DIGITAL WE DAYS 2023

ENOUGH WITH THE THEORY - WHAT IT REALLY TAKES TO GET SENSOR DATA INTO A CLOUD

WÜRTH ELEKTRONIK MORE THAN YOU EXPECT

TODAY'S SPEAKERS

PRESENTATION
Jens Ruckes | Balazs Markus
Software Development

MODERATION
Markus Eberle
Marketing Department

INFORMATION ABOUT THE WEBINAR

You are muted during the webinar.
However, you can ask us questions using the chat function.

Duration of the presentation	30 Min
Q&A:	10 – 15 Min

Any questions?
No problem! Email us digital-we-days@we-online.com

Please help us to optimize our webinars!
We are looking forward to your feedback.

On our channel	Würth Elektronik Group
And on	Digital WE Days 2023 YouTube Playlist

AGENDA

- **Part 1: IoT and Cloud Overview**
  - Introduction to IoT and Cloud
  - Why IoT Data in the Cloud?
  - Key Hardware Components for IoT
  - Wireless Technologies for IoT
  - Cloud Platforms for IoT Data
  - How to Implement IoT Data in the Cloud (In 4 Steps)
  - Challenges in IIoT Solution Development
- **Part 2: IoT Security**
  - IoT Vulnerabilities & Past Incidents
  - Reasons for Vulnerabilities
  - The EU's Cyber Resilience Act and Security Measures
  - Security Recommendations
  - Hidden Costs
- **Part 3: Applications & How to?**
  - Application Examples
  - Designing a Security Concept for an Embedded Device
  - Hands-on Workshop
  - Practical Example using Calypso IoT Kit
- **Q&A**

Part 1:
IoT and Cloud Overview

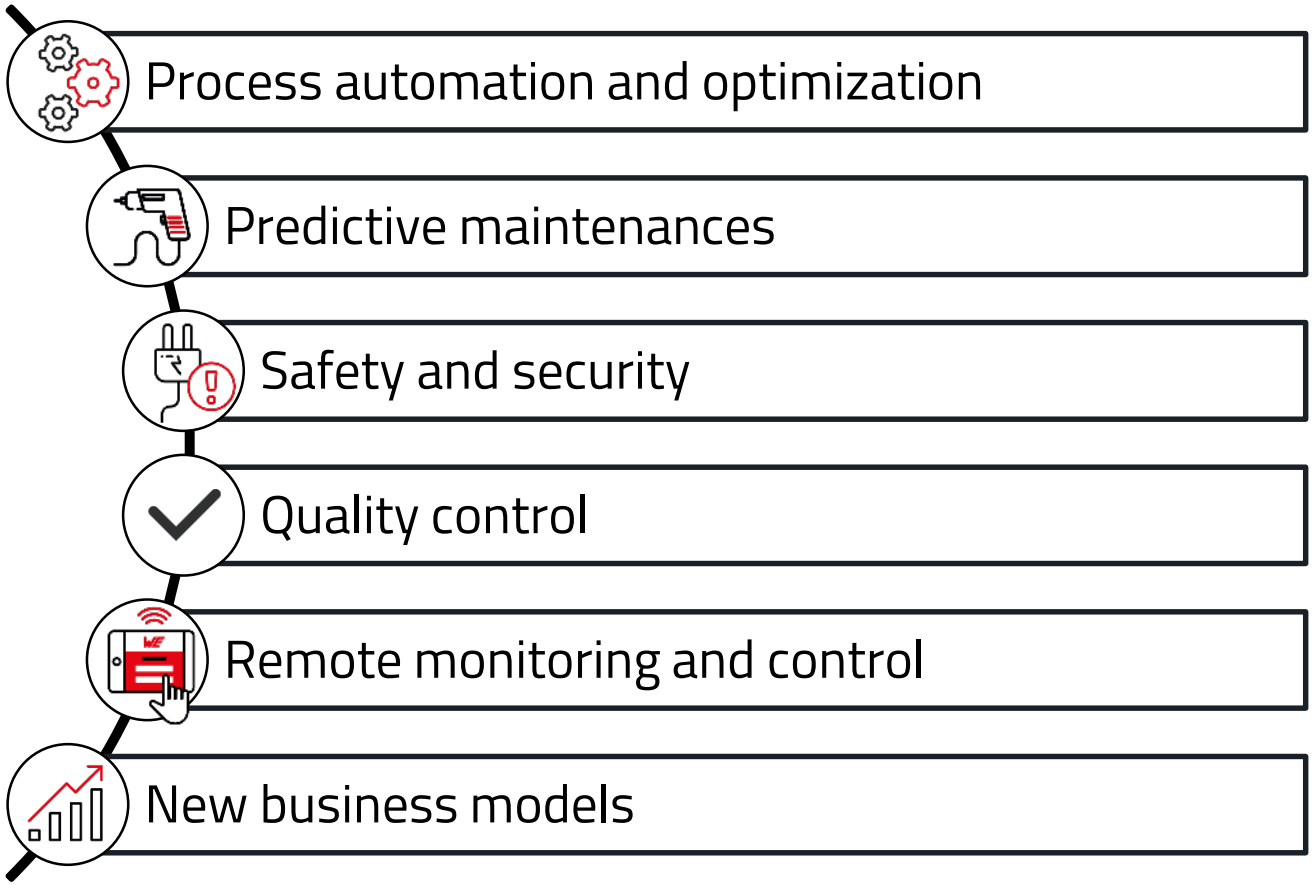
INTRODUCTION TO IOT AND CLOUD

IoT, IIoT, Cloud, SaaS, Paas, IaaS...

IoT

Cloud		
Deployment models	**Characteristics**	**Service models**
Private Cloud Community Cloud Public Cloud Hybrid Cloud	Shared Infrastructure Dynamic Provisioning Network Access Managed Metering	SaaS PaaS IaaS

MOTIVATION - WHY IOT DATA IN THE CLOUD?

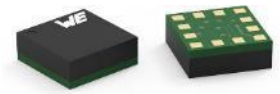


KEY HARDWARE COMPONENTS FOR IOT

Basics

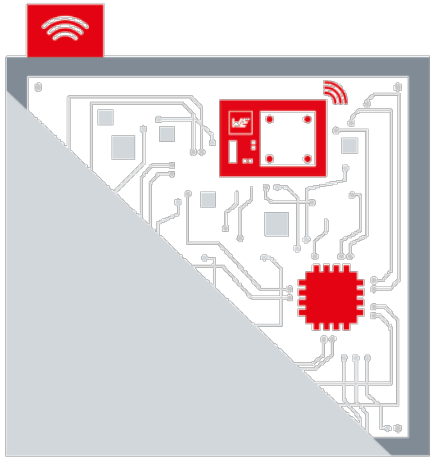
Sensors

Data acquisition



Host

Microcontroller



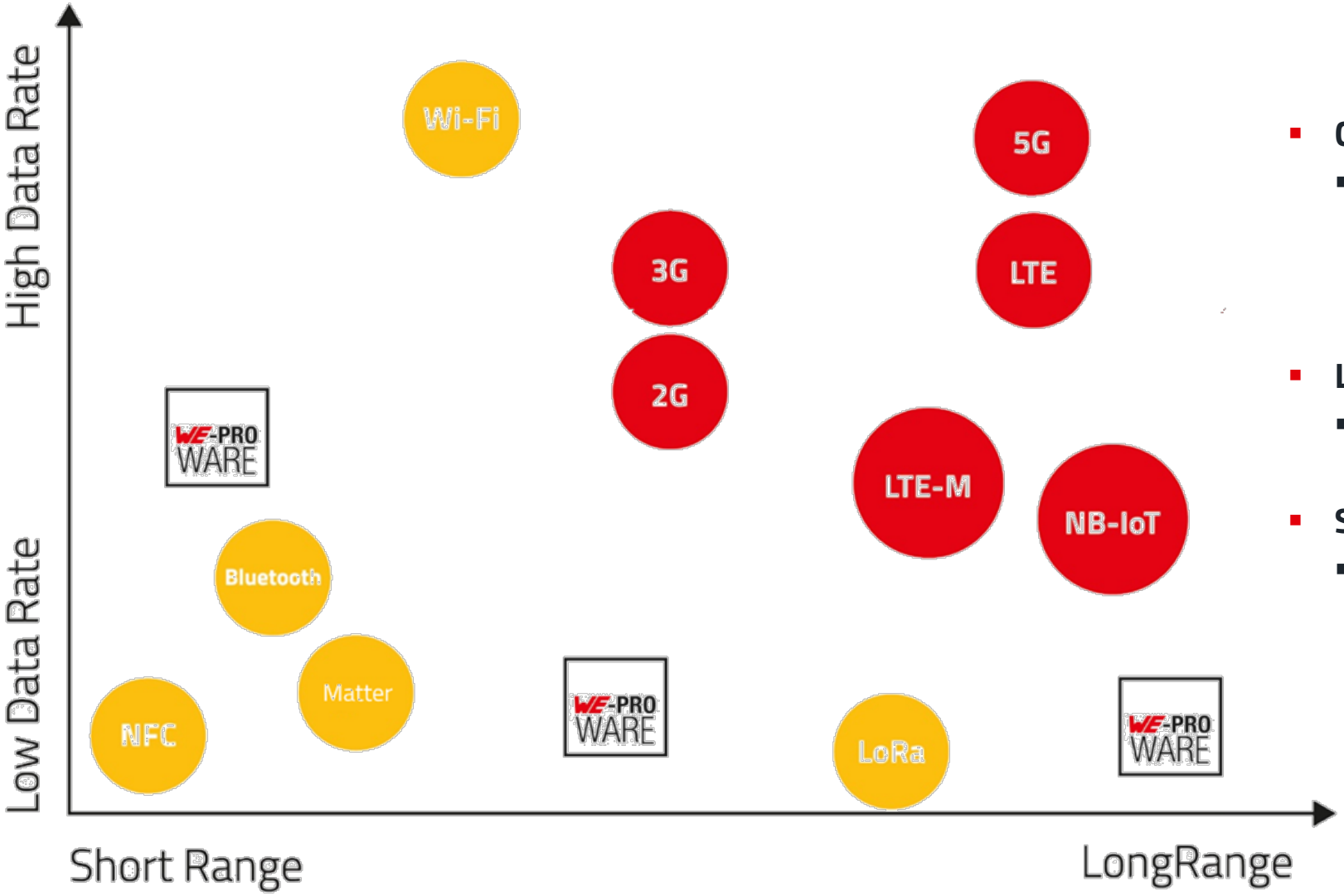
(Wireless) connectivity

Data communication, Internet

Cloud

Data lake, Services

WIRELESS TECHNOLOGIES FOR IOT



- **Cloud connectivity**
  - (asset tracking, home automation, industrial automation, etc.) using technologies like WiFi or cellular networks like NB-IoT, LTE-M, GSM, etc.
- **Long-range local networks**
  - (smart city, smart agriculture, etc.) using technologies like LoRa, Zigbee, Sigfox, etc.
- **Short-range local networks**
  - (tracking vital health parameters using wearables, smart door locks, etc.) using technologies like BLE, NFC, ZWave, etc.

CLOUD PLATFORMS FOR IOT DATA

Amazon Web Services (AWS)	Microsoft Azure IoT	Google Cloud Platform (GCP)	IBM Watson IoT Platform
aws	Azure IoT Central	Google Cloud	IBM Watson IoT
• **AWS IoT Core** for managing IoT devices and data ingestion • **AWS IoT Analytics** for data processing and transformation • **AWS IoT Events** for real-time event detection	• **Azure IoT Hub** for device management and communication • **Azure Stream Analytics** for real-time data processing • **Azure IoT Central** for application integration and scaling	• **Google Cloud IoT Core** for managing and processing IoT data • **Pub/Sub** for ingesting data and **Dataflow** for data processing • **BigQuery** for analytics and insights	• **Watson IoT Platform** for device management and connectivity • **Watson IoT Analytics** for data analysis and visualization • **Watson Studio** for AI-powered insights

HOW TO IMPLEMENT IOT DATA IN THE CLOUD (IN 4 STEPS)

1. Connect IoT Devices to the Cloud

Set up device communication using appropriate protocols (MQTT, HTTP, etc.).

2. Data Ingestion

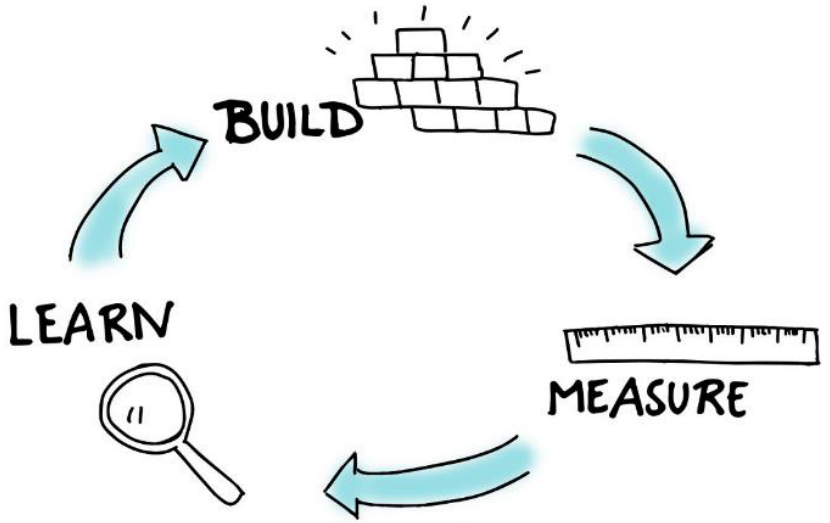
Configure cloud platform to ingest data from IoT devices.

3. Data Processing and Storage

Define data processing pipelines and storage mechanisms.

4. Analytics and Visualization

Utilize cloud platform tools for data analysis and visualization.



CHALLENGES IN IIOT SOLUTION DEVELOPMENT

- **Interoperability**
- **Scalability**
- **Reliability and Quality of Service (QoS)**
- **Data Management and Analytics**
- **Security and Privacy**

Part 2:
IoT Security

IOT VULNERABILITIES & PAST INCIDENTS

- **Your "smart" device might not be as smart as you think**
  - IoT transforms everything into a computer, creating a vast attack surface.
- **Small IoT devices are prime targets for hackers**
- **They can be used as entry points to your network**

- **Complexity in IoT systems increases vulnerability, and complexity is the enemy of security**
- **Shrinking the attack surface is crucial to mitigate risks associated with IoT devices**
- **Risks of IoT include privacy invasion, safety concerns, and potential for denial-of-service attacks**

- **Past Incidents**
  - Mirai botnet (2016)
    - exploited weak security in IoT cameras and routers, causing massive internet outages
  - WannaCry ransomware attack (2017)
    - targeted healthcare systems, highlighting the critical need for robust security in IoT

REASONS FOR VULNERABILITIES

- IoT devices lack the comprehensive security features found in computers, tablets, and phones
- Their simplicity, while appealing to users, is attractive to malicious actors
- Unlike more complex devices, IoT gadgets often lack up-to-date hardware and robust software security mechanisms
- There isn't a consistent set of security practices

THE EU'S CYBER RESILIENCE ACT AND SECURITY MEASURES

- The EU's Cyber Resilience Act extended the RED (radio equipment directive) with requirements on cybersecurity, harmonization is pending with due date: August 2025
  - ETSI EN 303 645, ETSI TS 103 929 and IEC 62443 are expected to provide inputs towards the new standard

- "Security by design & Secure by default"
  - Include security considerations from the start of the design
  - Use well established methods to establish End-to-End security
  - Zero trust by default: "never trust, always verify"
  - supports software updates for itself and it's components
  - Include Error reporting mechanisms

SECURITY RECOMMENDATIONS

End User	Manufacturer/Admininstrator
1. Credentials	1. Establish Security Policies
2. Network Segmentation	2. User Training
3. Regular Patching	3. Enable Security Controls
4. Principle of Least Privilege	4. Device Discovery
5. Conscious Feature Usage	5. Enforce Security Measures

HIDDEN COSTS

Provisioning & Maintenance

- The costs for Provisioning and Maintenance are often considered too late in the development or appear during product life
  - Provisioning gets more and more impact when scaling up – prefer: Zero touch provisioning
  - Keep certificates up to date (e.g. renewal each 3 months) – many providers charge per certificate
  - Change the cloud and/or connectivity provider when the system is already productive
  - Software Updates

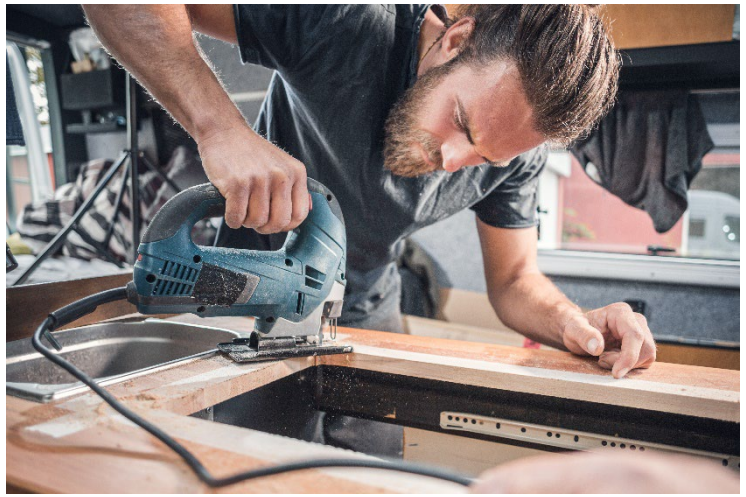
Part 3:
Applications & How to?

APPLICATION EXAMPLES

Smart Farming

- **Actuators can be controlled via RPC**
  - Turn on water pump to water the soil if the moisture is too low.
  - Automatically fertilize the soil.
  - Change the color and brightness of the LED depending on the time of day and the development of the plant.

Digital Tools



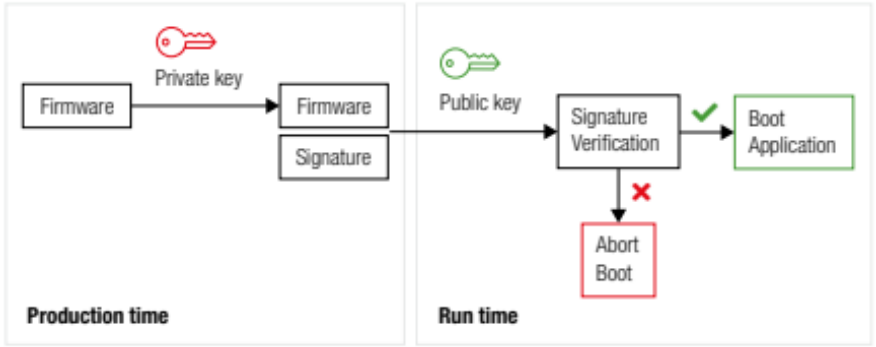
- **Access to device data at any time**
  - Contactless data access prevents the penetration of dust and water, extending device life.
  - Installation of further systems, e.g. for localizing the location of the molds or sensors with fall detection.
  - This data can be read out using a mobile app

Industry 4.0

- **Live monitoring**
  - Access is possible from anywhere, and system updates can be transmitted easily online by the manufacturer.
  - Access to the data can be ensured via NFC or LE authentication.
  - The use of cost-intensive displays can be avoided.

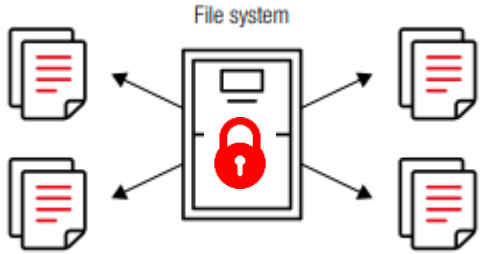
DESIGNING A SECURITY CONCEPT FOR AN EMBEDDED DEVICE

Common minimum security requirements for IIoT device

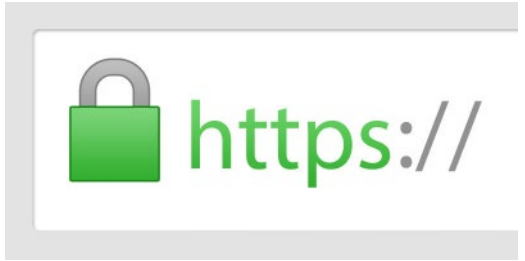


Secure production

Secure boot

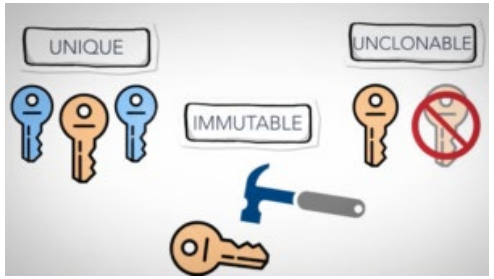


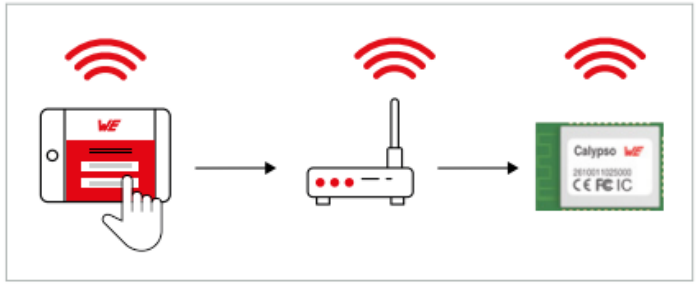
Secure storage



Secure connection

Secure root of trust





Secure FOTA

Security by design not an afterthought!

HANDS-ON WORKSHOP:
BUILD A SECURE IOT APPLICATION CONNECTED TO MICROSOFT AZURE CLOUD

- When? November 8th 2023, 8:30AM - 4PM CET
- Where? Würth Elektronik Hightech Innovation Center, Munich
- Free of charge!

Register at:
https://emea.info.mouser.com/wuerth-iotcloud-workshop

PRACTICAL EXAMPLE USING CALYPSO IOT KIT

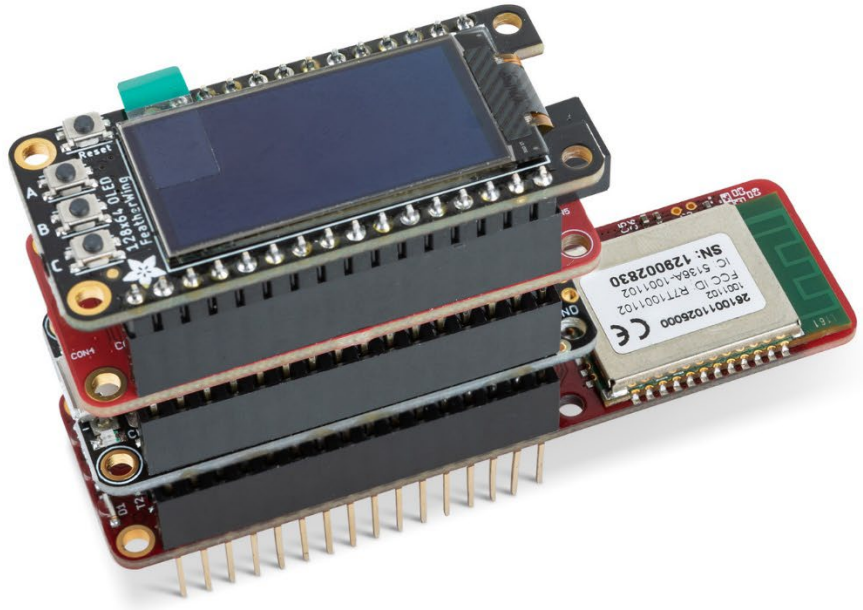
Solution – The engineer's way

Würth Elektronik eiSos offers a secure and high-performance solution for **rapid prototyping**, from the **sensor to the cloud**, that takes the customer by the hand and connects their devices and machines simply, securely and time-efficiently.

WE take care of IoT so that the customer can focus on his/her application.

Interested?
Check out our Wi-Fi Calypso IoT Design Kit!

LIVE DEMO:
YouTube – Würth Elektronik Group –
"How to get started with the
Microsoft Azure Certified Calypso IoT Design Kit?"
https://www.youtube.com/watch?v=d7C_oA74eXU



SUMMARY

- **Part 1: IoT and Cloud Overview**
  - Introduction to IoT and Cloud
  - Why IoT Data in the Cloud?
  - Key Hardware Components for IoT
  - Wireless Technologies for IoT
  - Cloud Platforms for IoT Data
  - How to Implement IoT Data in the Cloud (In 4 Steps)
  - Challenges in IIoT Solution Development

- **Part 2: IoT Security**
  - IoT Vulnerabilities & Past Incidents
  - Reasons for Vulnerabilities
  - The EU's Cyber Resilience Act and Security Measures
  - Security Recommendations
  - Hidden Costs

- **Part 3: Applications & How to?**
  - Application Examples
  - Designing a Security Concept for an Embedded Device
  - Hands-on Workshop
  - Practical Example using Calypso IoT Kit

- **Q&A**

Questions

& Answers

We are here for you now!
Ask us directly via our chat or via E-Mail.

digital-we-days@we-online.com
wcs@we-online.de