COMe + SMARC connect and secure

Kontron AG
Clemens.Mathijssen@kontron.com
+31 40 2024496

29 OKT ←
1931 CONGRESCENTRUM
BRABANTHALLEN
DEN BOSCH

D&E
event
2014

Kontron facts

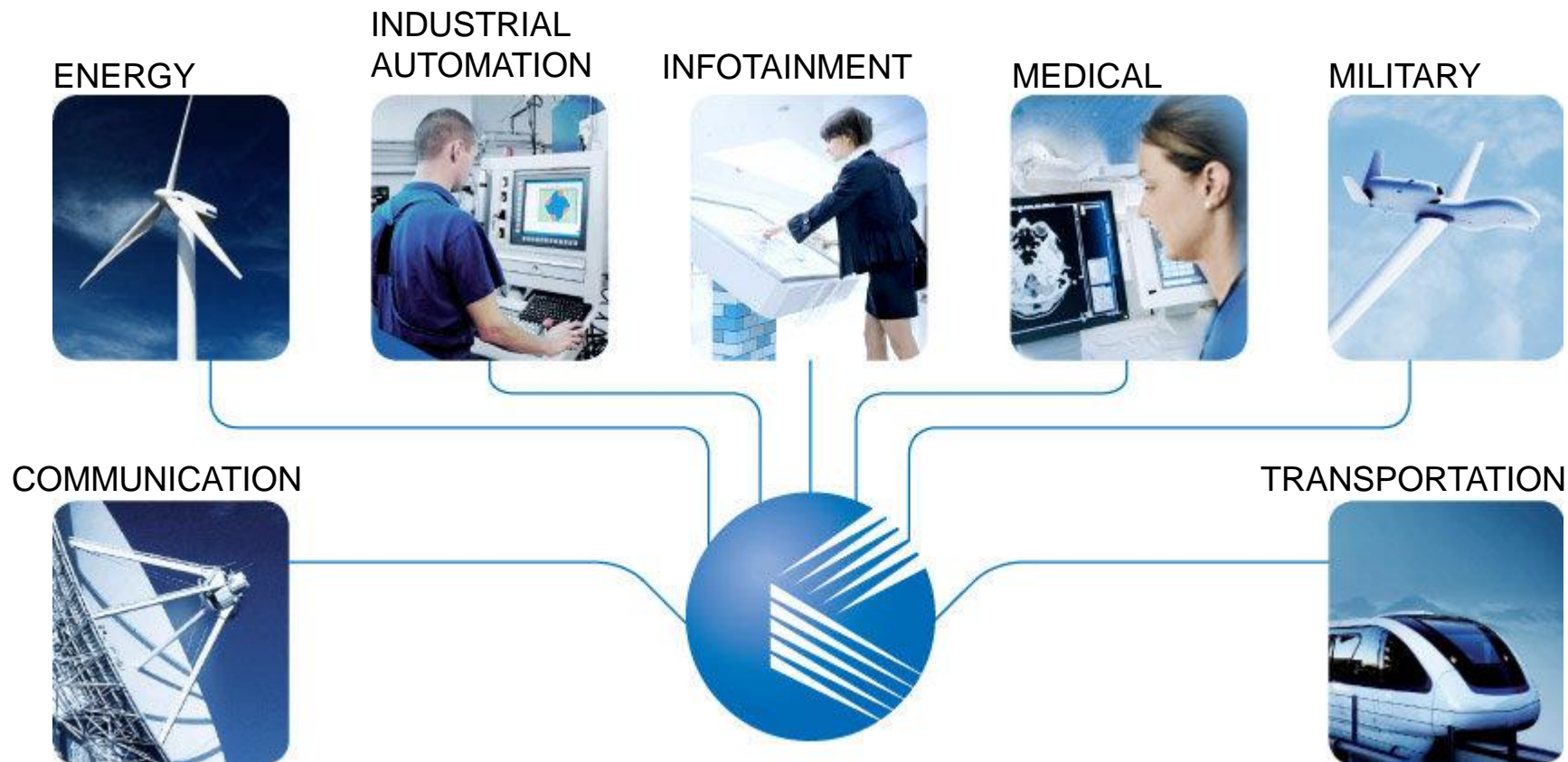- Founded   1999 (out BMW)
- Worldwide HQ   Munich, Germany
- Public listing   KBC at TecDAX
- Revenue   445 mio. € (2013)
- Employee size   1600
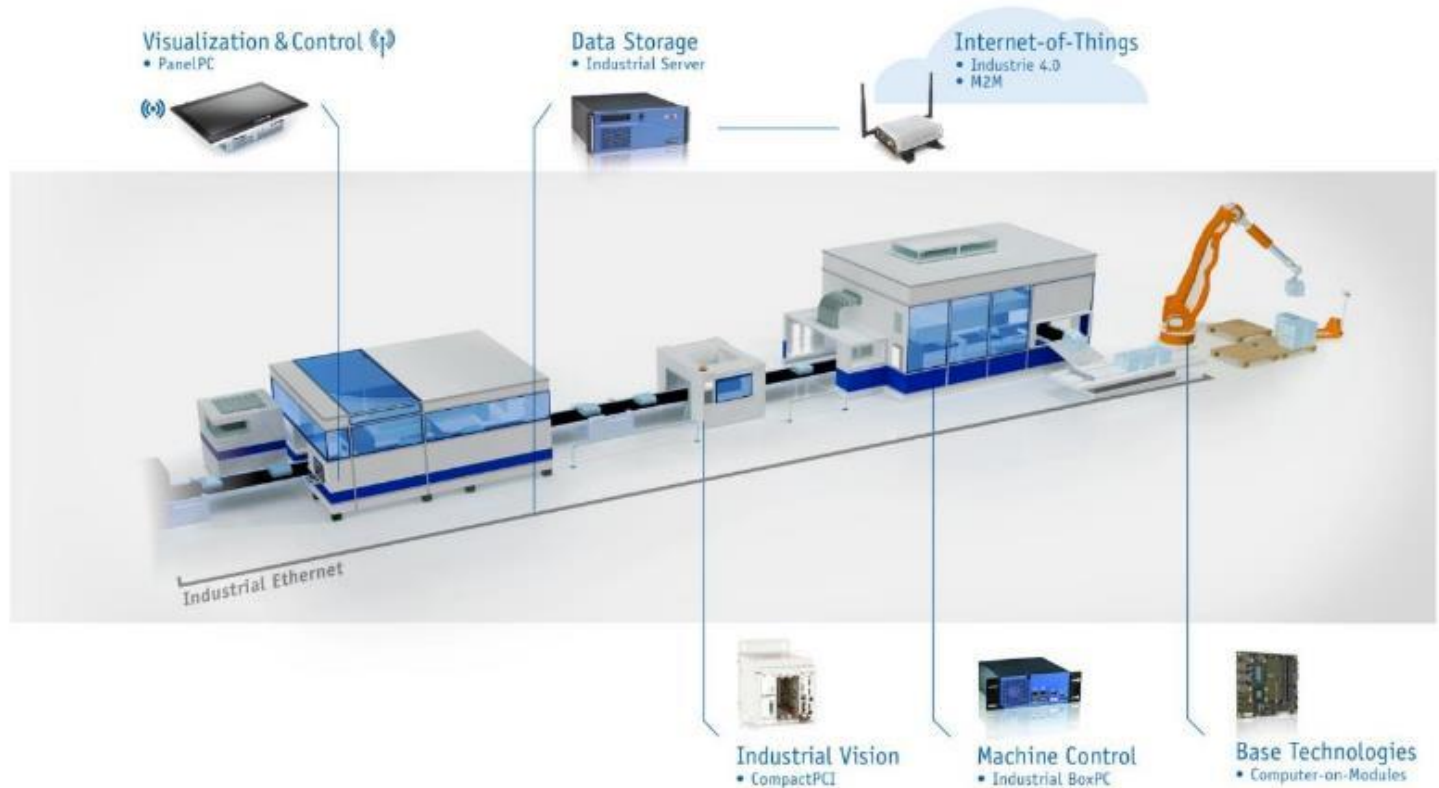- Represented in   56 countries
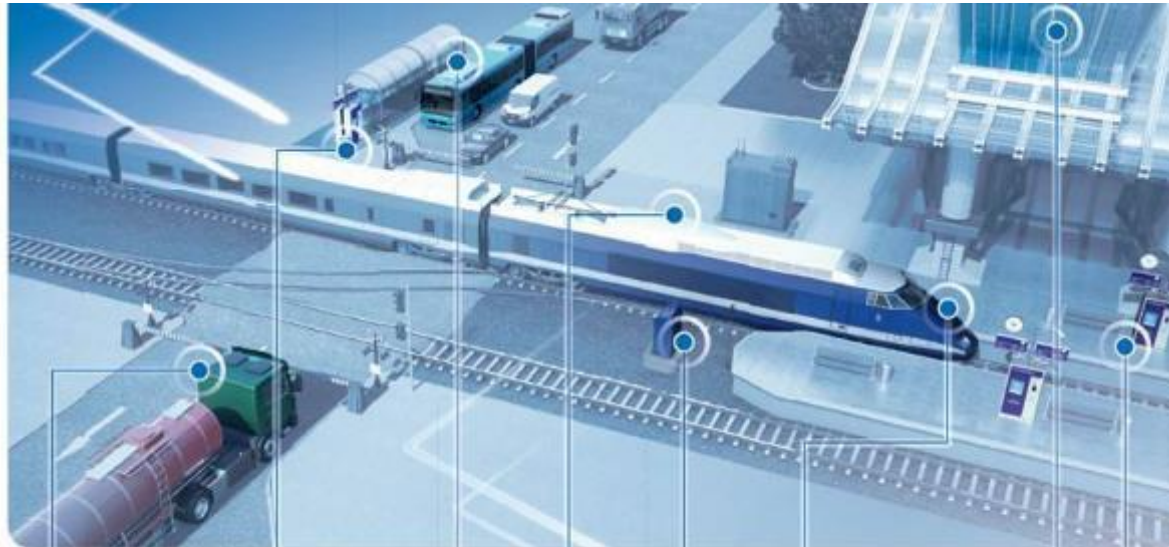 worldwide

Everyone needs (our) products

ENERGY

INDUSTRIAL AUTOMATION

INFOTAINMENT

MEDICAL

MILITARY

COMMUNICATION

TRANSPORTATION

Modules & Boards

Integrated Systems

Application Ready Platforms

Connect in Industrial Automation

Connect in Transportation

Connect in Infotainment
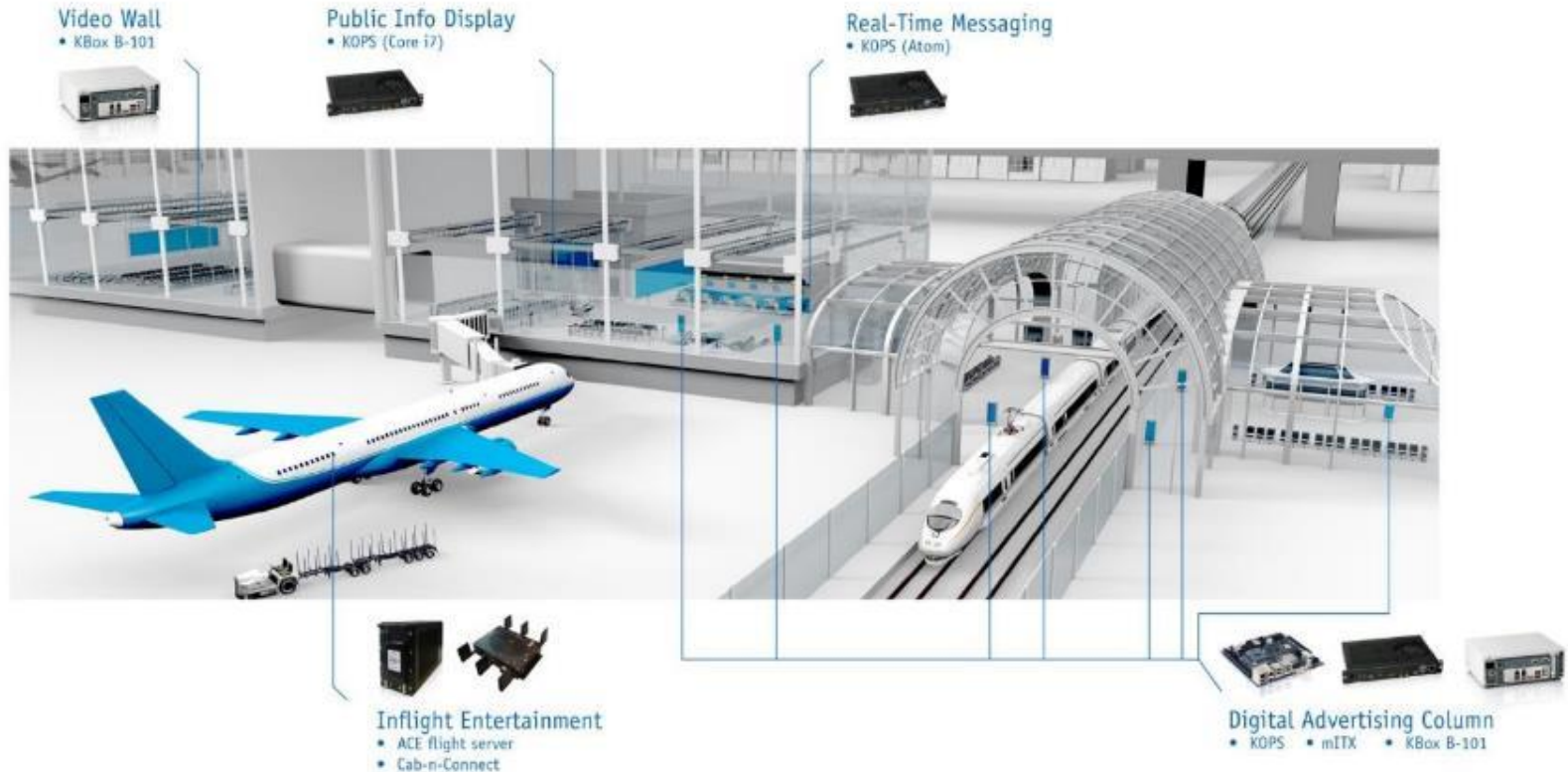
Trends in Embedded

Big Economic Impact

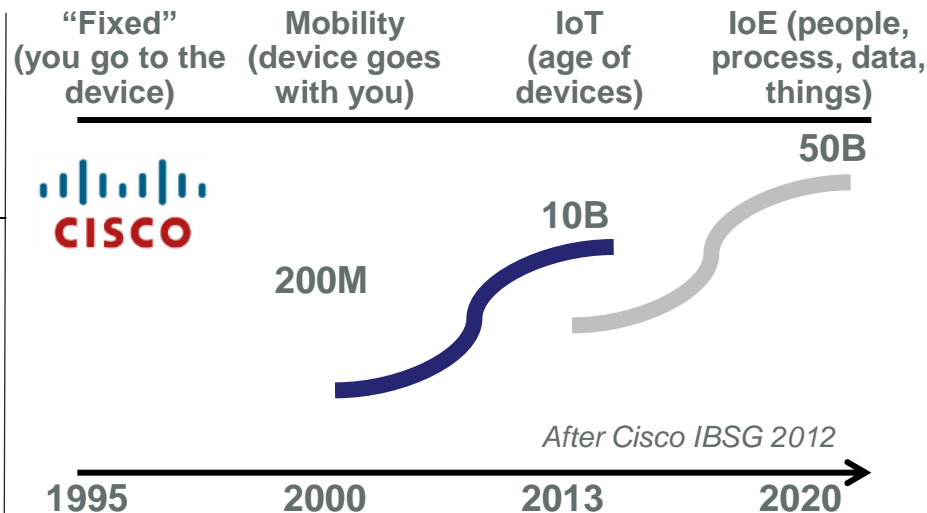IoT adds up to $15T to global GDP over the next 20 years (GE)

Services Drive Revenues & Growth

Value-added services are projected to be the largest and the fastest growning revenue sources in IoT. (Harbor Research, March 18, 2013)

"Fixed" (you go to the device)	Mobility (device goes with you)	IoT (age of devices)	IoE (people, process, data, things)

CISCO

200M

10B

50B

After Cisco IBSG 2012

1995	2000	2013	2020

Internet Inflection Points: Past & Future

On The Verge

The Smart Systems market is reaching its tipping point for dramatic growth. (Harbor Research, March 18, 2013)

Since 2008, More Devices

than People are Connected to the Internet (Cisco)

29 OKT ←
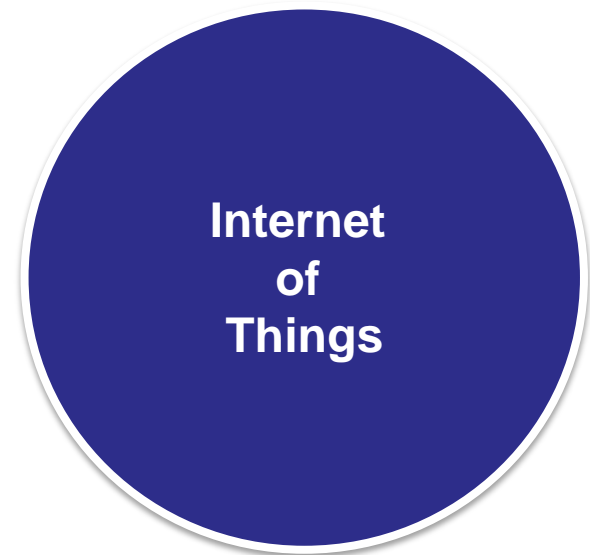1931 CONGRESCENTRUM
BRABANTHALLEN
DEN BOSCH

D&E event 2014

Why Security ?

- Proprietary OS
- Isolated network
- High development cost
- Low support cost
- Patching rare
- Limited security risk

- Generic OS
- Internet connected
- Low development cost
- Higher support cost
- Patching common
- Standard security risk

From M2M to IoT

M2M

data driven

Internet of Things

collaboration driven
by full digital integration

The challenges & the opportunity

predictive-analysis

connectivity

data-storage

trust

security

Embedded-platform

analytic-technology

data-abstraction-layer

remote-manageability

data-retrieval-performance

go-to-market

Wartungsfrei

event

processing

reliability

sensor-technology

real-time

Our Goal:

» Apply **end-to-end view** for your customers
» Leverage solutions into **multiple verticals**
» Reduce **complexity**

29 OKT ←
1931 CONGRESCENTRUM
BRABANTHALLEN
DEN BOSCH

D&E
event
2014

Precision Farming

Precision Farming

Soil sensors report data $\longrightarrow$ Get data from sensors

Load fertilization map $\longleftarrow$ Build soil geo map / fertilization planning

Auto Pilot controls vehicle $\longrightarrow$ Report / Store / Compute - Progress/Fuel consumption, fertilizer consumption, operating hours …
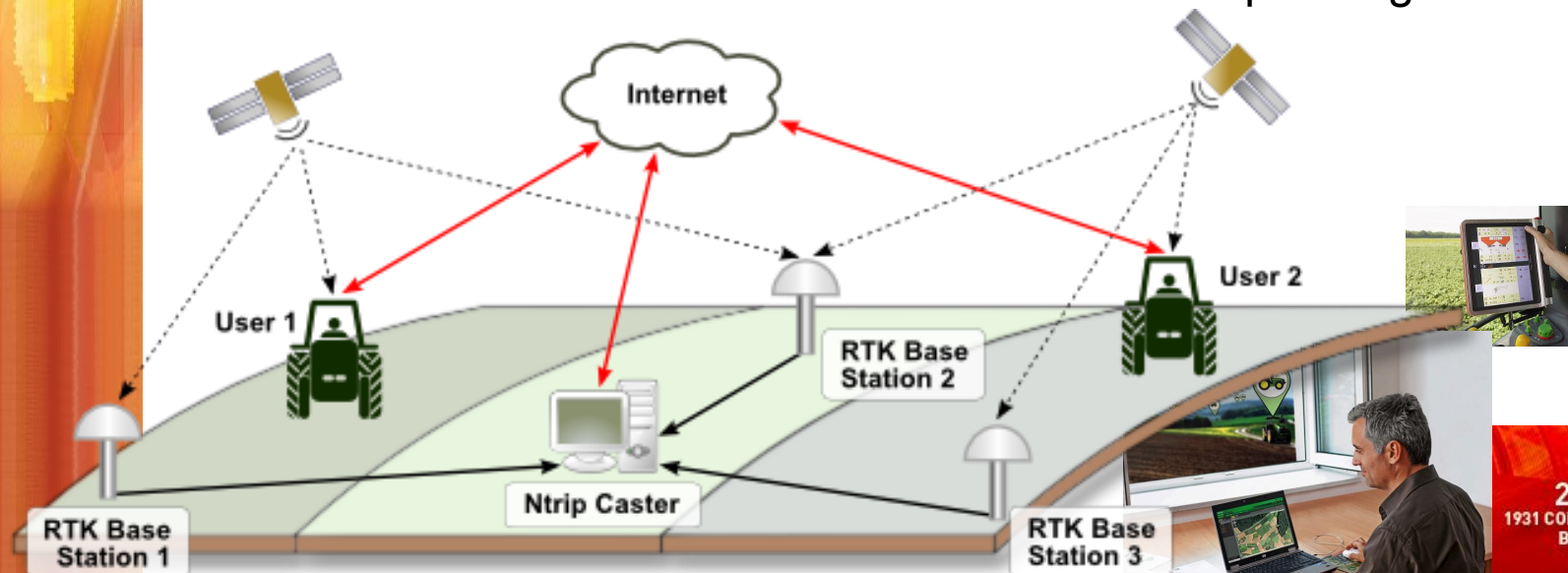
Data is money making

North America

Pesticide Cost Decrease	1B $US / Year
Yield Increase	5200 $US / 1000 Hectares / Year
Fuel Reduction	30-50%
CO2 Emission Reduction	15-25%

Data is the new currency

Is my design / product save?

Decomposition
COMe + SMARC

Am i secure?

Application software

Operating system

Bootloader
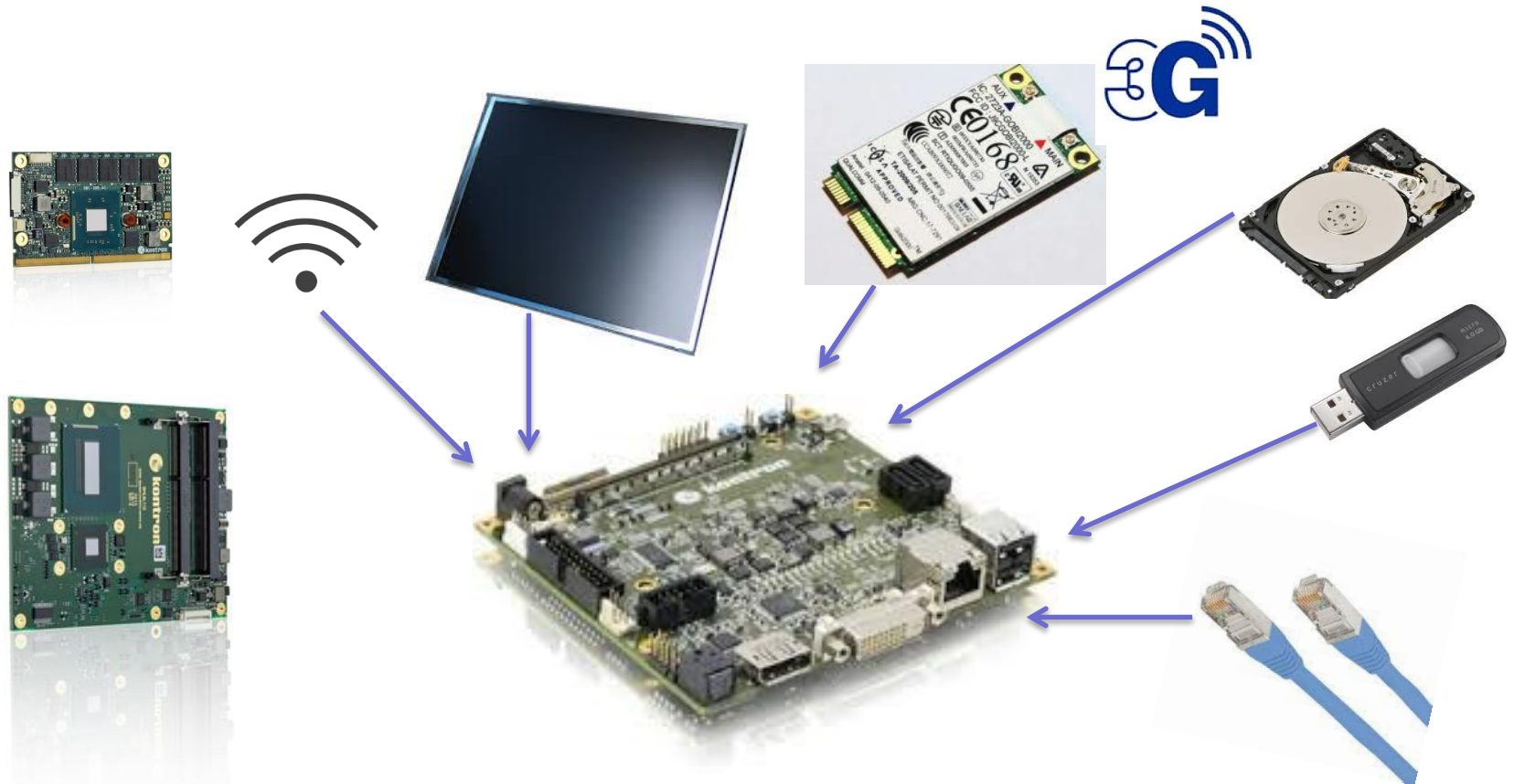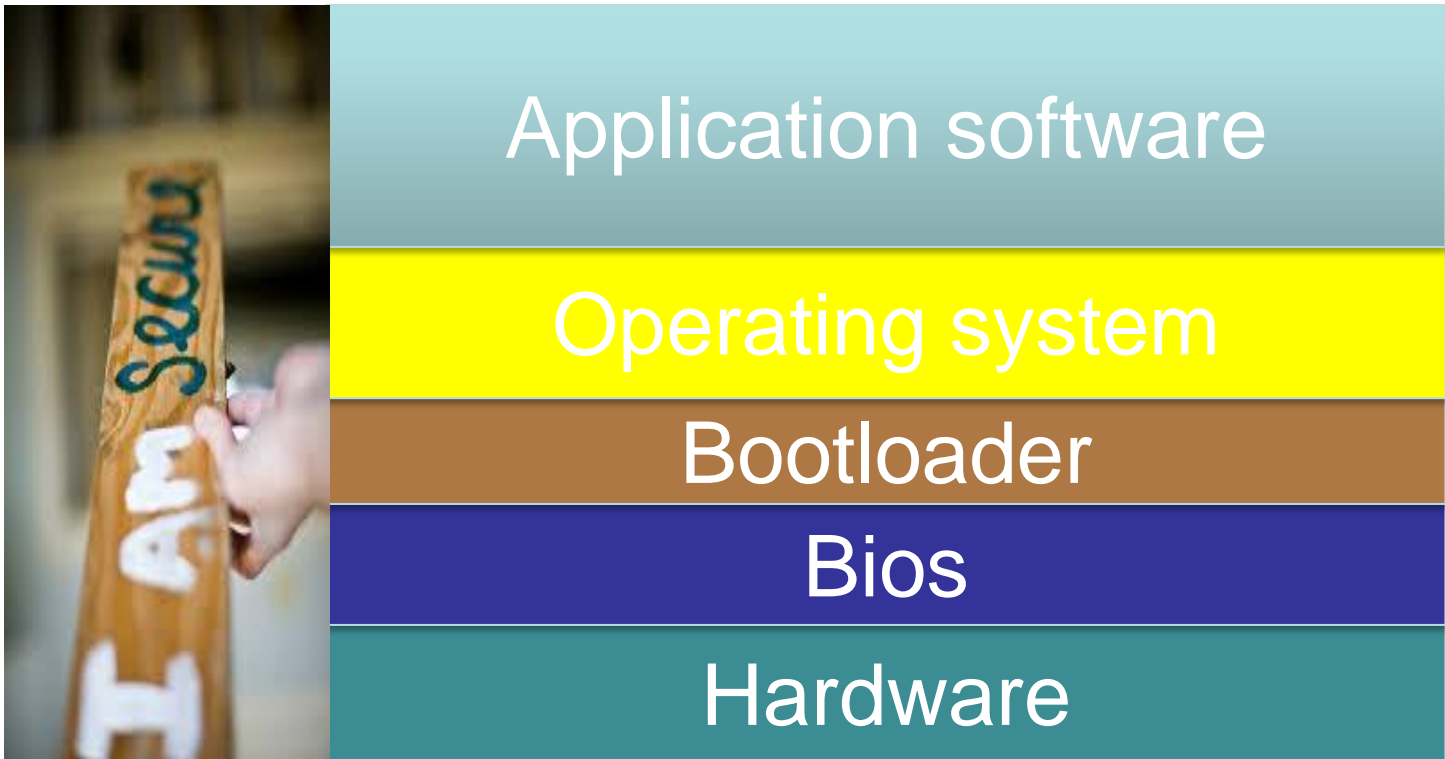
Bios
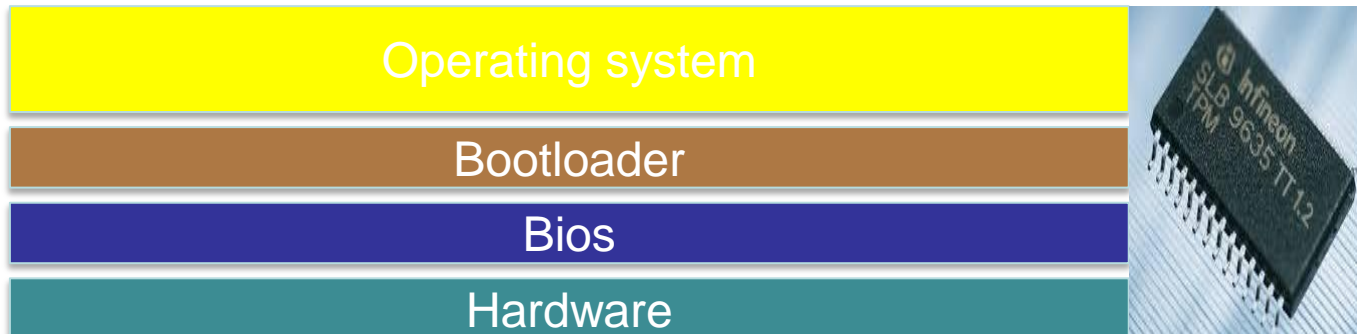
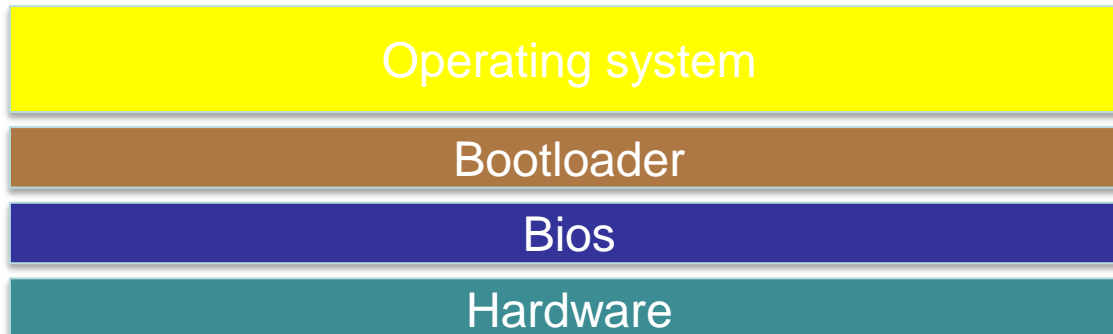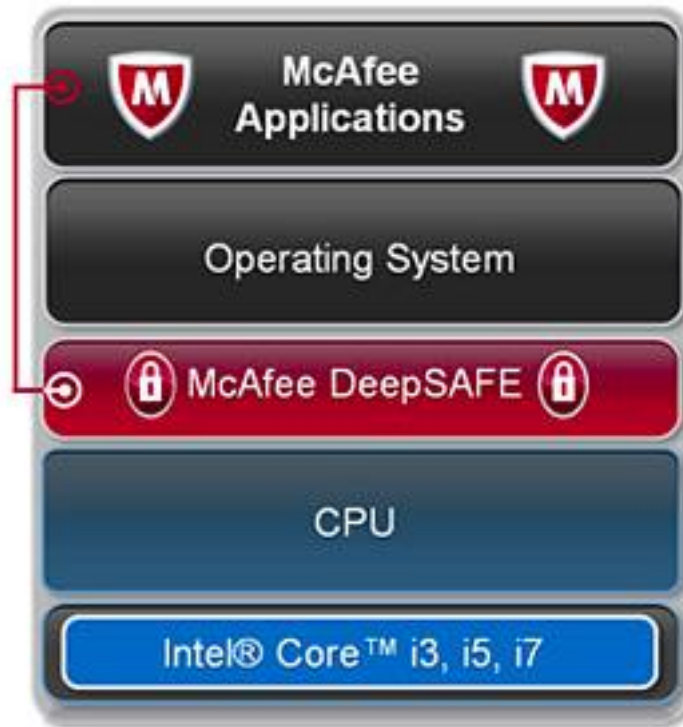Hardware

Bios adaptations

- Fast Boot 👍
- Dark boot, boot logo 👍
- Security Bios adaptations
  - Limit hardware initializations 👎
    - HDD, USB, PCIe devices
  - Add keys for operating system licenses 👎
  - Add special hardware recognition keys 👎
  - Serialnumbers, hardware recognition

TPM 1.2

- Both Software + Hardware
- Assures integrity of the platform.
- Encrypted data storage
  - Linux (dm-crypt)
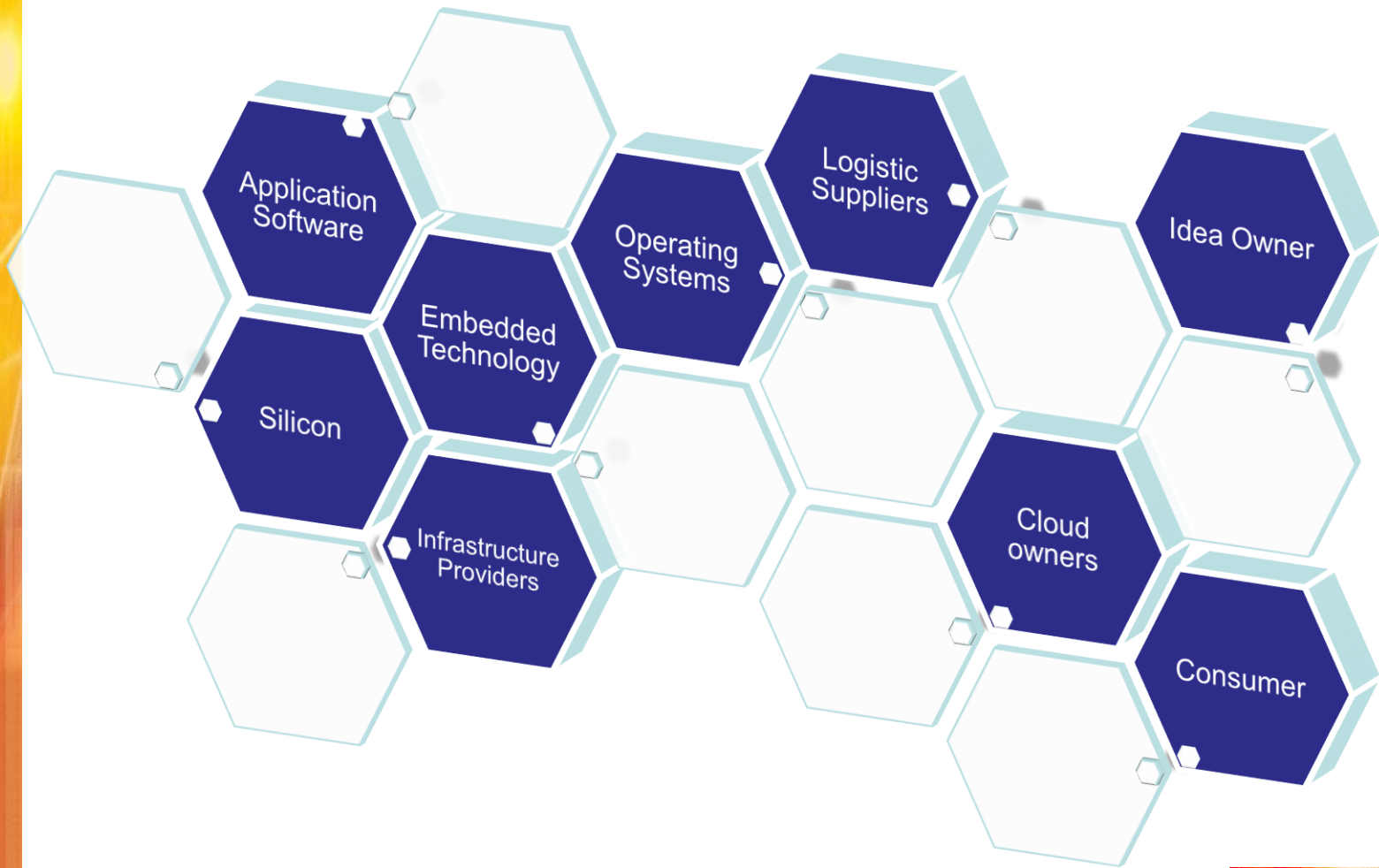 - Windows (Bitlocker)
- Encrypted password

| Operating system |
| Bootloader |
| Bios |
| Hardware |

Intel Deepsafe

Operating system	Rootkit
Bootloader	
Bios	
Hardware	

Is my communication secure?

IoT partnership

To build an E2E solution

Cloud Management	Cloudera
Data distribution services	RTI
Connectivity	Telekom
Cloud OS	Microsoft
Protection & Security	Wibu-Systems
More than Silicon	Intel

Back-end solutions

Edge solutions

# Kontron IoT/M2M
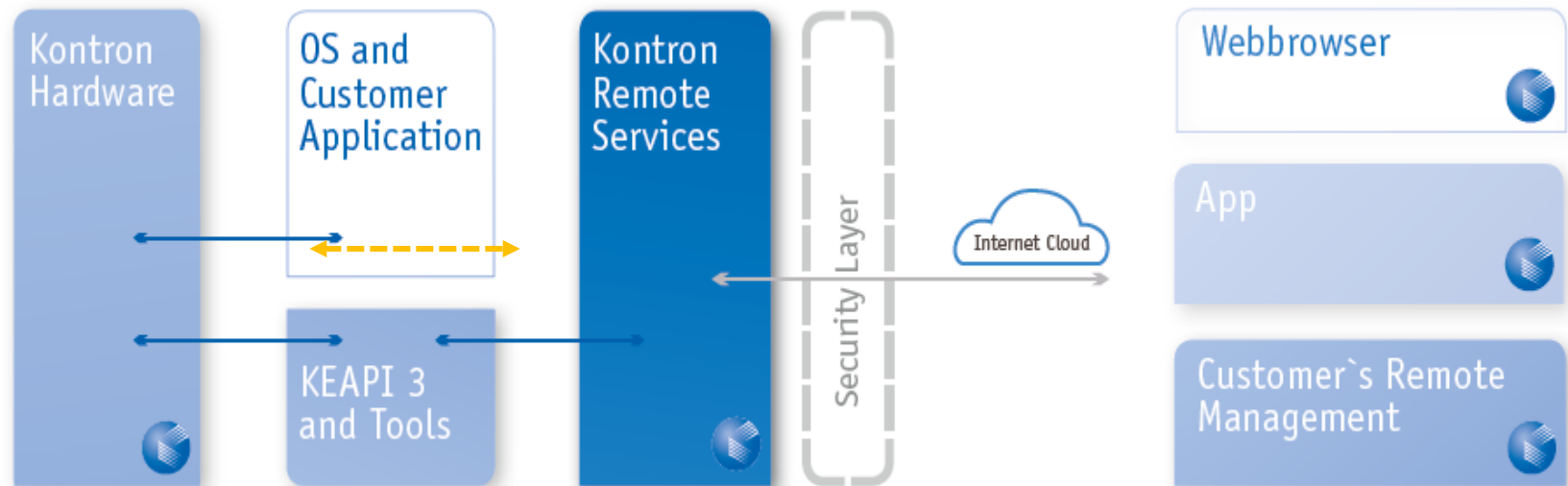
Local Installation on Kontron Hardware
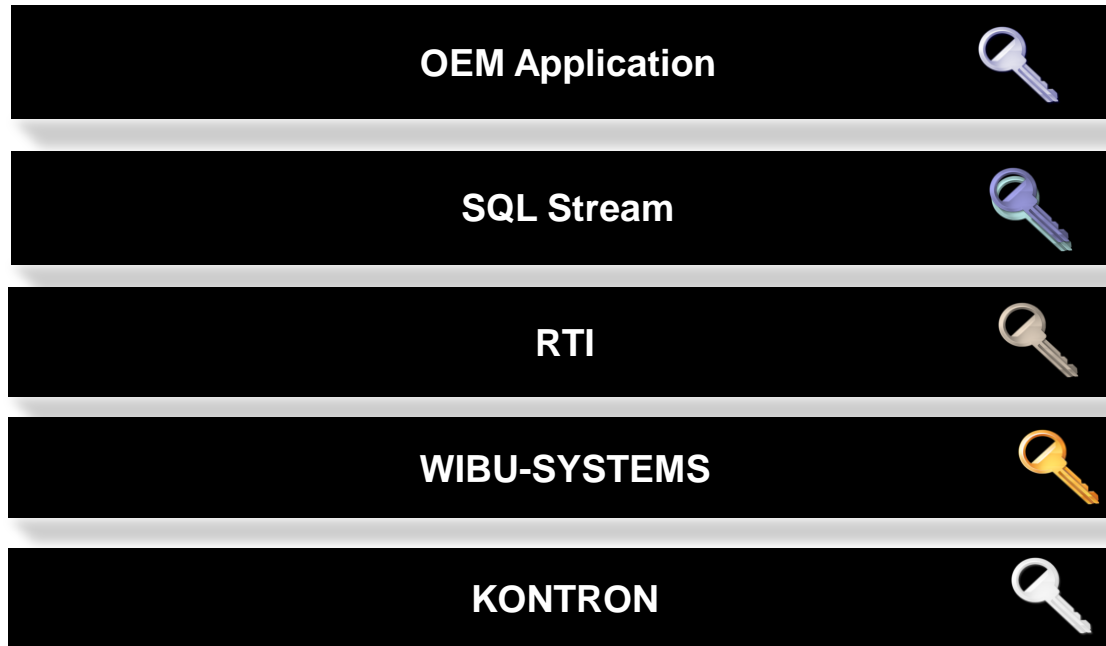
Remote Access for Management

Kontron Embedded API

» Single API in C/C++, C#/Java for hardware access

» I²C, SMBus, GPIOs, EEPROM

» PSU, Display Panel, Board information, BIOS version and more

» Additonal Tools

29 OKT ←
1931 CONGRESCENTRUM
BRABANTHALLEN
DEN BOSCH

D&E
event
2014

WIBU

IoT solution stack

OEM Application

SQL Stream

RTI

WIBU-SYSTEMS
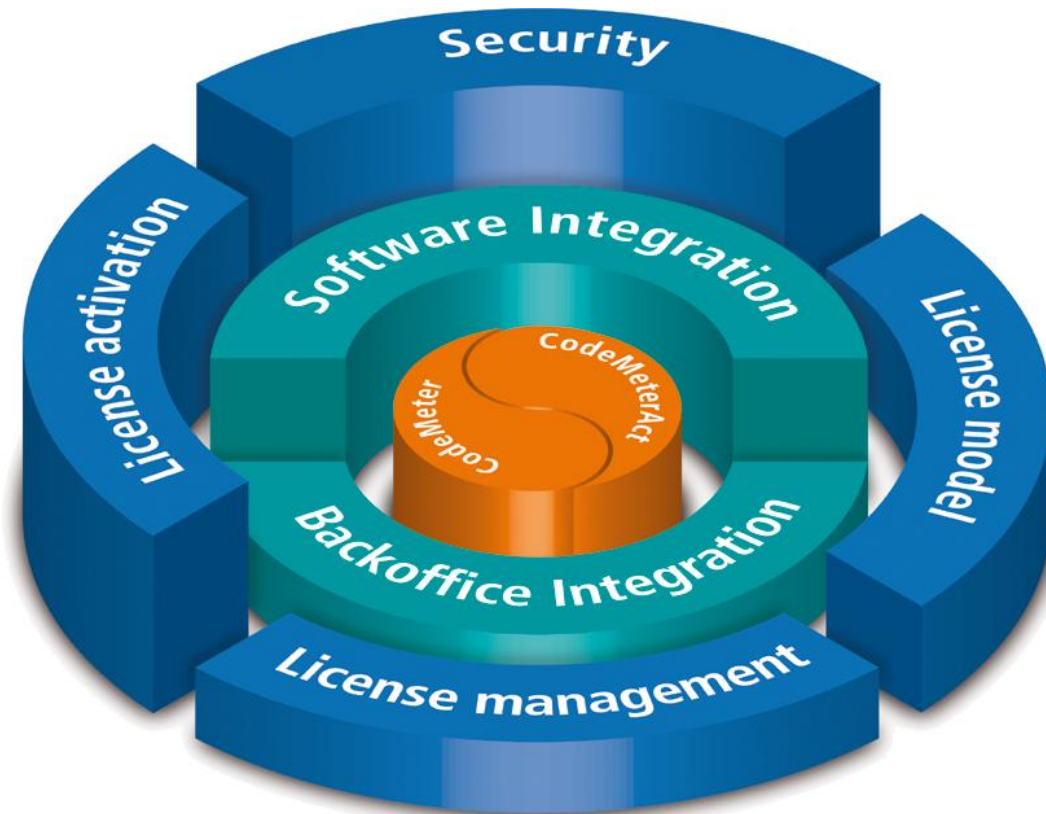
KONTRON

Remote secure Bios update
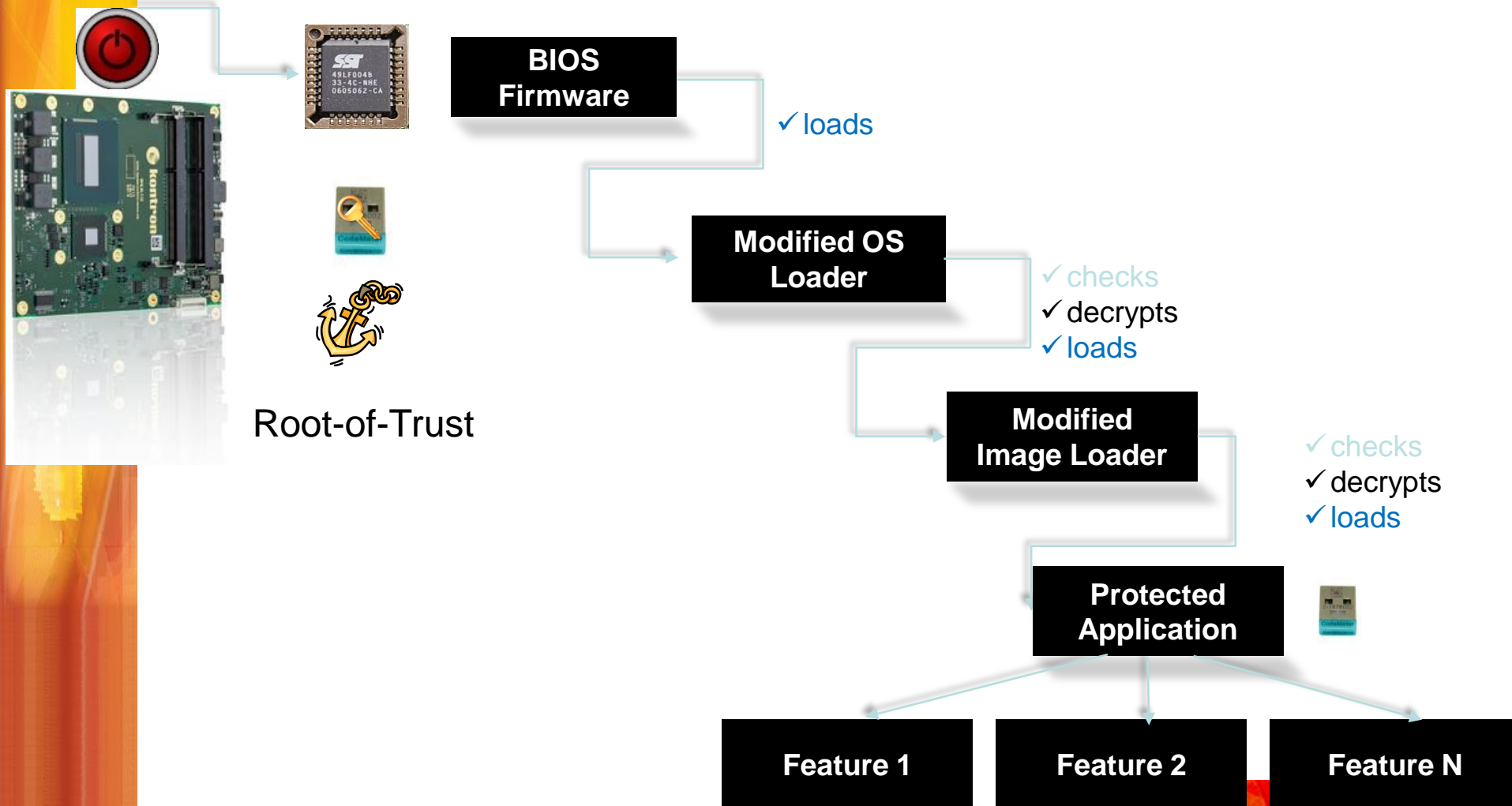

Root-of-Trust

BIOS Firmware

✓ loads

Secured Linux

✓ checks
✓ decrypts
✓ loads

Remote ROM Update Setup

✓ checks
✓ decrypts
✓ loads

Flashes Signed and Encrypted BIOS

Secure Boot

BIOS Firmware

✓ loads

Root-of-Trust

Modified OS Loader

✓ checks
✓ decrypts
✓ loads

Modified Image Loader

✓ checks
✓ decrypts
✓ loads

Protected Application

Feature 1   **Feature 2**   **Feature N**

29 OKT ←
1931 CONGRESCENTRUM
BRABANTHALLEN
DEN BOSCH

D&E
event
2014

Thank you!