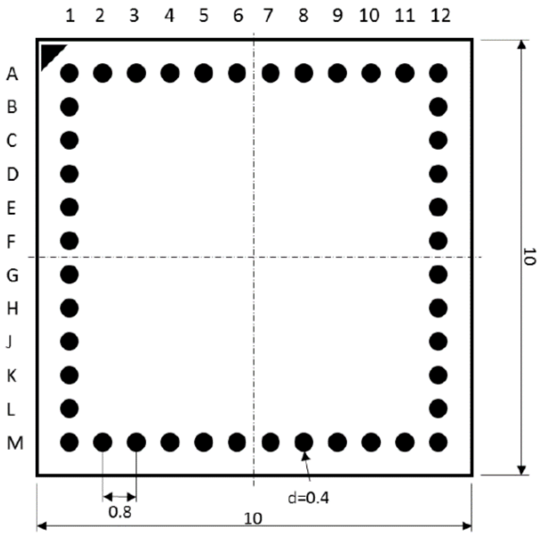


Figure 9: Array Package Outline – BGA 144 Balls, 10 mm x 10 mm, 0.8 mm pitch

The sensors can be selected by costumer from a list of supported sensors. The list will be extended continuously in order to support a various set of physical parameters. The current list under development is shown in Table 2 .

Table 2: Current list of Top-Level sensors

Sensor class	Sensor type	Manufacturer	Sensor name
Environment	Humidity	Sensirion	SHTW2
Environment	Temperature	Sensirion	SHTW2
Environment	Humidity	Texas Instruments	HDC2010
Environment	Temperature	Texas Instruments	HDC2010
Environment	Microphone	STMicroelectronics	MP34DT02
Environment	Humidity	Bosch Sensortec	BME680
Environment	Temperature	Bosch Sensortec	BME680
Environment	Air pressure	Bosch Sensortec	BME680
Environment	Air pressure	Infineon	DPS310
Environment	Temperature	Infineon	DPS310
Gas	VOC	Bosch Sensortec	BME680
Inertial	Acceleration	ENAS/ZfM	TI05G

Inertial	Acceleration	Bosch Sensortec	BMA456
Inertial	Vibration	ENAS/ZfM	AC20k
Inertial	Vibration	Analog Device	ADXL1002
Inertial	Vibration	Analog Device	ADIS16227
Inertial	Vibration	STMicroelectronics	MIS2DH
Inertial	Angular rate	Bosch Sensortec	BMG250
Optical	Image/Vision	Fraunhofer IIS EAS	VsoC2M

3.4.1 Example Top-Level assembly

The following figure describes a possible variant of sensor placement. The specific set of sensors will be available as a demo system.

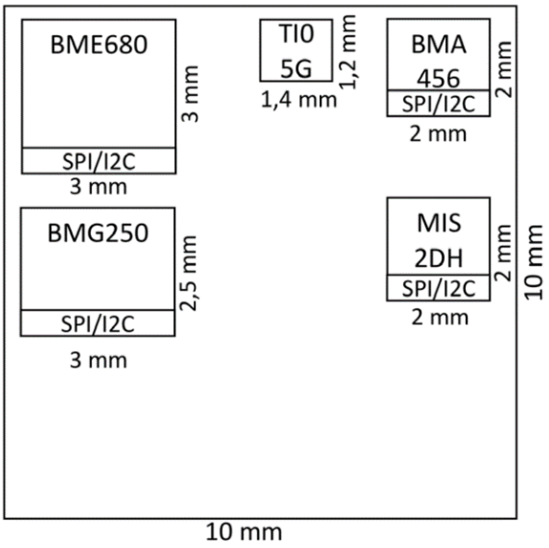


Figure 10: Top sensor placement, state 11.12.2018

The list of sensors in the demo system is specified in Table 3:

Table 3: Top-Level sensors demo setup

Device	Measured value	Man.	Size [mm]	I/F	Pack
BME680	Temperature, Pressure, Humidity, VOC	Bosch	3.0 x 3.0 x 0.93	SPI	LGA
BMA456	Acceleration (3-axis)	Bosch	2.0 x 2.0 x 0.65	SPI	LGA
MIS2DH	Vibration	ST Micro	2.0 x 2.0 x 1.0	I^2C	LGA
BMG250	Gyroscope (3-axis)	Bosch	2.5 x 3.0 x 0.83	SPI	LGA
TI05G	Acceleration (2-axis)	FhG ENAS	1.2 x 1.4 x 0.5	Analog	Die

4 Security Subsystem

The security-relevant aspects of the universal sensor platform consist of four key areas: the device state, cryptographic functions, watchdog timers, and system boot:

- **The device state** defines device permissions and access restrictions. It ensures that secrets and features of the platform are always protected and only accessible from an appropriate system state.

- **Cryptographic functions** protect the platform and accelerate common cryptographic operations. They include functions for key management, cryptographic acceleration, and secure non-volatile storage.

- **Watchdog timers** increase the resiliency of the platform. With security-focused features, the watchdog timers protect devices from malicious software and support remote management.

- **The system boot** describes how the system is bootstrapped into a secure state. This includes verification of all software running on the platform.

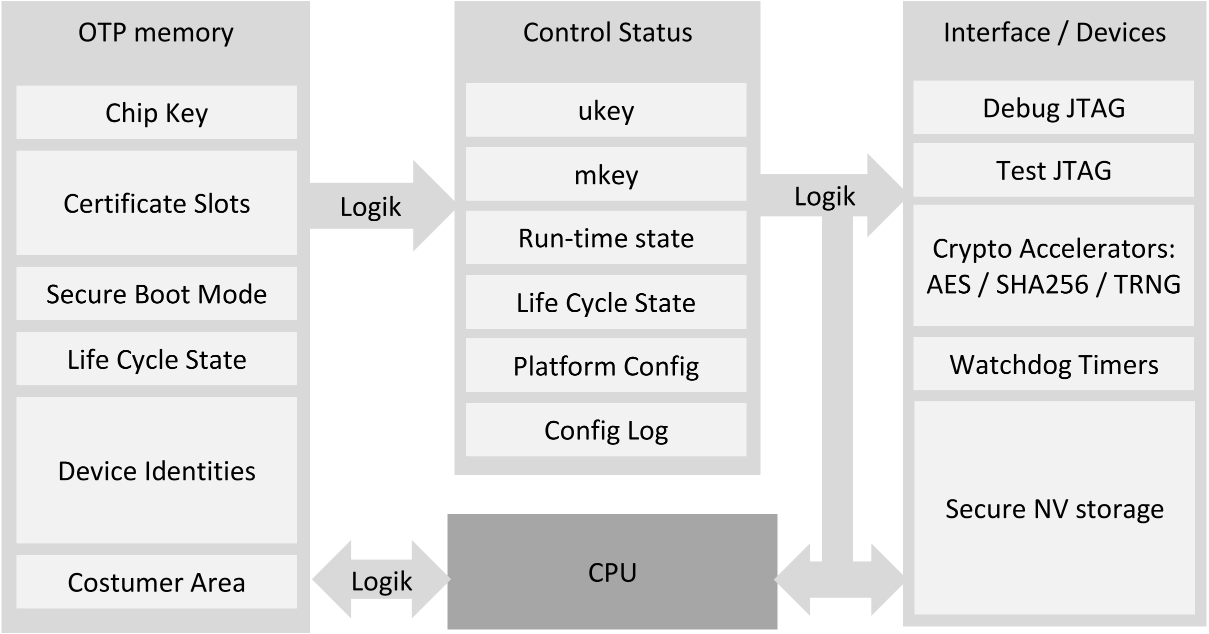


Figure 11: Universal Sensor Platform security subsystem overview

Figure 11 shows an overview of the hardware part of the security subsystem from a functional perspective. The chip key and key control and status registers (CSRs) are designed to be compatible with the Trusted Computing Group (TCG) Device Identifier Composition Engine (DICE) architectures specification.

4.1 The device states

The device states regulate the access to privileged information in the system. The device state consists of two parts: the life cycle and the run-time state. The life cycle state is persistent on the device, the run-time state will be initialized with every reset. Both states together controls read and write access to memory locations and CSRs. The level of access to sensitive information is determined by the device state.

4.1.1 The life cycle states

In general, there are four different life-cycle states:

1. **Unlocked factory:** initial state of all devices, active in factory
2. **Locked factory:** intermediate state, active in factory
3. **Unlocked:** initial state customers receive their devices in, active during development and at customers factory
4. **Locked:** final state, active in field

The allowed transition between the states is shown in Figure 12.

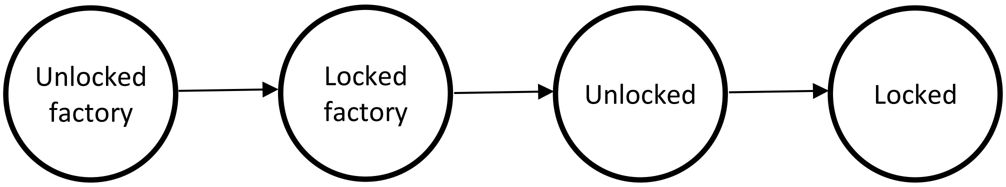


Figure 12: Universal Sensor Platform life cycle states

4.1.2 The run-time states

The run-time state primarily controls access to the chip key via the machine mode key (mkey). It is used by software, in its secondary function, to determine software access permissions. The Run-time state consists of four different states: evaluate, secure, non-secure, and security violation. It is a dynamic state, which is reevaluated at every reset.

1. **Evaluate:** The initial state after every reset is the evaluate state. It is an intermediate state only active during the secure boot process. The mkey CSR is reloaded with the reset value.
2. **Secure:** The secure state is entered if the secure boot process has been successfully completed. The mkey CSR is reloaded with the chip key on state entry. Software has read and write access to the CSR and may use it for cryptographic operations.
3. **Non-Secure:** In the unlocked factory and unlocked life cycle states, the nonsecure state is entered if unsigned software is running on the device. In the locked factory and locked life cycle states, the nonsecure state may be entered by software running in the secure runtime state.
4. **Security Violation:** The security violation state is entered to protect the system on errors. The mkey CSR is zeroized on entry to prevent software from accessing it. Keys derived from it and data protected with it are inaccessible.

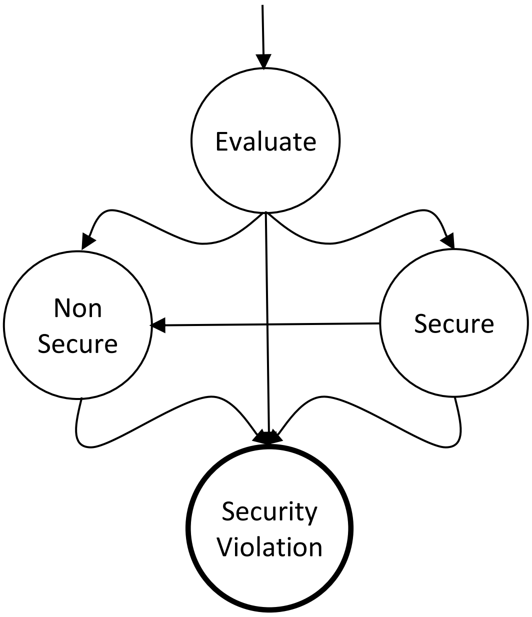


Figure 13: Universal Sensor Platform run-time states

Figure 13 shows the transition scheme between the four different states. The transit from one state to another, security conditions have to be fulfilled.

4.2 Cryptographic functions

Cryptographic functions provided by the platform are divided into four categories: key management, device identification, accelerators, and secure non-volatile memory. They are summarized below:

- Key management
    - Chip key
    - Key CSRs
    - Certificate slots
    - Device identification
- Cryptographic accelerators
    - AES {128,192,256}
    - SHA256
    - True Random Number Generator (TRNG)
- Secure Non-Volatile Storage

Key management consists of two parts, the chip key in combination with the key CSRs and certificate slots. Key CSRs are used on the platform to store and use cryptographic keys. The mkey CSR makes the chip key — a device-unique key — available to machine mode software. The user mode key (ukey) CSR is an optional key CSR available to user mode software. Certificate slots are used on the platform to store certificates for secure boot and secondary purposes. The platform has two certificate slots, one for Universal Sensor Platform and customer certificates each.

The platform provides a set of cryptographic accelerators, listed above. They are only available to the main processor. Additionally, the system provide dedicated non-volatile storage for security-critical information, including cryptographic keys, configuration data, and software states. It is only

Data and specifications are preliminary and subjects to change without notice

accessible to machine mode software, but parts of it may be made available to user mode software through an Application Programming Interface (API).

4.3 Security-enhanced Watchdog timers

A conventional watchdog timer consists of a timer with a software-configurable timeout interval. Once started, software can defer the watchdog timer to reset it to the specified timeout value. If the timer elapses and is not deferred, the device is reset by the watchdog timer.

The security-enhanced watchdog timer extends the conventional watchdog timer with a set of new requirements. Each requirement may be set to enforcing by software. However, the watchdog timer is only considered to be a security-enhanced watchdog timer if all requirements are set to enforcing.

4.4 System Boot

The system boot process securely starts and initializes the Universal Sensor Platform. This process is performed by ROM software, which is the first software to run after a reset. It performs the necessary steps to load and verify software images on the platform as part of secure boot.

Secure boot uses certificates verify software and data. The secure boot mode configuration determines how the certificate chain is used in the secure boot process. It must be set during manufacturing by configuring the relevant entry in OTP memory. There are two modes, CA mode (optionally with enforce CA signature configuration) and legacy mode.

The following describes the individual steps of the secure boot process. All steps of the process are implemented in ROM software. A security violation is raised if an error occurs at any part of the secure boot process:

1. **System Initialization:** The Main processor core is the first processor to start after areset. It runs from the on-chip ROM and contains the secure boot firmware. It performs all necessary system initialization steps before continuing to the software image search step.

2. **Software Image Search:** In the software image search step, all software sources are searched in the system boot order for valid software images. This includes flash storage, for example connected to the quad-SPI interface, but also communication interfaces such as UART. The latter may be used for development or recovery purposes, where there are no valid software images available locally. The software image is transferred into main processor memory, from where it is verified as part of the following steps.

3. **Certificate Chain Verification:** The certificates entry in the software image is verified in four steps, listed below. Certificates are installed for software verification in the next step, if the verification passes.
   a. Verify format of root certificates (including number of expected certificates)
   b. Verify certificates against hashed copy in certificate slots
   c. Verify certificate chain
   d. Verify certificate serial numbers (if required)

4. **Software Verification:** Software in the software blobs is verified using the type A certificates installed in the previous step. If software for the main processor is encrypted, it is decrypted after verification. Software is then started in the normal operation step. In the locked factory and locked device life cycle states, all software included in the software image must be signed. A security violation is raised if this is not the case. In the unlocked factory and unlocked device life cycle states, not all software must be signed. The unlocked factory state, in specific, requires no signed software; the unlocked state requires software to be signed.

5 Software Eco System

The Software Eco System consists of three parts:

- Development system including built tools and development environment
- Application programming interfaces (APIs) in form of libraries to control different system parts
- Client-side tools and example implementations

Generally, the embedded software is running as a Real-Time-OS (RTOS) implementation which divides in a Machine-Mode and User-Mode (comparable to Kernel- and User-Mode on Linux based Systems). The two modes allow a different level of access to critical parts of the system. Figure 14 shows the general functionality of the API system.

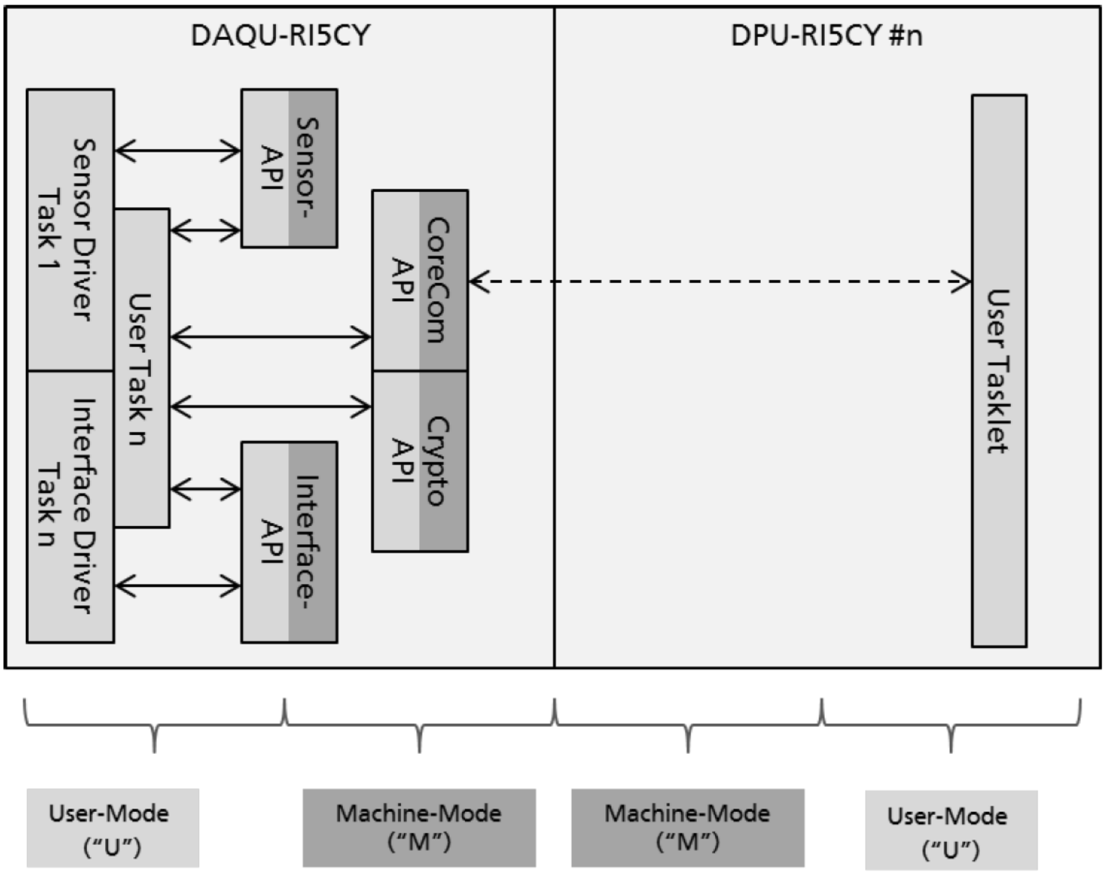


Figure 14: General software API overview

The Sensor API controls the low-level communication and data transfer between the sensor and the system. An overview of the Sensor API is shown in Figure 15.

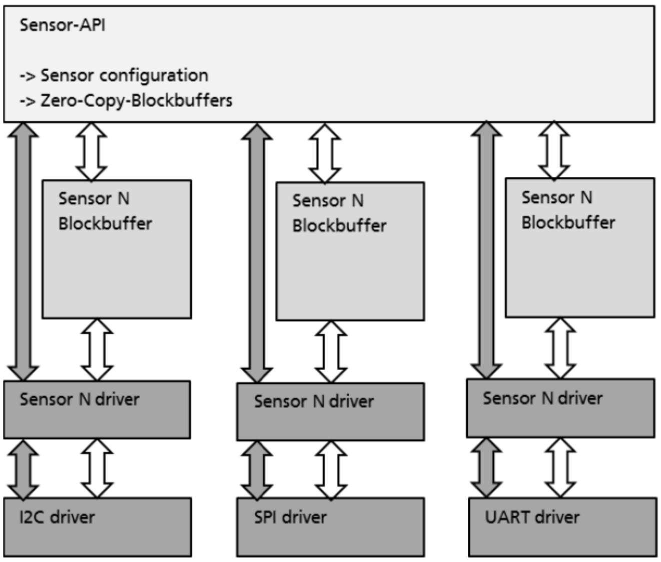


Figure 15: Sensor-API overview

The Interface-API provides a socket-based communication to all interfaces. An overview of the Interface-API is show in Figure 16.

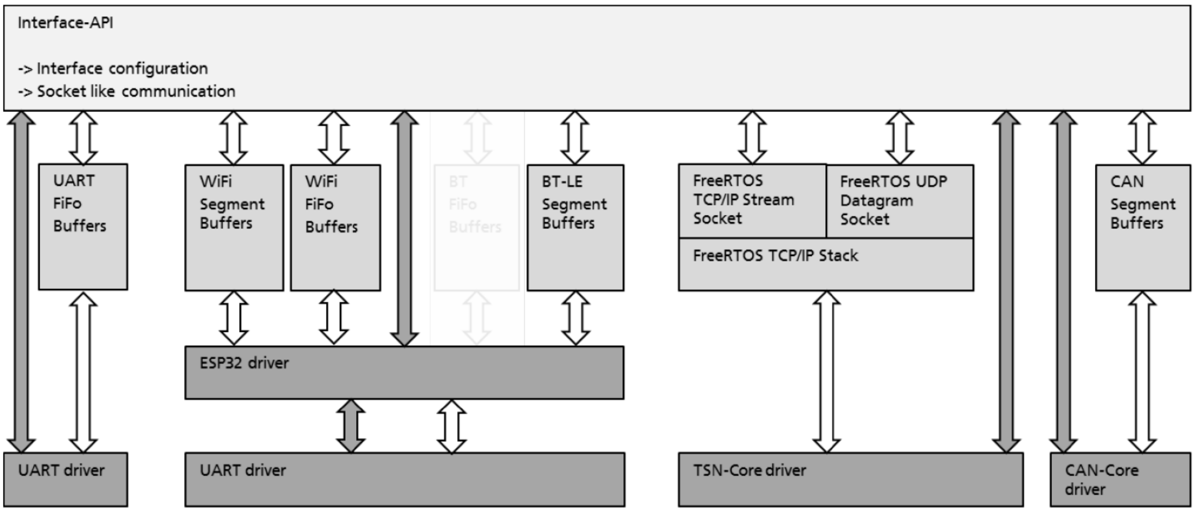


Figure 16: Interface-API overview

The CoreCom-API controls all operating system relevant features including management of the DPU cluster. This API initiate and controls “Tasklets” running independently on one of the DPU cores. The Security-API interfaces between the hardware security features and software.

Data and specifications are preliminary and subjects to change without notice