Secure smart metering with u-blox R5

June 26th, 2019

Harald Kröll, Product Manager Cellular Chipsets

Smart metering requirements

For LTE-M and NB-IoT cellular modules

Use case	Connectivity	Low Latency	Security	Energy Efficiency	Reliability	Longevity	Services	Edge Computing	Extended Coverage
Electricity metering, smart grid	LTE-M	Important	High assurance levels	Medium	Crucial	Up to 15Y	Firmware updates, analytics, reliability	Useful	Required
Gas and water metering	NB-IoT	Nice to have	High assurance levels	High	Crucial	Up to 15Y	Firmware updates, analytics, reliability	Nice to have	Required

Smart metering requirements

For LTE-M and NB-IoT cellular modules







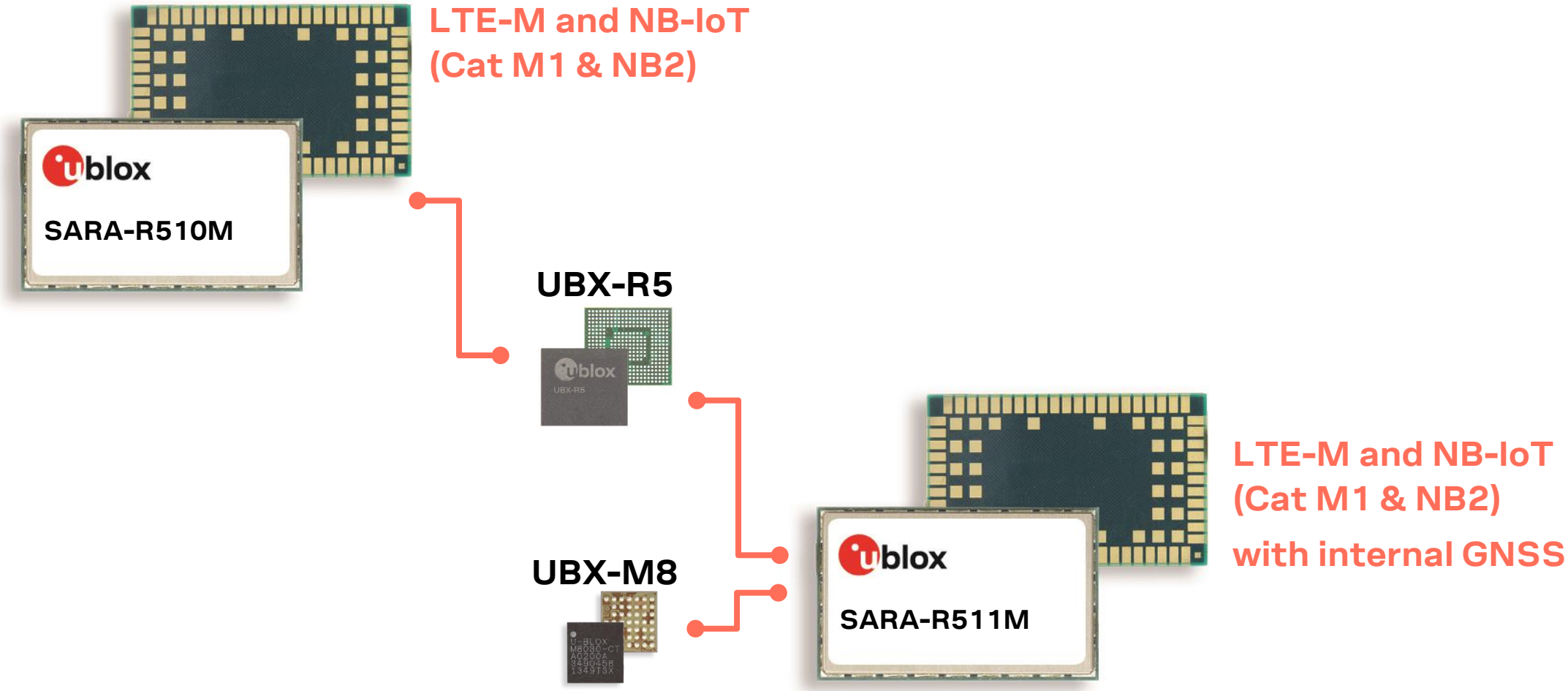


Use case	Connectivity	Low Latency	Security	Energy Efficiency	Reliability	Longevity	Services	Edge Computing	Extended Coverage
Electricity metering, smart grid	LTE-M	Important	High assurance levels	Medium	Crucial	Up to 15Y	Firmware updates, analytics, reliability	Useful	Required
Gas and water metering	NB-IoT	Nice to have	High assurance levels	High	Crucial	Up to 15Y	Firmware updates, analytics, reliability	Nice to have	Required

covered in this talk

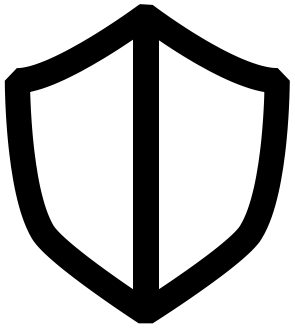
SARA-R5 series

LTE-M and NB-IoT module built on u-blox chipsets



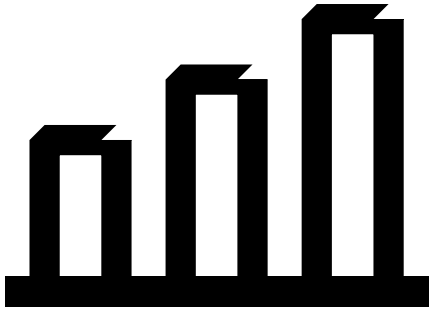
We add security

IoT security has quickly become an industry priority



More than **80% of senior executives** across industries, on average, say **IoT is critical** to some or all lines of their **business** in 2018.
(Source: Statista)

IoT security market is forecast to **grow at CAGR of 36%** between 2016 and 2021.
(Source: GSMA)



By 2020, **20% of annual security budgets** will be devoted to **IoT solutions** (up from 1% in 2015).
(Source: GSMA)

IoT security from the ground up

How we create trust to secure functions

Provision trust: Insert Root of Trust at production

An immutable chip ID and hardware-based Root of Trust provide foundational security and a unique device identity. The only product in the market.

CC EAL5+ High

Leverage trust: Derive trusted keys

Secure libraries allow generation of hardware-backed crypto functions and keys that securely connect to the cloud.

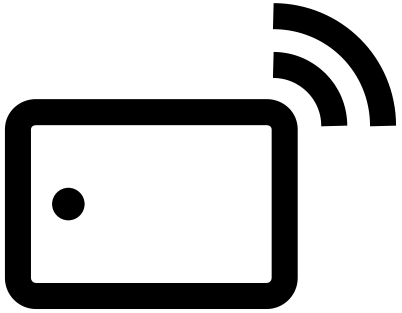
Guarantee trust: Use keys to secure any function

Ensures authenticity, integrity, and confidentiality to maintain control of device and data.

Security solutions developed in partnership with **Kudelski, a world leader in securing digital content.**

Securing the IoT from end-to-end

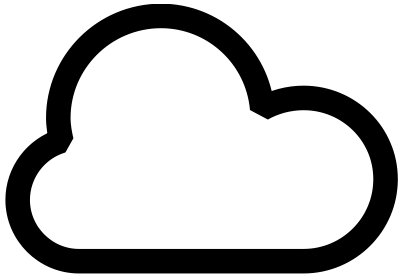
u-blox protects your business at different levels



Device Security

Your devices are protected from attack. You trust and control them

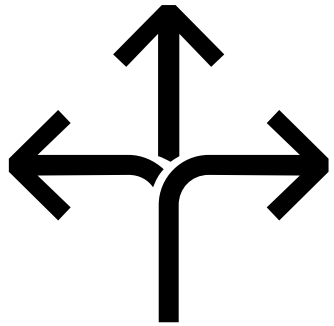
- Identity
- Authenticity
- Firmware protection



Data Security

The privacy of your data is protected from your devices to the cloud

- Confidentiality
- Integrity
- Authenticity



Access Management

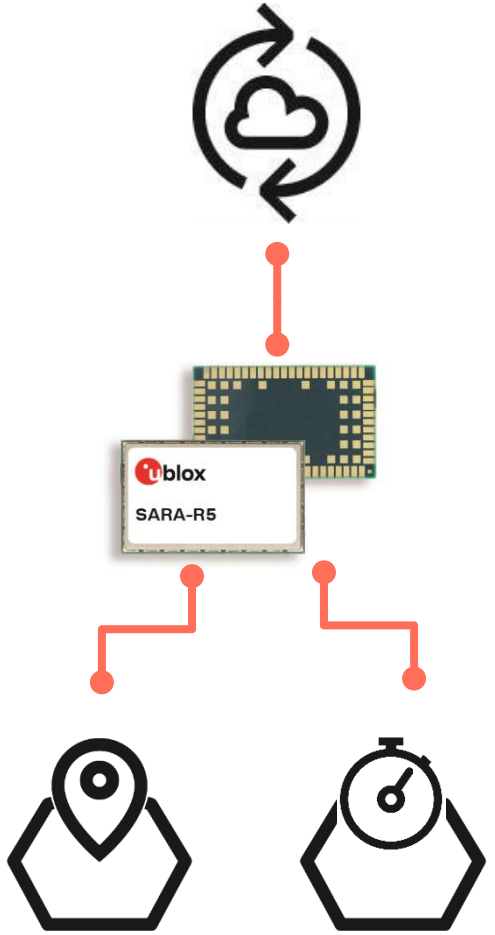
Control who has access to your data and products

- Device policies
- Data policies
- Feature authorization

Services @ the core

Adding value

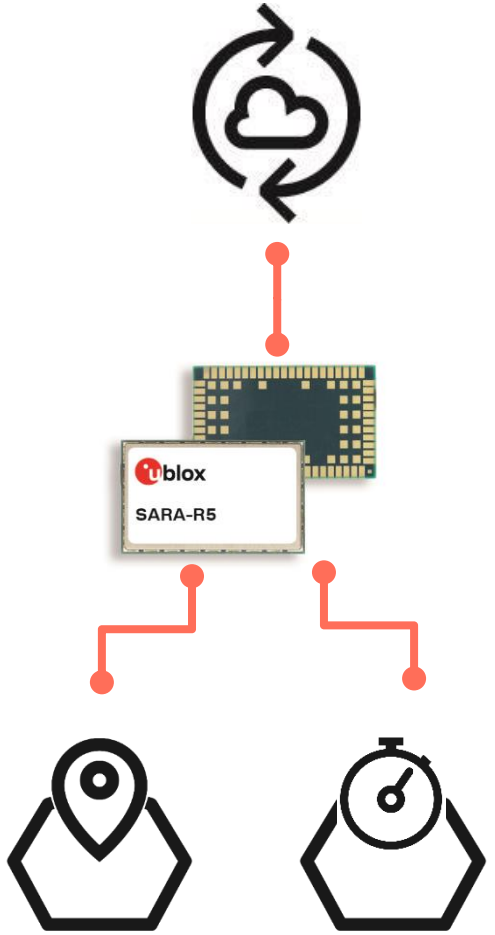
- **UBX-R5** is designed with a **service-driven architecture**
  - Low-level on-chip data sources are utilized to provide reliable and highly secure services to the customer
  - This includes events occurring deeply in the hardware or in the low layers of the communication stack
- **Localization** – reliable position outdoors and indoors with **CellLocate®**
- **Timing** – accurate timing information everywhere with **CellTime®**
- **Management** – always up to date with **uFOTA**
- **Scalable security** – tailored offering of features and services



Services @ the core

Adding value

- **UBX-R5** is designed with a **service-driven architecture**
  - Low-level on-chip data sources are utilized to provide reliable and highly secure services to the customer
  - This includes events occurring deeply in the hardware or in the low layers of the communication stack
- **Localization** – reliable position outdoors and indoors with **CellLocate®**
- **Timing** – accurate timing information everywhere with **CellTime®**
- **Management** – always up to date with **uFOTA**
- **Scalable security** – tailored offering of features and services



Real-world use case
- Leakage detection in water distribution system
- 1us synchronicity for measurements required to detect leak → **CellTime® Service**

Services @ the core

Edge computing in smart metering

- Process data directly on LTE-M / NB-IoT module
  - Analyze data locally, close to where it is created
  - Save cost of external MCU
- React faster to events
  - Carry out local inference from cloud-trained ML models e.g. with AWS IoT Greengrass
  - Compute moving average and compare it to threshold
- Be economical with reports to cloud
  - Minimize required reports (consolidate, aggregate, …)
  - See send-report-to-could as last resort
- Create custom microservices from IoT nodes

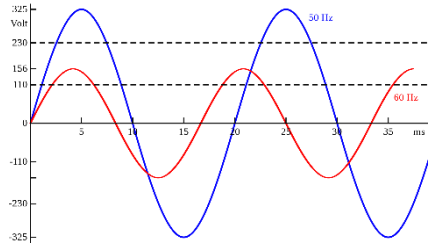
Services @ the core

Edge computing in smart metering

- Process data directly on LTE-M / NB-IoT module
  - Analyze data locally, close to where it is created
  - Save cost of external MCU
- React faster to events
  - Carry out local inference from cloud-trained ML models e.g. with AWS IoT Greengrass
  - Compute moving average and compare it to threshold
- Be economical with reports to cloud
  - Minimize required reports (consolidate, aggregate, …)
  - See send-report-to-could as last resort
- Create custom microservices from IoT nodes

Real-world use case

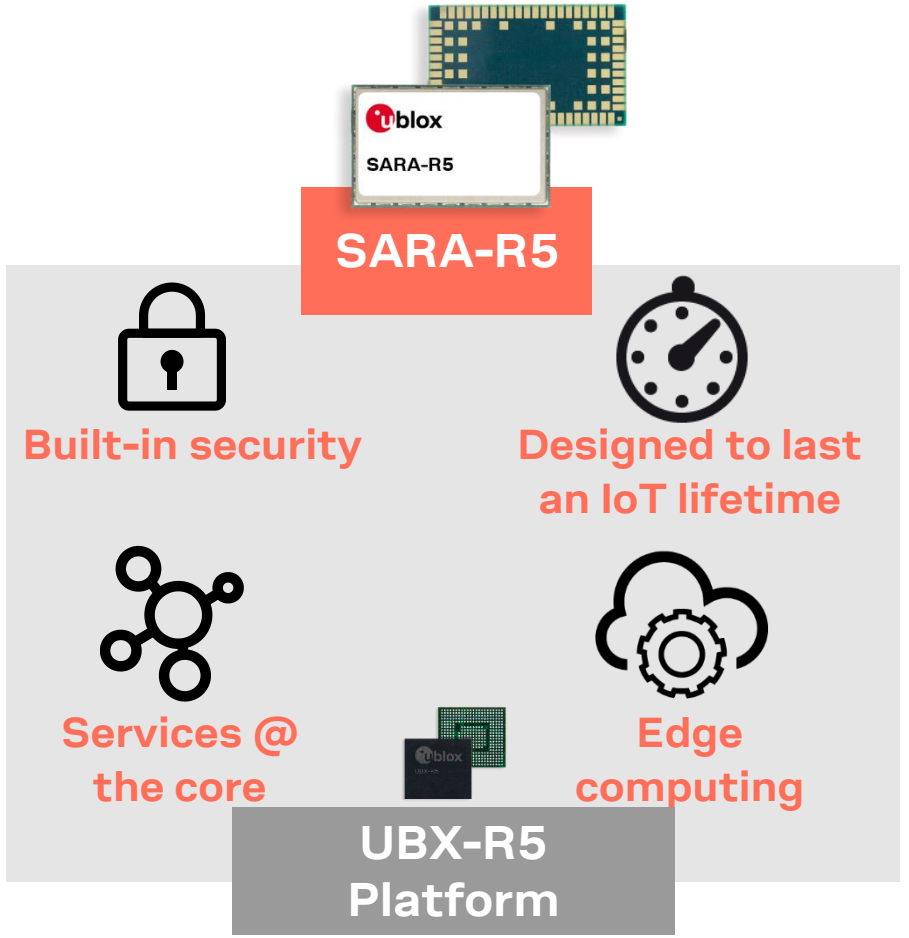
- Smart power meter
- Low-complexity Phasor measurement unit (PMU)
- PMU SoC connected to R5 module via I2C
- Local anomaly detection on modem



Summary

Smart metering demands secure end-to-end solutions

- Hardware based security
  - Root-of-trust at chipset level is required to provide secure services
- Secure services
  - Fundamental to serve applications with trusted and reliable data (time, position…)
- Edge computing
  - Use cases are emerging in various domains, benefits for cloud and device side



Thank you for your attention.